LA LOGIQUE pas à pas

Jacques Duparc

Presses polytechniques et universitaires romandes

La logique pas à pas

Jacques
Duparc

LA LOGIQUE
pas à pas

PRESSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES

Illustrations de couverture: © Studro (buse), © Nemia (manchot), www.fotolia.com

La Fondation des Presses polytechniques et universitaires romandes (PPUR) publie principalement les travaux d'enseignement et de recherche de l'Ecole polytechnique fédérale de Lausanne (EPFL), des universités et des hautes écoles francophones.
Le catalogue de leurs publications peut être obtenu par courrier aux Presses polytechniques et universitaires romandes, EPFL – Rolex Learning Center, CH-1015 Lausanne, par E-Mail à ppur@epfl.ch, par téléphone au (0)21 693 41 40, ou par fax au (0)21 693 40 27.

http://www.ppur.org

ISBN 978-2-88915-126-4
© Presses polytechniques et universitaires romandes, 2015
Tous droits réservés
Reproduction, même partielle, sous quelque forme ou sur quelque support que ce soit, interdite sans l'accord écrit de l'éditeur.

Imprimé en Espagne

Table des matières

Avant-Propos

Cet ouvrage est avant tout construit dans l'idée de mettre les bases fermes de la logique à la portée des étudiants non mathématiciens. Non seulement aucun bagage mathématique n'est requis pour y entrer de plein pied, mais ce livre a été spécialement élaboré pour les étudiants entretenant une relation agitée avec les sciences et ceux à qui les mathématiques et le formalisme cassent (*a priori*) les pieds.

Pour autant, au lieu de maintenir le lecteur à distance et de ne lui proposer de la logique que quelques aperçus lointains, ce livre se propose de "faire la trace" et de le guider pas à pas afin de l'amener au cœur de la matière. Pour ce faire, aux présentations traditionnelles arides et sévères sont préférées ici des expositions modernes articulées autour de la notion d'arbre et des concepts de jeux, privilégiant à la fois l'aspect visuel et le caractère ludique des choses.

Cet ouvrage est le fruit d'un cours d'introduction à la logique dispensé à l'Université de Lausanne à des étudiants de Bachelor provenant d'horizons très variés tels que la philosophie, la psychologie, la sociologie, le management, les sciences criminelles, la théologie, etc. Il a bénéficié des bons soins des assistants suivants : Christian W. Bach, Emilie Bruchez, Jérémie Cabessa, Raphaël Carroy, Alessandro Facchini, Kevin Fournier, Camille Jaccard, Rahel Kallweit, Coline Ladetto, Jennifer Lopes, Virginie Michaud, Nathalie Michel, Aline de Montmollin, Chloé Morend, Yann Péquignot. Enfin, ce livre est également issu des influences des professeurs Erich Grädel, Jean-Louis Krivine et Wolfgang Thomas.

Préambule

> *"La logique est le dernier refuge des gens sans imagination."*
>
> Oscar Wilde[1]

Pour quelle raison des étudiants auraient-ils besoin d'un cours d'introduction à la logique ? Qu'est-ce que cela pourrait leur apporter qu'ils ne savent pas déjà ? Et puis d'abord, qu'est-ce que c'est, la logique ? Est-ce un suffixe qui permet de transformer une quelconque activité humaine en science ? Parce qu'en effet, la logique induit toute une zoologie, une ornithologie, une longue généalogie, qui donne lieu à une interminable phraséologie...

Mais laissons plutôt la parole à ces philosophes vénérés qui assurent commentaires et explications de rencontres – sportives s'entend.

- " *c'est un match nul logique...* "
- " *un résultat logique...* "
- " *une défaite amère mais logique...* "
- " *une suite logique...* "

Il y a donc de la logique dans tout ça ? Pas grand chose de scientifique pourtant, n'est-ce pas ? Qu'est-ce que peut bien vouloir dire le mot "logique" dans cette acception ? Pourquoi un match nul peut-il être qualifié de "logique" ? Est-ce que c'est au vu du match que le résultat est logique ? Est-ce que c'est dû au fait que les deux équipes ont joué de manière équilibrée de sorte qu'aucune ne l'emporte sur l'autre (ni physiquement, ni techniquement, ni stratégiquement) ? Ou bien le résultat est-il déclaré logique au vu des forces en présence avant même que le match ne se soit déroulé ? S'agissait-il de deux équipes de forces équivalentes et qui se sont ainsi neutralisées ? Quelle que soit l'interprétation, il semble bien que le mot "logique" soit ici employé pour désigner un rapport de conséquence, une relation de cause à effet, que le score reflète le match ou les forces relatives des équipes. Le résultat était ainsi conforme à l'équilibre des forces, il était inéluctable, inévitable, à moins d'une grosse surprise. En un sens, on peut dire que cette interprétation comme rapport de conséquence est bien au cœur de la logique. Des causes et des principes provoquent répercussions et effets. Certaines choses *entraînent*, *impliquent*, *produisent*, *ont pour résultat* d'autres choses. Cette relation entre ce qui précède et ce qui succède est le rapport de conséquence.

1. *"Consistency is the Last Refuge of the Unimaginative."* Oscar Wilde, in *Conversation.*

C'est ce même rapport de conséquence, ce lien de cause à effet qui est encore présent dans les expressions suivantes :

- “ *la logique libérale...* ”
- “ *la logique capitaliste...* ”
- “ *la logique de l'honneur...* ”
- “ *la logique de l'action sociale...* ”
- “ *la logique de la désobéissance...* ”,
- “ *la logique du tueur...* ”
- “ *la logique du pire...* ”

Soit des principes entraînent des conséquences, soit des conséquences induisent des principes dont ils sont précisément la conséquence. Pourtant quelque chose d'autre transparaît dans ces utilisations du mot “logique”. Il y a comme une connexion étroite des éléments, une cohérence des idées qui ne met pas en jeu uniquement un rapport de conséquence, mais tous les rapports de conséquence possibles. Ainsi, *la logique libérale* fait intervenir non seulement les principes du libéralisme, mais aussi tout ce qui peut s'en déduire, l'ensemble des conséquences d'un mode de raisonnement.

La logique traite de formes de raisonnements. Elle ne s'intéresse pas tant au contenu qu'au squelette, à ce qui fait qu'un discours argumenté tienne debout. Si l'on pousse un peu cette métaphore, la logique décrit les articulations du discours, les superpositions d'arguments, qui eux-mêmes reposent sur des membres solidement ancrés dans le sol. L'humain est certes un animal bipède, mais surtout raisonnable, et la logique exhibe la structure de ces raisonnements, l'architecture des ponts de la pensée qui relient les unes aux autres les assertions déployées dans le discours.

Sous cette perspective, la logique met à jour le cadre, la structure – et procure également les outils – de la pensée dite *déductive*, en ce qu'elle s'occupe de déductions ou encore de démonstrations. C'est en effet en tant qu'art du bien raisonner, doctrine de la déduction, matière des démonstrations rigoureuses et discipline de la mécanisation des preuves que la logique est le plus généralement présentée.

> *“If I claim full justice for my art, it is because it is an impersonal thing – a thing beyond myself. Crime is common. Logic is rare. Therefore it is upon the logic rather than upon the crime that you should dwell. You have degraded what should have been a course of lectures into a series of tales.”*
>
> Sherlock Holmes, *The Adventure of the Copper Beeches*, [DP75].

Pourtant, la logique n'est pas seulement le domaine de la mécanique des démonstrations, c'est aussi le règne de l'imagination exubérante. C'est le lieu des interprétations, de la signification des énoncés, celui des modèles et des mondes possibles. Tout un univers imaginaire est ainsi convoqué pour donner sens aux énoncés. C'est ce que l'on retrouve en anglais dans l'expression *“it makes sense”* que l'on traduit souvent par *“c'est logique”*.

Ainsi, la logique se construit dans l'opposition entre *syntaxe* et *sémantique* :

- La *syntaxe* est le monde des symboles, de ces “coquilles vides” que manipulent les ordinateurs. C'est le lieu des opérations grammaticales indemnes de tout contenu, dépourvues de sens.
- La *sémantique* c'est au contraire le lieu des interprétations et des réalisations, des modèles ou mondes possibles là où toute la syntaxe “prend corps”. C'est le lieu de la signification.

Pour autant, cette dichotomie ne renvoie pas à deux visions de la logique. *Syntaxe* et *sémantique* sont comme deux faces d'une même feuille de papier. Ce sont deux axes différents qui permettent, dans l'entre-deux qu'ils génèrent, de faire faire apparaître le *sens*. Cette opposition, entre syntaxe d'une part et sémantique d'autre part, est ainsi semblable à celle que l'on trouve en linguistique entre *signifiant* (l'image acoustique d'un mot) et *signifié* (le concept, c'est-à-dire la représentation mentale d'une chose).

Une présentation métaphorique de la logique

1. Syntaxe

Une logique débute par la donnée de ce que l'on appelle un *langage*. C'est-à-dire précisément la mise à disposition d'un ensemble de symboles comme par exemple ceux-ci :

$$P,\ \exists,\ Q,\ \wedge,\ \longrightarrow,\ \neg,\ \Diamond,\ \Box,\ ),\ (,\ P_0,\ \vee,\ \longleftrightarrow,\ \forall,\ \ldots$$

De manière métaphorique, un langage fonctionne pour la logique comme des mots pour la langue courante. Ce sont les briques avec lesquelles on construit l'entier de l'édifice. Et précisément, que fait-on avec des mots ? On les met bout-à-bout pour en faire des phrases.

Du côté de la logique, l'équivalent des phrases s'appelle des *formules*. De la même manière que les phrases sont des mots les uns à la suite des autres – mais pas disposés n'importe comment ! –, les formules sont des suites d'éléments du langage, autrement dit, des suites de symboles, disposés selon des règles de construction précises. Par exemple *"table de joue huître l'tennis au hystérique"* n'est pas une phrase, au contraire de "*l'huître hystérique joue au tennis de table*". Du côté des formules, cela donne quelque chose comme "$\wedge P)(Q$" n'est pas une formule, au contraire de "$(P \wedge Q)$" qui en est une.

Ainsi, une phrase est un *énoncé bien formé*, une suite de mots correctement agencés, disposés suivant des règles grammaticales précises qui concourent à la production des phrases. De manière similaire, toute logique comprend la donnée de règles de construction qui permettent de distinguer, parmi les suites quelconques de symboles du langage, celles qui forment des formules et celles qui n'en sont pas.

Pour plus de précision encore, il nous faudrait pousser cette métaphore de la production des phrases jusqu'à la voir fonctionner dans un langage dont la signification nous serait inconnue. Sur la base d'un manuel de grammaire et la donnée de mots de base – dont nous ne connaîtrions pas pour autant la signification – nous pourrions très bien construire des phrases qui soient tout à fait correctes d'un point de vue grammatical, mais que nous ne comprendrions pas pour autant. Car la signification des formules vient avec leur interprétation. Or celle-ci relève du champ sémantique et non pas du champ syntaxique.

Que faisons-nous dès lors que nous avons des phrases à notre disposition ? Dans la langue courante nous construisons de beaux discours. Nous rédigeons des traités. Cela signifie simplement que nous prenons un certain nombre de phrases et les mettons les unes à la suite des autres. Nous les rassemblons pour en faire... et bien disons, pourquoi pas ? Un livre !

Du côté de la logique, une fois que nous avons des formules à disposition, nous faisons sensiblement la même chose. En effet, nous en prenons un certain nombre – et parfois même une infinité – et nous les rassemblons pour en faire un beau paquet que nous appelons une *théorie*. Une théorie n'est donc ni plus ni moins qu'un ensemble de formules – de la même manière que le livre *Le Petit Prince* n'est qu'un ensemble de phrases –, avec toutefois la différence notoire que l'ordre dans lequel les phrases se succèdent dans le livre a une importance capitale, alors que l'ordre des formules dans une théorie n'en a pas. C'est d'ailleurs pour cela qu'une théorie n'est qu'un *ensemble* de formules et non une *suite* de formules. Et un *ensemble* n'est autre qu'un *sac* dont le contenu est anarchique, c'est-à-dire sans ordre, sans prééminence. Deux ensembles qui contiendraient les mêmes formules n'en forment en réalité qu'un seul, alors que deux livres qui contiendraient les mêmes phrases mais ordonnées différemment seraient différents.

2. Sémantique

Et maintenant, que faisons-nous lorsque nous avons un livre en notre possession ? Afin que la métaphore soit précise, supposons que ce livre soit en fait un scénario. Que pouvons-nous faire de ce scénario – autrement dit de cette théorie ? D'un point de vue logique, nous avons la possibilité de nous engager dans deux directions très différentes. Nous pouvons d'une part rester dans le champ syntaxique et nous intéresser à ce que nous pouvons *déduire* de notre théorie. Ou d'autre part, nous pouvons quitter le champ syntaxique pour rejoindre le champ *sémantique*. Pour filer l'image du scénario, cette dernière attitude – celle qui consiste à investir le champ sémantique – amènera à *réaliser* ce scénario, autrement dit à l'interpréter sous la forme d'un film. Mais en général, le film n'est pas dicté par le scénario. Il existe le plus souvent non pas un film unique, mais bien une multitude de films qui puissent être issus d'un même scénario. En effet, un bon nombre de choses qui se dévoilent dans une production cinématographique ne sont pas consignées dans le scénario, à commencer par le choix des acteurs. Et même si le choix de chaque acteur est inscrit dans le scénario ou que le scénario soit encore plus précis que cela, il restera le plus souvent des éléments indéterminés, comme par exemple la couleur des lacets des chaussures de l'actrice principale dans la dernière scène. Ainsi il pourrait y avoir un film qui respecte scrupuleusement cet unique scénario dans lequel les lacets en question sont noirs, et un autre tout aussi rigoureusement fidèle dans lequel les lacets sont gris. Bien sûr, dans l'absolu, il se pourrait que le scénario soit si précis, qu'il contienne un *story-board* tellement minutieux, que chaque détail y soit consigné avec la plus extrême attention, et alors un seul et unique film serait désormais conforme à ce scénario. Mais dans la plupart des cas, les variations sont des plus nombreuses.

Il en va de même avec l'interprétation d'une théorie. Tout comme le scénario peut engendrer différents films, une théorie donne lieu à différents *modèles* ; chacun d'eux fonctionnant comme un *monde possible*, une *réalisation* de ce qui se trouve consigné dans le scénario. Dès lors, on voit que ce que nous appelons "le sens" de la théorie – ou celui du scénario – n'est autre que la variété des modèles qu'elle engendre, comme autant de films possibles se détachant sur le fond de tous ceux qui ne conviennent pas.

3. Syntaxe encore

Au lieu de nous engager dans la voie sémantique à partir de ce scénario – autrement dit de cette théorie –, nous pouvons demeurer dans le domaine syntaxique. Dès lors, nous n'allons pas nous intéresser aux films possibles, ni regarder des interprétations de notre scénario. Bien au contraire, nous allons nous cantonner à l'aspect discursif de notre texte. Et que pouvons-nous faire, qui ne relève pas de l'interprétation, lorsque nous restons en quelque sorte "englués" dans le texte ? Et bien tout simplement des *déductions* et des *démonstrations*. Entièrement située dans le champ syntaxique, l'entreprise de déduction concerne tout ce qui s'occupe des liens entre la théorie et ses implications, et ce qu'on peut déduire à partir d'elle et ce qui en découle. Ainsi pour prendre un exemple métaphorique et en considérant que notre théorie n'est autre que le livre *Le Petit Prince* de Saint-Exupéry, à partir des formules – bien évidemment des phrases – suivantes :

> *"Ainsi le petit prince apprivoisa le renard.*
> *Et quand l'heure du départ fut proche*
> *Ah ! dit le renard... Je pleurerai.*
> *C'est ta faute, dit le petit prince, je ne te souhaitais point de mal,*
> *mais tu as voulu que je t'apprivoise...*
> *Bien sûr, dit le renard.*
> *Mais, tu vas pleurer ! dit le petit prince.*
> *Bien sûr, dit le renard.*
> *Alors tu n'y gagnes rien !*
> *J'y gagne, dit le renard, à cause de la couleur des blés."*
>
> Antoine de Saint-Exupéry, *Le Petit Prince* [dSE99].

Avec un peu de perspicacité, nous pouvons déduire de ce petit texte que la couleur des cheveux du petit prince et celle des blés sont identiques. Par contre, nous n'avons aucun moyen d'en déduire que le petit prince ne reverra plus jamais le renard. Nous ne pouvons pas non plus en déduire le contraire, à savoir que le petit prince reverra bien un jour le renard. Les deux possibilités restent ouvertes. Un certain nombre de choses sont des conséquences du texte. Elles procèdent de ce qui est décrit. Un bon nombre d'autres choses par contre ne peuvent en être déduites. Elles demeurent ainsi dans l'indétermination.

4. Syntaxe et sémantique réconciliées

L'idée générale d'une sémantique – et ce pour une logique quelconque – est d'interpréter les symboles de base, de leur donner un sens en les faisant correspondre à des entités variées. Ensuite, à partir de l'interprétation de ces briques de base, on passe à l'interprétation des formules qui, elles, ne sont rapportées qu'au vrai ou au faux. Intuitivement, une formule dit quelque chose d'un monde possible, elle en est une description partielle – comme la phrase d'un livre ou l'indication d'un scénario s'illustrent dans un détail. Puis, une théorie n'étant qu'un ensemble de formules, elle est interprétée par des *modèles*, ou univers possibles, qui ne sont autres que les mondes qu'elle décrit.

Utilisons à nouveau le livre du *Petit Prince* pour exemplifier à nouveau métaphoriquement notre théorie. Un *modèle* du *Petit Prince* serait un film, exactement comme celui que nous imaginons dans notre tête lors de la lecture du livre. Il en serait la réalisation. Un film tiré du *Petit Prince* consiste à faire correspondre au personnage du petit prince un véritable acteur, à faire correspondre au renard un vrai renard, *etc.* Mais quand bien même il s'agirait d'un film qui soit au plus proche au texte, il se trouve d'innombrables manières de tourner un film à partir du *Petit Prince*, et donc autant de réalisations possibles.

Nous pouvons ainsi bénéficier de plusieurs modèles d'une théorie, comme plusieurs films extraits du *Petit Prince*, par exemple :

- un film dans lequel le petit prince rencontre le renard sur sa planète des années après,
- un autre dans lequel le renard se laisse mourir de chagrin après le départ du petit prince.

Autrement dit, s'il y a une formule qui n'est pas déductible de ma théorie et telle que sa négation ne l'est pas non plus, alors ma théorie admet au moins deux modèles : l'un dans lequel cette formule est vérifiée, et l'autre dans lequel elle est invalidée.

Par contre si nous pouvons déduire une formule de notre théorie, alors tout modèle de cette théorie verra également cette formule satisfaite. Ainsi, dans tout film tiré du *Petit Prince*, la couleur des champs de blé doit être la même que celle des cheveux du petit prince. Même si dans l'un de ces films les champs de blé sont violets à pois verts !

Tout ce que nous pouvons déduire de notre théorie doit se retrouver dans les interprétations que nous en faisons. Nous ne pouvons concevoir un film qui soit fidèle au *Petit Prince* mais dans lequel le personnage du petit prince serait brun et les blés seraient blonds. C'est là une exigence de liaison harmonieuse entre syntaxe et sémantique : si un fait est prouvable, démontrable, déductible à partir d'une théorie, alors il doit être présent dans tous les modèles de cette théorie. Si une formule est conséquence de notre théorie, alors elle doit être réalisée dans tout modèle de cette même théorie. Mais cette relation harmonieuse entre syntaxe et sémantique ne s'arrête pas là. Chose plus étonnante encore, l'inverse est également vrai. Si dans tous les modèles que nous pouvons concevoir, une même formule est toujours vérifiée, alors cette formule doit être prouvable à partir de la théorie. Si dans tous les films que nous pouvons imaginer, tout en respectant scrupuleusement les indications du scénario, un même fait est avéré, alors ce fait est une conséquence des consignes du scénario. L'idée étant que si ce fait en question n'était pas une conséquence du scénario, alors nous pourrions envisager au moins deux films différents : l'un dans lequel ce fait serait vérifié, et l'autre dans lequel il serait infirmé. Cette correspondance entre le domaine des preuves syntaxiques et celui des réalisations sémantiques fonctionne dans les deux directions. L'écart entre syntaxe et sémantique ménage un lieu où le sens voit le jour et où il croît ensuite dans le va-et-vient de cette correspondance bidirectionnelle.

Dès lors une question surgit : que se passe-t-il lorsque nous pouvons à la fois déduire une formule et la négation de celle-ci (c'est-à-dire son contraire) à partir d'une même théorie ? Que se passe-t-il si, d'un même scénario, nous concluons à deux faits ou événements qui se contredisent ? Il semble en effet bien difficile de réaliser un film qui doit satisfaire quelque chose et son contraire. Dans la littérature traditionnelle, ce drame porte un nom : la contradiction. Et ce drame doit être à tout prix évité. Pour cela, rien de tel qu'une loi : la *loi de non contradiction*. Elle porte sur ce qui ne devrait pas avoir lieu, elle légifère à propos d'un phénomène qu'il faudrait à tout prix éviter. Mais laissons cette vision "légaliste" des choses de côté. Si nous pouvons déduire une formule et sa négation – une assertion et son contraire – cela a pour conséquence deux phénomènes distincts, suivant que l'on considère l'aspect syntaxique ou l'aspect sémantique de la théorie.

Dans le champ syntaxique – du point de vue déductif – la conséquence est que nous pouvons dès lors déduire toutes les formules que nous voulons. Tout devient prouvable, démontrable, sans aucune restriction. Une telle théorie est appelée *contradictoire* ou *incohérente*. De manière métaphorique, cela veut dire que si d'un livre je peux déduire deux phrases qui se contredisent, alors de cette contradiction je peux en conclure tout ce qui me passe par la tête, je peux absolument tout dire. Mais bien évidemment, si je peux tout dire, alors plus rien n'a de sens, puisque je peux dire à la fois n'importe quoi et son contraire.

Dans le champ sémantique, la conséquence est radicale dans un autre sens. En effet, si nous pouvons déduire à la fois quelque chose et son contraire d'une théorie, alors ces deux choses doivent se trouver dans tous les modèles de notre théorie. Par conséquent, chaque film particulier doit satisfaire à la fois cette chose démontrée et son contraire. Mais comment réaliser cela ? Comment un même film pourrait-il mettre en scène un fait et le contraire exact de celui-ci ? Comment pourrait-il faire co-exister deux réalités qui se contredisent ? C'est bien évidemment impossible. Il semble donc que nous soyons confrontés à un problème insoluble. D'une part tous les films produits à partir d'un scénario doivent satisfaire ce qu'il s'en peut être déduit, et d'autre part, tout et n'importe quoi peuvent être déduits (puisque deux choses contradictoires). Il n'existe dès lors qu'une seule solution : il n'y a en réalité aucun film qui soit conforme au scénario. Ainsi il est bien vrai que dans chaque film que nous pouvons réaliser tout ce qui est déductible du scénario soit vérifié puisqu'il n'y a aucun film à considérer. Une théorie contradictoire n'a tout simplement pas de sens, puisque nous ne pouvons lui donner une signification quelconque et ce, pour la bonne raison qu'il est impossible de l'interpréter. Si, du point de vue syntaxique, une théorie qui se contredit est appelée *contradictoire* ou *incohérente*, du point de vue sémantique, elle est dite *inconsistante* puisqu'elle ne correspond à rien, elle ne se réalise en rien, elle ne "consiste" en rien.

Pour le redire de nouveau : puisque tout ce qui peut être déduit d'une théorie devrait être vérifié dans chacun de ses modèles, il en va de même d'une théorie contradictoire. Or, cela signifie précisément que tout et son contraire devraient être vérifiés dans chacun de ses modèles. En conséquence, de tels modèles n'existent tout simplement pas. Ainsi, une théorie inconsistante (contradictoire) est une théorie à la fois extrêmement riche au niveau de la syntaxe, puisqu'on y peut prouver tout ce que l'on veut, mais extrêmement pauvre au niveau de la sémantique, puisqu'elle n'admet aucune interprétation. D'un coté, on peut tout dire à partir d'une théorie contradictoire car l'on peut tout prouver, mais de l'autre – et précisément parce que l'on peut tout dire – plus rien n'a de sens, plus rien n'a de signification.

Introduction

1. Une minuscule histoire de la logique

Si des arguments logiques étaient déjà connus et employés par des mathématiciens grecs tels que Thalès de Milet (625 – 547 av. J.-C) ou Pythagore de Samos (580 – 497 av. J.-C), ou par des philosophes comme Platon d'Athènes (428/427 - 347/346 av. J.-C.), celui unanimement considéré comme le père fondateur de la logique est Aristote de Stagire (384 – 322 av. J.-C). Pour développer sa logique, Aristote s'appuie sur le modèle de rigueur scientifique en vogue à l'époque : la mathématique ou plus précisément la géométrie [2]. Cette même géométrie est consignée par Euclide (325 – 265 av. J.-C) dans les *Éléments* [Euc90] – une sorte de compilation du savoir géométrique qui demeurent pendant près de deux millénaires au cœur de l'enseignement mathématique comme un modèle de rectitude et de précision pour de très nombreux philosophes [3].

S'appuyant sur les types d'argumentations à l'œuvre dans la géométrie de son temps, et mettant à jour des méthodes de démonstrations restées implicites, Aristote a rédigé divers traités de logique que la tradition scolastique a rassemblés en un ouvrage intitulé *Organon* [Ari70, Ari92, Ari95, Ari97, Ari00] [4]. Il représente un exposé systématique des formes de la pensée démonstrative sous forme de six traités :

(1) *Les Catégories* : une analyse des termes, les éléments les plus simples des propositions.

(2) *De l'Interprétation* : une analyse des énoncés.

(3) *Premiers Analytiques* [5] : un exposé des règles et des formes de la démonstration syllogistique, des conditions formelles auxquelles toute preuve est subordonnée.

(4) *Seconds Analytiques* [6] : pièce maîtresse de la logique d'Aristote qui expose la méthode démonstrative appelée syllogistique, fondée sur des prémisses nécessaires et qui aboutit, grâce à cette science démonstrative, à des conclusions elles aussi nécessaires [7].

---

2. *"Que nul n'entre s'il n'est géomètre"* est une phrase dont la tradition veut qu'elle ait été gravée à l'entrée de l'Académie, l'école fondée à Athènes par Platon.

3. *"On peut avoir trois principaux objets dans l'étude de la vérité : l'un, de la découvrir quand on la cherche ; l'autre, de la démontrer quand on la possède ; le dernier, de la discerner d'avec le faux quand on l'examine. [. . .] La géométrie, qui excelle en ces trois genres. . . "*, Blaise Pascal, *Réflexions sur la géométrie en général. De l'esprit géométrique et de l'art de persuader* [Pas79], vers 1657-58.

4. *Outil* ou *instrument* en grec ancien.

5. *"Il faut d'abord établir quel est le sujet de notre enquête et de quelle discipline elle relève : son sujet c'est la démonstration, et c'est la science démonstrative dont elle dépend"* [Ari92].

6. *"Par démonstration j'entends le syllogisme scientifique, et j'appelle scientifique un syllogisme dont la possession même constitue pour nous la science"* [Ari00].

7. L'exemple le plus célèbre de tous étant : *Tout homme est mortel, Socrate est un homme, donc Socrate est mortel.*

(5) *Les Topiques*[8] : une analyse des méthodes argumentatives qui procèdent à partir d'arguments probables plutôt que certains.

(6) *Les Réfutations Sophistiques*[9] : une analyse des faux-semblants du raisonnement que sont les sophismes et des moyens de les réfuter.

La seconde figure marquante de la logique dans l'antiquité est le philosophe stoïcien Chrysippe de Soles (280 – 206 av. J.-C.) qui n'étudiait pas la logique à dessein de constituer un système formel, mais afin de connaître les opérations de la raison ($\lambda\acute{o}\gamma o\varsigma$) : le *logos* qui gouverne l'univers dont les êtres humains font partie. Il cherchait à trouver les règles correctes d'inférence et les formes de preuves qui pourraient nous guider dans la vie philosophique, qui n'est elle-même que la recherche de la raison droite [Chr04]. Chrysippe et les stoïciens ont une approche de la logique qui se concentre sur les arguments conditionnels du type : *si le vent vient de l'Est le soir, alors il pleuvra demain. Le vent vient de l'Est ce soir, donc il pleuvra demain.* Ainsi, contrairement à la logique aristotélicienne qui se concentrait sur les relations entre les termes sujets et prédicats (*tout homme est mortel, tout Grec est un homme, donc tout Grec est mortel*), la logique stoïcienne s'occupait des relations entre les propositions (*si les loups aboient alors les loups attaqueront; les loups aboient, donc les loups attaqueront*). Supplantée par la logique aristotélicienne, dont elle semblait n'être qu'un habillage, ce n'est qu'au XX^e^ siècle qu'il est apparu que l'entreprise de Chrysippe constituait un remarquable travail en direction de ce qui deviendra le calcul propositionnel, une logique certes rudimentaire mais au caractère nettement plus achevé et accompli que la logique aristotélicienne avec laquelle elle ne se confond pas pour autant.

Par la suite, les développements de la logique se sont bornés à quelques commentaires lors de recopies ou de traductions, qui pour l'essentiel concernaient les œuvres d'Aristote. Une large part de ces travaux émanent du monde arabe et c'est un perse, Avicenne (980 – 1037), qui renouvelle l'étude de la logique en s'intéressant en particulier à ce que nous appellerions aujourd'hui les logiques temporelles [Avi07]. Ces logiques mettent en jeu des concepts comme `quelquefois`, `toujours`, `jamais`. Le XII^e^ siècle marque un intérêt renouvelé pour la logique et plus particulièrement pour les *raisonnements fallacieux*, reprenant le travail amorcé par Aristote dans *Les Réfutations Sophistiques*. Ensuite, graduellement aux XVI^e^ et XVII^e^ siècles, les réponses aux mystères du monde se trouvent de moins en moins dans les enseignements de la religion, mais plutôt dans une explication mécanique. La logique devient alors fondamentale en tant qu'outil de la Raison.

A la Renaissance, suivant en cela l'exemple de l'algèbre qui met en jeu des symboles abstraits et prend peu à peu le pas sur la géométrie, Gottfried Leibniz (1646 – 1716) engage pour la première fois la logique vers la logique symbolique. Ce tournant est accompagné du grand espoir que la logique permettrait de transformer la philosophie, la politique et la religion en de simples entreprises de calcul. Leibniz envisage de rectifier nos raisonnements, de sorte à les rendre irrévocables et intangibles comme le sont les mathématiques [Lei11]. Cela permettrait à terme de résoudre les controverses ou disputes entre les hommes par l'exécution d'un calcul : "il n'y aura plus besoin entre deux philosophes de discussions plus longues qu'entre deux mathématiciens, puisqu'il suffira qu'ils saisissent leur plume, qu'ils

8. *"Le but de ce traité est de trouver une méthode qui nous mette en mesure d'argumenter sur tout problème proposé, en partant de prémisses probables et d'éviter, quand nous soutenons un argument, de rien dire nous-mêmes qui y soit contraire"* [Ari97].

9. *"Parlons maintenant des réfutations sophistiques, c'est-à-dire des réfutations qui n'en ont que l'apparence, mais qui sont en réalité des paralogismes"* [Ari95].

s'asseyent à leur table de calcul (en faisant appel, s'ils le souhaitent, à un ami) et qu'ils se disent l'un à l'autre : Calculons !" (Couturat 1961, p.98, note 3) [Cou13] [10].

Néanmoins, cette logique symbolique dont Leibniz avait l'espoir doit attendre le XIX^e siècle pour voir le jour. Tout d'abord avec la figure emblématique de George Boole (1815 – 1864), précurseur de la logique symbolique en ce qu'il met à jour une algèbre qui traite d'opérations logiques élémentaires sur le vrai et le faux [Boo47, Boo54] et qui porte aujourd'hui son nom (*algèbre de Boole*). Puis vinrent ensuite le père de la théorie des ensembles Georg Cantor (1845 – 1918) [Can32], l'inventeur des premiers systèmes formels de logique Gottlob Frege (1848 – 1925) [Fre71], reformulés par Bertrand Russell (1872 – 1970) [RW12]. Pourtant le plus connu des logiciens de ce siècle est un tout autre personnage : Charles Dodgson (1832 – 1898), professeur à Oxford [11], plus connu sous le nom de Lewis Carroll [Car03].

> *"Contrariwise," continued Tweedledee, "if it was so, it might be, and if it were so, it would be, but as it isn't, it ain't. That's logic."*
>
> Lewis Carroll, *Through the Looking Glass* [Car03].

Le XX^e siècle voit une explosion du développement de la logique symbolique, encore accéléré par la venue de l'informatique. Pour faire image, nous dirions que le décalage entre ce qu'était la logique de ses origines à la première moitié du XIX^e siècle et ce qu'elle est devenue à la fin du XX^e siècle est du même ordre que celui qui sépare la physique des Grecs de celle du début du troisième millénaire. Une immense accélération du processus d'expansion de cette discipline s'est opérée.

2. L'algèbre de Boole des ensembles

Qu'est-ce qu'un ensemble ? Une première réponse serait de dire que c'est une collection d'objets, un tas de choses, un ensemble d'éléments réunis et regroupés. Il s'agit d'un rassemblement de certaines choses sous une bannière commune. Ainsi, la bonne métaphore d'un ensemble serait un vulgaire sac, ou plutôt n'importe quel contenant dans la mesure où il contient. C'est le contenant en tant qu'il contient, dans son essence de contenant, et non pas pour ce qu'il est lui-même. Ce n'est pas tel sac par opposition à tel autre, mais en tant qu'il est un sac et sert à retenir – ensemble précisément – des objets. Les exemples sont légion. La vie quotidienne fourmille d'ensembles de toute sorte, à commencer par tout ce qui est rassemblé dans un sac – un vrai cette fois – comme l'ensemble des provisions qui quittent le supermarché. Mais aussi tout ce que nous pouvons regrouper par la pensée (l'ensemble des dents de notre bouche, des individus sur la planète, des tâches à faire aujourd'hui, des Marx Brothers...). Lorsque le contenu d'un ensemble n'est pas trop grand, on note cet ensemble de manière extensive en énumérant les objets qu'il contient à l'intérieur d'accolades : {*Chico*, *Groucho*, *Harpo*, *Zeppo*} ou bien {*noûs*, *thumos*, *epithumia*}.

Dès que nous regroupons divers objets par la pensée, nous les mettons dans un sac immatériel : un ensemble. Tous les ensembles dont nous venons de parler sont finis. Ils ne

10. "*... quando orientur controversiae, non magis disputatione opus erit inter duos philosophos, quam inter duos Computistas. Sufficiet enim calamos in manus sumere sedereque ad abacos, et sibi mutuo (accito si placet amico) dicere : c a l c u l e m u s.*" [Lei84].

11. Plus exactement à *Christ Church* : là même où furent tournés les épisodes des films *Harry Potter*...

comportent chacun qu'un nombre fini d'objets. Néanmoins, nous sommes entourés également d'ensembles infinis, comme l'ensemble des entiers naturels ($\mathbb{N} = \{0, 1, 2, 3, \ldots\}$), des entiers relatifs ($\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$), des rationnels ($\mathbb{Q}$), des réels ($\mathbb{R}$).

Parmi tous les ensembles, il en est un de très particulier : celui qui ne contient rien. Il faut imaginer un sac vide, un contenant sans contenu. Un contenant qui ne contient rien n'est pas pour autant rien. Il n'y a rien dans le sac, mais il y a bien un sac. Un sac vide est quelque chose qui peut même vous coûter jusqu'à 30.- centimes ! En tant qu'ensemble, un ensemble qui ne contient rien est un ensemble qui est dit *vide*. On l'appelle d'ailleurs l'ensemble vide et on le note $\emptyset$. Cette manière de le noter fait référence au nombre 0, c'est-à-dire au nombre d'élément que contient cet ensemble. Si on voulait l'écrire de manière extensive, ce serait des accolades sans rien à l'intérieur ; exactement comme cela : $\{\}$.

Une première chose à noter lorsqu'on parle d'ensemble, c'est qu'il n'y a pas d'ordre sur les éléments que contient un ensemble. En particulier, il n'y a pas d'ordre de préséance entre ces divers éléments. Si j'écris {*noûs*, *thumos*, *epithumia*} ou bien { *thumos*,*noûs*, *epithumia*}, je parle bien du même ensemble : l'ensemble des trois parties de l'âme, chez Platon – le *noûs* (νοῦς, l'intellect, cause de la raison) dont le siège corporel est la tête et la vertu est la sagesse ; le *thumos*, (θυμός, le coeur) dont le siège est la poitrine et la vertu est le courage ; l'*epithumia* (ἐπιθυμία, cause des appétits et des pulsions), dont le siège est le ventre et la vertu est la tempérance [Pla82].

Dans un sac, les objets ne sont pas rangés, ils sont en tas. C'est exactement l'image qu'il faut avoir à l'esprit lorsque l'on parle d'ensemble. En cela un ensemble se distingue d'une suite qui, comme son nom l'indique, mentionne l'ordre dans lequel défilent les éléments. La suite ⟨*noûs*, *thumos*, *epithumia*⟩ est différente de la suite ⟨*thumos*, *noûs*, *epithumia*⟩ car dans la première, le premier élément est *noûs*, alors que dans la seconde, c'est *epithumia*. Un autre phénomène à noter est que si je mets deux fois le même élément dans un ensemble, je ne fais pas autre chose que si je l'avais simplement mis une fois.

FIGURE 1 – Les Marx Brothers.

Ainsi l'ensemble {*Chico*, *Groucho*, *Harpo*, *Zeppo*} et l'ensemble {*Groucho*, *Chico*, *Groucho*, *Harpo*, *Zeppo*} ne sont qu'un seul et même ensemble qui contient quatre éléments. Au contraire des deux suites ⟨*Chico*, *Groucho*, *Harpo*, *Zeppo*⟩ et ⟨*Groucho*, *Chico*, *Groucho*, *Harpo*, *Zeppo*⟩ qui sont bien différentes. Pour donner un autre exemple, disons que la suite

$\langle$*Groucho*, *Groucho*$\rangle$ est une suite de longueur 2 puisqu'elle fait se suivre deux éléments – quand bien même il s'agit deux fois du même élément ! –, au contraire de la suite $\langle$*Groucho*$\rangle$ qui est de longueur 1. Ces deux suites ne sont donc pas les mêmes. Tout au contraire, les deux ensembles $\{$*Groucho*, *Groucho*$\}$ et $\{$*Groucho*$\}$ sont un même ensemble qui ne contient qu'un seul élément : Groucho. C'est exactement ce qui se passerait si l'épicier vous disait : *"dans votre sac, je vous mets cette courge, et je vous mets également encore une fois cette même courge, ça vous fait donc le prix de deux courges"*. Vous n'accepteriez certainement pas son offre. Vous auriez au contraire le sentiment d'être floué et vous lui répondriez *"vous me prenez pour une courge ?"*.

C'est qu'en fait un ensemble n'est défini que par ce qu'il contient. On appelle cela son *extension*. Deux ensembles qui contiennent les mêmes choses – qui ont donc la même extension – ne forment tout bonnement qu'un seul et unique ensemble. Cette propriété s'appelle l'*extensionnalité* : deux ensembles sont égaux si et seulement s'ils contiennent les mêmes éléments. Par conséquent l'ensemble $\{\emptyset\}$ et l'ensemble $\emptyset$ – qui se note également $\{\}$ – sont deux ensembles différents. Car l'ensemble vide ($\emptyset$) ne contient aucun élément, alors que $\{\emptyset\}$ contient un élément. De même, $\{$*noûs*, *thumos*, *epithumia*$\}$ et $\{$*noûs*, *epithumia*$\}$ sont différents, car le premier contient trois éléments et le second deux. Par contre $\{$*noûs*, *thumos*, *epithumia*$\}$ et $\{$*noûs*, *epithumia*, *thumos*, *noûs*, *epithumia*$\}$ ne sont qu'un même ensemble. En effet, il n'y a aucun élément que le premier ensemble contiendrait mais qui ne serait pas dans le second ; et réciproquement : tout élément qui se trouve dans le second ensemble est aussi présent dans le premier. Une conséquence notoire du principe d'*extensionnalité* est qu'il n'y a qu'un seul ensemble vide. En effet, si nous considérons deux ensembles quelconques qui ne possèdent chacun aucun élément, alors tous deux possèdent exactement les mêmes éléments, puisqu'ils n'en possèdent aucun. C'est donc que ces deux ensembles n'en forment qu'un (noté $\emptyset$).

La relation qu'entretien un ensemble avec ses éléments est appelée relation d'appartenance. On la note "$\in$". Nous écrirons *Groucho* $\in \{$*Chico*, *Groucho*, *Harpo*, *Zeppo*$\}$ pour dire que l'élément Groucho appartient à l'ensemble des quatre Marx Brothers. Ainsi pour n'importe quel élément a, la relation "$a \in \emptyset$" est fausse ; ce que l'on écrira "$a \notin \emptyset$".

Dans toute la suite de cette section, E désignera un ensemble quelconque – possiblement infini – que l'on peut considérer comme une sorte d'ensemble universel, c'est-à-dire l'ensemble des objets auxquels on s'intéresse dans une application particulière.

Les ensembles sous forme de patatoïdes

On représente le plus souvent les ensembles abstraits sous forme de patatoïdes que l'on appelle du nom savant de diagrammes de Venn. Cette représentation remonte à 1880, elle est due au logicien anglais John Venn (1834 – 1923) [Ven94]. Sous une forme à peine différente, cette représentation est déjà présente un siècle auparavant dans les *Lettres à une princesse d'Allemagne sur divers sujets de physique et de philosophie* que le mathématicien suisse Leonhard Euler (1707 -1783) échange avec la princesse d'Anhalt-Dessau, la nièce de Frédéric II [Eul03]. A des fins d'explication de la logique syllogistique, Euler emploie des figures à deux dimensions qui se superposent ou non, s'intersectent ou s'incluent. Apparemment, cette représentation des ensembles, Euler l'avait reprise de son maître le mathématicien suisse Jean Bernoulli (1667 – 1748) qui l'aurait lui-même retirée de Gottfried Leibniz (1646 – 1716).

Les variations entre les formes de représentation de Venn ou d'Euler sont minimes. L'idée forte reste la même : un ensemble est représenté par une forme curviligne fermée que l'on appelle *"patate"*. A l'intérieur de cette forme, sur la surface qu'elle délimite, sont disposés les éléments que l'ensemble contient.

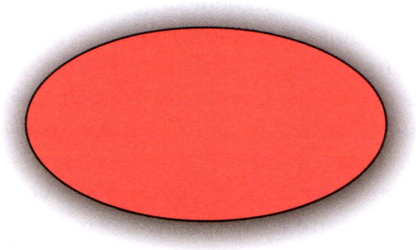


FIGURE 2 – une patate représentant un ensemble.

Très généralement, le dessin d'une forme curviligne fermée ne suffit pas. Il faut dénommer l'ensemble que l'on a ainsi représenté. Pour cela on utilise une flèche qui pointe sur la courbe de la patate et l'on note le nom de l'ensemble à l'origine de celle-ci.

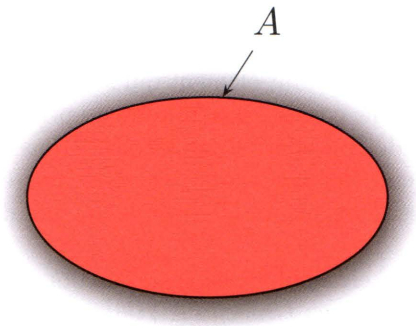


FIGURE 3 – un ensemble dénommé A.

Un ensemble en général peut être vide ou bien contenir des éléments. Si l'on veut signifier que l'ensemble en question n'est pas vide, on indique par de petites croix certains des éléments qu'il contient.

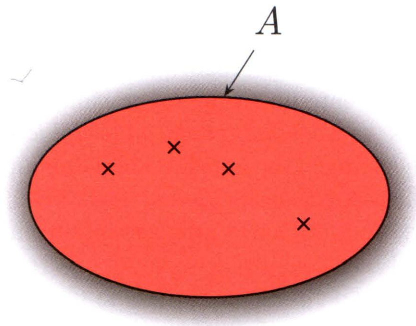


FIGURE 4 – l'ensemble A contient au moins 4 éléments.

Si l'on veut indiquer les noms précis des éléments, on le fait également au moyen de flèches qui pointent vers les noms considérés comme dans la figure ci-dessous :

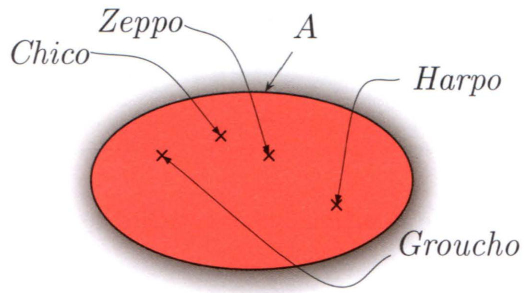


FIGURE 5 – l'ensemble A contient les 4 Marx Brothers.

On peut aussi indiquer les noms des éléments directement à coté des petites croix. Lorsque différents moyens d'expressions seront possibles, on choisira toujours celui qui rendra la lecture la plus aisée ou celui qui permettra de dissiper les ambiguités.

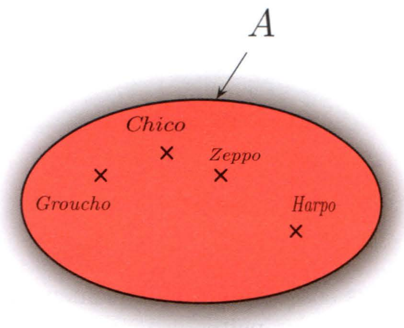


FIGURE 6 – l'ensemble A contient les 4 Marx Brothers.

Les sous-ensembles et l'inclusion

A partir d'un ensemble quelconque E, on forme les sous-ensembles de cet ensemble. Un sous-ensemble n'est pas autre chose qu'un ensemble. Dire que c'est un sous-ensemble d'un ensemble E signifie simplement que chacun de ses éléments a été délicatement prélevé dans l'ensemble E. Ainsi, si l'on prend pour E l'ensemble des trois parties de l'âme chez Platon :

$$E = \{\nu o\tilde{\upsilon}\varsigma, \theta \upsilon \mu \acute{o} \varsigma, \grave{\epsilon}\pi\iota\theta\upsilon\mu\acute{\iota}\alpha\}$$

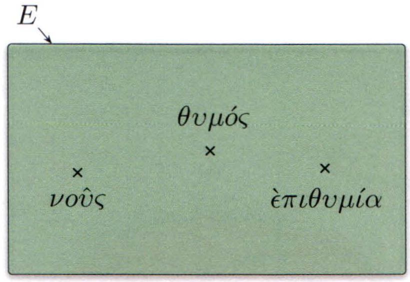


FIGURE 7 – l'ensemble E contenant les 3 parties de l'âme selon Platon.

Les sous-ensembles de E sont les ensembles dont les éléments sont parmi les trois parties de l'âme chez Platon : $νοῦς, θυμός$, et $ἐπιθυμία$. Parmi ces sous-ensembles, il y a ceux qui contiennent exactement un élément (on les appelle les *singletons*). Puisque l'ensemble E contient trois éléments, les singletons qui nous intéressent sont au nombre de trois tels qu'indiqués dans le dessin suivant : $\{νοῦς\}$; $\{θυμός\}$; $\{ἐπιθυμία\}$.

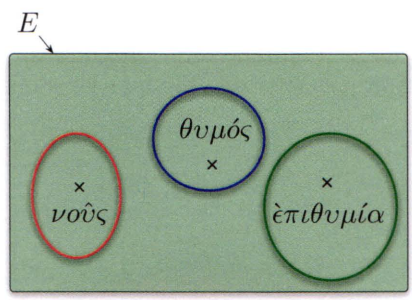


FIGURE 8 – les singletons de E.

On trouve également des sous-ensembles à deux éléments (dénommés *paires* – à ne pas confondre avec les *couples* qui sont des paires ordonnées, autrement dit des suites à deux éléments, alors que les paires ne sont que des ensembles) : $\{νοῦς, θυμός\}$; $\{ἐπιθυμία, θυμός\}$ et $\{νοῦς, ἐπιθυμία\}$, qui sont tous trois représentés dans le schéma suivant.

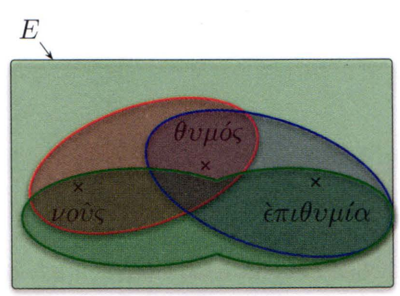


FIGURE 9 – les paires de E.

Il reste encore deux autres types de sous-ensembles de l'ensemble E. Puisque E possède trois éléments et que nous n'avons considéré que les sous-ensembles à un élément (singletons) ou à deux éléments (paires), il reste ceux à trois éléments et à zéro éléments. En effet, il nous reste E tout entier ($\{\nu o\hat{\upsilon}\varsigma, \theta\upsilon\mu\acute{o}\varsigma, \grave{\epsilon}\pi\iota\theta\upsilon\mu\acute{\iota}\alpha\}$) et l'ensemble vide ($\emptyset$). Ils sont tous deux représentés dans le schéma suivant.

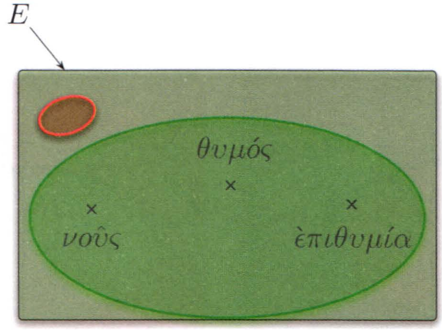


FIGURE 10 – les sous-ensembles de E à 0 ou 3 éléments.

Lorsqu'un ensemble A fait partie des sous-ensembles d'un ensemble E, on dit que A est *inclus* dans E et on le note $A \subset E$. Si ce n'est pas le cas, cela signifie qu'il existe un élément de A qui n'appartient pas à l'ensemble E et on le note $A \not\subset E$. Dans l'exemple ci-dessous, l'ensemble A est inclus dans l'ensemble C, mais l'ensemble B ne l'est pas.

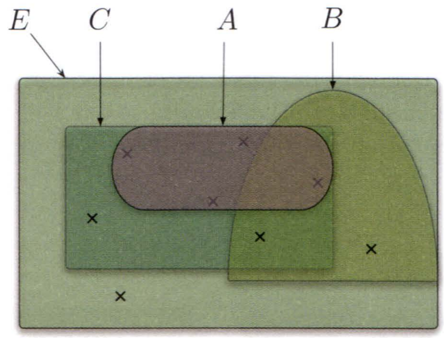


FIGURE 11 – $A \subset C$ mais $B \not\subset C$.

Il est important de noter que pour n'importe quel ensemble E, la relation $\emptyset \subset E$ est vraie. En effet, pour le vérifier, il nous faut nous assurer que chaque élément qui appartient à l'ensemble vide, appartient également à l'ensemble E. Et cela est vrai pour la simple et bonne raison qu'il n'y a pas de tel élément dans l'ensemble vide. Une autre manière de voir la chose consiste à dire que deux ensembles A et B ne vérifient pas la relation $A \subset B$ s'il existe au moins un élément qui soit dans A mais ne soit pas dans B. Donc si $\emptyset \not\subset E$ devait être vrai, on devrait alors trouver un élément dans l'ensemble vide qui ne soit pas dans l'ensemble E. Nous pouvons chercher longtemps un tel élément, nous ne risquons pas de le trouver puisque l'ensemble vide est absolument, résolument et désespérément... *vide*.

Le complémentaire

Situons-nous dans un ensemble E quelconque et considérons A comme un sous-ensemble de E. Le complémentaire de A est le plus grand (au sens de l'inclusion) sous-ensemble de E qui ne contient aucun élément en commun avec A. Autrement dit, le complémentaire de A – que l'on note $A^{\complement}$ – est l'ensemble de tous les éléments de E qui n'appartiennent pas à A.

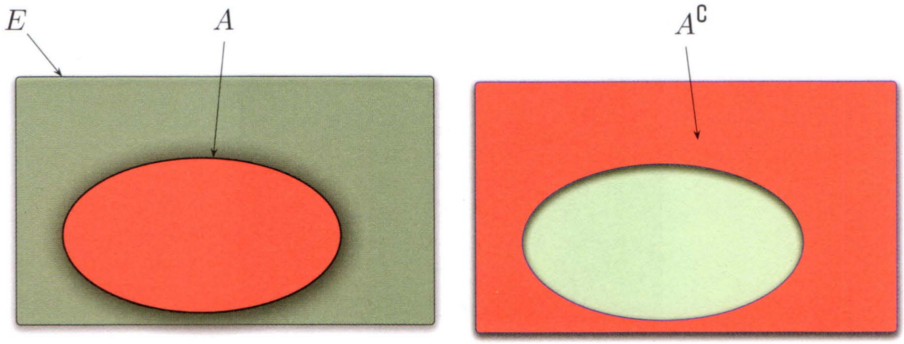


FIGURE 12 – l'ensemble A et son complémentaire.

Il va sans dire que pour tout ensemble A, le complémentaire du complémentaire de A n'est autre que A lui-même : $A^{\complement^{\complement}} = A$.

L'intersection

Si deux patates se superposent, la région qui fait partie à la fois de l'une et de l'autre représente l'intersection de ces deux patates : les éléments qu'elle contient sont tous ceux qui appartiennent aux deux ensembles. Elle délimite ce que l'on appelle l'*intersection* de ces deux ensembles. Cette intersection des deux ensembles A et B est elle-même un ensemble que l'on note $A \cap B$.

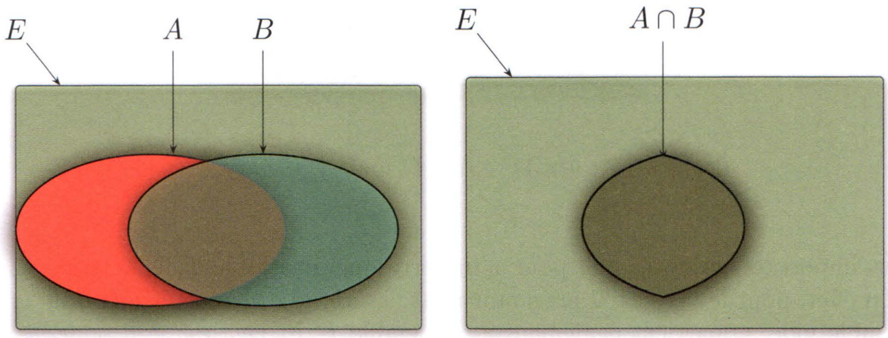


FIGURE 13 – l'ensemble $A \cap B$.

Lorsqu'un élément appartient à la fois à A et B, l'ensemble $A \cap B$ est différent de l'ensemble vide puisqu'il contient au moins cet élément. Pour cela on dit que $A \cap B$ est *non* *vide.* Dans la représentation sous forme de patatoïdes, on indiquera par une croix située dans l'intersection de A et de B que $A \cap B$ est non vide.

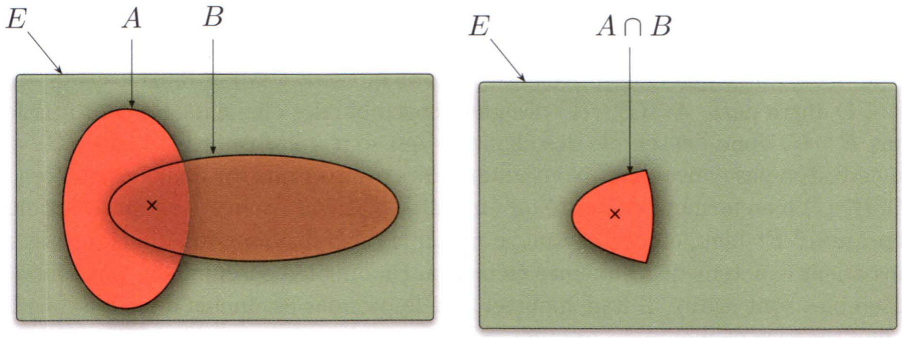


FIGURE 14 – l'ensemble $A \cap B$ est non vide.

Cette opération peut se répéter. On peut ainsi partir de trois ensembles A, B, C et former tout d'abord l'intersection de A et de B, ce qui donne $A \cap B$, puis former l'intersection de $A \cap B$ avec C, pour obtenir ce que l'on notera $(A \cap B) \cap C$.

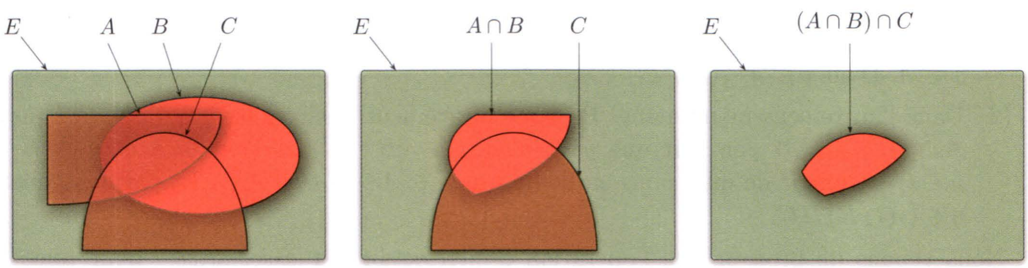


FIGURE 15 – l'ensemble $(A \cap B) \cap C$.

On peut également, à partir de trois ensembles A, B, C quelconques, former tout d'abord l'intersection de B et de C – ce qui donne $B \cap C$ – puis former l'intersection de A avec $B \cap C$, pour obtenir ce que l'on notera $A \cap (B \cap C)$.

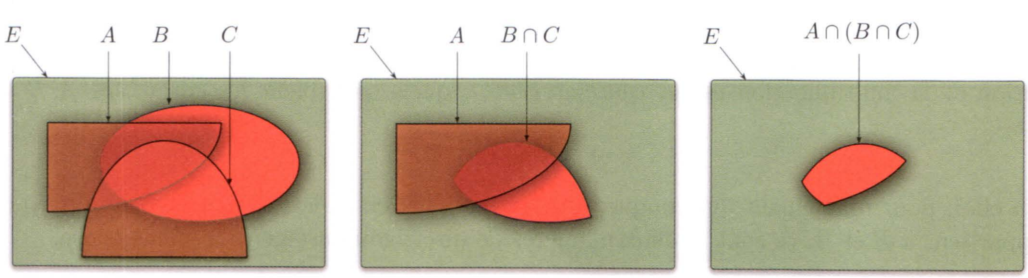


FIGURE 16 – l'ensemble $A \cap (B \cap C)$.

Que remarque-t-on ? Les patates représentant $(A \cap B) \cap C$ et $A \cap (B \cap C)$ sont rigoureusement identiques. Est-ce là un heureux hasard ou bien le fait d'une propriété fondamentale de cette opération qu'est l'intersection ? Réfléchissons en revenant à la définition. Tout d'abord, $(A \cap B) \cap C$ désigne l'ensemble des éléments qui sont à la fois dans $A \cap B$ et dans C. Comme $A \cap B$ désigne l'ensemble des éléments qui sont à la fois dans A et dans B, il apparaît que $(A \cap B) \cap C$ n'est autre que l'ensemble des éléments qui sont à la fois dans les trois ensembles A, B et C. D'autre part, $A \cap (B \cap C)$ désigne l'ensemble des éléments qui sont à la fois dans A et dans $B \cap C$, donc l'ensemble des éléments qui sont à la fois dans A, B et C.

Cela ne vous a pas convaincu ? Nous allons alors prouver que ces deux ensembles $(A \cap B) \cap C$ et $A \cap (B \cap C)$ n'en forment en vérité qu'un seul. Comment prouve-t-on que deux ensembles sont identiques ? Et bien, en appliquant le principe d'extensionnalité. Nous devons montrer qu'ils possèdent exactement les mêmes éléments. En langage ensembliste, pour montrer que deux ensembles sont égaux, il faut montrer que le premier est inclus dans le second (ce qui montre que tous les éléments du premier se trouvent dans le second) et inversément, que le second est inclus dans le premier (ce qui montre que tous les éléments du second se trouvent dans le premier). Cela s'écrit : pour montrer $X = Y$, il faut montrer $X \subset Y$ et $Y \subset X$. Nous allons donc montrer qu'un élément quelconque de $(A \cap B) \cap C$ fait aussi partie de $A \cap (B \cap C)$, puis qu'un élément quelconque pris dans $A \cap (B \cap C)$ appartient également à $(A \cap B) \cap C$.

(1) Commençons par prendre un élément x qui appartient à $(A \cap B) \cap C$. Puisque $x \in (A \cap B) \cap C$, il s'en suit qu'à la fois $x \in (A \cap B)$ et $x \in C$. Nous allons maintenant utiliser le fait que $x \in (A \cap B)$ pour en déduire que $x \in A$ et $x \in B$. Nous obtenons donc que $x \in A$ et $x \in B$ et $x \in C$. De là, nous en déduisons que $x \in (B \cap C)$ et $x \in A$. D'où $x \in A \cap (B \cap C)$.

(2) Dans l'autre sens maintenant ! Prenons un élément quelconque y qui appartienne à $A \cap (B \cap C)$. Il s'en suit que $y \in A$ et $y \in (B \cap C)$, d'où $y \in A$ et $y \in B$ et $y \in C$. A partir de quoi nous en déduisons $y \in A \cap B$ et $y \in C$. Et par conséquent $y \in (A \cap B) \cap C$.

Nous venons de prouver que l'opération d'intersection est *associative* : pour tous les ensembles A, B, C, on a :

$$(A \cap B) \cap C = A \cap (B \cap C).$$

C'est une propriété qu'elle partage avec l'addition ($[x + y] + z = x + [y + z]$) et la multiplication ($[x \times y] \times z = x \times [y \times z]$) par exemple, mais pas avec la soustraction ($0 = [3 - 2] - 1 \neq 3 - [2 - 1] = 2$).

Puisque écrire $(A \cap B) \cap C$ ou bien $A \cap (B \cap C)$ revient à désigner le même ensemble, on se passera par la suite de parenthèses et on écrira $A \cap B \cap C$ en lieu et place de $(A \cap B) \cap C$.

Une seconde propriété tout aussi notoire que partage l'opération d'intersection avec l'addition et la multiplication est la *commutativité* : quels que soient les ensembles A, B on a :

$$A \cap B = B \cap A.$$

En effet, pour un élément quelconque, dire qu'il appartient à la fois à A et B ou dire qu'il appartient à B et A, ce sont là deux manières de dire rigoureusement la même chose.

La réunion

L'opération duale de l'intersection est la réunion. Au lieu de former le sous-ensemble qui contient à la fois les éléments de A et de B, on forme cette fois-ci le sous-ensemble qui contient tous les éléments qui se trouvent dans A ou dans B.

L'union des deux ensembles A et B est bien sûr elle-même un ensemble que l'on note $A \cup B$.

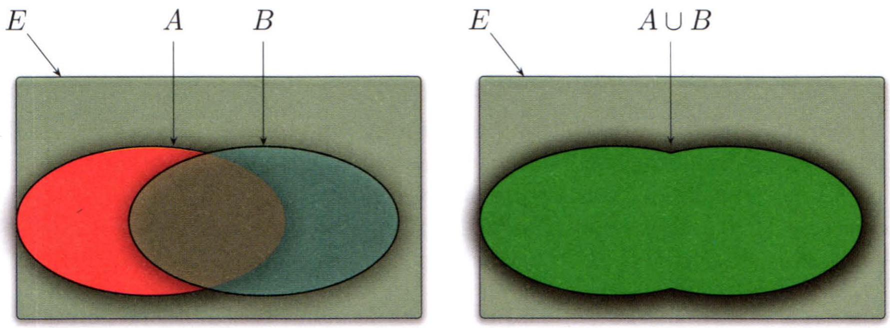


FIGURE 17 – l'ensemble $A \cup B$.

Cette opération peut se répéter. On peut ainsi, à partir de trois ensembles A, B, C, former tout d'abord l'union de A et de B, ce qui donne $A \cup B$, puis former l'union de $A \cup B$ avec C, pour obtenir $(A \cup B) \cup C$.

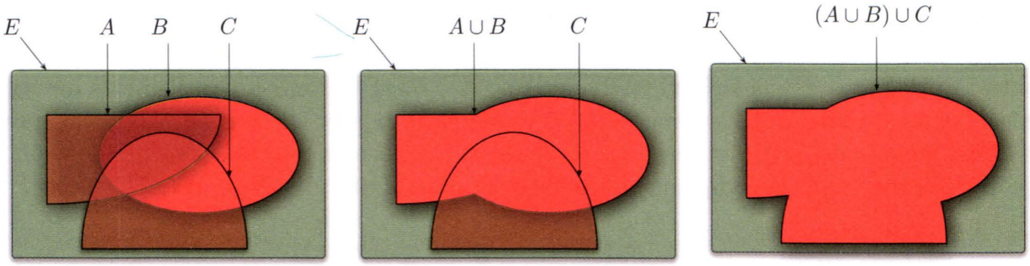


FIGURE 18 – l'ensemble $(A \cup B) \cup C$.

On peut également, à partir des mêmes trois ensembles A, B, C, former tout d'abord l'union de B et de C, ce qui donne $B \cup C$, puis l'union de A avec $B \cup C$, pour obtenir $A \cup (B \cup C)$.

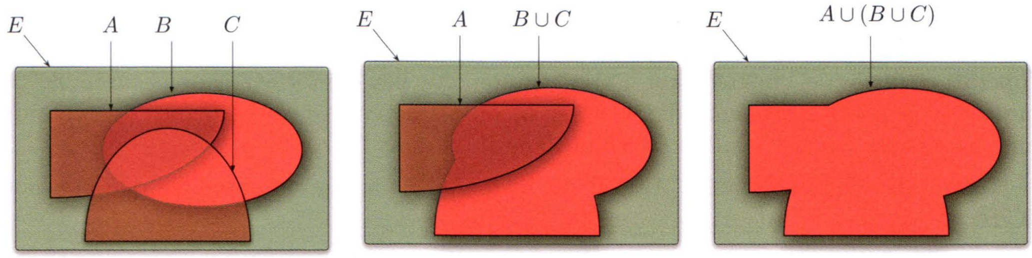


FIGURE 19 – l'ensemble $A \cup (B \cup C)$.

Que remarque-t-on à nouveau ? Les patates représentant $(A \cup B) \cup C$ et $A \cup (B \cup C)$ sont rigoureusement identiques. C'est encore une fois une conséquence de ce que la réunion est une opération transitive : pour tous ensembles A, B, C, $(A \cup B) \cup C = A \cup (B \cup C)$. La preuve en est également directe puisque $(A \cup B) \cup C$ n'est autre que l'ensemble des éléments qui sont soit dans A, soit dans B, soit dans C et il en va de même pour $A \cup (B \cup C)$.

Puisque $(A \cup B) \cup C$ et $A \cup (B \cup C)$ désignent le même ensemble, on écrira $A \cup B \cup C$ pour $(A \cup B) \cup C$.

La réunion est également *commutative* puisque pour tous ensembles A, B on a :

$$A \cup B = B \cup A.$$

La différence

La réunion ressemble à l'addition, puisque l'ensemble $A \cup B$ contient tous les éléments qui sont dans A *plus* tous ceux qui sont dans B. Quelle serait l'opération qui fonctionnerait avec les ensembles de la même manière que la soustraction ? Pour faire image, cette opération donnerait à partir de A et de B l'ensemble des éléments qui sont dans A *moins* tous ceux qui sont dans B. Cette opération s'appelle la *différence*. Elle se définit de diverses manières toutes équivalentes. On peut d'une part dire que $A \setminus B$ est l'ensemble des éléments qui sont dans A sans être dans B. Et comme "ne pas être dans B" signifie être dans le complémentaire de B, on peut également dire que $A \setminus B$ contient précisément tous les éléments qui sont à la fois dans A et dans le complémentaire de B, ce qui s'écrit : $A \setminus B = A \cap B^{\complement}$.

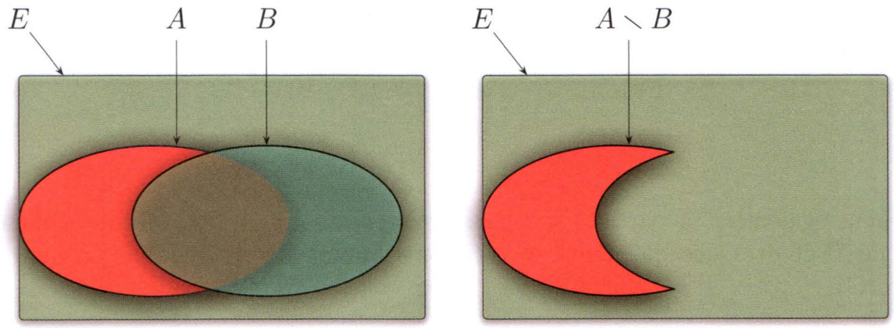


FIGURE 20 – l'ensemble $A \setminus B$.

Cette fois-ci, contrairement à l'intersection et à la réunion, la différence n'est pas une opération associative. Pour prouver cela, il nous suffit d'exhiber trois ensembles A, B, C, tels que $(A \setminus B) \setminus C$ est différent de $A \setminus (B \setminus C)$. Par exemple, si $A = \{\theta\upsilon\mu\acute{o}\varsigma\}$, $B = \emptyset$ et $C = \{\theta\upsilon\mu\acute{o}\varsigma\}$, alors $(A \setminus B) = \{\theta\upsilon\mu\acute{o}\varsigma\}$ et donc $(A \setminus B) \setminus C = \{\theta\upsilon\mu\acute{o}\varsigma\} \setminus \{\theta\upsilon\mu\acute{o}\varsigma\} = \emptyset$; alors que $(B \setminus C) = \emptyset \setminus \{\theta\upsilon\mu\acute{o}\varsigma\} = \emptyset$, d'où $A \setminus (B \setminus C) = \{\theta\upsilon\mu\acute{o}\varsigma\} \setminus \emptyset = \{\theta\upsilon\mu\acute{o}\varsigma\}$. L'exemple suivant offre une représentation picturale du même phénomène.

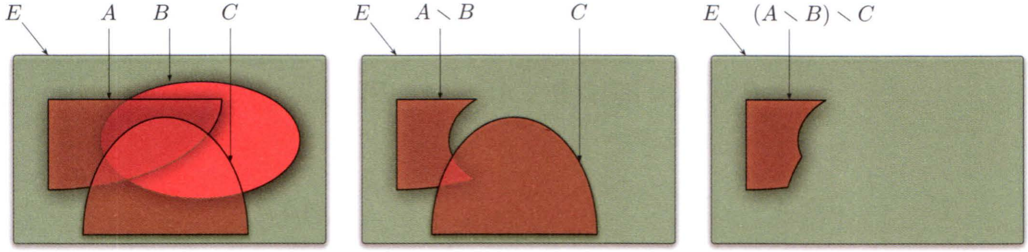


FIGURE 21 – construction de l'ensemble $(A \setminus B) \setminus C$.

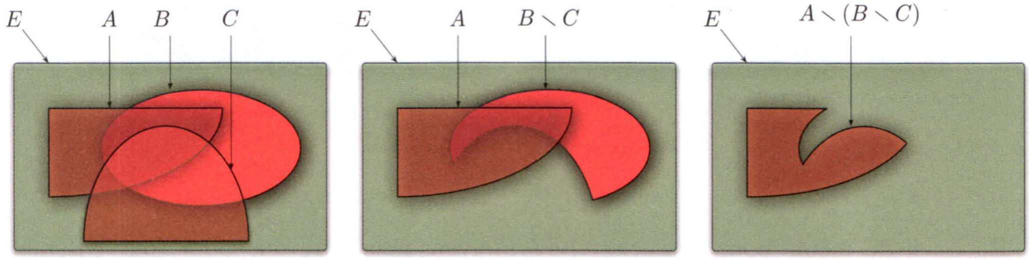


FIGURE 22 – construction de l'ensemble $A \setminus (B \setminus C)$.

Pas plus qu'elle n'est associative, la différence n'est commutative :

$$\{\theta\upsilon\mu\acute{o}\varsigma\} = \{\theta\upsilon\mu\acute{o}\varsigma\} \setminus \emptyset \neq \emptyset \setminus \{\theta\upsilon\mu\acute{o}\varsigma\} = \emptyset.$$

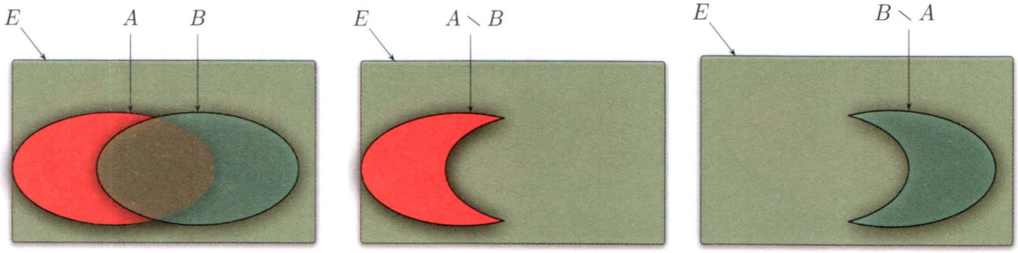


FIGURE 23 – les ensembles $A \setminus B$ et $B \setminus A$.

La différence symétrique

N'y aurait-il pas un moyen de récupérer l'associativité tout en conservant l'idée d'une différence ? La différence symétrique est là précisément pour répondre positivement à cette question. Elle se définit en disant qu'à partir de A et de B, on ne conserve que ce qui est dans A mais pas dans B ou bien dans B mais pas dans A. Ainsi, la différence symétrique de A et de B – que l'on note $A\Delta B$ – est l'ensemble qui contient tous les éléments de $A \smallsetminus B$ *plus* tous ceux de $B \smallsetminus A$. Autrement dit $A\Delta B$ n'est autre que l'ensemble de tous les éléments de $A \cup B$ *moins* tous ceux de $A \cap B$. On obtient ainsi les égalités suivantes :

$$A\Delta B = (A \smallsetminus B) \cup (B \smallsetminus A) = (A \cup B) \smallsetminus (A \cap B).$$

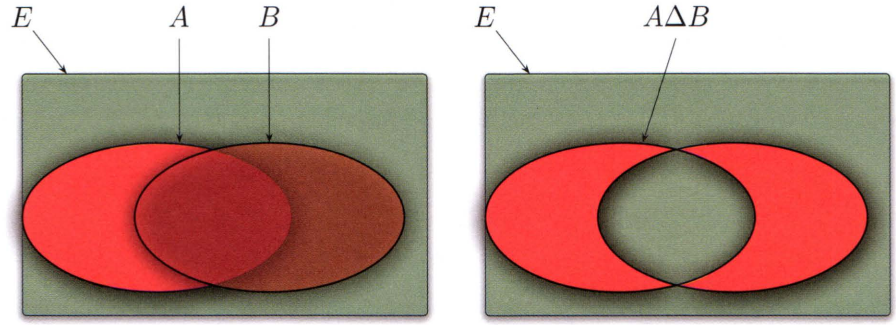


FIGURE 24 – l'ensemble $A\Delta B$.

En est-il de même pour l'associativité ? Pouvons-nous dire que pour tous ensembles A, B, C, on a bien $(A\Delta B)\Delta C = A\Delta(B\Delta C)$? Il y a deux solutions : soit la réponse est affirmative et il nous faut alors une preuve qui consisterait à montrer que tout élément qui appartient à $(A\Delta B)\Delta C$ appartient également à $A\Delta(B\Delta C)$, et réciproquement que tout élément qui appartient à $A\Delta(B\Delta C)$ appartient aussi à $(A\Delta B)\Delta C$; soit la réponse est négative, et dans ce cas il nous faudrait produire un *contre-exemple*, c'est-à-dire un exemple de trois ensembles A, B, C qui ne vérifieraient pas cette égalité.

Mais avant d'aller plus en avant dans l'une de ces directions, tentons de nous convaincre en considérant un schéma suffisamment général.

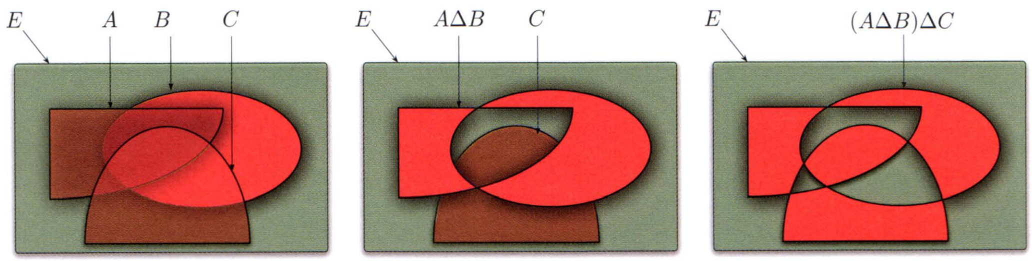


FIGURE 25 – construction de l'ensemble $(A\Delta B)\Delta C$.

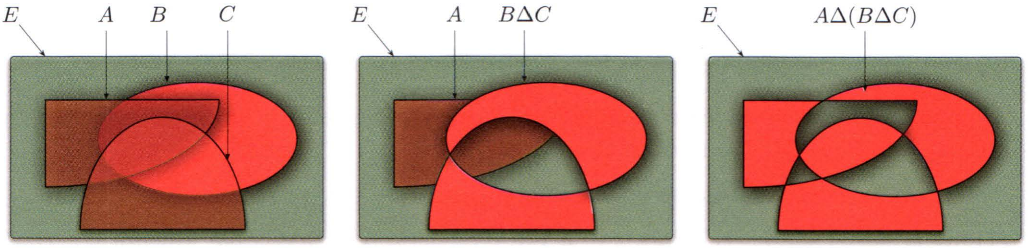


FIGURE 26 – construction de l'ensemble $A\Delta(B\Delta C)$.

Il semble, au vu de ces figures, que la différence symétrique soit associative. Mais si nous avons bien une idée, nous n'avons pour l'instant rien montré. Pour cela, nous allons considérer les ensembles suivants qui constituent, par leur réunion, l'union des trois ensembles A, B et C. Il est clair que par définition $(A\Delta B)\Delta C$ et $A\Delta(B\Delta C)$ sont des sous-ensembles de $A\cup B\cup C$, puisqu'un élément qui n'appartient ni à A, ni à B, ni à C, n'appartient également ni à $(A\Delta B)\Delta C$ ni à $A\Delta(B\Delta C)$.

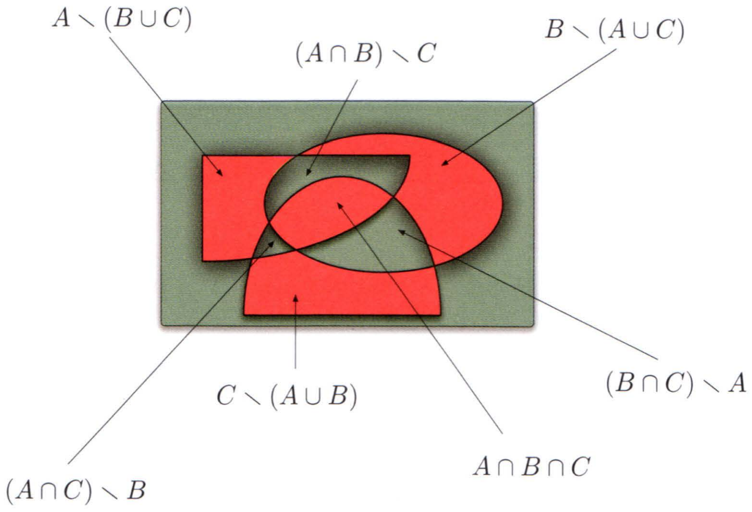


FIGURE 27 – un éclaté de l'ensemble $A\Delta(B\Delta C)$.

Un élément qui appartient à $A\cup B\cup C$ appartient :

(1) soit à un seul de ces ensembles :
  (a) uniquement à A, c'est-à-dire à $A\smallsetminus(B\cup C)$
  (b) uniquement à B, c'est-à-dire à $B\smallsetminus(A\cup C)$
  (c) uniquement à C, c'est-à-dire à $C\smallsetminus(A\cup B)$

(2) soit à deux seuls de ces ensembles :
  (a) uniquement à A et à B, c'est-à-dire à $(A\cap B)\smallsetminus C$
  (b) uniquement à B et à C c'est-à-dire à $(B\cap C)\smallsetminus A$

(c) uniquement à A et à C, c'est-à-dire à $(A \cap C) \setminus B$

(3) soit à ces trois ensembles à la fois, c'est-à-dire à $A \cap B \cap C$

Nous allons donc considérer les sept cas ci-dessus et pour chacun d'eux montrer que $(A\Delta B)\Delta C$ et $A\Delta(B\Delta C)$ se rejoignent.

Soit x un élément quelconque de $A \cup B \cup C$,

(1) (a) si $x \in A \setminus (B \cup C)$ alors $x \in A\Delta B$, d'où $x \in (A\Delta B)\Delta C$; par ailleurs $x \notin B\Delta C$, d'où $x \in A\Delta(B\Delta C)$. $\boxed{\checkmark}$

(b) si $x \in B \setminus (A \cup C)$ alors $x \in A\Delta B$, d'où $x \in (A\Delta B)\Delta C$; par ailleurs $x \in B\Delta C$, d'où $x \in A\Delta(B\Delta C)$. $\boxed{\checkmark}$

(c) si $x \in C \setminus (A \cup B)$ alors $x \notin A\Delta B$, d'où $x \in (A\Delta B)\Delta C$; par ailleurs $x \in B\Delta C$, d'où $x \in A\Delta(B\Delta C)$. $\boxed{\checkmark}$

(2) (a) si $x \in (A \cap B) \setminus C$ alors $x \notin A\Delta B$, d'où $x \notin (A\Delta B)\Delta C$; par ailleurs $x \in B\Delta C$, d'où $x \notin A\Delta(B\Delta C)$. $\boxed{\checkmark}$

(b) si $x \in (B \cap C) \setminus A$ alors $x \in A\Delta B$, d'où $x \notin (A\Delta B)\Delta C$; par ailleurs $x \notin B\Delta C$, d'où $x \notin A\Delta(B\Delta C)$. $\boxed{\checkmark}$

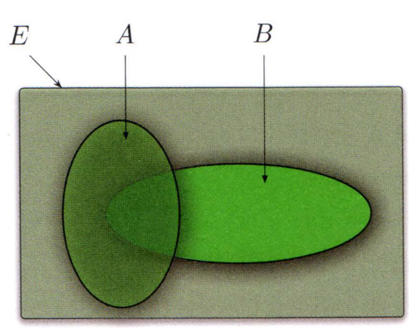
(c) si $x \in (A \cap C) \setminus B$ alors $x \in A\Delta B$, d'où $x \notin (A\Delta B)\Delta C$; par ailleurs $x \in B\Delta C$, d'où $x \notin A\Delta(B\Delta C)$. $\boxed{\checkmark}$

(3) si $x \in A \cap B \cap C$ alors $x \notin A\Delta B$, d'où $x \in (A\Delta B)\Delta C$; par ailleurs $x \notin B\Delta C$, d'où $x \in A\Delta(B\Delta C)$. $\boxed{\checkmark}$

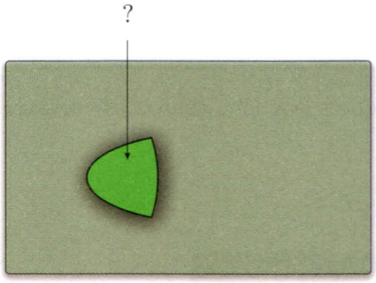
Voilà qui termine cette laborieuse preuve de l'associativité de la différence symétrique.

Passons à quelques exercices maintenant.

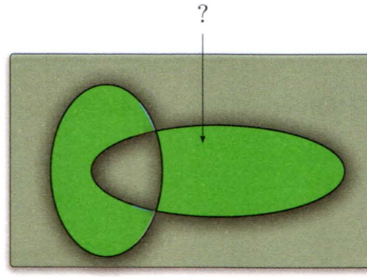
Exercise 1 On considère les ensembles représentés par les patates suivantes :



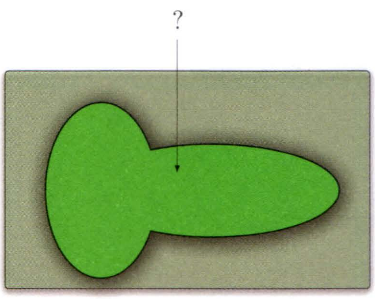
Comment qualifier les représentations qui suivent ?



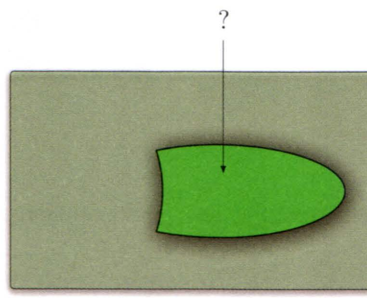
(1)



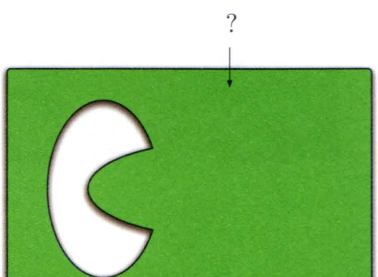
(2)



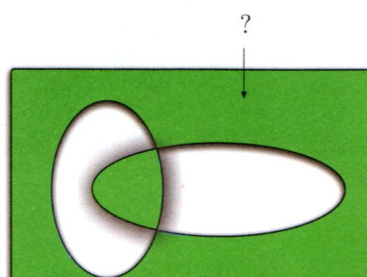
(3)



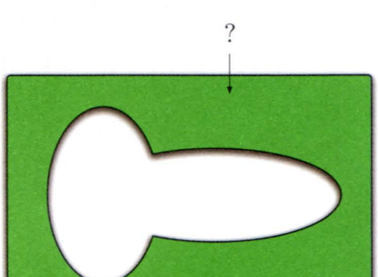
(4)



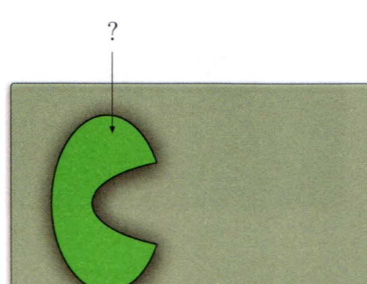
(5)



(6)



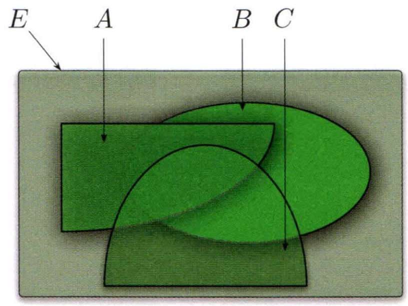
(7)



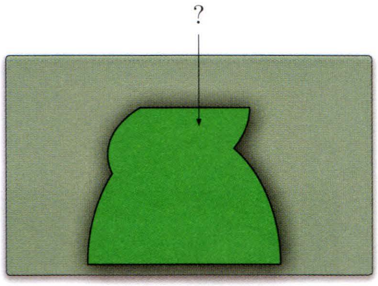
(8)

Pour obtenir les réponses à l'exercice 1, voir ci-dessous[12].

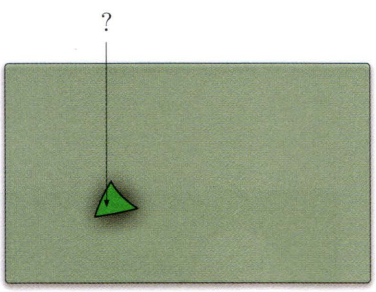
Exercise 2 On considère les ensembles représentés par les patatoïdes suivantes :



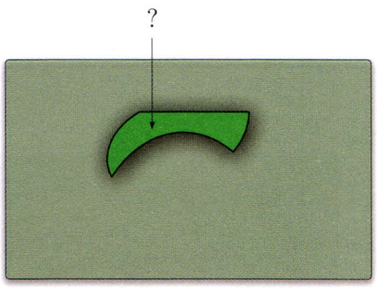
Comment qualifier les représentations qui suivent ?



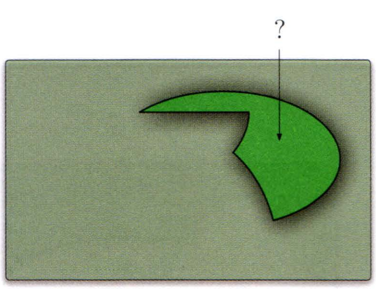
(1)



(2)

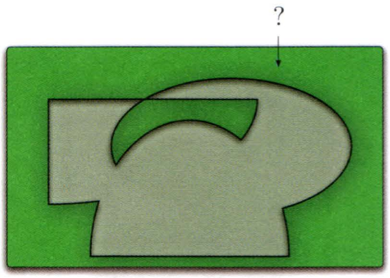


(3)

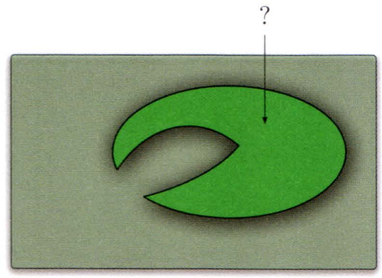


(4)

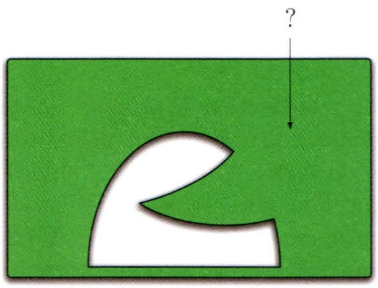
12. (1) $A \cap B$; (2) $A \Delta B$; (3) $A \cup B$; (4) $B \setminus A$; (5) $(A \setminus B)^C$; (6) $(A \Delta B)^C$; (7) $(A \cap B)^C$; (8) $(A \setminus B)$



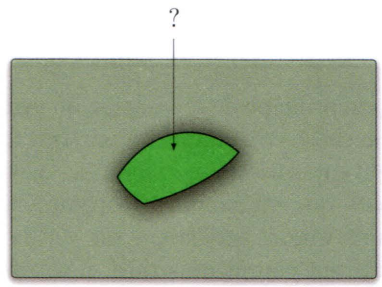
(5)



(6)

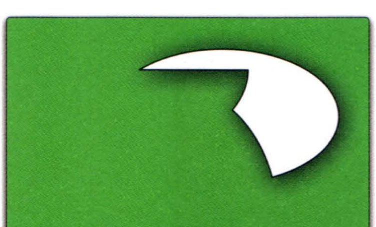


(7)

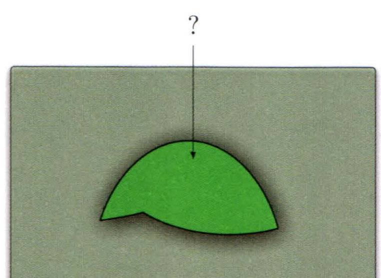


(8)

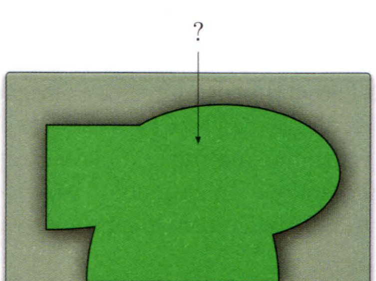
E



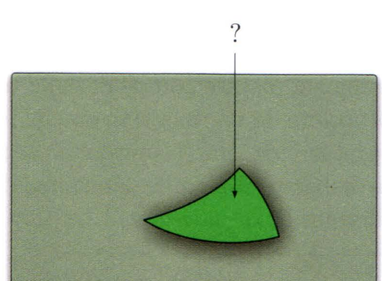
(9)



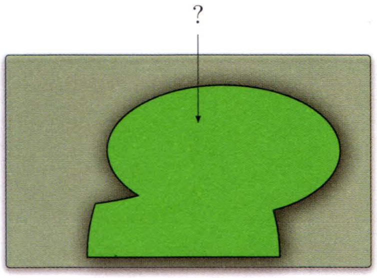
(10)



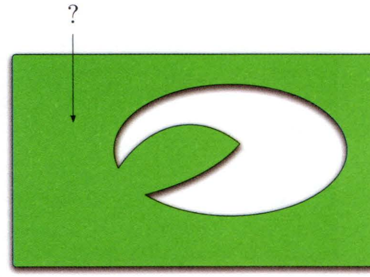
(11)



(12)



(13)



(14)

Pour obtenir les réponses à l'exercice 2, voir ci-dessous[13].

Propriété et principe de compréhension

Appelé aussi principe de séparation ou principe de spécification, le principe de compréhension énonce une chose très simple : à partir d'un ensemble donné quelconque E et d'une propriété P que peuvent satisfaire ou non ses éléments, on forme le sous-sensemble de E de tous les éléments qui satisfont cette propriété et que l'on note $\{x \in E \mid \mathsf{P}(x)\}$. La notation $\mathsf{P}(x)$ signifie que x satisfait – ou vérifie – la propriété désignée par P. Pour des raisons qui deviendront claires plus tard, nous convenons d'écrire $\neg\mathsf{P}(x)$ pour *“x ne satisfait pas la propriété* P”. Par exemple, si E désigne l'ensemble des Grecs à l'époque de Socrate, et P la propriété “être athénien”, alors $\{x \in E \mid \mathsf{P}(x)\}$ désigne l'ensemble des athéniens de l'époque socratique.

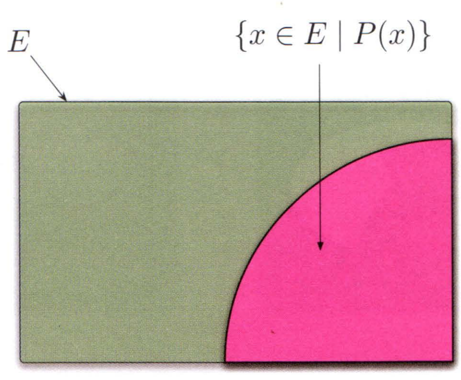


FIGURE 28 – $\{x \in E \mid \mathsf{P}(x)\}$.

De même, si maintenant E désigne toujours l'ensemble des Grecs à l'époque de Socrate et P la propriété de vivre la tête en bas pendu par les pieds, alors $\{x \in E \mid \mathsf{P}(x)\}$ n'est autre que l'ensemble vide. Une propriété n'est pas un ensemble, mais lorsqu'elle est rapportée à un ensemble de base (ici E), elle détermine de manière unique un ensemble : le sous-ensemble de E des individus qui la satisfont. Une propriété est en quelque sorte une promesse d'ensembles,

13. (1) $(A \cap B) \cup C$; (2) $(A \smallsetminus B) \cap C$; (3) $(A \cap B) \smallsetminus C$; (4) $B \smallsetminus (A \cup C)$; (5) $(A \cup B \cup C)^{\mathsf{c}} \cup ((A \cap B) \smallsetminus C)$; (6) $B \smallsetminus (A \cap C)$; (7) $(C \smallsetminus (B \smallsetminus A))^{\mathsf{c}}$; (8) $A \cap B \cap C$; (9) $(B \smallsetminus (A \cup C))^{\mathsf{c}}$; (10) $C \cap (A \cup B)$; (11) $(A \cup B \cup C)$; (12) $C \cap (B \smallsetminus A)$; (13) $B \cup (C \smallsetminus A)$; (14) $(B \smallsetminus (A \cap B \cap C))^{\mathsf{c}}$.

puisqu'elle sépare tout ensemble E en deux sous-ensembles : celui des éléments de E qui la satisfont – $\{x \in E \mid \mathsf{P}(x)\}$ – et celui de ceux qui ne la satisfont pas – $\{x \in E \mid \neg\mathsf{P}(x)\}$.

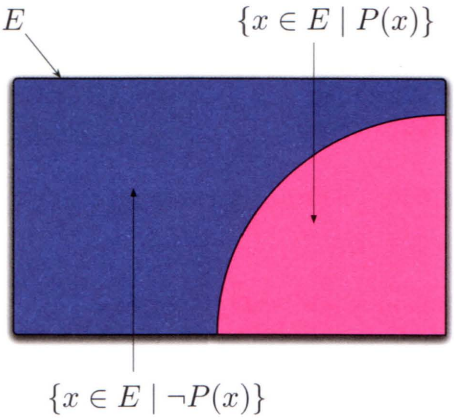


FIGURE 29 – Séparation de E par la propriété P.

Le fait d'appartenir ou non à un ensemble A quelconque est une propriété particulière : $\mathsf{P}(x)$ équivaut à $x \in A$. Si maintenant munis de cette propriété et d'un ensemble E nous formons $\{x \in E \mid \mathsf{P}(x)\}$, nous obtenons alors $\{x \in E \mid x \in A\}$ qui n'est autre que l'ensemble $E \cap A$.

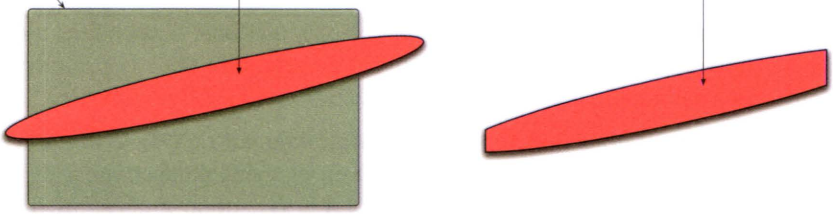


FIGURE 30 – lorsque $\mathsf{P}(x)$ signifie $x \in A$.

Inversement, le fait de ne pas appartenir à un ensemble A est également une propriété particulière : la négation d'une propriété est elle-même une propriété. A partir d'un ensemble E, si nous formons $\{x \in E \mid \neg\mathsf{P}(x)\}$, nous obtenons alors $\{x \in E \mid x \notin A\}$ qui n'est autre que l'ensemble $E \setminus A$.

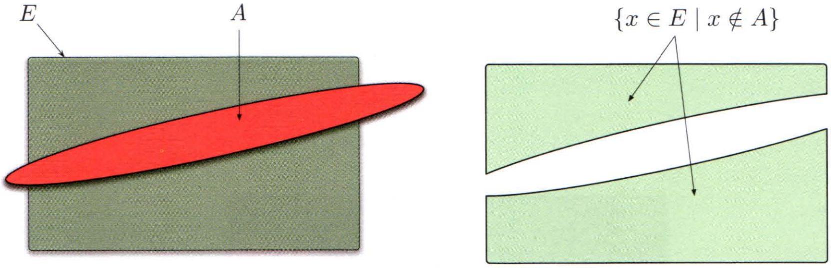


FIGURE 31 – Séparation par la propriété $x \notin A$.

Les opérations booléennes ensemblistes revisitées

Nous allons réécrire les opérations ensemblistes au moyen de principe de compréhension, en utilisant le fait que $x \in A$, $x \notin B$ sont des propriétés particulières. Pour cela, nous partons avec A, B deux sous-ensembles d'un ensemble E – ce que nous écrivons $A, B \subset E$.

- $A \cap B = \{x \in E \mid x \in A \text{ et } x \in B\}$
- $A \cup B = \{x \in E \mid x \in A \text{ ou } x \in B\}$
- $A^{\complement} = \{x \in E \mid x \notin A\}$
- $A \setminus B = \{x \in E \mid x \in A \text{ et } x \notin B\}$
- $A \Delta B = \{x \in E \mid x \in A \text{ ou } x \in B, \text{mais } x \notin A \cap B\}$.

Proposition 3 (lois de De Morgan) *Les deux relations suivantes sont vérifiées :*

(1) $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$

(2) $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$.

Preuve de la Proposition 3 : Si l'on veut démontrer ces propositions, il nous faut montrer les inclusions dans les deux sens sous-jacentes à l'égalité. Par exemple, pour la première égalité, il nous faut montrer les deux inclusions suivantes : $(A \cup B)^{\complement} \subset A^{\complement} \cap B^{\complement}$ et $A^{\complement} \cap B^{\complement} \subset (A \cup B)^{\complement}$.

$\mathbf{(A \cup B)^{\complement} \subset A^{\complement} \cap B^{\complement}}$ **:** Il nous faut montrer que tout élément de $(A \cup B)^{\complement}$ est également un élément de $A^{\complement} \cap B^{\complement}$. Pour ce faire, prenons un élément *quelconque* $x \in (A \cup B)^{\complement}$. Puisque $x \in (A \cup B)^{\complement}$, cela signifie que $x \notin (A \cup B)$, donc x n'est ni dans A, ni dans B, autrement dit $x \notin A$ et $x \notin B$. D'où $x \in A^{\complement}$ et $x \in B^{\complement}$. Par conséquent, $x \in (A^{\complement} \cap B^{\complement})$.

$\mathbf{A^{\complement} \cap B^{\complement} \subset (A \cup B)^{\complement}}$ **:** Il nous faut montrer que tout élément de $A^{\complement} \cap B^{\complement}$ est également un élément de $(A \cup B)^{\complement}$. Pour ce faire, prenons un élément *quelconque* $x \in (A^{\complement} \cap B^{\complement})$. Cet x appartient à la fois à $A^{\complement}$ et $B^{\complement}$. Donc $x \notin A$ et $x \notin B$ sont tous les deux vérifiés. Puisque x n'appartient ni à A, ni à B, x n'appartient pas à l'union de A et de B. Cela s'écrit $x \notin (A \cup B)$ et n'est pas autre chose que $x \in (A \cup B)^{\complement}$.

Pour la seconde égalité nous pouvons directement utiliser ce que nous venons de prouver. En effet, considérons $A^{\complement} \cup B^{\complement}$, ou plutôt son complémentaire, c'est-à-dire $(A^{\complement} \cup B^{\complement})^{\complement}$. D'après la Proposition (1)

$$(A^{\complement} \cup B^{\complement})^{\complement} = A^{\complement^{\complement}} \cap B^{\complement^{\complement}}.$$

Et comme le complémentaire du complémentaire n'est autre que l'ensemble lui-même on obtient : .

$$(A^{\complement} \cup B^{\complement})^{\complement} = A \cap B.$$

Par conséquent, si ces ensembles sont égaux, leurs complémentaires aussi sont égaux :

$$(A^{\complement} \cup B^{\complement})^{\complement^{\complement}} = (A \cap B)^{\complement}.$$

D'où il ressort que $(A^{\complement} \cup B^{\complement}) = (A \cap B)^{\complement}$.

$\dashv$ 3

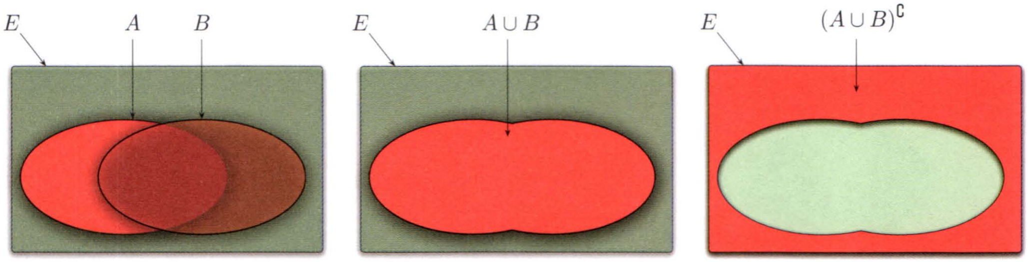


FIGURE 32 – construction de $(A \cup B)^{\complement}$.

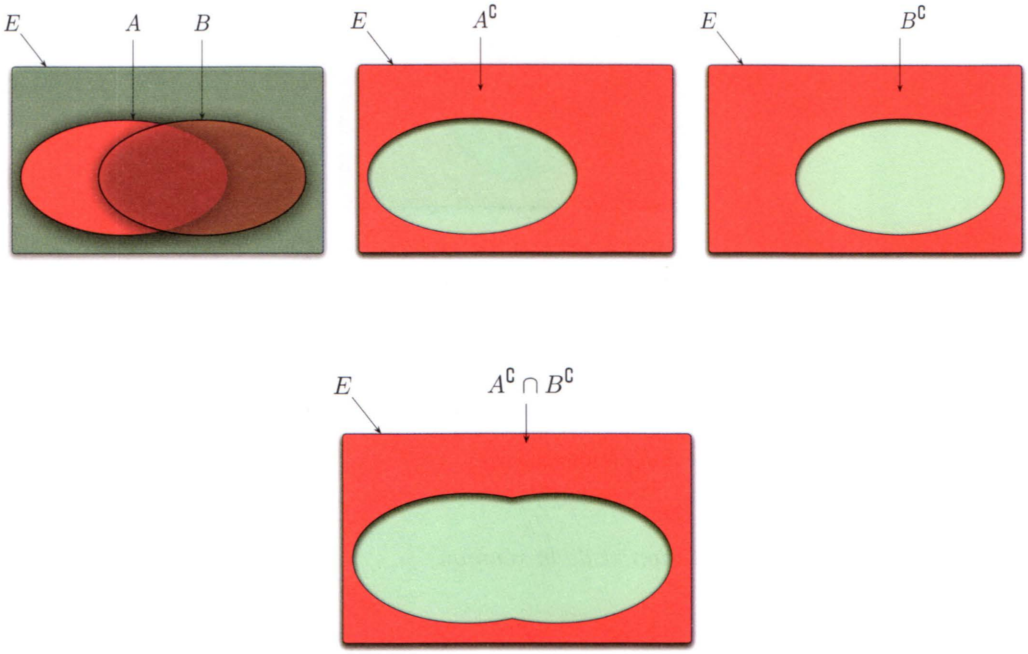


FIGURE 33 – construction de $A^{\complement} \cap B^{\complement}$.

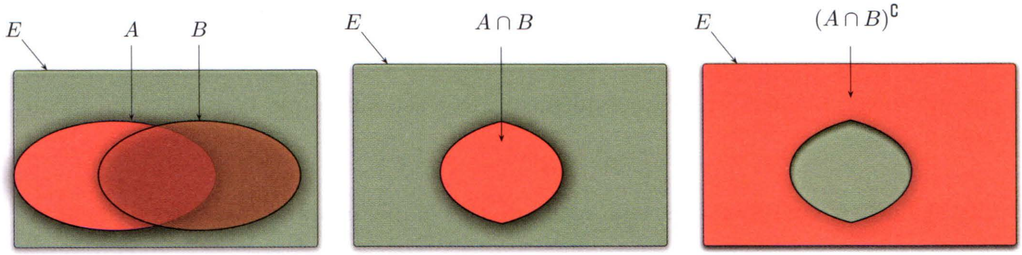


FIGURE 34 – construction de $(A \cap B)^{\complement}$.

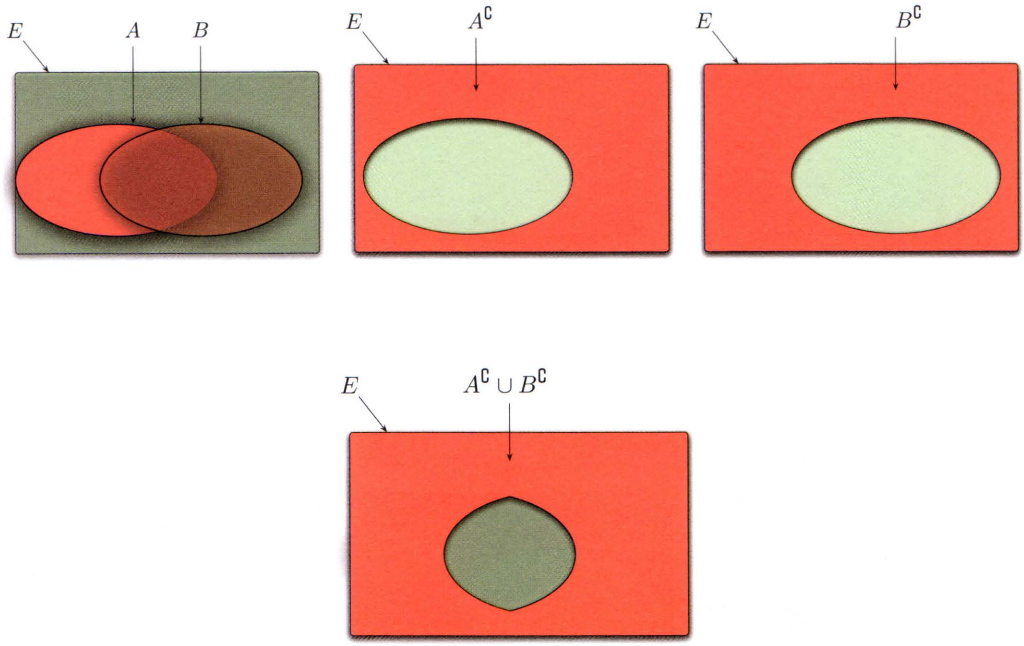


FIGURE 35 – construction de $A^{\complement} \cup B^{\complement}$.

Proposition 4 *Pour tous ensembles A, B les relations suivantes sont vérifiées :*

(1) élimination de la double complémentation

- $A^{\complement^{\complement}} = A$

(2) idempotence de l'intersection et de la réunion

- $(A \cap A) = A$
- $(A \cup A) = A$

(3) commutativité de l'intersection et de la réunion

- $(A \cap B) = (B \cap A)$

∘ $(A \cup B) = (B \cup A)$

(4) associativité de l'intersection et de la réunion

∘ $(A \cap B) \cap C = A \cap (B \cap C)$

∘ $(A \cup B) \cup C = A \cup (B \cup C)$

(5) distributivité de l'intersection par rapport à la réunion et réciproquement

∘ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

∘ $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

(6) lois d'absorption

∘ $A \cap (A \cup B) = A$

∘ $A \cup (A \cap B) = A$

(7) lois de De Morgan

∘ $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$

∘ $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$

(8) contraposée

∘ $A \subset B$ *si et seulement si* $B^{\complement} \subset A^{\complement}$.

Preuve de la Proposition 4 : laissée au lecteur à titre d'exercices.

$\dashv$ 4

3. Application aux syllogismes

Tous les hommes sont mortels... En guise d'échauffement, nous allons nous intéresser au syllogisme d'Aristote le plus connu :

∘ *tous les hommes sont mortels,*
∘ or *tous les Grecs sont des hommes,*
∘ donc *tous les Grecs sont mortels.*

Ce syllogisme mentionne trois propriétés : *"être homme", "être grec", "être mortel"*. Chacune de ces propriétés, à l'intérieur d'un ensemble E pris suffisamment large – par exemple l'ensemble de toutes les choses sur terre à l'époque d'Aristote – définit un ensemble : *l'ensemble des hommes, l'ensemble des Grecs, l'ensemble des mortels.* Nous commençons par dessiner de la manière la plus générale possible trois patates : $A =$*l'ensemble des hommes,* $B =$ *l'ensemble des Grecs,* $C =$*l'ensemble des mortels.* En sorte qu'apparaissent distinctement 2^3 régions de l'espace correspondant à :

(1) $A \cap B \cap C$	(3) $A \setminus (B \cup C)$	(5) $B \setminus (A \cup C)$	(7) $C \setminus (A \cup B)$
(2) $A \cap B \setminus C$	(4) $B \cap C \setminus A$	(6) $C \cap A \setminus B$	(8) $(A \cup B \cup C)^{\complement}$

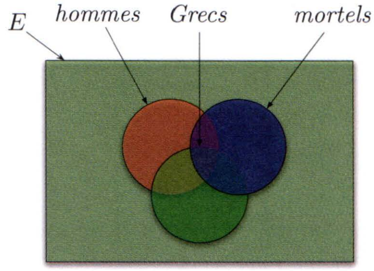


FIGURE 36 – les trois ensembles du syllogisme.

Ensuite nous considérons la première prémisse : *tous les hommes sont mortels.* Elle nous indique que *l'ensemble des hommes* est inclus dans *l'ensemble des mortels.* Nous faisons alors en sorte d'effacer la partie de la patatoïde représentant *l'ensemble des hommes* qui n'est pas incluse dans *l'ensemble des mortels.* Autrement dit, nous effaçons la région correspondant à $A \setminus C$ (*ens. des hommes* $\setminus$ *ens. des mortels*).

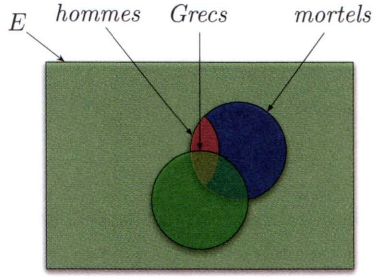


FIGURE 37 – après la prise en compte de la première prémisse.

Puis nous considérons la seconde prémisse : *tous les Grecs sont des hommes.* Elle nous indique que *l'ensemble des Grecs* est inclus dans *l'ensemble des hommes.* Nous faisons dès lors en sorte d'effacer la partie de la patate représentant *l'ensemble des Grecs* qui n'est pas incluse dans *l'ensemble des hommes.* Nous effaçons la région correspondant à $B \setminus A$ (*ens. des Grecs* $\setminus$ *ens. des hommes*).

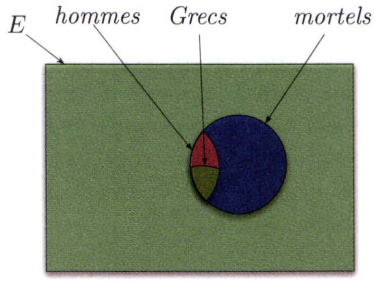


FIGURE 38 – après la prise en compte de la seconde prémisse.

Nous considérons enfin la conclusion : *tous les Grecs sont mortels.* Elle affirme que *l'ensemble des Grecs* est inclus dans *l'ensemble des mortels.* Nous vérifions que c'est bien le cas sur notre figure. Donc effectivement, si l'on admet les deux prémisses, on doit également admettre la conclusion.

Chacune des deux prémisses définit une condition sur l'inclusion d'ensemble : *tous les hommes sont mortels* dit que l'ensemble des hommes est inclus dans celui des mortels ; *tous les Grecs sont des hommes* dit que l'ensemble des Grecs est inclus dans celui des hommes. Les deux inclusions sont telles que dessinées dans la figure qui suit – mais l'étaient tout autant dans la figure précédente.

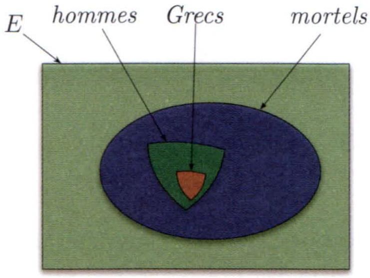


FIGURE 39 – les inclusions induites par les deux prémisses.

Considérons maintenant un second type de syllogisme :
- *tout athénien est grec,*
- or *quelque athénien est philosophe,*
- donc *quelque philosophe est grec.*

Ce syllogisme mentionne trois propriétés : *"être athénien"* , *"être grec"*, *"être philosophe"*. Ces propriétés, à l'intérieur d'un ensemble E suffisamment large définissent les ensembles : A =*l'ensemble des athéniens*, G =*l'ensemble des Grecs*, P =*l'ensemble des philosophes.* Nous dessinons de la manière la plus générale possible trois patates, en sorte qu'apparaissent distinctement 2^3 régions de l'espace correspondant à :

(1) $A \cap G \cap P$	(3) $A \setminus (G \cup P)$	(5) $G \setminus (A \cup P)$	(7) $P \setminus (A \cup G)$
(2) $A \cap G \setminus P$	(4) $G \cap P \setminus A$	(6) $P \cap A \setminus G$	(8) $(A \cup G \cup P)^{\complement}$

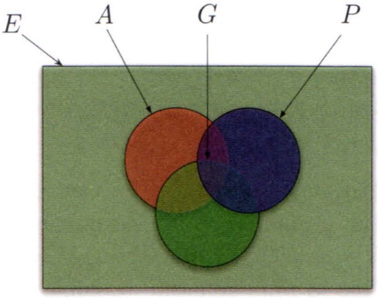


FIGURE 40 – les trois ensembles du syllogisme.

En prenant en compte la première prémisse (*tous les athéniens sont grecs*) qui indique que *l'ensemble des athéniens* est inclus dans *l'ensemble des Grecs*, nous obtenons le schéma suivant :

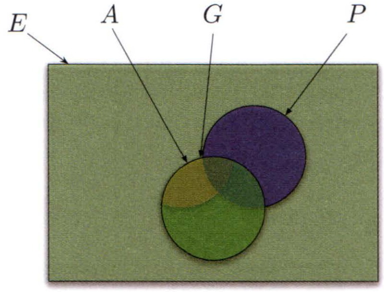


FIGURE 41 – après la prise en compte de la première prémisse.

Puis nous considérons la seconde prémisse : *quelque athénien est philosophe.* Elle nous informe que *l'intersection de l'ensemble des athéniens et de l'ensemble des philosophes* est non vide. Nous mettons donc une croix dans cet ensemble pour indiquer qu'il y a au moins un élément qui s'y trouve.

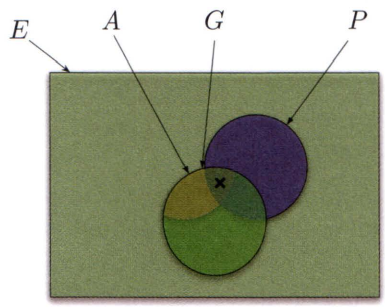


FIGURE 42 – après la prise en compte de la seconde prémisse.

Nous considérons enfin la conclusion : *quelque Grec est philosophe.* Elle affirme que *l'intersection de l'ensemble des Grecs avec celui des philosophes* est non vide. Ce que nous reconnaissons immédiatement grâce à la présence de la petite croix dans cette intersection.

Attelons-nous à un troisième exemple de syllogisme :

- *aucun béotien n'est athénien,*
- or *tout athénien est grec,*
- donc *quelque Grec n'est pas béotien.*

Ce syllogisme mentionne trois propriétés : *"être béotien"*, *"être athénien"*, *"être grec"*. Ces propriétés, à l'intérieur d'un ensemble E suffisamment large définissent les ensembles : B =*l'ensemble des béotiens*, G =*l'ensemble des Grecs*, A =*l'ensemble des athéniens.* Nous dessinons toujours de la manière la plus générale possible trois patates, en sorte qu'apparaissent distinctement 2^3 régions de l'espace correspondant à :

(1) $A \cap G \cap B$ (3) $A \setminus (G \cup B)$ (5) $G \setminus (A \cup B)$ (7) $B \setminus (A \cup G)$

(2) $A \cap G \setminus B$ (4) $G \cap B \setminus A$ (6) $B \cap A \setminus G$ (8) $(A \cup G \cup B)^{\complement}$

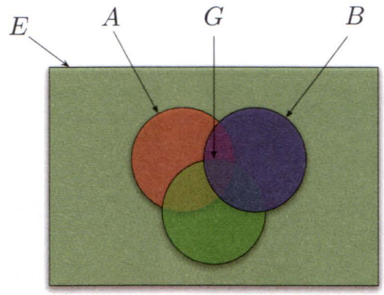


FIGURE 43 – les trois ensembles du syllogisme.

Prenons en compte la première prémisse : *aucun béotien n'est athénien*. Elle indique que *l'intersection entre l'ensemble des béotiens et celui des athéniens* est vide. Nous obtenons donc le schéma qui suit :

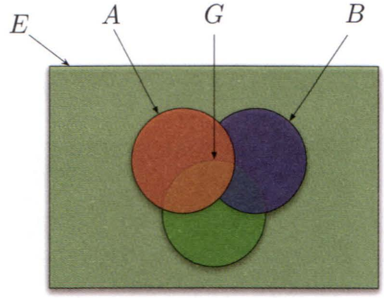


FIGURE 44 – après la prise en compte de la première prémisse.

Puis nous considérons la seconde prémisse : *tout athénien est grec*. Elle nous indique que *l'ensemble des athéniens est inclus dans l'ensemble des Grecs*. Ce qui donne :

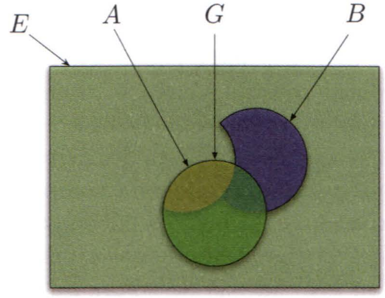


FIGURE 45 – après la prise en compte de la seconde prémisse.

Nous considérons enfin la conclusion : *quelque Grec n'est pas béotien*. Et là, à notre grande surprise, nous ne pouvons conclure du dessin que nous avons fait que cette conclusion s'impose. En effet, il faudrait pour cela que l'un des deux ensembles précisés ci-dessous soit non vide.

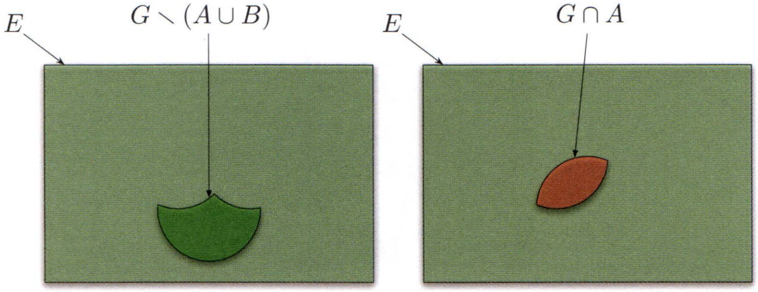


FIGURE 46 – la conclusion exige que l'un des ensembles soit non vide.

Or rien ne nous permet de dire cela... Il n'y a aucune raison pour laquelle l'ensemble $G \setminus (A \cup B)$ soit non vide. En tout cas rien ne permet d'affirmer dans les hypothèses qu'il existe au moins un Grec qui ne soit ni athénien ni béotien. De même, rien ne nous permet de dire qu'il existe un athénien qui soit béotien. En effet, il se pourrait très bien qu'il n'y ait pas d'athénien du tout. On se retrouverait avec le schéma suivant :

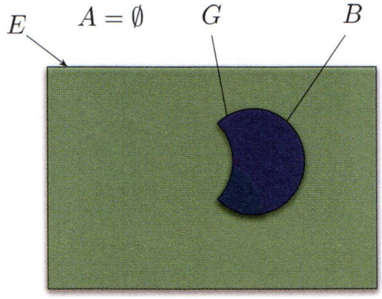


FIGURE 47 – un cas de figure dans lequel la conclusion ne s'applique pas.

Nous venons de montrer que ce syllogisme n'est pas valide. La conclusion ne ressort pas de la prise en considération des deux prémisses.

Et pourtant... ce syllogisme était considéré par les Grecs et leurs suivants comme valide. Mais aujourd'hui nous ne le considérons plus comme valide. Que s'est-il passé entre eux et nous ? Avaient-ils tort de considérer ce syllogisme comme concluant et nous raison ? Avons-nous tort ? Avons-nous tous les deux raisons ? Cette dernière possibilité semble devoir tout de suite être écartée. Sauf si... nous admettons que nous comprenons les énoncés des prémisses dans deux sens différents. Et c'est en effet bien ce qui se passe. Actuellement, lorsque nous disons *tout trozoï est glichnik*, cela signifie qu'il n'y a pas de *trozoï* qui ne soit *glichnik*, et cela reste vrai dans le cas où il n'y a pas de *trozoï* du tout. Alors que pour les Grecs, lorsqu'on dit *tout trozoï est glichnik*, cela suppose également qu'il existe au moins un *trozoï* (qui par conséquent se trouve être également *glichnik*). Autrement dit, pour les Grecs, *"tout trozoï est glichnik"* implique *"quelque trozoï est glichnik"*.

Si maintenant nous reprenons les schémas successifs que nous avons pris en compte en y ajoutant cette donnée supplémentaire, cela nous conduit à :

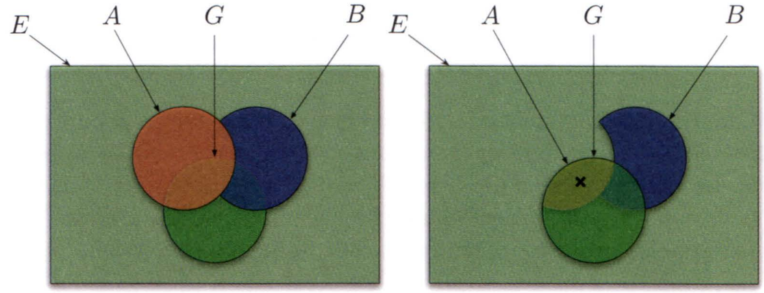


FIGURE 48 – après la prise en compte de la première, puis de la seconde prémisse.

Et la conclusion s'impose alors dans toute sa clarté.

Pourquoi avons-nous adopter une convention différente de celle des Grecs ou du Moyen-Âge ? Pourquoi préférons-nous convenir que *"tout trozoï est glichnik"* soit vrai, quand bien même il n'existe pas de *trozoï* ? Une raison simple à cela consiste à regarder ce qui se passe lorsque nous prenons la négation de cet énoncé. Il semble naturel que s'il n'est pas vrai que *"tout trozoï est glichnik"*, alors nous devrions être capable de produire un individu qui soit *trozoï* mais non *glichnik*. Or nous ne pouvons le faire dans le cas où il n'existe pas de *trozoï* du tout. Si nous voulons que *"tout trozoï est glichnik"* soit la négation de *"il existe un trozoï qui n'est pas glichnik"*, alors cette première affirmation doit être vraie lorsqu'il n'y a pas de *trozoï*.

L'acception des Grecs fait de la négation de *"tout trozoï est glichnik"* l'affirmation *"il existe un trozoï qui n'est pas glichnik ou bien il n'existe pas de trozoï du tout"*.

4. Les syllogismes

La science des syllogismes s'appelle la syllogistique. Elle a été enseignée d'Aristote jusqu'à la fin du XIX^e siècle [14].

En logique aristotélicienne, le syllogisme (terme provenant du grec ancien "$\sigma\upsilon\lambda\lambda o\gamma\iota\sigma\mu\acute{o}\varsigma$" lui-même construit sur la base des termes *syn* et *logos* "parole qui va avec" – une autre parole) est une forme de raisonnement qui fait intervenir trois propositions :

- deux hypothèses que l'on appelle les prémisses ($\mathbf{P_1}$ = *tout homme est mortel*, $\mathbf{P_2}$ = *Socrate est un homme*),
- et une conclusion ($\mathbf{C}$ = *Socrate est mortel*).

Plus tard, nous écrirons formellement toute preuve de ce type sous la forme : $\mathbf{P_1}, \mathbf{P_2} \vdash \mathbf{C}$. A gauche du symbole de preuve "$\vdash$", nous indiquerons les hypothèses que nous prenons en considération, et à sa droite nous placerons la conclusion. Et nous lirons "$\mathbf{P_1}, \mathbf{P_2} \vdash \mathbf{C}$" comme signifiant : "en supposant $\mathbf{P_1}$ et $\mathbf{P_2}$, nous parvenons à la conclusion $\mathbf{C}$". Ou plus généralement : "les hypothèses $\mathbf{P_1}$ et $\mathbf{P_2}$ prouvent $\mathbf{C}$".

14. Aristote : *Premiers Analytiques* [Ari92] ; Antoine Arnauld indexauArnauld, Antoine et Pierre Nicole : *La logique ou L'art de penser* [AN92] ; Leibniz : *Dissertatio de Arte Combinatoria* [Lei12].

P_1	tous les hommes sont mortels
P_2	tous les Grecs sont des hommes
C	tous les Grecs sont mortels

La manière dont le raisonnement se déroule consiste à mettre en rapport dans la conclusion deux termes : le *majeur* et le *mineur*, au moyen d'un terme que l'on appelle précisément le *moyen terme*. Le *majeur* et le *mineur* ne doivent apparaître qu'une fois chacun dans les prémisses, le *moyen terme* est présent dans chaque prémisse. La prémisse qui contient le terme *majeur* est appelée *prémisse majeure*, et celle qui contient le terme *mineur* : *prémisse mineure*.

P_1	tous les *hommes*	sont	*mortels*
P_2	tous les *Grecs*	sont	des *hommes*
C	tous les *Grecs*	sont	*mortels*

Ainsi, les termes majeur, mineur et moyen désignent des propriétés qui sont attribuées à des objets, ou pour le dire autrement, ces termes désignent chacun un ensemble d'objets : précisément ceux qui tombent sous leur extension. Il est ainsi facile de voir dans l'exemple qui précède que le moyen terme concerne la propriété "être un homme" – autrement dit l'ensemble des hommes – puisque c'est la seule propriété qui se situe dans les deux prémisses à la fois. Mais où sont le majeur et le mineur ? Généralement, le majeur se trouve dans la première prémisse et le mineur dans la seconde. Mais ce n'est pas l'ordre des arguments qui définit majeur et mineur. Le terme majeur est celui le plus général – celui dont l'extension est la plus grande –, alors que le mineur est le plus particulier – celui dont l'extension est la plus restreinte.

P_1	Aucun *Dieu*	n'est	*mortel*
P_2	quelque *homme*	est	*mortel*
C	quelque *homme*	n'est pas	un *Dieu*

P_1	quelque *homme*	n'est pas	*philosophe*
P_2	tout *homme*	est	*bipède*
C	quelque *bipède*	n'est pas	*philosophe*

Le moyen terme est présent dans chacune des prémisses. Dans chacune des prémisses, il est mis en relation avec un autre terme – le majeur et le mineur. Mais la manière dont il est mis en relation avec chacun de ces autres termes peut prendre les deux formes suivantes :

- l'ensemble de ce qui tombe sous l'extension du moyen terme tombe également sous celle du second terme, ou bien

- l'ensemble de ce qui tombe sous l'extension du second terme tombe sous celle du moyen terme.

C'est là la différence entre les deux propositions "quelque *homme* est *philosophe*" et "quelque *philosophe* est *homme*" dans les deux syllogismes qui suivent.

$\mathbf{P_1}$	quelque *homme*	est	*philosophe*
$\mathbf{P_2}$	tout *homme*	est	*bipède*
C	quelque *bipède*	est	*philosophe*

$\mathbf{P_1}$	quelque *philosophe*	est	*homme*
$\mathbf{P_2}$	tout *homme*	est	*bipède*
C	quelque *philosophe*	est	*bipède*

Le terme majeur et le terme mineur se retrouvent seuls dans la conclusion. Le moyen terme n'aura servi que de transition, de tremplin en quelque sorte, pour faire se rejoindre majeur et mineur. Majeur et mineur se rejoignent donc dans la conclusion qui n'est autre qu'une proposition de la forme *sujet (**S**) copule prédicat (**P**)*. Nous avons vu que le sujet comme le prédicat induisaient chacun, par l'extension de leur désignation, un ensemble. Comme il en est de même du moyen terme (**M**), il est tout naturel de comparer les extensions de ces différents ensembles au moyen de l'inclusion : est-ce que $\mathbf{M} \subset \mathbf{S}$ ou bien $\mathbf{S} \subset \mathbf{M}$? Est-ce que $\mathbf{M} \subset \mathbf{P}$ ou bien $\mathbf{P} \subset \mathbf{M}$?

C'est précisément la position de ce moyen terme qui donne lieu à ce que la tradition a convenu d'appeler les quatre figures du syllogisme [AN92] :

- *1ère figure :* $\mathbf{M} \subset \mathbf{P}$ et $\mathbf{S} \subset \mathbf{M}$
- *2ème figure :* $\mathbf{P} \subset \mathbf{M}$ et $\mathbf{S} \subset \mathbf{M}$
- *3ème figure :* $\mathbf{M} \subset \mathbf{P}$ et $\mathbf{M} \subset \mathbf{S}$
- *4ème figure :* $\mathbf{P} \subset \mathbf{M}$ et $\mathbf{M} \subset \mathbf{S}$

Que ce soient les deux prémisses ou la conclusion, chacune des trois est une proposition de la forme *sujet* relié par une copule à un *prédicat* :

- quelque *Dieu* est *courroucé*
- tout *homme* est *bipède*
- *Socrate* est *un homme*
- quelque *Grec* n'est pas *béotien*

Il est clair que la copule [15] indique ceci : des individus [16] vérifiant la propriété spécifiée par le sujet vérifient également – ou ne vérifient pas du tout – celle que mentionne le prédicat. *S est P* signifie que tous les individus qui satisfont la propriété *S* satisfont également la propriété *P*.

Pour Aristote et tous les tenants de la syllogistique, une même proposition *S est P* peut subir des modifications de *quantité* et de *qualité*.

15. Le plus souvent *"est"* ou *"sont"*.
16. *Tous* ou *certains* ou *quelque* ou *aucun*, suivant les cas.

La *qualité* est ce qui distingue les deux propositions suivantes : *Socrate est bipède* et *Socrate n'est pas bipède.* Ces deux propositions ont les mêmes sujets et les mêmes prédicats, mais la première est *affirmative* alors que la seconde est *négative.* Il en est de même par exemple de *tout homme est bipède* et de *aucun homme n'est bipède*, puisque la seconde n'est autre que la négation de la première. Nous utiliserons la notation suivante : si ϕ tient lieu de la proposition *"S est P"*, nous écrirons $\neg\phi$ pour la négation de *"S est P"*, autrement dit *"S n'est pas P"*.

La *quantité* est ce qui distingue *tout homme est bipède* de *quelque homme est bipède.* Ces deux propositions partagent les mêmes sujets ainsi que les mêmes prédicats, mais la première *quantifie* le sujet de manière *universelle*, alors que la seconde le fait de manière *particulière*[17]. Un autre exemple serait *aucun Dieu n'est mortel*[18] et *quelque Dieu n'est pas mortel.* Si ϕ tient lieu de la proposition *S est P*, nous écrirons $\exists x\ \phi$ pour la proposition particulière *quelque (individu vérifiant) S est P*, et $\forall x\ \phi$ pour la proposition universelle *tout (individu vérifiant) S est P.*

En résumé, si ϕ désigne *S est P*, où le sujet (S) est *homme* et le prédicat (P) est *mortel*, en distinguant suivant la qualité et la quantité, nous obtenons les quatre propositions qui suivent :

(1) proposition universelle affirmative : $\forall x\ \phi$ (*tout homme est mortel*),

(2) proposition universelle négative : $\forall x\ \neg\phi$ (*aucun homme n'est mortel*[19]),

(3) proposition particulière affirmative : $\exists x\ \phi$ (*quelque homme est mortel*),

(4) proposition particulière négative : $\exists x\ \neg\phi$ (*quelque homme n'est pas mortel*).

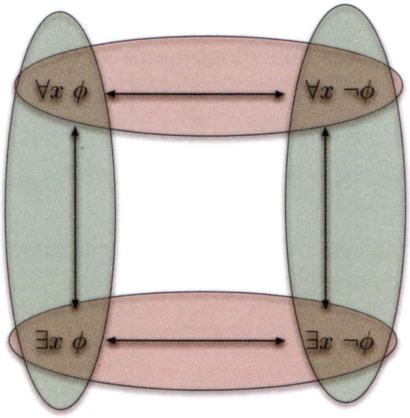


FIGURE 49 – qualités identiques et quantités identiques.

Il va sans dire que la notation – $\forall x\ \phi$, $\forall x\ \neg\phi$, $\exists x\ \phi$, $\exists x\ \neg\phi$ – est très récente. Elle est en fait issue de la logique des prédicats (encore appelée logique du 1er ordre). Pendant

17. Nous dirions aujourd'hui que cette quantification est *existentielle.*

18. Quantification universelle, puisque *aucun Dieu n'est mortel* signifie *tous les Dieux sont immortels*, la quantification porte sur tous les Dieux et non sur certains d'entre eux.

19. *Stricto sensu* il nous faudrait écrire *tout homme est non mortel* ou bien *tout homme est immortel.*

tout l'enseignement de la syllogistique, des voyelles sont attribuées à chacun de ces types de propositions.

(1) proposition notée A, universelle affirmative : $\forall x\ \phi$,

(2) proposition notée E, universelle négative : $\forall x\ \neg\phi$,

(3) proposition notée I, particulière affirmative : $\exists x\ \phi$,

(4) proposition notée O, particulière négative : $\exists x\ \neg\phi$.

Le choix des lettres (A,E,I,O) provient du latin *AffIrmo* et *nEgO* qui signifient respectivement *j'affirme* et *je nie*. La première voyelle de chacun de ces deux termes correspond à la proposition universelle et la seconde à la proposition particulière.

La tradition scolastique s'est également pourvue de dénominations pour caractériser les relations de ces propositions entre elles :

- Deux propositions qui s'opposent à la fois par la qualité et la quantité sont dites *contradictoires*. C'est le cas de $\forall x\ \phi$ et $\exists x\ \neg\phi$ d'une part ; et de $\forall x\ \neg\phi$ et $\exists x\ \phi$ d'autre part. (*Tous les hommes sont mortels* et *quelque homme est immortel*; et *aucun homme n'est immortel* et *quelque homme est immortel*).
- Deux propositions *contraires* sont des propositions universelles qui s'opposent par la qualité. C'est donc le cas de $\forall x\ \phi$ (*tous les hommes sont mortels*) et de $\forall x\ \neg\phi$ (*aucun homme n'est mortel*).
- Deux propositions particulières qui s'opposent par la qualité sont dites *subcontraires*. C'est ainsi le cas de $\exists x\ \phi$ (*quelque homme est mortel*) et de $\exists x\ \neg\phi$ (*quelque homme n'est pas mortel*).
- Deux propositions qui s'opposent par la quantité sont dites *subalternes*. C'est le cas des propositions affirmatives $\forall x\ \phi$ et $\exists x\ \phi$, ainsi que des propositions négatives $\forall x\ \neg\phi$ et $\exists x\ \neg\phi$. Cela donne par exemple l'opposition subalterne entre *tous les homme sont mortels* et *quelque homme est mortel*, ou bien celle entre *aucun homme n'est mortel* et *quelque homme est immortel*.

Ces relations sont présentées traditionnellement sous la forme d'une figure géométrique appelée le *carré des oppositions* [AN92].

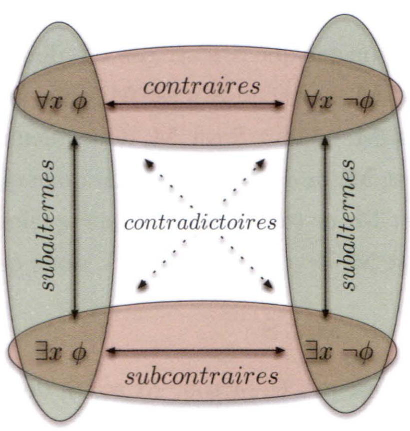


FIGURE 50 – carré des oppositions.

Il est temps de faire le point. Nous savons désormais les choses suivantes :

- chaque syllogisme est constitué de trois propositions (les deux prémisses et la conclusion),
- que chacune de ces propositions peut prendre l'une des quatre formes A,E,I,O ;
- les rapports entre mineur, majeur et moyen termes s'organisent suivant quatre figures possibles.

Cela laisse donc la place à 4 types (A,E,I,O) pour la première prémisse $\times$ 4 types pour la seconde prémisse $\times$ 4 types pour la conclusion $\times$ 4 figures. Ce qui nous fait $4 \times 4 \times 4 \times 4 = 4^4 = 256$ modes possibles.

Parmi ces 256 modes possibles, seuls 24 sont concluants, c'est-à-dire qu'ils produisent un raisonnement correct – également appelé valide. Ces 24 modes concluants se distribuent harmonieusement puisqu'il y en a exactement 6 pour chacune des 4 figures. De plus, à chacun de ces 24 modes valides, la tradition scolastique a attribué un nom qui n'a pas de signification particulière mais constitue un moyen mnémotechnique pour se souvenir de l'agencement des types (A,E,I,O) dans les prémisses et la conclusion. Ainsi "Barbari" signifie que les prémisses sont de type A – ce sont des propositions affirmatives universelles – et la conclusion est de type I – affirmative particulière – tandis que "Celarent"indique que la seconde prémisse est de type A, la première prémisse et la conclusion étant toutes deux de type E – négatives universelles.

Les modes concluants de la :

- *1ère figure :* $\mathbf{M} \subset \mathbf{P}$ et $\mathbf{S} \subset \mathbf{M}$

(1) Barbara : tout **M** est **P**, or tout **S** est **M**, donc tout **S** est **P**

(2) Celarent : aucun **M** n'est **P**, or tout **S** est **M**, donc aucun **S** n'est **P**

(3) Darii : tout **M** est **P**, or quelque **S** est **M**, donc quelque **S** est **P**

(4) Ferio : aucun **M** n'est **P**, or quelque **S** est **M**, donc quelque **S** n'est pas **P**

(5) Barbari : tout **M** est **P**, or tout **S** est **M**, donc quelque **S** est **P**

(6) Celaront : aucun **M** n'est **P**, or tout **S** est **M**, donc quelque **S** n'est pas **P**

- *2ème figure :* $\mathbf{P} \subset \mathbf{M}$ et $\mathbf{S} \subset \mathbf{M}$

(1) Baroco : tout **P** est **M**, or quelque **S** n'est pas **M**, donc quelque **S** n'est pas **P**

(2) Camestres : tout **P** est **M**, or aucun **S** n'est **M**, donc aucun **S** n'est **P**

(3) Cesare : aucun **P** n'est **M**, or tout **S** est **M**, donc aucun **S** n'est **P**

(4) Festino : aucun **P** n'est **M**, or quelque **S** est **M**, donc quelque **S** n'est pas **P**

(5) Cesaro : aucun **P** n'est **M**, or tout **S** est **M**, donc quelque **S** n'est pas **P**

(6) Camestrop : tout **P** est **M**, or aucun **S** n'est **M**, donc quelque **S** n'est pas **P**

- *3ème figure :* $\mathbf{M} \subset \mathbf{P}$ et $\mathbf{M} \subset \mathbf{S}$

(1) Bocardo : quelque **M** n'est pas **P**, or tout **M** est **S**, donc quelque **S** n'est pas **P**

(2) Darapti : tout **M** est **P**, or tout **M** est **S**, donc quelque **S** est **P**

(3) Datisi : tout **M** est **P**, or quelque **M** est **S**, donc quelque **S** est **P**

(4) Disamis : quelque **M** est **P**, or tout **M** est **S**, donc quelque **S** est **P**

(5) Felapton : aucun **M** n'est **P**, or tout **M** est **S**, donc quelque **S** n'est pas **P**

(6) Ferison : aucun **M** n'est **P**, or quelque **M** est **S**, donc quelque **S** n'est pas **P**

- *4ème figure (dite Galénique) :* $\mathbf{P} \subset \mathbf{M}$ et $\mathbf{M} \subset \mathbf{S}$

(1) Bamalip : tout **P** est **M**, or tout **M** est **S**, donc quelque **S** est **P**

(2) Camenes : tout **P** est **M**, or aucun **M** n'est **S**, donc aucun **S** n'est **P**

(3) Dimatis : quelque **P** est **M**, or tout **M** est **S**, donc quelque **S** est **P**

(4) Fesapo : aucun **P** n'est **M**, or tout **M** est **S**, donc quelque **S** n'est pas **P**

(5) Fresison : aucun **P** n'est **M**, or quelque **M** est **S**, donc quelque **S** n'est pas **P**

(6) Calemop : tout **P** est **M**, or aucun **M** n'est **S**, donc quelque **S** n'est pas **P**

Il serait extrêmement fastidieux de passer en revue ces 256 modes et de montrer, pour chaque figure, que 58 d'entre eux ne sont pas concluants et seuls les 6 mentionnés le sont. Nous allons simplement, en guise d'exemple, nous intéresser à deux cas.

Tout d'abord attachons-nous au cas (2) Celarent de la première figure :

(A) Celarent : aucun **M** n'est **P**, or tout **S** est **M**, donc aucun **S** n'est **P**.

La résolution de ce syllogisme donne la succession des diagrammes de Venn suivants :

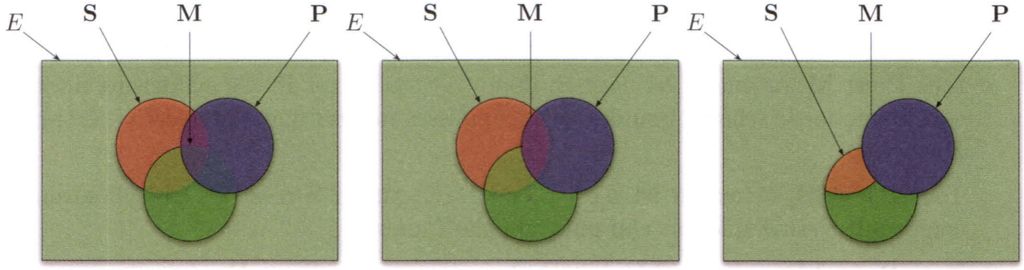


FIGURE 51 – Celarent : aucun **M** n'est **P**, or tout **S** est **M**, donc aucun **S** n'est **P**.

Il apparaît clairement dans le troisième schéma qu'aucun **S** n'est **P**. Le syllogisme est donc concluant.

Il n'en est pas de même si nous remplaçons le mode EAE par le mode EAA. Autrement dit, aucun **M** n'est **P**, or tout **S** est **M**, donc tout **S** est **P**, n'est pas un raisonnement valide. On s'en convainc aisément puisque la prise en compte des deux premières prémisses nous conduit aux mêmes schémas ci-dessus que pour le mode EAE, mais bien sûr si la conclusion aucun **S** n'est **P** s'imposait, la nouvelle conclusion tout **S** est **P** montre son invalidité.

Plus généralement, si l'on s'attache à la première figure et que les deux premières prémisses sont de type EA, il s'en suit que la conclusion ne peut être que de type E (aucun **S** n'est **P**) ou bien de type O (quelque **S** n'est **P**)[20].

20. Ici encore, il faut faire attention à ce que "aucun **S** n'est **P**" relève pour les Grecs d'une quantification universelle qui implique une quantification existentielle. Autrement dit, "aucun **S** n'est **P**" signifie que tous les individus qui tombent sous l'extension de **S** sortent de l'extension de **P** ; or "tous les individus" entraîne qu'il existe au moins un individu qui satisfait cette propriété.

Attachons-nous ensuite au dernier cas (6) Calemop de la quatrième figure :

(B) Calemop : tout **P** est **M**, or aucun **M** n'est **S**, donc quelque **S** n'est pas **P**.

La résolution de ce syllogisme donne la succession des diagrammes de Venn suivants :

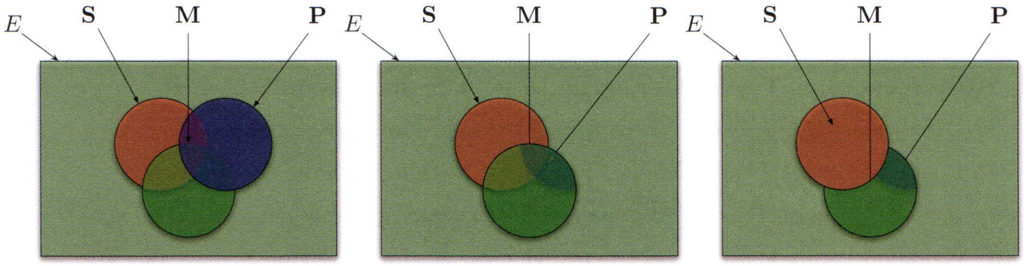


FIGURE 52 – Calemop : tout **P** est **M**, or aucun **M** n'est **S**, donc quelque **S** n'est pas **P**.

Comme tel, le syllogisme ne semble pas concluant. C'est ici qu'il faut se souvenir que pour les Grecs, si aucun **S** n'est **P**, il s'ensuit que quelque **S** n'est pas **P**, puisque parler de tout **S** entraîne qu'il existe un individu qui satisfait **S** et donc que cet individu ne satisfait pas la propriété **P**.

Par contre, si nous conservons les mêmes deux prémisses et que nous changeons le type de la conclusion, nous ne parvenons pas nécessairement à un syllogisme concluant :

- tout **P** est **M**, or aucun **M** n'est **S**, donc (A) tout **S** est **P**. Ce syllogisme n'est pas concluant, car le schéma issu des deux prémisses montre que l'intersection entre **S** et **P** est vide.
- Tout **P** est **M**, or aucun **M** n'est **S**, donc (E) aucun **S** n'est **P**. Ce syllogisme est concluant, c'est d'ailleurs celui qui s'appelle Camenes.
- Tout **P** est **M**, or aucun **M** n'est **S**, donc (I) quelque **S** est **P**. Ce syllogisme n'est pas concluant, puisque au contraire aucun **S** n'est **P**.

5. Les limitations du syllogisme

Afin de mesurer à quel point le syllogisme a revêtu une importance capitale pendant toute la période qui court de la Grèce antique avec Aristote jusqu'au XIX^{e} siècle et les premiers linéaments de la logique symbolique, attardons-nous sur un petit texte du philosophe anglais Thomas Hobbes (1588 – 1679), plus connu pour ses écrits de philosophie politique que pour ses textes sur la logique, qui ont pourtant influencé Leibniz.

Le premier chapitre du recueil *The English Works of Thomas Hobbes of Malmesbury : Elements of philosophy*, s'intitule *Computation or Logic* et présente entre autres choses la méthode syllogistique [Hob39]. Dans la section intitulée *of Errings, Falsity, and Captions*, l'auteur s'attache à la résolution d'un raisonnement qui a l'apparence de la validité mais se trouve être fallacieux [21] :

21. *The English Works of Thomas Hobbes of Malmesbury : Elements of philosophy*; Ed. William Molesworth; facsimile reprint of a 1839 edition by John Bohn, London, p. 62.

"The hand toucheth the pen,	*La main touche le stylo,*
The pen toucheth the paper,	*Le stylo touche la feuille,*
Therefore, The hand toucheth the paper."	*Donc, la main touche la feuille.*

Il va de soi que la main peut très bien toucher le stylo qui lui-même touche la feuille sans que la main ne touche la feuille. Ce raisonnement est évidemment fallacieux. Il s'agit donc de débusquer la supercherie, de montrer ce qui ne va pas. Confronté à un tel raisonnement, nous commencerions par dire que *"toucher"* est en fait une relation *binaire*.

Cela veut dire qu'elle met en relation deux individus, deux éléments : le premier touchant le second. De telles relations binaires sont légions, par exemple *"aimer"*, *"être le père de"*, *"avoir le même âge que"*, *"tuer"*, *"soudoyer"*, *"précéder"*, *"éclairer"*...

Nous dirions ensuite que de telles relations binaires sont sujettes à vérifier de nombreuses propriétés parmi lesquels la *réflexivité*, la *symétrie*, la *transitivité*... Or c'est précisément cette dernière, la *transitivité* qui est en question dans l'exemple de Hobbes. Une relation binaire est *transitive* si quelque soient trois éléments quelconques a, b, c, si a est en relation avec b et b est en relation avec c, alors il s'en suit que a est en relation avec c. C'est le cas par exemple de la relation *"avoir le même âge que"* : si Paul a le même âge que Zoé et Zoé a le même âge que Stéphanie, alors Paul a bien le même âge que Stéphanie. C'est également celui de la relation *"précéder"* : si a précède b qui précède c alors a précède c. Par contre la relation *"être le père de"* n'est pas transitive, car en général le grand père d'un individu n'est pas également son père. Il en va de même de la relation *"aimer"*, car il se peut très bien que Pierre aime Catherine qui aime à son tour Lionel, mais que Pierre n'aime pas du tout Lionel.

Qu'en est-il de la relation binaire *"toucher"*? Elle n'est pas transitive! Voilà ce que nous dirions aujourd'hui. Et ce raisonnement fallacieux qu'étudie Hobbes ne tient pas tout simplement parce que la relation *"toucher"* n'est pas transitive, alors que le raisonnement s'appuie sur le fait qu'elle le serait.

Mais si c'est bien là la manière dont nous aborderions cet exemple aujourd'hui, Hobbes, lui, le regarde avec les yeux de l'expert en syllogisme. Or comme nous l'avons vu, le syllogisme fait intervenir des propositions du type *"Sujet copule Prédicat"*, le *Sujet* comme le *Prédicat* sont pensés de manière extensive comme des ensembles, alors qu'une relation binaire ne peut être considérée comme un ensemble d'invidus, au mieux comme un ensemble de *couples* d'individus. Cependant, un objet et un couple d'objets sont des choses très éloignées. On peut toujours récupérer la notion d'objet à partir du couple, mais des objets dans un grand sac ne nous donnerons jamais une relation binaire.

La manière dont Hobbes analyse son exemple consiste à le rapporter à la forme syllogistique pour en déduire qu'il constitue un syllogisme mal formé, donc non concluant. Pour cela Hobbes se doit de "casser" la relation binaire. Il lui faut exprimer le fait *La main touche le stylo* non pas comme une relation entre ces deux objets que sont la main d'une part et le stylo d'autre part, mais bien sous forme d'un rapport *"Sujet copule Prédicat"*. La solution que propose Hobbes consiste donc à réécrire la phrase *"la main touche le stylo"*[22] en *"la main est touchant le stylo"*[23]. Le sujet est *"la main"*, le prédicat étant *"touchant le stylo"*.

La seconde prémisse subit le même sort. *"Le stylo touche la feuille"*[24] devient *"le stylo*

22. The hand toucheth the pen.
23. The hand is touching the pen.
24. The pen toucheth the paper.

est touchant le papier"[25]. Et selon Hobbes, il ressort de tout cela qu'il n'y a pas trois termes en jeux (majeur, moyen et mineur) mais bien quatre : *"la main"*, *"touchant le stylo"*, *"le stylo"*, *"la feuille"*. Ce serait donc un syllogisme prétendu qui n'en serait pas un du tout puisque *"touchant le stylo"* et *"le stylo"* ne sont pas les mêmes termes.

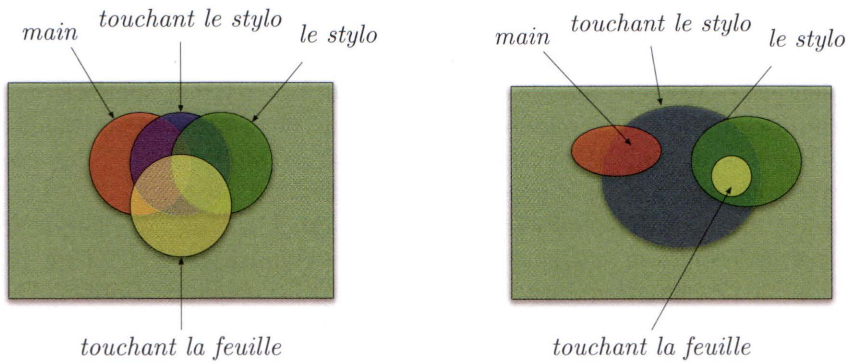


FIGURE 53 – diagrammes de Venn du "*syllogisme*" fallacieux.

On voit dans l'écart entre la manière dont Hobbes comprend la fausseté de ce raisonnement et celle qui nous apparaît aujourd'hui tout le poids que représentait la figure du syllogisme dans la logique de son temps.

Faisons maintenant quelques pas de plus en direction des limitations du syllogisme.

(1) Le syllogisme apporte une conclusion qui découle de deux hypothèses. En toute généralité un raisonnement pourra faire intervenir plus de deux hypothèses, un nombre fini voire même infini.

(2) Le syllogisme ne fait intervenir que des propositions du type *Sujet copule Prédicat*. Il s'agit du point de vue extensionnel de deux ensembles. Il ne permet pas de prendre en compte des relations binaires, encore moins des relations ternaires – à trois éléments[26].

(3) Le syllogisme ne prend pas en compte des hypothèses formellement plus sophistiquées que *Sujet copule Prédicat*. Il ne rend pas compte de propositions du type :

- *si telle chose alors telle autre,*
- *telle chose ou telle autre,*
- *si ou bien telle chose ou alors si telle autre alors une troisième, alors une quatrième...*

(4) Le syllogisme utilise la négation *a minima*, il ne prend pas en compte des hypothèses de la forme :

- *il est faux qu'aucun homme ne soit pas non mortel,*

25. The pen is touching the paper.

26. Par exemple celle qui met en relation le triptyque enfant, mère et père : R(*enfant, mère, père*), ou bien la relation qu'entretiennent le *début*, le *milieu* et la *fin* d'une histoire : H(*début, milieu, fin*).

- *si ou bien telle chose est fausse ou alors s'il est faux que telle autre soit fausse alors une troisième, alors il est faux que telle quatrième...*

(5) Le syllogisme utilise également la quantification *a minima*. Cela vient entre autre de ce qu'il ne prend pas en compte les relations binaires. Comment rendre compte, à l'intérieur d'un syllogisme, de l'énoncé suivant :

- *tout Grec a un béotien qu'il méprise ?*

Cette phrase est en effet bien différente de :

- *il y a un béotien que tous les Grecs méprisent.*

Et comment rendre compte également d'un énoncé dans lequel les quantifications universelles et existentielles [27] s'enchevêtrent :

- *toute femme aime un homme qui aime une femme qui n'aime pas tous les hommes ?*

Chacune des différentes limitations de la syllogistique que nous venons de pointer du doigt sera levée lorsque nous étudierons la logique du 1^er^ ordre, appelée la logique des prédicats. S'il s'agira bien de prédicats dans cette logique, ce ne seront pas nécessairement les prédicats tels que nous les avons rencontrés jusqu'ici. Ceux auxquels la syllogistique s'intéresse sont des prédicats appelés *"monadiques"* en logique du 1^er^ ordre. Ce sont des prédicats qui portent sur des individus par oppositions à des couples d'individus ou mêmes des triplets, voire des n-uplets d'individus.

Ainsi la science du syllogisme prendra place au sein de la logique du 1^er^ ordre. Elle s'y présentera ensuite comme un fragment de sa théorie de la démonstration. Un fragment qui pourtant était d'un poids écrasant pendant plus de deux millénaires, et demeuré quasiment indemne de toute évolution pendant tout ce temps, mais qui n'apparaît désormais que comme un cas très particulier d'un plan beaucoup plus général.

6. Quelques rudiments sur les fonctions

Afin d'avoir les idées claires, nous rappelons ici quelques notions élémentaires au sujet des objets formels que sont les *fonctions*. De manière imagée, nous pouvons dire d'ores et déjà qu'une fonction *fait quelque chose*. Une fonction prend un objet et nous en rend un autre. C'est comme une machine qui aurait une entrée et une sortie. Ce qu'elle fait réellement, on ne sait pas. On sait seulement ce que l'on obtient à la sortie en *fonction* de ce que l'on place à l'entrée.

- Une *fonction* f d'un ensemble A (appelé ensemble ou espace de *départ*) vers un ensemble B (appelé ensemble ou espace d'*arrivée*) associe à chaque élément $a \in A$ un unique élément de B que l'on note $f(a)$. On note cela de la manière suivante :

$$\begin{array}{cccccc} f & : & A & \longrightarrow & B \\ & & a & \longrightarrow & f(a). \end{array}$$

L'élément b est appelé l'*image* de a par la fonction f, tandis que a est appelé *antécédent* de b par f. Chaque élément de l'espace de départ a donc une unique image. Par contre, un élément de l'espace d'arrivée peut avoir un nombre quelconque d'antécédents, y compris aucun.

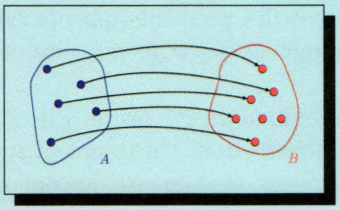
27. Particulières.

- Le *graphe* d'une telle fonction est l'ensemble des couples que forme la fonction f :

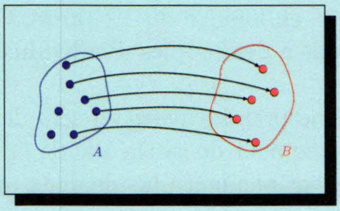
$$\mathcal{G}_f = \{(a, b) \in A \times B \mid f(a) = b\}.$$

- chaque sous ensemble $G \subseteq A \times B$ n'est pas nécessairement le graphe d'une fonction. Seuls le sont ceux qui vérifient que pour tout $a \in A$, il existe un *unique* $b \in B$, tel que $(a, b) \in G$. La fonction f telle que $\mathcal{G}_f = G$ est alors définie par le fait que pour tout $a \in A$, $f(a)$ est l'*unique* $b \in B$, tel que $(a, b) \in G$.
- On appelle *image* de f (noté $\Im m_f$) l'ensemble des éléments de l'espace d'arrivée qui ont au moins un antécédent. On parle également de l'image par f d'un sous-ensemble A' de A pour désigner l'ensemble des éléments de l'espace d'arrivée qui ont un antécédent à l'intérieur de A'.

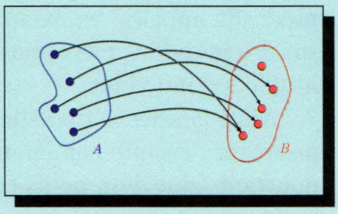
Exemples 5 Quelques exemples de graphes dont certains sont des fonctions et d'autres pas. Il est à noter que la fonction qui envoie tous les éléments de A sur un unique élément de B est appelée *fonction constante.*



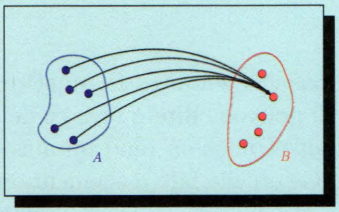
une fonction



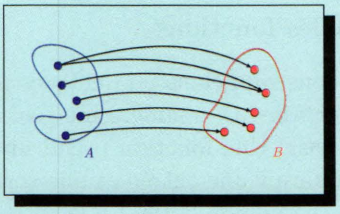
~~*une fonction*~~



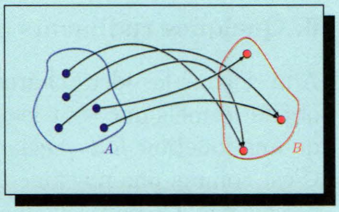
une fonction



une fonction "constante"



~~*une fonction*~~ [28]



une fonction

Définition 6 *Une fonction*

$$f : \begin{array}{ccc} A & \longrightarrow & B \\ a & \longrightarrow & f(a). \end{array}$$

est dite :

(1) injective *s'il n'existe pas d'élément de l'espace d'arrivée ayant plusieurs antécédents.* [29]

(2) surjective *si chaque élément de l'espace d'arrivée admet un antécédent.*

(3) bijective *si elle est à la fois* injective *et* bijective.

28. Deux éléments de l'espace de départ n'ont pas d'image.
28. Un élément de l'espace d'arrivée a deux antécédents.
29. Ceci équivaut à dire que pour tous éléments $a, a' \in A$, si $f(a) = f(a')$, alors $a = a'$.

On utilise souvent les termes *injection*, *surjection*, *bijection* pour désigner des fonctions respectivement injective, surjective, bijective.

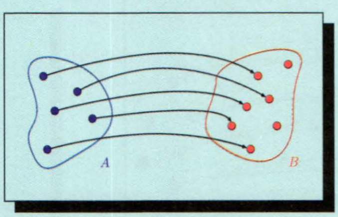
Intuitivement, si une fonction est injective, l'espace de départ *s'injecte* en quelque sorte dans l'espace d'arrivée. Si elle est surjective, l'espace d'arrivée est entièrement touché par la fonction.

Il est également à noter que toute bijection $f : A \longrightarrow B$ induit une *fonction inverse*[30]

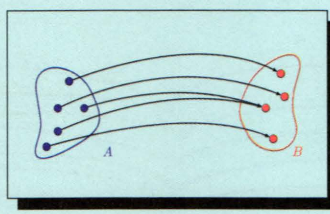
$$\begin{array}{rccc} f^{-1} & : B & \longrightarrow & A \\ & b & \longrightarrow & f^{-1}(b). \end{array}$$

définie par $f^{-1}(b)$ est l'unique[31] antécédent de b. De plus, il est très facile de montrer que f^{-1} est elle-même une bijection.

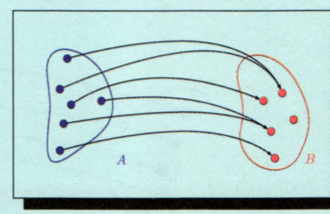
Exemples 7 Quelques exemples de fonctions :



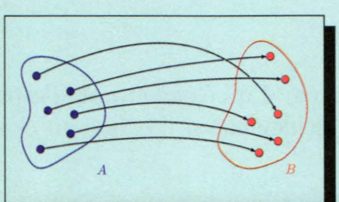
injective, ~~*surjective*~~



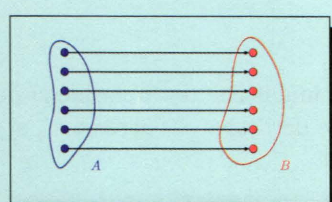
~~*injective*~~, *surjective*



~~*injective*~~, ~~*surjective*~~



injective, *surjective*, *bijective*



injective, *surjective*, *bijective*

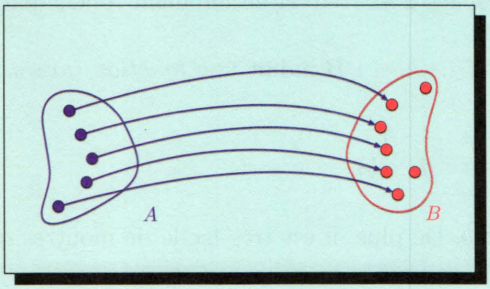
Lorsqu'on a deux fonctions $f : A \longrightarrow B$ et $g : B \longrightarrow C$ dont l'espace de départ de la seconde correspond à celui d'arrivée de la première, on peut alors composer ces deux fonctions pour en obtenir une troisième $h : A \longrightarrow C$ notée $h = g \circ f$ et définie par le fait que pour tout $a \in A$:

$$g \circ f(a) = g\big(f(a)\big).$$

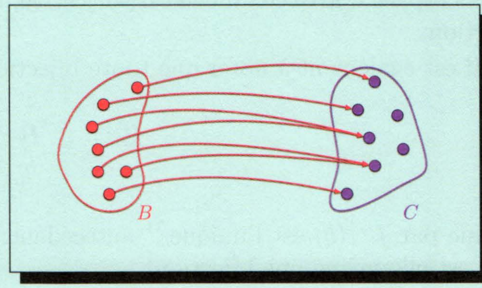
30. Elle est définie sur l'entier de B grâce au fait que f soit surjective.

31. L'unicité provient du fait que f est injective.

Exemple 8 Considérons deux fonctions ci-dessous :

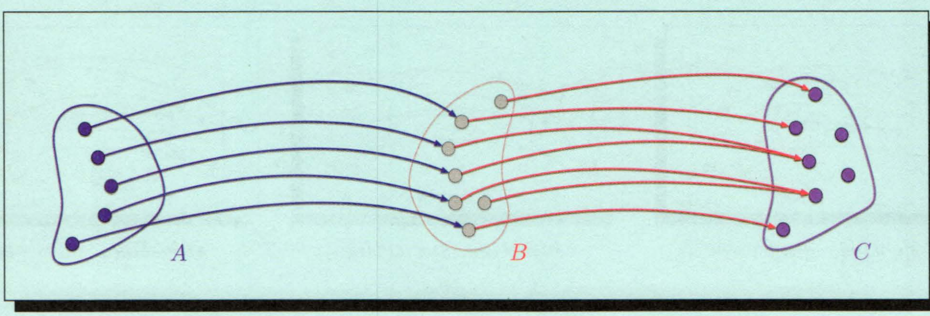


$f : A \longrightarrow B$



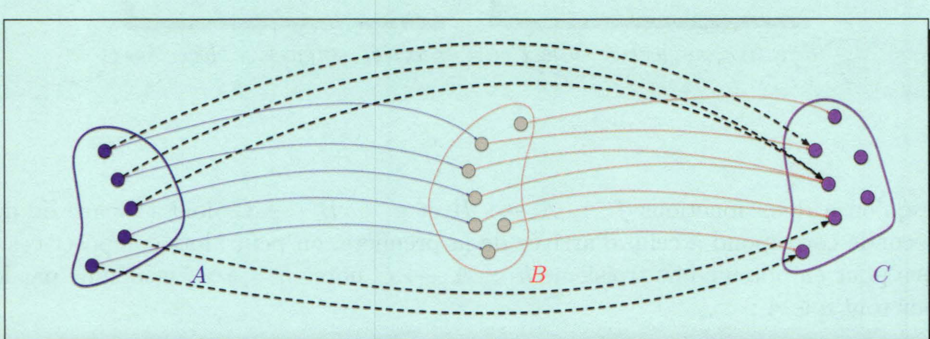
$g : B \longrightarrow C$

Pour en former la composition, on commence par *relier* les graphes des deux fonctions :

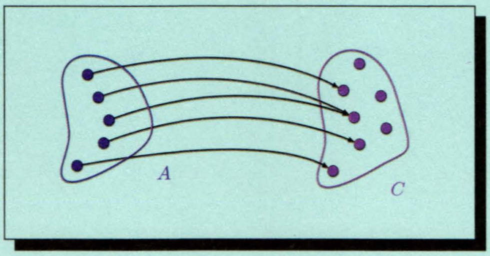


$g \circ f : A \longrightarrow C$

Puis on trace une flèche (en pointillé ci-dessous) d'un élément a de l'espace de départ A vers un élément c de l'espace d'arrivée C, si et seulement si il existe un chemin menant de a vers c :



Après avoir effacé B, f, g on obtient alors la fonction composée $g \circ f$:



$$g \circ f \ : \ A \longrightarrow C$$

Il est très facile de voir que la composée de deux fonctions qui sont toutes deux *injectives* est *injective*; celle de deux fonctions qui sont toutes deux *surjectives* est *surjective*. Par conséquent, la composée de deux *bijections* est elle-même une *bijection*.

Pour aller plus avant :

Au sujet des syllogismes, le lecteur qui le souhaite lira avec attention les ouvrages qui constituent l' *"Organon"* d'Arisote et plus particulièrement le *"Volume 4, Les Seconds Analytiques"* [Ari00]. Il en est de même de l'ouvrage dû aux logiciens Arnauld et Nicole, intitulé *"La logique ou l'art de penser"* [AN92], ainsi qu'au texte *"Lettres à une princesse d'Allemagne : sur divers sujets de physique et de philosophie"* que Euler écrivit pour enseigner la résolution des syllogismes à la Princesse d'Anhalt-Dessau [Eul03].

Pour des ouvrages plus récents, le lecteur pourra se reporter aux livres d'introduction à la logique suivants : *"La logique ou l'art de raisonner"* de Yannis Delmas-Rigoutsos et René Lalement [DRL00], *"Introduction à la logique"* de François Rivenc [Riv03], *"Introduction à la logique standard : calcul des propositions des prédicats et des relations"* de Denis Vernant [Ver01], *"La logique"* de Pierre Wagner [Wag11] ou encore *"Logic For Dummies"* de Mark Zegarelli [Zeg10].

Par ailleurs, le lecteur qui souhaiterait retrouver dans des manuels plus avancés les opérations ensemblistes rudimentaires que nous avons présentées en introduction à cet ouvrage, pourra porter son regard vers les livres suivants : *"Théorie des ensembles"* de Nicolas Bourbaki [Bou70], *"Théorie des ensembles"* de Jean-Louis Krivine [Kri07], *"Basic set theory"* de Azriel Levy [Lev12], *"Notes on set theory"* de Yannis N Moschovakis [Mos94], ou encore *"Basic set theory"* de Alexander Shen et Nikolai K Vereshchagin [SV02].

Première partie

Calcul Propositionnel

Chapitre 1

Syntaxe

1 Le langage

***Résumé* № 1** *Le langage du Calcul Propositionnel comporte trois ingrédients : les variables propositionnelles –* $P, Q, R, \ldots, P_0, P_1, P_2, P_3, P_4, \ldots$ *–; les connecteurs logiques –* $\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow$ *–, et les parenthèses –) et (– qui ne sont utiles que pour la représentation linéaire des formules. Il y a deux types de connecteurs. Le connecteur* $\neg$ *qui est unaire (il permet de construire une formule sur la base d'une autre) et se prononce "non". Les connecteurs binaires (ils ont besoin de deux formules pour en construire une troisième)* $\vee, \wedge, \longrightarrow, \longleftrightarrow$ *qui se prononcent respectivement "ou", "et", "implique" et "équivaut".* ※

Le langage du Calcul Propositionnel est composé de trois différents types de symboles : les variables propositionnelles, les connecteurs logiques et les parenthèses.

1.1 Les variables propositionnelles

La nature exacte de l'ensemble des variables propositionnelles importe peu. Ce qui compte avant tout, c'est de pouvoir distinguer les symboles qui sont des variables propositionnelles de ceux qui sont des connecteurs logiques ou encore des parenthèses. Le but est que la lecture d'une formule ne soit pas équivoque, ambigüe.

Traditionnellement, on utilise des lettres majuscules pour dénoter les variables propositionnelles $(P, Q, R, \ldots)$ auxquelles on adjoint un indice entier $(P_0, P_1, P_2, \ldots)$ lorsqu'on veut en utiliser un grand nombre - voire même une infinité. Mais il ne s'agit là que d'une convention parfaitement arbitraire. La seule chose qui importe lorsqu'on se trouve face à un symbole quelconque est de pouvoir déterminer la nature de ce symbole : à quelle famille se rapporte-t-il ?

On désignera donc par VAR l'*ensemble des variables propositionnelles* :

$$VAR = \{P, Q, R, \ldots, P_0, P_1, P_2, P_3, P_4, \ldots\}.$$

1.2 Les connecteurs logiques

Il en est de même des symboles de connecteurs logiques. Il existe dans la littérature différentes manières de les représenter, et celle que nous donnons ci-dessous n'en est qu'une parmi d'autres. On se donne donc les cinq symboles suivants : $\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow$

(1) $\neg$ est appelé symbole de *négation*, on le prononce *"non"*.

(2) $\vee$ est appelé symbole de *disjonction*, on le prononce *"ou"*.

(3) $\wedge$ est appelé symbole de *conjonction*, on le prononce *"et"*.

(4) $\longrightarrow$ est appelé symbole d'*implication*, on le prononce *"implique"*.

(5) $\longleftrightarrow$ est appelé symbole de *double implication*, ou encore symbole d'*équivalence*, on le prononce *"si et seulement si"* ou encore *"équivaut à"*.

L'usage de ces connecteurs, et plus généralement de tous les connecteurs logiques imaginables, est de mettre en "connection" un certain nombre de formules pour en obtenir une nouvelle.

Ainsi le premier de ces symboles ($\neg$) est un connecteur *unaire*, cela signifie qu'il est à une place, qu'il permet de fabriquer une formule à partir d'une seule formule : avec ϕ, il permet de constuire la formule $\neg\phi$.

Par contre, les quatre autres connecteurs sont des connecteurs *binaires* ou encore à deux places. Chacun d'eux nécessite deux formules pour en construire une troisième (même s'il s'agit de deux fois la même formule!). Ainsi à partir des formules ϕ et ψ, on construit la nouvelle formule $(\phi \wedge \psi)$.

Mais on peut, et nous le ferons plus tard, considérer des connecteurs logiques à $3, 4, 5\ldots$ places.

1.3 Les parenthèses

Ce dernier type de symboles est certainement le plus simple. Il n'intervient que lorsque les formules sont écrites sous forme linéaire. Il n'est pas nécessaire lorsque les formules sont présentées sous forme d'arbre. Il s'agit de la parenthèse fermante et de la parenthèse ouvrante :

$$) \;,\; ($$

Ainsi le langage $\mathcal{L}$ du *Calcul Propositionnel* est l'ensemble suivant :

$$\begin{aligned}
\mathcal{L} &= VAR \cup \{\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\} \cup \{), (\} \\
&= \{P, Q, R, \ldots, P_0, P_1, P_2, P_3, P_4, \ldots\} \cup \{\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\} \cup \{), (\} \\
&= \{P, Q, R, \ldots, P_0, P_1, P_2, P_3, P_4, \ldots, \neg, \vee, \wedge, \longrightarrow, \longleftrightarrow,), (\}.
\end{aligned}$$

2 Les formules

Résumé № 2 *Les formules du Calcul Propositionnel sont des arbres dont toutes les feuilles sont des variables propositionnelles et dont tous les autres nœuds sont des connecteurs logiques. Chaque branchement de l'arbre est soit unaire, soit binaire, en fonction précisément de l'arité du connecteur en jeu. La hauteur d'une formule θ (notée $ht(\theta)$) est donnée par la longueur de s(a/es) plus longue(s) branche(s). Ainsi une formule de hauteur 0 est une variable propositionnelle. Une formule de hauteur $n+1$ est soit de la forme qui suit – avec ϕ un formule de hauteur n,*

$$\begin{tikzcd} \neg \arrow[d, dash] \\ \phi \end{tikzcd}$$

soit de l'une des quatre formes suivantes – avec le maximum des hauteurs de ϕ et de ψ qui vaut n :

$$\begin{tikzcd}[column sep=small] & \vee \arrow[dl, dash] \arrow[dr, dash] & \\ \phi & & \psi \end{tikzcd}, \quad \begin{tikzcd}[column sep=small] & \wedge \arrow[dl, dash] \arrow[dr, dash] & \\ \phi & & \psi \end{tikzcd}, \quad \begin{tikzcd}[column sep=small] & \longrightarrow \arrow[dl, dash] \arrow[dr, dash] & \\ \phi & & \psi \end{tikzcd}, \quad \begin{tikzcd}[column sep=small] & \longleftrightarrow \arrow[dl, dash] \arrow[dr, dash] & \\ \phi & & \psi \end{tikzcd}.$$

※

Nous allons représenter les formules sous forme d'arbre et non sous forme linéaire comme on a coutume de le faire. Néanmoins, ces deux représentations sont deux manières équivalentes d'écrire une même chose. Le seul avantage de la représentation linéaire est sa conformation à la manière dont le français – comme bien d'autres langues – s'écrit : sous forme de ligne précisément. Par symétrie, l'inconvénient majeur de la représentation arborescente est son étalement spatial, son manque de concision. Par contre s'il s'agit de comprendre comment une formule fonctionne, la regarder sous forme d'un arbre est toujours plus parlant.

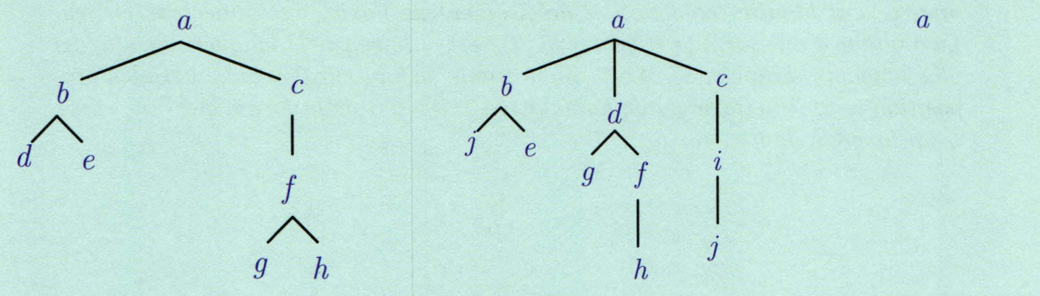
Mais qu'est-ce qu'un arbre au juste ? Les arbres qui nous intéressent ici sont les arbres finis non vides. Chaque arbre commence par la donnée d'un ensemble de nœuds (N) ainsi que d'une relation binaire (R) entre ces nœuds. On note $a \longrightarrow b$ le fait que le nœud a soit en relation R avec le nœud b. On dit dans ce cas que a est le parent de b et b le descendant (immédiat – fils ou fille) de a. On dit qu'il y a un chemin de a vers b lorsqu'il existe une suite de nœuds $\langle a_0, a_1, \ldots, a_n\rangle$ tel que $a = a_0$, $b = a_n$ et $a_0 \longrightarrow a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_n$ est vérifié.

Cette relation doit vérifier que pour tous nœuds a, b, s'il existe un chemin de a vers b alors ce chemin est unique. Cette condition entraîne :

- l'irréflexivité : $a \longrightarrow a$ n'est jamais vérifié.
- l'antisymétrie : si $a \longrightarrow b$ est vérifié, alors $b \longrightarrow a$ ne l'est pas (ce que l'on note $b \not\longrightarrow a$).
- l'antitransitivité : pour aucun nœud a, b, c les trois relations $a \longrightarrow b$, $b \longrightarrow c$ et $a \longrightarrow c$ ne sont vérifiées.
- l'absence de cycle : pour aucune suite de nœuds $\langle a_0, a_1, \ldots, a_n\rangle$ le chemin $a_0 \longrightarrow a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_n \longrightarrow a_0$ n'existe.

De plus nous exigeons qu'il n'y ait qu'un seul nœud r tel que $a \not\longrightarrow r$ soit vérifié pour tout nœud a. Cet unique nœud qui n'a pas d'ancêtre s'appelle la *racine* de l'arbre.

Exemple 9 Trois exemples d'arbres dont le dernier est réduit à sa seule racine.

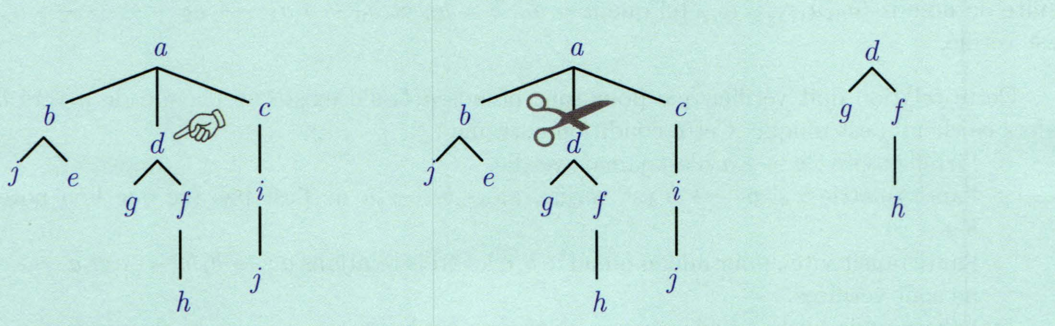


Les nœuds a de l'arbre qui vérifient $a \not\longrightarrow b$ pour tout nœud b, autrement dit qui n'ont pas de descendants, sont appelés *feuilles*.

Une branche est un chemin qui part de la racine et se termine à une feuille. La hauteur d'un arbre est donnée par la longueur de sa plus longue branche. Ainsi, dans l'exemple 9 ci-dessus, les deux premiers arbres ont une hauteur 3, alors que le troisième, réduit à sa seule racine a une hauteur 0.

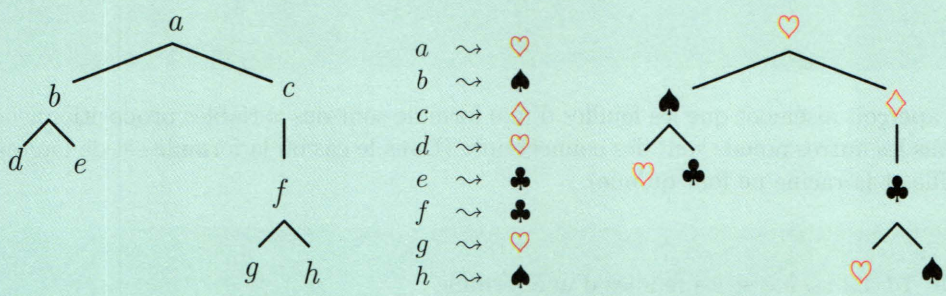
On parle également des *sous-arbres* d'un arbre. Pour obtenir un sous-arbre à partir d'un arbre donné, l'idée est de pointer du doigt l'un des nœuds de cet arbre, de couper le lien de ce nœud à son parent – ou de ne rien faire du tout si ce nœud n'a pas de parent (auquel cas il s'agit de la racine de cet arbre) – puis de retirer toute partie de l'arbre qui ne se trouve pas reliée à ce nœud que l'on avait désigné. On obtient ainsi un arbre dont la nouvelle racine est ce nœud en question. On l'appelle le sous-arbre *engendré* par ce nœud. Cela est montré dans l'exemple qui suit.

Exemple 10 A partir d'un arbre donné et de l'un de ses nœuds (le nœud d), on obtient le sous-arbre engendré par le nœud d.



Les arbres qui nous intéressent sont un peu plus sophistiqués que ceux que nous venons de définir. En effet, nous allons nous donner un alphabet A, puis nous allons coller des étiquettes provenant de l'alphabet sur les noms des nœuds de l'arbre. Mais dans ce changement, plusieurs nœuds de l'arbre pourront avoir maintenant la même étiquette. Précisément, nous nous donnons une fonction f de l'ensemble des nœuds N dans l'alphabet A. Cette fonction f assigne à chaque nœud a un élément $f(a)$ de l'alphabet A. Ce qu'il reste de l'arbre originel est la structure de celui-ci, mais le nom des nœuds a en quelque sorte disparu puisque nous ne nous intéressons qu'aux étiquettes.

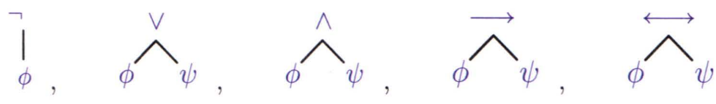
Exemple 11 Un arbre, un étiquetage des nœuds et l'arbre étiqueté qui en résulte.



Nous sommes maintenant en mesure de définir les formules du Calcul Propositionnel. Ce sont des arbres finis étiquetés par des éléments du langage du Calcul Propositionnel.

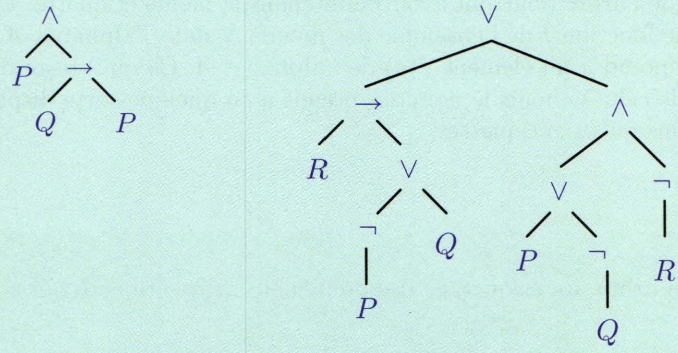
Définition 12 *L'ensemble $\mathcal{F}$ des* formules du Calcul Propositionnel *est le plus petit ensemble d'arbre qui*

- *contient chaque arbre réduit à sa racine qui est une variable propositionnelle.*
- *chaque fois qu'il contient des formules ϕ et ψ contient également les formules suivantes :*



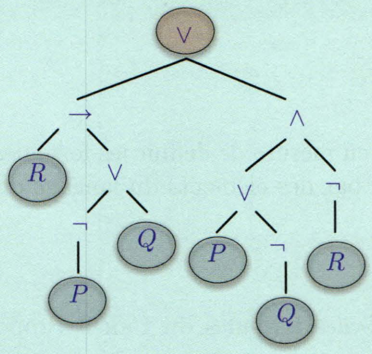
On définit la hauteur d'une formule comme étant la longueur de sa plus longue branche – ou de ses plus longues branches lorsqu'il y en a plusieurs.

Exemple 13 Deux formules, la première de hauteur 2, la seconde de hauteur 4 :



On s'aperçoit aisément que les feuilles d'une formule sont des variables propositionnelles et que tous les autres nœuds sont des connecteurs. (Dans le cas où la formule est de hauteur 0, la feuille et la racine ne font qu'une).

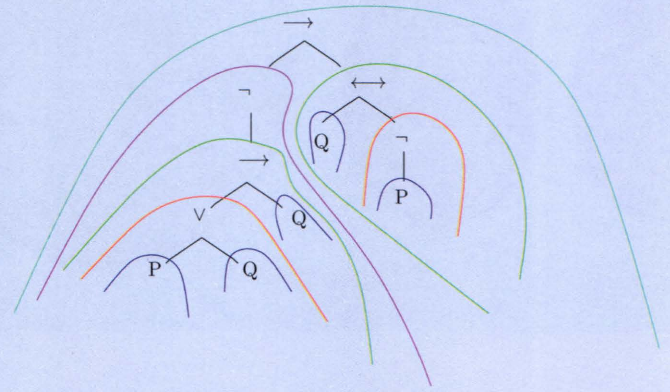
Exemple 14 La racine et les feuilles d'une formule :



La définition que nous venons de donner de l'ensemble des formules est ce qu'on appelle une définition *inductive*, également dénommée définition par *récurrence*. Elle repose sur la définition de briques de base – ici il s'agit des formules de hauteur 0 qui sont les variables propositionnelles – ainsi que des modalités de construction de l'édifice arborescent. On construit ainsi un arbre étiqueté sur la base de un ou deux arbres étiquetés en utilisant un connecteur comme nouvelle racine où viennent se brancher ce ou ces arbres étiquetés. La construction d'une formule ressemble ainsi à une succession de boutures ou de greffes.

3 Les sous-formules

***Résumé* № 3** *Une sous-formule d'une formule ϕ est un sous-arbre de ϕ dont l'un des nœuds de ϕ est la racine.*

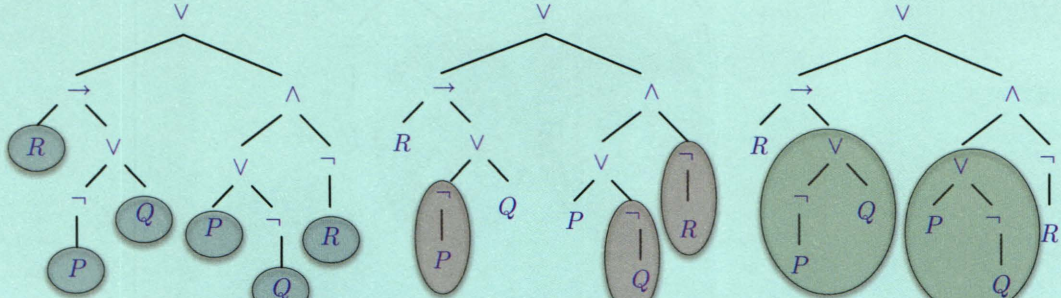


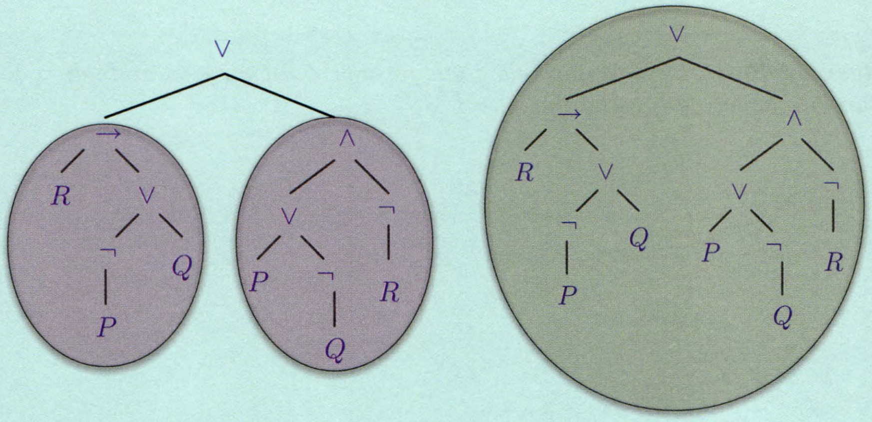
※

Définition 15 *Une sous-formule d'une formule ϕ est un sous-arbre de ϕ engendré par un nœud de ϕ.*

Cela signifie qu' on obtient une sous-formule de ϕ en pointant l'un de ses nœuds et ne gardant de la formule ϕ que ce nœud-ci et tous ses descendants. On obtient ainsi une nouvelle formule dont le nœud pointé est la racine.

Exemple 16 Les sous-formules de hauteurs respectives $0, 1, 2, 3, 4$ d'une même formule ϕ.

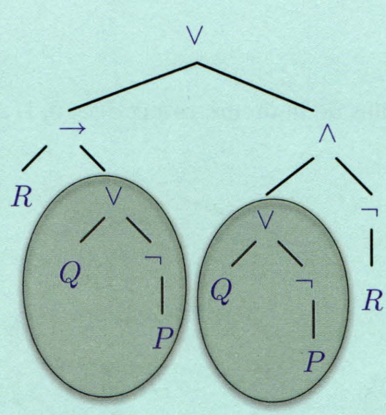




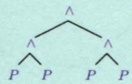
Remarque 17 Lors de sa construction, une formule est établie sur la base de ses sous-formules. Ou, pour le dire autrement, chaque sous-formule d'une formule intervient à un moment ou à un autre dans la construction de cette formule. Considérer les sous-formules d'une formule, c'est en quelque sorte déshabiller celle-ci, lui ôter les différentes couches qui la constituent.

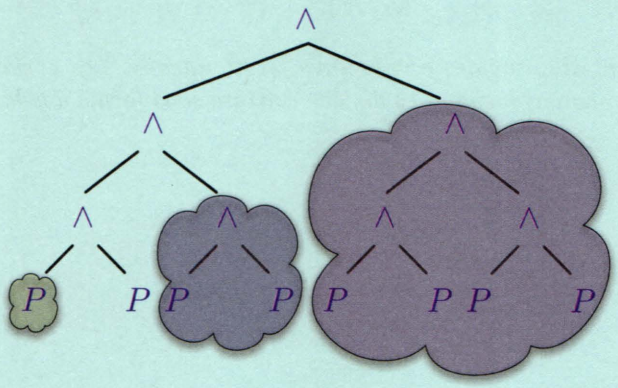
Une formule donnée peut apparaître à plusieurs reprises comme sous-formule d'une formule ϕ. Chacune de ces "apparitions" s'appelle une occurrence.

Exemple 18 Deux occurrences d'une même sous-formules d'une formule ϕ.



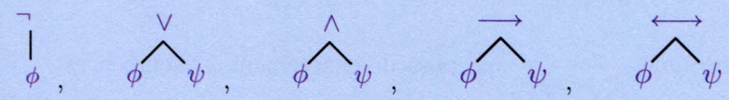
Exemple 19 Dans la formule ci-dessous, il y a :

- la sous-formule P qui possède exactement 8 occurrences ;
- la sous-formule  qui possède exactement 4 occurrences ;
- la sous-formule  qui possède exactement 2 occurrences.



4 La linéarisation d'une formule

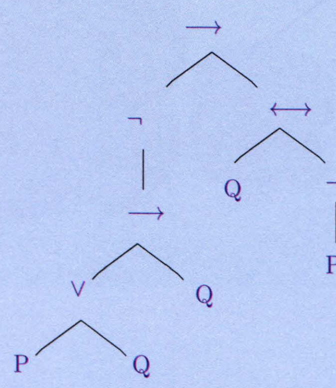
***Résumé* № 4** *L'écriture d'une formule sous forme linéaire consiste à transfomer :*



en respectivement

$$\neg\phi, \quad (\phi \vee \psi), \quad (\phi \wedge \psi), \quad (\phi \longrightarrow \psi), \quad (\phi \longleftrightarrow \psi)$$

où ϕ et ψ sont elles-mêmes écrites sous forme linéaire. Les variables propositionnelles demeurent inchangées de leur écriture sous forme d'arbre (P) à celle linéaire (P).
Ainsi :



se linéarise en : $(\neg((P \vee Q) \longrightarrow Q) \longrightarrow (Q \longleftrightarrow \neg P)).$ ※

Les formules sont des arbres. Ces arbres ont une représentation linéaire, c'est-à-dire qu'ils peuvent être représentés par des suites de caractères placés sur une ligne. En cela un arbre peut "s'écrire" comme une phrase du français – mais bien sûr avec des symboles autres que ceux de l'alphabet latin. Il y a bien entendu de nombreuses manières de linéariser un arbre, qui toutes reposent sur le fait d'ordonner les descendants immédiats d'un nœud. Pour nous, il est très simple d'ordonner les fils (ou filles) d'un nœud puisque trois cas seulement existent : soit il n'y a pas de descendant, soit il y en a un seul – et dans ces deux cas il n'y a rien à ordonner du tout – soit il y a deux descendants et l'on considère naturellement l'ordre gauche / droite. On pourrait commencer la linéarisation d'un arbre en partant des feuilles et en remontant à la racine, ou bien en partant de la feuille la plus à gauche et en remontant vers son parent pour redescendre ensuite vers la feuille immédiatement à droite de la première, etc. Mais nous allons choisir une autre voie – qui correspond à la manière dont les formules sont généralement présentées – nous allons partir de la racine pour descendre vers les feuilles.

Nous allons ainsi procéder par *induction* sur la hauteur de la formule concernée. Cela signifie que nous allons expliquer comment faire pour linéariser une formule d'une certaine hauteur *en supposant* que nous savons le faire pour les formules de hauteur strictement plus petites. Cela présuppose que nous sachions procéder pour les formules de hauteur nulle, puis que nous indiquions comment passer des formules d'une certaine hauteur à celles dont la hauteur est juste supérieure. C'est exactement comme si les formules étaient disposées sur une échelle en fonction de leurs hauteurs et qu'il nous fallait pour les linéariser toutes, être capable de gravir l'échelle jusqu'au sommet (qui dans notre exemple est bien évidemment infini). Parcourir toute l'échelle présuppose deux choses :

(1) être capable de mettre le pied sur le premier barreau.[1]

(2) être ensuite à même de progresser d'un barreau à l'autre.

Pour vérifier la seconde condition, il nous faudra *présupposer* que nous avons atteint un certain barreau – sans savoir duquel il pourrait bien s'agir – et montrer que nous pouvons alors atteindre le suivant. Dès lors, si nous satisfaisons les deux conditions (1) et (2), nous pourrons désormais affirmer que nous sommes en mesure de parcourir l'échelle toute entière.

Nous dirons que nous procéderons *par induction* chaque fois que nous emprunterons une telle échelle de la manière que nous venons d'indiquer. Nous parlerons aussi bien de *construction par induction* lorsque nous l'utiliserons pour définir une famille d'objets, que de *preuve par induction* lorsque nous parcourrons cette échelle afin de montrer que les éléments d'une famille donnée vérifient bien une certaine propriété.

Dans la littérature, on trouve souvent le terme de *récurrence* en lieu et place de celui d'*induction* que nous utilisons ici. On y mentionne généralement le *raisonnement par récurrence. Stricto sensu*, il nous semble plus utile de distinguer :

- la *preuve par induction*, qui emprunte l'échelle des entiers naturels pour démontrer qu'une propriété vaut pour des objets qui ont été préalablement disposés sur les barreaux de cette échelle.
- la *construction par récurrence*, qui élabore un objet se situant sur un niveau de l'échelle à partir des objets qui ont été déjà préalablement construits et disposés sur des niveaux inférieurs.

En ce sens, la récurrence est liée à la notion plus générale de *récursivité* que nous aborderons dans le chapitre 15. Afin de ne pas créer de confusion entre les notions de récurrence et de récursivité, nous prenons le parti de n'employer ici que le terme d'induction pour caractériser à la fois les preuves et les constructions qui relève de ce procédé.

Définition 20 *Soit θ une formule, on définit la linéarisation de θ (notée $\overline{\theta}$) par induction sur la hauteur de θ.*

$ht(\theta)$=0 *: θ n'est autre qu'un arbre réduit à sa seule racine qui est nécessairement une variable propositionnelle P. La linéarisation de θ donne $\overline{\theta} = P$.*

$ht(\theta)$>0 *: il nous faut distinguer suivant l'étiquette de la racine.*

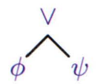
la racine est $\neg$ *: θ est de la forme*

$$\begin{array}{c}\neg\\ |\\ \phi\end{array}$$

la linéarisation de θ donne $\overline{\theta} = \neg\overline{\phi}$,

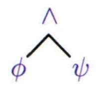
1. C'est le cas des formules de hauteur 0.

la racine est $\vee$ *: θ est de la forme*



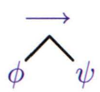
la linéarisation de θ donne $\overline{\theta} = (\overline{\phi} \vee \overline{\psi})$,

la racine est $\wedge$ *: θ est de la forme*



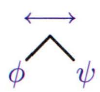
la linéarisation de θ donne $\overline{\theta} = (\overline{\phi} \wedge \overline{\psi})$,

la racine est $\longrightarrow$ *: θ est de la forme*



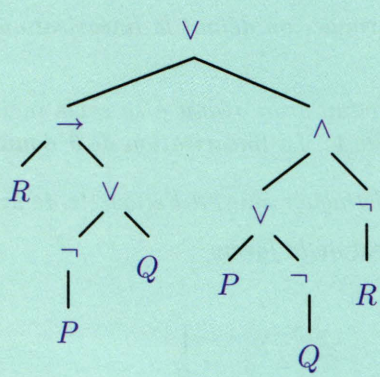
la linéarisation de θ donne $\overline{\theta} = (\overline{\phi} \longrightarrow \overline{\psi})$,

la racine est $\longleftrightarrow$ *: θ est de la forme*



la linéarisation de θ donne $\overline{\theta} = (\overline{\phi} \longleftrightarrow \overline{\psi})$.

Exemple 21 Linéarisation de la formule ϕ suivante :



$$\overline{\phi} = \Big((R \longrightarrow (\neg P \vee Q)) \vee ((P \vee \neg Q) \wedge \neg R)\Big).$$

On voit que l'écriture linéaire d'une formule peut très rapidement devenir embarrassante. Dès qu'il y a beaucoup de parenthèses par exemple, il devient difficile de reconnaître rapidement quel est le connecteur qui était à la racine de l'arbre. Bien sûr en comptant attentivement les parenthèses ouvrantes et les parenthèses fermantes on retrouve ce que l'on cherche. Mais cela reste fastidieux.

Pour aller plus avant :

La présentation de la syntaxe du Calcul Propositionnel, telle qu'on la trouve dans les multiples ouvrages qui traitent de cette logique, est généralement inverse à celle que nous avons privilégiée ici. Les formules sont tout d'abord présentées comme des expressions linéaires et l'on parle ensuite de leur arbre de décomposition. Cette manière de faire tient essentiellement au caractère linéaire du discours ainsi que de sa représentation sous forme écrite. Le lecteur qui voudrait se faire une idée de la manière classique dont ces notions sont introduites pourra consulter avec profit :

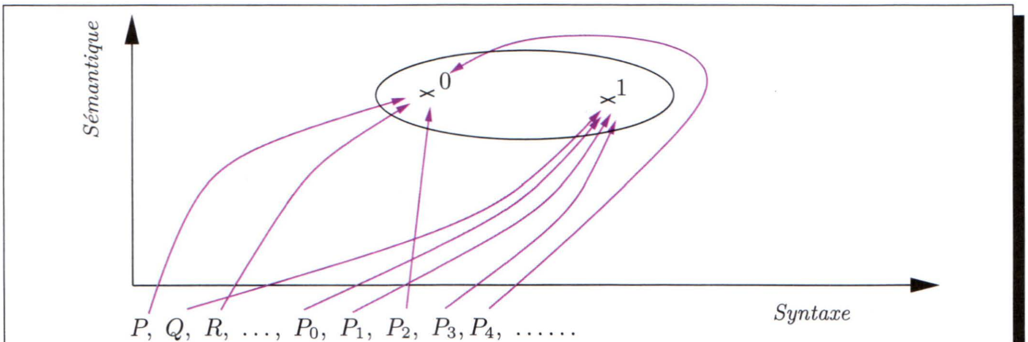
- quelques ouvrages de langue française suivants : *"Introduction à la logique contemporaine"* de Robert Blanché [Bla87], *"La logique ou l'art de raisonner"* de Yannis Delmas-Rigoutsos et René Lalement [DRL00], *"Logique, méthodes pour l'informatique fondamentale"* de Paul Gochet et Pascal Gribomont [GG00], *"Logique moderne"* ou *"Logique des classes et des propositions"* tous deux de Jean-Blaise Grize [Gri73, Gri67], *"Eléments de logique contemporaine"* de François Lepage [Lep01], *"Introduction à la logique"* de Jean Leroux [Ler98], *"Introduction à la logique"* de François Rivenc [Riv03], *"Introduction à la logique formelle et symbolique : avec des exercices et leurs corrigés"* de Jean Salem [Sal94], *"Logique symbolique"* de Xavier Verley [Ver99], *"Introduction à la logique standard : calcul des propositions des prédicats et des relations"* de Denis Vernant [Ver01], *"La logique"* de Pierre Wagner [Wag11], *"Logic For Dummies"* de Mark Zegarelli [Zeg10] ;
- ainsi que ces deux publications plus difficiles d'accès : *"Logique mathématique, tome 1 : Calcul propositionnel; algèbre de Boole; calcul des prédicats"* de René Cori et Daniel Lascar [CLK03a] et *"Logique élémentaire : cours de base pour informaticien"* de Jacques Zahnd [Zah98].
- un livre en allemand : *"Einführung in die mathematische Logik"* de Heinz-Dieter Ebbinghaus, Jörg Flum et Wolfgang Thomas [EFT78].
- quelques manuels de langue anglaise suivants : *"Intermediate logic"* de David Bostock [Bos97], *"Mathematical logic"* de Ian Chiswell et Wilfrid Hodges [CH07], *"A mathematical introduction to logic"* de Herbert B. Enderton [End72], *"A first course in logic : an introduction to model theory, proof theory, computability, and complexity"* de Shawn Hedman [Hed04], *"Introduction to mathematical logic"* d'Elliot Mendelson [Men97], *"Mathematical logic : a first course"* de Joel W. Robbin [Rob69], *"An introduction to formal logic"* de Peter Smith [Smi03], *"Mathematical logic"* de George Tourlakis [Tou11b].
- Puis pour finir, trois ouvrages de langue anglaise de rédaction plus ancienne, mais dont les auteurs demeurent des figures majeures de la logique au XX^e siècle : *"Introduction to Mathematical Logic"* d'Alonzo Church [Chu96], *"Mathematical Logic"* de Stephen C. Kleene [Kle67], *"Introduction à la logique"* d'Alfred Tarski [Tar69].

Chapitre 2

Sémantique

L'interprétation des formules du Calcul Propositionnel commence par l'interprétation des briques de base de ces formules. En ce qui nous concerne, il s'agit des variables propositionnelles. Or, tout de suite, ça commence très mal : les variables propositionnelles sont interprétées de manière extrêmement primitive. En fait, une variable propositionnelle ne peut être interprétée que par 0 ou par 1. Intuitivement, 0 signifie *faux* et 1 signifie *vrai*. Pourtant, on aimerait une logique dans laquelle les interprétations des éléments de base nous permettent de retrouver les paquets de biscuits de notre enfance ou les millions de flocons sur lesquels on a skié. Mais cela est impossible avec le Calcul Propositionnel. Il faut attendre le Calcul des Prédicats pour cela. Pour l'instant, nous sommes malheureusement réduits à visiter des mondes frustres où nos misérables variables propositionnelles prennent l'allure de 0 ou de 1. A partir de là, une formule est aussi un objet que l'on interprète par 0 ou 1 en fonction de la valeur des variables propositionnelles et suivant des règles particulières pour chaque connecteur logique.

Afin d'alléger le texte, nous conviendrons désormais de nous passer des parenthèses extérieures dans l'écriture linéaire d'une formule. Ainsi nous écrirons par exemple $P \longleftrightarrow (P \wedge Q)$ en lieu et place de $(P \longleftrightarrow (P \wedge Q))$.



1 Distribution de valeurs de vérité

***Résumé* № 5** *Une distribution de valeurs de vérité est la donnée, pour chacune des variables propositionnelles considérées, d'une valeur symbolisée par 1 pour "vrai", ou par 0 pour "faux".* ※

Définition 22 *Un modèle $\mathcal{M}$ du Calcul Propositionnel est la donnée d'un élément particulier appelé* distribution de valeurs de vérité *: δ*

- *la* distribution de valeurs de vérité *est une fonction d'ensemble de départ VAR et d'ensemble d'arrivée $\{0, 1\}$, ce que l'on notera δ: $VAR \longrightarrow \{0,1\}$.*

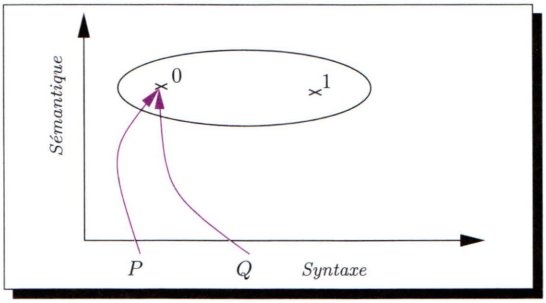
Remarques 23

(1) Lorsque l'on considère un modèle, c'est toujours par rapport à une formule ou un ensemble de formules. On s'intéresse à savoir quelles sont, parmi ces formules, celles qui sont satisfaites dans le modèle et celles qui ne le sont pas. Or pour cela, on n'a besoin que de connaître les *valeurs de vérité* des seules variables propositionnelles qui interviennent dans ces formules. Les autres ne nous sont d'aucun intérêt. On peut donc se restreindre à ne mentionner que la distribution de valeurs de vérité de ces seules variables qui apparaîssent dans notre formule ou dans notre ensemble de formules.

(2) Imaginons que nous ne nous intéressons qu'à un ensemble de formules dans lesquelles les seules variables propositionnelles qui apparaîssent soient P et Q. Combien de modèles différents possibles puis-je considérer ? Chaque variable peut prendre deux valeurs (0 ou 1) et il y a deux variables. Cela fait donc quatre modèles :

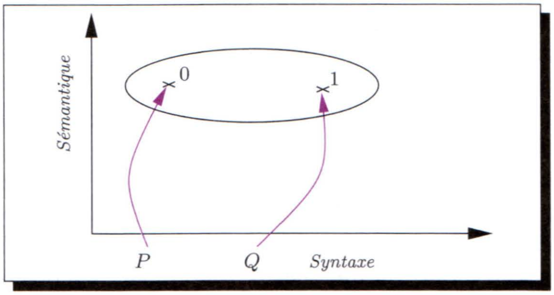
(a) $\mathcal{M}_1$ pour lequel la distribution de valeurs de vérité δ_1 est définie par :

$$\delta_1(P) = 0,\ \delta_1(Q) = 0$$



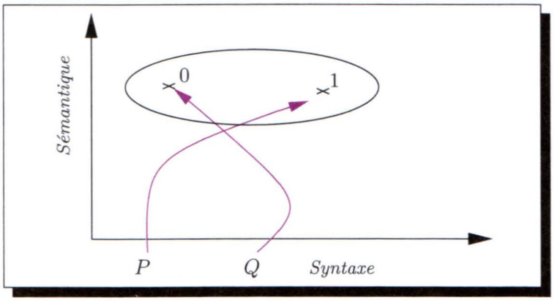
(b) $\mathcal{M}_2$ pour lequel la distribution de valeurs de vérité δ_2 est définie par :

$$\delta_2(P) = 0,\ \delta_2(Q) = 1$$



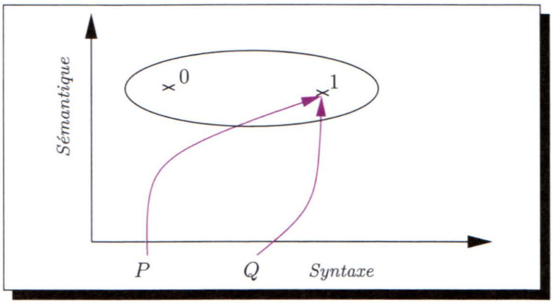
(c) $\mathcal{M}_3$ pour lequel la distribution de valeurs de vérité δ_3 est définie par :

$$\delta_3(P) = 1,\ \delta_3(Q) = 0$$



(d) $\mathcal{M}_4$ pour lequel la distribution de valeurs de vérité δ_4 est définie par :

$$\delta_4(P) = 1,\ \delta_4(Q) = 1$$



Si maintenant on considère trois variables propositionnelles au lieu de deux, c'est-à-dire si l'on ajoute R à P et Q, alors nous aurons quatre modèles comme ceux ci-dessus, dans lesquels R sera vrai ; et quatre autres modèles identiques (pour P et Q) dans lesquels R sera faux. Cela nous fait donc $2 \times 4 = 8$ modèles possibles. Ce calcul se généralise aisément à n variables propositionnelles : si l'on en a une seule, on a deux modèles, et chaque fois qu'on en ajoute une on double le nombre de modèles. On obtient donc

$$\underbrace{2 \times 2 \times \ldots \times 2}_{n \text{ fois}} = 2^n$$

modèles possibles.

Est-ce que 2^n vous fait peur ? Bien sûr, ce n'est là qu'un nombre fini et pourquoi devrait-on avoir peur d'un nombre fini ? Mais d'un point de vue pratique cette fois, est-ce qu'il faudrait beaucoup de temps pour passer en revue 2^n modèles ? Si nous imaginons que nous consacrons pas plus d'une seconde d'attention à chacun de ces 2^n modèles ; et pour faire simple prenons 50 comme valeur pour n. A raison d'une seconde par modèle, combien de temps faudrait-il pour passer en revue tous ces 2^{50} modèles ? Il est très facile d'écrire une formule comportant 50 variables propositionnelles différentes. Cela prend certainement un petit peu de temps, mais raisonnablement cette tâche peut être réalisée en quelques minutes et de toute évidence en bien moins qu'une heure. Par contre, la considération cas par cas de chacun des 2^{50} modèles possibles n'est pas du ressort d'une vie humaine [1].

Notation 24 *Etant donné un modèle $\mathcal{M}$ du Calcul Propositionnel défini par sa distribution de vérité δ, pour une variable propositionnelle P quelconque on notera :*
- $\mathcal{M} \models P$ *pour* $\delta(P) = 1$, *et*
- $\mathcal{M} \models \neg P$ *(ou également* $\mathcal{M} \not\models P$*) pour* $\delta(P) = 0$.

Intuitivement $\mathcal{M} \models P$ signifie que dans le modèle $\mathcal{M}$, P est vraie, alors que $\mathcal{M} \models \neg P$ ($\mathcal{M} \not\models P$) signifie que P est fausse. Ainsi, si nous considérons par exemple trois variables distinctes P, Q, R, nous écrirons $\mathcal{M} \models P, \neg Q, R$ pour dire que dans le modèle $\mathcal{M}$, les deux variables P et R sont vraies mais que Q est fausse.

1. Il faudrait en fait deux milliards d'années, à raison d'une minute par modèle... Ce phénomène se reproduit si l'on replie en deux une feuille de papier et que l'on répète cette opération une trentaine de fois, alors l'épaisseur obtenue dépasse la centaine de kilomètres...

2 Evaluation des formules du Calcul Propositionnel

***Résumé* № 6** *On étend la distribution de valeurs de vérité des variables propositionnelles (qui sont les formules de hauteur 0) aux formules quelconques.*

$\begin{array}{c}\neg\\ |\\ \phi\end{array}$ est vraie si et seulement si ϕ est fausse,

$\begin{array}{ccc} & \vee & \\ \phi & & \psi\end{array}$ est toujours vraie sauf lorsque ϕ et ψ sont toutes les deux fausses,

$\begin{array}{ccc} & \wedge & \\ \phi & & \psi\end{array}$ n'est vraie que lorsque ϕ et ψ sont toutes deux vraies,

$\begin{array}{ccc} & \longrightarrow & \\ \phi & & \psi\end{array}$ est toujours vraie sauf lorsque ϕ est vraie et ψ est fausse,

$\begin{array}{ccc} & \longleftrightarrow & \\ \phi & & \psi\end{array}$ est vraie si ϕ et ψ ont la même valeur de vérité.

※

Après s'être donné un modèle du Calcul Propositionnel $\mathcal{M}$ muni de sa distribution de vérité δ, on étend la fonction de distribution de valeurs de vérité δ de l'ensemble des variables propositionnelles à toutes les formules (les variables propositionnelles sont des formules parmi d'autres). Ainsi étendue, δ devient une fonction de $\mathcal{F}$ (l'ensemble des formules) vers $\{0,1\}$. Si l'on se rappelle que 0 et 1 tiennent bien du faux et du vrai, δ devient donc une fonction qui attribue à chaque formule soit la valeur vrai (1), soit la valeur faux (0). *Stricto sensu*, il faudrait donner un autre nom à δ, l'appeler, par exemple, $\delta_{\mathcal{F}}$. Mais le fait est que cette fonction $\delta_{\mathcal{F}}$ est simplement construite sur la base de δ en appliquant les règles ci-dessous.

Définition 25 *Soit* $\delta \ : \ VAR \longrightarrow \{0,1\}$, *la fonction* $\delta_{\mathcal{F}} \ : \ \mathcal{F} \longrightarrow \{0,1\}$ *est définie par induction sur la construction des formules par :*

(1) $\delta_{\mathcal{F}}(\phi) = \delta(\phi)$ *si* ϕ *est une variable propositionnelle,*

(2) $\delta_{\mathcal{F}}(\neg\phi) = 1 - \delta_{\mathcal{F}}(\phi)$,

(3) $\delta_{\mathcal{F}}(\phi \vee \psi) = \max(\delta_{\mathcal{F}}(\phi), \delta_{\mathcal{F}}(\psi))$,

(4) $\delta_{\mathcal{F}}(\phi \wedge \psi) = \delta_{\mathcal{F}}(\phi) \cdot \delta_{\mathcal{F}}(\psi)$,

(5) $\delta_{\mathcal{F}}(\phi \longrightarrow \psi) = \max\Big(1 - \delta_{\mathcal{F}}(\phi), \delta_{\mathcal{F}}(\psi)\Big)$,

(6) $\delta_{\mathcal{F}}(\phi \longleftrightarrow \psi) = \max\Big((\delta_{\mathcal{F}}(\phi) \cdot \delta_{\mathcal{F}}(\psi), (1 - \delta_{\mathcal{F}}(\phi)) \cdot (1 - \delta_{\mathcal{F}}(\psi))\Big)$.

Remarques 26 Ces définitions correspondent aux cas suivants :

(1) $\phi \vee \psi$ est toujours vraie sauf dans le cas où les deux sous-formules ϕ et ψ sont fausses,

(2) $\phi \wedge \psi$ est toujours fausse sauf dans le cas où les deux sous-formules ϕ et ψ sont vraies,

(3) $\phi \longrightarrow \psi$ est toujours vraie sauf quand à la fois ϕ est vraie et ψ est fausse,

(4) $\phi \longleftrightarrow \psi$ est vraie lorsque ϕ et ψ ont la même valeur de vérité (sont toutes les deux vraies ou bien toutes les deux fausses).

Nous allons désormais regarder directement sur les formules (présentées sous forme arborescente) ce que la signification des connecteurs nous apprend. Pour cela, nous allons regarder les différents modèles possibles induits. S'il s'agit de la formule $\neg\phi$, nous devrons considérer deux modèles possibles : le premier dans lequel ϕ est vraie et le second dans lequel ϕ est fausse. Utilisons pour cela le procédé de coloriage suivant : si la formule est vraie, colorions-la en vert et si elle est fausse, colorions-la en rouge. Puis colorions de manière adéquate le symbole de négation ($\neg$) situé à la racine de $\neg\phi$. Cela nous donnes les deux coloriages suivants :

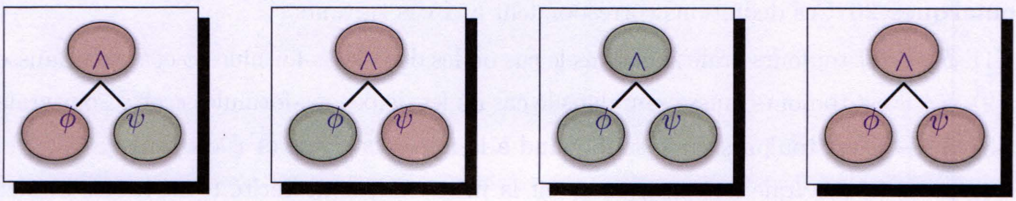
Valeurs de vérité de $\neg\phi$ en fonction de celles de ϕ :

Dans le modèle de gauche, ϕ est vraie et $\neg\phi$ est fausse. Dans celui de droite, c'est l'inverse.

Reprenons la même idée pour les quatre connecteurs binaires. Il va nous falloir à chaque fois considérer non pas deux mais quatre modèles possibles afin de déterminer la valeur de vérité de la formule en question.

Valeurs de vérité de $\phi \vee \psi$ en fonction de celles de ϕ et ψ :

Valeurs de vérité de $\phi \wedge \psi$ en fonction de celles de ϕ et ψ :



Valeurs de vérité de $\phi \longrightarrow \psi$ en fonction de celles de ϕ et ψ :

Valeurs de vérité de $\phi \longleftrightarrow \psi$ en fonction de celles de ϕ et ψ :

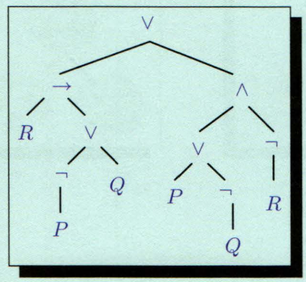
Nous allons utiliser ce petit procédé de coloriage pour déterminer si, étant donnés un modèle et une formule, la formule est vraie ou non dans ce modèle. Cela s'appelle *évaluer la formule* dans le modèle. On détermine sa valeur en quelque sorte. Nous allons pour cela passer par l'évaluation de toutes les sous-formules de la formule à évaluer, en commençant par les sous-formules de hauteur 0, puis celles de hauteur 1, puis celles de hauteur 2, etc., jusqu'à ce que nous arrivions à la hauteur de la formule dont nous sommes partis.

Pour cela, nous savons facilement déterminer la valeur de chacune des sous-formules de hauteur 0, puisqu'elle nous est donnée par le modèle lui-même dans lequel nous effectuons cette évaluation. Ensuite, pour tout connecteur apparaîssant dans la formule, si nous connaissons la valeur de vérité de son ou ses descendants immédiats, nous n'avons qu'à nous référer à la définition de ce connecteur pour en déduire immédiatement la valeur de cette sous-formule.

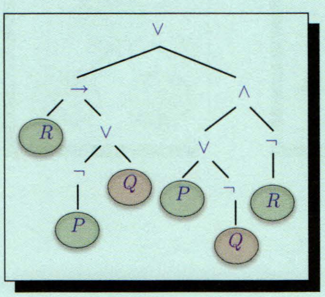
C'est en gardant ce principe simple de raisonnement que nous proposons, étant donnés un modèle $\mathcal{M}$ ainsi qu'une formule ϕ, l'algorithme de coloriage suivant :

- Tout d'abord nous colorions chaque feuille de ϕ – qui est nécessairement une variable propositionnelle X – en vert si $\mathcal{M} \models X$, et en rouge si $\mathcal{M} \not\models X$.
- Ensuite, nous colorions chaque nœud – qui est nécessairement étiqueté par un connecteur – dont tous les descendants ont préalablement été coloriés, en fonction de la définition de la valeur de vérité de ce connecteur.
- Ce processus s'arrête lorsqu'il n'y a plus de nœud à colorier. La valeur de vérité de ϕ est alors donnée par la *couleur de sa racine*.

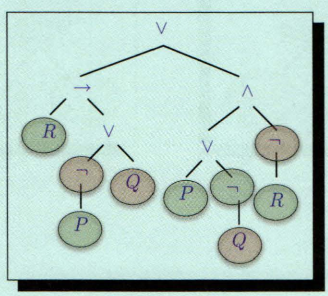
Exemple 27 Soit le modèle $\mathcal{M}$ définit par $\mathcal{M} \models P, \neg Q, R$ et la formule ϕ suivante :



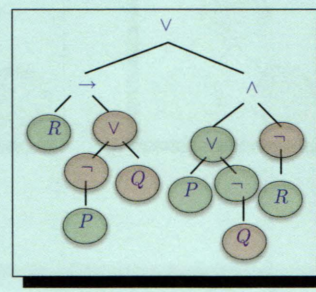
L'évaluation de ϕ dans $\mathcal{M}$ étape par étape donne la suite de formules coloriées suivantes :



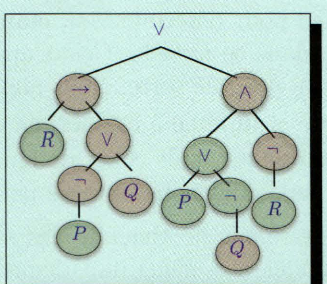
hauteur 0



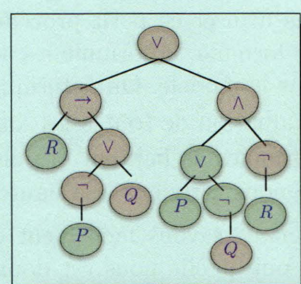
hauteur 1



hauteur 2



hauteur 3

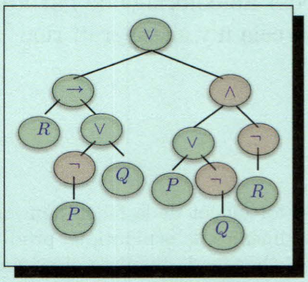


hauteur 4

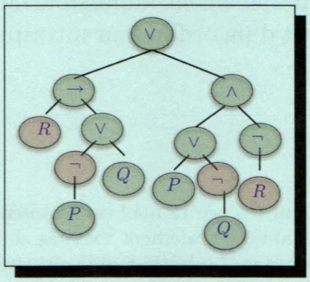
La racine est rouge, ϕ est donc fausse dans ce modèle : $\mathcal{M} \not\models \phi$

Dans l'exemple qui suit, nous considérons toujours la même formule, mais nous faisons varier les modèles.

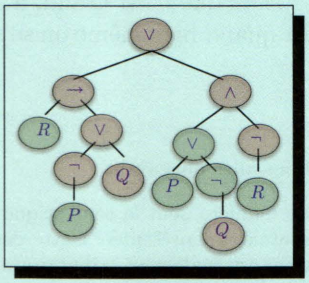
Exemple 28 Evaluation de ϕ dans les huit modèles possibles :



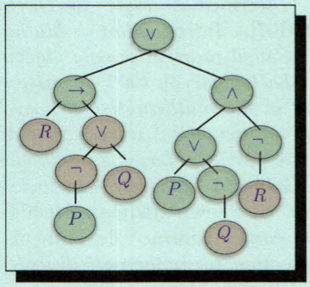
$\mathcal{M} \models P, Q, R$



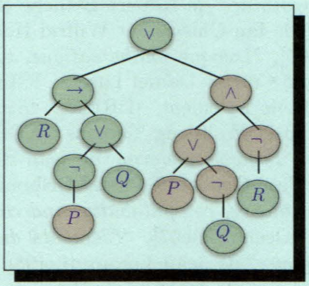
$\mathcal{M} \models P, Q, \neg R$



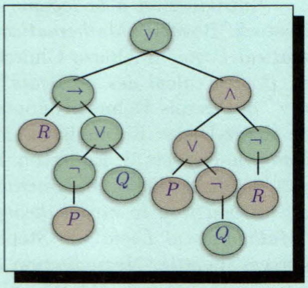
$\mathcal{M} \models P, \neg Q, R$



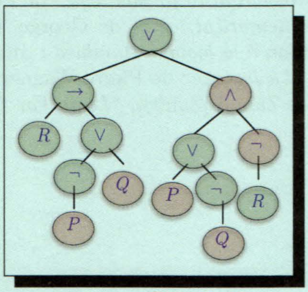
$\mathcal{M} \models P, \neg Q, \neg R$



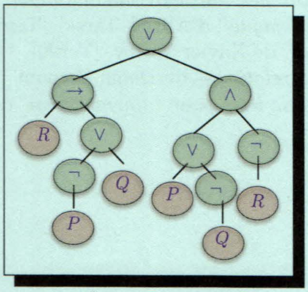
$\mathcal{M} \models \neg P, Q, R$



$\mathcal{M} \models \neg P, Q, \neg R$



$\mathcal{M} \models \neg P, \neg Q, R$



$\mathcal{M} \models \neg P, \neg Q, \neg R$

Cette formule n'est fausse que dans le seul modèle $\mathcal{M} \models P, \neg Q, R$.

On se rend compte ici que l'évaluation d'une formule dans un modèle n'est pas une chose facile. Chaque étape du procédé algorithmique lui-même est rudimentaire, mais il faut beaucoup d'étapes pour déterminer si la formule est vraie ou fausse dans un modèle donné. Si la formule a une hauteur n, combien y a-t-il de nœuds qui ne sont pas des feuilles ? La borne supérieure est atteinte si l'on considère que chacun de ces nœuds correspond à un connecteur binaire.

Ce cas nous donne un nœud pour la racine, puis deux nœuds pour ses descendants, puis deux nœuds pour chacun de ses descendants, etc. Cela fait donc $0+1+2+2^2+2^3+\ldots+2^{n-1} = 2^n - 1$ nœuds [2] qui ne sont pas des feuilles.

Dès que n est grand, il est matériellement impossible de procéder au coloriage de l'arbre. Et quand bien même on se servirait d'un ordinateur ultra-puissant, cela n'y changerait rien [3].

Pour aller plus avant :

La manière dont la sémantique du Calcul Propositionnel est exposée dépend fortement de la façon dont la syntaxe est présentée. Cette dernière étant généralement exhibée sous forme linéaire, la sémantique prodiguée est également tributaire de cette forme. Le lecteur qui souhaiterait appréhender la manière classique d'introduire la sémantique du Calcul Propositionnel pourra se référer avec intérêt à certains ouvrages parmi les suivants :

"Introduction à la logique contemporaine" de Robert Blanché [Bla87], *"Intermediate logic"* de David Bostock [Bos97], *"Mathematical logic"* de Ian Chiswell et Wilfrid Hodges [CH07], *"Introduction to Mathematical Logic"* d'Alonzo Church [Chu96], *"Logique mathématique, tome 1 : Calcul propositionnel; algèbre de Boole; calcul des prédicats"* de René Cori et Daniel Lascar [CLK03a], *"La logique ou l'art de raisonner"* de Yannis Delmas-Rigoutsos et René Lalement [DRL00], *"Einführung in die mathematische Logik"* de Heinz-Dieter Ebbinghaus, Jörg Flum et Wolfgang Thomas [EFT78], *"A mathematical introduction to logic"* de Herbert B. Enderton [End72], *"Logique moderne"* de Jean-Blaise Grize [Gri73], *"Logique, méthodes pour l'informatique fondamentale"* de Paul Gochet et Pascal Gribomont [GG00], *"A first course in logic : an introduction to model theory, proof theory, computability, and complexity"* de Shawn Hedman [Hed04], *"Mathematical Logic"* de Stephen C. Kleene [Kle67], *"Eléments de logique contemporaine"* de François-Lepage [Lep01], *"Introduction à la logique"* de Jean Leroux [Ler98], *"Introduction to mathematical logic"* d'Elliot Mendelson [Men97], *"Introduction à la logique"* de François Rivenc [Riv03], *"Mathematical logic : a first course"* de Joel W. Robbin [Rob69], *"Introduction à la logique formelle et symbolique : avec des exercices et leurs corrigés"* de Jean Salem [Sal94], *"An introduction to formal logic"* de Peter Smith [Smi03], *"Introduction à la logique"* d'Alfred Tarski [Tar69], *"Mathematical logic"* de George Tourlakis [Tou11b], *"Logique symbolique"* de Xavier Verley [Ver99], *"Introduction à la logique standard : calcul des propositions des prédicats et des relations"* de Denis Vernant [Ver01], *"La logique"* de Pierre Wagner [Wag11], *"Logique élémentaire : cours de base pour informaticien"* de Jacques Zahnd [Zah98], *"Logic For Dummies"* de Mark Zegarelli [Zeg10].

---

2. Ce résultat se démontre encore une fois de manière inductive. Pour cela il nous faut vérifier :

(1) que l'on peut monter sur le premier barreau de l'échelle, celui qui correspond à la valeur $n = 0$. En effet, si nous calculons $2^0 - 1$ nous obtenons $1 - 1$, c'est-à-dire 0 qui est bien le nombre de nœud qui ne soit pas des feuilles dans un arbre de hauteur 0, puisqu'un arbre de hauteur 0 possède un seul nœud qui est à la fois racine et feuille, par conséquent aucun nœud qui ne soit pas une feuille.

(2) que si l'on se trouve déjà sur un barreau n quelconque, on peut alors monter sur le barreau situé un étage au-dessus. Pour cela on suppose vérifié $0+1+2+2^2+2^3+\ldots+2^{n-1} = 2^n - 1$ et l'on cherche à montrer que l'on a bien $0+1+2+2^2+2^3+\ldots+2^{n-1}+2^n = 2^{n+1} - 1$; ce qui est aisé puisque :

$$0+1+2+2^2+2^3+\ldots+2^{n-1}+2^n = \Big(0+1+2+2^2+2^3+\ldots+2^{n-1}\Big)+2^n.$$

En utilisant l'hypothèse d'induction, on obtient alors le résultat escompté :

$$0+1+2+2^2+2^3+\ldots+2^{n-1}+2^n = \Big(2^n-1\Big)+2^n = \Big(2^n+2^n\Big)-1 = 2^{n+1}-1.$$

3. Si une telle machine avait été lancée au début du *Big Bang* – et qu'elle ne se soit jamais arrêtée – elle serait encore très loin d'en avoir fini pour les valeurs de n au-delà de 75.

3 Comment utiliser le Calcul Propositionnel ?

Résumé № 7 *Les variables propositionnelles représentent des objets insécables capables de vérité ou de fausseté. Le connecteur "$\neg$" transcrit la négation. Les deux connecteurs "$\wedge$" et "$\longleftrightarrow$" traduisent respectivement la conjonction ("et") et la double implication ("si et seulement si"). Le connecteur "$\vee$" représente la disjonction : le "ou" inclusif – qui se distingue du "ou" exclusif qui n'est vrai que lorsque l'une seulement des deux sous-formules en jeu est vraie. Le connecteur "$\longrightarrow$" représente l'implication "si..., alors...".* ※

Un regard, même des plus étourdis, sur l'agencement du langage courant – en l'occurrence le français – permet de remarquer que les phrases sont souvent élaborées sur la base de phrases plus courtes par l'utilisation de connecteurs du type *et, ou, mais, or, si... alors..., par contre, etc.* On remarque en effet qu'il existe nombre de phrases indécomposables qui fonctionnent comme des pièces de *Lego*® et peuvent ensuite être juxtaposées – reliées au moyen de terme qui ne sont là que pour effectuer la connexion – afin de permettre la constitution de phrases plus longues.

Les phrases construites sur la base de phrases simples sont dites *composées.* Les phrases simples sont par opposition dites *atomiques.* Ainsi, nous pourrons dire que les deux phrases *"Carole vient dîner ce soir"* et *"il n'y a rien dans le frigo"* sont atomiques. Alors que *"il n'y a rien dans le frigo et Carole vient dîner ce soir"* est une phrase composée par la conjonction de deux énoncés simples.

Néanmoins, si les phrases atomiques sont plus courtes que les phrases dans la composition desquelles elles entrent, elles peuvent elles-mêmes être relativement longues, comme par exemple : *"Le soir du 19 septembre 2013, à 16:40 précises, le pilote suisse du vol LX 40 entreprit de poser son appareil sur la piste 24 L de LAX".*

3.1 Les phrases atomiques

Avec la sémantique que nous avons introduite précédemment, l'utilisation du Calcul Propositionnel est toute tracée. En effet, puisque l'interprétation des éléments atomiques de cette logique est restreinte à 0 ou 1 (qui symbolisent le Faux et le Vrai), les variables propositionnelles ne peuvent être utilisées que rapportées à des choses susceptibles d'être vraies ou fausses. En termes plus savants : *les variables propositionnelles représentent des objets simples du savoir susceptibles de vérité ou de fausseté.* Par objets simples, nous entendons des énoncés qui ne sont pas décomposables. Ils sont susceptibles de vérité ou de fausseté si ces énoncés peuvent être dits vrais ou faux (sous-entendu à l'aide de moyens d'investigation qui ne sont pas nécessairement à notre portée [4]). Ce sont des énoncés pour lesquels quelqu'un d'omniscient serait en mesure d'attester de leur véracité ou de leur fausseté.

Les exemples suivants sont des énoncés vrais ou faux. Ils peuvent donc être associés à une variable propositionnelle.

4. Par exemple l'énoncé *"il y a actuellement une personne sur le sommet du Cervin"* est soit vrai soit faux, bien que nous n'en sachions strictement rien. De même, l'énoncé *"l'une de ces trois étudiantes échouera à l'examen"* est vrai ou faux, mais il nous faudrait nous reporter à la fin du semestre pour pouvoir en déterminer sa valeur de vérité.

Exemples 29

(1) *Nelson mange un pain au chocolat.*
(2) *Aucun d'entre vous ne réussira.*
(3) *De nos jours, les âmes charitables sont plus rares que les êtres arrogants.*
(4) *La reine d'Angleterre est assise sur son trône.*
(5) $2+2=3$.
(6) *Les gens heureux n'ont pas d'histoire.*
(7) *C'est bien plus beau lorsque c'est inutile.*
(8) *Ce sont toujours les meilleurs qui partent les premiers.*
(9) *Les tonneaux vides sont ceux qui font le plus de bruit.*
(10) $2+2=4$.

Ainsi, on pourra écrire $P := 2+2=3$, $Q :=$*les vaches regardent passer le train* et construire la formule " $P \longrightarrow Q$" qui correspond à l'énoncé *"si* $2+2=3$ *alors les vaches regardent passer le train"*; ou comme " $P \vee Q$" qui se traduit par " $2+2=3$ *ou les vaches regardent passer le train"*.

Au contraire, les exemples suivants ne sont pas des énoncés susceptibles d'être vrais ou faux. On ne peut donc pas leur assigner une variable propositionnelle :

Exemples 30

(1) *Nelson mange-t-il un pain au chocolat ?*
(2) *Ah oui ?*
(3) *Viendra-t-il ce soir ?*
(4) *C'est combien le kilo ?*
(5) *Est-ce bien vrai ?*
(6) *Sommes-nous dans une telle déréliction ?*

La raison pour laquelle les exemples précédents ne sont pas susceptibles d'être vrais ou faux provient du fait qu'ils sont des énoncés interrogatifs. Ce ne sont ni des affirmations ni des négations.

Les exemples qui suivent, bien qu'ils ne soient pas des interrogations, ne sont pas non plus susceptibles d'être vrais ou faux.

Exemples 31

(1) *Soyez sages !*
(2) *Qu'on ouvre toutes les portes de la cité !*
(3) *Allez en paix mes bien chères soeurs !*
(4) *Ouh là là !...*
(5) *Oui !*
(6) *Non !*
(7) *Catastrophe !*
(8) *Gentil ! Tout doux le chien !*

Aucun des énoncés précédents n'est déclaratif. Ce sont tous des énoncés exclamatifs, des ordres, des commandements. Comme tels, ils ne peuvent être ni vrais ni faux.

Voici encore quelques exemples de phrases simples qui ne peuvent être traitées à l'aide du Calcul Propositionnel :

Exemples 32

(1) *Oui.*

(2) *Non.*

(3) *Merci.*

(4) *Et ron et ron petit patapon.*

Il se trouve également que même parmi les énoncés simples susceptibles d'être vrais ou faux, il faut comprendre leur signification pour en conclure leur valeur de vérité. Ainsi, pour prendre un exemple immédiat, il est parfois nécessaire de distinguer le locuteur afin de déterminer si l'énoncé en question est vrai ou faux.

Exemples 33

(1) *J'ai lu tous les livres.* Cet énoncé pris à la lettre se rapporte à moi-même. On pourrait donc convenir d'écrire $P :=$ *j'ai lu tous les livres.* Mais si l'on fait attention à spécifier le locuteur, cet énoncé, lorsqu'il apparaît au sein du poème *Brise Marine*, se rapporte à son auteur (Stéphane Mallarmé). On conviendra dès lors d'écrire : $P :=$ *Mallarmé a lu tous les livres.*

(2) *Souvent je me suis couché de bonne heure.* On retrouve ici le même argument. La signification véritable est bien : $Q :=$*Marcel Proust s'est souvent couché de bonne heure.*

Le seul critère à retenir pour savoir si un énoncé simple tombe sous le coup du Calcul Propositionnel, c'est de savoir si cet énoncé peut être dit vrai ou faux.

Constatons à nouveau que cela ne dépend pas obligatoirement de notre connaissance actuelle. Si je dis par exemple : *"il y a une bombe sous le bureau"*, on va m'accorder que cet énoncé est soit vrai soit faux, et cela, avant même d'avoir passé la tête sous le bureau pour le vérifier.

Par conséquent un énoncé est susceptible de vérité ou de fausseté dès que l'on peut envisager un moyen de le vérifier, même si ce moyen n'est pas à la mesure de nos forces. Ainsi l'énoncé *il y a d'autres humains qui vivent actuellement dans d'autres galaxies* est quelque chose que l'on pourrait vérifier si l'on était omnipotent.

Le futur ne pose pas non plus de problème. Si je dis *l'un d'entre vous réussira ce semestre*, il nous suffit de tous voyager dans le temps pour nous situer à la fin de cette année, puis de considérer le cas de chacun d'entre vous eu égard à la réussite en question. Il devient alors très facile pour nous de conclure par vrai ou par faux.

Par contre, ce qui peut poser question dans la transcription d'un énoncé – fut-il simple – c'est la signification même de cet énoncé. Il peut très bien être de la forme *"sujet-verbe-complément"*, mais le fait de le prendre au pied de la lettre lui fait manquer sa véritable signification. Concentrons-nous par exemple sur le premier vers du poème *Brise Marine*[5].

Exemples 34

- *La chair est triste* : je peux toujours traduire cet énoncé par $P :=$ *la chair est triste.* Cela ne crée certes pas de perturbation dans l'univers de la logique. Mais est-ce pour autant judicieux ? Si P intervient ensuite dans un raisonnement, au sein d'autres formulations, n'aurais-je pas manqué l'essentiel de ce que dit *La chair est triste* ? Mais au fait, que dit vraiment cet énoncé ? Mallarmé veut certainement déclarer quelque chose comme son désarroi, son affliction quant à la sexualité. Pourtant le mot de *tristesse* qu'il emploie pour dire son absence de goût, dit à la fois un abattement, une prostration, une apathie, un découragement, un ennui. Et la *chair* dont il est question est-ce vraiment la sexualité ? Ne serait-ce pas également la libido, la concupiscence, la volupté, la sensualité, l'érotisme ? En un mot, si cet énoncé est susceptible d'être vrai ou faux, de quelle vérité s'agit-il ?

Considérons à nouveau le premier vers d'un poème – le *Rondel à l'adieu*[6] – en guise de second exemple.

Exemple 35

- *Partir c'est mourir un peu* : il semble à première vue difficile de vérifier un tel énoncé. Il faut en premier lieu s'entendre sur ce qu'il signifie. Il nous fait partager le sentiment de perte de soi, de dépérissement qui accompagne le fait de partir, de quitter ce que l'on aime. Mais est-ce bien là tout ce qui se joue dans cet énoncé ?

---

5. **Brise marine**

La chair est triste, hélas ! et j'ai lu tous les livres.
Fuir ! là-bas fuir ! Je sens que des oiseaux sont ivres
D'être parmi l'écume inconnue et les cieux !
Rien, ni les vieux jardins reflétés par les yeux
Ne retiendra ce coeur qui dans la mer se trempe
O nuits ! ni la clarté déserte de ma lampe
Sur le vide papier que la blancheur défend
Et ni la jeune femme allaitant son enfant.
Je partirai ! Steamer balançant ta mâture,
Lève l'ancre pour une exotique nature !
Un Ennui, désolé par les cruels espoirs,
Croit encore à l'adieu suprême des mouchoirs !
Et, peut-être, les mâts, invitant les orages
Sont-ils de ceux qu'un vent penche sur les naufrages
Perdus, sans mâts, sans mâts, ni fertiles îlots...
Mais, ô mon coeur, entends le chant des matelots !

Stéphane Mallarmé (1842-1898)

6. **Rondel à l'adieu**

Partir, c'est mourir un peu,
C'est mourir à ce qu'on aime :
On laisse un peu de soi-même
En toute heure et dans tout lieu.
C'est toujours le deuil d'un voeu,
Le dernier vers d'un poème :
Partir, c'est mourir un peu !
C'est mourir à ce qu'on aime.
Et l'on part, et c'est un jeu,
Et jusqu'à l'adieu suprême
C'est son âme que l'on sème,
Que l'on sème à chaque adieu !
Partir, c'est mourir un peu...

Edmond Haraucourt (1856-1941)

Mais finalement, ce qui se joue avec *"la chair est triste"* comme avec *"partir, c'est mourir un peu"*, n'est-ce pas la simple description d'un sentiment ? Ne s'agit-il pas moins de décrire un état du monde, qu'un état mental ? Celui de la personne qui énonce ces paroles. Et en ce sens, la vérité ou la fausseté d'un tel énoncé n'est-t-elle pas illusoire ? Ce dont il s'agit n'est-t-il pas, à travers la signification de l'énoncé, de décrire un sentiment ?

Par contre, si je dis que *"les huîtres ont souvent des peines de coeur"*, il ne semble pas que je cherche à exposer un sentiment qui me soit propre, mais bien un état de fait du monde. Pour autant, ce dont je parle peut être plus ou moins clair. Bien sûr, tout le monde connait les *huîtres*, les *peines de coeur* et la signification du mot *"souvent"*. Mais les peines de coeur des huîtres semblent quelque chose de mal défini. Il y a deux manières de voir cela. Soit, étant plus informé de la vie amoureuse des huîtres, je serais en mesure de répondre par oui ou par non à la question *les huîtres ont-elles souvent des peines de coeur ?* et alors je pourrais effectivement considérer P := *Les huîtres ont souvent des peines de coeur*. Soit une telle question n'a pas de sens et je ne vois pas du tout comment elle pourrait en avoir. Dans ce cas-ci, je ne peux pas utiliser le Calcul Propositionnel pour traiter cet énoncé.

Il ne faudrait néanmoins pas croire que l'aspect farfelu d'un énoncé soit un critère permettant de conclure que celui-ci ne peut pas être traité par le Calcul Propositionnel. Ainsi l'énoncé suivant – tout à fait farfelu – ne pose pas de problème : *chaque année, au moins 65 % des huîtres écrivent au moins une lettre à leurs parents*. Imaginez que l'on s'aperçoive que les huîtres, grâce à de magnifiques contorsions, arrivent à modifier leur aspect jusqu'à distinguer de miniscules petits bras verts terminés par de fins doigts velus avec lesquels elles prélèvent l'encre des seiches pour écrire de petits mots à leurs parents sur des algues préalablement traitées...

Venons-en maintenant à une critique beaucoup plus fondamentale. Si je dis *"il fait chaud dans cette pièce"*. Si la température est supérieure à trente degrés, tout le monde s'accordera pour dire qu'il fait chaud, et si elle descend en dessous de 10 degrés, tout le monde s'accordera également pour dire qu'il ne fait pas chaud. Mais à partir de quelle température puis-je dire qu'il fait chaud ? Il semble qu'il y ait bien une fourchette de températures pour lesquelles l'énoncé *"il fait chaud dans cette pièce"* admette non pas une valeur de vérité soit 1 soit 0, mais des valeurs intermédiaires que l'on appelle précisément des *degrés*[7] de vérité. Ces degrés de vérité sont des valeurs probabilistes comprises entre 0 (totalement faux) et 1(totalement vrai).

Le degré de vérité de l'énoncé *"elle roulait à vive allure sur l'autoroute"* est 1 si la vitesse de l'automobiliste était de 200 km/h, et il est 0 si sa vitesse était au contraire de 80 km/h. Mais quel est le degré de vérité de cet énoncé dans le cas d'une automobiliste roulant à 125 km/h ? Est-ce que cet énoncé est vrai à 30% et faux à 70% ?

Le langage ordinaire regorge de références qui seraient de type probabiliste s'il fallait les préciser et dont le statut exact de vérité demeure problématique. C'est le cas dans l'utilisation des formes : *parfois*, *souvent*, *le plus souvent*, *maintes fois*, *la plupart du temps*, *couramment*, *habituellement*, *d'ordinaire*, *généralement*, *fréquemment*, *beaucoup*, *communément*.

C'est aussi le cas lorsqu'on attribue simplement une propriété à un objet. Ainsi, en regardant la figure ci-après, *"cette patatoïde est rouge"* est un énoncé que vous attribueriez à combien d'entre elles ?

7. Sans jeu de mot.

Pour certaines, il est clair qu'elles ne sont pas rouges, mais d'autres possèdent du rouge sans être complètement rouges. Diriez-vous de celles-là qu'elles sont rouges ? Diriez-vous qu'elles ne sont pas rouges ? Il est tentant dans certains cas d'associer à cet énoncé (*Cette patatoïde est rouge*) une valeur de vérité qui se situe entre 0 et 1 – mais où précisément ?

Même un énoncé aussi peu problématique que *Nelson mange un pain au chocolat* peut très bien prêter à discussion. Il semble en effet qu'il n'y ait aucune raison de mettre en doute que cet énoncé tombe sous le coup du Calcul Propositionnel. Il va de soi qu'on peut écrire $P :=$ *Nelson mange un pain au chocolat* sans la moindre hésitation. Il est d'ailleurs évident de vérifier si un tel énoncé est vrai ou faux. Mais est-ce vraiment non problématique ? Que se passe-t-il si Nelson mange une patisserie qui ressemble beaucoup à un pain au chocolat mais contient des raisins secs ? ou des morceaux de dragées ? Et si Nelson mastique bien un pain au chocolat, mais le recrache ensuite après en avoir avalé le "jus" ? On voit bien qu'on peut toujours être confronté à des cas limites, y compris pour des énoncés apparemment anodins.

Là se situe le point d'achoppement : la précision, la rigueur, l'exactitude. D'un coté, la logique – bi-valuée telle que présentée dans ce cours – semble inappropriée à rendre compte de la fragilité [8] des énoncés du langage courant. La logique semble donc incapable d'atteindre un texte dans son épaisseur, sa vraie richesse sémantique, sa densité, sa profondeur, ses multiples clés.

D'un autre côté, la démarche inverse, qui consiste à faire entrer le langage dans la forme logique, impose cet exercice de rigueur, de précision et d'exactitude, puisque tout doit y devenir explicite au risque de souffrir de platitude. C'est afin de mettre en œuvre une lente mais sûre progression dans l'argumentation que cette exigence d'une explicitation est requise.

Nous considérerons donc que le but de notre entreprise consiste à clarifier ce dont nous parlons, à préciser ce que nous disons, avec toujours comme direction maîtresse de lever autant que possible les ambiguités afin d'offrir un discours sans équivoque.

3.2 Les phrases composées

Les phrases simples que l'on vient de distinguer sont souvent reliées les unes aux autres par l'intermédiaire de connecteurs grammaticaux que nous allons tenter de rapprocher des

8. D'aucuns diraient imprécision et incertitude.

connecteurs logiques. Ce sont entre autres : *mais, ou, or, donc, alors, ou bien, cependant, ainsi, puis, en revanche, et, néanmoins, par contre, pourtant, toutefois, par conséquent*, etc.

La négation

La règle d'évaluation de la négation, c'est-à-dire celle du connecteur logique "$\neg$", est tout à fait évidente. Elle correspond point pour point à la négation dans son aspect grammatical : dans le langage courant, nier un énoncé, c'est affirmer la vérité de sa négation.

Exemples 36 Soit $P :=$ *les ornithorynques*[9] *sont des mammifères*, chacun des énoncés suivants se laisse traduire par $\neg P$:

(1) *Les ornithorynques* **ne** *sont* **pas** *des mammifères.*

(2) **Il n'est pas vrai que** *les ornithorynques sont des mammifères.*

(3) **Il est faux que** *les ornithorynques sont des mammifères.*

La conjonction

La règle d'évaluation de la conjonction est elle aussi très naturelle. Intuitivement, la conjonction n'est vraie que si les deux énoncés qu'elle lie sont vérifiés. Ainsi les phrases composées à l'aide du connecteur grammatical *et* sont traduites à l'aide du connecteur logique "$\wedge$".

Exemples 37 Soit $P :=$ *Albert se voyait déjà en haut de l'affiche* et $Q :=$ *Marie mourut avant d'avoir vécu.*

Chacun des énoncés suivants se laisse traduire par $P \wedge Q$.

(1) *Albert se voyait déjà en haut de l'affiche* **et** *Marie mourut avant d'avoir vécu.*

(2) **A la fois** *Albert se voyait déjà en haut de l'affiche* **et** *Marie mourut avant d'avoir vécu.*

(3) *Albert se voyait déjà en haut de l'affiche* **mais** *Marie mourut avant d'avoir vécu.*

(4) *Albert se voyait déjà en haut de l'affiche* **malgré que** *Marie mourut avant d'avoir vécu.*

(5) **Bien qu'***Albert se voyait déjà en haut de l'affiche, Marie mourut avant d'avoir vécu.*

(6) **Pendant qu'***Albert se voyait déjà en haut de l'affiche, Marie mourut avant d'avoir vécu.*

(7) **Alors qu'***Albert se voyait déjà en haut de l'affiche, Marie mourut avant d'avoir vécu.*

Mais la simple présence du mot "et" dans une phrase ne suffit pas à en faire un connecteur grammatical, encore moins un connecteur grammatical que l'on pourrait traduire par le connecteur logique "$\wedge$".

9. Mammifère australien amphibie et ovipare, à bec corné et doigts palmés munis de griffes.

Exemples 38 Dans ces exemples, le " *et*" n'est pas traduisible par "$\wedge$" :

(1) *Carole* **et** *Laurent sont dans la même classe.*

(2) *Deux* **et** *deux font quatre.*

(3) *Tout ce qui est jouissif est illégal, immoral* **et** *fait grossir.*

La première phrase *"Carole* **et** *Laurent sont dans la même classe"*, ne peut pas s'écrire directement sous la forme $P \wedge Q$ en prenant par exemple $P :=$ *Carole est dans la même classe* et $Q :=$ *Laurent est dans la même classe.* Il faudrait d'abord pouvoir la transformer en : *"Carole* **et** *Laurent sont dans la classe X"*; ou encore mieux : *"Carole est dans la classe X* **et** *Laurent est dans la classe X".*

La seconde phrase *"Deux* **et** *deux font quatre"* n'a aucune chance de pouvoir être modifiée pour faire apparaître une conjonction. *Deux* **et** *deux font quatre* signifie simplement que " $2 + 2 = 4$". C'est un énoncé simple, insécable et surtout non recomposable à l'aide de la conjonction.

La dernière phrase des exemples précédents peut par contre être traduite par la phrase équivalente suivante dans laquelle chaque *"et"* correspond bien à une conjonction logique : *"Tout ce qui est jouissif est illégal* **et** *tout ce qui est jouissif est immoral* **et** *tout ce qui est jouissif fait grossir".*

Les disjonctions

Apparemment, il en va de même de la disjonction de deux énoncés. Celle-ci n'est fausse que lorsque les deux énoncés sont faux. Mais dans la réalité, ce n'est pas toujours le cas. Le *"ou"* n'est pas systématiquement employé au même sens que notre connecteur logique "$\vee$". Il peut avoir deux significations différentes qui correspondent à deux connecteurs logiques différents : le *"ou exclusif"* et le *"ou inclusif"*, notre "$\vee$" logique correspondant au *"ou inclusif"*. Par exemple, dans la phrase suivante :

"Cette année je fais l'ascension de la face nord de l'Eiger ou celle du Cervin."

Ici, la proposition n'est fausse que si je ne réussis l'ascension d'aucune de ces deux montagnes. Par contre, que je réussisse à gravir seulement l'une des deux ou bien toutes les deux, mon assertion sera vérifiée. C'est ce qu'on appelle l'usage *inclusif* du *ou.* Si je pose $P :=$ *cette année je fais l'ascension de la face nord de l'Eiger* et $Q :=$ *cette année je fais l'ascension de la face nord du Cervin*, la phrase *"Cette année je fais l'ascension de la face nord de l'Eiger ou celle du Cervin"* se laisse tout naturellement traduire par $P \vee Q$.

Au contraire, si l'on avait affaire à un *"ou exclusif"*, la possibilté des deux ascensions réussies dans l'année serait exclue. L'usage *exclusif* du *"ou"* se rencontre par exemple dans une phrase telle que

"Le gagnant remporte une voiture neuve ou \$25'000".

Ici, la proposition est fausse dans le cas où le gagnant ne remporte aucun lot, mais elle est également fausse dans le cas où le gagnant remporte les deux lots à la fois. Elle n'est valide que si le gagnant remporte ou bien la voiture neuve, ou bien \$25'000, mais pas les deux. Si l'on pose $P :=$ *le gagnant remporte une voiture neuve* et $Q :=$ *le gagnant remporte \$25'000*, la phrase *"le gagnant remporte une voiture neuve ou \$25'000"* se laisse naturellement traduire par la formule un petit peu plus compliquée :

$$(P \vee Q) \wedge \neg(P \wedge Q).$$

Ou pour le dire en mots : *"l'un ou l'autre, mais pas les deux"*.

Considérons tout d'abord des exemples de phrases dans lesquelles le connecteur grammatical peut être traduit par le "*ou inclusif*" qu'est "$\vee$".

Exemples 39 Soit $P :=$ *il pleuvra demain* et $Q :=$ *il neigera demain.*

Chacun des énoncés suivants se laisse traduire par $P \vee Q$:

(1) *Il pleuvra* **ou** *il neigera demain.*
(2) *Il pleuvra* **ou bien** *il neigera demain.*
(3) **Ou bien** *il pleuvra* **ou bien** *il neigera demain.*
(4) *Il pleuvra* **ou alors** *il neigera demain.*

On peut discuter sur le fait que le troisième énoncé de l'exemple précédent corresponde bien à un usage inclusif du *"ou"* plutôt qu'à un usage exclusif. Mais c'est là matière à interprétation.

Considérons ensuite des exemples de phrases dans lesquelles le connecteur grammatical est un *"ou"* au sens exclusif :

Exemples 40

(1) *Le gagnant remporte une voiture neuve* **ou** *\$25'000.*
(2) *Le gagnant remporte une voiture neuve* **ou bien** *\$25'000.*
(3) *Le gagnant remporte* **ou bien** *une voiture neuve* **ou bien** *\$25'000.*
(4) *Le gagnant remporte une voiture neuve* **ou alors** *\$25'000.*

Chacune des phrases précédentes a exactement la même signification que la phrase suivante :

"Le gagnant remporte une voiture neuve ou \$25'000, mais pas les deux".

Si l'on pose $P :=$ *le gagnant remporte une voiture neuve* et $Q :=$ *le gagnant remporte \$25'000*, cette phrase se traduit sans aucune difficulté par la formule :

$$(P \vee Q) \wedge \neg(P \wedge Q).$$

Cette formule est fausse si et seulement si à la fois P et Q sont tous deux faux ou tous deux vrais. Autrement dit, la formule $(P \vee Q) \wedge \neg(P \wedge Q)$ et la formule $\neg(P \longleftrightarrow Q)$ sont vraies dans exactement les mêmes modèles. Aucun modèle ne peut vérifier l'une et falsifier l'autre. La dernière étant une traduction possible de l'énoncé : *"Il est faux que le gagnant remporte une voiture neuve si et seulement s'il remporte $25'000"*.

Il est intéressant de remarquer qu'un même connecteur (par exemple : *"ou"*, *"ou bien"*, ou *"alors"*) peut être traduit par un *"ou inclusif"* ou par un *"ou exclusif"*. Cela montre qu'il n'y a pas de signification univoque qui soit attachée à un connecteur grammatical. La manière dont il doit être traduit dépend de ce qu'il signifie dans l'énoncé que l'on considère. Tout est donc affaire d'interprétation. Dès lors, l'intérêt de la traduction d'un énoncé composé en formule du Calcul Propositionnel réside précisément dans le fait de lever toutes les ambiguïtés.

L'implication et la double implication

Tout comme pour la (les) disjonction(s), la règle d'évaluation de l'implication ne va pas réellement de soi. La règle d'évaluation de ce connecteur logique n'est pas toujours vraiment conforme à ce que l'on en attendrait. Intuitivement, l'implication semble correspondre à des énoncés de la forme *"si ... alors ..."*. Ce sont des énoncés dans lesquels une cause *implique* une conséquence, comme par exemple : *" s'il fait beau demain, je viens skier avec toi "*. Il y a un rapport de causalité entre le temps demain et le fait d'aller skier. Généralement, on interprète un tel énoncé comme signifiant : si le temps est au beau demain, je vais effectivement venir skier, mais si le temps n'est pas fameux, je n'irai tout simplement pas skier.

Pour se convaincre de cela, considérons l'énoncé que l'on peut emprunter à un père frustre et quelque peu brutal s'adressant à son fils : *"si tu n'arrêtes pas immédiatement de gesticuler, je te donne une paire de claques"*. Si ce rapport de causalité entre les gesticulations du fils et la paire de claques est perçu comme une implication au sens du Calcul Propositionnel, alors en se conformant à la définition de la règle d'évaluation de l'implication, le père ne serait en faute (logique) que si le fils n'arrête pas de gesticuler et qu'il ne lui administre pas la paire de claques promise. Ainsi, le père serait tout à fait dans son bon droit de donner une paire de claques à son fils, quand bien même celui-ci aurait cessé de s'agiter. La morale de cette histoire, c'est que l'implication de la logique n'est pas toujours conforme à l'implication du langage courant. Elle ne se confond pas avec les énoncés de la forme *"si ... alors ..."*. Cela dépend des cas, et comme pour les autres connecteurs, il faut à chaque fois interroger ce qu'est sensé signifier l'énoncé pour en déterminer sa traduction logique.

La phrase *"si tu n'arrêtes pas immédiatement de gesticuler, je te donne une paire de claques"* est certainement comprise par nous tous comme une double implication entre la perpétuation de l'agitation et l'administration de la paire de claques. On entend en effet : *si tu arrêtes de gesticuler, je ne te donne pas de claques, mais si tu n'arrêtes pas, alors je te gifle*. Cela signifie simplement que le connecteur logique en jeu n'est pas l'implication mais la double implication.

L'implication correspond à ce que les Stoïciens appelaient proposition *conditionnelle* (*s'il fait jour, il fait clair*), qu'ils distinguaient de la proposition *subconditionnelle* (*puisqu'il fait jour, il fait clair*) qui indique non seulement qu'il y a un rapport d'implication entre l'antécédent (*il fait jour*) et le conséquent (*il fait clair*), mais qu'en plus l'antécédent est avéré. Cette *subconditionnelle* correspond à la formule $(P \longrightarrow Q) \wedge P$ (*s'il fait jour, il fait clair ; et il fait jour*).

Exemples 41 Soit $P :=$ *vous avez une meilleure idée* et $Q :=$ *je suis toutes ouïes.*

Chacun des énoncés suivants se laisse traduire par $P \longrightarrow Q$.

(1) **Si** *vous avez une meilleure idée,* **alors** *je suis toutes ouïes.*

(2) **Si** *vous avez une meilleure idée, je suis toutes ouïes.*

(3) **Dans la mesure où** *vous avez une meilleure idée, je suis toutes ouïes.*

(4) *Vous avez une meilleure idée,* **par conséquent** *je suis toutes ouïes.*

(5) **Si** *vous avez une meilleure idée,* **il s'en suit que** *je suis toutes ouïes.*

Ci-dessous quelques exemples de phrases composées traduites par une formule avec connecteur de double implication. On verra un peu plus loin dans quels cas on utilise l'expression *si et seulement si* pour rendre compte de la double implication en logique.

Exemples 42 Soit $P :=$ *Carole est enceinte* et $Q :=$ *le test de grossesse est positif.*

Chacun des énoncés suivants se laisse traduire par $P \longleftrightarrow Q$:

(1) *Carole est enceinte* **si et seulement si** *le test de grossesse est positif.*

(2) *Carole est enceinte* **exactement lorsque** *le test de grossesse est positif.*

(3) *Carole est enceinte* **précisément si** *le test de grossesse est positif.*

(4) *Carole est enceinte* **dans la mesure exacte où** *le test de grossesse est positif.*

(5) *Carole est enceinte* **dans le cas uniquement où** *le test de grossesse est positif.*

On utilisera l'abréviation *ssi* au lieu d'écrire *si et seulement si.*

Quelques exemples de traduction de phrases composées

Les phrases qui utilisent *"à moins que"*. Les phrases comme *"à moins que tu ne t'excuses tout de suite, je te trainerais devant les tribunaux"*, sont comprises comme signifiant *"si tu ne t'excuses pas tout de suite alors je te traînerais devant les tribunaux"* indiquant par là que les démarches judiciaires sont les conséquences certaines de l'absence d'excuse. Elles sont donc traduites en formules propostionnelles comme le serait cette dernière.

Exemples 43 Chacun des énoncés suivants se laisse traduire par $\neg Q \longrightarrow P$:

(1) $\underbrace{\textit{Carole vient manger ce soir}}_{P}$ **à moins que** $\underbrace{\textit{le test de grossesse ne soit positif.}}_{Q}$

(2) **A moins que** $\underbrace{\textit{vous ne soyez accompagné,}}_{Q}$ $\underbrace{\textit{vous ne pouvez pas voyager en avion.}}_{P}$

(3) **A moins qu'** $\underbrace{\textit{on ne m'agresse,}}_{Q}$ $\underbrace{\textit{je tâcherai d'être plaisant.}}_{P}$

Les phrases qui utilisent *"seulement si"*. Les phrases comme *"je viendrai ce soir seulement si je fais partie des invités"*, sont perçues comme voulant dire *"si je viens ce soir alors c'est que je fais partie des invités, sinon je ne viens pas"*. Il est sous-entendu que cette proposition est fausse dans le seul cas où je viens ce soir sans avoir été invité. Elles sont donc traduites en formules propositionnelles comme la phrase *"si je viens ce soir, alors je fais partie des invités"*.

Exemples 44 Chacun des énoncés suivants se laisse traduire par $P \longrightarrow Q$:

(1) $\underbrace{\textit{Carole vient manger ce soir}}_{P}$ **seulement si** $\underbrace{\textit{le test de grossesse est négatif.}}_{Q}$

(2) $\underbrace{\textit{J'arriverai à mes fins}}_{P}$ **seulement si** $\underbrace{\textit{je m'en donne la peine.}}_{Q}$

(3) $\underbrace{\textit{Le Diable existe}}_{P}$ **seulement si** $\underbrace{\textit{Dieu existe.}}_{Q}$

Remarque 45 La raison pour laquelle on traduit en parole la double implication logique par un *"si et seulement si"* réside en ce qu'une formule $\phi \longleftrightarrow \psi$ est équivalente à la conjonction des deux formules $\phi \longrightarrow \psi$ et $\phi \longleftarrow \psi$ (où $\phi \longleftarrow \psi$ est simplement une autre manière d'écrire la formule $\psi \longrightarrow \phi$). Maintenant si l'on veut prononcer ces deux formules, on dira pour $\phi \longrightarrow \psi$: "ϕ *implique* ψ", ou encore "ϕ *seulement si* ψ". Et pour $\phi \longleftarrow \psi$, on dira " si ψ *alors* ϕ", ou encore "ϕ *si* ψ".

En combinant les deux, on obtient donc que $\phi \longleftrightarrow \psi$ correspond à "ϕ *si et seulement si* ψ" (le *si* étant la direction $\longleftarrow$ de l'implication, le *seulement si* correspondant à la direction $\longrightarrow$).

On appelle également la formule $\phi \longleftrightarrow \psi$ une double implication (parce qu'il y a une implication dans les deux sens : de droite à gauche " $\longleftarrow$" et de gauche à droite " $\longrightarrow$"; ou encore une biconditionnelle pour les mêmes raisons, car l'implication est aussi appelée conditionnelle.

Les phrases qui utilisent *"ni... ni... "*. De telles phrases comme *"il n'y a plus ni miel ni confiture"* se laissent traduire par la formule $\neg P \wedge \neg Q$[10] où $P :=$ *il y a du miel* et $Q :=$ *il y a de la confiture.*

Quelques exemples de traduction de phrases composées

Exemples 46 Considérons les phrases atomiques suivantes :

P := Les tortues sont têtues.

Q := Les sirènes ont de grands yeux en amande.

R := La paperasse s'accumule.

10. Ou de manière équivalente par $\neg(P \vee Q)$.

On traduit alors les phrases composées suivantes par :

(1) Il est faux que si les sirènes ont de grands yeux en amande, alors la paperasse ne s'accumule pas.
$$\neg(Q \longrightarrow \neg R).$$

(2) les tortues sont têtues et la paperasse s'accumule toujours, ou alors les sirènes ont de grands yeux en amande.
$$(P \wedge R) \vee Q.$$

(3) Les tortues ne sont pas têtues si et seulement s'il est faux que la paperasse s'accumule.
$$\neg P \longleftrightarrow \neg R.$$

(4) Si les sirènes ont de grands yeux en amande, alors non seulement les tortues sont têtues mais en plus il est faux que la paperasse s'accumule.
$$Q \longrightarrow (P \wedge \neg R).$$

Nous savons désormais comment effectuer la traduction du langage courant en formule et réciproquement. Nous pouvons maintenant passer à l'étape suivante qui est de comparer les énoncés en comparant les formules qu'ils génèrent.

Pour aller plus avant :

Le lecteur intéressé aux relations entre logique et langage naturel est invité à regarder les ouvrages suivants : *"Introduction à la logique naturelle et approche logique du langage"* de Jean-Blaise Grize [Gri82b], *"Introduction à la logique pertinente"* de François Rivenc [Riv05], *"Raisonnement et pensée critique : introduction à la logique informelle"* de Martin Montminy [Mon09], *"Construire le sens"* de Jean-Blaise Grize et Josiane Boutet [BG94] et *"Logic and philosophy : A modern introduction"* de Paul Tidman et Howard Kahane [TK03].

Il pourra également porter son intérêt vers le chapitre de l'Encyclopédie de la Pléiade consacrée à Jean Piaget intitulé *"Logique des classes et des propositions"* et rédigé par Jean-Blaise Grize [Gri67].

---

4 Formules logiquement équivalentes

Résumé № 8 *Deux formules sont logiquement équivalentes si elles sont vraies dans exactement les mêmes modèles. Elles ne sont pas logiquement équivalentes s'il existe un modèle qui vérifie l'une et falsifie l'autre.* ※

Ce que nous avons fait jusque là consistait à nous poser la question de la valeur de la formule dans un modèle : étant donnée une formule quelconque ϕ du Calcul Propositionnel, et un modèle $\mathcal{M}$ de celui-ci, nous posions la question de la valeur de vérité de cette formule dans ce modèle. A savoir, ϕ est-elle satisfaite dans $\mathcal{M}$? (c'est-à-dire si δ est la distribution de valeurs de vérité qui caractérise $\mathcal{M}$, la question se présente comme “est-ce que $\delta_{\mathcal{F}}(\phi) = 1$?”). Nous introduisons une notation très pratique pour dire cela qui généralise celle que nous avions employée pour décrire quelle était la distribution de valeurs de vérité sur les variables propositionnelles d'un modèle.

Notation 47 *Soient $\mathcal{M}$, un modèle du Calcul Propositionnel et δ sa distribution de valeurs de vérité, ainsi que ϕ une formule.*

$$\mathcal{M} \vDash \phi \textit{ signifie } \delta_{\mathcal{F}}(\phi) = 1 \ ; \quad \mathcal{M} \nvDash \phi \textit{ signifie } \delta_{\mathcal{F}}(\phi) = 0.$$

Dans la définition d'un modèle, la distribution de valeur de vérité est une fonction de VAR dans $\{0, 1\}$, donc une fonction de l'ensemble de toutes les variables propositionnelles de notre logique. Or, pour connaître la valeur d'une formule donnée dans ce modèle, seules les valeurs de vérité des variables propositionnelles qui apparaîssent dans cette formule sont nécessaires. Pour ce qui est des autres, peu nous importe leur valeur. Voilà pourquoi, lorsque l'on considère la valeur de vérité d'une formule ou d'un ensemble de formules, on peut toujours se restreindre à ne considérer que les valeurs de vérité des seules variables propositionnelles apparaîssant dans ces formules.

Comparer deux formules quelconques ϕ et ψ revient à regarder ce qui les différencie. Les comparer sur le plan sémantique consiste donc à scruter ce qui, au niveau de leurs interprétations, permet de les distinguer. Autrement dit, cela revient à consulter le catalogue de tous les modèles possibles et discriminer parmi eux ceux qui permettent de les différencier : les modèles dans lesquels l'une des formules est vraie alors que l'autre est fausse. S'il n'est pas possible de trouver un modèle qui distingue ces formules, alors ces formules sont dites équivalentes, ce que l'on note $\phi \equiv \psi$.

Définition 48 *Soient $\phi, \psi \in \mathcal{F}$,*

$$\phi \textit{ et } \psi \textit{ sont équivalentes ssi elles sont satisfaites dans les mêmes modèles}$$

i.e. elles prennent les mêmes valeurs dans les mêmes modèles

$$\phi \equiv \psi \textit{ ssi } \Big(\mathcal{M} \vDash \phi \textit{ ssi } \mathcal{M} \vDash \psi\Big) \textit{ pour tout modèle } \mathcal{M}.$$

Une conséquence immédiate de cette définition est que deux formules sont équivalentes précisément lorsque l'équivalence logique de ces deux formules est vérifiée dans tout modèle.

Corollaire 49 *Soient* $\phi, \psi \in \mathcal{F}$,

$$\phi \equiv \psi \textit{ ssi } \Big(\textit{pour tout modèle } \mathcal{M}, \quad \mathcal{M} \vDash \phi \longleftrightarrow \psi \Big)$$

Preuve du Corollaire 49 : Considérons un modèle quelconque $\mathcal{M}$. Si les deux formules ϕ et ψ sont équivalentes, elles prennent donc la même valeur dans ce modèle. Ce qui veut dire $\delta_{\mathcal{F}}(\phi) = \delta_{\mathcal{F}}(\psi)$. Par conséquent, la formule $\phi \longleftrightarrow \psi$ est vraie dans ce modèle : $\delta_{\mathcal{F}}(\phi \longleftrightarrow \psi) = 1$.

Inversément, si la formule $\phi \longleftrightarrow \psi$ est vraie dans tout modèle, cela signifie que dans n'importe quel modèle, les valeurs que prennent ϕ et ψ sont identiques. $\dashv$ 49

Exemple 50

(1) On a les équivalences suivantes :

(a) $P \wedge P \equiv P$

(b) $P \vee P \equiv P$

(c) $\neg\neg P \equiv P$

(d) $P \longrightarrow Q \equiv \neg P \vee Q$

(e) $P \longleftrightarrow Q \equiv (P \longrightarrow Q) \wedge (Q \longrightarrow P)$

(f) $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$

(2) On a les inéquivalences suivantes :

(a) $P \wedge P \not\equiv Q \wedge Q$ $\rightsquigarrow$ *prendre* $\mathcal{M}$ *tel que* $\mathcal{M} \models P, \neg Q$

(b) $P \longrightarrow P \not\equiv P$ $\rightsquigarrow$ *prendre* $\mathcal{M}$ *tel que* $\mathcal{M} \models \neg P$

(c) $P \longleftrightarrow Q \not\equiv P \longrightarrow Q$ $\rightsquigarrow$ *prendre* $\mathcal{M}$ *tel que* $\mathcal{M} \models \neg P, Q$

(d) $P \longrightarrow (P \longrightarrow P) \not\equiv (P \longrightarrow P) \longrightarrow P$ $\rightsquigarrow$ *considérer le modèle* $\mathcal{M} \models \neg P$

La remarque qui suit montre que la relation $\equiv$ est une relation réflexive, symétrique et transitive. C'est donc une relation d'équivalence, ce qui justifie sa dénomination.

Remarque 51 Pour toutes formules ϕ, ψ, $\theta \in \mathcal{F}$, les propriétés suivantes sont vérifiées :

réflexivité : $\phi \equiv \phi$

symétrie : $\phi \equiv \psi$ si et seulement si $\psi \equiv \phi$

transitivité : Si $(\phi \equiv \psi$ et $\psi \equiv \theta)$ alors $\phi \equiv \theta$.

Il est bon de noter que la disjonction comme la conjonction sont des opérations commutatives. En conséquence, du point de vue sémantique, nous pourrons ne pas faire grand cas de l'ordre dans lequel des formules apparaîssent au sein d'une disjonction ou d'une conjonction. De même, ces deux opérations étant également associatives, nous avons les équivalences suivantes pour toutes formules ϕ, ψ, θ :

- $(\phi \vee \psi) \vee \theta \equiv \phi \vee (\psi \vee \theta) \equiv \psi \vee (\theta \vee \phi) \equiv \theta \vee (\phi \vee \psi) \equiv (\theta \vee \phi) \vee \psi \equiv (\phi \vee \theta) \vee \psi \equiv \ldots$

- $(\phi \wedge \psi) \wedge \theta \equiv \phi \wedge (\psi \wedge \theta) \equiv \psi \wedge (\theta \wedge \phi) \equiv \theta \wedge (\phi \wedge \psi) \equiv (\theta \wedge \phi) \wedge \psi \equiv (\phi \wedge \theta) \wedge \psi \equiv \ldots$

Cette remarque nous conduit à la notation suivante dans laquelle l'ordre sur les formules n'importe guère du point de vue sémantique.

Notation 52 *Afin d'éviter de surcharger le texte entre parenthèses, nous utilisons les notations suivantes :*

(1) $(\phi_0 \wedge \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_k)$ *ou bien* $\bigwedge_{0 \leq i \leq k} \phi_i$ *à la place de* $(\phi_0 \wedge (\phi_1 \wedge (\phi_2 \wedge (\ldots \wedge \phi_k \underbrace{)))}_{k} \ldots)$.

(2) $(\phi_0 \vee \phi_1 \vee \phi_2 \vee \ldots \vee \phi_k)$ *ou bien* $\bigvee_{0 \leq i \leq k} \phi_i$ *au lieu de* $(\phi_0 \vee (\phi_1 \vee (\phi_2 \vee (\ldots \vee \phi_k \underbrace{)))}_{k} \ldots)$.

Nous obtenons donc les équivalences suivantes :

(1) $\bigwedge_{0 \leq i \leq k} \neg\phi_i \equiv \neg \bigvee_{0 \leq i \leq k} \phi_i$ (2) $\bigvee_{0 \leq i \leq k} \neg\phi_i \equiv \neg \bigwedge_{0 \leq i \leq k} \phi_i$.

que l'on mémorisera aisément en disant que la négation se distribue à l'intérieur d'une disjonction (respectivement une conjonction) en inversant le signe (de haut en bas ou de bas en haut). La disjonction devient alors une conjonction, et la conjonction se change en disjonction.

5 Théorie et conséquence logique

Résumé № 9

- *Une* théorie $\mathcal{T}$ *du Calcul Propositionnel est un ensemble de formules. Elle est* satisfaite *dans le modèle* $\mathcal{M}$ *– noté* $\mathcal{M} \models \mathcal{T}$ *– si pour toute formule* $\phi \in \mathcal{T}$, $\mathcal{M} \models \phi$*. On dit alors que* $\mathcal{M}$ *est un* modèle *de* $\mathcal{T}$.
- *Une théorie est* satisfaisable *si elle est satisfaite dans un modèle, elle est* inconsistante *sinon.*
- *Deux théories sont dites équivalentes si elles sont satisfaites dans les mêmes modèles.*
- *Une formule* ϕ *est* conséquence *de* $\mathcal{T}$ *– noté* $\mathcal{T} \models \phi$ *– si tout modèle satisfaisant* $\mathcal{T}$ *satisfait également* ϕ. ※

En introduction, nous avons vu qu'une formule se comporte métaphoriquement comme une phrase du langage courant. La comparaison entre logique et langage se poursuit avec le livre ou le discours comme ensemble de phrases. La *théorie* constitue l'équivalent logique du discours, avec la différence notoire qu'une théorie est un ensemble de formules, alors qu'un discours ou un livre sont des suites de phrases : l'ordre des phrases est primordial, alors que dans une théorie, l'ordre des formules n'a aucune importance. Il n'y a d'ailleurs pas d'ordre du tout entre les formules.

Définition 53 *Une théorie* $\mathcal{T}$ *du Calcul Propositionnel est un ensemble de formules :*

$$\mathcal{T} \subseteq \mathcal{F}.$$

La sémantique associée à la notion de théorie est la plus naturelle qui soit : on interprète une théorie comme on interprète les formules qui la constituent. On rappelle qu'un modèle du Calcul Propositionnel est de la forme $\mathcal{M}$, où la distribution de valeurs de vérité δ associe à *chaque variable propositionnelle* la valeur 0 ou 1.

Définition 54 *Soit* $\mathcal{T} \subseteq \mathcal{F}$, $\mathcal{T}' \subseteq \mathcal{F}$, $\phi \in \mathcal{F}$ *et* $\mathcal{M}$ *un modèle du Calcul Propositionnel,*

(1) $\mathcal{T}$ *est* satisfaite *dans le modèle* $\mathcal{M}$*, ou encore* $\mathcal{M}$ *est un modèle de* $\mathcal{T}$ *– noté* $\mathcal{M} \models \mathcal{T}$ *– si pour toute formule* $\phi \in \mathcal{T}$, $\mathcal{M} \models \phi$.

(2) $\mathcal{T}$ *est* satisfaisable *ou* consistante *s'il existe au moins un modèle* $\mathcal{M}$ *tel que* $\mathcal{M} \models \mathcal{T}$.

(3) $\mathcal{T}$ *est* inconsistante *si* $\mathcal{T}$ *n'est pas satisfaisable.*

Remarques 55

(1) Tout se passe donc au niveau sémantique, comme si la théorie n'était pas autre chose que la conjonction des formules qui la constituent. C'est effectivement le cas lorsque la théorie est finie. Une théorie finie se comporte exactement comme la formule donnée par la conjonction des formules qu'elle contient. Par contre, la conjonction d'une infinité de formules n'est pas une formule, puisque toute formule est une suite finie de symboles. Pourtant, par extension, il est commode de penser à une théorie infinie comme à une "formule" qui serait la conjonction infinie des formules la constituant.

La raison de cela réside dans le fait qu'une théorie est satisfaite dans un modèle si et seulement si chacune de ses formules l'est ; ce qui revient à dire que la conjonction de celles-ci l'est.

(2) Intuitivement, une théorie est consistante si elle ne se contredit pas et possède donc une certaine consistance. Autrement dit, si elle n'est pas que du vent. Cela signifie qu'elle a au moins un modèle, donc qu'elle énonce quelque chose, qu'elle dit réellement quelque chose qui fasse sens.

(3) Cette notion n'a d'intérêt que pour les théories infinies. Nous verrons plus loin qu'elle permet un résultat très surprenant sur la satisfaction de théories ; où l'infini se nourrit du fini.

(4) Une théorie est inconsistante lorsqu'elle n'a pas de modèle. Elle dit à la fois quelque chose et son contraire, ce qui ne peut être vérifié nulle part. Donc elle ne raconte rien, elle ne dit rien, elle ne décrit rien. Les théories inconsistantes sont celles qu'on souhaiterait fuir comme la peste. Malheureusement, il n'est pas toujours facile de savoir si une théorie est consistante ou non.

Du point de vue sémantique, une théorie désigne l'ensemble des modèles qui la satisfont et qui constituent en quelque sorte la signification de cette théorie. En conséquence, deux théories peuvent être comparées d'un point de vue sémantique en mettant en parallèle leurs ensembles de modèles respectifs au moyen de l'inclusion.

Définition 56 *Soit $\mathcal{T} \subseteq \mathcal{F}$, $\mathcal{T}' \subseteq \mathcal{F}$ et $\mathcal{M}$ un modèle du Calcul Propositionnel,*

(1) $\mathcal{T}'$ est une conséquence sémantique de $\mathcal{T}$ – noté $\mathcal{T} \models \mathcal{T}'$ – si tout modèle satisfaisant $\mathcal{T}$ satisfait également $\mathcal{T}'$.

(2) $\mathcal{T}$ et $\mathcal{T}'$ sont deux théories équivalentes – noté $\mathcal{T} \equiv \mathcal{T}'$ – si elles ont exactement les mêmes modèles.

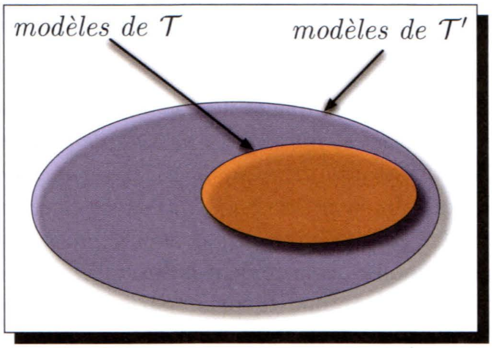
Intuitivement, plus une théorie raconte de choses, moins elle possède de modèle. A la limite, si elle raconte trop de choses, elle devient inconsistante et n'est donc plus satisfaite dans aucun modèle.

Notation 57

- *Lorsqu'une théorie se réduit à un singleton, on omet généralement les accolades pour alléger l'écriture. On écrit ainsi $\mathcal{T} \models \phi$ au lieu de $\mathcal{T} \models \{\phi\}$ et $\mathcal{T} \equiv \phi$ au lieu de $\mathcal{T} \equiv \{\phi\}$.*
- *on écrit $\models \phi$ pour $\emptyset \models \phi$.*

La théorie vide ne dit rien du tout. En cela non seulement elle n'est pas inconsistante, mais elle est satisfaite dans tout modèle quel qu'il soit. Dès lors, dire que ϕ est conséquence logique de la théorie vide, c'est dire que ϕ est vraie dans tout modèle. On appelle une telle formule une *tautologie*.

La notion de conséquence repose sur l'étude des modèles que satisfait une théorie. C'est donc une notion sémantique de conséquence. En toute rigueur, on devrait l'appeler conséquence logique sémantique. Mais pour alléger le texte, nous parlons simplement de conséquence. Nous verrons dans le chapitre suivant une autre espèce de conséquence, qui n'est pas sémantique mais syntaxique. Il s'agira de la notion de conséquence telle qu'elle apparaît dans les démonstrations. Cette conséquence syntaxique n'a pas affaire avec des modèles, elle n'a pas à voir avec la signification des énoncés. Elle repose sur des règles de réécriture. Elle ne s'intéresse pas au contenu des formules – leurs signification, les modèles dans lesquelles elles sont vraies – mais à leur forme. Ici, la conséquence sémantique ne s'intéresse qu'à la signification des énoncés. Une formule est conséquence sémantique d'une théorie si elle est vraie partout où cette théorie est vraie. Autrement dit, cette formule est satisfaite dans tout modèle vérifiant chacune des formules qui constitue la théorie. Une autre vue de la chose consiste à faire remarquer que $\mathcal{T} \vDash \phi$ si et seulement si l'ensemble des modèles de ϕ contient l'ensemble des modèles de $\mathcal{T}$.



Inclusion des ensembles de modèles respectifs de $\mathcal{T}$ et de $\mathcal{T}'$ lorsque $\mathcal{T} \vDash \mathcal{T}'$ est vérifié.

La notion d'équivalence (sémantique) entre deux théories reprend l'idée qui préside à l'équivalence de deux formules. Des formules équivalentes ont exactement les mêmes modèles. *Stricto sensu* nous devrions changer de notation et utiliser un symbole pour dénoter que deux formules sont équivalentes et un symbole différent pour dire que deux théories sont équivalentes. Mais on comprendra aisément que le cas de deux formules équivalentes – $\phi \equiv \psi$ – tombe sous celui de deux théories équivalentes – $\{\phi\} \equiv \{\psi\}$ – en prenant les théories formées des singletons de chacune de ces formules. Deux formules équivalentes sont vraies dans les mêmes modèles et fausses dans les mêmes modèles également. C'est la même chose pour les théories. Deux théories équivalentes ont exactement les mêmes modèles, ce qui revient à dire qu'il n'existe pas de modèle permettant de les discriminer. Elles signifient la même chose ; elles parlent des mêmes choses, même si elles le font de manière différente. Elles ne sont pas nécessairement égales, car elles ne sont pas nécessairement le même ensemble de formules ; mais elles sont égales sur le plan sémantique puisqu'elles signifient la même chose. Il apparaît immédiatement que $\mathcal{T} \equiv \mathcal{T}'$ correspond à avoir à la fois $\mathcal{T} \models \mathcal{T}'$ et $\mathcal{T}' \models \mathcal{T}$ vérifiés.

Pour plus de clarté dans le discours, nous considérons dans les exemples qui suivent que P_0 traduit en Calcul Propositionnel la proposition *"je skierai aujourd'hui"*, P_1 traduit *"je skierai demain"*, et plus généralement P_k traduit *"je skierai dans k jours à compter d'aujourd'hui"*. Nous imaginons également que Q représente *"dès leur plus jeune âge, les huîtres savent parfaitement skier, sans bâtons."*

Exemple 58 Les théories suivantes sont toutes équivalentes :

(1) $\mathcal{T}_0 = \{\neg(P_0 \wedge P_3), P_1 \wedge P_2, P_3\}$

(2) $\mathcal{T}_1 = \{\neg P_0 \longrightarrow P_3, \neg(P_1 \longrightarrow \neg P_2), \neg P_1 \longrightarrow P_0, \neg P_0\}$

(3) $\mathcal{T}_2 = \{P_3, P_1, P_2, \neg P_0 \vee \neg P_3\}$

(4) $\mathcal{T}_3 = \{P_1, P_2, P_3, \neg P_0 \vee \neg P_3\}$

(5) $\mathcal{T}_4 = \{\neg P_0, P_1, P_2, P_3\}$

Intuitivement, des théories équivalentes *"racontent"* la même chose, mais avec des termes différents. C'est le cas de $\mathcal{T}_1$ dans l'exemple ci-dessus qui dit : *"si je ne skie pas aujourd'hui, je skie dans 3 jours, par ailleurs il est faux que si je skie demain alors je ne skie pas après-demain, et également si je ne skie pas demain, je ne skie pas aujourd'hui, mais je ne skie pas aujourd'hui."* Et de $\mathcal{T}_4$ qui dit la même chose, mais de manière beaucoup plus directe, moins alambiquée : *"je ne skie pas aujourd'hui, je skie demain, après-demain et dans trois jours."* Dire qu'elles sont équivalentes, cela revient à dire qu'il n'existe pas de modèle capable de les différencier. Si l'on convient qu'une théorie "parle" des modèles dans lesquels toutes ses formules sont vérifiées, alors deux théories équivalentes parlent exactement des mêmes modèles. Elles "décrivent" les mêmes mondes possibles, elles racontent donc la même chose.

Exemple 59 Les théories suivantes sont toutes inconsistantes. Elles sont donc par ailleurs également toutes équivalentes les unes aux autres.

- $\mathcal{T}_5 = \{P_0, P_0 \longrightarrow P_1, P_2 \longrightarrow \neg P_1, P_2 \vee \neg P_0\}$
- $\mathcal{T}_7 = \{P_0 \wedge \neg P_0\}$
- $\mathcal{T}_6 = \{P_0, P_0 \longrightarrow P_2, P_0 \longrightarrow \neg P_2\}$
- $\mathcal{T}_8 = \{Q, \neg Q\}$

Une théorie inconsistante est une théorie sans modèle. Elle ne décrit rien, elle ne parle de rien. Ou pour le dire autrement, elle parle pour ne rien dire. Très naturellement, nous écrivons $\mathcal{T} \not\models \phi$ pour dire que $\mathcal{T} \models \phi$ est faux.

Exemple 60 Soit $\mathcal{T} = \{\neg P_0 \longrightarrow P_3, \neg(P_1 \longrightarrow \neg P_2), \neg P_1 \longrightarrow P_0, \neg P_0\}$,

(1) $\mathcal{T} \models P_1 \wedge P_2 \wedge (P_3 \vee \neg P_3)$

(2) $\mathcal{T} \models P_1 \longrightarrow P_2$

(3) $\mathcal{T} \models P_1 \longrightarrow P_1$

(4) $\mathcal{T} \not\models \neg P_0 \longrightarrow \neg P_1$

(5) $\mathcal{T} \not\models \neg(\neg P_0 \vee P_0)$

(6) $\mathcal{T} \not\models P_0 \vee P_1$

La notion de conséquence logique est essentielle. Elle est la version sémantique de la notion de déduction. Dire qu'une formule est une conséquence logique d'une théorie, c'est dire que partout où cette théorie est satisfaite, cette formule l'est également. Ou pour le dire en termes métaphoriques : dans chaque univers où notre théorie est vérifiée, la formule en question est également assertée. Cette formule découle donc de la théorie. Nous verrons plus tard que dans une logique correctement constituée, une formule est une conséquence d'une théorie si elle peut être déduite de cette théorie et réciproquement.

Exemple 61 Les théories suivantes sont équivalentes :

(1) $\mathcal{T}_9 = \{P_0 \wedge P_1, (P_0 \wedge P_1 \wedge P_2), \ldots\ldots\ldots, (P_0 \wedge P_1 \wedge P_2 \wedge \ldots \wedge P_k), \ldots\ldots\}$

(2) $\mathcal{T}_{10} = \{P_0, P_0 \longrightarrow P_1, P_1 \longrightarrow P_2, \ldots\ldots\ldots, P_k \longrightarrow P_{k+1}, , P_{k+1} \longrightarrow P_{k+2}, \ldots\ldots\ldots\}$

(3) $\mathcal{T}_{11} = \{P_0, P_1, P_2, \ldots\ldots\ldots, P_k, \ldots\ldots\}$

Chacune de ces théories est satisfaisable. Par contre, aucune d'entre elles n'est équivalente à une théorie finie.

Remarques 62

(1) (a) Si $\mathcal{T}$ est satisfaisable et $\mathcal{T}' \subseteq \mathcal{T}$, alors $\mathcal{T}'$ est également satisfaisable.
En restreignant une théorie, on conserve la non-contradiction. C'est là un résultat qui découle directement de la définition même. Par contre le contraire n'est pas vrai, si une théorie $\mathcal{T}'$ est satisfaisable, il n'est pas nécessairement vrai que $\mathcal{T}$ – qui contient $\mathcal{T}'$ – le soit. L'image qu'il faut avoir en tête est que plus on ajoute de formules nouvelles à une théorie, plus le nombre des modèles qui la satisfait diminue. Et inversément, plus on retranche de formules à une même théorie, plus le nombre de ses modèles s'accroît, pour atteindre à la limite tous les modèles possibles lorsque la théorie devient vide.

(b) Si $\mathcal{T}'$ est inconsistante et $\mathcal{T}' \subseteq \mathcal{T}$, alors $\mathcal{T}'$ est inconsistante.
C'est là une conséquence du cas précédent. Etendre une théorie inconsistante ne peut jamais permettre de la rendre satisfaisable.

(c) Si $\mathcal{T}$ est satisfaisable, alors toute théorie *finie* $\mathcal{T}' \subseteq \mathcal{T}$ est satisfaisable.
C'est là un cas particulier du cas (1)(a).

(d) Si $\mathcal{T}' \vDash \phi$ et $\mathcal{T}' \subseteq \mathcal{T}$, alors $\mathcal{T} \vDash \phi$. Si ϕ est conséquence d'une théorie, alors elle est conséquence de toute théorie qui étend celle-ci. En effet, lorsqu'on étend une théorie, on restreint l'ensemble des modèles qui satisfont cette théorie étendue.

(2) (a) $\mathcal{T}$ est inconsistante ssi $\mathcal{T} \vDash \phi \wedge \neg\phi$.

(b) $\mathcal{T}$ est inconsistante ssi il existe une *contradiction* ϕ, telle que $\mathcal{T} \vDash \phi$.

(c) $\mathcal{T}$ est inconsistante ssi pour *toute formule* ϕ, $\mathcal{T} \vDash \phi$.

(d) $\mathcal{F}$ est inconsistante.

Etre inconsistant signifie ne pas avoir de modèle. Si une théorie a pour conséquence une contradiction, alors elle n'est vraie nulle part, et inversément. $\mathcal{F}$ est la plus grande théorie possible, elle contient chaque formule et sa négation, elle est donc évidemment inconsistante.

(3) (a) $\mathcal{T} \models \phi \wedge \psi$ ssi $\mathcal{T} \models \phi$ et $\mathcal{T} \models \psi$.

C'est là une conséquence immédiate de l'interprétation du connecteur "$\wedge$".

(b) En remplaçant dans $\mathcal{T}$ chaque formule par une formule logiquement équivalente, on obtient une théorie équivalente à $\mathcal{T}$.

C'est une conséquence immédiate des définitions. Il n'y a rien d'étonnant à cela puisque la notion d'équivalence repose sur une approche sémantique. En effectuant les substitutions de formules équivalentes, on ne change pas les modèles visés.

(c) $\{\phi_0, \phi_1, \ldots, \phi_k\}$ et $\{\psi_0, \psi_1, \ldots, \psi_n\}$ sont deux théories équivalentes si et seulement si l'équivalence suivante est vérifiée : $(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_k) \equiv (\psi_0 \wedge \psi_1 \wedge \ldots \wedge \psi_n)$.

(4) $\mathcal{T} \models \phi$ ssi $\mathcal{T} \cup \{\neg\phi\}$ est inconsistante.

Il nous faut montrer les deux sens du "si et seulement si". Montrons tout d'abord que si $\mathcal{T} \models \phi$ alors $\mathcal{T} \cup \{\neg\phi\}$ est inconsistante. Dire que ϕ est conséquence sémantique de $\mathcal{T}$, c'est dire que ϕ est vraie dans tous les modèles de $\mathcal{T}$. Donc $\neg\phi$ est fausse dans tous les modèles de $\mathcal{T}$. Ainsi, si l'on considère un modèle quelconque, soit c'est un modèle qui ne satisfait pas $\mathcal{T}$, donc a fortiori ne satisfait pas $\mathcal{T} \cup \{\neg\phi\}$, soit c'est un modèle qui satisfait $\mathcal{T}$, mais alors comme il ne satisfait pas $\neg\phi$, il ne satisfait pas $\mathcal{T} \cup \{\neg\phi\}$.

Montrons maintenant que si $\mathcal{T} \cup \{\neg\phi\}$ est inconsistante alors $\mathcal{T} \models \phi$. Si $\mathcal{T} \cup \{\neg\phi\}$ est inconsistante, alors $\neg\phi$ est fausse dans chaque modèle de $\mathcal{T}$, ce qui signifie que ϕ est vraie dans tous modèles de $\mathcal{T}$ et donc $\mathcal{T} \models \phi$.

(5) $\mathcal{T} \cup \{\phi\} \models \psi$ ssi $\mathcal{T} \models \phi \longrightarrow \psi$.

Montrons les deux sens du si et seulement si. Supposons tout d'abord que ψ est conséquence sémantique de $\mathcal{T} \cup \{\phi\}$, regardons alors les modèles de $\mathcal{T}$. Ils se subdivisent entre ceux dans lesquels ϕ est vraie et ceux où ϕ est fausse. Lorsque ϕ est vraie ψ est également vraie puisque ψ est conséquence sémantique de $\mathcal{T} \cup \{\phi\}$. Par conséquent dans ce cas là, $(\phi \longrightarrow \psi)$ est vraie. Dans l'autre cas, lorsque ϕ est fausse, $(\phi \longrightarrow \psi)$ est vraie par définition de l'implication. Donc dans les deux cas $(\phi \longrightarrow \psi)$ est vraie, ce qui est le résultat que nous cherchions à montrer.

Inversement, supposons que $(\phi \longrightarrow \psi)$ soit conséquence de $\mathcal{T}$. Considérons les seuls modèles de $\mathcal{T} \cup \{\phi\}$. Dans ceux-ci, ψ est nécessairement vraie puisque $(\phi \longrightarrow \psi)$ est vraie dans tous les modèles de ϕ. Donc ψ est conséquence de $\mathcal{T} \cup \{\phi\}$.

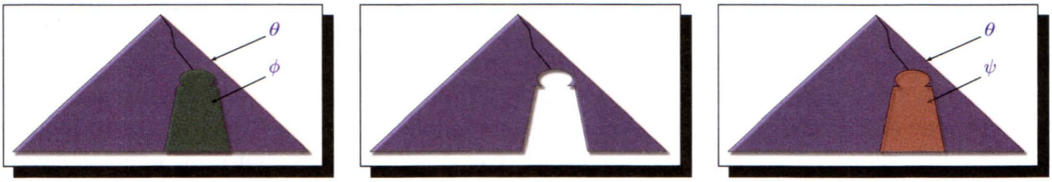
La bonne manière de regarder ce résultat est la suivante. La théorie $\mathcal{T}$ représente l'ensemble des hypothèses dans lesquelles on se place et dont on souhaite déterminer les conséquences. Ainsi, ce résultat nous dit qu'ajouter ϕ à nos hypothèses pour obtenir ψ comme conséquence, c'est la même chose que d'avoir pour conséquence à nos hypothèses $(\phi \longrightarrow \psi)$. Autrement dit, déduire $(\phi \longrightarrow \psi)$ de nos hypothèses $\mathcal{T}$, c'est la même chose que déduire ψ en faisant l'hypothèse supplémentaire qu'on a ϕ.

6 Substitutions de sous-formules équivalentes

***Résumé* № 10** *A l'intérieur d'une formule, substituer une sous-formule par une formule équivalente produit une formule équivalente à l'originale. Pour chaque formule $\phi \in \mathcal{F}$, il existe deux formules qui lui sont équivalentes :*
- *une formule $\phi_{\neg,\vee}$ dont tous les connecteurs logiques sont parmi $\{\neg, \vee\}$,*
- *une formule $\phi_{\neg,\wedge}$ dont tous les connecteurs logiques sont parmi $\{\neg, \wedge\}$.*

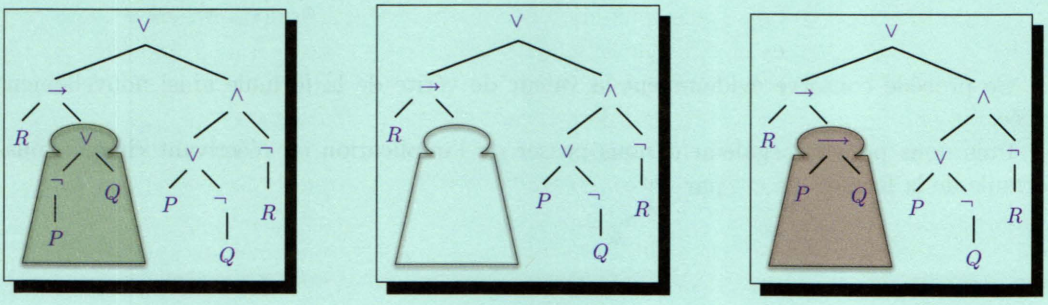
※

Une des choses qu'on aimerait pouvoir faire avec une formule, c'est la simplifier. Cela veut dire trouver une formule qui lui soit équivalente mais dont la lecture et l'intelligibilité soient plus aisées. Une autre chose serait, lorsqu'on souhaite pouvoir comparer deux formules, de trouver un jeu de réécriture qui rapproche ces deux formules et facilite ainsi le travail de comparaison. Cette idée de réécriture est toute entière contenue dans la notion de substitution. Substituer dans une formule une sous-formule par une autre formule consiste à effectuer l'opération décrite dans les trois figures suivantes.



On arrache la sous-formule ϕ de la formule θ, pour la remplacer par ψ. Lorsqu'on arrache ϕ de θ, la racine de ϕ laisse un trou : la terminaison vide d'une branche. C'est sur le bout vide de cette branche que vient se fixer la racine de la formule ψ. Cette opération ressemble finalement à la taille d'un arbre pour venir ensuite en quelque sorte y fixer un greffon.

Exemple 63 Substitution de $P \longrightarrow Q$ à $\neg P \vee Q$:



Proposition 64 *Soient θ, ϕ, ψ trois formules du Calcul Propositionnel, si ϕ est une sous-formule de θ et $\psi \equiv \phi$ alors la formule θ' obtenue en substituant ψ à ϕ dans θ vérifie $\theta' \equiv \theta$.*

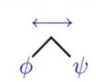
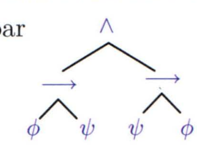
Preuve de la Proposition 64 : Montrer que θ' et θ sont équivalentes consiste à prendre un modèle quelconque $\mathcal{M}$ et prouver que les formules prennent toutes deux la même valeur dans ce modèle. Attachons-nous au coloriage de la formule θ engendré par le modèle $\mathcal{M}$. Ce procédé de coloriage procède des feuilles vers la racine.

Nous allons nous intéresser à la fois au coloriage de ϕ et à celui de θ. Le coloriage de ϕ termine à la racine de ϕ qui est soit verte soit rouge. Considérons maintenant la formule θ à laquelle nous arrachons la sous-formule ϕ pour lui substituer un simple nœud c (c n'étant pas le nom d'une variable propositionnelle). Ce nœud c est maintenant une feuille de cet arbre nouveau. Colorions cette feuille en vert si la racine de ϕ est verte, et en rouge si la racine de ϕ est rouge. Et colorions toutes les autres feuilles de cet arbre (qui sont des variables propositionnelles) conformément au modèle $\mathcal{M}$. Appliquons ensuite l'algorithme de coloriage à cet arbre. De quelle couleur sera sa racine ? Il est tout à fait évident qu'elle aura exactement la même couleur que la racine de la formule θ évaluée par l'algorithme de coloriage dans le modèle $\mathcal{M}$.

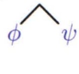
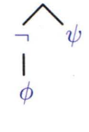
Maintenant, si nous venons fixer à la place de ce nœud c l'arbre de la formule ψ toute entière pour obtenir la formule θ', puis que nous évaluons θ' dans $\mathcal{M}$ au moyen de l'algorithme de coloriage, nous remarquons que la couleur de la racine de ψ sera exactement la même que celle de c puisque ψ et ϕ sont équivalentes. Les feuilles qui sont communes à θ et θ' – c'est-à-dire celles qui concernent θ privée de ψ – sont coloriées de la même manière dans θ' et dans θ, il s'en suit de ces différentes considérations que la racine de θ et celle de θ' obtiennent une couleur identique à la fin du processus de coloriage. Elles sont donc toutes les deux vraies ou toutes les deux fausses dans ce modèle $\mathcal{M}$.

Puisque nous avons procédé avec un modèle $\mathcal{M}$ quelconque, notre conclusion ne dépend pas du modèle. Elle est donc vraie quel que soit le modèle. En conséquence, aucun modèle ne permet de séparer les deux formules θ et θ'. Ces deux formules sont donc équivalentes.

$\dashv$ 64

Puisque la substitution d'une sous-formule par une formule équivalente ne change pas la formule initiale du point de vue sémantique, nous pouvons procéder à différentes opérations de simplification afin de réduire le nombre des types de connecteurs en jeu dans une formule. Tout d'abord, nous pouvons nous passer de la double implication et réécrire toute formule en remplaçant chaque sous-formule de la forme  par 

Ce procédé conserve évidemment la valeur de vérité de la formule ainsi nouvellement créée.

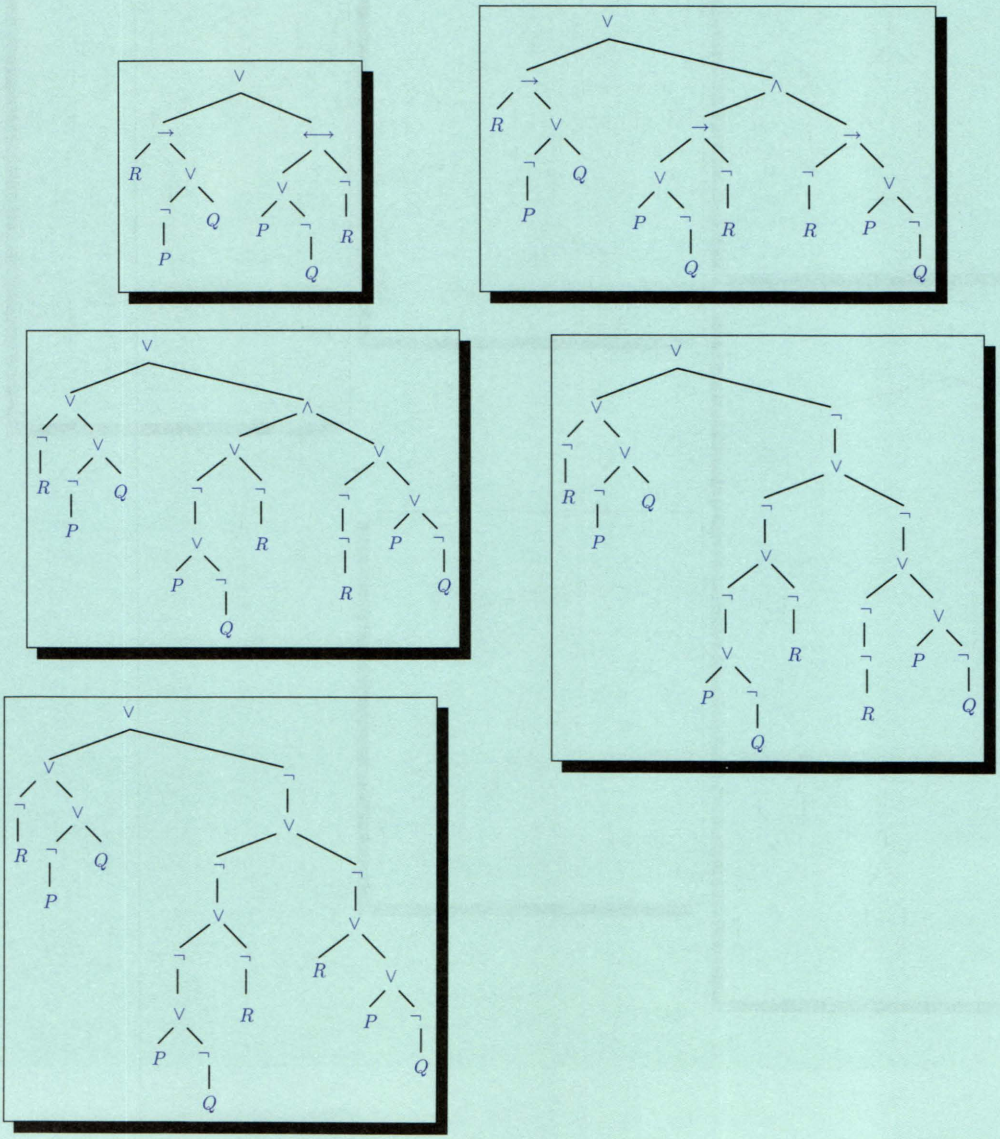
Puis nous pouvons également nous passer de l'implication en réécrivant chaque sous-formule de la forme  par 

Dès lors, nous pouvons pour toute formule θ construire une formule θ' qui lui soit équivalente mais ne comporte ni symbole d'implication, ni symbole de double implication. Est-ce que nous pouvons aller plus loin ? La réponse est oui, et ce de deux manières différentes en utilisant les deux équivalences qui suivent :

Rien de tel qu'un petit exemple pour voir fonctionner ces transformations. Nous allons, dans un premier temps, transformer une formule en une formule équivalente dont les seuls connecteurs sont parmi $\{\neg, \vee\}$.

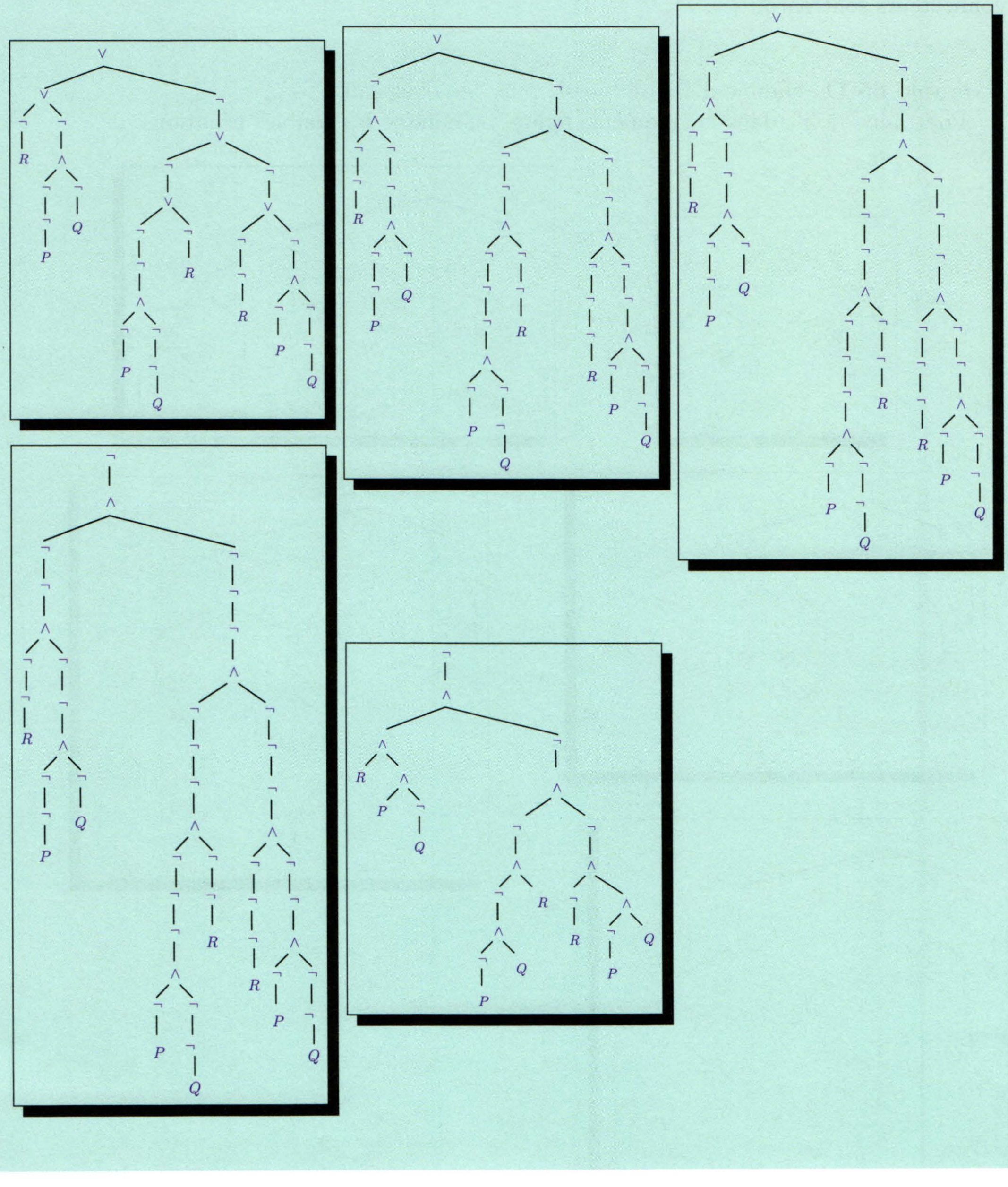
Exemple 65 On élimine d'abord "$\longleftrightarrow$", puis "$\longrightarrow$" et enfin "$\wedge$".

Pour faire "joli", dans la cinquième figure, on élimine les doubles négations.



Dans un deuxième temps nous transformons la formule de l'exemple précédent en une formule équivalente dont les seuls connecteurs sont parmi $\{\neg, \wedge\}$. Pour cela nous repartons de l'étape dans laquelle notre formule originale ne comportait que des connecteurs parmi $\{\neg, \vee, \wedge\}$ et nous éliminons la disjonction étape par étape pour faciliter la compréhension.

Exemple 66 On élimine "$\vee$" des feuilles vers la racine, puis les doubles négations.



Ce que nous venons de montrer s'énonce dans la proposition qui suit.

Proposition 67 *Pour toute formule* $\varphi \in \mathcal{F}$*, il existe :*

(1) une formule $\phi_{\neg,\vee,\wedge} \equiv \varphi$ *avec tous ses connecteurs logiques dans* $\{\neg, \vee, \wedge\}$,

(2) une formule $\phi_{\neg,\vee} \equiv \varphi$ *avec tous ses connecteurs logiques dans* $\{\neg, \vee\}$,

(3) une formule $\phi_{\neg,\wedge} \equiv \varphi$ *avec tous ses connecteurs logiques dans* $\{\neg, \wedge\}$.

Preuve de la Proposition 67 : effectuée immédiatement avant l'énoncé de la Proposition.

$\dashv$ 67

Cette proposition sera très utile pour la section qui suit. Nous allons en effet tirer profit du fait que toute formule du Calcul Propositionnel est équivalente à une formule ne comportant que les deux seuls connecteurs binaires $\wedge$ et $\vee$ ainsi que la négation ($\neg$).

7 Jeux d'évaluation

***Résumé* № 11** *L'évaluation d'une formule ϕ,à l'intérieur d'un modèle $\mathcal{M}$ est présentée comme la résolution d'un jeu : $\mathbb{E}v\,(\mathcal{M}, \phi)$. Ce jeu comporte deux joueurs – le* **V**érificateur *et le* **F**alsificateur *– qui opèrent des choix de bifurcation sur l'arbre de la formule ϕ. Un partie consiste en un chemin de la racine vers une feuille. Elle est gagnée par le* **V**érificateur *si cette feuille correspond à une variable propositionnelle vraie dans $\mathcal{M}$, elle est gagnée par son adversaire sinon.*
$\mathcal{M} \models \phi$ si et seulement si le **V**érificateur *possède une stratégie gagnante dans le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$.*

※

7.1 Jeux finis à deux joueurs et à information parfaite

L'évaluation d'une formule dans un modèle peut être regardée comme un jeu fini à deux joueurs, l'un cherchant à montrer la véracité de la formule, l'autre au contraire tentant d'établir sa fausseté. Pour les jeux auxquels on s'intéresse ici, il faut que soient présents trois ingrédients qui sont comme les trois piliers sur lesquels repose cette notion :

Définition 68 *Jeu := 3 ingrédients :*

(1) ***Joueurs*** *: ce sont les éléments interactifs qui participent au jeu. On leur donne différents noms dans la littérature : Joueur et Opposant, Adam et Eve, Abélard et Eloïse, Il et Elle, I et II,* **0** *et* **1**. *Leurs actions sont appelées des coups du jeu.*

(2) ***Règles du jeu*** *: ce sont elles qui déterminent* lequel *des joueurs peut jouer,* quel coup, *à* quel moment. *Elles spécifient la* forme *du jeu.*

(3) ***Conditions de gain*** *: elles décident* qui *remporte* quoi *à la fin de la partie.*

Les jeux qui nous préoccupent pour l'évaluation des formules sont des jeux :

- *à deux joueurs* (dès qu'il y a plus de deux joueurs, des problèmes de coalition apparaissent).
- *sans chance* : il n'y a pas de dés lancés, pas de cartes tirées au sort, ...
- à *information parfaite* : il n'y a pas de coups simultanés et tous les joueurs ont, à tout instant, une connaissance pleine et entière de tout le déroulement de la partie, de toutes les configurations du jeu. Exactement comme aux échecs, par opposition à la bataille navale par exemple, où un joueur ne connaît pas toute la configuration de la partie puisqu'il n'a pas connaissance des positions des bateaux de son adversaire.
- *à condition de gain de type 0-1* : un joueur gagne et l'autre perd, il n'y a pas de match nul. A la fin de la partie, un joueur l'emporte, son adversaire est vaincu.
- *finis* : la partie s'arrête après un nombre fini de coups joués.

Pour toute la suite de cette section consacrée aux jeux, nous ne considérerons plus que les seuls jeux de cette forme.

7.2 Un exemple : le jeu de Nim

Dans le film *L'année dernière à Marienbad*[11], un personnage prénommé M persuade de manière répétée un autre personnage appelé X, de jouer à un jeu simple. Il arrange les cartes sur une table en une forme triangulaire :

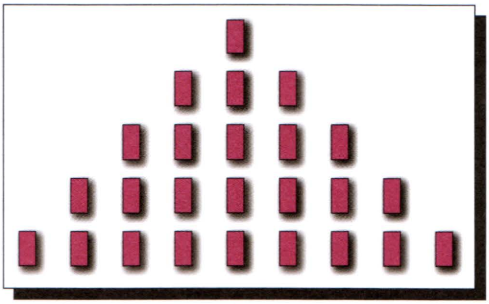


FIGURE 2.1 – Configuration initiale du jeu de Marienbad.

Les joueurs jouent à tour de rôle, prélevant chacun autant de carte qu'ils le souhaitent mais d'une seule ligne à chaque fois. Cela continue ainsi jusqu'à ce qu'un des joueurs prenne la dernière carte et perde.

Dans le film, poliment, M laisse toujours X débuter la partie. Malheureusement, X perd à chaque fois.

Ce jeu est une des nombreuses versions du *jeu de Nim*, l'un des plus anciens des jeux mathématiques à deux joueurs que l'on connaisse aujourd'hui. Le mot *Nim* remonte à l'allemand *nehmen* (prendre). Le nom ainsi que la théorie complète de ce jeu sont dûs à Charles L. Bouton (Harvard)[12] il y a plus d'un siècle.

11. Dir. A. Resnais, sc. Alain Robbe-Grillet – 1961.

12. Nous considérons la version du *jeu de Nim* dans laquelle les joueurs (I et II) prélèvent à tour de rôle des allumettes disposées en tas. Le joueur I débute, celui des deux joueurs qui prend la dernière allumette gagne la partie.

Par convention, nous appelons *configuration perdante* une configuration telle que si un quelconque *joueur* (I ou II) se trouve, à un moment donné de la partie, en charge d'une telle configuration et que c'est à lui de jouer, alors quoi qu'il fasse, son adversaire peut toujours jouer de manière à le battre. Toute autre configuration s'appelle *configuration gagnante*. Une configuration est donc gagnante lorsque le joueur qui se trouve en charge d'une telle configuration possède une stratégie gagnante. Par exemple, la configuration $(2,2)$ est perdante car il suffit à l'adversaire d'enlever 2 allumettes au cas où le premier joueur en enlève deux, et d'en enlever une au cas où le premier joueur n'en enlève qu'une seule. Dans ce dernier cas, le deuxième tour de la partie fait enlever par le premier joueur une allumette dans un des tas, auquel son adversaire répond en enlevant la dernière.

Nous définissons maintenant une *configuration correcte* :

(1) Tout d'abord, nous exprimons en binaire le nombre d'allumettes dans chaque colonne. Par exemple, la configuration $(3,9)$ donne $(11,1001)$.

(2) Ensuite, nous écrivons ces nombres les uns en dessous des autres,

(3) et finalement, nous additionnons un à un les chiffres se trouvant dans chaque colonne.

Ainsi, la configuration $(2,3,6,7)$ donne lieu à :

$$\begin{array}{ccc} & 1 & 0 \\ & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ \hline \\ 2 & 4 & 2 \end{array}$$

Dans la version la plus générale de ce jeu, les joueurs jouent à tour de rôle en enlevant des objets (jetons, cailloux, pièces de monnaies, morceaux de papier,...) de tas (piles, rangées, boîtes), mais uniquement d'un seul tas à la fois. Il y a deux variantes à ce jeu, suivant celui des 2 joueurs qui est déclaré vainqueur à la fin de la partie :

- dans la version *normale*, le joueur prenant le dernier objet remporte le gain de la partie ;
- dans la version *misere*, le joueur prélevant le dernier objet perd.

La configuration est *correcte* si la somme de chaque colonne est *paire*, dans tous les autres cas, la configuration est dite *incorrecte.*

Théorème 69 *Une configuration du jeu de* Nim *est perdante si et seulement si elle est correcte.*

Preuve du Théorème 69 :

(1) Considérons tout d'abord le cas spécial dans lequel chaque tas ne contient qu'une seule allumette. Il est immédiat de voir qu'une telle configuration est perdante si et seulement si le nombre d'allumette est pair, autrement dit, s'il s'agit d'une configuration correcte.

(2) Ensuite, si un joueur prend d'une configuration correcte, alors il remplace nécessairement le nombre d'allumette d'un des tas par un nombre plus petit. Par conséquent, dans le calcul tel que décrit ci-dessus, une et une seule des lignes est modifiée : le nombre en binaire qui y est indiqué étant remplacé par un plus petit. Cela a pour effet qu'au moins un des 1 est remplacé par un 0, entraînant du même coup le caractère incorrecte de la configuration ainsi obtenue.

(3) Si une configuration est incorrecte, en considérant la colonne dont la somme impaire est la plus à gauche, et l'une des lignes qui possède un 1 dans cette même colonne, il est alors possible en ne prélevant que dans le tas correspondant à cette ligne de restaurer la rectitude de cette configuration. Pour fixer les idées, imaginons que le configuration soit du type $(pair, pair, impaire, pair, impaire, pair)$, en sorte que c'est à la troisième colonne la plus à gauche que nous nous intéressons. Il y a nécessairement un 1 dans cette colonne. Supposons, toujours pour fixer les idées, qu'une des lignes possédant un 1 dans cette colonne soit : 011101. Alors en remplaçant ce nombre par le nombre 010111 (qui est effectivement plus petit), nous restaurons la rectitude de la configuration. La solution consiste donc à prélever exactement

$$\begin{array}{cccccccc} & 0 & 1 & 1 & 1 & 0 & 1 & \\ - & 0 & 1 & 0 & 1 & 1 & 1 & \\ \hline & 0 & 0 & 0 & 1 & 1 & 0 & = 6 \end{array}$$

allumettes de ce tas.

Cela prouve qu'un joueur à qui l'on présente une configuration incorrecte peut toujours jouer de manière à rendre à son adversaire une configuration correcte.

(4) Finalement, si un joueur transmet une configuration correcte, son adversaire se retrouve contraint et forcé de la transformer en une configuration incorrecte. Le premier joueur peut alors jouer en sorte de rendre à nouveau cette configuration correcte. Ce processus continue jusqu'à ce que chaque tas soit vidé, ou bien ne contienne qu'une seule allumette. Le théorème est ainsi réduit au cas (1) qui est d'ores et déjà démontré.

$\dashv$ 69

Ce théorème prouve deux choses :

(1) si la configuration originale est incorrecte, alors le premier joueur possède une stratégie gagnante,

(2) si la configuration originale est correcte, alors c'est le joueur qui joue en deuxième qui cette fois possède une stratégie gagnante.

En conséquence de quoi :

(1) il prouve que ce jeu est *déterminé,*

(2) il indique lequel des deux *joueurs* possède une stratégie gagnante,

(3) il exhibe une telle *stratégie gagnante.*

Représenté sous *forme extensive*, ce jeu prend l'allure d'un *arbre*, dont les branches sont les parties possibles selon les règles du jeu. C'est l'*arbre* de toutes les suites possibles de coups *légaux*, c'est-à-dire l'arbre de toutes les suites autorisées de configurations. On appelle *position*, une suite légale de configuration.

Prenons le cas du jeu de Marienbad avec seulement deux lignes. C'est bien sûr un exemple trop simple pour être réellement intéressant. Mais l'arbre de ce jeu, c'est-à-dire ce jeu présenté sous forme extensive, est déjà suffisamment compliqué.

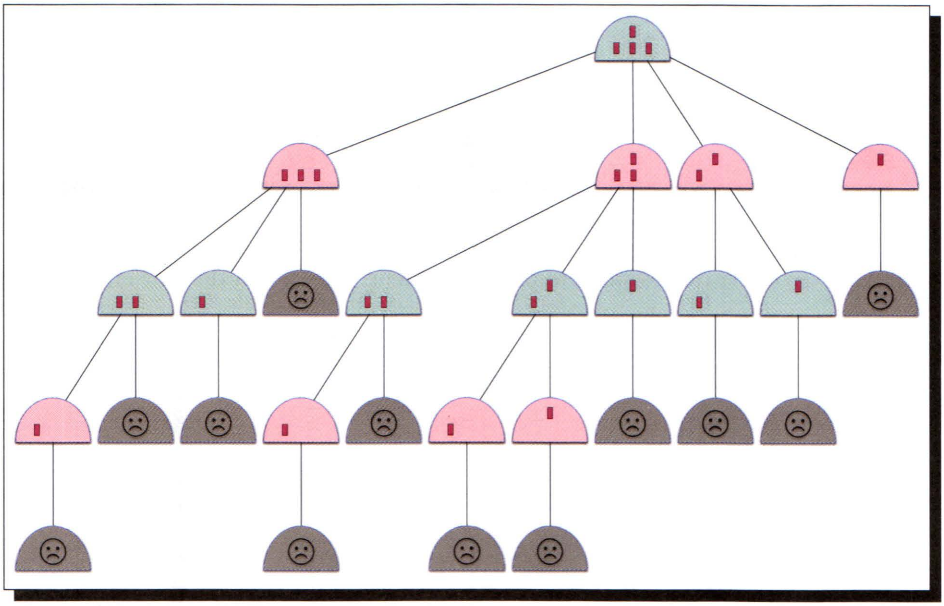


FIGURE 2.2 – Arbre pour le jeu de Marienbad avec 2 lignes.

A l'intérieur de tout nœud, chaque petit rectangle de couleur rouge représente une carte. Chacun des nœud représente une configuration du jeu puisqu'il indique :

- le nombre de cartes présentes sur chaque ligne,
- le joueur à qui il appartient de jouer : les nœuds bleus sont des positions pour le joueur qui débute la partie, les nœuds rouges sont des positions pour son adversaire, enfin les nœuds gris correspondent à des positions terminales du jeu, lorsqu'il ne reste plus de carte à retirer et que la partie s'arrête.

Finalement, les fils d'un nœud donné représentent toutes les configurations possibles atteignables en un coup conformément aux règles, c'est-à-dire, toutes les configurations légales. On doit également indiquer les conditions de gain qui se trouvent être dans notre cas : le joueur qui aura joué le dernier coup de la partie sera déclaré perdant.

Si nous avons l'arbre de jeu sous les yeux, il apparait qu'une *stratégie* n'est pas autre chose qu'un sous-arbre de cet arbre de jeu : un sous-arbre ayant, bien évidemment, la même racine que l'arbre de jeu. C'est donc en quelque sorte un sous-jeu, c'est-à-dire un jeu dans lequel le joueur en question s'est imposé volontairement des restrictions : chaque fois que c'est à son tour de jouer, il ne s'autorise qu'un seul coup possible, il n'a plus d'autre choix que celui-ci. Par contre, lorsque c'est à son adversaire de jouer, celui-ci conserve l'entière liberté de mouvement qu'il avait dans le jeu au complet.

Regardons maintenant quelques exemples de stratégies pour chacun des joueurs.

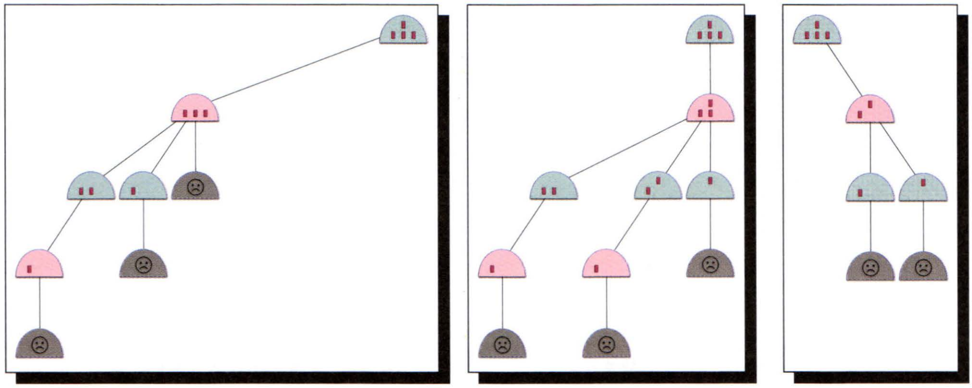


Figure 2.3 – Trois stratégies pour le premier joueur dans le jeu de Marienbad-2 lignes.

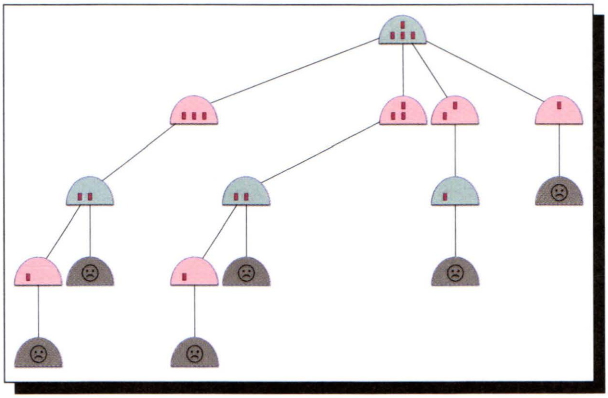


Figure 2.4 – Une stratégie pour le second joueur dans le jeu de Marienbad-2 lignes.

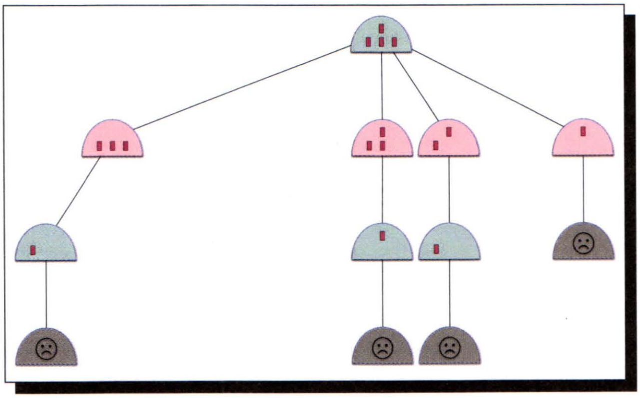


Figure 2.5 – Une stratégie pour le second joueur dans le jeu de Marienbad-2 lignes.

On remarquera que dans la figure 2.3, aucune des trois stratégies proposées n'est une stratégie gagnante pour le joueur qui débute la partie, puisque dans chacune d'entre elles le second joueur peut prendre toutes les cartes de la table à l'exception d'une seule, laissant ainsi la main à son adversaire qui perdra aussitôt.

Il en va de même dans les figures 2.4 et 2.5, puisqu'aucune de ces deux stratégies pour le second joueur ne lui permette d'emporter la partie. En effet, pour chacune d'entre elle, le premier joueur peut choisir au premier coup d'ôter de la table la rangée de trois cartes, laissant alors à son adversaire la seule dernière carte à retirer.

On voit aisément que le premier joueur possède une stratégie gagnante – qui par ailleurs est unique – qui consiste à prendre les trois cartes de la rangée du bas. Cette stratégie est présentée dans la figure 2.6.

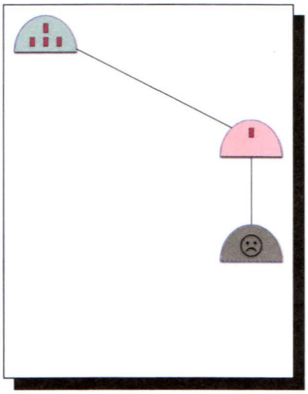


FIGURE 2.6 – Une stratégie gagnante pour le premier joueur dans le jeu de Marienbad-2 lignes.

On remarque également que si les deux joueurs appliquent une stratégie, alors le jeu se déroule de manière univoque, il n'y a jamais de choix fait par aucun des deux joueurs. Cela définit donc une unique *partie*, c'est-à-dire une unique branche de l'arbre. Par exemple, si le premier joueur applique la seconde stratégie de la figure 2.3 alors que le second joueur applique celle de la figure 2.4, on obtient la partie présentée dans la figure 2.7.

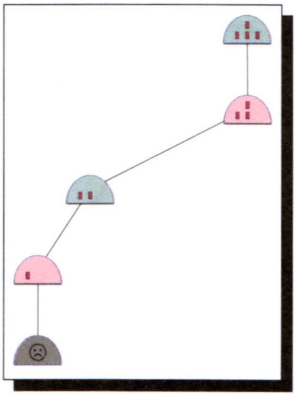


FIGURE 2.7 – Une partie dans le jeu de Marienbad-2 lignes.

7.3 Jeu sous forme extensive, parties, stratégies et stratégies gagnantes

La représentation d'un jeu sous forme extensive est un arbre dont les nœuds sont des configurations du jeu (voir fig. 2.8).

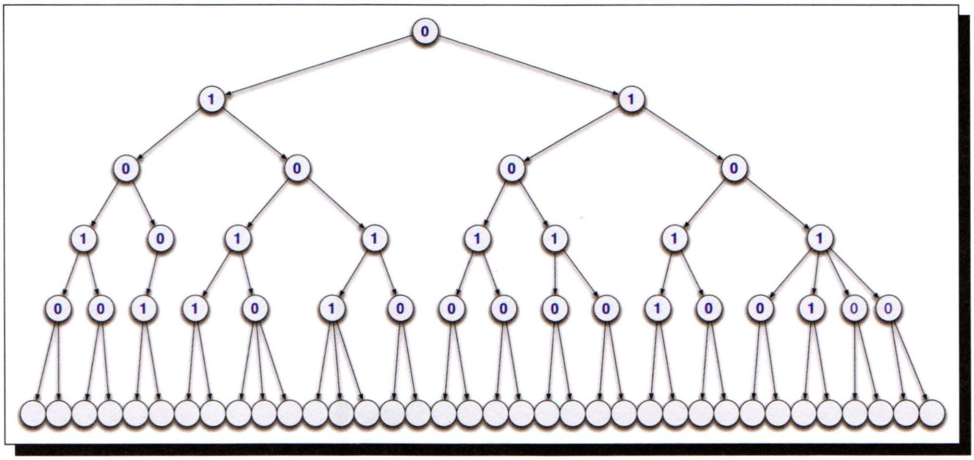


FIGURE 2.8 – Un jeu sous forme extensive.

La racine de l'arbre est la configuration initale de la partie. Chaque nœud est associé au joueur dont c'est au tour de jouer ; les fils d'un nœud sont toutes les configurations possibles que le joueur, auquel ce nœud est associé, peut atteindre en un coup en respectant bien sûr les règles du jeu.

Nous appelons *partie* une branche maximale de l'arbre (de la racine jusqu'à une feuille, voir figs 2.9 et 2.10). Dès lors, une *position* au cours d'une partie est une branche de l'arbre (pas nécessairement maximale !). Une position est donc donnée par un nœud de l'arbre ainsi que tous les parents de ce nœud. Cette branche indique quel a été le cheminement de la partie depuis le début jusqu'à la configuration dans laquelle on se trouve (voir fig. 2.10).

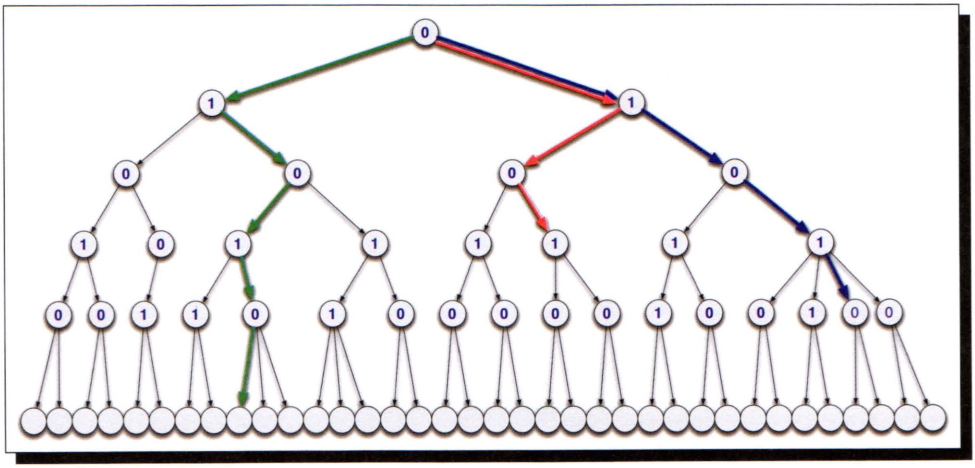


FIGURE 2.9 – Une partie, une position pour **0**, une position pour **1**.

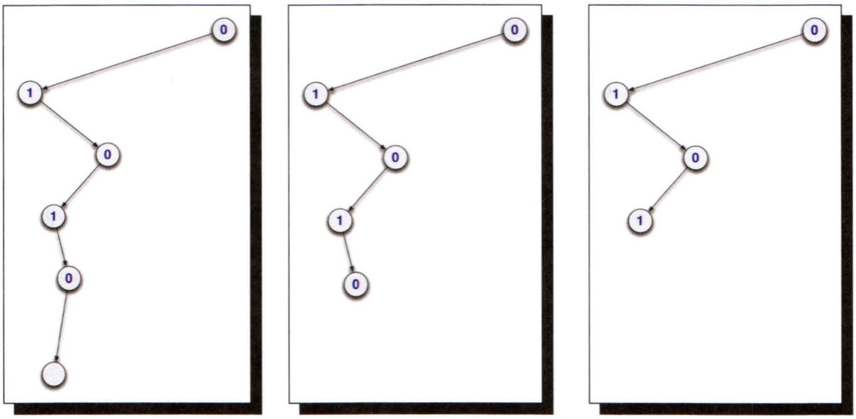


FIGURE 2.10 – Une partie, une position pour **0** dans cette partie, ainsi qu'une position pour **1**.

Exemple 70 Prenons l'exemple du jeu d'échecs (pour éviter le problème des parties nulles, convenons que les blancs l'emportent en cas de match nul) :

- une *configuration* d'une partie d'échecs est simplement composée de deux choses :
  (1) la place exacte de chacune des pièces sur l'échiquier,
  (2) le joueur qui doit maintenant jouer.
- *l'arbre de jeu* est caractérisé par le fait :
  (1) qu'il a pour racine la configuration initiale de ce jeu : celle dans laquelle les pièces sont disposées au début de la partie, avec, en plus, l'information que c'est au tour du joueur en charge des blancs de jouer.
  (2) les successeurs d'une configuration (les fils ou filles du nœud) sont toutes les configurations que le joueur qui doit maintenant jouer, peut atteindre en un coup. Elles correspondent à tous les coups possibles pour ce joueur à partir de cette configuration. Et ces successeurs sont, bien sûr, des configurations pour l'adversaire.
  (3) Les feuilles de l'arbre (les nœuds de l'arbre sans descendant) sont les configurations finales : configurations dans lesquelles la partie s'arrête.
- une *position* du jeu constitue la donnée de tout le déroulement de la partie jusqu'à la configuration dans laquelle on se trouve.
- une *partie* constitue une position maximale du jeu, autrement dit une position dont la configuration associée n'est autre qu'une feuille de l'arbre, c'est-à-dire une configuration finale.

Définition 71 *Soit T un arbre représentant un jeu sous forme extensive. On appelle* **0** *et* **1** *les deux joueurs. Une* stratégie σ *pour un joueur $i \in \{0,1\}$ est* un sous-arbre de T *qui vérifie les conditions suivantes :*

- *la racine de σ est la même que celle de T,*
- *chaque nœud de σ qui est une position pour le joueur i n'a qu'un seul successeur,*
- *chaque nœud de σ qui est une position pour le joueur $1-i$ a exactement les mêmes successeurs que dans T.*

Intuitivement une stratégie pour un joueur est donc un sous-jeu dans lequel ce joueur, à chaque fois qu'il doit jouer, restreint ses coups possibles à un seul ; tandis que lorsque c'est au tour de son adversaire de jouer, entière mobilité lui est laissée.

On dit qu'un joueur *applique la stratégie* σ si toute la partie se déroule dans le sous-arbre σ.

Dans la figure 2.11 les flèches pointillées représentent les flèches qui ne peuvent pas être parcourues par aucun des deux joueurs lorsque le joueur **0** applique la stratégie σ telle que représentée dans le second dessin. La figure 2.12 représente la même idée, mais cette fois-ci pour une stratégie $\mathcal{T}$ pour le joueur **1**, qui est représentée également dans le second dessin.

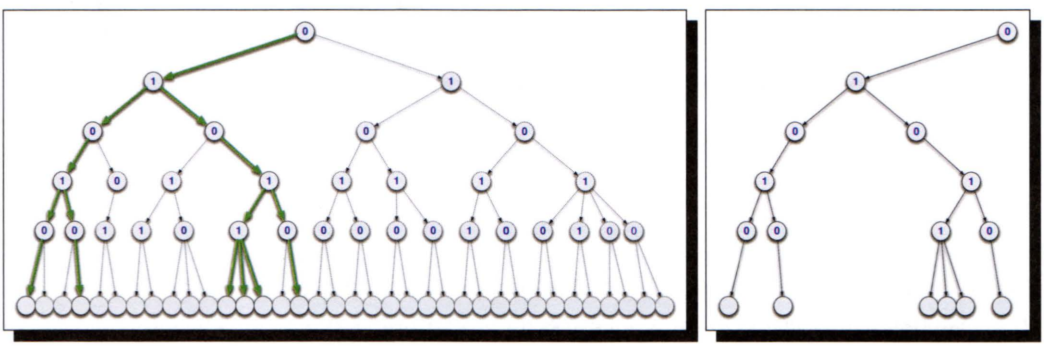


FIGURE 2.11 – Une stratégie σ pour **0**.

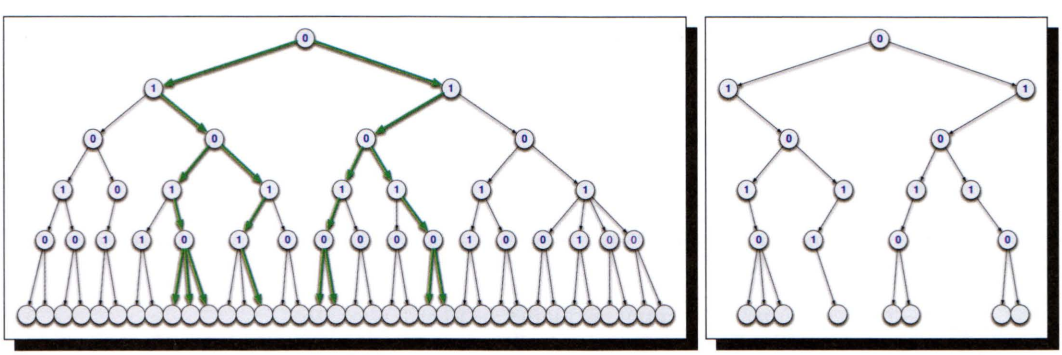


FIGURE 2.12 – Une stratégie $\mathcal{T}$ pour **1**.

Définition 72 *Soit T un arbre représentant un jeu sous forme extensive et σ une stratégie pour le joueur $i \in \{0, 1\}$:*

σ est une stratégie gagnante ssi toutes les configurations finales de σ sont gagnantes pour i.

Autrement dit, σ est une stratégie gagnante pour le joueur i si ce même joueur, appliquant scrupuleusement la stratégie σ, remporte toutes les parties, quoique fasse son adversaire.

Dans la figure 2.13, un arbre de jeu dont les conditions de gains pour le joueur **0** et pour le joueur **1** sont indiquées par les couleurs des configurations finales (nous convenons que les configurations vertes sont gagnantes pour **0**, alors que les configurations rouges sont gagnantes pour **1**). Dans la figure 2.14, nous donnons une stratégie pour le joueur **1** qui n'est pas gagnante – on remarquera que certaines feuilles sont de couleur verte. Dans la figure 2.14, nous donnons une stratégie gagnante pour le joueur **1** – on remarquera que cette fois-ci toutes les feuilles sont de couleur rouge.

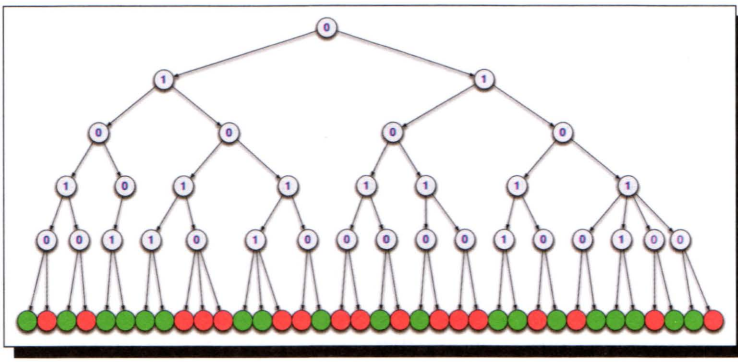


FIGURE 2.13 – Un jeu avec conditions de gain vertes pour le joueur **0** et rouges pour le joueur **1**.

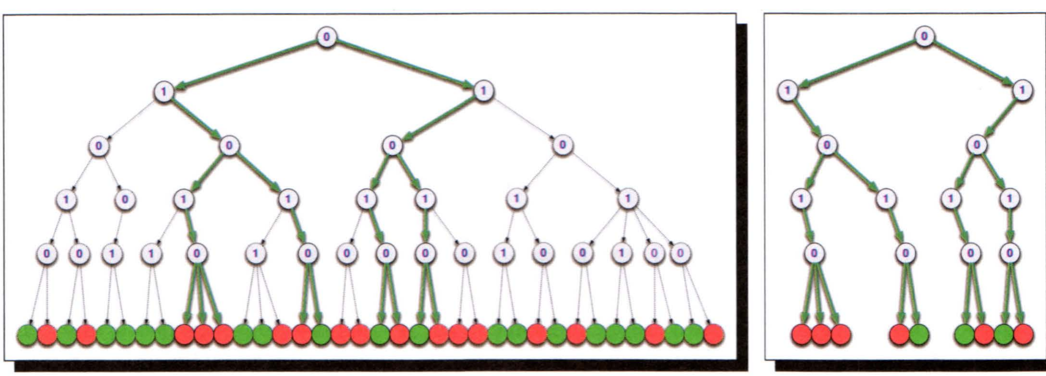


FIGURE 2.14 – Une stratégie pour le joueur **1** qui n'est pas gagnante.

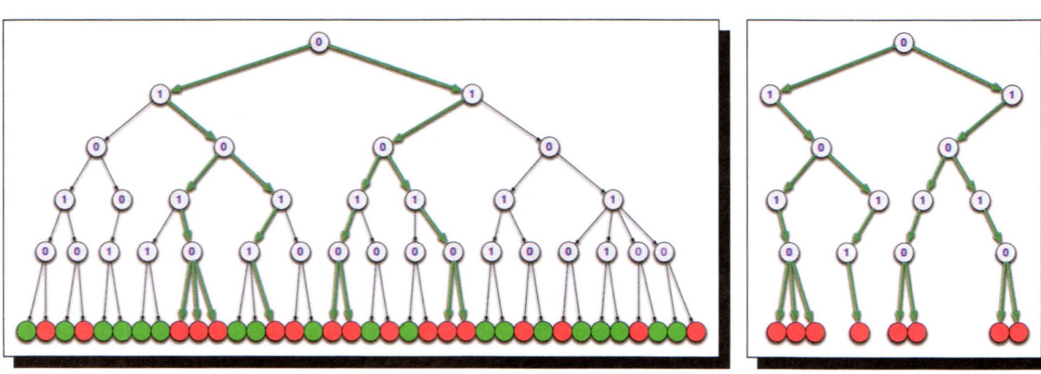


FIGURE 2.15 – Une stratégie gagnante pour le joueur **1**.

7.4 Détermination des jeux finis à deux joueurs et à information parfaite

Une notion essentielle en théorie des jeux consiste à savoir si l'un des joueurs possède une stratégie gagnante. Sans cela, on ne peut pas faire grand chose. Heureusement, les jeux que nous considérons possèdent cette propriété. On dit qu'ils sont *déterminés.*

Définition 73 *Un jeu est* déterminé *si l'un des joueurs possède une stratégie gagnante.*

Remarque 74 Pour les jeux qui nous intéressent, si un tel jeu est déterminé, alors un des deux joueurs possède une stratégie gagnante. Le joueur est donc certain qu'en appliquant cette stratégie, il remportera toutes les parties quoique fasse son adversaire.

Par conséquent les deux joueurs ne peuvent avoir chacun une stratégie gagnante, puisqu'en appliquant tous les deux leurs stratégies gagnantes respectives, ils remporteraient tous les deux la partie. Ce qui contredit le fait que dans ces jeux si l'un gagne, l'autre perd.

Pour ce qui concerne les jeux finis, on dispose, depuis environ un siècle, d'un résultat à la fois très simple et très utile :

Théorème 75 (Zermelo) *Tous les jeux finis à deux joueurs et à information parfaite sont déterminés.*

Ainsi, le jeu d'échecs est déterminé si l'on convient, par exemple, que les joueurs blancs gagnent en cas de match nul. Cela signifie que :

- Soit les noirs ont une stratégie gagnante, c'est-à-dire une stratégie telle qu'ils puissent gagner chaque partie,
- Soit les blancs ont une stratégie pour ne pas perdre, c'est-à-dire une stratégie telle qu'ils remportent chaque partie ou fassent, au pire, match nul.

Pour résumer, on peut dire que soit les blancs soit les noirs possèdent une stratégie pour ne jamais perdre...

Or, si l'on connait ce résultat depuis un siècle, on ne dispose toujours pas d'une telle stratégie. Pire encore : on ne sait toujours pas lequel des deux joueurs possède cette stratégie pour ne pas perdre... La raison de cela se trouve dans la complexité de l'arbre de ce jeu. Si l'on disposait en effet de cet arbre, il serait immédiat, comme nous le verrons dans un instant, de conclure au résultat, mais cet arbre est horriblement compliqué. Il contient un nombre exponentiel de nœuds par rapport au nombre de coups joués. Il est donc totalement impossible de demander à un ordinateur de faire le calcul, tout au moins pour autant qu'on souhaite avoir le résultat avant quelques milliards de milliards d'années.

Preuve du Théorème 75 : On se donne tout d'abord le jeu sous forme extensive, c'est-à-dire sous forme d'arbre de jeu. Nous allons décrire un algorithme, c'est-à-dire un processus de calcul basé sur la répétition d'opérations très simples, qui permet de déterminer, pour chaque sous-arbre induit par un nœud de l'arbre, lequel des deux joueurs possède une stratégie gagnante dans le sous-jeu qui débute à ce nœud.

(1) On commence par colorier en rouge les feuilles (c'est-à-dire les nœuds finaux de l'arbre) qui sont gagnantes pour le joueur **1**. Les autres, qui sont donc gagnantes pour le joueur **0** sont coloriées en vert.

(2) On répète ensuite cette procédure : si tous les successeurs d'un nœud c ont déjà été coloriés, on exécute une des actions suivantes :

(a) si arrivé au nœud c, c'est au tour du joueur **1** de jouer,
- il faut colorier c en rouge si au moins l'un des successeurs est colorié en rouge,
- il faut colorier c en vert si au contraire tous les successeurs de c sont coloriés en vert.

(b) si arrivé au nœud c, c'est au tour du joueur **0** de jouer,
- il faut colorier c en vert si au moins l'un des successeurs est colorié en vert,
- il faut colorier c en rouge si, au contraire, tous les successeurs de c sont coloriés en rouge.

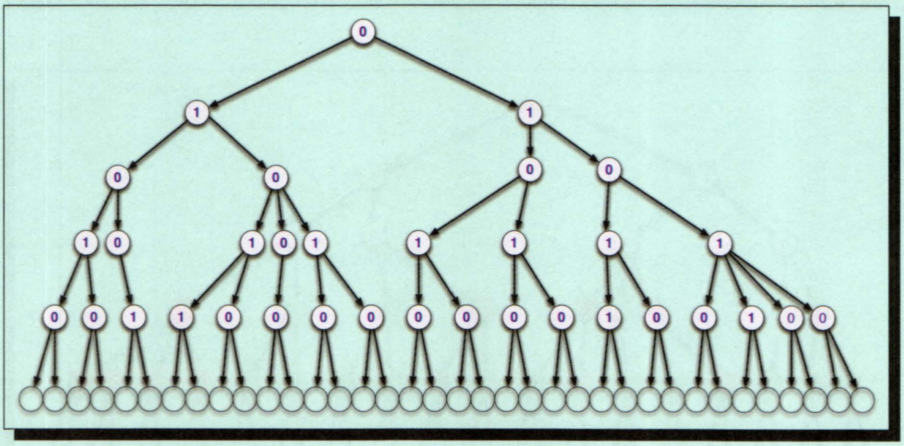
Petit à petit, chacun des nœuds de l'arbre reçoit la couleur verte ou rouge.

Il est facile de voir que ce procédé attribue la couleur verte à chacun des nœuds qui correspond à une position gagnante pour le joueur **0** (c'est-à-dire une position à partir de laquelle ce joueur possède une stratégie gagnante) ; et de manière duale, la couleur rouge est attribuée à chacun des nœuds correspondant à des positions gagnantes pour le joueur **1**.

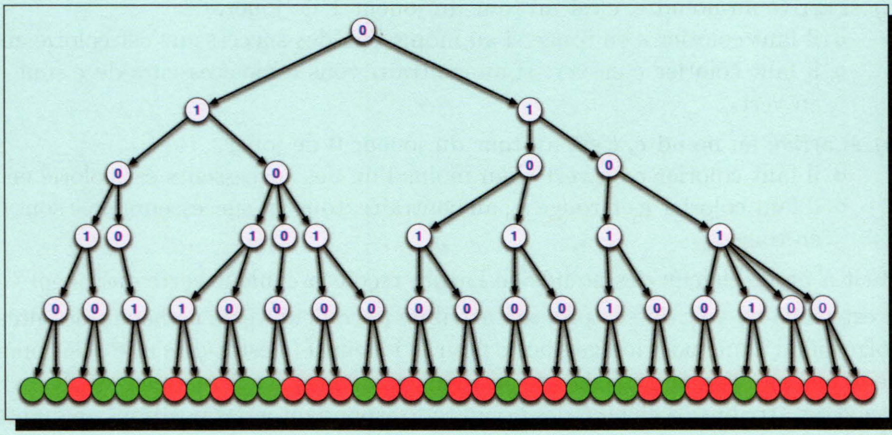
En effet, le joueur **0** possède une stratégie gagnante depuis le nœud c, si et seulement si l'une des trois situations suivantes est vérifiée :
- c est une feuille gagnante pour le joueur **0**,
- c'est au tour de **0** de jouer et il y a un coup possible qui mène directement à un nœud, d'où **0** possède une stratégie gagnante,
- c'est au tour de **1** de jouer, mais tous les coups possibles pour le joueur **1** mènent à des nœuds d'où **0** possède une stratégie gagnante.

⊣ 75

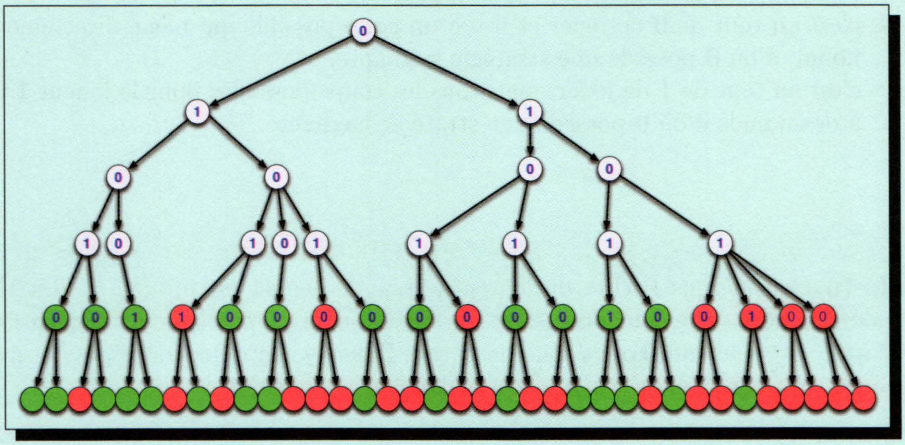
Exemple 76 Considérons l'arbre de jeu suivant, dans lequel est indiqué à l'intérieur de chaque nœud le nom du joueur dont c'est le tour de jouer (à partir de cette position). On voit ainsi que c'est le joueur **0** qui débute la partie. Il peut jouer deux coups possibles comme premier coup, chacun menant à une position dévolue au joueur **1** :

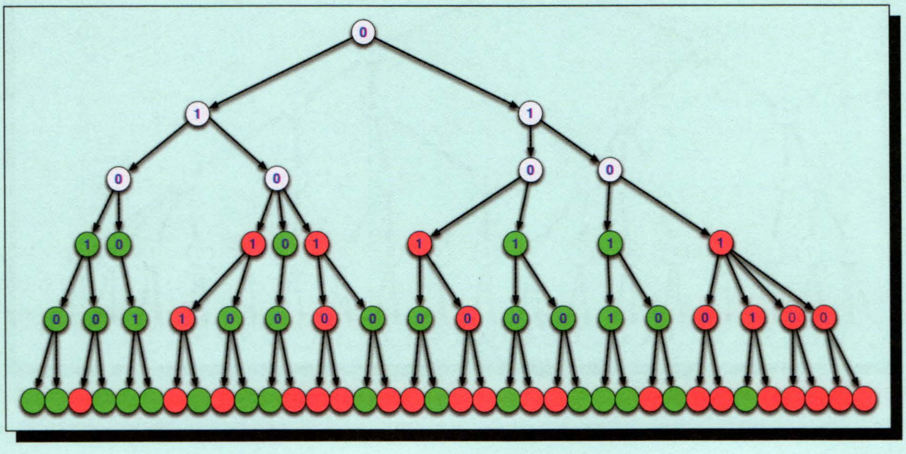


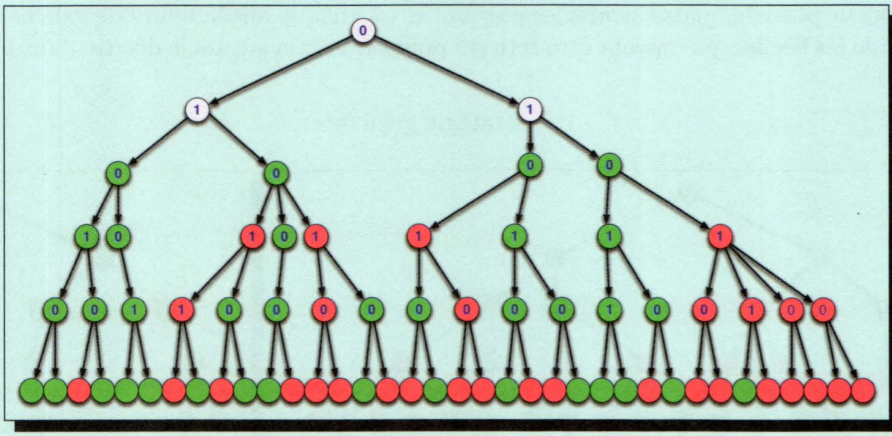
On colorie ensuite les feuilles de l'arbre en fonction du gagnant de la partie :

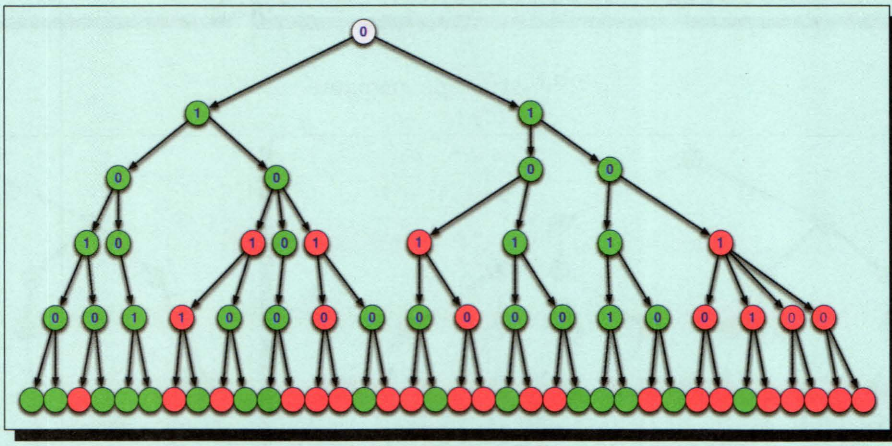


Puis, étage par étage, on remonte des feuilles vers la racine en appliquant l'algorithme présenté dans la preuve du Théorème 75.

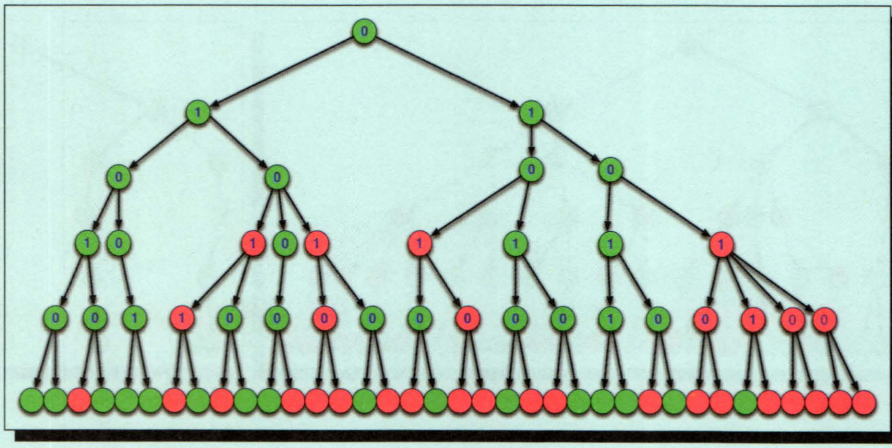






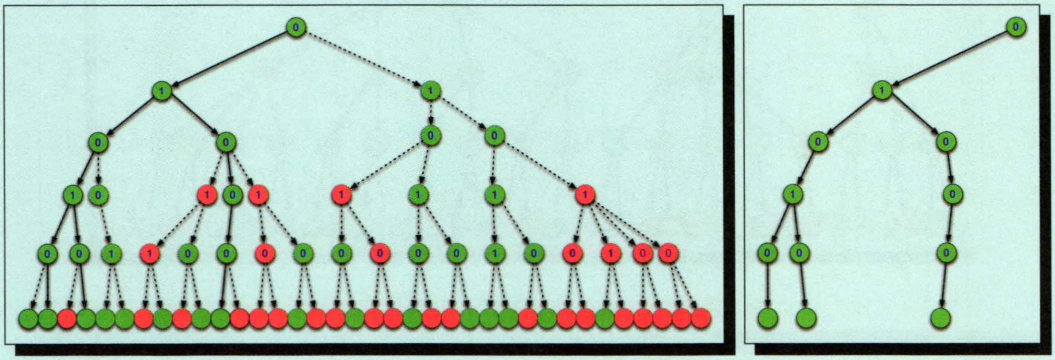


On aboutit finalement à colorier la racine de cet arbre en vert, c'est donc le joueur **0** qui possède une stratégie gagnante dans ce jeu :

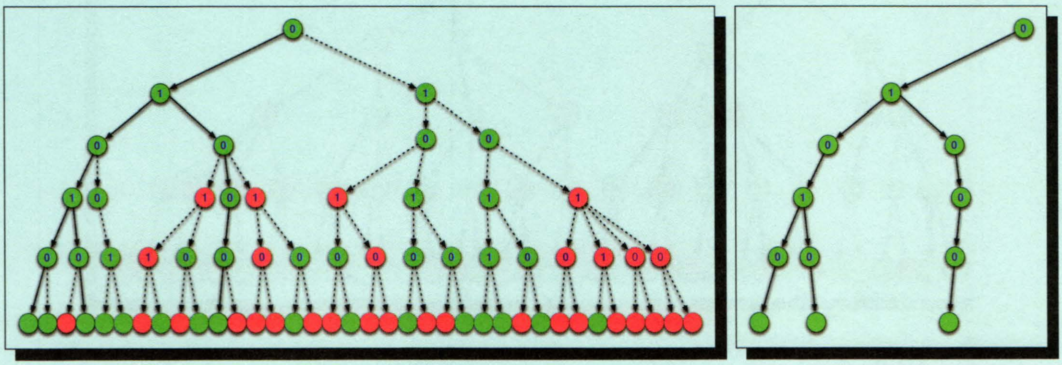


Ce joueur possède quatre stratégies gagnantes – à chaque fois la figure de gauche signale en pointillé les flèches qui doivent être retirées pour obtenir la stratégie décrite dans la figure de droite.

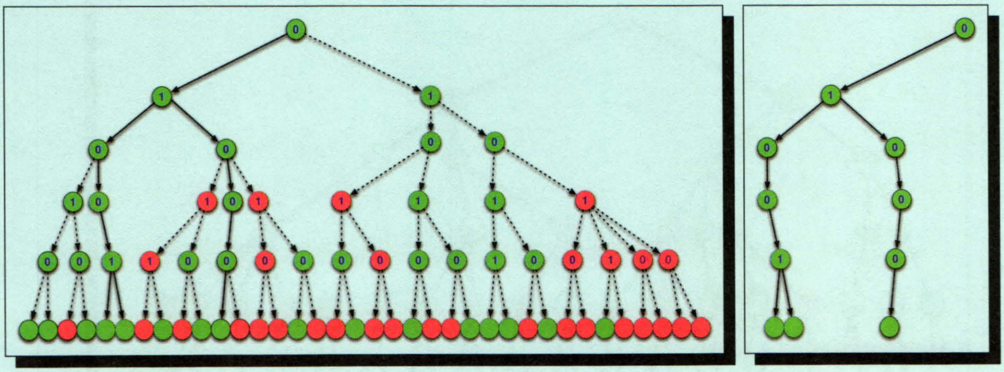
1$^{\text{ère}}$ stratégie gagnante :



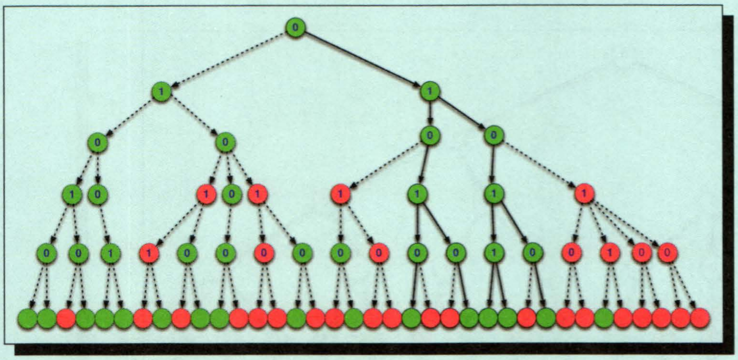
2$^{\text{ème}}$ stratégie gagnante :

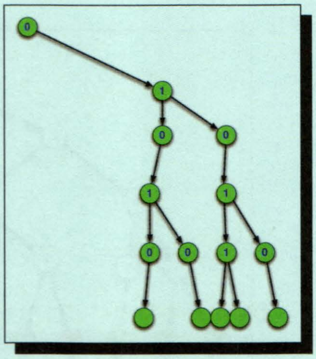


3$^{\text{ème}}$ stratégie gagnante :



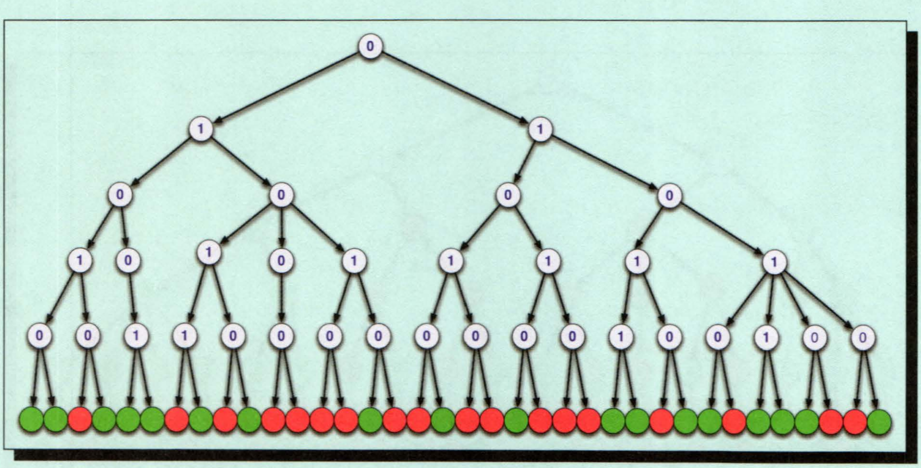
4$^{\text{ème}}$ stratégie gagnante :



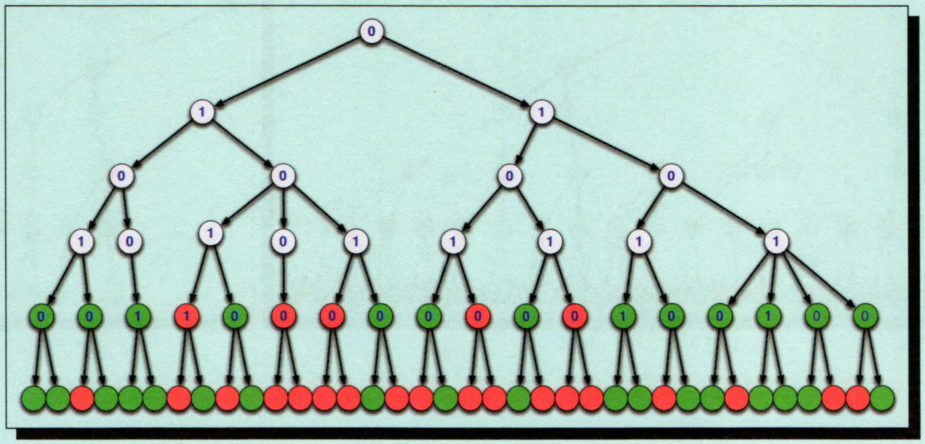


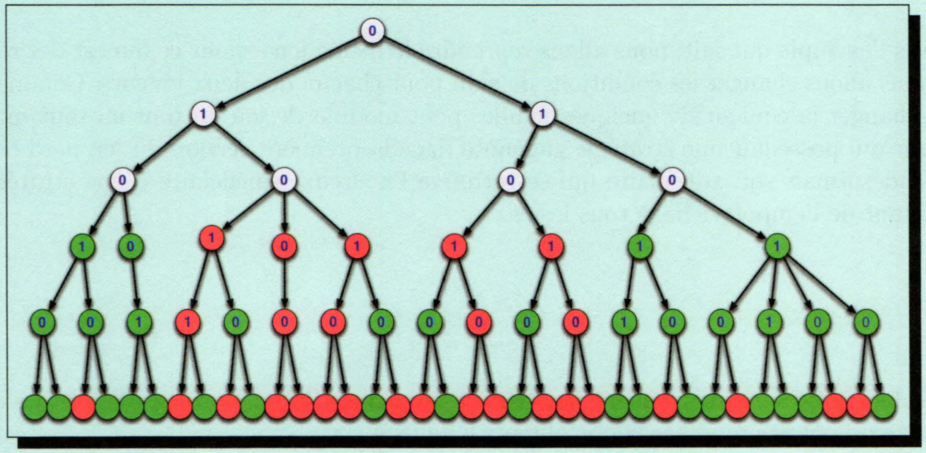
Dans l'exemple qui suit, nous allons reprendre le même jeu – pour ce qui est des règles – mais nous allons changer les conditions de gain pour chacun des deux joueurs. Comme on le verra, changer la couleur de quelques feuilles peut modifier le jeu du tout au tout, puisque le joueur qui possédait une stratégie gagnante dans la première version du jeu perd celle-ci, et c'est désormais son adversaire qui se retrouve l'heureux bénéficiaire d'une stratégie lui permettant de l'emporter dans tous les cas.

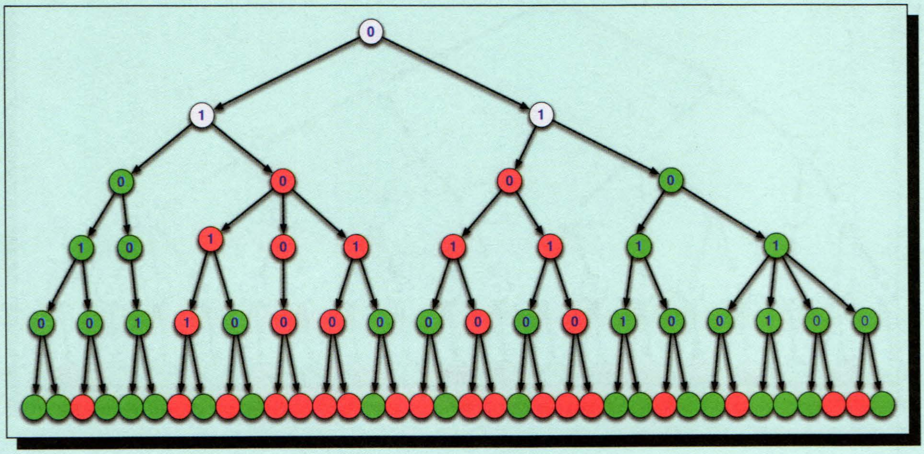
Exemple 77 Considérons le même arbre de jeu que dans l'exemple 76, mais dont les conditions de gain ont été modifiées pour obtenir le jeu suivant :

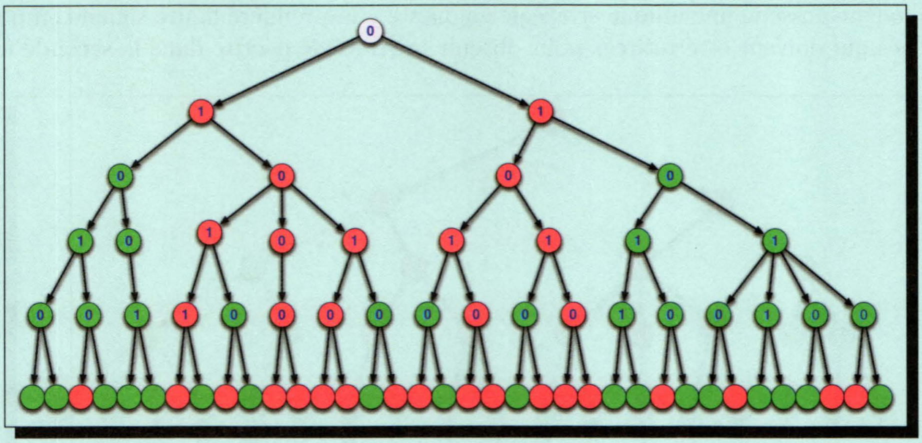


Appliquons étage par étage, en remontant des feuilles vers la racine, l'algorithme présenté dans la preuve du Théorème 75 :

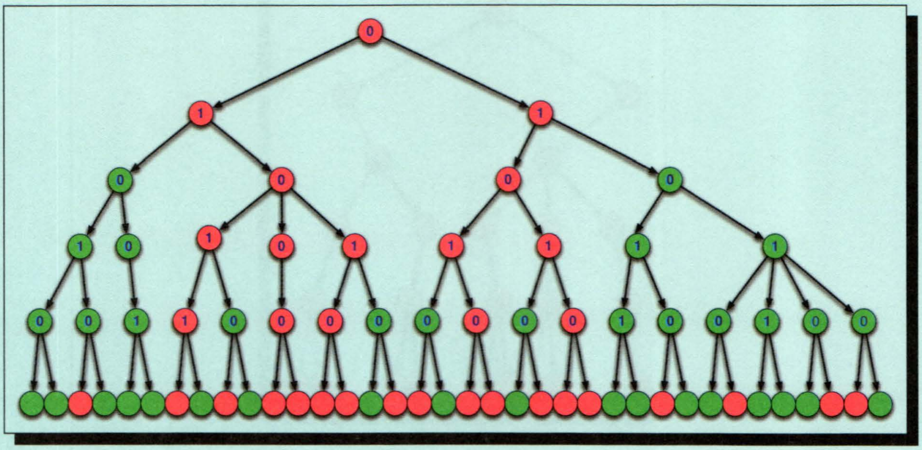




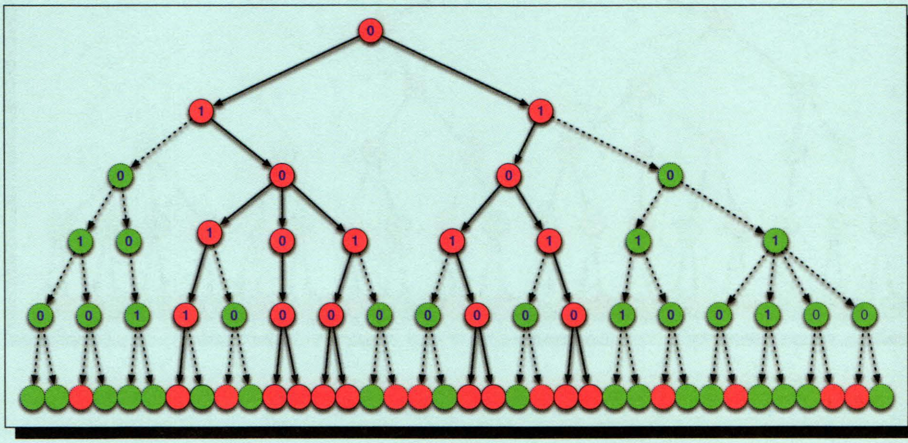


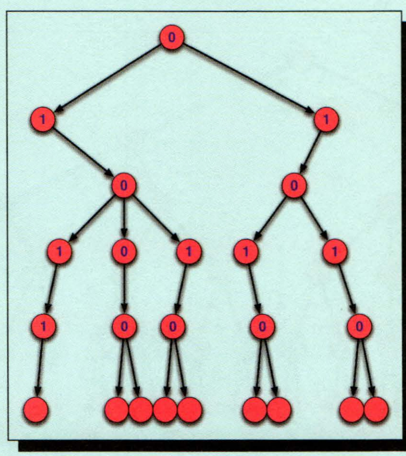


Finalement, on en vient à colorier la racine de cet arbre en rouge, c'est donc le joueur **1** qui possède une stratégie gagnante dans ce jeu :



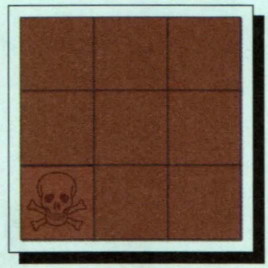
Ce joueur possède une unique stratégie gagnante – la première figure signale en pointillé les flèches qui doivent être retirées pour obtenir la stratégie décrite dans la seconde figure.



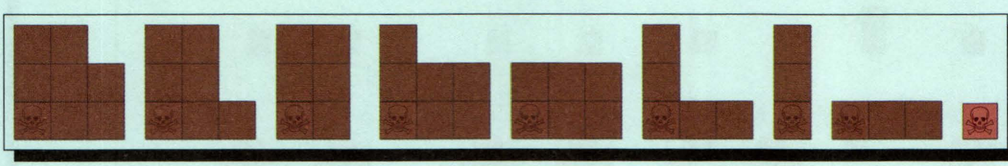


Maintenant que nous savons comment déterminer celui des deux joueurs qui possède une stratégie gagnante dans un jeu fini à information complète et dans lequel il y a soit victoire, soit défaite, regardons un exemple de jeu réel et déterminons lequel des deux joueurs sait à coup sûr comment l'emporter sur son adversaire.

Exemple 78 On considère un jeu dans lequel les joueurs dévorent à tour de rôle des carrés de la plaque de chocolat suivante :



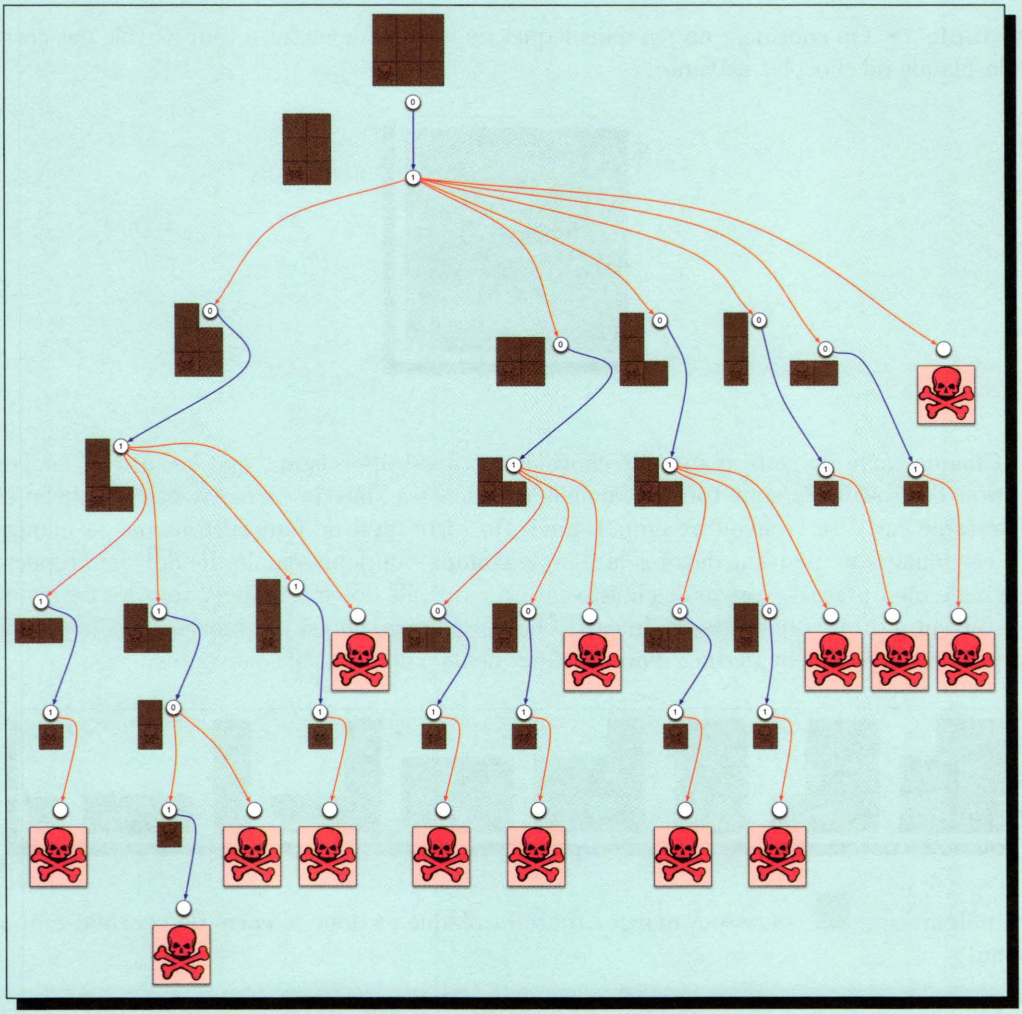
Chaque carré de cette plaque de chocolat est aussi appétissant que les autres. (A l'exception d'un seul, ils sont tous également excellents.) Mais le carré en bas à gauche est redoutable car il se trouve être empoisonné. De sorte qu'il ne faut surtout pas le manger. Or, ces joueurs ne peuvent dévorer la plaque comme bon leur semble. Ils doivent respecter une règle bien précise : lorsqu'ils choisissent un carré, ils doivent manger tous les carrés qui se trouvent à droite ou au dessus du carré choisi – ce carré choisi y compris. Ainsi le premier coup du premier joueur permet d'accéder aux neufs configurations suivantes :



la configuration  consiste à manger toute la plaque et donc le carré de chocolat empoisonné !

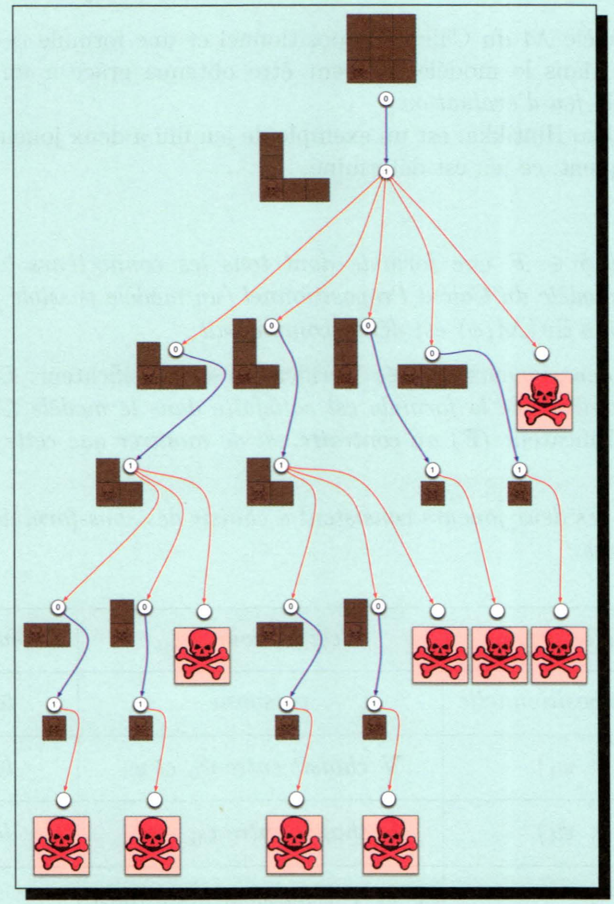
Même pour un jeu aussi simple, l'arbre de jeu est en fait trop compliqué pour pouvoir être dessiné de manière élégante sur une simple page. Il comporte en effet de trop nombreux nœuds.

Voici, ci-dessous un exemple de stratégie pour le joueur qui débute la partie. On vérifiera aisément que cette stratégie n'est pas gagnante.



Existe-t-il une stratégie pour le premier joueur qui à la fois débute par ce premier coup – menant à la configuration  et soit gagnante pour lui ?

Dans ce jeu, le joueur qui débute la partie possède une stratégie gagnante. Une telle stratégie gagnante est détaillée dans la figure qui suit.



L'idée qui sous-tend la définition de cette stratégie est la suivante :

(1) Le joueur qui débute la partie – en l 'occurrence le joueur 0 – mange en sorte qu'il ne reste à disposition de son adversaire qu'une seule ligne et qu'une seule colonne.

(2) Son adversaire – en l 'occurrence le joueur 1 –est alors obligé de manger :

  (a) soit tout le chocolat – auquel cas il meurt immédiatement,

  (b) soit une partie terminale de la ligne,

  (c) soit une partie, terminale de la colonne

(3) Les cas (2)(b) et (2)(c) produisent une dissymétrie : dans le cas (2)(b), la ligne devient plus courte que la colonne et dans le cas (2)(c) la colonne se réduit par rapport à la ligne. Le joueur 0 n'a plus dès lors qu'à rétablir la symétrie entre ligne et colonne pour renvoyer à nouveau son adversaire dans la position de l'étape (2) ; le contraignant ainsi en un temps fini à manger le dernier carré de chocolat et périr sur le champ.

On voit ainsi que cette stratégie fonctionne pour toute plaque de chocolat, pourvu qu'elle soit carrée et de format (n, n) pour un entier $n > 1$. Le cas $n = 1$ correspond à n'avoir qu'un seul carré de chocolat. Ce carré étant par ailleurs empoisonné, il est évident que dans le cas $n = 1$, le premier joueur meurt immédiatement et n'a donc pas de stratégie gagnante.

7.5 Evaluation d'une formule dans un modèle par un jeu

Etant donné un modèle $\mathcal{M}$ du Calcul Propositionnel et une formule $\phi \in \mathcal{F}$, la valeur que prend la formule ϕ dans le modèle $\mathcal{M}$ peut être obtenue grâce à un jeu. Ce jeu, noté $\mathbb{E}v(\mathcal{M}, \phi)$, est appelé *jeu d'évaluation.*

Ce jeu, dû à Jaakko Hintikka, est un exemple de jeu fini à deux joueurs et à information parfaite. Par conséquent, ce jeu est déterminé.

Définition 79 *Soit $\phi \in \mathcal{F}$ une formule dont tous les connecteurs logiques sont parmi $\{\neg, \vee, \wedge\}$ et $\mathcal{M}$ un modèle du Calcul Propositionnel (un modèle possible pour ϕ).*

Le jeu d'évaluation $\mathbb{E}v(\mathcal{M}, \phi)$ est défini comme suit :

(1) Il comprend deux joueurs appelés **V**érificateur *et* **F**alsificateur. *Le* **V**érificateur *(***V***) cherche à montrer que la formule est satisfaite dans le modèle ($\mathcal{M} \models \phi$), alors que le but du* **F**alsificateur *(***F***) au contraire est de montrer que cette formule est fausse ($\mathcal{M} \not\models \phi$).*

(2) Les coups de ces deux joueurs consistent à choisir des sous-formules en respectant les règles suivantes :

si ϕ est de la forme...	*c'est au tour de...*	*le jeu continue avec...*
variable propositionnelle	*personne*	*le jeu s'arrête*
$(\psi_0 \vee \psi_1)$	**V** *choisit entre ψ_0 et ψ_1*	*le choix de* **V**
$(\psi_0 \wedge \psi_1)$	**F** *choisit entre ψ_0 et ψ_1*	*le choix de* **F**
$\neg\varphi$	**F** *et* **V** *échangent leurs rôles*	φ

(3) Les conditions de gain de la partie n'apparaîssent qu'une fois celle-ci terminée, lorsque la sous-formule en jeu se réduit à une variable propositionnelle de la forme P :

- **V** *gagne si P est vraie dans ce modèle (c'est-à-dire lorsque $\mathcal{M} \models P$), et*
- **F** *l'emporte dans le cas contraire (c'est-à-dire lorsque $\mathcal{M} \not\models P$).*

Ainsi, une partie peut être regardée comme le fait de pousser un jeton le long d'une branche de la formule ϕ. Au début, le jeton se trouve placé sur la racine. Celui des deux joueurs qui est désigné comme le ***Vérificateur*** à l'origine pose le chapeau du ***Vérificateur*** sur sa tête, l'autre joueur pose celui du ***Falsificateur*** sur la sienne. Le connecteur associé au nœud détermine le joueur qui va pousser le jeton plus avant. S'il s'agit de "$\vee$", c'est le ***Vérificateur***, si c'est "$\wedge$", c'est le ***Falsificateur***, et si c'est un "$\neg$", les deux joueurs échangent leurs chapeaux et le jeton est poussé vers le seul descendant de ce connecteur de négation. De la sorte, après un nombre fini de coup, le jeton termine sa course sur une feuille. La partie s'arrête. Et le vainqueur est désigné en regardant la valeur de vérité de cette feuille dans le modèle considéré. Cette feuille étant nécessairement une variable propositionnelle, si elle est vraie dans le modèle, le joueur qui a le chapeau du ***Vérificateur*** à ce moment-là de la partie sur la tête est déclaré vainqueur. Dans le cas où cette variable est fausse, c'est le joueur au chapeau *"Falsificateur"* qui est déclaré vainqueur.

C'est ici qu'il faut faire attention à une chose très importante. Suivant la parité du nombre de négations rencontrées pendant la partie, le ***Vérificateur*** à l'origine peut ou ne peut pas être celui de la fin de la partie. On distinguera donc toujours le joueur qui avait le chapeau de ***Vérificateur*** à l'origine, et c'est par rapport à ce joueur que l'on dira que la partie est gagnée ou perdue.

Exemple 80 Soit $\mathcal{M} = (\{0,1\}, \delta)$ avec $\delta(P) = \delta(Q) = 1, \delta(R) = 0$, et

$$\phi = ((P \wedge (R \vee \neg P)) \vee (R \wedge Q))$$

Une partie possible dans le jeu $\mathbb{E}v\,(\mathcal{M}, ((P \wedge (R \vee \neg P)) \vee (R \wedge Q)))$:

(1) **V** choisit $(P \wedge (R \vee \neg P))$

(2) **F** choisit $(R \vee \neg P)$

(3) **V** choisit $\neg P$

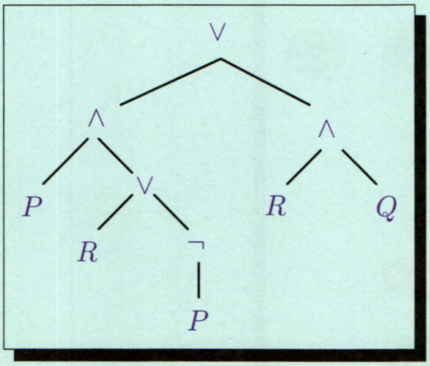
(4) **V** échange avec **F**

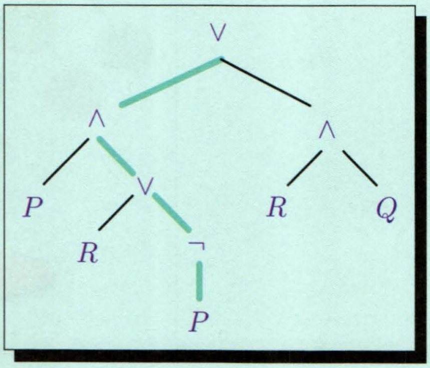
(5) **V** gagne

A noter que le joueur qui remporte cette partie n'est pas le joueur qui avait en charge le rôle de ***Vérificateur*** au début de la partie : il y a eu un échange de rôles. La partie se termine bien avec, comme vainqueur, le joueur ***Vérificateur***. Mais ce joueur n'est autre que celui auquel était attribué le rôle de ***Falsificateur*** au tout début de la partie. Pour le dire encore autrement, le joueur qui remporte cette partie est celui qui était le ***Falsificateur*** au début de la partie.

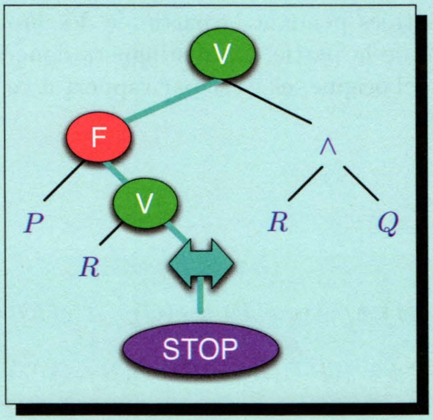
Considérons à nouveau la formule $((P \wedge (R \vee \neg P)) \vee (R \wedge Q))$, mais cette fois sous sa forme d'arbre.

Nous apercevons alors que cette partie se déroule le long d'une branche maximale de cet arbre (ce qui ne devrait pas surprendre si l'on se souvient que choisir une sous-formule revient à choisir un nœud de l'arbre). Ci-après, la partie est indiquée par le chemin de couleur bleu ciel :





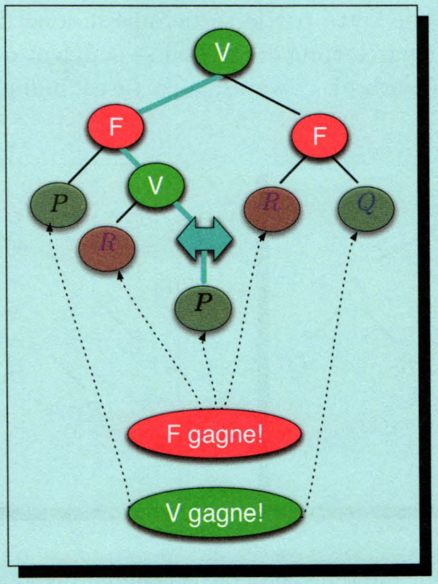
Le long de ce chemin sont indiqués, dans le schéma ci-dessous, par qui sont effectués les choix de bifurcation le long de la formule : V désigne un choix pour le ***Vérificateur***, F un choix pour le ***Falsificateur*** et un changement de chapeaux.



Ces jeux sont clairement déterminés puisqu'ils sont un cas particulier de ceux pris en considération dans le Théorème 75. Par conséquent, étant donnés une formule et un modèle, soit le ***Vérificateur***, soit le ***Falsificateur*** possède une stratégie gagnante dans le jeu sous-jacent.

Dans notre cas, c'est le ***Falsificateur*** qui possède une *stratégie gagnante* :

- si **V**, au premier coup, choisit $(R \wedge Q)$, il lui suffit de choisir ensuite R pour l'emporter.
- si **V**, au premier coup, choisit $(P \wedge (R \vee \neg P))$, alors il choisit $(R \vee \neg P)$. Puis
  - si **V** choisit R, **V** perd immédiatement,
  - si **V** choisit $\neg P$, c'est finalement le joueur en charge du rôle de ***Vérificateur*** qui l'emporte, mais comme il y a dans ce cas un échange de rôle, c'est en fait le joueur qui était le ***Falsificateur*** au début de la partie qui gagne. Donc **V** perd également la partie.



En fait, les règles de ce jeu sont définies pour que l'on ait le résultat suivant :

Théorème 81

$$\mathcal{M} \models \phi \textit{ ssi } \mathbf{V} \textit{ a une stratégie gagnante dans } \mathbb{E}v\,(\mathcal{M}, \phi)\,.$$

Preuve du Théorème 81 : La preuve est par induction sur la hauteur de la formule ϕ. On montre simultanément que :

(a) si $\mathcal{M} \models \phi$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi)$,

(b) si $\mathcal{M} \models \neg\phi$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi)$.

(1) $ht(\phi)$=0 correspond au cas où ϕ est une variable propositionnelle. Vérifier dès lors les points (a) et (b) est immédiat.

(2) $ht(\phi)$=$n+1$ correspond aux différents cas où ϕ est une négation, une disjonction ou bien une conjonction.

(a) Si $\phi = \neg\psi$, alors l'hypothèse d'induction opère sur ψ :

(a) si $\mathcal{M} \models \psi$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \psi)$,

(b) si $\mathcal{M} \models \neg\psi$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \psi)$.

La seule différence entre le jeu d'évaluation impliquant ψ et celui impliquant ϕ est un changement de chapeau au début de la partie. Il est alors évident que si **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \psi)$, alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi)$, et *vice-versa*. Ce qui montre que ϕ vérifie (a) et (b).

(b) Si $\phi = \phi_0 \wedge \phi_1$, alors l'hypothèse d'induction opère sur ϕ_0 et sur ϕ_1 :

(a) si $\mathcal{M} \models \phi_0$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0)$; si $\mathcal{M} \models \phi_1$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_1)$,

(b) si $\mathcal{M} \models \neg\phi_0$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0)$; si $\mathcal{M} \models \neg\phi_1$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_1)$.

V a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0 \wedge \phi_1)$ si et seulement si **V** possède une stratégie gagnante dans chacun des jeux $\mathbb{E}v\,(\mathcal{M}, \phi_0)$ et $\mathbb{E}v\,(\mathcal{M}, \phi_1)$. **F** possède une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0 \wedge \phi_1)$ dans les trois autres cas. Ce qui montre immédiatement que (a) et (b) sont vérifiés pour ϕ.

(c) Si $\phi = \phi_0 \vee \phi_1$, alors l'hypothèse d'induction opère sur ϕ_0 et sur ϕ_1 :

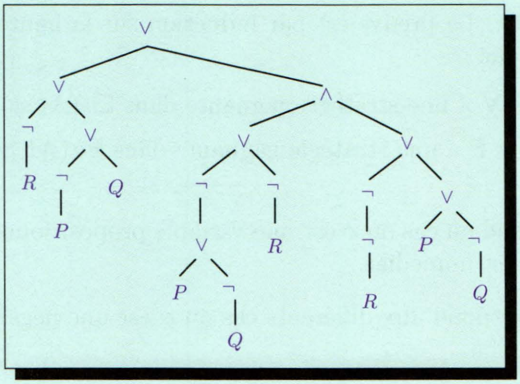
(a) si $\mathcal{M} \models \phi_0$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0)$; si $\mathcal{M} \models \phi_1$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_1)$,

(b) si $\mathcal{M} \models \neg\phi_0$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0)$; si $\mathcal{M} \models \neg\phi_1$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_1)$.

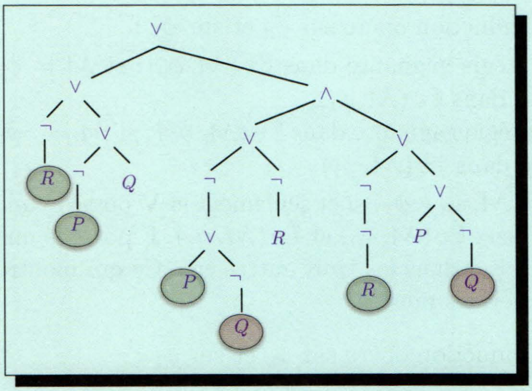
F a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0 \vee \phi_1)$ si et seulement si **F** possède une stratégie gagnante dans chacun des jeux $\mathbb{E}v\,(\mathcal{M}, \phi_0)$ et $\mathbb{E}v\,(\mathcal{M}, \phi_1)$. **V** possédant une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi_0 \vee \phi_1)$ dans les trois autres cas. Ce qui montre immédiatement que (a) et (b) sont vérifiés pour ϕ.

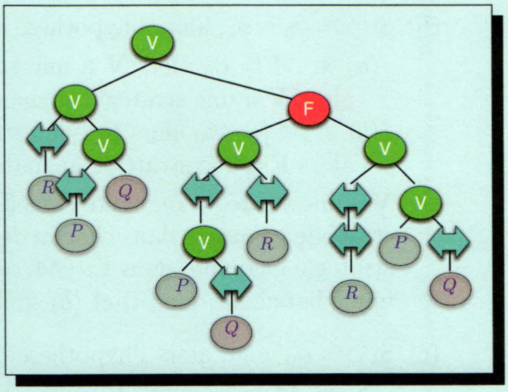
$\dashv$ 81

Exemple 82 Considérons la formule ci-dessous, ainsi que le modèle $\mathcal{M}$, dans lequel P et R sont toutes les deux vraies, mais Q est fausse :

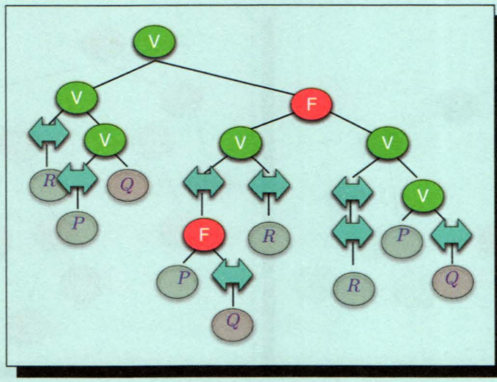


Nous allons déterminer lequel des deux joueurs a une stratégie gagnante dans le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$. La formule prise en compte dans le domaine correspond à l'arbre dont les feuilles sont coloriées ci-dessous. Nous pouvons ensuite remplacer chacune des occurrences des connecteurs $\vee$, $\wedge$, $\neg$, respectivement par les symboles V, F, ⇔.



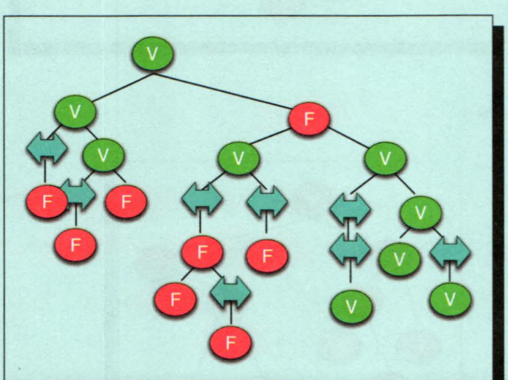


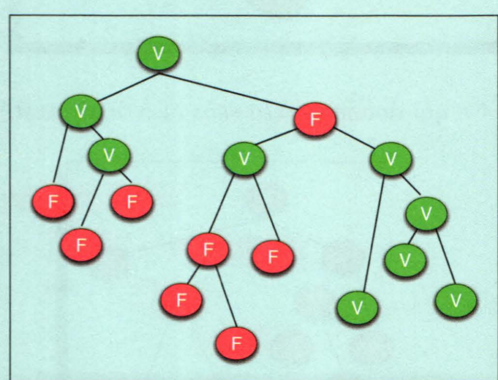
Le procédé précédent associe à chaque nœud qui n'est pas une feuille ni le symbole de négation, le nom du joueur qui doit effectuer le choix à ce moment de la partie. Nous allons maintenant associer à chacun de ces nœuds non pas le nom du joueur qui joue à ce moment de la partie, mais son nom à l'origine de la partie. Pour cela et pour chacun des nœuds, nous comptons combien de symboles ⇔ se trouvent sur le chemin qui mène de ce nœud à la racine. Si ce nombre est pair, nous laissons ce nœud inchangé. Si ce nombre est impair nous changeons ce nœud de V en F, et *vice-versa*.



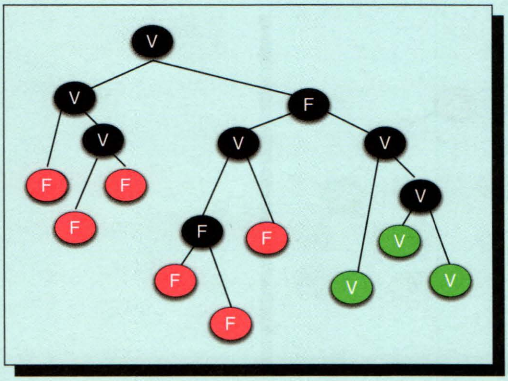
Ensuite nous posons des symboles V et F sur les feuilles de l'arbre afin d'indiquer quel est le gagnant de la partie. Pour cela, nous comptons le nombre de nœud $\Leftrightarrow$ se trouvant sur le chemin qui mène de cette feuille à la racine. Nous plaçons le symbole V lorsque ou bien la feuille est de couleur verte et ce nombre est pair, ou bien la feuille est de couleur rouge et ce nombre est impair. Nous plaçons le symbole F lorsque ou bien la feuille est de couleur verte et ce nombre est impair, ou bien la feuille est de couleur rouge et ce nombre est pair.

Nous pouvons finalement retirer les symboles $\Leftrightarrow$ pour obtenir l'arbre de jeu associé au jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi)$.

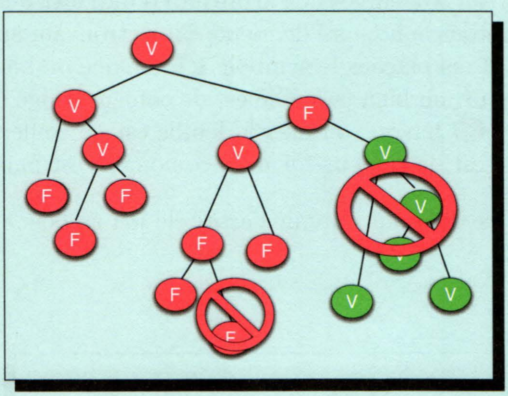




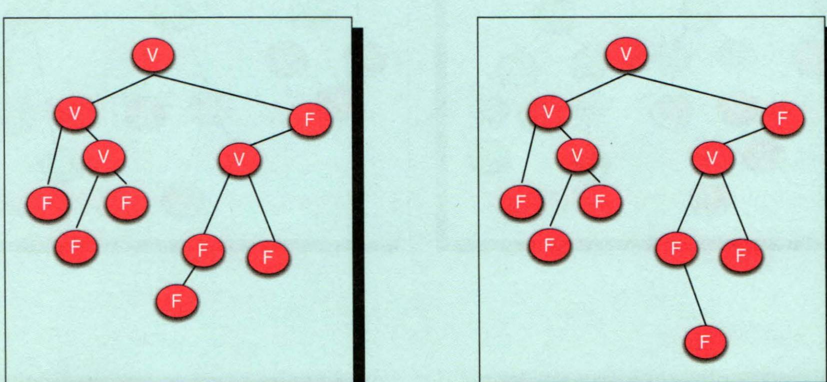
Il ne nous reste plus qu'à trouver lequel des deux joueurs possède une stratégie gagnante dans ce jeu. Pour cela nous commençons par noircir chaque nœud qui n'est pas une feuille. Ensuite, nous appliquons l'algorithme de coloriage présenté dans la preuve du Théorème 75 qui consiste à associer à chaque nœud la couleur du joueur qui possède une stratégie gagnante dans le sous-jeu induit par ce nœud. Nous obtenons ainsi le graphe suivant, à partir duquel il est aisé de récupérer les stratégies gagnantes pour le vainqueur.



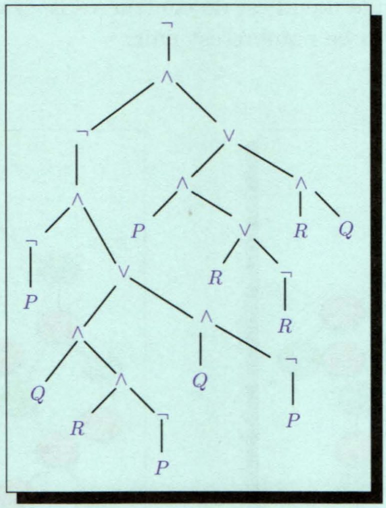
Nous voyons que le ***Falsificateur*** possède exactement deux stratégies gagnantes. Elles sont indiquées dans les deux schémas ci-dessous.



Ce qui donne *stricto sensu* les deux stratégies :



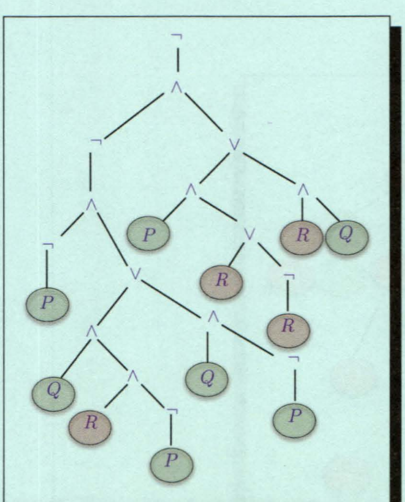
Exemple 83 Considérons la formule ϕ ci-dessous, ainsi que le modèle $\mathcal{M} \models P, Q, \neg R$:

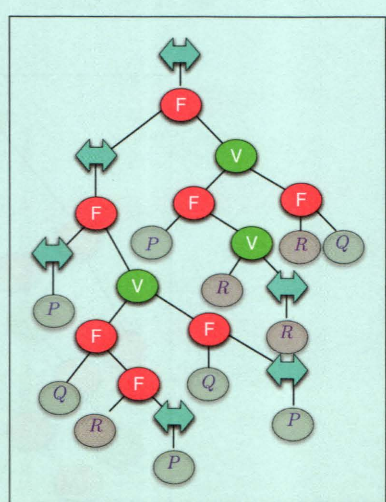


$$\overline{\phi} = \neg\Big((\neg(\neg P \wedge ((Q \wedge (R \wedge \neg P)) \vee (Q \wedge \neg P))) \wedge (P \wedge (R \vee \neg R)) \vee (R \wedge Q))\Big).$$

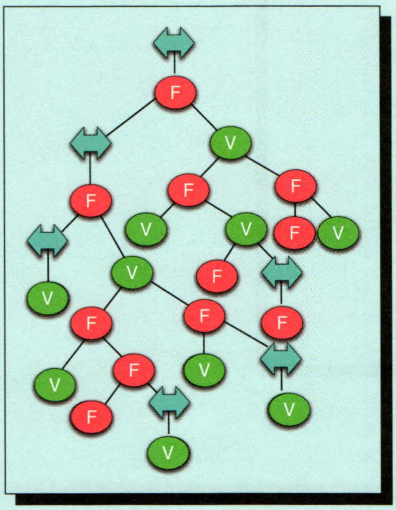
Nous déterminons lequel des deux joueurs a une stratégie gagnante dans le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$. Tout d'abord nous colorions les feuilles de l'arbre conformément au modèles $\mathcal{M}$.

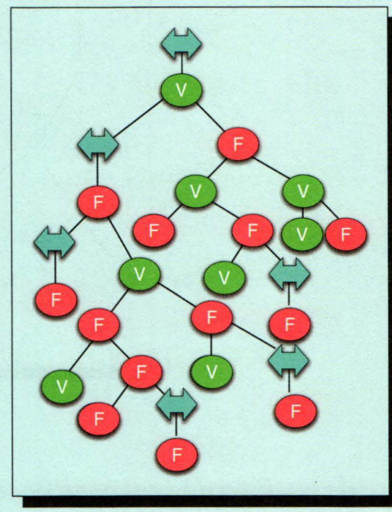
Nous remplaçons ensuite chacune des occurrences des connecteurs $\vee$, $\wedge$, $\neg$, respectivement par les symboles V, F, ⇔.



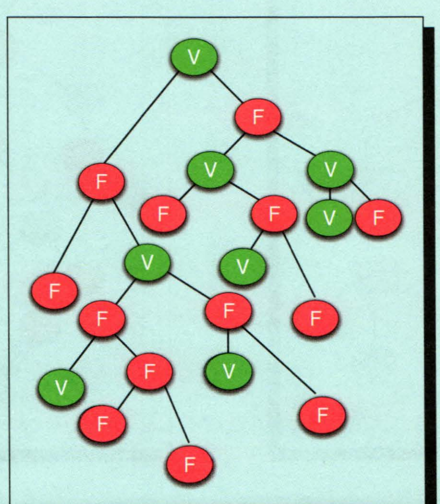


Nous remplaçons ensuite chacune des feuilles vertes par V, et chacune des feuilles rouges par F. Puis – dans le second dessin – pour chaque nœud (y compris les feuilles) nous comptons le nombre de nœud ⇔ se trouvant sur le chemin qui mène de ce nœud vers la racine. Nous plaçons le symbole V lorsque ou bien le nœud est de couleur verte et ce nombre est pair, ou bien le nœud est de couleur rouge et ce nombre est impair. Nous plaçons le symbole F lorsque ou bien le nœud est de couleur verte et ce nombre est impair, ou bien le nœud est de couleur rouge et ce nombre est pair.

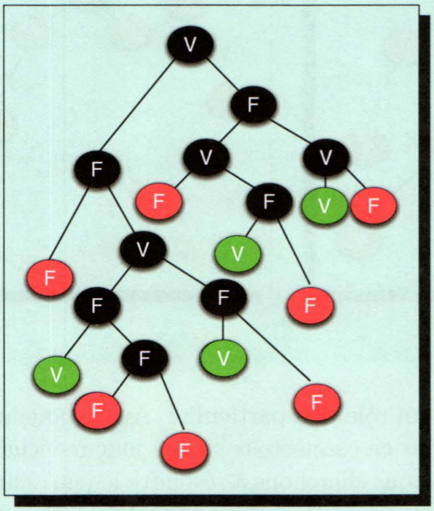


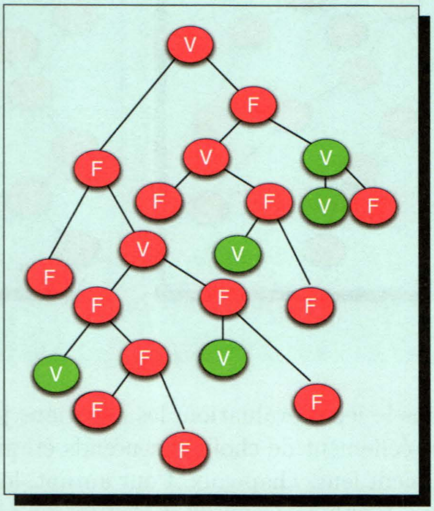


Nous retirons finalement les symboles ⇔ pour obtenir l'arbre de jeu associé au jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi)$.

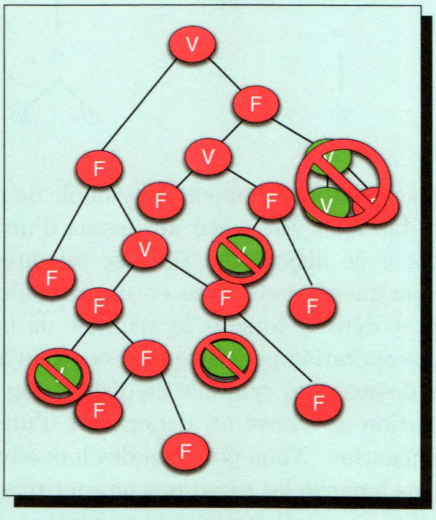


Il ne reste qu'à trouver lequel des deux joueurs possède une stratégie gagnante dans ce jeu. A cette fin, nous colorions préalablement en noir tous les nœuds qui ne sont pas des feuilles. Puis nous appliquons l'algorithme de coloriage présenté dans la preuve du Théorème 75.

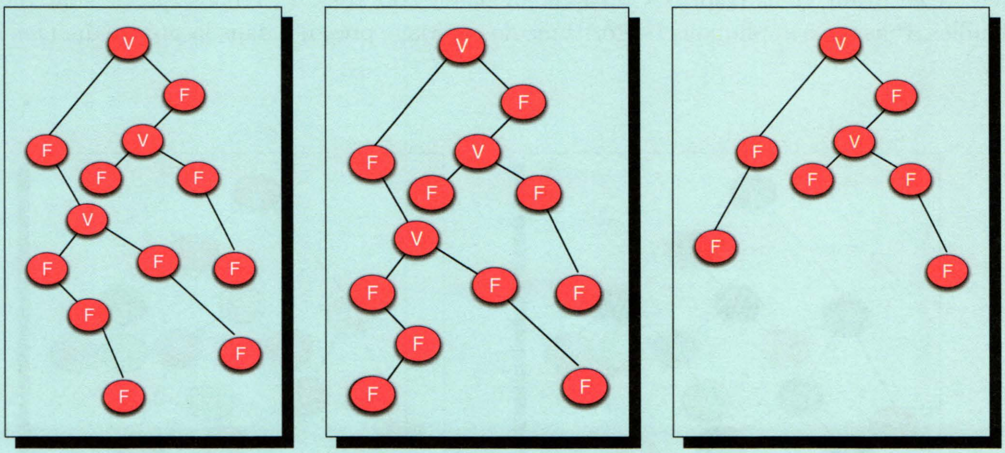




Le ***F****alsificateur* possède donc une stratégie gagnante. Les régions qu'il doit éviter sont spécifiées dans le dessin qui suit.



On distingue alors trois stratégies gagnantes pour le ***Falsificateur*** :



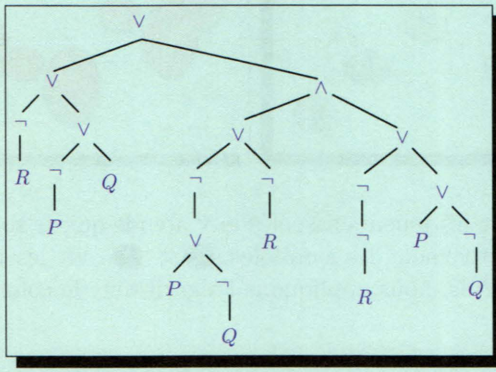
Dans le jeu d'évaluation, les négations jouent un rôle très particulier. Aucun joueur n'effectue réellement de choix aux nœuds étiquetés par ce connecteur [13]. Les joueurs échangent simplement leurs chapeaux. Pour autant, lorsque nous cherchons à résoudre le jeu – chercher celui du ***Vérificateur*** ou du ***Falsificateur*** qui possède une stratégie gagnante – les négations nous compliquent rudement la tâche. Pour remédier à cela, une solution consiste à évaluer non pas la formule qui nous est donnée, mais une formule équivalente dans laquelle les négations poseront beaucoup moins de problème. A cette fin, il suffit de se souvenir des équivalences de formules suivantes :

$$\neg(\phi \vee \psi) \equiv (\neg\phi \wedge \neg\psi) \quad \text{et} \quad \neg(\phi \wedge \psi) \equiv (\neg\phi \vee \neg\psi)$$

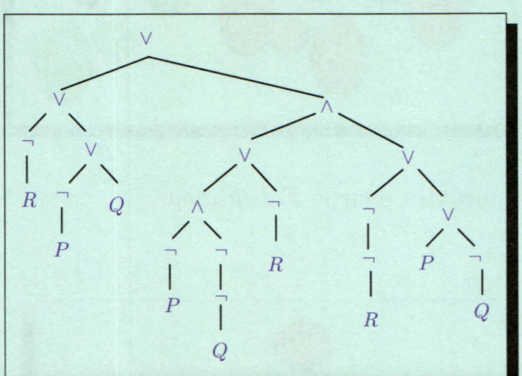
Chacune de ces équivalences indique comment le symbole de négation peut être "poussé" plus avant dans la formule. Lorsqu'il est placé au dessus d'un symbole de disjonction, il "passe au travers" du symbole de disjonction pour se retrouver dédoublé en dessous de celui-ci qui est aussi immédiatement transformé en un symbole de conjonction. La même opération *mutatis mutandis* se déroule lorsque le symbole de négation est au dessus d'un symbole de conjonction. Cette opération peut être répétée jusqu'à ce que plus aucun symbole de négation ne se trouve au dessus d'un symbole de disjonction ni de conjonction. Dans ce cas, chaque symbole de négation se trouve au dessus soit d'une variable propositionnelle, soit d'un autre symbole de négation. Nous pouvons dès lors éliminer les doubles négations pour obtenir une formule dans laquelle les négations ne sont plus qu'au-dessus des variables propositionnelles, ce qui facilite ensuite beaucoup la résolution du jeu d'évaluation associé.

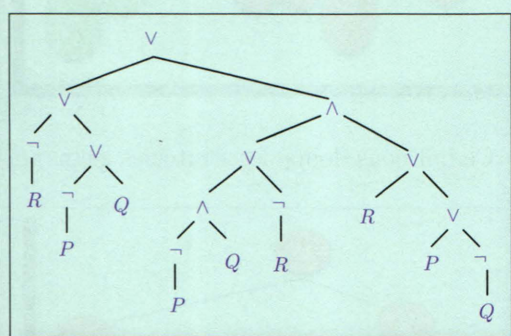
13. Peu importe qui descend le jeton, puisqu'il n'y a aucun autre choix possible que de le pousser vers le connecteur suivant.

Exemple 84 Considérons la formule ci-dessous dans le modèle $\mathcal{M} \models P, \neg Q, R$:



Nous commençons par pousser les symboles de négation vers les feuilles. Ensuite nous éliminons les doubles négations.

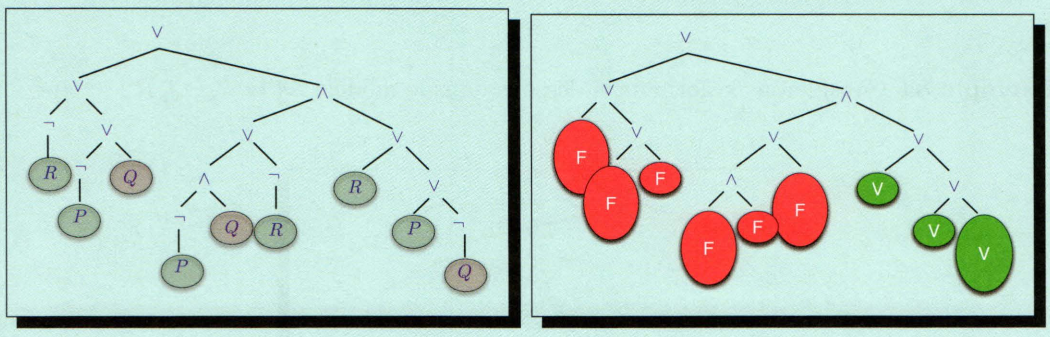




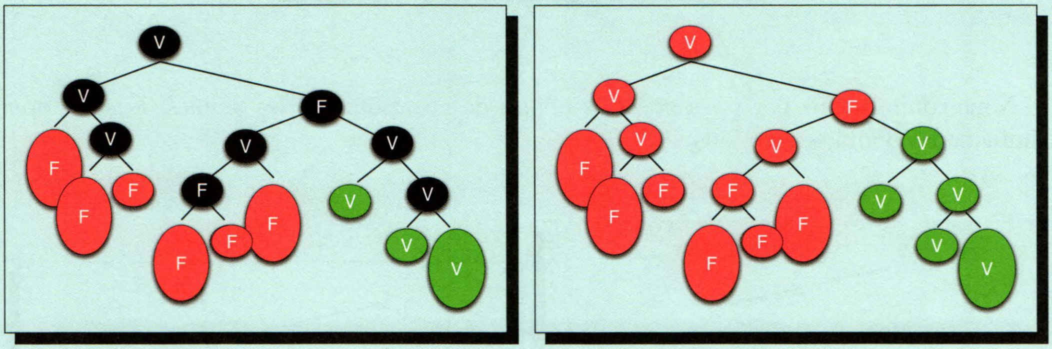
Nous colorions ensuite les feuilles conformément au modèle $\mathcal{M}$.

Puis, nous considérons en même temps les variables propositionnelles et les négations de variables propositionnelles pour indiquer lequel des joueurs gagne la partie à ce point de l'arbre. Pour cela :

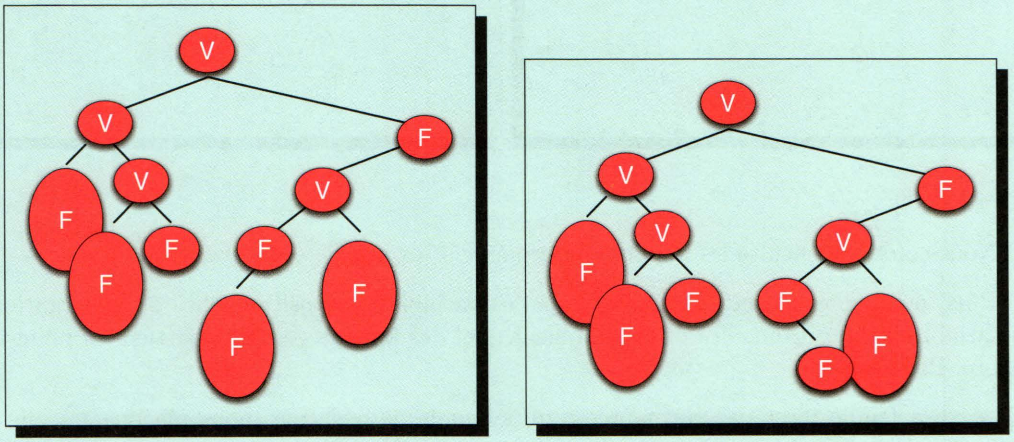
- si la feuille n'est pas surmontée d'un symbole de négation, nous plaçons sur elle le symbole V si la feuille est coloriée en vert, et F si la feuille est coloriée en rouge.
- si la feuille est surmontée d'un symbole de négation, nous plaçons un jeton qui la recouvre elle-même ainsi que le symbole de négation. Ce jeton est V si la feuille est coloriée en rouge, et F si la feuille est coloriée en vert.



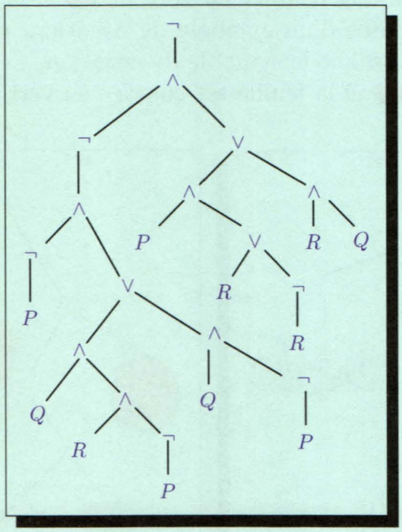
Nous désignons ensuite les joueurs associés aux nœuds qui ne sont pas des feuilles. Pour cela, nous plaçons respectivement les symboles V et F sur les nœuds occupés par respectivement "$\vee$" et "$\wedge$". Puis, nous appliquons l'algorithme de coloriage pour déterminer le vainqueur.



Ce qui nous donne les stratégies gagnantes suivantes pour le ***Falsificateur***.

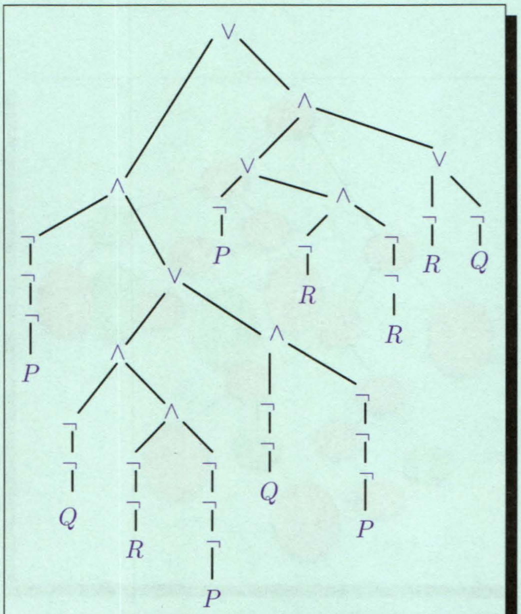


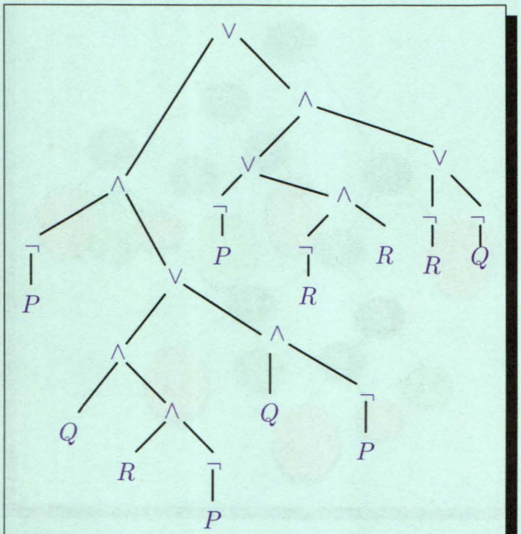
Exemple 85 Considérons à nouveau la formule ϕ ci-dessous, ainsi que le modèle $\mathcal{M} \models P, Q, \neg R$:



$$\overline{\phi} = \neg\Big((\neg(\neg P \wedge ((Q \wedge (R \wedge \neg P)) \vee (Q \wedge \neg P))) \wedge (P \wedge (R \vee \neg R)) \vee (R \wedge Q))\Big).$$

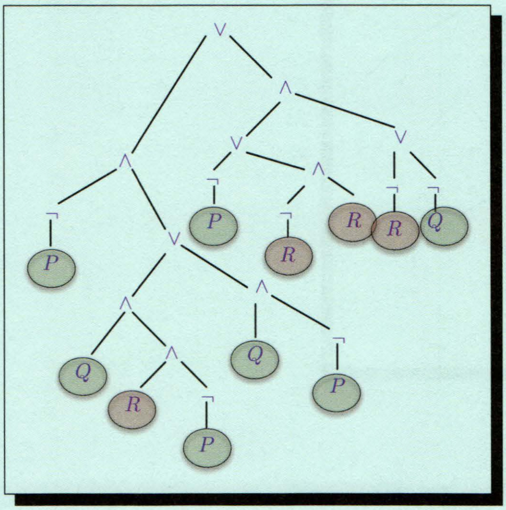
Nous commençons par pousser les symboles de négation vers les feuilles. Ensuite nous éliminons les doubles négations.

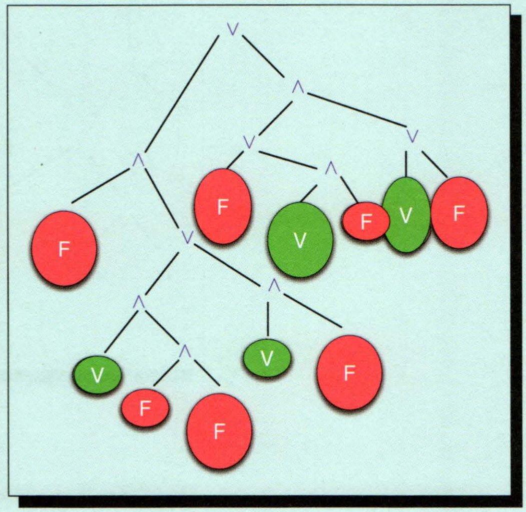




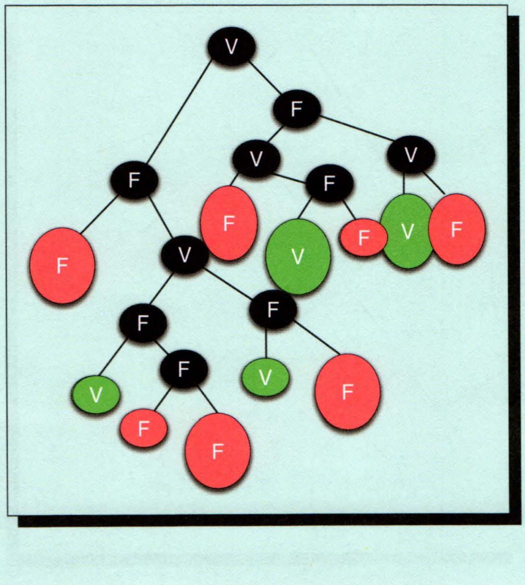
Nous colorions les feuilles conformément au modèle, puis nous indiquons quel joueur gagne la partie aux variables et négations de variables propositionnelles. Pour cela :

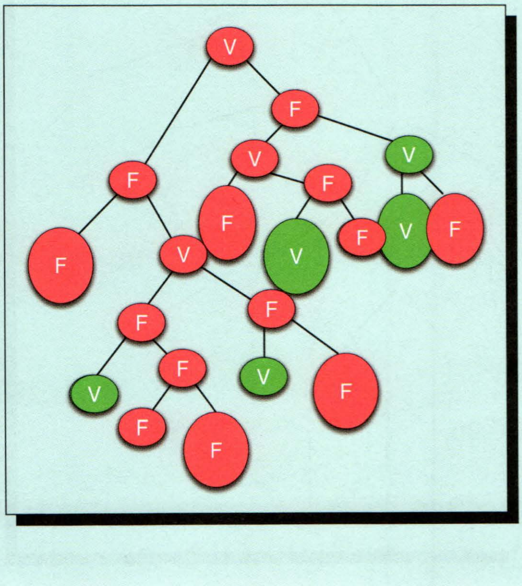
- si la feuille n'est pas surmontée d'un symbole de négation, nous plaçons sur elle le symbole V si la feuille est coloriée en vert, et F si la feuille est coloriée en rouge.
- si la feuille est surmontée d'un symbole de négation, nous plaçons un jeton qui la recouvre elle-même ainsi que le symbole de négation. Ce jeton est V si la feuille est coloriée en rouge, et F si la feuille est coloriée en vert.



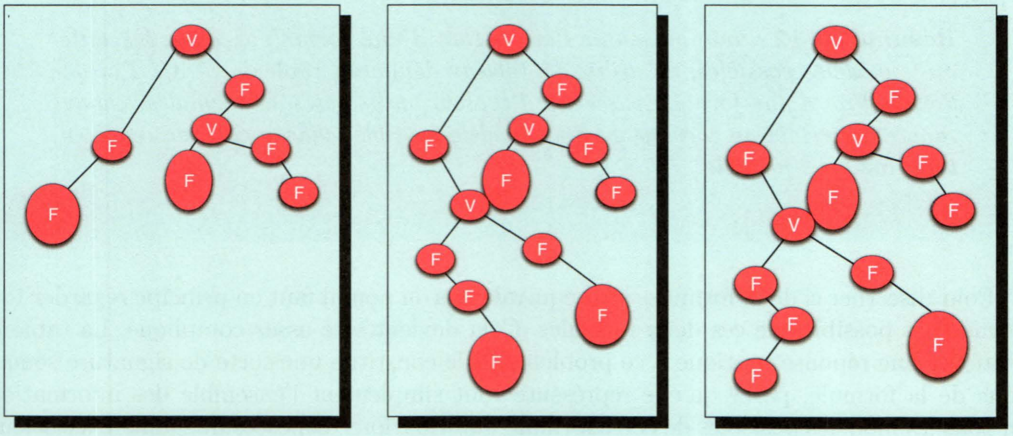


Nous désignons ensuite les joueurs associés aux nœuds qui ne sont pas des feuilles. Pour cela, nous plaçons respectivement les symbole V et F sur les nœuds occupés par respectivement "$\vee$" et "$\wedge$". Puis, nous appliquons l'algorithme de coloriage pour déterminer le vainqueur.





Ce qui nous donne les stratégies gagnantes suivantes pour le ***Falsificateur***.



8 Table de vérité

Résumé № 12 *Pour présenter l'évaluation d'une formule ϕ dans ses différents modèles possibles, on utilise un tableau dénommé* table de vérité. *Puisque l'évaluation d'une formule passe par l'évaluation de ses sous-formules, chaque rangée de ce tableau correspond à un modèle possible, chaque colonne représentant une sous-formule.*

※

Pour discerner si deux formules sont équivalentes ou non, il faut en principe regarder tous les modèles possibles de ces deux formules. Cela devient vite assez compliqué. La table de vérité est une réponse pratique à ce problème. Elle constitue une sorte de signature sémantique de la formule, parce qu'elle représente tout simplement l'ensemble des informations sur tous les modèles possibles de cette formule, informations disposées de manière astucieuse sous forme de tableau.

Si l'on s'arrête quelques secondes sur l'évaluation d'une formule dans un modèle, on s'aperçoit que pour évaluer correctement la formule, il nous faut évaluer **toutes** ses sous-formules. En effet, si l'on regarde la formule comme un arbre, on voit bien que pour trouver la valeur de vérité de la racine de cet arbre (et donc de la formule elle-même), il nous faut petit à petit calculer la valeur de vérité pour chacun des nœuds de l'arbre, en commençant par les feuilles (qui ne comportent que des variables propositionnelles) et en remontant à la racine. Si l'on se rappelle qu'un nœud de l'arbre définit une sous-formule (celle dont l'arbre est précisément le sous-arbre dont ce nœud forme la racine) et réciproquement, on s'aperçoit qu'évaluer une formule revient à évaluer chacune de ses sous-formules.

Cela nécessite encore plus d'effort, lorsqu'il s'agit de procéder à l'évaluation d'une formule dans chacun des modèles possibles. En supposant que cette formule contienne n variable propositionnelle, 2^n modèles doivent être considérés et, dans chacun d'eux, toutes les sous-formules doivent être évaluées.

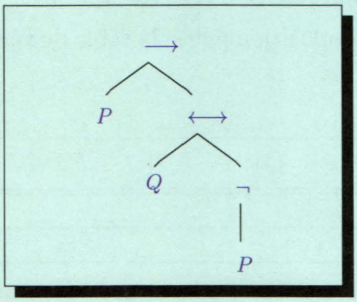
La table de vérité est simplement une mise à disposition plus ou moins élégante de ce processus quelque peu rébarbatif. Au sens strict, lorsqu'on parle de la table de vérité d'une formule, il s'agit uniquement d'une présentation des évaluations de cette formule dans chacun de ses modèles possibles. Au sens large, la table de vérité inclut les étapes de la construction de ces évaluations qui passent nécessairement par l'évaluation des sous-formules.

Plutôt que de donner une définition générale et rigoureuse qui serait extrêmement ennuyeuse, prenons tout de suite un exemple :

Exemple 86 Considérons la formule $\phi := P \longrightarrow (Q \longleftrightarrow \neg P)$.
La table de vérité de ϕ est définie de la manière suivante :
Tout d'abord, on s'inquiète de savoir quel est le nombre de variables propositionnelles qu'il y a dans ϕ. Dans notre cas il y en a 2, cela induit une table de vérité avec $1 + 4$ lignes. Si la formule avait k variables propositionnelles, cela donnerait une table avec $1 + 2^k$ lignes. Les k premières colonnes sont réservées aux variables propositionnelles, la $k + 1^{\text{ème}}$ est pour la formule elle-même. Mais cette dernière colonne est subdivisée en autant de colonnes qu'il y a d'occurrences de connecteurs logiques dans la formule elle-même.

P	Q	$(P$	$\longrightarrow$	$(Q$	$\longleftrightarrow$	$\neg$	$P))$
0	0						
0	1						
1	0						
1	1						

Le but de ce calcul est de donner une présentation de toutes les différentes valeurs de la formule ϕ en fonction des valeurs de vérité des variables propositionnelles. Mais pour cela, il faut procéder par ordre en calculant les valeurs des sous-formules, des plus petites aux plus grandes. On commence donc par chercher les sous-formules de hauteur 1. En regardant l'arbre que constitue la formule, c'est immédiat :



Il n'y a qu'une seule sous-formule de hauteur 1 c'est $\neg P$, cela donne le début de tableau suivant :

P	Q	$(P$	$\longrightarrow$	$(Q$	$\longleftrightarrow$	$\neg$	$P))$
0	0					1	
0	1					1	
1	0					0	
1	1					0	

On passe alors aux sous-formules de hauteur 2. Là aussi, il n'y en a qu'une, il s'agit de $Q \longleftrightarrow \neg P$. On peut donc aisément construire maintenant le tableau ci-dessous :

P	Q	$(P$	$\longrightarrow$	$(Q$	$\longleftrightarrow$	$\neg$	$P))$
0	0				0	1	
0	1				1	1	
1	0				1	0	
1	1				0	0	

Ensuite, on passe aux sous-formules de hauteur 3. Là pour le coup il n'y en a encore qu'une seule et c'est celle qui nous interesse, la formule ϕ elle-même. Donc, sous le connecteur $\longrightarrow$ de $P \longrightarrow (Q \longleftrightarrow \neg P)$ se trouve la dernière colonne :

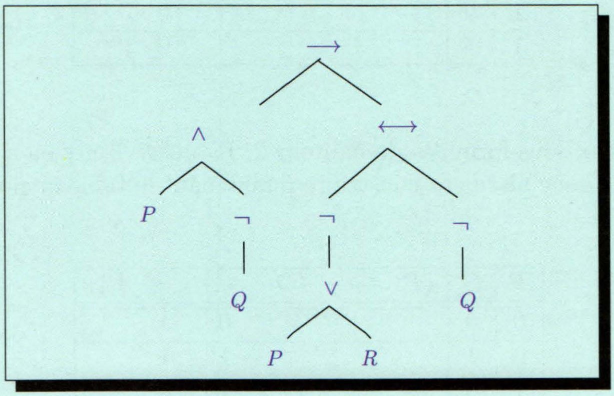
P	Q	$(P$	$\longrightarrow$	$(Q$	$\longleftrightarrow$	$\neg$	$P))$
0	0		1		0	1	
0	1		1		1	1	
1	0		1		1	0	
1	1		0		0	0	

Considérons un second exemple, un peu plus sophistiqué que le précédent :

Exemple 87 Considérons la formule $\phi := \Big((P \wedge \neg Q) \longrightarrow (\neg(P \vee R) \longleftrightarrow \neg Q)\Big)$.
Comme ϕ contient 3 variables propositionnelles, la table de vérité de ϕ doit contenir $1+2^3 = 9$ lignes.

P	Q	R	$\Big((P$	$\wedge$	$\neg$	$Q)$	$\longrightarrow$	$(\neg$	$(P$	$\vee$	$R)$	$\longleftrightarrow$	$\neg$	$Q)\Big)$
0	0	0												
0	0	1												
0	1	0												
0	1	1												
1	0	0												
1	0	1												
1	1	0												
1	1	1												

Jetons un oeil à l'arbre de notre formule afin de repérer les sous-formules de hauteur 1 :



Ici, il y a trois sous-formules de hauteur 1 : $\neg Q$ qui apparaît deux fois, et $P \vee R$. Cela permet de remplir les trois colonnes suivantes :

P	Q	R	$\big((P$	$\wedge$	$\neg$	$Q)$	$\longrightarrow$	$(\neg$	$(P$	$\vee$	$R)$	$\longleftrightarrow$	$\neg$	$Q)\big)$
0	0	0			1					0			1	
0	0	1			1					1			1	
0	1	0			0					0			0	
0	1	1			0					1			0	
1	0	0			1					1			1	
1	0	1			1					1			1	
1	1	0			0					1			0	
1	1	1			0					1			0	

On passe ensuite aux sous-formules de hauteur 2. Il y en a deux : $P \wedge \neg Q$ et $\neg(P \vee R)$. On passe donc aux deux sous-colonnes correspondant à ces deux sous-formules :

P	Q	R	$\big((P$	$\wedge$	$\neg$	$Q)$	$\longrightarrow$	$(\neg$	$(P$	$\vee$	$R)$	$\longleftrightarrow$	$\neg$	$Q)\big)$
0	0	0		0	1			1		0			1	
0	0	1		0	1			0		1			1	
0	1	0		0	0			1		0			0	
0	1	1		0	0			0		1			0	
1	0	0		1	1			0		1			1	
1	0	1		1	1			0		1			1	
1	1	0		0	0			0		1			0	
1	1	1		0	0			0		1			0	

On passe ensuite aux sous-formules de hauteur 3. Là, cette fois, il n'y en a qu'une seule. Il s'agit de $\big(\neg(P \vee R) \longleftrightarrow \neg Q\big)$. Le tableau devient donc :

P	Q	R	$\big((P$	$\wedge$	$\neg$	$Q)$	$\longrightarrow$	$(\neg$	$(P$	$\vee$	$R)$	$\longleftrightarrow$	$\neg$	$Q)\big)$
0	0	0		0	1			1		0		1	1	
0	0	1		0	1			0		1		0	1	
0	1	0		0	0			1		0		0	0	
0	1	1		0	0			0		1		1	0	
1	0	0		1	1			0		1		0	1	
1	0	1		1	1			0		1		0	1	
1	1	0		0	0			0		1		1	0	
1	1	1		0	0			0		1		1	0	

On arrive enfin à la formule elle-même puisqu'elle est de hauteur 4. En s'appuyant sur les colonnes coloriées en bleu foncé, pour le dernier connecteur, nous obtenons la table de vérité suivante :

P	Q	R	$\big((P$	$\wedge$	$\neg$	$Q)$	$\longrightarrow$	$(\neg$	$(P$	$\vee$	$R)$	$\longleftrightarrow$	$\neg$	$Q)\big)$
0	0	0		0	1		1	1		0		1	1	
0	0	1		0	1		1	0		1		0	1	
0	1	0		0	0		1	1		0		0	0	
0	1	1		0	0		1	0		1		1	0	
1	0	0		1	1		0	0		1		0	1	
1	0	1		1	1		0	0		1		0	1	
1	1	0		0	0		1	0		1		1	0	
1	1	1		0	0		1	0		1		1	0	

9 Tautologies et contradictions

***Résumé* № 13** *Les formules vraies dans tous les modèles possibles sont appelées* tautologies. *Les formules fausses dans tous les modèles possibles sont appelées* contradictions.

※

Une tautologie est une formule vraie dans tout modèle possible. Autrement dit, aucun modèle ne permet de l'invalider. Elle est toujours vraie, quelles que soient les circonstances.

Définition 88 *Soit ϕ une formule du Calcul Propositionnel,*

$$\phi \text{ est une tautologie ssi pour tout modèle } \mathcal{M},\ \mathcal{M} \vDash \phi.$$

Notation 89 *On dénote par $\top$ ("top", "true") une formule vraie dans tout modèle ; Et $\bot$ ("bottom", "false") une formule qui n'est vraie dans aucun modèle.*

Ou pour le dire autrement, ϕ est une tautologie si et seulement si $\phi \equiv \top$; elle est donc universellement valide.

Remarque 90 Il y a un lien très fort entre la notion de tautologie et celle d'équivalence : deux formules ϕ et ψ sont équivalentes si et seulement si la formule $\phi \longleftrightarrow \psi$ est une tautologie.

Définition 91 *Soit $\phi \in \mathcal{F}$*

$$\phi \text{ est une contradiction ssi } \neg\phi \text{ est une tautologie.}$$
$$i.e.\ \phi \text{ est une contradiction ssi } \phi \equiv \bot.$$

Une contradiction est donc une formule qui est fausse dans tout modèle possible, elle n'a par conséquent pas de modèle, ce qui correspond à la notion intuitive de contradiction comme quelque chose qui ne peut jamais avoir lieu. Du point de vue logique, une contradiction est quelque chose qui ne peut jamais être réalisée, si l'on entend par réalisation d'une formule son interprétation dans un modèle qui la satisfait, c'est-à-dire dans lequel elle est vraie.

Exemples 92 les formules suivantes sont des tautologies :

(1) idempotence de la conjonction et de la disjonction

(a) $(P \wedge P) \longleftrightarrow P$ (b) $(P \vee P) \longleftrightarrow P$

(2) commutativité de la conjonction, disjonction et de la double implication

(a) $(P \vee Q) \longleftrightarrow (Q \vee P)$

(b) $(P \wedge Q) \longleftrightarrow (Q \wedge P)$

(c) $(P \longleftrightarrow Q) \longleftrightarrow (Q \longleftrightarrow P)$

(3) associativité de la disjonction, de la conjonction et de la double implication

(a) $((P \vee Q) \vee R) \longleftrightarrow (P \vee (Q \vee R))$

(b) $((P \wedge Q) \wedge R) \longleftrightarrow (P \wedge (Q \wedge R))$

(c) $((P \longleftrightarrow Q) \longleftrightarrow R) \longleftrightarrow (P \longleftrightarrow (Q \longleftrightarrow R))$

(4) distributivité de la disjonction par rapport à la conjonction et réciproquement

(a) $(P \vee (Q \wedge R)) \longleftrightarrow ((P \vee Q) \wedge (P \vee R))$

(b) $(P \wedge (Q \vee R)) \longleftrightarrow ((P \wedge Q) \vee (P \wedge R))$

(5) lois d'absorption

(a) $(P \wedge (P \vee Q)) \longleftrightarrow P$ (b) $(P \vee (P \wedge Q)) \longleftrightarrow P$

(6) lois de De Morgan

(a) $\neg(P \vee Q) \longleftrightarrow (\neg P \wedge \neg Q)$ (b) $\neg(P \wedge Q) \longleftrightarrow (\neg P \vee \neg Q)$

(7) contraposée

(a) $(P \longrightarrow Q) \longleftrightarrow (\neg Q \longrightarrow \neg P)$

(8) version sémantique de l'absurde classique[14]

(a) $\neg\neg P \longleftrightarrow P$ (b) $(P \longrightarrow Q) \longleftrightarrow (\neg P \vee Q)$.

Le dual de la notion de tautologie est parfois appelé du vieux nom d'antilogie, d'autres fois de celui de contradiction.

Remarque 93 Un raisonnement consiste généralement à partir d'une tautologie et à cheminer par implication jusqu'à la formule désirée. Comme le point de départ, c'est-à-dire la prémisse de notre suite d'implications, est une tautologie (donc une formule vraie dans n'importe quel modèle), chaque conséquence d'une implication est également une tautologie. Par conséquent, la formule finale est elle-même une tautologie. Ou pour le dire autrement, un raisonnement (pour autant qu'il soit valide) chemine généralement de tautologie en tautologie.

Dans le *raisonnement par l'absurde* – encore appelé *preuve par l'absurde* ou *preuve par contradiction* – la notion de contradiction joue un rôle primordial. Dans ce type de raisonnement, on souhaite montrer qu'une formule ϕ est une tautologie.

14. Voir le chapitre sur la théorie de la démonstration à la page 200.

On procède comme suit : on suppose premièrement que ϕ n'est pas une tautologie et donc que $\neg\phi$ est vraie dans au moins un modèle. Puis, au terme d'une suite de déductions, on aboutit à une contradiction (ψ). Le raisonnement a donc montré que la supposition entraînait une contradiction. Pour être plus précis, on se retrouve avec le fait que *dans les modèles où* $\neg\phi$ *est vraie*, la formule $\neg\phi \longrightarrow \psi$ est également vraie puisque le raisonnement est valide. Or cette formule est équivalente à la formule $\neg\neg\phi \vee \psi$, elle-même équivalente à $\phi \vee \bot$, puisque ψ est une contradiction. Finalement, la formule $\phi \vee \bot$ est trivialement équivalente à ϕ, ce qui montre que *dans les modèles où* $\neg\phi$ *est vraie*, la formule ϕ est vraie. Par conséquent, il n'y a pas de modèle où $\neg\phi$ est vraie. C'est donc que $\neg\phi$ est une contradiction, d'où l'on déduit immédiatement que ϕ est une tautologie.

En suivant ce raisonnement, nous trouvons la tautologie suivante : $\neg\phi \longrightarrow \psi$. Il s'agit bien d'une tautologie, puisque dans les modèles où $\neg\phi$ est fausse, la formule $\neg\phi \longrightarrow \psi$ est vraie chaque fois ; et dans ceux où $\neg\phi$ est vraie, le raisonnement a montré qu'on aboutissait à ψ, qui est toujours fausse.

10 Formes normales

***Résumé* № 14** *Etant donnée une formule ϕ, ses formes normales sont de la forme $\phi_{\wedge,\vee}$ et $\phi_{\vee,\wedge}$. Elles satisfont $\phi_{\wedge,\vee} \equiv \phi_{\vee,\wedge} \equiv \phi$ et répondent au souhait suivant : quel que soit le modèle $\mathcal{M}$, dans le jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi_{\vee,\wedge})$ le* **V**érificateur *choisit d'abord, le* **F**alsificateur *ensuite, puis le jeu s'arrête. Dans le jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi_{\wedge,\vee})$, le* **F**alsificateur *choisit d'abord, le* **V**érificateur *ensuite, puis le jeu s'arrête.*

※

Ce que l'on appelle généralement *forme normale*, c'est simplement la présentation d'un objet sous un aspect plus alléchant, sous une forme plus sympathique. Transcrire une formule sous une forme normale consistera donc, pour nous, à la mettre à disposition dans un habit attrayant de simplicité. Pour le dire encore autrement, nous allons remplacer cette formule par une formule équivalente dont les connecteurs sont joliment disposés, bien proprement rangés, magnifiquement ordonnés.

10.1 Forme normale disjonctive

Supposons que l'on se donne un ensemble fini de variables propositionnelles : $\{P_1, \dots, P_n\}$ ainsi qu'un modèle $\mathcal{M}$ du Calcul Propositionnel – par conséquent, une distribution de valeurs de vérité δ sur ces variables $P_1, \dots, P_n$. On aimerait trouver une formule ϕ qui contienne toutes ces variables (et elles seules) et ne soit vraie que dans ce seul modèle $\mathcal{M}$. A ce problème, il y a une réponse toute simple :

$$\phi = (\varepsilon_0 P_0 \wedge \varepsilon_1 P_1 \wedge \dots \wedge \varepsilon_n P_n) = \bigwedge_{1 \leq i \leq n} \varepsilon_i P_i.$$

Où ε_i désigne "$\neg$" si $\delta(P_i) = 0$ et $\not\neg$ si $\delta(P_i) = 1$ avec pour convention $\not\neg P = P$.

Une manière de décrire la formule ϕ ci-dessus est de dire que sa table de vérité ne comporte que des 0 sauf sur la ligne correspondant aux valeurs de $P_1, \dots, P_n$ définies par δ.

Exemple 94 Soit $\mathcal{M} = \delta$ avec $\delta(P) = \delta(Q) = \delta(S) = \delta(U) = \delta(W) = 1$ et $\delta(R) = \delta(T) = \delta(V) = 0$,

la formule suivante n'est vraie que dans ce seul modèle (parmi les 2^8 modèles possibles) :

$$(P \wedge Q \wedge \neg R \wedge S \wedge \neg T \wedge U \wedge \neg V \wedge W).$$

Progressons à présent dans notre raisonnement en considérant toujours un ensemble fini de variables propositionnelles : $\{P_1, \dots, P_n\}$. Choisissons parmi les 2^n modèles possibles un certain nombre d'entre eux $\{\mathcal{M}_i \colon\ i \in I\}$. On aimerait maintenant se doter d'une formule ϕ qui contienne uniquement ces variables propositionnelles et dont les modèles soient précisément ceux que l'on s'est donné. Ou pour le dire autrement, nous recherchons ϕ qui soit vraie dans tous les modèles $\mathcal{M}_i$ pour $i \in I$ et fausse dans tous les autres.

$$\mathcal{M} \models \phi \quad \text{ssi} \quad \text{il existe } i \in I \;\; \mathcal{M} = \mathcal{M}_i$$

Là encore, nous avons une réponse toute trouvée puisque nous savons déjà, pour chaque modèle $\mathcal{M}_i$, écrire une formule ϕ_i qui ne soit vraie que dans ces seuls modèles. Il nous suffit d'écrire :

$$\phi = \bigvee_{i \in I} \phi_i.$$

Exemple 95 Soit

(1) $\mathcal{M}_1 = \delta_1$ avec $\delta_1(P) = \delta_1(Q) = 1$ et $\delta_1(R) = 0$,

(2) $\mathcal{M}_2 = \delta_2$ avec $\delta_2(P) = 1$ et $\delta_2(Q) = \delta_2(R) = 0$,

(3) $\mathcal{M}_3 = \delta_3$ avec $\delta_3(Q) = 1$ et $\delta_3(P) = \delta_3(R) = 0$,

la formule suivante n'est vraie que dans ce seul modèle (parmi les $2^3 = 8$ modèles possibles) :

$$(\ P \ \wedge \ Q \ \wedge \ \neg R\ ) \vee (\ P \ \wedge \ \neg Q \ \wedge \ \neg R\ ) \vee (\ \neg P \ \wedge \ Q \ \wedge \ \neg R\ ).$$

En fait, sans nous en rendre compte, nous venons en chemin de démontrer le théorème suivant :

Théorème 96

Pour tout ϕ il existe ψ sous forme normale disjonctive telle que $\phi \equiv \psi$.

Définition 97 *Une formule ϕ est sous forme normale disjonctive (en abrégé* FND*) s'il existe :*

(1) un entier $k \geq 1$,

(2) des entiers $n_1, \ldots, n_k$,

(3) et pour chaque $i \in \{1, 2, \ldots, k\}$ il existe :

(a) n_i variables propositionnelles : $P_{i,j_1}, \ldots, P_{i,j_{n_i}}$,

(b) n_i éléments : $\varepsilon_{i,j_1}, \ldots, \varepsilon_{i,j_{n_i}}$ parmi $\{\neg, \not\neg\}$

tels que :

$$\phi = \bigvee_{1 \leq i \leq k} (\bigwedge_{1 \leq j \leq n_i} \varepsilon_{i,j} P_{i,j})$$

(où par convention $\not\neg P = P$).

Preuve du Théorème 96 : Avant tout, traitons le cas de ϕ lorsque celle-ci n'a pas de modèles. Dans ce cas, ϕ est équivalente à n'importe quelle contradiction, par exemple $P \wedge \neg P$. Au contraire, lorsque ϕ admet au moins un modèle, il suffit de considérer la table de vérité de la formule ϕ et de relever les modèles dans lesquels cette formule est vraie, pour ensuite procéder comme nous l'avons fait au début de cette section.

⊣ 96

10.2 Forme normale conjonctive

Nous venons de voir que toute formule pouvait être mise sous forme normale disjonctive (en abrégé *FND*), c'est-à-dire sous forme d'une disjonction de conjonctions de littéraux. Un littéral étant soit une formule atomique, soit la négation d'une formule atomique. Il est possible de faire de même en inversant disjonctions et conjonctions.

Définition 98 *Une formule ϕ est sous forme normale conjonctive s'il existe :*

(1) un entier $k \geq 1$,

(2) des entiers $n_1, \dots, n_k$,

(3) et pour chaque $i \in \{1, 2, \dots, k\}$ il existe :

(a) n_i variables propositionnelles : $P_{i,j_1}, \dots, P_{i,j_{n_i}}$,

(b) n_i éléments : $\varepsilon_{i,j_1}, \dots, \varepsilon_{i,j_{n_i}}$ parmi $\{\neg, \not\neg\}$

tels que :

$$\phi = \bigwedge_{1 \leq i \leq k} \left(\bigvee_{1 \leq j \leq n_i} \varepsilon_{i,j} P_{i,j} \right)$$

(où par convention $\not\neg P = P$).

Nous remarquons que nous avons le même genre de résultat pour les formes normales conjonctives (en abrégé *FND*) que pour les formes normales disjonctives.

Théorème 99

Pour toute formule ϕ, il existe ψ sous FNC telle que $\phi \equiv \psi$.

Preuve du Théorème 99 : Nous allons donner deux preuves différentes de ce théorème. La première est similaire à celle du théorème précédent sur les FND. Elle est donc sémantique au sens où l'on regarde les modèles d'une formule pour conclure. La seconde est syntaxique, elle est basée sur quelques règles de réécriture.

(1) Soit ϕ la formule à mettre sous FNC, dont les variables propositionnelles sont $P_1, \dots, P_n$. Considérons $\{\mathcal{M}_i \colon\ i \in I\}$ l'ensemble des modèles dans lesquels cette formule est *fausse*. Si cet ensemble est vide, alors ϕ est une tautologie et $\psi = \top$ marche. Sinon, considérons pour chaque i dans I, la formule :

$$\begin{aligned} \psi &= \neg(\varepsilon_1 P_1 \wedge \varepsilon_2 P_2 \wedge \cdots \wedge \varepsilon_k P_k) \\ &= (\varepsilon_1 \neg P_1 \vee \varepsilon_2 \neg P_2 \vee \cdots \vee \varepsilon_k P_k) \\ &= \bigvee\nolimits_{1 \leq j \leq k} \bar{\varepsilon_j} P_j \end{aligned}$$

$$\begin{array}{lllllll} \text{où} & \bar{\varepsilon_i} & \neg & \text{ssi} & \mathcal{M}_i \models P_i & \text{ssi} & \varepsilon_i = \not\neg \\ & \bar{\varepsilon_i} & \not\neg & \text{ssi} & \mathcal{M}_i \not\models P_i & \text{ssi} & \varepsilon_i = \neg \end{array}$$

Par construction, la formule ψ_i est vraie dans tous les modèles possibles de ϕ, à l'exception de $\mathcal{M}_i$. Ainsi la formule $\psi = \bigwedge_{i \in I} \psi_i$ est vraie dans tous les modèles possibles, à l'exception de tous les $\mathcal{M}_i$ pour i appartenant à I. Autrement dit, ψ est vraie dans tous les modèles de ϕ :

$$\mathcal{M} \models \psi \text{ ssi } \mathcal{M} \models \phi$$

ce qui signifie bien $\psi \equiv \phi$.

(2) La seconde preuve repose sur un jeu de réécriture, lui-même défini à partir de substitutions de formules équivalentes. C'est d'ailleurs une méthode qui pourra tout aussi bien être utilisée pour mettre une formule sous forme normale disjonctive.

L'idée est la suivante :

(a) on part de ϕ qui est écrite dans le langage du Calcul Propositionnel, donc potentiellement ϕ recèle les connecteurs "$\longrightarrow$" et "$\longleftrightarrow$". La première chose à faire consiste à se passer d'eux. Pour cela, on utilise (par exemple) les équivalences suivantes :

(A) $\varphi_0 \longrightarrow \varphi_1 \equiv \neg\varphi_0 \vee \varphi_1$

(B) $\varphi_0 \longleftrightarrow \varphi_1 \equiv (\neg\varphi_1 \vee \varphi_0) \wedge (\neg\varphi_0 \vee \varphi_1)$.

Cela permet de transformer ϕ en la formule ϕ' qui ne comporte plus que des connecteurs parmi $\{\neg, \vee, \wedge\}$.

(b) On peut également, et ce, à chaque étape, se passer des doubles négations puisque $\neg\neg\varphi$ est équivalent à φ.

Exemple 100 Soit $\phi = \neg((\neg P \longrightarrow Q) \longrightarrow \neg(Q \longleftrightarrow P))$,

$$\begin{aligned}
\phi &\equiv \neg(\neg(\neg P \longrightarrow Q) \vee \neg(Q \longleftrightarrow P)) \\
&\equiv \neg(\neg(\neg\neg P \vee Q) \vee \neg(Q \longleftrightarrow P)) \\
&\equiv \neg(\neg(\neg\neg P \vee Q) \vee \neg((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
&\equiv \neg(\neg(P \vee Q) \vee \neg((\neg Q \vee P) \wedge (\neg P \vee Q)).
\end{aligned}$$

(c) On peut ensuite utiliser les lois de De Morgan pour faire entrer les négations à l'intérieur des formules :

- $\neg(\varphi_0 \vee \varphi_1) \equiv \neg\varphi_0 \wedge \neg\varphi_1$
- $\neg(\varphi_0 \wedge \varphi_1) \equiv \neg\varphi_0 \vee \neg\varphi_1$.

Exemple 101 Soit $\phi = \neg(\neg(P \vee Q) \vee \neg((\neg Q \vee P) \wedge (\neg P \vee Q))$,

$$\begin{aligned}
\phi &\equiv \neg\neg(P \vee Q) \wedge \neg\neg((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
&\equiv (P \vee Q) \wedge ((\neg Q \vee P) \wedge (\neg P \vee Q)) \\
&\equiv (P \vee Q) \wedge (\neg Q \vee P) \wedge (\neg P \vee Q).
\end{aligned}$$

En répétant ce processus, on se retrouve avec une formule ϕ'' dont tous les symboles de négation sont placés devant une variable propositionnelle et dont les seuls connecteurs binaires sont parmi $\{\vee, \wedge\}$.

(d) Il ne reste plus qu'à distribuer la disjonction par rapport à la conjonction en utilisant :

$$\varphi_0 \vee (\varphi_1 \wedge \varphi_2) \equiv (\varphi_0 \vee \varphi_1) \wedge (\varphi_0 \vee \varphi_2)$$

et le tour est joué...

Bien sûr, il est souvent nécessaire de répéter de nombreuses fois cette opération de distribution de la disjonction par rapport à la conjonction, mais il est clair qu'à chacune de ces opérations, les symboles "$\vee$" *descendent* dans l'arbre de la formule, pour finalement ne plus relier entre eux que des littéraux.

Une preuve en bonne et due forme de ce théorème se fait par induction sur la hauteur de la formule ϕ considérée. On montre que la propriété est vraie pour les formules de hauteur 0, ce qui est évident. Puis on considère que ϕ est de hauteur $n+1$ en supposant que toutes les formules de hauteur n peuvent se mettre sous FNC. Il faut alors considérer les différents cas possibles pour ϕ : négation, disjonction, conjonction, implication et double implication, chacun d'eux renvoyant à de multiples sous-cas. La preuve est longue et ennuyeuse, mais facile et surtout correcte.

$\dashv$ 99

Remarque 102 Le même argument que précédemment *mutatis mutandis* permet d'obtenir une formule sous FND. Il suffit, en effet, au lieu d'appliquer la distributivité de la disjonction par rapport à la conjonction, d'appliquer la distributivité inverse :

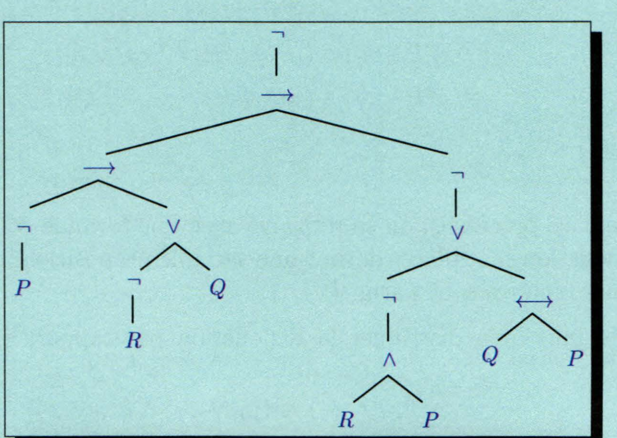
$$\varphi_0 \wedge (\varphi_1 \vee \varphi_2) \equiv (\varphi_0 \wedge \varphi_1) \vee (\varphi_0 \wedge \varphi_2).$$

Ainsi, au lieu de faire *rentrer* le "$\vee$" et faire *sortir* le "$\wedge$", on fait l'inverse. Pour le reste, le processus est identique.

A noter également que si, au lieu de partir d'une formule quelconque, on part d'une formule déjà sous FNC, alors on obtient une formule sous FND en n'appliquant que cette seule règle de distributivité du "$\wedge$" par rapport au "$\vee$".

Exemple 103 Considérons la formule ci-dessous (sous forme linéaire et arborescente) :

$$\phi := \neg((\neg P \longrightarrow (\neg R \vee Q)) \longrightarrow \neg((\neg(R \wedge P) \vee (Q \longleftrightarrow P)))).$$



$$
\begin{aligned}
\phi &\equiv \neg(\neg(\neg P \longrightarrow (\neg R \vee Q)) \vee \neg((\neg(R \wedge P) \vee (Q \longleftrightarrow P)))) \\
&\equiv \neg(\neg(\neg\neg P \vee (\neg R \vee Q)) \vee \neg((\neg(R \wedge P) \vee (Q \longleftrightarrow P)))) \\
&\equiv \neg(\neg(\neg\neg P \vee (\neg R \vee Q)) \vee \neg((\neg(R \wedge P) \vee ((\neg Q \vee P) \wedge (\neg P \vee Q))))) \\
&\equiv \neg(\neg(\neg\neg P \vee (\neg R \vee Q)) \vee \neg(((\neg R \vee \neg P) \vee ((\neg Q \vee P) \wedge (\neg P \vee Q))))) \\
&\equiv \neg(\neg(P \vee (\neg R \vee Q)) \vee \neg(((\neg R \vee \neg P) \vee ((\neg Q \vee P) \wedge (\neg P \vee Q))))) \\
&\equiv (\neg\neg(P \vee (\neg R \vee Q)) \wedge \neg\neg(((\neg R \vee \neg P) \vee ((\neg Q \vee P) \wedge (\neg P \vee Q))))) \\
&\equiv ((P \vee \neg R \vee Q) \wedge (((\neg R \vee \neg P) \vee ((\neg Q \vee P) \wedge (\neg P \vee Q))))) \\
&\equiv ((P \vee \neg R \vee Q) \wedge (((\neg R \vee \neg P) \vee (\neg Q \vee P)) \wedge (((\neg R \vee \neg P) \vee (\neg P \vee Q))))) \\
&\equiv (P \vee \neg R \vee Q) \ \wedge \ (\neg R \vee \neg P \vee \neg Q \vee P) \ \wedge \ (\neg R \vee \neg P \vee \neg P \vee Q) \quad \hookleftarrow\mathbf{FNC} \\
&\equiv (P \vee \neg R \vee Q) \ \wedge \ \top \ \wedge \ (\neg R \vee \neg P \vee Q) \quad \hookleftarrow\mathbf{FNC} \\
&\equiv (P \vee \neg R \vee Q) \ \wedge \ (\neg R \vee \neg P \vee Q) \quad \hookleftarrow\mathbf{FNC} \\
&\equiv ((P \vee \neg R \vee Q) \ \wedge \ \neg R) \ \vee \ ((P \vee \neg R \vee Q) \ \wedge \ \neg P) \ \vee \ ((P \vee \neg R \vee Q) \ \wedge \ Q) \\
&\equiv (P \wedge \neg R) \ \vee \ (\neg R \wedge \neg R) \ \vee \ (Q \wedge \neg R) \ \vee \ (P \wedge \neg P) \ \vee \ (\neg R \wedge \neg P) \\
&\qquad \vee (Q \wedge \neg P) \ \vee \ (P \wedge Q) \ \vee \ (\neg R \wedge Q) \ \vee \ (Q \wedge Q) \quad \hookleftarrow\mathbf{FND} \\
&\equiv (P \wedge \neg R) \vee \neg R \vee (Q \wedge \neg R) \vee (\neg R \wedge \neg P) \vee (Q \wedge \neg P) \vee (P \wedge Q) \vee Q \quad \hookleftarrow\mathbf{FND} \\
&\equiv \neg R \ \vee \ (Q \wedge \neg P) \ \vee \ (P \wedge Q) \ \vee \ Q \quad \hookleftarrow\mathbf{FND} \\
&\equiv \neg R \ \vee \ Q \quad \hookleftarrow\mathbf{FND}\,.
\end{aligned}
$$

11 Les connecteurs binaires

***Résumé* № 15** *Passage en revue des 16 connecteurs binaires possibles.*

※

Par abus de langage, on parle de la table de vérité du connecteur "$\wedge$" pour désigner la table de vérité de la formule $P \wedge Q$. De même, on parle de la table de vérité du connecteur "$\vee$" pour désigner celle de la formule $P \vee Q$. Ce procédé se généralise à n'importe quel connecteur. Ainsi, si $*$ est un connecteur n-aire, on parlera de la table de vérité du connecteur $*$ pour désigner en fait la table de vérité de la formule $*(P_1, \ldots, P_n)$. Par exemple, la table de vérité de la négation est la table de vérité de $\neg P$:

P	$\neg$
0	1
1	0

La table de vérité de "$\longrightarrow$" est celle de $P \longrightarrow Q$:

P	Q	$\longrightarrow$
0	0	1
0	1	1
1	0	0
1	1	1

Si l'on songe maintenant à un connecteur *binaire* quelconque, que nous appelons $*$, sa table de vérité témoigne de la valeur de $*(P, Q)$ - formule que l'on note généralement $P * Q$ plutôt que $*(P, Q)$ lorsqu'on a affaire à un connecteur binaire - dans les modèles possibles. Comme les variables propositionnelles P et Q peuvent prendre chacune deux valeurs, cela fait donc quatre modèles à considérer. Et comme également, dans chaque modèle, la formule $P * Q$ peut prendre la valeur 0 ou 1, cela nous donne $2^4 = 16$ possibilités pour la table de vérité de ce connecteur binaire. Autrement dit, il y a exactement 16 connecteurs binaires différents. Voici leurs tables de vérité résumés en un seul et unique tableau :

P	Q	$\bot$	$\not\vee$	$\not\longleftarrow$	$\not\pi_1$	$\not\longrightarrow$	$\not\pi_2$	$\not\longleftrightarrow$	$\not\wedge$	$\wedge$	$\longleftrightarrow$	π_2	$\longrightarrow$	π_1	$\longleftarrow$	$\vee$	$\top$
0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

Que remarque-t-on ?

- Tout d'abord, on retrouve les quatre connecteurs binaires que nous utilisons depuis le début de ce chapitre ($\vee$, $\wedge$, $\longrightarrow$, $\longleftrightarrow$).

Mais également le dual de chacun d'eux ($\not\vee$, $\not\wedge$, $\not\longrightarrow$, $\not\longleftrightarrow$), c'est-à-dire les opposés exacts des précédents, ceux qui prennent la valeur exactement inverse dans un même modèle. Pour être tout à fait précis, on a l'équivalence suivante entre un connecteur et son dual :

$$P \not* Q \equiv \neg(P * Q).$$

- On trouve aussi l'implication inverse ($\longleftarrow$) avec son dual ($\not\longleftarrow$).
- On trouve également un connecteur ($\top$) qui prend toujours la valeur 1. On l'appelle d'ailleurs $\top$ pour *true*, car il donne toujours le Vrai dans n'importe quel modèle. Et puis il y a son dual ($\perp$) qui prend toujours la valeur 0 dans n'importe quel modèle. Il est par conséquent associé au Faux.
- Et finalement, on trouve les deux connecteurs – π_1, π_2 – qui donnent à la formule $P * Q$, respectivement la valeur de P et la valeur de Q, ainsi que leurs duaux – $\not\pi_1$, $\not\pi_2$.

Remarque 104 Chacun des 16 connecteurs binaires peut être exprimé par une formule du Calcul Propositionnel. Ou pour le dire plus précisément, à chaque connecteur binaire $*$ correspond une ou plusieurs formules du Calcul Propositionnel ϕ (avec pour seule variable propositionnelle P et Q), telle que $P * Q$ et ϕ sont équivalentes. Ce qui revient à dire que tout ce qui peut être exprimé en utilisant ces connecteurs, peut également l'être en n'utilisant que ceux du Calcul Propositionnel.

Exemples 105

(1) $P \perp Q \equiv P \longleftrightarrow \neg P$

(2) $P \not\vee Q \equiv \neg(P \vee Q)$

(3) $P \not\longrightarrow Q \equiv \neg(P \longrightarrow Q)$

(4) $P \not\pi_1 Q \equiv \neg P$

(5) $P \not\longleftarrow Q \equiv \neg(Q \longrightarrow P)$

(6) $P \not\pi_2 Q \equiv \neg Q$

(7) $P \not\longleftrightarrow Q \equiv \neg(P \longleftrightarrow Q)$

(8) $P \not\wedge Q \equiv \neg(P \wedge Q)$

(9) $P \longleftarrow Q \equiv Q \longrightarrow P$

(10) $P \top Q \equiv P \longleftrightarrow P$

(11) $P \pi_1 Q \equiv P$

(12) $P \pi_2 Q \equiv Q$

On peut donc aisément déduire de ce qui précède que pour n'importe quelle formule écrite en utilisant la négation et n'importe lesquels de ces connecteurs, on peut trouver une formule écrite avec les seuls connecteurs du Calcul Propositionnel ($\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow$) qui lui soit totalement équivalente.

Un résultat encore plus intéressant nous attend. Ce que nous venons de faire pour les connecteurs binaires peut également être entrepris pour les connecteurs d'arités supérieures quelconques. On peut très bien imaginer des connecteurs n-aires pour un entier n quelconque. Un connecteur n-aire est simplement quelque chose qui prend n formules et vous en rend une. La seule petite différence réside dans la manière de les écrire. En effet, avec les connecteurs unaires (c'est-à-dire pour nous la négation), nous écrivions le connecteur juste devant la formule, tandis qu'avec les connecteurs binaires, nous disposions ceux-ci entre les deux formules qu'ils reliaient. Là, il nous faut imaginer un autre artifice. Mais l'idée du connecteur reste la même, le connecteur relie toujours des formules. On peut par exemple utiliser la notation $\$(P_1, \ldots, P_n)$, c'est là simplement le même genre de notation que si l'on écrivait $\neg(P)$ au lieu de $\neg P$ ou $\vee(P, Q)$ au lieu de $P \vee Q$. Dès lors, donner l'interprétation sémantique de ce connecteur revient tout simplement à procurer sa table de vérité.

Si l'on définit tous les connecteurs d'arité quelconque que l'on souhaite, et qu'ensuite on forme la formule de notre choix avec tous ces connecteurs (en les réutilisant à volonté), alors cette formule obtenue est toujours équivalente à une formule du Calcul Propositionnel. La raison de tout cela réside dans la remarque suivante :

Trouver une formule ϕ du Calcul Propositionnel équivalente à une formule quelconque γ, c'est trouver une formule qui ait exactement les mêmes modèles que γ. Il suffit simplement que ϕ décrive ces modèles et rien que ceux-là pour obtenir le résultat escompté. Dans le cas particulier où la formule γ n'a pas de modèle, n'importe quelle formule ϕ qui est une contradiction fait l'affaire.

Supposons que les variables propositionnelles de γ soient $P_1, P_2, P_3, P_4, P_5, P_6$ et imaginons que $\mathcal{M}$ soit un modèle de γ ($\mathcal{M} \models \gamma$) dans lequel P_2 et P_5 sont faux et toutes les autres variables vraies. La formule suivante n'est vraie que dans ce seul modèle de ϕ (parmi les 2^6 modèles possibles :

$$\phi_{\mathcal{M}} = \Big(P_1 \wedge \neg P_2 \wedge P_3 \wedge P_4 \wedge \neg P_5 \wedge P_6\Big).$$

Maintenant, considérons $\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_n$ une énumération de tous les modèles de ϕ (tous les $\mathcal{M}_i$ tels que $\mathcal{M}_i \models \gamma$) et formons la disjonction des formules $\phi_{\mathcal{M}_i}$ pour tous ces modèles, on obtient alors une formule qui est vraie dans un modèle possible de γ si et seulement si γ est vraie dans ce modèle :

$$\phi = \bigvee_{1 \leq i \leq n} \phi_{\mathcal{M}_i}.$$

Notation 106

- $\top$ *(pour "True") désigne le connecteur 0-aire (cela signifie qu'il ne prend pas de formule et vous en rend une) que l'on* **interpète toujours par 1**.
- $\bot$ *désigne le dual de* $\top$, *c'est donc le connecteur 0-aire que l'on* **interpète toujours par 0**.

12 Systèmes complets de connecteurs

***Résumé* № 16** *Un système de connecteurs est complet s'il permet, à équivalence près, d'engendrer toute formule. Il est de plus minimal si aucun connecteur ne peut en être retiré sans détruire la complétude du système. Les systèmes* $\{\neg, \wedge\}$, $\{\neg, \vee\}$ *et* $\{\neg, \longrightarrow\}$ *sont complets minimaux. Les deux seuls connecteurs binaires, qui chacun engendre un système complet, sont les barres de Sheffer disjonctive et conjonctive* $\not\wedge, \not\vee$. *Les règles du jeu d'évaluation associé à la barre de Sheffer conjonctive déterminent un jeu alternant parfait, le* **V**érificateur *commençant la partie. Celles du jeu associé à la barre de Sheffer disjonctive sont rigoureusement les mêmes, le* **F**alsificateur *débutant la partie.*

※

Nous avons vu qu'étant donné un ensemble de connecteurs quelconques, n'importe quelle formule écrite dans ce langage pouvait être équivalente à une formule du Calcul Propositionnel. Cela signifie que tout ce que l'on peut exprimer dans le cadre de la logique propositionnelle peut l'être également sous la forme du Calcul Propositionnel (basé sur le système de connecteurs $\{\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\}$) que nous avons choisi.

Mais nous avons en fait beaucoup mieux que cela, puisque nous savons qu'une formule du Calcul Propositionnel est toujours équivalente, non seulement à une formule écrite avec pour seuls connecteurs "$\neg$" et "$\vee$", mais aussi à une formule écrite avec pour tous connecteurs "$\neg$" et "$\wedge$".

Est-ce que cette propriété est encore vérifiée si l'on ne considère plus que "$\vee$" ou bien plus que "$\wedge$" ? La réponse est négative et nous allons voir pourquoi.

Définition 107 *Soit* $\{\$_1, \ldots, \$_k\}$ *un ensemble de connecteurs d'arités quelconques,*

(1) $\{\$_1, \ldots, \$_k\}$ *est un système complet ssi pour toute formule* $\phi \in \mathcal{F}$, *il existe une formule* γ *écrite dans le langage* $VAR \cup \{\$_1, \ldots, \$_k\} \cup \{), (\}$ *telle que*

$$\phi \equiv \gamma$$

(2) $\{\$_1, \ldots, \$_k\}$ *est un système complet minimal si aucun sous-ensemble strict* $A \subsetneq \{\$_1, \ldots, \$_k\}$ *n'est un système complet de connecteurs.*

Remarques 108

(1) $\{\neg, \vee\}$ est un système complet de connecteurs.

(2) $\{\neg, \wedge\}$ est un système complet de connecteurs.

(3) $\{\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\}$ est un système complet de connecteurs, mais ce n'est pas un système complet minimal puisque $\{\neg, \vee\}$ en est un sous-ensemble strict qui est un système complet de connecteurs.

Proposition 109

(1) $\{\neg, \vee\}$ *est un système complet minimal de connecteurs.*

(2) $\{\neg, \wedge\}$ *est également un système complet minimal de connecteurs.*

(3) $\{\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\}$ *est un système complet de connecteurs, mais ce n'est pas un système complet minimal puisque* $\{\neg, \vee\}$ *en est un sous-ensemble strict qui est un système complet de connecteurs.*

Preuve de la Proposition 109 : Les preuves de (1) et (2) sont rigoureusement les mêmes, en intervertissant "$\vee$" et "$\wedge$". Nous prouvons donc uniquement (1). Il nous suffit de montrer qu'aucun sous-ensemble strict de $\{\neg, \vee\}$ n'est un système complet. Nous étudions donc les différents cas, les seuls sous-ensembles de $\{\neg, \vee\}$ étant :

(1) $\{\ \} = \emptyset$: dans ce cas, le résultat est évident puisque les seules formules que l'on peut construire avec ce système de connecteurs sont les variables propositionnelles. Or, il est par exemple rigoureusement impossible de trouver une formule qui ne soit qu'une variable propositionnelle R et soit équivalente à $P \vee Q$. Puisque dans tous les cas ($R = P$, ou bien $R = Q$, ou bien encore $R \neq P, Q$), la formule $R \longleftrightarrow (P \vee Q)$ n'est pas une tautologie :

   (a) si $R = P$, considérer le modèle dans lequel P est faux, alors que Q est vrai,

   (b) si $R = Q$, considérer le modèle dans lequel Q est faux, alors que P est vrai,

   (c) si $R \neq P, Q$, considérer n'importe quel modèle dans lequel R est faux, alors que P est vrai.

(2) $\{\neg\}$: ce cas est très semblable au précédent, puisqu'une formule écrite avec ce système de connecteurs est de la forme $\underbrace{\neg \ldots \neg}_{n} R$.

   Elle est donc elle-même équivalente à R si elle contient un nombre pair de symbole de négation, et à $\neg R$ si elle en contient un nombre impair. Il nous suffit de trouver une formule du Calcul Propositionnel qui ne puisse être équivalente à une formule de la forme R ou $\neg R$. La même formule $P \vee Q$ convient tout à fait :

   (a) si $R = P$:

      (A) si le nombre de négation est pair : considérer le modèle dans lequel P est faux, alors que Q est vrai,

      (B) si le nombre de négation est impair : considérer n'importe quel modèle dans lequel P est vrai.

   (b) si $R = Q$:

      (A) si le nombre de négation est pair : considérer le modèle dans lequel Q est faux, alors que P est vrai,

      (B) si le nombre de négation est impair : considérer n'importe quel modèle dans lequel Q est vrai.

   (c) si $R \neq P, Q$:

(A) si le nombre de négation est pair : considérer n'importe quel modèle dans lequel R est faux, alors que P est vrai.

(B) si le nombre de négation est impair : considérer n'importe quel modèle dans lequel R est vrai, alors que P est vrai.

(3) $\{\vee\}$: ce cas est un peu plus compliqué car nous pouvons créer une infinité de formules non équivalentes, deux à deux, avec ce seul connecteur. Mais nous allons montrer que nous ne pouvons pas créér de formule équivalente à $\neg P$. Remarquons tout d'abord que les seules formules que nous pouvons construire sont de la forme $(P_1 \vee \ldots \vee P_k)$. Procédons alors par l'absurde, c'est-à-dire que nous allons supposer le contraire : il existe une formule $(P_1 \vee \ldots \vee P_k)$ équivalente à $\neg P$. Il suffira de considérer un modèle dans lequel $P, P_1 \ldots P_k$ sont toutes vraies pour obtenir une contradiction.

$\dashv$ 109

Nous avons donc trouvé un système à deux connecteurs qui soit non seulement complet, mais aussi minimal. Existe-t-il un ensemble qui ne contienne qu'un seul connecteur et soit complet (et donc nécessairement minimal) ? Il apparaît clairement que s'il en existe un, ce ne peut pas être un connecteur unaire. Qu'en est-t-il des connecteurs binaires ? La réponse est positive : il y en a en fait deux.

Définition 110 *Les connecteurs binaires* $\not\vee$ *et* $\not\wedge$ *sont appelés, respectivement,* barre de Sheffer disjonctive *et* barre de Sheffer conjonctive, *ils sont définis par :*

(1) $P \not\vee Q \equiv \neg(P \vee Q)$,

(2) $P \not\wedge Q \equiv \neg(P \wedge Q)$.

Ces connecteurs sont appelés barre de Sheffer, car ils sont souvent notés sous forme d'une barre verticale. Nous préférons les noter $\not\vee$ et $\not\wedge$ afin de mieux représenter ce qu'ils signifient.

Proposition 111

(1) $\{\not\vee\}$ *est un système complet minimal.*

(2) $\{\not\wedge\}$ *est également un système complet minimal.*

Preuve de la Proposition 111 : Les deux cas se traitent de manière similaire. Nous allons considérer simplement le cas de la barre de Sheffer conjonctive. Le caractère minimal est immédiat, il nous suffit donc de montrer que $\{\not\vee\}$ est un système complet. Il nous faut montrer que pour toute formule $\phi \in \mathcal{F}$, il existe une formule ψ écrite avec pour seul connecteur $\not\vee$. Pour faciliter la preuve, on peut déjà supposer, sans perte de généralité, que la formule ϕ ne comporte que la négation et la disjonction pour seuls connecteurs logiques. (Nous pouvons effectivement faire cette supposition car $\{\neg, \vee\}$ est un système complet). La preuve se déroule par induction sur la hauteur des formules :

(1) Si ϕ est de hauteur 0, alors $\phi = P$ et la formule $(P \not\vee P) \not\vee (P \not\vee P)$ convient tout à fait puisque nous avons :

$$\begin{aligned}
(P \not\vee P) \not\vee (P \not\vee P) &\equiv \neg((P \not\vee P) \vee (P \not\vee P)) \\
&\equiv \neg(P \not\vee P) \\
&\equiv \neg\neg(P \vee P) \\
&\equiv \neg\neg P \\
&\equiv P.
\end{aligned}$$

(2) Nous supposons maintenant que la propriété que nous voulons montrer est vérifiée de toutes les formules de hauteur au plus n. Nous cherchons à montrer qu'elle est alors également vérifiée pour des formules de hauteur $n+1$. Soit donc ϕ de hauteur $n+1$. Nous devons distinguer deux cas :

(a) Si $\phi = \neg\varphi$: par hypothèse d'induction, puisque φ est de hauteur n, elle est équivalente à une formule ψ' qui ne s'écrit qu'avec le connecteur $\not\vee$. La formule $\psi' \not\vee \psi'$ convient puisque :

$$\begin{aligned}
\psi' \not\vee \psi' &\equiv \neg(\psi' \vee \psi') \\
&\equiv \neg\psi' \\
&\equiv \neg\varphi \\
&\equiv \phi.
\end{aligned}$$

(b) Si $\phi = \phi_0 \vee \phi_1$: par hypothèse d'induction, puisque ϕ_0 et ϕ_1 sont de hauteur au plus n, elles sont équivalentes respectivement à ϕ_0' et ϕ_1', deux formules qui ne s'écrivent qu'avec le connecteur $\not\vee$. La formule $(\phi_0' \not\vee \phi_1') \not\vee (\phi_0' \not\vee \phi_1')$ convient puisque :

$$\begin{aligned}
(\phi_0' \not\vee \phi_1') \not\vee (\phi_0' \not\vee \phi_1') &\equiv \neg((\phi_0' \not\vee \phi_1') \vee (\phi_0' \not\vee \phi_1')) \\
&\equiv \neg(\phi_0' \not\vee \phi_1') \\
&\equiv \neg\neg(\phi_0' \vee \phi_1') \\
&\equiv \phi_0' \vee \phi_1' \\
&\equiv \phi_0 \vee \phi_1 \\
&\equiv \phi
\end{aligned}$$

$\dashv$ 111

Cette preuve conclut l'étude des systèmes complets de connecteurs et avec elle, celle de la sémantique du Calcul Propositionnel. Ce chapitre concernait la notion de modèle. Dans le chapitre suivant, nous nous intéresserons à la notion de preuve. Le but est ensuite de faire se rejoindre ces deux approches au travers du théorème de complétude (Théorème 139).

Pour aller plus avant :

La sémantique du Calcul Propositionnel telle que nous l'avons présentée – c'est-à-dire sous forme ludique ou *dynamique* par le biais de jeux d'évaluation, par opposition à la manière *statique* via les notions de distributions de valeurs de vérité étendues et de tables de vérité – fait partie de ce que l'on appelle la *sémantique des jeux*. Parmi les auteurs récents qui adoptent une telle approche, le lecteur pourra se reporter avec intérêt aux travaux de Johan van Benthem [vB01][vB03] [vB06]. Avant lui, la sémantique des jeux fut popularisée par Jaakko Hintikka [HS79]. Elle remonte encore plus avant, puisqu'elle trouve son origine dans la notion de *logique dialogique* – ou *"dialogische Logik"* en allemand – introduite dans les années 1950 par Paul Lorenzen et Kuno Lorenz [LL78].

Le lecteur qui souhaiterait pénétrer le vaste domaine que constitue la théorie des jeux pourra se référer à *"Game theory : a very short introduction"* de Ken Binmore [Bin07], *"Playing for Real : A Text on Game Theory"* de Ken Binmore [Bin12], *"Game theory. 1991"* de Drew Fudenberg et Jean Tirole [FT91], *"A primer in game theory"* de Robert Gibbons [Gib92], *"A course in game theory"* de Martin J. Osborne et Ariel Rubinstein [OR94], *"Theory of games and economic behavior "* de John von Neumann et Oskar Morgenstern [vNM07], *"An introduction to game theory"* de Martin J. Osborne [Osb04].

Le lecteur curieux retrouvera, dans la plupart des manuels de logique traitants du Calcul Propositionnel, les résultats entrevus dans ce chapitre. S'il souhaite aiguiser son appétit, il pourra le frotter aux ouvrages suivants : *"Intermediate logic"* de David Bostock [Bos97], *"Mathematical logic"* de Ian Chiswell et Wilfrid Hodges [CH07], *"Introduction to Mathematical Logic"* d'Alonzo Church [Chu96], *"Logique mathématique, tome 1 : Calcul propositionnel; algèbre de Boole; calcul des prédicats"* de René Cori et Daniel Lascar [CLK03a], *"La logique ou l'art de raisonner"* de Yannis Delmas-Rigoutsos et René Lalement [DRL00], *"Einführung in die mathematische Logik"* de Heinz-Dieter Ebbinghaus, Jörg Flum et Wolfgang Thomas [EFT78], *"A mathematical introduction to logic"* de Herbert B. Enderton [End72], *"A first course in logic : an introduction to model theory, proof theory, computability, and complexity"* de Shawn Hedman [Hed04], *"Mathematical Logic"* de Stephen C. Kleene [Kle67], *"Introduction to mathematical logic"* d'Elliot Mendelson [Men97], *"Mathematical logic : a first course"* de Joel W. Robbin [Rob69], *"An introduction to formal logic"* de Peter Smith [Smi03], *"Introduction à la logique"* d'Alfred Tarski [Tar69], *"Mathematical logic"* de George Tourlakis [Tou11b], *"Logique élémentaire : cours de base pour informaticien"* de Jacques Zahnd [Zah98].

Enfin et pour des raisons historiques, nous recommandons au lecteur philosophe tourné vers Kant de jeter un œil à *"Sur la logique et la théorie de la science"* de Jean Cavaillès [Cav47].

Tout autre chose, parmi les applications de la logique, il en est une relativement immédiate : la résolution d'énigmes. En règle général, leurs résolutions passent par le fait d'expliciter l'ensembles des modèles possibles à considérer, puis à éliminer ceux qui ne satisfont pas telle ou telle condition de l'énigme. Les livres de Raymond M. Smullyan recèlent d'énigmes à foison : *"This book needs no title : a budget of living paradoxes"* [Smu86], *"What is The Name of This Book ?(The Riddle of Dracula and Other Logic Puzzles)"* de Raymond M. Smullyan [Smu11b], mais encore *"The Lady or the Tiger ? : and Other Logic Puzzles"* [Smu09a], *"Alice in puzzle-land : A Carrollian tale for children under eighty"* [Smu11a], *"To Mock a Mockingbird : and other logic puzzles including an amazing adventure in combinatory logic"* [Smu00], *"Logical labyrinths"* [Smu09b].

Chapitre 3

Théorie de la démonstration

1 Avant-goûts sur la notion de preuve

Nous rappelons que, pour des raisons de lisibilité, nous omettons d'écrire les parenthèses extérieures dans les formules sous forme linéaire. Ainsi, nous écrivons par exemple $\phi \wedge \psi$ au lieu de $(\phi \wedge \psi)$, ou bien $\phi \longrightarrow (\phi \vee \neg \psi)$ au lieu de $(\phi \longrightarrow (\phi \vee \neg \psi))$.

Qu'est-ce qu'une argumentation, un raisonnement, une preuve ? Dans ce chapitre, nous répondons à la question "qu'est-ce qu'une preuve ?", "en quoi consiste une démonstration ?", "comment se déroule un raisonnement ?" "comment se construit une argumentation ?". Nous faisons même mieux que simplement définir ce qu'est une démonstration, on en explicite la théorie. Ainsi, la démonstration elle-même devient un objet d'étude, un objet sur lequel nous allons nous pencher pour en étudier la nature.

Intuitivement, une preuve est un argument qu'un interlocuteur propose à quelqu'un pour le convaincre de la véracité d'une assertion. Cet argument repose sur un certain nombre d'hypothèses admises par les différents protagonistes. Donc une preuve est un objet :

- de longueur finie,
- vérifiable par des moyens mécaniques rudimentaires,
- qui comporte une conclusion,
- s'appuyant sur des hypothèses.

Autrement dit, une preuve repose sur l'usage de règles de déductions simples, appliquées en chaîne à des hypothèses, pour aboutir à une conclusion.

Nous allons dans un deuxième temps nous intéresser à ces règles de déductions simples et exprimer de manière formelle ce qu'est une preuve et ce qu'est une démonstration en logique propositionnelle. Mais avant cela, nous allons entrer dans un premier temps en contact avec ce qui se joue de manière *informelle* dans les argumentations, les raisonnements que nous rencontrons quotidiennement.

Quelques exemples d'argumentation

Prenons tout de suite un exemple d'argumentation – de type démonstratif – emprunté à *"Critical Thinking : A concise guide"* de Tracy Bowell et Gary Kemp [BK10] que nous présentons ici traduite en français.

"Une fois de plus, nous devons faire face à l'attitude sordide des jeunes s'adonnant à la boisson en centre ville et se révélant un facteur de chaos. Les récents troubles à l'ordre public perpétrés à York étaient parmi les pires que nous ayons connus. Cela se produit tellement souvent qu'il semble maintenant que les gens en soient réduits à hausser les épaules et accepter de telles prouesses comme un fait de la vie, ou une loi de la nature.

Alors, devons-nous simplement nous résigner à accepter cela ? En sommes-nous réduits à accepter que nos jeunes perdent les meilleures années de leur vie à se conduire en voyous ? Devons-nous rester les bras croisés ?

Pour ma part je ne le crois pas. D'autant qu'il y a une solution toute trouvée. Tournons-nous en effet vers un vieux remède afin de traiter un mal nouveau : le service militaire obligatoire. Puisqu'on enseignerait à ces jeunes des habitudes de discipline et qu'on les formerait à l'esprit communautaire, il est évident que ces jeunes gens seraient bien moins sujets à créer toute sorte de troubles lorsqu'ils en auraient fini avec la vie militaire."[1]

Lorsqu'on tente de reconstruire l'argumentation d'un texte comme celui-ci, la première chose que l'on fait consiste à se débarrasser des oripeaux sans rapport avec le raisonnement. C'est le cas par exemple des expressions du type *"Tournons-nous en effet vers un vieux remède... "* ou de *"... il y a une solution toute trouvée"*. Cela permet de retrouver la structure argumentative de ce discours qui fonctionne comme une sorte de squelette du raisonnement. Nous pouvons en effet dégager les deux hypothèses ou prémisses suivantes qui mènent à une première conclusion intermédiaire :

(P1) Si les jeunes britanniques parvenaient à acquérir des habitudes de discipline et un esprit communautaire, alors le problème de l'alcoolisme et de l'hooliganisme serait réduit.

(P2) S'ils effectuaient leur service militaire, les jeunes britanniques parviendraient à acquérir des habitudes de discipline et un esprit communautaire.

(C1) Si les jeunes britanniques effectuaient leur service militaire, le problème de l'alcoolisme et de l'hooliganisme parmi eux serait réduit.

Cette première conclusion intermédiaire est ensuite utilisée comme prémisse ou hypothèse pour, mise en rapport avec une troisième hypothèse, mener à la conclusion finale.

(C1) Si les jeunes britanniques parvenaient à acquérir des habitudes de discipline et un esprit communautaire, alors le problème de l'alcoolisme et de l'hooliganisme serait réduit.

(P3) Quelque chose doit être fait pour réduire le problème de l'alcoolisme et de l'hooliganisme parmi la jeunesse britannique.

(C2) La Grande-Bretagne devrait réintroduire le service militaire obligatoire pour les jeunes britanniques.

1. Extrait de *Critical Thinking : A concise guide* de Tracy Bowell et Gary Kemp.

Nous formaliserons ce raisonnement de la manière suivante : nous avons tout d'abord deux hypothèses **P1** et **P2** desquelles découle une première conclusion **C1**, nous écrirons cela

$$\mathbf{P1}\ ,\ \mathbf{P2} \vdash \mathbf{C1}$$

La première attitude à tenir face à une argumentation consiste à la dépouiller de son ornementation oratoire, puis en distinguer les hypothèses des conclusions. Ensuite, dans un deuxième temps, on pourra considérer la validité du raisonnement.

Mais restons encore un peu sur cette première phase de la structuration des arguments démonstratifs. Si vous entendez un ami vous dire *"Cette pauvre Carole s'est fait coincée en train de piquer dans la caisse. Elle est foutue"*. Vous reconstruirez l'argument comme suit, ce qui nécessite au préalable d'avoir désamorcé la rhétorique associée.

(P1) Si Carole est prise en flagrant délit pour le vol de l'argent de la société, alors elle sera licenciée.

(P2) Carole a été pris en flagrant délit pour le vol de l'argent de la société.

(C1) Carole sera licenciée.

En plus de désamorcer la rhétorique, il nous faut également, dans la reconstruction d'arguments, faire intervenir des énoncés qui ne sont pas explicitement présents. Ils sont pourtant nécessaires à la bonne compréhension de l'argument. Un exemple de tel *énoncé implicite* se trouve dans l'argumentation suivante :

– "Est-ce qu'Evelyne est une personne bien éduquée ?"
– "Bien évidemment ! Ne savez-vous pas qu'Evelyne est une femme politique réputée ?"

La reconstruction de l'argument fait apparaître un énoncé implicite : toute femme politique réputée est bien éduquée. Il se présente donc ainsi :

(P1) Evelyne est une femme politique réputée.

(P2) Toute femme politique réputée est bien éduquée.

(C1) Evelyne est bien éduquée.

Comme nous l'avons vu, il se peut aussi qu'un argument fasse intervenir des énoncés qui ne sont pas précis. C'est le cas des énoncés qui sont flous. C'est aussi le cas des énoncés qui sont ambigus. Le caractère vague ou flou d'un énoncé ne doit pourtant pas être confondu avec son ambiguïté. Un énoncé est ambigu s'il admet deux significations distinctes. C'est le cas par exemple de l'énoncé suivant :

Le président Obama a annulé son voyage en Suisse pour faire du ski.

Est-ce que le but du voyage d'Obama en Suisse était de skier ? Ou bien, le président a-t-il annulé son voyage en Suisse précisément parce qu'il souhaitait aller skier ?

Pour continuer avec les présidents des Etats-Unis, l'énoncé suivant joue sur le caractère flou, vague, imprécis de l'expression *"relations sexuelles"* :

"I want you to listen to me. I'm going to say this again : I did not have sexual relations with that woman, Miss Lewinsky."[2]

2. Bill Clinton, le 26 janvier 1998.

Cette phrase n'est pas ambiguë, elle ne prête pas à diverses interprétations contradictoires, mais le président de l'époque joue sur le caractère incertain, indéterminé de l'expression "*relations sexuelles*".

Lors d'un raisonnement, un type d'argument qui ne procède pas de la démonstration à proprement parlé intervient fréquemment. Il s'agit de l'argument *inductif*. Au contraire de l'argument déductif qui procède du général vers le particulier, celui-ci fonctionne à rebours : il procède du particulier vers le général. C'est le cas par exemple dans l'énoncé qui suit.

- *"Mon scarabée est passé au sèche-linge."*
- *"Il est mort."*
- *"Donc tous les scarabées meurent s'ils passent au sèche-linge."*

C'est le type d'argument que l'on retrouve lorsqu'on *induit* du fait qu'un certain échantillon de la population possède une propriété **P**, que tout individu de la population en question possède cette même propriété **P**. Si l'on voulait reconstruire un argument inductif sous forme de démonstration, il faudrait faire intervenir un facteur probabiliste dans l'attribution de la validité du raisonnement.

- *"Mon scarabée est passé au sèche-linge."*
- *"Il est mort."*
- *"Donc probablement tous les scarabées meurent s'ils passent au sèche-linge."*

La question serait alors celle de la probabilité de la conclusion. Quelle est la probabilité que je peux associer au fait que tous les scarabées meurent si on les passe au sèche-linge ?

La démonstration plus formellement

Venons-en maintenant à ce qui se joue au coeur de la notion de démonstration. Regardons tout d'abord les choses de manière intuitive. Nous verrons ensuite comment ces intuitions prennent formes lorsque nous étudierons le Calcul des Séquents.

Un raisonnement est constitué d'énoncés. Chaque énoncé est soit une destination, un objectif, un but à atteindre, soit au contraire une hypothèse, quelque chose qui est considéré comme donné et peut donc être utilisé dans la preuve. A tout moment d'un raisonnement, il est toujours de la plus grande importance de bien faire la distinction entre ce qui doit être prouvé (et il peut y avoir de multiples objectifs) et ce qui au contraire peut être utilisé dans la preuve. Si on ne porte pas suffisamment attention à cette distinction, on court le risque de prendre comme hypothèse ce qui précisément est à démontrer, ce qui rend la démonstration caduque.

Au début d'une démonstration, il y a un but unique et un certain nombre d'hypothèses. Mais ces hypothèses peuvent ensuite varier et l'objectif unique du départ se diviser en divers buts à atteindre.

C'est le cas par exemple des étapes suivantes, qui toutes subdivisent un but en fonction de sa forme logique. Si le but est de la forme :

$\longleftrightarrow$: on remplace ce but $\phi \longleftrightarrow \psi$ par les deux buts $\phi \longrightarrow \psi$ et $\psi \longrightarrow \phi$.

$\longrightarrow$: deux directions sont alors possibles :

- on remplace le but $\phi \longrightarrow \psi$ par le but ψ tout en ajoutant l'énoncé ϕ à notre liste d'hypothèses. Cela signifie que pour démontrer un argument de la forme "Si A, alors B", je suppose A et je cherche à démontrer B.
- Ou bien on remplace tout simplement le but $\phi \longrightarrow \psi$ par sa *contraposée* $\neg\psi \longrightarrow \neg\phi$. Pour montrer "Si A, alors B", je cherche à montrer "Si non B, alors non A".

$\wedge$: on remplace le but $\phi \wedge \psi$ par les deux buts ϕ et ψ.

$\vee$: deux directions sont alors possibles :
- soit on remplace le but $\phi \vee \psi$ par le but ϕ et l'on ajoute l'énoncé $\neg\psi$ aux hypothèses.
- soit on remplace le but $\phi \vee \psi$ par le but ψ et l'on ajoute l'énoncé $\neg\phi$ aux hypothèses.

$\neg$: deux directions sont également possibles :
- soit on remplace le but $\neg\phi$ par un nouveau but en "rentrant" le symbole de négation à l'intérieur de ϕ à l'aide des lois de De Morgan.
- soit on remplace le but $\neg\phi$ par le but $\perp$ – c'est-à-dire que l'on cherche à obtenir une contradiction – et on ajoute aux hypothèses l'énoncé ϕ. Autrement dit, pour montrer la négation d'un énoncé, je suppose cet énoncé et je cherche à obtenir une contradiction.

$\perp$: il s'agit du cas où l'objectif est une contradiction. C'est typiquement ce qui apparaît lorsque la démonstration procède par *l'absurde*. Dans ce cas, l'objectif est de montrer à la fois une formule et sa négation. On cherche donc à montrer à la fois ϕ et $\neg\phi$ pour une formule ϕ bien choisie.

Il faut ajouter à ces différentes utilisations du but d'une démonstration, celui qui découle de la démonstration par l'absurde. Dans ce type de démonstration, pour montrer un but ϕ – et ce quel que soit la forme de ce but – on ajoute simplement l'hypothèse $\neg\phi$ aux hypothèses et on remplace le but ϕ par le nouveau but $\perp$, c'est-à-dire la contradiction.

Comment pouvons-nous également utiliser les hypothèses au cours d'une démonstration ? De manière similaire à ce que nous venons de voir pour les objectifs, nous distinguons l'usage que nous faisons des hypothèses en fonction de leur forme logique. Si une hypothèse est de la forme :

$\longleftrightarrow$: on remplace l'hypothèse $\phi \longleftrightarrow \psi$ par les deux hypothèses $\phi \longrightarrow \psi$ et $\psi \longrightarrow \phi$.

$\longrightarrow$: deux directions sont alors possibles à partir de l'hypothèse $\phi \longrightarrow \psi$.
- soit on dispose du but ψ et on remplace alors le but ψ par le but ϕ.
- soit on dispose également de l'hypothèse ϕ et on ajoute alors ψ aux hypothèses.

$\wedge$: on remplace l'hypothèse $\phi \wedge \psi$ par les deux hypothèses ϕ et ψ.

$\vee$: on utilise l'hypothèse $\phi \vee \psi$ afin de prouver le but courant θ, en prouvant ce dernier par deux fois :
- une première fois en prenant ϕ comme hypothèse,
- une seconde fois en prenant ψ comme hypothèse.

$\neg$: on remplace l'hypothèse $\neg\phi$ par une nouvelle hypothèse en "rentrant" le symbole de négation à l'intérieur de ϕ à l'aide des lois de De Morgan.

Après ce petit préambule qui faisait appel à ce qui se joue intuitivement lorsque nous effectuons une démonstration, revenons maintenant vers la notion de preuve en un sens plus formel et tachons d'entrevoir ce qui se joue dans l'entre-deux, entre démonstration d'une part et conséquence sémantique d'autre part.

La notion de preuve ou de démonstration se situe du côté de ce que nous appellerons la *vérité syntaxique*, par opposition à la notion de vérité que nous connaissions jusque-là, qui elle, fait intervenir les modèles d'une formule ou d'une théorie : c'est la *vérité sémantique*.

Ainsi, prenons une théorie finie quelconque $\mathcal{T}$ et une formule ϕ. Dire que la formule ϕ est vraie dans la théorie $\mathcal{T}$ a deux significations, suivant que l'on s'occupe du champ sémantique ou du champ syntaxique. La formule ϕ est vraie – au sens sémantique du mot - dans la théorie $\mathcal{T}$, si elle est vraie dans tous les modèles de la théorie $\mathcal{T}$. Nous notons cela $\mathcal{T} \models \phi$. C'est la notion de vérité qui correspond à la conséquence logique, que l'on pourrait désormais rebaptiser *conséquence logique sémantique*, pour insister sur le fait qu'elle ne se réfère qu'aux modèles.

Il existe un autre type de conséquence logique : la *conséquence logique syntaxique*. On dira que la formule ϕ est une conséquence syntaxique de la théorie $\mathcal{T}$ si elle se déduit de $\mathcal{T}$, c'est-à-dire s'il existe une preuve – encore appelée démonstration - de ϕ sur la base des hypothèses contenues dans la théorie $\mathcal{T}$. On notera $\mathcal{T} \vdash \phi$ le fait que ϕ est prouvable dans la théorie $\mathcal{T}$. C'est la notion de *vérité syntaxique*. Il n'y a donc plus de modèles auxquels on se réfère, ils ont disparu et on ne s'intéresse plus qu'à la syntaxe de la formule en question, à celle des différentes formules qui composent la théorie $\mathcal{T}$, et on applique un tout petit nombre fini de règles de déductions étonnantes de simplicité.

La notion de vérité syntaxique que constitue la démonstration repose ainsi sur un jeu de réécriture, bien éloigné de l'univers des modèles possibles.

Un problème survient alors immédiatement : qu'en est-il de la relation entre ces deux notions de vérité ? Il est clair que l'on souhaite que ces deux notions coïncident. Cela signifie que si je peux déduire la formule ϕ de la théorie $\mathcal{T}$ (par des procédés syntaxiques), je souhaite également que dans ce cas, la formule ϕ soit une conséquence logique sémantique de la théorie $\mathcal{T}$, c'est-à-dire qu'elle soit vraie dans tous les modèles de $\mathcal{T}$. Autrement dit, on veut que $\mathcal{T} \vdash \phi$ entraîne $\mathcal{T} \models \phi$. Mais on souhaite également la réciproque : si $\mathcal{T} \models \phi$ alors $\mathcal{T} \vdash \phi$, c'est-à-dire si ϕ est une conséquence logique sémantique de $\mathcal{T}$, si elle est vérifiée dans tous les modèles de $\mathcal{T}$, alors elle doit être prouvable à partir des hypothèses contenues dans cette théorie.

Tout cela revient donc à dire que les règles de déduction, les règles de démonstration que nous devons mettre en place doivent être rigoureusement choisies pour atteindre cet objectif. Le but ultime d'un système de règles de démonstration est d'obtenir la coïncidence entre vérité syntaxique et vérité sémantique :

$$\mathcal{T} \models \phi \text{ si et seulement si } \mathcal{T} \vdash \phi.$$

En particulier, si l'on considère la théorie vide, c'est-à-dire la théorie qui n'a aucune formule, on veut qu'une formule soit une tautologie si et seulement si elle est prouvable sans utiliser d'hypothèses. Cela se note :

$$\models \phi \text{ si et seulement si } \vdash \phi.$$

Les différents systèmes de démonstration

Nous distinguerons trois familles de systèmes de démonstration différents pour le Calcul Propositionnel.

(1) les Systèmes axiomatiques,

(2) la Déduction Naturelle,

(3) le Calcul des Séquents.

Nous devons ces deux derniers systèmes à la même personne : Gerhard Gentzen, le Calcul des Séquents étant postérieur à la Déduction Naturelle de quelques années. Ces deux systèmes sont apparus au début des années 1930. Ils reposent tous deux sur la notion de séquents que nous introduirons prochainement. Le premier, comme son nom l'indique, présente la notion de démonstration de manière tout à fait naturelle, tandis que le second a été mis en place pour dégager des propriétés structurelles de la notion même de démonstration.

Les systèmes axiomatiques, quant à eux, sont dus au célébre mathématicien David Hilbert. Ils sont presque aussi nombreux que les ouvrages qui les mentionnent et se rapprochent beaucoup de la pratique mathématique. Ils sont définis à partir de schémas d'axiomes et de quelques règles de démonstration. Par contre, ils ne reposent pas sur la notion de séquent et ne s'appuient donc pas sur la dualité hypothèses/conclusion.

Pour aller plus avant :

Il existe, dans le monde anglo-saxon, de nombreux ouvrages traitant de *"critical thinking"*, que l'on traduit parfois en français par "esprit critique". Dans ces ouvrages, il s'agit en fait de mentionner des usages et concepts logiques, sans nécessairement faire appel à une quelconque formalisation. Dans ce préambule à la théorie de la démonstration, nous nous sommes largement inspiré de l'ouvrage *"Critical thinking : A concise guide"* de Tracey Bowell et Gary Kemp [BK10]. Le lecteur, qui souhaiterait investiguer le domaine du raisonnement informel, pourra se reporter au livre *boîte à outils* de Julian Baggini et Peter S. Fosl : *"The Philosopher's Toolkit : A compendium of philosophical concepts and methods"* [BF11], ainsi qu'à l'ouvrage destiné plutôt à un public scientifique : *"How to prove it : a structured approach"* de Daniel J. Velleman [Vel06]. Mais également aux ouvrages suivants : *"De la logique à l'argumentation"* de Jean-Blaise Grize [Gri82a], la *"Logique de l'argumentation"* de Pierre Blackburn [Bla02] ou encore *"Thinking from A to Z"* de Nigel Warburton [War07].

---

2 Les systèmes axiomatiques

***Résumé* № 17** *Les systèmes axiomatiques possèdent l'avantage de la concision. Par contre, ils sont très éloignés de la pratique de la démonstration. Ils apportent une manière d'établir la vérité, mais non d'étudier les processus à l'oeuvre dans la construction effective de cette vérité.*

※

Ces systèmes ont été construits sur le modèle des systèmes axiomatiques dont raffolent les mathématiciens. Ils ont l'avantage de fournir une formalisation très simple de la notion de démonstration. En effet, on se donne un petit nombre de vérités élémentaires (les axiomes) et de constructions qui préservent la vérité (les règles). Ici, une démonstration ressemble à la preuve d'un théorème en mathématiques. Ces systèmes de preuve sont une manière d'établir la vérité, et non de découvrir ou d'étudier des méthodes pour manipuler la vérité (au contraire de la Déduction Naturelle ou du Calcul des Séquents).

Nous allons donner un exemple d'une telle théorie axiomatique. Afin de simplifier les choses de manière notoire, nous allons travailler uniquement avec les seuls connecteurs $\longrightarrow$ et $\neg$. Il est clair que $\{\longrightarrow, \neg\}$ forme un système complet de connecteurs (minimal de surcroît). En effet, il suffit de remarquer que $\neg\phi \longrightarrow \psi$ est équivalent à $\phi \vee \psi$, et que $\{\vee, \neg\}$ est un système complet.

Axiomes

(1) $\phi \longrightarrow (\psi \longrightarrow \phi)$

(2) $(\phi \longrightarrow (\psi \longrightarrow \theta)) \longrightarrow ((\phi \longrightarrow \psi) \longrightarrow (\phi \longrightarrow \theta))$

(3) $(\neg\psi \longrightarrow \neg\phi) \longrightarrow ((\neg\psi \longrightarrow \phi) \longrightarrow \psi)$.

Règle

Le seul *modus ponens* : de ϕ et $\phi \longrightarrow \psi$ on déduit ψ.

Une déduction de la formule φ à partir d'un ensemble de formules Γ, est une suite finie de formules $\langle \varphi_0, \varphi_1, \ldots, \varphi_n \rangle$ telle que :

- chaque φ_i vérifie l'une des trois conditions suivantes :
  - φ_i est un axiome,
  - φ_i est une hypothèse ($\varphi_i \in \Gamma$),
  - φ_i est obtenu à partir de l'application de la règle du *modus ponens* à deux formules d'indices inférieurs φ_j et φ_k $(j, k < i)$.
- $\varphi_n = \varphi$.

Exemple 112 Sans hypothèse, c'est-à-dire à partir d'un ensemble vide d'hypothèses ($\Gamma = \emptyset$), une démonstration de la formule $\varphi \longrightarrow \varphi$ dans ce système prend la forme suivante :

(1) $(\varphi \longrightarrow ((\varphi \longrightarrow \varphi) \longrightarrow \varphi)) \longrightarrow ((\varphi \longrightarrow (\varphi \longrightarrow \varphi)) \longrightarrow (\varphi \longrightarrow \varphi))$ (*Axiome* 2)

(2) $\varphi \longrightarrow ((\varphi \longrightarrow \varphi) \longrightarrow \varphi)$ (*Axiome* 1)

(3) $(\varphi \longrightarrow (\varphi \longrightarrow \varphi)) \longrightarrow (\varphi \longrightarrow \varphi)$ (*modus ponens* 1-2)

(4) $\varphi \longrightarrow (\varphi \longrightarrow \varphi)$ (*Axiome* 1)

(5) $\varphi \longrightarrow \varphi$. (*modus ponens* 3-4)

Remarque 113 La démonstration de la formule $\varphi \longrightarrow \varphi$ dans l'Exemple 112 semble totalement arbitraire. En effet, elle ne nous dit rien sur la formule que l'on démontre, à savoir sur $\varphi \longrightarrow \varphi$. Il manque donc une chose essentielle que l'on aimerait voir présente dans toute démonstration : une explication du pourquoi ce que l'on a démontré est vrai, une explicitation des raisons qui font que notre formule est vraie. Dans ces systèmes axiomatiques, il n'y a pas de renseignement direct sur ce qui est démontré. Tout cela semble très loin de l'usage que l'on fait de la démonstration. En un mot, ces systèmes axiomatiques ne rendent pas compte de l'aspect usuel de la démonstration.

Pour aller plus avant :

Le lecteur qui souhaiterait plonger de plein pied dans les systèmes de Hilbert pourra consulter avec délices le livre original de 1928 de Hilbert et Ackermann, intitulé *"Grundzüge der Theoretischen Logik"* [HA28], ou sa traduction anglaise remontant à 1950 : *"Principles of mathematical logic"* [HAL50]. Il pourra également retrouver ces systèmes dans l'ouvrage *"Introduction to mathematical logic"* d'Elliot Mendelson [Men97], ainsi que dans *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00].

---

3 la Déduction Naturelle

Résumé **№ 18** *La Déduction Naturelle fait reposer la notion de démonstration sur l'agencement de règles simples, si proches de la pratique démonstrative qu'elle s'intitule "naturelle".*
Le coeur de ce système de démonstration est le séquent – $\Gamma \vdash \phi$ – dans lequel un ensemble d'hypothèses – Γ – prouve une formule ϕ. Une démonstration est un arbre dont les nœuds sont des séquents, la racine étant le séquent démontré, et les feuilles, des axiomes. Les relations entre un nœud de l'arbre et ses successeurs étant définies par une petite vingtaine de règles, chacune d'elles est composée de prémisses et d'un séquent conclusion de la règle. Il existe un ensemble de règles minimal dont l'emploi donne lieu à la logique minimale. *En lui adjoignant la règle de l'absurde intuitionniste qui affirme que d'hypothèses menant à une contradiction, il est possible de déduire n'importe quelle formule, on obtient l'ensemble des règles de la* logique intuitionniste. *En remplaçant la règle de l'absurde intuitionniste par l'absurde classique – si à partir d'hypothèses et supposant fausse une formule, on arrive à une contradiction, alors cette formule se déduit de ces hypothèses – on obtient la* logique classique *dont la particularité est de coïncider sur le plan* syntaxique *à la sémantique naturelle du Calcul Propositionnel. Ainsi une formule est conséquence sémantique d'une théorie si et seulement si elle est conséquence syntaxique de cette même théorie pour la logique classique.*

$$\mathcal{T} \models \phi \quad ssi \quad \mathcal{T} \vdash_c \phi.$$

※

Définition 114 *Un séquent (noté $\Gamma \vdash \phi$) est un couple où :*

- Γ *est un ensemble fini de formules,*
- ϕ *est une formule.*

Remarque 115

- Γ représente les hypothèses que l'on peut utiliser.
- ϕ est la conclusion du séquent. C'est intuitivement la formule que l'on veut démontrer.
- Le signe $\vdash$ se lit "démontre" ou "prouve".
- Si $\Gamma = \emptyset$, on notera $\vdash \phi$ au lieu de $\emptyset \vdash \phi$.
- Si $\Gamma = \{\phi_0, \ldots, \phi_k\}$, on pourra noter $\phi_0, \ldots, \phi_k \vdash \phi$ au lieu de $\{\phi_0, \ldots, \phi_k\} \vdash \phi$.
- De même, si $\Gamma_1, \ldots, \Gamma_k$ sont des ensembles finis de formules, on pourra noter $\Gamma_1, \ldots, \Gamma_k \vdash \phi$ au lieu de $\Gamma_1 \cup \Gamma : 2 \cup \ldots \cup \Gamma_k \vdash \phi$.
- On notera finalement $\Gamma, \psi \vdash \phi$ au lieu de $\Gamma \cup \{\psi\} \vdash \phi$.

Définition 116

- *Un séquent est* prouvable *(ou* démontrable*, ou* dérivable*) s'il peut être obtenu par une application finie de règles de démonstration.*
- *Une formule ϕ est prouvable si le séquent $\vdash \phi$ est prouvable.*

Remarque 117

- $\Gamma \vdash \phi$ représente à la fois le séquent et la phrase $\Gamma \vdash \phi$ *est prouvable.* Mais il n'y a en général pas d'ambiguité.
- On écrit $\Gamma \nvdash \phi$ pour $\Gamma \vdash \phi$ *n'est pas prouvable.*

Les règles de démonstration sont les briques de base qui permettent de construire les dérivations. Une dérivation formelle est un assemblage fini de règles. La manière la plus courante et la plus parlante de représenter cet assemblage est un arbre, pour la simple raison que l'on est amené sans cesse à effectuer des branchements de bouts de démonstrations les uns sur les autres.

Dans la pratique, entre autres dans l'activité mathématique, on utilise d'autres règles, mais toutes peuvent se déduire des règles de démonstration propement dites. Pour cette raison, elles sont appelées règles dérivées.

Anatomie d'une règle

(1) Chaque règle est composée :
   - d'un ensemble de *prémisses* (il peut y en avoir 0, 1, 2 ou 3). Chacune de ces prémisses étant un séquent.
   - d'un séquent *conclusion* de la règle.
   - d'une barre horizontale séparant les prémisses (en haut) de la conclusion (en bas). Et sur la droite de la barre, le nom de la règle est indiqué en abrégé.

Exemple 118 Une règle de démonstration.

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\wedge i$$

(2) Une règle se lit de haut en bas : si on a prouvé les prémisses, alors on a également prouvé la conclusion. Mais elle a également une signification si on la lit de bas en haut : afin de prouver la conclusion, il me faut chercher à prouver les prémisses.

(3) A chaque connecteur logique correspondent deux types de règles :

   (a) les règles d'*introduction* qui permettent de prouver une formule dont ce connecteur est l'opérateur principal.

   (b) les règles d'*élimination* qui permettent d'utiliser dans les prémisses une formule ayant ce connecteur comme opérateur principal.

(4) On ne considère que les seuls connecteurs $\neg, \wedge, \vee, \longrightarrow$, étant entendu que les formules du genre $\phi \longleftrightarrow \psi$ correspondent à $(\phi \longrightarrow \psi) \wedge (\psi \longrightarrow \phi)$.

Les règles En dehors des axiomes représentés par le séquent $\phi \vdash \phi$, le système a deux sortes de règles : des règles logiques (subdivisées en règles d'introduction et en règles d'élimination des différents connecteurs) et des règles structurelles qui permettent de manipuler les hypothèses, d'en décrire précisément la gestion (l'affaiblissement permettant d'ajouter de nouvelles hypothèses et la contraction permettant de confondre deux occurrences d'une même hypothèse).

Axiome

$$\frac{}{\phi \vdash \phi}\,{\scriptstyle ax}$$

Un séquent, dans lequel la conclusion est aussi l'hypothèse, est prouvable.

Introduction de la conjonction

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\,{\scriptstyle \wedge i}$$

Si l'on a montré ϕ et par ailleurs ψ, alors on a montré $\phi \wedge \psi$.

Elimination de la conjonction

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\,{\scriptstyle \wedge e_g} \qquad\qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\,{\scriptstyle \wedge e_d}$$

De $\phi \wedge \psi$, on peut déduire d'une part ϕ, et d'autre part ψ.

Introduction de l'implication

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \rightarrow \psi}\,{\scriptstyle \rightarrow i}$$

Pour prouver $\phi \longrightarrow \psi$, il suffit de prendre ϕ comme hypothèse et de prouver ψ.

Elimination de l'implication (*modus ponens*)

$$\frac{\Gamma \vdash \phi \rightarrow \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\,{\scriptstyle \rightarrow e}$$

Si l'on a prouvé ϕ et, par ailleurs, $\phi \longrightarrow \psi$, alors on a prouvé ψ. Ou encore, pour démontrer ψ, il suffit de montrer à la fois $\phi \longrightarrow \psi$ et ϕ.

Introduction de la négation

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg \phi}\,{\scriptstyle \neg i}$$

Pour montrer $\neg\phi$, il suffit de montrer une contradiction en supposant ϕ.

Elimination de la négation

$$\frac{\Gamma \vdash \neg\phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \bot}\ {\scriptstyle \neg e}$$

Si on a montré à la fois ϕ et $\neg\phi$, alors on a montré une contradiction.

On verra plus loin que $\neg\phi$ est équivalent (au sens syntaxique comme au sens sémantique) à $\phi \longrightarrow \bot$, on aurait donc pu se passer de ces deux règles concernant la négation.

Introduction de la disjonction

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\ {\scriptstyle \vee i_g} \qquad\qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\ {\scriptstyle \vee i_d}$$

Cette règle peut paraître très étrange car la conclusion est clairement plus faible que la prémisse. Pourtant, il est de nombreux raisonnements dans lesquels on a besoin d'affaiblir la conclusion, ne serait-ce que pour la faire coïncider avec la prémisse d'une autre règle. Par exemple, si vous avez un ticket restaurant, vous savez que pour payer ce menu il vous faut ou bien un ticket restaurant, ou bien 10 CHF. Vous allez déduire du fait que vous avez un ticket restaurant, le fait que vous avez ou un ticket restaurant ou 10 CHF, ce qui va vous permettre d'obtenir le repas souhaité. Ou encore, dans la pratique mathématique, il est courant d'avoir une propriété du type "si un nombre est supérieur ou égal à 0 alors..." et de vouloir l'appliquer à un nombre dont vous avez montré qu'il est strictement positif. Vous êtes alors obligés de passer du fait que ce nombre est strictement positif au fait qu'il est positif ou nul pour montrer qu'il vérifie la propriété désirée.

Elimination de la disjonction

$$\frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta}\ {\scriptstyle \vee e}$$

Si on a montré $\phi \vee \psi$, alors pour montrer θ, il suffit de montrer θ en supposant ϕ, et encore de le montrer en supposant ψ.

Affaiblissement

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle aff}$$

Si je peux prouver ψ avec les hypothèses Γ, alors je peux encore prouver ψ si j'ajoute d'autres hypothèses à Γ. Autrement dit, il y a des hypothèses qui peuvent ne pas servir dans une démonstration.

Contraction

$$\frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle ctr}$$

Cette règle est une conséquence immédiate de la définition du séquent, puisque lorsque l'on écrit $\Gamma, \phi, \phi \vdash \psi$, on écrit en vérité $\Gamma \cup \{\phi, \phi\} \vdash \psi$. Or, $\{\phi, \phi\}$, par définition, n'est autre que l'ensemble qui contient un seul élément : ϕ. On a donc l'égalité suivante : $\{\phi, \phi\} = \{\phi\}$. Par conséquent $\Gamma \cup \{\phi, \phi\}$ et $\Gamma \cup \{\phi\}$ sont le même ensemble, d'où $\Gamma \cup \{\phi, \phi\} \vdash \psi$ et $\Gamma \cup \{\phi\} \vdash \psi$ sont la même chose. Pour utiliser les conventions d'écriture que nous avons : $\Gamma, \phi, \phi \vdash \psi$ et $\Gamma \cup \phi \vdash \psi$ sont en fait le même séquent.

Axiome

$$\frac{}{\phi \vdash \phi}\ ax$$

Règles logiques

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\ \wedge i \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ \wedge e_g \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ \wedge e_d$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \rightarrow \psi}\ \rightarrow i \qquad \frac{\Gamma \vdash \phi \rightarrow \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\ \rightarrow e$$

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg \phi}\ \neg i \qquad \frac{\Gamma \vdash \neg \phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \bot}\ \neg e$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\ \vee i_g \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\ \vee i_d \qquad \frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta}\ \vee e$$

Règles structurelles

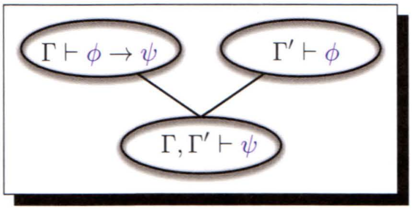
$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ aff \qquad \frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ ctr$$

FIGURE 3.1 – Règles de la *logique minimale* en Déduction Naturelle.

Chacune de ces règles – à l'exception de l'Axiome – fait intervenir un séquent conclusion et 1, 2 ou 3 prémisses. Ainsi, chaque règle peut être regardée comme définissant une structure arborescente simple. Par exemple, la règle de l'élimination de l'implication :

$$\frac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi} \to_e$$

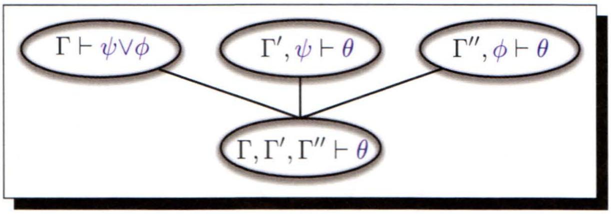
peut être regardée comme un arbre de hauteur 1, avec une racine ($\Gamma, \Gamma' \vdash \psi$) et deux feuilles ($\Gamma \vdash \phi \to \psi$ et $\Gamma' \vdash \phi$).



De même, la règle de l'élimination de la disjonction :

$$\frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta} \vee_e$$

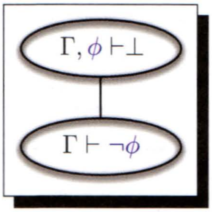
donne lieu, cette fois-ci, à un arbre avec une racine et trois feuilles.



Par contre la règle de l'introduction de la négation :

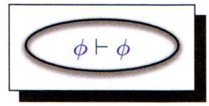
$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi} \neg_i$$

lorsqu'on la regarde comme un arbre, donne une racine et une simple feuille.



Et finalement, la seule des règles qui ne donne lieu qu'à une malheureuse racine (ou feuille) est la règle de l'axiome :

$$\frac{}{\phi \vdash \phi} ax$$



Une déduction, dans le système de la Déduction Naturelle, est un arbre fini – représenté la racine en bas et les feuilles en haut – dont les nœuds sont des séquents, et chaque relation entre un nœud quelconque et ses descendants immédiats est une instance de l'une des règles de la Déduction Naturelle.

Définition 119 *Une déduction (*en logique minimale*), dans le système de la Déduction Naturelle, est un arbre fini dont les nœuds sont des séquents $(S_i)_{i \leq k}$, et tel que :*

Pour chaque nœud S_i de la déduction :

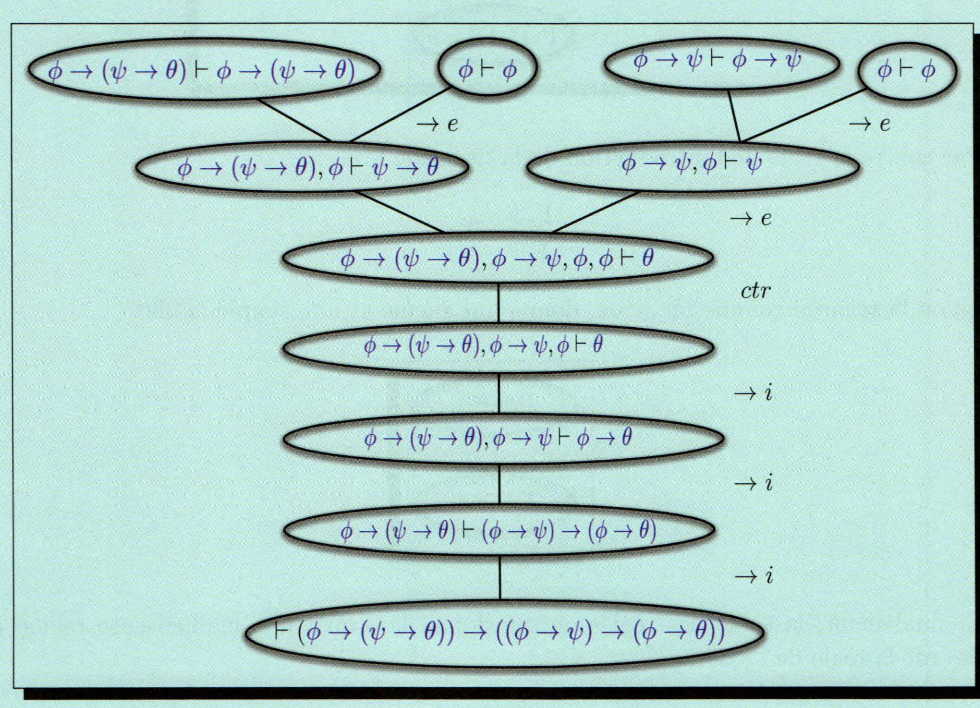
- *S_i est une feuille si et seulement si S_i est un axiome,*
- *si S_i n'est pas une feuille, alors l'arbre dont S_i est la racine et les fils/filles de S_i sont les feuilles est une instance de l'une des règles présentée dans le tableau 3.1.*

Une formule ϕ est déductible des hypothèses Γ s'il existe une déduction dont la racine soit le séquent $\Delta \vdash \phi$ pour un ensemble d'hypothèses $\Delta \subseteq \Gamma$ (ce que l'on notera $\Gamma \vdash_m \phi$).

Considérons maintenant une preuve pour chacun des deux premiers axiomes du système axiomatique que nous avons présenté plus haut.

Exemple 120 Une preuve du fait que $(\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))$ est un théorème du Calcul Propositionnel. Autrement dit, une déduction du séquent

$$\vdash_m \phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))$$



Nous avons indiqué le nom de chacune des règles utilisées pour former cet arbre. Mais cette présentation n'est guère esthétique. On lui préférera la présentation suivante :

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\boxed{\phi \to (\psi\to\theta) \vdash \phi \to (\psi\to\theta)}}\,{\scriptstyle ax} \quad \dfrac{}{\boxed{\phi \vdash \phi}}\,{\scriptstyle ax}}{\boxed{\phi \to (\psi \to \theta), \phi \vdash \psi \to \theta}}\,{\scriptstyle \to e} \quad \dfrac{\dfrac{}{\boxed{\phi \to \psi \vdash \phi \to \psi}}\,{\scriptstyle ax} \quad \dfrac{}{\boxed{\phi \vdash \phi}}\,{\scriptstyle ax}}{\boxed{\phi \to \psi, \phi \vdash \psi}}\,{\scriptstyle \to e}}{\boxed{\phi \to (\psi \to \theta), \phi \to \psi, \phi, \phi \vdash \theta}}\,{\scriptstyle \to e}}{\boxed{\phi \to (\psi \to \theta), \phi \to \psi, \phi \vdash \theta}}\,{\scriptstyle ctr}}{\boxed{\phi \to (\psi \to \theta), \phi \to \psi \vdash \phi \to \theta}}\,{\scriptstyle \to i}}{\boxed{\phi \to (\psi \to \theta) \vdash (\phi \to \psi) \to (\phi \to \theta)}}\,{\scriptstyle \to i}}{\boxed{\vdash (\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))}}\,{\scriptstyle \to i}
$$

ou encore la présentation plus succincte qui suit :

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \to (\psi\to\theta) \vdash \phi \to (\psi\to\theta)}\,{\scriptstyle ax} \quad \dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\phi \to (\psi \to \theta), \phi \vdash \psi \to \theta}\,{\scriptstyle \to e} \quad \dfrac{\dfrac{}{\phi \to \psi \vdash \phi \to \psi}\,{\scriptstyle ax} \quad \dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\phi \to \psi, \phi \vdash \psi}\,{\scriptstyle \to e}}{\phi \to (\psi \to \theta), \phi \to \psi, \phi, \phi \vdash \theta}\,{\scriptstyle \to e}}{\phi \to (\psi \to \theta), \phi \to \psi, \phi \vdash \theta}\,{\scriptstyle ctr}}{\phi \to (\psi \to \theta), \phi \to \psi \vdash \phi \to \theta}\,{\scriptstyle \to i}}{\phi \to (\psi \to \theta) \vdash (\phi \to \psi) \to (\phi \to \theta)}\,{\scriptstyle \to i}}{\vdash (\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))}\,{\scriptstyle \to i}
$$

Exemple 121 Une preuve du fait que $\phi \to (\psi \to \phi)$ est un théorème du Calcul Propositionnel. Autrement dit, une déduction du séquent $\vdash_m \phi \to (\psi \to \phi)$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\phi, \psi \vdash \phi}\,{\scriptstyle aff}}{\phi \vdash \psi \to \phi}\,{\scriptstyle \to i}}{\vdash \phi \to (\psi \to \phi)}\,{\scriptstyle \to i}
$$

Exemple 122 Une preuve du fait que $\phi \to \neg\neg\phi$ est un théorème du Calcul Propositionnel. Autrement dit, une déduction du séquent $\vdash_m \phi \to \neg\neg\phi$:

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\phi \vdash \neg\phi}\,{\scriptstyle ax} \quad \dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\neg\phi, \phi \vdash \perp}\,{\scriptstyle \neg e}}{\phi \vdash \neg\neg\phi}\,{\scriptstyle \neg i}}{\vdash \phi \to \neg\neg\phi}\,{\scriptstyle \to i}
$$

Remarques 123

(1) On ne peut prouver l'implication inverse avec les règles que nous nous sommes données. En effet, dans le cadre de la logique minimale (c'est-à-dire avec les seules règles vues jusqu'ici), on ne peut montrer $\vdash_m \neg\neg\phi \rightarrow \phi$. On ne peut donc pas éliminer les doubles négations. Pour pouvoir le faire, il nous faudra considérer un système déductif plus fort que celui sur lequel nous nous sommes arrêtés. Ainsi, la logique dans laquelle nous nous aventurons n'a pas le pouvoir expressif de la logique classique. Il y manque encore une règle : la règle de l'absurde classique.

(2) Afin de raccourcir les preuves, nous nous autoriserons désormais à intégrer les contractions et les affaiblissements aux autres règles. Ainsi nous utiliserons des mixtes de règles logiques et de règles structurelles. Par exemple, une preuve de $\phi \rightarrow \neg\neg\phi$ pourrait être :

$$\dfrac{\dfrac{\dfrac{}{\phi, \neg\phi \vdash \phi}\,{\scriptstyle ax+aff} \qquad \dfrac{}{\neg\phi, \phi \vdash \neg\phi}\,{\scriptstyle ax+aff}}{\neg\phi, \phi \vdash \bot}\,{\scriptstyle \neg e+\mathrm{ctr}}}{\phi \vdash \neg\neg\phi}\,{\scriptstyle \neg i}$$

Exemple 124 Montrons que $\vdash_m \neg\phi \longleftrightarrow (\phi \rightarrow \bot)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\phi, \phi \vdash \neg\phi}\,{\scriptstyle ax+aff} \qquad \dfrac{}{\neg\phi, \phi \vdash \phi}\,{\scriptstyle ax+aff}}{\neg\phi, \phi \vdash \bot}\,{\scriptstyle \neg e+\mathrm{ctr}}}{\neg\phi \vdash \phi \rightarrow \bot}\,{\scriptstyle \rightarrow i}}{\vdash \neg\phi \rightarrow (\phi \rightarrow \bot)}\,{\scriptstyle \rightarrow i} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\phi \rightarrow \bot, \phi \vdash \phi \rightarrow \bot}\,{\scriptstyle ax+aff} \qquad \dfrac{}{\phi \rightarrow \bot, \phi \vdash \phi}\,{\scriptstyle ax+aff}}{\phi \rightarrow \bot, \phi \vdash \bot}\,{\scriptstyle \rightarrow e+\mathrm{ctr}}}{\phi \rightarrow \bot \vdash \neg\phi}\,{\scriptstyle \neg i}}{\vdash (\phi \rightarrow \bot) \rightarrow \neg\phi}\,{\scriptstyle \rightarrow i}}{\vdash (\neg\phi \rightarrow (\phi \rightarrow \bot)) \wedge (\phi \rightarrow \bot) \rightarrow \neg\phi)}\,{\scriptstyle \wedge i}$$

La notion de démonstration, de preuve, repose sur une notion de conséquence : à partir d'un ensemble d'hypothèses Γ, on prouve une formule ϕ. Mais cette conséquence n'est pas la conséquence logique que nous avions vu dans le cadre *sémantique*. C'est une conséquence logique qui se situe dans le champ *syntaxique*. De même, nous avions défini une notion d'équivalence entre formules. Deux formules sont équivalentes si elles sont vraies dans les mêmes modèles. Cette notion d'équivalence est donc de nature *sémantique*, puisqu'elle se réfère aux modèles. Et nous avons vu que dire $\phi \equiv \psi$ revenait à dire qu'à la fois $\phi \models \psi$ et $\psi \models \phi$ étaient vérifiés. Nous pouvons désormais définir une notion d'équivalence au sens *syntaxique*, de manière tout à fait similaire, en nous appuyant sur la notion de conséquence *syntaxique*.

Définition 125 *Deux formules ϕ et ψ sont dites équivalentes pour la logique minimale si on a à la fois $\phi \vdash_m \psi$ et $\psi \vdash_m \phi$ (relation d'équivalence que l'on note $\phi \equiv_m \psi$).*

Nous verrons plus tard que les notions d'équivalence *syntaxique* et *sémantique* coïncident pour autant que l'on choisisse la bonne sémantique...

3.1 La logique intuitionniste

Les règles de déduction que nous avons vues jusqu'à présent ne permettent pas de rendre compte de tous les raisonnements que nous faisons, en particulier de tous ceux que pratiquent les mathématiciens. Mais, sans même aller chercher les raisonnements mathématiques, il est des raisonnements qui nous semblent tout à fait évidents et dont nous ne pouvons pas rendre compte avec ce seul système de règles présenté jusqu'ici. Par exemple, nous ne pouvons prouver dans ce système *le tiers exclu* : $\vdash \phi \vee \neg\phi$. Il nous faut pour cela de nouvelles règles. Et ces règles concernent le symbole de contradiction : $\perp$.

Le système de règles que nous avons vu jusqu'ici constitue les règles de la *logique minimale*. Si l'on ajoute la règle suivante, dénommée *absurdité intuitionniste* (ou *élimination de la contradiction*), on obtient un système déductif plus expressif : la *logique intuitionniste*.

Axiome

$$\frac{}{\phi \vdash \phi}\ {\scriptstyle ax}$$

Règles logiques

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\ {\scriptstyle \wedge i} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ {\scriptstyle \wedge e_g} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ {\scriptstyle \wedge e_d}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\ {\scriptstyle \to i} \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\ {\scriptstyle \to e}$$

$$\frac{\Gamma, \phi \vdash \perp}{\Gamma \vdash \neg\phi}\ {\scriptstyle \neg i} \qquad \frac{\Gamma \vdash \neg\phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \perp}\ {\scriptstyle \neg e}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\ {\scriptstyle \vee i_g} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\ {\scriptstyle \vee i_d} \qquad \frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta}\ {\scriptstyle \vee e}$$

Règles structurelles

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle aff} \qquad \frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle ctr}$$

Absurdité intuitionniste

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash \phi}\ {\scriptstyle \perp e}$$

FIGURE 3.2 – règles de la *logique intuitionniste* en Déduction Naturelle.

Absurdité intuitionniste

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\ {\scriptstyle \bot e}$$

La notion de démonstration reste bien évidemment la même que précédemment, avec cette nouvelle règle qui s'ajoute à celles déjà à notre disposition.

Cette règle n'est pas démontrable dans le cadre de la logique minimale. Elle enrichit donc strictement cette dernière. Cela signifie non seulement qu'il existe des déductions possibles en logique intuitionniste qui ne le sont pas en logique minimale (toutes celles qui utilisent une instance de cette règle !), mais en plus qu'il existe des séquents démontrables en logique intuitionniste mais non démontrables en logique minimale. Par conséquent, il est des formules qui sont des théorèmes de la logique intuitionniste, mais restent non prouvables dans le cadre restreint de la logique minimale.

Définition 126 *Une déduction (*en logique intuitionniste*), dans le système de la Déduction Naturelle, est un arbre fini dont les nœuds sont des séquents $(S_i)_{i\leq k}$, et tel que :*
Pour chaque nœud S_i de la déduction :

- *S_i est une feuille si et seulement si S_i est un axiome,*
- *si S_i n'est pas une feuille, alors l'arbre dont S_i est la racine et les fils/filles de S_i sont les feuilles est une instance de l'une des règles présentée dans le tableau 3.2.*

Une formule ϕ est déductible des hypothèses Γ s'il existe une déduction dont la racine soit le séquent $\Delta \vdash \phi$ pour un ensemble d'hypothèses $\Delta \subseteq \Gamma$ (ce que l'on notera $\Gamma \vdash_i \phi$).

De même que nous avons défini l'équivalence $\equiv_m$ sur la base de la conséquence $\vdash_m$, nous définissons l'équivalence *syntaxique* de formules pour la logique intuitionniste.

Définition 127 *Deux formules ϕ et ψ sont dites équivalentes pour la logique intuitionniste si on a à la fois $\phi \vdash_i \psi$ et $\psi \vdash_i \phi$ (relation d'équivalence que l'on note $\phi \equiv_i \psi$).*

Exemple 128 La formule $\neg\neg(\neg\neg\phi \rightarrow \phi)$ est démontrable en logique intuitionniste :

$$\begin{prooftree}
\AxiomC{}
\RightLabel{\scriptsize ax}
\UnaryInfC{$\neg\neg\phi \vdash \neg\neg\phi$}
\AxiomC{}
\RightLabel{\scriptsize ax+aff}
\UnaryInfC{$\phi, \neg\neg\phi \vdash \phi$}
\RightLabel{\scriptsize $\rightarrow i$}
\UnaryInfC{$\phi \vdash \neg\neg\phi\rightarrow\phi$}
\AxiomC{}
\RightLabel{\scriptsize ax}
\UnaryInfC{$\neg(\neg\neg\phi\rightarrow\phi) \vdash \neg(\neg\neg\phi\rightarrow\phi)$}
\RightLabel{\scriptsize $\neg e$}
\BinaryInfC{$\neg(\neg\neg\phi\rightarrow\phi), \phi \vdash \bot$}
\RightLabel{\scriptsize $\neg i$}
\UnaryInfC{$\neg(\neg\neg\phi\rightarrow\phi) \vdash \neg\phi$}
\RightLabel{\scriptsize $\neg e$}
\BinaryInfC{$\neg\neg\phi, \neg(\neg\neg\phi\rightarrow\phi) \vdash \bot$}
\RightLabel{\scriptsize $\bot e$}
\UnaryInfC{$\neg\neg\phi, \neg(\neg\neg\phi\rightarrow\phi) \vdash \phi$}
\RightLabel{\scriptsize $\rightarrow i$}
\UnaryInfC{$\neg(\neg\neg\phi\rightarrow\phi) \vdash \neg\neg\phi\rightarrow\phi$}
\AxiomC{}
\RightLabel{\scriptsize ax}
\UnaryInfC{$\neg(\neg\neg\phi\rightarrow\phi) \vdash \neg(\neg\neg\phi\rightarrow\phi)$}
\RightLabel{\scriptsize $\neg$e+ctr}
\BinaryInfC{$\neg(\neg\neg\phi\rightarrow\phi) \vdash \bot$}
\RightLabel{\scriptsize $\neg i$}
\UnaryInfC{$\vdash \neg\neg(\neg\neg\phi\rightarrow\phi)$}
\end{prooftree}$$

3.2 La logique classique

La logique classique s'obtient en ajoutant à la logique minimale, non pas la règle de l'absurdité intuitionniste, mais la règle de *l'absurdité classique.*

Absurdité classique

$$\frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\ {\scriptstyle \bot c}$$

La notion de démonstration reste inchangée, cette nouvelle règle étant simplement ajoutée à celles de la logique minimale.

Cette règle n'est pas démontrable dans le cadre de la logique minimale. Elle ne l'est pas non plus en logique intuitionniste. Elle constitue donc un enrichissement strict de la logique intuitionniste et, *a fortiori*, un enrichissement encore plus important de la logique minimale.

Définition 129 *Une déduction (*en logique classique*), dans le système de la Déduction Naturelle, est un arbre fini dont les nœuds sont des séquents $(S_i)_{i \leq k}$, et tel que :*

Pour chaque nœud S_i de la déduction :

- *S_i est une feuille si et seulement si S_i est un axiome,*
- *si S_i n'est pas une feuille, alors l'arbre dont S_i est la racine et les fils/filles de S_i sont les feuilles est une instance de l'une des règles présentée dans le tableau 3.3.*

Une formule ϕ est déductible des hypothèses Γ s'il existe une déduction dont la racine soit le séquent $\Delta \vdash \phi$ pour un ensemble d'hypothèses $\Delta \subseteq \Gamma$ (ce que l'on notera $\Gamma \vdash_c \phi$).

Maintenant que nous sommes pourvus de la notion de conséquence *syntaxique* pour la logique classique, nous définissons la notion d'équivalence *syntaxique* de formules pour la logique classique. On montrera plus tard que conséquence *syntaxique* pour la logique classique et conséquence *sémantique* coïncident.

Définition 130 *Deux formules ϕ et ψ sont dites équivalentes pour la logique classique si on a à la fois $\phi \vdash_c \psi$ et $\psi \vdash_c \phi$ (relation d'équivalence que l'on note $\phi \equiv_c \psi$).*

Exemple 131 La règle de l'absurde intuitionniste est un cas particulier de la règle de l'absurde classique qui correspond au cas où l'hypothèse $\neg\phi$ n'apparaît pas. Elle s'en déduit donc immédiatement par :

$$\dfrac{\dfrac{\Gamma \vdash \bot}{\Gamma, \neg\phi \vdash \bot}\ {\scriptstyle aff}}{\Gamma \vdash \phi}\ {\scriptstyle \bot c}$$

Exemple 132 Un autre exemple de formule démontrable en logique classique et non en logique intuitionniste : $\vdash \phi \vee \neg\phi$ encore appelée la règle (ou la loi) du *tiers exclu* :

$$\dfrac{\dfrac{\dfrac{}{\neg(\phi\vee\neg\phi) \vdash \neg(\phi\vee\neg\phi)}\ {\scriptstyle ax} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg(\phi\vee\neg\phi) \vdash \neg(\phi\vee\neg\phi)}\ {\scriptstyle ax} \qquad \dfrac{\dfrac{}{\phi \vdash \phi}\ {\scriptstyle ax}}{\phi \vdash \phi\vee\neg\phi}\ {\scriptstyle \vee ig}}{\neg(\phi\vee\neg\phi), \phi \vdash \bot}\ {\scriptstyle \neg e}}{\neg(\phi\vee\neg\phi) \vdash \neg\phi}\ {\scriptstyle \neg i}}{\neg(\phi\vee\neg\phi) \vdash \phi\vee\neg\phi}\ {\scriptstyle \vee id}}{\neg(\phi\vee\neg\phi) \vdash \bot}\ {\scriptstyle \neg e}}{\vdash \phi\vee\neg\phi}\ {\scriptstyle \bot c}$$

Axiome

$$\frac{}{\phi \vdash \phi}\ {\scriptstyle ax}$$

Règles logiques

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\ {\scriptstyle \wedge i} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ {\scriptstyle \wedge e_g} \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ {\scriptstyle \wedge e_d}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\ {\scriptstyle \to i} \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\ {\scriptstyle \to e}$$

$$\frac{\Gamma, \phi \vdash \perp}{\Gamma \vdash \neg \phi}\ {\scriptstyle \neg i} \qquad \frac{\Gamma \vdash \neg \phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \perp}\ {\scriptstyle \neg e}$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\ {\scriptstyle \vee i_g} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\ {\scriptstyle \vee i_d} \qquad \frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta}\ {\scriptstyle \vee e}$$

Règles structurelles

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle aff} \qquad \frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle ctr}$$

Absurdité classique

$$\frac{\Gamma, \neg \phi \vdash \perp}{\Gamma \vdash \phi}\ {\scriptstyle \perp c}$$

FIGURE 3.3 – Règles de la *logique classique* en Déduction Naturelle.

Exemple 133 Encore un exemple de formule démontrable en logique classique et non en logique intuitionniste : $\vdash (\neg\phi \longrightarrow \phi) \longrightarrow \phi$ encore appelée *la loi de Peirce*[3] :

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\phi \vdash \neg\phi}\,ax \qquad \dfrac{\dfrac{}{\neg\phi \to \phi \vdash \neg\phi \to \phi}\,ax \qquad \dfrac{}{\neg\phi \vdash \neg\phi}\,ax}{\neg\phi \to \phi, \neg\phi \vdash \phi}\,{\to}e}{\neg\phi \to \phi, \neg\phi \vdash \bot}\,\neg e{+}ctr}{\neg\phi \to \phi \vdash \phi}\,\bot c}{\vdash (\neg\phi \to \phi) \to \phi}\,{\to}i
$$

Exemple 134 L'élimination des doubles négations est démontrable en logique classique et non en logique intuitionniste : $\vdash \neg\neg\phi \longrightarrow \phi$.

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\neg\phi \vdash \neg\neg\phi}\,ax \qquad \dfrac{}{\neg\phi \vdash \neg\phi}\,ax}{\neg\neg\phi, \neg\phi \vdash \bot}\,\neg e}{\neg\neg\phi \vdash \phi}\,\bot c}{\vdash \neg\neg\phi \to \phi}\,{\to}i
$$

Exemple 135 La contraposition est encore un exemple de règle démontrable en logique classique et non en logique intuitionniste : $\vdash (\neg\psi \longrightarrow \neg\phi) \longrightarrow (\phi \longrightarrow \psi)$.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\psi \to \neg\phi \vdash \neg\psi \to \neg\phi}\,ax \qquad \dfrac{}{\neg\psi \vdash \neg\psi}\,ax}{\neg\psi \to \neg\phi, \neg\psi \vdash \neg\phi}\,{\to}e \qquad \dfrac{}{\phi \vdash \phi}\,ax}{\neg\psi \to \neg\phi, \neg\psi, \phi \vdash \bot}\,\neg e}{\neg\psi \to \neg\phi, \phi \vdash \psi}\,\bot c}{\neg\psi \to \neg\phi \vdash \phi \to \psi}\,{\to}i}{\vdash (\neg\psi \to \neg\phi) \to (\phi \to \psi)}\,{\to}i
$$

3. La loi de Peirce est plus générale que la version restreinte que nous en donnons. Elle est généralement présentée comme $\vdash \big((\phi \longrightarrow \psi) \longrightarrow \phi\big) \longrightarrow \phi$. Si l'on se souvient que la formule $\neg\phi$ est équivalente à $\phi \longrightarrow \bot$, on voit que notre version $\vdash (\neg\phi \longrightarrow \phi) \longrightarrow \phi$ n'est que le cas particulier où $\psi = \bot$.

Exemple 136 L'axiome (3) du système d'axiome "à la Hilbert" que nous avons présenté – voir page 188 – est démontrable en logique classique : $\vdash (\neg\psi \longrightarrow \neg\phi) \longrightarrow ((\neg\psi \longrightarrow \phi) \longrightarrow \psi)$.

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\psi \longrightarrow \neg\phi \vdash \neg\psi \longrightarrow \neg\phi}{\scriptstyle ax} \quad \dfrac{}{\neg\psi \vdash \neg\psi}{\scriptstyle ax}}{\neg\psi \longrightarrow \neg\phi, \neg\psi \vdash \neg\phi}{\scriptstyle \rightarrow e} \quad \dfrac{\dfrac{}{\neg\psi \longrightarrow \phi \vdash \neg\psi \longrightarrow \phi}{\scriptstyle ax} \quad \dfrac{}{\neg\psi \vdash \neg\psi}{\scriptstyle ax}}{\neg\psi \longrightarrow \phi, \neg\psi \vdash \phi}{\scriptstyle \rightarrow e}}{\neg\psi \longrightarrow \neg\phi, \neg\psi \longrightarrow \phi, \neg\psi, \neg\psi \vdash \bot}{\scriptstyle \neg e}}{\neg\psi \longrightarrow \neg\phi, \neg\psi \longrightarrow \phi, \neg\psi \vdash \bot}{\scriptstyle ctr}}{\neg\psi \longrightarrow \neg\phi, \neg\psi \longrightarrow \phi \vdash \psi}{\scriptstyle \bot c}}{\neg\psi \longrightarrow \neg\phi \vdash (\neg\psi \longrightarrow \phi) \longrightarrow \psi}{\scriptstyle \rightarrow i}}{\vdash (\neg\psi \longrightarrow \neg\phi) \longrightarrow ((\neg\psi \longrightarrow \phi) \longrightarrow \psi)}{\scriptstyle \rightarrow i}
$$

Remarque 137 La logique intuitionniste diffère de la logique classique en ce qu'elle cherche à rendre compte de l'accès qu'on a à la vérité plutôt que de la vérité elle-même. En logique classique, le séquent $\vdash \phi$ signifie que ϕ est vrai, alors qu'en logique intuitionniste, il signifie un peu plus que ça : il signifie que l'on sait que ϕ, que l'on obtient – au terme d'un cheminement – la vérité de ϕ. Il est clair que la règle de l'absurdité classique, celle qui est à l'oeuvre dans toutes les démonstrations précisément dites *par l'absurde*, ne construit pas la vérité de ϕ. Tout au plus, elle met à disposition cette vérité sur la base d'une contradiction mettant en jeu $\neg\phi$. Pour prendre un autre exemple, le tiers exclu nous affirme que $\phi \vee \neg\phi$, mais cela ne nous dit pas laquelle des deux formules ϕ et $\neg\phi$ est vraie.

L'exemple le plus courant de démonstration mathématique simple faisant intervenir le tiers exclu et pour lequel il existe une démonstration intuitionniste beaucoup plus compliquée est le suivant :

On cherche s'il existe un couple de nombres irrationnels (a, b) $(a, b \in \mathbb{R} \setminus \mathbb{Q})$ tels que a^b soit rationnel $(a^b \in \mathbb{Q})$. Etant bien connu que $\sqrt{2}$ est irrationnel, on distingue deux cas :

- si $\sqrt{2}^{\sqrt{2}}$ est rationnel, alors on prend $a = b = \sqrt{2}$
- si $\sqrt{2}^{\sqrt{2}}$ est irrationnel, alors on prend $a = \sqrt{2}^{\sqrt{2}}$ et $b = \sqrt{2}$, puisqu'on a

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\left(\sqrt{2}\cdot\sqrt{2}\right)} = \sqrt{2}^{2} = 2.$$

On a bien ainsi répondu à la question, puisque, par le principe du tiers exclu, on se trouve dans un cas ou bien dans l'autre. Mais, pour savoir laquelle des deux options est la bonne, il faut savoir si $\sqrt{2}^{\sqrt{2}}$ est rationnel ou non. En fait, on sait que $\sqrt{2}^{\sqrt{2}}$ n'est pas rationnel, mais le prouver demande des moyens très au-dessus de la petite démonstration que nous venons de produire. Nous retrouverons cet exemple dans le cadre de la logique du 1^{er}ordre qui lui offrira le cadre idéal à sa formulation.

Il ressort de ce qui précède que la logique intuitionniste vise à obtenir des preuves constructives. En logique intuitionniste, si l'on a réussi à démontrer le séquent $\vdash_i \phi \vee \psi$, c'est soit parce que l'on a démontré le séquent $\vdash_i \phi$, soit parce que l'on a démontré le séquent $\vdash_i \psi$. L'importance que revêt la logique intuitionniste – en tant que logique constructive – sera exposé au chapitre 17.

Remarque 138 Il y a différentes manières d'obtenir la logique classique, que ce soit à partir de la logique minimale ou de la logique intuitionniste. Par exemple :

$$\begin{aligned}
\textit{log. cl.} &= \textit{log. int.} + \dfrac{}{\vdash \phi \vee \neg\phi}\,{\scriptstyle ax} && \textit{(principe du tiers exclu)}\\
&= \textit{log. int.} + \dfrac{}{\neg\phi \longrightarrow \phi \vdash \phi}\,{\scriptstyle ax} && \textit{(loi de Peirce)}\\
&= \textit{log. min.} + \dfrac{}{\neg\neg\phi \vdash \longrightarrow \phi}\,{\scriptstyle ax} && \textit{(élimination des doubles négations)}\\
&= \textit{log. min.} + \dfrac{}{\neg\psi \longrightarrow \neg\phi \vdash \phi \longrightarrow \psi}\,{\scriptstyle ax} && \textit{(contraposition)}
\end{aligned}$$

Preuve de la Remarque 138 : Pour chacune de ces quatre égalités, nous allons montrer que les inclusions sont vérifées dans les deux sens. Tout d'abord les quatre inclusions suivantes :

(1) $\textit{log. cl.} \supset \textit{log. int.} + \dfrac{}{\vdash \phi \vee \neg\phi}\,{\scriptstyle ax}$

(2) $\textit{log. cl.} \supset \textit{log. int.} + \dfrac{}{\neg\phi \longrightarrow \phi \vdash \phi}\,{\scriptstyle ax}$

(3) $\textit{log. cl.} \supset \textit{log. min.} + \dfrac{}{\neg\neg\phi \vdash \longrightarrow \phi}\,{\scriptstyle ax}$

(4) $\textit{log. cl.} \supset \textit{log. min.} + \dfrac{}{\neg\psi \longrightarrow \neg\phi \vdash \phi \longrightarrow \psi}\,{\scriptstyle ax}$

sont respectivement conséquences immédiates des Exemples 132, 133, 134 et 135, dans lesquels nous avons montré successivement que le principe du tiers exclu, la loi de Peirce, l'élimination des doubles négation ainsi que la contraposition étaient toutes quatre démontrables sans hypothèse en logique classique.

Attachons nous maintenant à montrer les inclusions inverses. Il nous faut vérifier que pour chacune d'elle, la règle de l'absurdité classique peut être obtenue dans la logique considérée :

(1) $\textit{log. cl.} \subset \textit{log. int.} + \dfrac{}{\vdash \phi \vee \neg\phi}\,{\scriptstyle ax}$:

$$\dfrac{\dfrac{}{\vdash \phi \vee \neg\phi}\,{\scriptstyle ax} \qquad \dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax} \qquad \dfrac{\Gamma, \neg\phi \vdash \bot}{\Gamma, \neg\phi \vdash \phi}\,{\scriptstyle \bot\, i}}{\Gamma \vdash \phi}\,{\scriptstyle \vee\, e}$$

(2) $\textit{log. cl.} \subset \textit{log. int.} + \dfrac{}{\neg\phi \longrightarrow \phi \vdash \phi}\,{\scriptstyle ax}$:

$$\dfrac{\dfrac{\dfrac{}{\neg\phi \longrightarrow \phi \vdash \phi}\,{\scriptstyle ax}}{\vdash (\neg\phi \longrightarrow \phi) \longrightarrow \phi}\,{\scriptstyle \rightarrow\, i} \qquad \dfrac{\dfrac{\Gamma, \neg\phi \vdash \bot}{\Gamma, \neg\phi \vdash \phi}\,{\scriptstyle \bot\, i}}{\Gamma \vdash \neg\phi \longrightarrow \phi}\,{\scriptstyle \rightarrow\, i}}{\Gamma \vdash \phi}\,{\scriptstyle \rightarrow\, e}$$

(3) $\textit{log. cl.} \subset \textit{log. min.} + \dfrac{}{\neg\neg\phi \vdash \longrightarrow \phi}\,{\scriptstyle ax}$:

$$\dfrac{\dfrac{}{\vdash \neg\neg\phi \longrightarrow \phi}\,{\scriptstyle ax} \qquad \dfrac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \neg\neg\phi}\,{\scriptstyle \neg\, i}}{\Gamma \vdash \phi}\,{\scriptstyle \rightarrow\, e}$$

(4) *log. cl.* $\subset$ *log. min.* + $\dfrac{}{\neg\psi \longrightarrow \neg\phi \vdash \phi \longrightarrow \psi}\,{\scriptstyle ax}$:

Nous allons prendre en compte pour cette preuve, une instance de l'axiome de la contraposition ci-dessus dans laquelle $\psi := \phi$ et $\phi := \neg\bot$; à savoir $\dfrac{}{\neg\phi \longrightarrow \neg\neg\bot \vdash \neg\bot \longrightarrow \phi}\,{\scriptstyle ax}$.

$$\dfrac{\dfrac{\dfrac{}{\neg\phi \longrightarrow \neg\neg\bot \vdash \neg\bot \longrightarrow \phi}\,{\scriptstyle ax}}{\vdash (\neg\phi \longrightarrow \neg\neg\bot) \longrightarrow (\neg\bot \longrightarrow \phi)}\,{\scriptstyle \rightarrow i} \quad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\bot \vdash \bot}\,{\scriptstyle ax} \quad \dfrac{}{\neg\bot \vdash \neg\bot}\,{\scriptstyle ax}}{\bot, \neg\bot \vdash \bot}\,{\scriptstyle \rightarrow e}}{\bot \vdash \neg\neg\bot}\,{\scriptstyle \neg i}}{\vdash \bot \longrightarrow \neg\neg\bot}\,{\scriptstyle \rightarrow i} \quad \Gamma, \neg\phi \vdash \bot}{\Gamma, \neg\phi \vdash \neg\neg\bot}\,{\scriptstyle \rightarrow e}}{\Gamma \vdash \neg\phi \longrightarrow \neg\neg\bot}\,{\scriptstyle \rightarrow i}}{\Gamma \vdash \neg\bot \longrightarrow \phi}\,{\scriptstyle \rightarrow e} \quad \dfrac{\dfrac{}{\bot \vdash \bot}\,{\scriptstyle ax}}{\vdash \neg\bot}\,{\scriptstyle \neg i}}{\Gamma \vdash \phi}\,{\scriptstyle \rightarrow e}$$

$\dashv$ 138

3.3 Le théorème de complétude de la logique classique

Il est temps de nous intéresser aux liens entre vérité sémantique d'une part et vérité syntaxique d'autre part. Or, c'est précisément ce que prend en charge le théorème de complétude.

En effet, il faut nous assurer que les règles de la Déduction Naturelle (dans sa version logique classique) n'ont pas été définies au hasard mais au contraire, qu'elles rendent compte de la notion de vérité que nous connaissions jusqu'ici, c'est-à-dire la vérité sémantique. Il nous faut nous assurer que la notion de conséquence logique (au sens sémantique) est bien en correspondance avec celle de conséquence (au sens de la théorie de la démonstration). Ou pour le dire encore autrement, il nous faut montrer que toute tautologie est démontrable sans utiliser d'hypothèse; et inversement, toute formule démontrable sans hypothèse est bien une tautologie.

Théorème 139 *Soient* Γ*, un ensemble fini de formules et* ϕ*, une formule du Calcul Propositionnel,*

$$\Gamma \models \phi \quad ssi \quad \Gamma \vdash_c \phi.$$

Corollaire 140 *Soit* ϕ *une formule du Calcul Propositionnel,*

$$\models \phi \quad ssi \quad \vdash_c \phi.$$

Preuve du Corollaire 140 : C'est une conséquence immédiate du Théorème 139 en prenant pour ensemble d'hypothèses Γ, l'ensemble vide. $\dashv$ 140

Preuve du Théorème 139 : La preuve de ce théorème est longue et fastidieuse. Comme d'habitude, avec une condition de la forme *si et seulement si*, nous allons considérer les deux directions de cette double implication.

"$\Gamma \vdash_c \phi$ implique $\Gamma \vDash \phi$"

Il s'agit tout d'abord de montrer que si l'on a une preuve en logique classique du séquent $\Gamma \vdash \phi$, alors la formule ϕ est vraie dans tous les modèles de Γ (c'est-à-dire dans tous les modèles dans lesquels toutes les formules de Γ sont vérifiées). Or, une preuve (ou une démonstration, c'est la même chose) est une suite finie de séquents. Nous allons donc utiliser cette propriété linéaire des preuves et faire une démonstration par induction sur la longueur de la preuve. Comme une preuve a une longueur d'au moins 1, nous démarrons notre preuve par induction en considérant les preuves de longueur 1 :

- Si la preuve a une longueur 1, il est absolument évident que le séquent en question ne peut être qu'un axiome. Il s'agit donc de $\phi \vdash \phi$. Il nous faut donc vérifier que $\phi \vDash \phi$ est bien correct. Ceci est une totale évidence puisque par définition, $\phi \vDash \phi$ est vraie si ϕ est vraie dans chaque modèle dans lequel ϕ est vraie.
- Nous supposons maintenant que la propriété que nous voulons prouver est vérifiée par des séquents obtenus suivant une démonstration en logique classique de longueur au plus n. Nous considérons le cas des preuves de longueur $n+1$. Si le dernier séquent est un axiome, nous nous retrouvons dans le cas traité ci-dessus. Les seuls cas intéressants sont ceux dans lesquels l'une des règles est appliquée. Nous allons donc distinguer les cas correspondants aux différentes règles :

$\wedge i$

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi} \wedge i$$

Il nous faut montrer que $\Gamma, \Gamma' \vdash \phi \wedge \psi$ implique $\Gamma, \Gamma' \vDash \phi \wedge \psi$. Or, nous savons que chacun des deux séquents au-dessus de la barre horizontale est issu d'une preuve de longueur au plus n. Donc, par hypothèse d'induction, nous déduisons, du fait que $\Gamma \vdash \phi$ et $\Gamma' \vdash \psi$, le fait que $\Gamma \vDash \phi$ et $\Gamma' \vDash \psi$. Puisque ϕ est vraie dans tous les modèles de Γ, elle est vraie dans tous les modèles de Γ et de Γ' (ces modèles sont ceux dans lesquels toutes les formules à la fois de Γ et de Γ' sont vraies). De même, comme ψ est vraie dans tous les modèles de Γ', elle est vraie dans tous les modèles de Γ et de Γ'. Par conséquent, les deux formules ϕ et ψ sont toutes deux vraies dans tous les modèles de Γ et de Γ'. Or, cela n'est pas autre chose que de dire que la formule $\phi \wedge \psi$ est vraie dans tous les modèles de Γ et de Γ'.

$\wedge e_g$

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi} \wedge e_g$$

Comme $\Gamma \vdash \phi$ est obtenu au terme d'une démonstration de longueur $n+1$, le séquent $\Gamma \vdash \phi \wedge \psi$ est, quant à lui, obtenu par une démonstration de longueur, précisément, n. On peut donc appliquer l'hypothèse d'induction : de $\Gamma \vdash \phi \wedge \psi$ nous en déduisons que $\Gamma \vDash \phi \wedge \psi$. Mais alors, si la formule $\phi \wedge \psi$ est vraie dans tous les modèles de Γ, il en est de même de la formule ϕ, c'est-à-dire $\Gamma \vDash \phi$.

$\wedge e_d$

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi} \wedge e_d$$

Ce cas est rigoureusement identique au précédent en échangeant ϕ et ψ.

$\rightarrow i$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \rightarrow \psi} \rightarrow i$$

Ce cas est un tout petit peu plus intéressant que les précédents. Toujours par hypothèse d'induction, nous savons que $\Gamma, \phi \vdash \psi$ implique $\Gamma, \phi \models \psi$, ou pour être plus précis $\Gamma \cup \{\phi\} \models \psi$. Ce qu'il nous faut montrer, c'est $\Gamma \models \phi \rightarrow \psi$. Or la formule $\phi \rightarrow \psi$ est toujours vraie lorsque ϕ est fausse, donc $\phi \rightarrow \psi$ est vraie dans tous les modèles de Γ dans lesquels ϕ est fausse. Pour ce qui est des modèles de Γ dans lesquels ϕ est vraie, nous savons par hypothèse que ψ est vérifiée dans ces modèles (c'est précisément ce que dit $\Gamma \cup \{\phi\} \models \psi$). Par conséquent, dans tous les modèles de Γ dans lesquels ϕ est vraie, la formule $\phi \rightarrow \psi$ est également vraie. En considérant maintenant tous les modèles de Γ (ceux dans lesquels ϕ est fausse et ceux dans lesquels ϕ est vraie), la formule $\phi \rightarrow \psi$ est vraie, ce qui s'écrit précisément $\Gamma \models \phi \rightarrow \psi$.

$\rightarrow e$

$$\frac{\Gamma \vdash \phi \rightarrow \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi} \rightarrow e$$

Toujours par hypothèse d'induction, nous savons que $\Gamma \models \phi \rightarrow \psi$ et $\Gamma' \models \phi$ sont vérifiés. Il nous faut alors montrer $\Gamma, \Gamma' \models \psi$. Or, dans les modèles de $\Gamma \cup \Gamma'$, à la fois $\phi \rightarrow \psi$ et ϕ sont vérifiés. Par conséquent, puisque la formule $\phi \rightarrow \psi$ ne peut être vraie lorsque ϕ est vraie que si ψ est vraie, il en résulte que ψ est vraie dans ces modèles. C'est précisément ce que l'on chercher à montrer : $\Gamma, \Gamma' \vdash \psi$.

$\neg i$

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg \phi} \neg i$$

Ce cas est plus troublant. Par hypothèse d'induction, nous savons que $\Gamma, \phi \models \bot$, c'est-à-dire que $\Gamma \cup \{\phi\}$ n'a pas de modèle, ou pour le dire autrement, cette théorie a toujours au moins l'une de ses formules fausse dans n'importe quel modèle possible. Il nous faut montrer $\Gamma \models \neg \phi$, c'est-à-dire que $\neg \phi$ est vraie dans tous les modèles de Γ. Mais si $\neg \phi$ était fausse dans un modèle de Γ, cela signifierait que dans au moins un modèle de Γ, la formule ϕ serait vraie. Or, ce modèle serait un modèle de la théorie $\Gamma \cup \{\phi\}$, ce qui contredirait le fait qu'elle est contradictoire.

$\neg e$

$$\frac{\Gamma \vdash \neg \phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \bot} \neg e$$

Ce cas est assez clair puisque par hypothèse d'induction, nous savons que $\Gamma \models \neg \phi$ et $\Gamma' \models \phi$. Par conséquent, dans les modèles de la théorie $\Gamma \cup \Gamma'$, à la fois $\neg \phi$ et ϕ sont vérifiés. C'est donc qu'il n'existe pas de tels modèles. Autrement dit $\Gamma, \Gamma' \models \bot$.

$\vee i_g$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi} \; {\scriptstyle \vee i_g}$$

Ce cas est très facile puisque par hypothèse d'induction, nous savons que $\Gamma \models \phi$. Il est donc immédiat d'en conclure $\Gamma \models \phi \vee \psi$.

$\vee i_d$

$$\frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi} \; {\scriptstyle \vee i_d}$$

Ce cas est rigoureusement identique au précédent.

$\vee e$

$$\frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta} \; {\scriptstyle \vee e}$$

Par hypothèse d'induction, nous savons que la formule $\psi \vee \phi$ est vraie dans tous les modèles de Γ ($\Gamma \models \psi \vee \phi$), que la formule θ est vraie dans tous les modèles de Γ' qui satisfont la formule ψ ($\Gamma', \psi \models \theta$) et finalement que cette même formule θ est vraie dans tous les modèles de Γ'' qui satisfont la formule ϕ ($\Gamma'', \phi \models \theta$).
Donc, si nous considérons les modèles de $\Gamma' \cup \Gamma''$, nous voyons que la formule θ est satisfaite dans ceux qui satisfont ϕ et dans ceux qui satisfont ψ. Par conséquent, la même remarque vaut pour tous les modèles de $\Gamma \cup \Gamma' \cup \Gamma''$: la formule θ est vraie dans ces modèles qui vérifient ψ et également dans ceux qui vérifient ϕ. Or, la réunion des modèles qui vérifient ψ et de ceux qui vérifient ϕ constitue bien l'ensemble des modèles de $\Gamma \cup \Gamma' \cup \Gamma''$, puisque la formule $\psi \vee \phi$ est vraie dans tous ces modèles. Il s'en suit donc $\Gamma, \Gamma', \Gamma'' \models \theta$.

aff

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi} \; {\scriptstyle aff}$$

Ici, tout est immédiat, puisque si l'on a $\Gamma \models \psi$, on a *a fortiori* $\Gamma, \phi \models \psi$.

ctr

$$\frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi} \; {\scriptstyle ctr}$$

Ici, il n'y a rien à montrer, puisque $\Gamma, \phi, \phi \models \psi$ et $\Gamma, \phi \models \psi$ disent rigoureusement la même chose.

$\perp c$

$$\frac{\Gamma, \neg\phi \vdash \perp}{\Gamma \vdash \phi} \perp c$$

Par hypothèse d'induction, nous avons $\Gamma, \neg\phi \vDash \perp$. Autrement dit, il n'y a aucun modèle de Γ dans lequel la formule $\neg\phi$ soit vraie. Cela revient à dire que la formule $\neg\phi$ est fausse dans tous les modèles de Γ. Par la définition même de l'interprétation sémantique du connecteur de négation, dire que la formule $\neg\phi$ est fausse dans tous les modèles de Γ, c'est dire que la formule ϕ est vraie dans ces mêmes modèles.

Ainsi se termine la preuve du sens facile du théorème de complétude. Nous savons désormais que la vérité syntaxique implique la vérité sémantique.

"$\Gamma \vDash \phi$ **implique** $\Gamma \vdash_c \phi$"

Soit ϕ, une formule quelconque du Calcul Propositionnel dont les variables sont parmi $\{P_1, \ldots, P_n\}$. Etant donné $\mathcal{M}$, un modèle possible de ϕ (c'est-à-dire un modèle dans lequel des valeurs de vérité sont attribuées aux variables propositionnelles $P_1, \ldots, P_n$), on note

- $P_i^{\mathcal{M}} = P_i$ si la variable propositionnelle P_i est vraie dans $\mathcal{M}$,
- $P_i^{\mathcal{M}} = \neg P_i$ dans le cas contraire.

On pose également :

- $\phi^{\mathcal{M}} = \phi$ si $\mathcal{M} \vDash \phi$,
- $\phi^{\mathcal{M}} = \neg\phi$ dans le cas contraire (si $\mathcal{M} \nvDash \phi$, c'est-à-dire si $\mathcal{M} \vDash \neg\phi$).

Par induction sur la hauteur de ϕ on montre le résultat préparatoire suivant :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi^{\mathcal{M}}.$$

(1) Si la hauteur de ϕ est 0, alors ϕ est une variable propositionnelle P_i et il est immédiat que :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c P_i^{\mathcal{M}}.$$

(2) Si la hauteur de ϕ est n+1, alors :

(a) Si $\phi = \neg\psi$ deux cas se présentent :

(A) Si $\mathcal{M} \vDash \phi$, alors $\phi^{\mathcal{M}} = \phi = \neg\psi$. Comme la hauteur de ψ est n, nous pouvons appliquer l'hypothèse d'induction. En effet, nous savons que :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \psi^{\mathcal{M}}.$$

Or, $\mathcal{M} \vDash \phi$ entraîne que $\mathcal{M} \nvDash \psi$ et donc $\psi^{\mathcal{M}} = \neg\psi = \phi$, d'où le résultat.

(B) Si $\mathcal{M} \not\models \phi$, alors $\phi^{\mathcal{M}} = \neg\phi = \neg\neg\psi$. Par hypothèse d'induction, nous savons que :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \psi^{\mathcal{M}}.$$

Or, $\mathcal{M} \not\models \phi$ entraîne que $\mathcal{M} \models \psi$ et donc $\psi^{\mathcal{M}} = \psi$. Il suffit alors d'utiliser le théorème démontré dans l'exemple 122 pour obtenir le résultat. En effet, dans cet exemple, nous avons prouvé le séquent $\vdash \theta \to \neg\neg\theta$ et ici nous avons $\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \psi^{\mathcal{M}}$. Par *modus ponens* il résulte alors :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\neg\psi^{\mathcal{M}}.$$

Ce qui donne le résultat recherché puisque $\neg\neg\psi^{\mathcal{M}} = \neg\neg\psi = \phi^{\mathcal{M}}$.

(b) Si $\phi = \phi_0 \longrightarrow \phi_1$, deux cas se présentent :

(A) Si $\mathcal{M} \not\models \phi_0$, alors $\mathcal{M} \models \phi$ et donc $\phi^{\mathcal{M}} = \phi$, et $\phi_0^{\mathcal{M}} = \neg\phi_0$. Par hypothèse d'induction nous avons :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}}$$

c'est-à-dire :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_0.$$

Considérons la règle suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\overline{\neg\phi_0, \phi_0 \vdash \phi_0}\,{\scriptstyle ax+aff} \qquad \overline{\neg\phi_0, \phi_0 \vdash \neg\phi_0}\,{\scriptstyle ax+aff}}{\neg\phi_0, \phi_0 \vdash \bot}\,{\scriptstyle \bot i}}{\neg\phi_0, \phi_0 \vdash \phi_1}\,{\scriptstyle \bot c}}{\neg\phi_0 \vdash \phi_0 \to \phi_1}\,{\scriptstyle \to i}}{\vdash \neg\phi_0 \to (\phi_0 \to \phi_1)}\,{\scriptstyle \to i}$$

En utilisant cette règle et le *modus ponens* nous obtenons :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0 \to \phi_1.$$

Ce qui est le résultat recherché puisque $\phi_0 \to \phi_1 = \phi^{\mathcal{M}}$.

(B) Si $\mathcal{M} \models \phi_0$, alors :

(1) Si $\mathcal{M} \models \phi_1$, alors $\mathcal{M} \models \phi$ et donc $\phi^{\mathcal{M}} = \phi$, $\phi_0^{\mathcal{M}} = \phi_0$ et $\phi_1^{\mathcal{M}} = \phi_1$. Par hypothèse d'induction nous avons :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}} \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1^{\mathcal{M}}$$

c'est-à-dire :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0 \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1.$$

Le résultat est quasi immédiat, puisque de :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1$$

on déduit par affaiblissement

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\}, \phi_0 \vdash_c \phi_1$$

puis par introduction de l'implication :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0 \to \phi_1.$$

(2) Si $\mathcal{M} \not\models \phi_1$, alors $\mathcal{M} \not\models \phi$ et donc $\phi^{\mathcal{M}} = \neg\phi$, $\phi_0^{\mathcal{M}} = \phi_0$ et $\phi_1^{\mathcal{M}} = \neg\phi_1$. Par hypothèse d'induction nous avons :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}} \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1^{\mathcal{M}}$$

c'est-à-dire :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0 \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_1.$$

D'où l'on déduit immédiatement que :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0 \wedge \neg\phi_1.$$

Considérons la règle suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\phi_0\wedge\neg\phi_1 \vdash \phi_0\wedge\neg\phi_1}\,{\scriptstyle ax}}{\phi_0\wedge\neg\phi_1 \vdash \neg\phi_1}\,{\scriptstyle \wedge e_d} \qquad \dfrac{\dfrac{\dfrac{}{\phi_0\wedge\neg\phi_1 \vdash \phi_0\wedge\neg\phi_1}\,{\scriptstyle ax}}{\phi_0\wedge\neg\phi_1 \vdash \phi_0}\,{\scriptstyle \wedge e_g} \qquad \dfrac{}{\phi_0\to\phi_1 \vdash \phi_0\to\phi_1}\,{\scriptstyle ax}}{\phi_0\wedge\neg\phi_1, \phi_0\to\phi_1 \vdash \phi_1}\,{\scriptstyle \to e}}{\phi_0\wedge\neg\phi_1, \phi_0\to\phi_1 \vdash \bot}\,{\scriptstyle \neg e}}{\phi_0\wedge\neg\phi_1 \vdash \neg(\phi_0\to\phi_1)}\,{\scriptstyle \neg i}}{\vdash (\phi_0\wedge\neg\phi_1)\to\neg(\phi_0\to\phi_1)}\,{\scriptstyle \to i}$$

Ensuite, il suffit d'appliquer la règle du *modus ponens* pour obtenir :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg(\phi_0 \to \phi_1)$$

qui est précisément le résultat recherché.

(c) Si $\phi = \phi_0 \vee \phi_1$ deux cas se présentent :

(A) Si $\mathcal{M} \not\models \phi$ alors nécessairement $\mathcal{M} \not\models \phi_0$ et $\mathcal{M} \not\models \phi_1$. Par conséquent, $\mathcal{M} \models \neg\phi$ et donc $\phi^{\mathcal{M}} = \neg\phi$, $\phi_0^{\mathcal{M}} = \neg\phi_0$ et $\phi_1^{\mathcal{M}} = \neg\phi_1$. Par hypothèse d'induction, nous avons :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}} \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1^{\mathcal{M}}$$

c'est-à-dire :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_0 \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_1.$$

D'où :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_0 \wedge \neg\phi_1.$$

Considérons la règle suivante :

$$\dfrac{\dfrac{\dfrac{}{\phi_0\vee\phi_1 \vdash \phi_0\vee\phi_1}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{\dfrac{}{\neg\phi_0\wedge\neg\phi_1 \vdash \neg\phi_0\wedge\neg\phi_1}\,{\scriptstyle ax}}{\neg\phi_0\wedge\neg\phi_1 \vdash \neg\phi_0}\,{\scriptstyle \wedge e_g} \qquad \dfrac{}{\phi_0 \vdash \phi_0}\,{\scriptstyle ax}}{\neg\phi_0\wedge\neg\phi_1, \phi_0 \vdash \perp}\,{\scriptstyle \neg e} \qquad \dfrac{\dfrac{\dfrac{}{\neg\phi_0\wedge\neg\phi_1 \vdash \neg\phi_0\wedge\neg\phi_1}\,{\scriptstyle ax}}{\neg\phi_0\wedge\neg\phi_1 \vdash \neg\phi_1}\,{\scriptstyle \wedge e_d} \qquad \dfrac{}{\phi_1 \vdash \phi_1}\,{\scriptstyle ax}}{\neg\phi_0\wedge\neg\phi_1, \phi_1 \vdash \perp}\,{\scriptstyle \neg e}}{\dfrac{\neg\phi_0\wedge\neg\phi_1, \phi_0\vee\phi_1 \vdash \perp}{\neg\phi_0\wedge\neg\phi_1 \vdash \neg(\phi_0\vee\phi_1)}\,{\scriptstyle \neg i}}\,{\scriptstyle \vee e}}{\vdash (\neg\phi_0\wedge\neg\phi_1)\to\neg(\phi_0\vee\phi_1)}\,{\scriptstyle \to i}$$

A l'aide de cette règle et du *modus ponens*, nous obtenons le résultat recherché :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg(\phi_0\vee\phi_1).$$

(B) Si $\mathcal{M} \models \phi$ alors nécessairement $\mathcal{M} \models \phi_0$ ou bien $\mathcal{M} \models \phi_1$. Par symétrie, supposons que $\mathcal{M} \models \phi_0$. On a donc par hypothèse d'induction :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}}$$

avec $\phi_0^{\mathcal{M}} = \phi_0$. En appliquant la règle de l'introduction de la disjonction on obtient :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0\wedge\phi_1$$

c'est-à-dire précisément :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi^{\mathcal{M}}.$$

(d) Si $\phi = \phi_0\wedge\phi_1$, deux cas se présentent :

(A) Si $\mathcal{M} \models \phi$, alors nécessairement $\mathcal{M} \models \phi_0$ et $\mathcal{M} \models \phi_1$. On a donc par hypothèse d'induction :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}} \quad \text{et} \quad \{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1^{\mathcal{M}}$$

c'est-à-dire :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0 \quad \text{et} \quad \{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_1.$$

D'où l'on déduit immédiatement, par application de la règle d'introduction de la conjonction :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0\wedge\phi_1$$

c'est-à-dire :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi^{\mathcal{M}}.$$

(B) Si $\mathcal{M} \not\models \phi$, alors nécessairement $\mathcal{M} \not\models \phi_0$ ou $\mathcal{M} \not\models \phi_1$. Par conséquent, $\phi^{\mathcal{M}} = \neg\phi$, et, ou bien $\phi_0^{\mathcal{M}} = \neg\phi_0$, ou bien $\phi_1^{\mathcal{M}} = \neg\phi_1$. Par symétrie, supposons que nous avons $\mathcal{M} \not\models \phi_0$ et donc $\phi_0^{\mathcal{M}} = \neg\phi_0$. Par hypothèse d'induction nous avons :

$$\{P_1^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi_0^{\mathcal{M}}$$

c'est-à-dire :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_0.$$

D'où par application de la règle d'introduction de la disjonction :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg\phi_0 \vee \neg\phi_1.$$

Considérons la règle suivante :

$$\dfrac{\dfrac{\dfrac{}{\phi_0 \vee \phi_1 \vdash \phi_0 \vee \phi_1}\,{\scriptstyle ax} \quad \dfrac{\dfrac{\dfrac{}{\phi_0 \wedge \phi_1 \vdash \phi_0 \wedge \phi_1}\,{\scriptstyle ax}}{\phi_0 \wedge \phi_1 \vdash \phi_0}\,{\scriptstyle \wedge e_g} \quad \dfrac{}{\neg\phi_0 \vdash \neg\phi_0}\,{\scriptstyle ax}}{\neg\phi_0 \wedge \neg\phi_1, \phi_0 \vdash \bot}\,{\scriptstyle \neg e} \quad \dfrac{\dfrac{\dfrac{}{\phi_0 \wedge \phi_1 \vdash \phi_0 \wedge \phi_1}\,{\scriptstyle ax}}{\phi_0 \wedge \phi_1 \vdash \phi_1}\,{\scriptstyle \wedge e_d} \quad \dfrac{}{\neg\phi_1 \vdash \neg\phi_1}\,{\scriptstyle ax}}{\neg\phi_0 \wedge \neg\phi_1, \phi_1 \vdash \bot}\,{\scriptstyle \neg e}}{\dfrac{\neg\phi_0 \vee \neg\phi_1, \phi_0 \wedge \phi_1 \vdash \bot}{\neg\phi_0 \vee \neg\phi_1 \vdash \neg(\phi_0 \wedge \phi_1)}\,{\scriptstyle \neg i}}\,{\scriptstyle \vee e}}{\vdash (\neg\phi_0 \vee \neg\phi_1) \rightarrow \neg(\phi_0 \wedge \phi_1)}\,{\scriptstyle \rightarrow i}$$

A l'aide de cette règle et du *modus ponens*, nous obtenons le résultat recherché :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \neg(\phi_0 \wedge \phi_1).$$

Ceci termine, pour tout formule ϕ, la preuve du résultat préparatoire :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi^{\mathcal{M}}.$$

Nous allons maintenant prouver que pour toute formule ϕ, si ϕ est une tautologie, alors ϕ est un théorème de la logique classique.

Soit ϕ, une formule quelconque du Calcul Propositionnel dont les variables sont $P_1, \ldots, P_n$. Et $\mathcal{M}$, un modèle possible de ϕ (c'est-à-dire aussi un modèle de ϕ puisque ϕ est une tautologie). Nous avons montré que :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi^{\mathcal{M}}$$

or, $\mathcal{M} \models \phi$ est vérifié, donc $\phi^{\mathcal{M}} = \phi$. D'où :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_n^{\mathcal{M}}\} \vdash_c \phi.$$

Mais puisque ce résultat est valable pour n'importe quel modèle, considérons $\mathcal{M}$ et $\mathcal{M}'$ qui ne diffèrent qu'en ce que $\mathcal{M} \models P_n$, alors que $\mathcal{M}' \models \neg P_n$. Pour toutes les autres variables P_i $(i < n)$, les deux modèles distribuent les mêmes valeurs de vérité (c'est-à-dire $\mathcal{M} \models P_i$ ssi $\mathcal{M}' \models P_i$).

D'après le résultat préparatoire, nous avons à la fois :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_{n-1}^{\mathcal{M}}, P_n{}^{\mathcal{M}}\} \vdash_c \phi \quad \text{et} \quad \{P_1{}^{\mathcal{M}'}, \ldots, P_{n-1}^{\mathcal{M}'}, P_n{}^{\mathcal{M}'}\} \vdash_c \phi$$

d'où :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_{n-1}^{\mathcal{M}}, P_n\} \vdash_c \phi \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_{n-1}^{\mathcal{M}}, \neg P_n\} \vdash_c \phi$$

ou pour l'écrire autrement :

$$\{P_1{}^{\mathcal{M}}, \ldots, P_{n-1}^{\mathcal{M}}\}, P_n \vdash_c \phi \quad \text{et} \quad \{P_1{}^{\mathcal{M}}, \ldots, P_{n-1}^{\mathcal{M}}\}, \neg P_n \vdash_c \phi.$$

Par application du tiers exclu, on remarque que l'on a la règle suivante :

$$\dfrac{\overline{\vdash \psi \vee \neg\psi} \quad \overline{\Gamma, \psi \vdash \phi} \quad \overline{\Gamma, \neg\psi \vdash \phi}}{\Gamma \vdash \phi}\ \vee e$$

En appliquant cette règle à notre cas, nous obtenons finalement :

$$\{P_1{}^{\mathcal{M}}, \dots, P_{n-1}^{\mathcal{M}}\} \vdash_c \phi$$

et ce résultat est vrai pour n'importe quel modèle $\mathcal{M}$! En recommençant le même raisonnement on obtient, successivement :

$$\{P_1{}^{\mathcal{M}}, \dots, P_{n-2}^{\mathcal{M}}\} \vdash_c \phi\ , \quad \{P_1{}^{\mathcal{M}}, \dots, P_{n-3}^{\mathcal{M}}\} \vdash_c \phi\ , \quad \{P_1{}^{\mathcal{M}}, \dots, P_{n-4}^{\mathcal{M}}\} \vdash_c \phi\ , \dots$$

On arrive ainsi finalement à :

$$P_1 \vdash_c \phi \quad \text{et} \quad \neg P_1 \vdash_c \phi.$$

D'où l'on déduit $\vdash_c \phi$ par application du tiers exclu.

Nous avons donc montré que $\models \phi$ implique $\vdash_c \phi$. Il nous reste encore à montrer que pour toute formule ϕ et pour tout ensemble fini d'hypothèse $\Gamma = \{\psi_0, \dots, \psi_k\}$, $\Gamma \models \phi$ implique $\Gamma \vdash_c \phi$.

Or, il apparait immédiatement que :

$$\Gamma \models \phi \text{ si et seulement si } \models (\psi_0 \wedge \psi_1 \wedge \dots \wedge \psi_k) \rightarrow \phi.$$

Par le résultat précédent sur les tautologies nous en déduisons :

$$\vdash_c (\psi_0 \wedge \psi_1 \wedge \dots \wedge \psi_k) \rightarrow \phi.$$

Par ailleurs, de manière tout à fait évidente nous avons

$$\Gamma \vdash_c (\psi_0 \wedge \psi_1 \wedge \dots \wedge \psi_k).$$

Par conséquent, une simple application du *modus ponens* nous donne :

$$\Gamma \vdash_c \phi.$$

⊣ 139

Corollaire 141 *Soient ϕ, ψ deux formules du Calcul Propositionnel,*

$$\phi \equiv \psi \quad \textit{ssi} \quad \phi \equiv_c \psi.$$

Preuve du Corollaire 141 : C'est une conséquence immédiate du Théorème 139 puisque $\phi \equiv \psi$ si et seulement si à la fois $\phi \models \psi$ et $\psi \models \phi$ si et seulement si à la fois $\phi \vdash_c \psi$ et $\psi \vdash_c \phi$ si et seulement si $\phi \equiv_c \psi$. ⊣ 141

Remarque 142 On rappelle que $\mathcal{M} \models \Gamma$ si chaque formule ϕ de Γ est vraie dans le modèle $\mathcal{M}$ ($\mathcal{M} \models \phi$). Une conséquence immédiate du théorème de complétude est que pour toute théorie finie Γ, et pour tout modèle $\mathcal{M}$ de cette théorie, si une formule est démontrable à partir des hypothèses Γ, alors elle est vraie dans ce modèle $\mathcal{M}$. Autrement dit, toute formule qui est une conséquence syntaxique d'une théorie est vraie dans tous les modèles de cette théorie. Tout ce que l'on peut déduire d'une théorie est vrai dans un modèle quelconque de cette théorie.

$$\text{si } \Gamma \vdash_c \phi \text{ et } \mathcal{M} \models \Gamma \text{ alors } \mathcal{M} \models \phi.$$

Le théorème de complétude de la logique classique nous dit finalement que la sémantique que nous avons prise en considération pour le Calcul Propositionnel correspond à la logique classique – on pourrait d'ailleurs parler à cet égard de *"sémantique classique"*. Donc, s'il est vrai que la logique classique a un pouvoir expressif supérieur à la logique intuitionniste, cette même sémantique ne peut correspondre à cette dernière. Autrement dit, si nous voulons établir un théorème de complétude pour la logique intuitionniste, il nous faudra prendre en compte une sémantique qui soit différente de la sémantique classique. Pour ce faire, nous allons introduire dans la section qui suit, la *sémantique des mondes possibles*, encore appelée *sémantique de Kripke.*

Pour aller plus avant :

La Déduction Naturelle est due à Gerhard Gentzen [Sza69]. Elle renonce à la linéarité des preuves dans les systèmes formels "à la Hilbert" au profit d'une structure arborescente rendant plus "naturelle" la formalisation du raisonnement usuel. Une variante de la déduction naturelle, due à Frederic Brenton Fitch [Fit52], est souvent enseignée en lieu et place de la présentation originelle de Gentzen. Pour une présentation approfondie de la Déduction Naturelle, le lecteur pourra se reporter à l'*"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* de René David, Karim Nour et Christophe Raffalli [DNR04], *"Proofs and types"* de Jean-Yves Girard, Yves Lafont et traduit par Paul Taylor [GTL89], *"Le point aveugle, tome 1 : vers la perfection"* de Jean-Yves Girard [Gir06], *"Logique moderne"* de Jean-Blaise Grize [Gri73], *"A first course in logic : an introduction to model theory, proof theory, computability, and complexity"* de Shawn Hedman [Hed04], *"Introduction to mathematical logic"* d'Elliot Mendelson [Men97], *"Natural Deduction : A Proof-Theoretical Study"* de Dag Prawitz [Pra06], *"Proof Theory"* de Gaisi Takeuti [Tak13], *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00].

La logique intuitionniste – développée à l'origine par le hollandais Luitzen Egbertus Jan Brouwer [Bro23], puis ses élèves Valéry Glivenko et Arend Heyting – est apparue comme une position mathématique rejetant comme n'étant pas intuitives, certaines formes du raisonnement classique au profit des seules formes dites *constructives.* A la notion classique de vérité, la logique intuitionniste préfère celle de *"prouvabilité constructive"*. Là où un énoncé quelconque est soit vrai soit faux en logique classique, en logique intuitionniste, il est soit prouvable (de manière constructive), soit il ne l'est pas. Il existe ainsi des énoncés (ϕ) qui ne sont pas prouvables de manière constructive tout comme leurs négations ($\neg\phi$). Par conséquent le principe du *tiers exclu* ($\phi \vee \neg\phi$) se trouve pris en défaut puisqu'une preuve constructive de $\phi \vee \neg\phi$ passe nécessairement par une preuve soit de ϕ soit de $\neg\phi$. Andreï Kolmogorov [Kol25], puis Kurt Gödel [Göd86] ont montré que l'on peut représenter la logique classique à l'intérieur de la logique intuitionniste : pour toute formule prouvable en logique classique, il existe une formule équivalente [4] – équivalente en logique classique ! – qui est prouvable en logique intuitionniste [5]. Par ailleurs, la logique intuitionniste permet, grâce à l'isomorphisme de Curry-Howard, de mettre en correspondance les preuves à l'intérieur d'un système logique et les programmes utilisés en informatique, comme nous le verrons dans le chapitre 17. Le lecteur qui souhaiterait creuser ce sujet, pourra se plonger dans l'ouvrage de Jean van Heijenoort , intitulé *"From Freege to Gödel : A Source Book in Mathematical Logic, 1879-1931"* [vH77] : ainsi que dans celui de Martin Davis : *"Engines of Logic : Mathematicians and the Origin of the Computer"* [Dav01].

---

4. Voir Définition 466.
5. Voir Théorème 468.

4 Les modèles de Kripke du Calcul Propositionnel intuitionniste

***Résumé* № 19** *La sémantique des* mondes possibles *de Kripke relie entre eux de manière arborescente des modèles du Calcul Propositionnel. Un modèle de Kripke est un arbre de modèles de la logique classique. L'évaluation des formules change et repose sur la notion de* "forcing"*, définie localement pour chaque monde possible en fonction toutefois des relation de ce monde avec tous ses descendants. Une formule est vraie dans un modèle de Kripke si elle est* "forcée" *dans chaque monde possible. Les modèles de Kripke de la logique intuitionniste induisent une notion de conséquence sémantique –* $\models_i$ *– qui coïncide avec la notion de conséquence syntaxique en logique intuitionniste.*

$$\mathcal{T} \models_i \phi \text{ ssi } \mathcal{T} \vdash_i \phi.$$

※

Nous venons de montrer que la notion de vérité sémantique et la notion de vérité syntaxique coïncident. Autrement dit, une formule est une tautologie si et seulement si elle est prouvable dans la logique classique. Mais qu'en est-il de la prouvabilité intuitionniste ? Que peut-on dire d'une formule qui est prouvable dans la logique intuitionniste ? Bien sûr, une telle formule est prouvable dans la logique classique et donc est une tautologie. Mais existe-t-il une approche sémantique différente de celle que nous avons présentée et qui corresponde à la prouvabilité en logique intuitionniste ?

Les modèles de Kripke sont une telle réponse. Ils permettent de copier trait pour trait la proposition *une formule est démontrable en logique classique si et seulement si elle est vraie dans tous les modèles (classiques) possibles.* On a en effet *une formule est démontrable en logique intuitionniste si et seulement si elle est réalisée dans tous les modèles de Kripke possibles.* Ainsi, on peut voir les modèles de Kripke comme les modèles de la logique intuitionniste.

Définition 143 *Soit* $\{P_1, \ldots, P_k)$ *un ensemble de variables propositionnelles,* $\mathcal{K} = (T_\mathcal{K}, \Vdash)$ *est un modèle de Kripke arborescent fini portant sur les variables* $P_1, \ldots, P_k$ *si :*

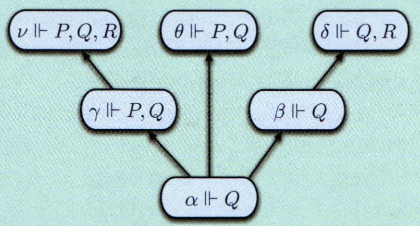
(1) $T_\mathcal{K}$ *est un arbre fini dont la relation d'ancestralité entre deux nœuds est notée par* $\alpha \leq \beta$*, ce qui signifie que* α *est un ancêtre de* β*, ou pour le dire autrement, il y a une branche de l'arbre qui contient à la fois* α *et* β*, telle que* α *soit plus proche de la racine que* β *ou bien* $\alpha = \beta$*.*

(2) $\Vdash$ *est une relation binaire appelée relation de* forcing *entre d'une part les nœuds de* $T_\mathcal{K}$ *et d'autre part les variables propositionnelles, qui vérifie :*

   (a) pour **tout** *nœud* α *:* $\alpha \nVdash \bot$

   (b) pour tout nœuds α, β *et variable propositionnelle* P_i*, si à la fois* $\alpha \leq \beta$ *et* $\alpha \Vdash P_i$ *alors on a* $\beta \Vdash P_i$*.*

Exemple 144 un modèle de Kripke portant sur les variables propositionnelles P, Q, R



Remarque 145

(1) Il faut voir un modèle de Kripke comme un arbre dont les nœuds sont comme des modèles classiques du Calcul Propositionnel. Au sens où à chacun des nœuds sont spécifiées les variables qui sont "vraies". Une bonne intuition des modèles de Kripke consiste à interpréter la relation d'ancestralité comme une relation de temporalité. Ainsi, intuitivement, $\alpha \leq \beta$ signifie α est antérieur à β et $\alpha \Vdash P_i$ signifie que P_i est vrai au temps α. Mais attention, il ne s'agit pas d'un temps linéaire, plutôt d'un temps arborescent. Pour le dire autrement, la relation d'ordre $\leq$ n'est pas une relation totale, il peut y avoir des éléments incomparables pour cette relation d'ordre. C'est le cas lorsque α et β ne sont l'ancêtre ni de l'un, ni de l'autre. La condition (2)(b) dit alors précisément que si quelque chose est vrai au temps α, alors cette même chose doit être vraie aux temps futurs (les temps β tels que $\alpha \leq \beta$).

(2) Un modèle de Kripke qui n'aurait qu'un seul nœud peut être vu comme un modèle de la logique classique. En effet, les conditions de la relation de forcing ($\Vdash$) sont alors identiques à celles de la relation de vérité sémantique ($\models$).

Tout comme dans le cas classique, nous avons étendu la notion de vérité transportée par les distributions de valeurs de vérité des simples variables popositionnelles aux formules, la relation de forcing est également étendue aux formules.

Définition 146 *Soit $\mathcal{K} = (T_{\mathcal{K}}, \Vdash)$ un modèle de Kripke arborescent fini portant sur les variables $P_1, \ldots, P_k$, α un nœud de $T_{\mathcal{K}}$ et ϕ, ψ des formules du Calcul Propositionnel dont les variables sont parmi $\{P_1, \ldots, P_k\}$,*

(1) $\alpha \Vdash \phi \wedge \psi$ ssi $\alpha \Vdash \phi$ et $\alpha \Vdash \psi$.

(2) $\alpha \Vdash \phi \vee \psi$ ssi $\alpha \Vdash \phi$ ou $\alpha \Vdash \psi$.

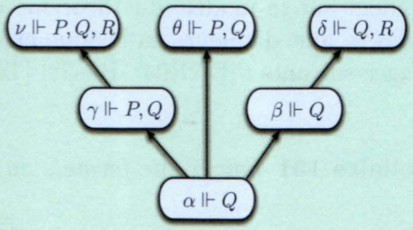
(3) $\alpha \Vdash \phi \longrightarrow \psi$ ssi pour tout nœud β de $T_{\mathcal{K}}$ tel que $\alpha \leq \beta$, si $\beta \Vdash \phi$ alors $\beta \Vdash \psi$.

(4) $\alpha \Vdash \neg\phi$ ssi pour tout nœud β de $T_{\mathcal{K}}$ tel que $\alpha \leq \beta$, $\beta \nVdash \phi$.
En fait la négation $\neg\phi$ est interprétée comme la formule $\phi \longrightarrow \perp$. D'où, par définition de la condition de forcing de l'implication : $\alpha \Vdash \phi \longrightarrow \perp$ ssi pour tout nœud β de $T_{\mathcal{K}}$ tel que $\alpha \leq \beta$, si $\beta \Vdash \phi$ alors $\beta \Vdash \perp$. Or, la condition $\beta \Vdash \perp$ est interdite par définition des modèles de la logique intuitionniste, donc $\beta \Vdash \perp$ n'est satisfait nulle

part, d'où la formulation de la négation en termes de "$\beta \Vdash \phi$ n'est safisfait en aucun nœud au-dessus de α". (On verra plus loin que la condition qu'aucun nœud ne force le faux n'est plus de mise pour les modèles de la logique minimale).

Exemple 147 Ainsi, dans le modèle présenté dans l'exemple 144, nous avons les relations de forcing suivantes :

- $\theta \Vdash Q \wedge P$ mais $\beta \nVdash P \wedge Q$
- $\alpha \Vdash P \longrightarrow Q$ mais $\alpha \nVdash Q \longrightarrow P$
- $\beta \Vdash \neg P$ mais $\alpha \nVdash \neg P$
- $\gamma \Vdash \neg Q \vee P$ mais $\alpha \nVdash P \vee \neg P$
- $\alpha \nVdash P$, $\alpha \nVdash \neg P$ et $\alpha \nVdash \neg\neg P$



Définition 148 *Soit $\mathcal{K} = (T_{\mathcal{K}}, \Vdash)$ un modèle de Kripke arborescent fini portant sur les variables $P_1, \dots, P_k$, α un nœud de $T_{\mathcal{K}}$, ϕ une formule et Γ un ensemble fini de formules dont toutes les variables sont parmi $\{P_1, \dots, P_k)$,*

(1) $\alpha \Vdash \Gamma$ ssi $\alpha \Vdash \psi$ pour toute formule de Γ.

(2) ϕ (respectivement Γ) est **réalisée** *dans $\mathcal{K}$ si pour tout nœud α de $T_{\mathcal{K}}$, $\alpha \Vdash \phi$ (respectivement $\alpha \Vdash \Gamma$).*

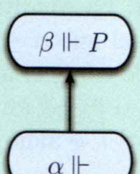
(3) ϕ est conséquence intuitionniste de Γ (noté $\Gamma \vDash_i \phi$) ssi pour tout modèle de Kripke $\mathcal{K} = (T_{\mathcal{K}}, \Vdash)$ et tout nœud α si $\alpha \Vdash \Gamma$ alors $\alpha \Vdash \phi$.

En particulier, on note $\vDash_i \phi$ si ϕ est réalisée dans tout modèle de Kripke.

Exemple 149 Un modèle de Kripke dans lequel ni le tiers exclu ($P \vee \neg P$), ni l'élimination des doubles négations ($\neg\neg P \longrightarrow P$) ne sont réalisés, puisque on remarque en effet que :

(1) $\alpha \nVdash P$ par définition et $\alpha \nVdash \neg P$ puisque $\alpha \leq \beta$ et $\beta \Vdash P$. Donc $\alpha \nVdash P \vee \neg P$.

(2) $\alpha \nVdash \neg P$ et $\beta \nVdash \neg P$ d'où $\alpha \Vdash \neg\neg P$ et $\beta \Vdash \neg\neg P$. D'où $\beta \Vdash \neg\neg P \longrightarrow P$ et $\alpha \nVdash \neg\neg P \longrightarrow P$.



4.1 Le théorème de complétude de la logique intuitionniste

Les modèles de Kripke, tels que nous les avons présentés, offrent une sémantique pour la logique intuitionniste au sens où ils permettent de prouver le résultat qui suit.

Théorème 150 *Soient Γ un ensemble fini de formules et ϕ une formule du Calcul Propositionnel,*

$$\Gamma \models_i \phi \quad ssi \quad \Gamma \vdash_i \phi.$$

Preuve du Théorème 150 : Les preuves de ce théorème sont longues et fastidieuses. Elles s'appuient sur le modèle du théorème de complétude de la logique classique (les preuves usuelles se font d'ailleurs en logique classique). Nous renvoyons le lecteur intéressé vers les ouvrages suivants : [DNR04] [Bus98] [TvD88] [TS00] [Tak13].

$\dashv$ 150

Corollaire 151 *Soit ϕ une formule du Calcul Propositionnel,*

$$\models_i \phi \quad ssi \quad \vdash_i \phi.$$

Preuve du Corollaire 151 : Le résultat est un cas particulier du Théorème 150 en prenant pour Γ un ensemble d'hypothèses qui soit vide. $\dashv$ 150

4.2 Le théorème de complétude de la logique minimale

Si la logique minimale possède un pouvoir expressif moindre par rapport à la logique intuitionniste, il nous faut une sémantique appropriée qui soit distincte de celle offerte par les modèles de Kripke tels que nous les avons vus. En ne changeant qu'un tout petit rien à ces modèles, on obtient la sémantique recherchée.

Définition 152 *Soit $\{P_1, \ldots, P_k)$ un ensemble de variables propositionnelles, $\mathcal{K} = (T_{\mathcal{K}}, \Vdash)$ est un modèle de Kripke* **minimal** *arborescent fini portant sur les variables $P_1, \ldots, P_k$ si :*

(1) $T_{\mathcal{K}}$ est un arbre fini dont la relation d'ancestralité entre nœuds est notée $\alpha \leq \beta$;

(2) $\Vdash$ est une relation binaire entre les nœuds de $T_{\mathcal{K}}$ et les variables propositionnelles, qui vérifie : pour tout nœud α, β et variable propositionnelle P_i, si à la fois $\alpha \leq \beta$ et $\alpha \Vdash P_i$ alors on a $\beta \Vdash P_i$.

Remarque 153

(1) Comme on le voit aisément, la notion de modèle de Kripke de la logique minimale n'est rien d'autre que celle de modèle de Kripke en général, dans laquelle la condition (2)(a) : pour **tout** nœud α : $\alpha \nVdash \perp$, a été abandonnée.

(2) Attention ! La condition $\alpha \Vdash \neg\phi$ n'est plus définie par : $\alpha \Vdash \neg\phi$ ssi pour tout nœud β de $T_{\mathcal{K}}$ tel que $\alpha \leq \beta$, $\beta \nVdash \phi$. Il faut en effet se souvenir que la négation $\neg\phi$ est interprétée comme la formule $\phi \longrightarrow \perp$. D'où, ici, la définition de la négation par la condition $\alpha \Vdash \neg\phi$ ssi $\alpha \Vdash \phi \longrightarrow \perp$, c'est-à-dire ssi pour tout nœud β de $T_{\mathcal{K}}$ tel que $\alpha \leq \beta$, si $\beta \Vdash \phi$ alors $\beta \Vdash \perp$.

Sur cette base, on définit à chaque nœud les mêmes extensions de la relation de forcing des variables propositionnelles aux formules. On définit de même les notions de réalisabilité et de conséquence logique minimale, que l'on note cette fois-ci $\Gamma \models_m \phi$. Cela permet d'obtenir le théorème de complétude de la logique minimale suivant.

Théorème 154 *Soient Γ un ensemble fini de formules et ϕ une formule du Calcul Propositionnel,*

$$\Gamma \models_m \phi \quad ssi \quad \Gamma \vdash_m \phi.$$

Preuve du Théorème 154 : Nous renvoyons le lecteur vers [DNR04] [Bus98] [TvD88] [TS00] [Tak13]. $\dashv$ 154

Corollaire 155 *Soit ϕ une formule du Calcul Propositionnel,*

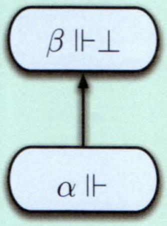
$$\models_m \phi \quad ssi \quad \vdash_m \phi.$$

Preuve du Corollaire 155 : La preuve est immédiate en prenant $\Gamma = \emptyset$. $\dashv$ 155

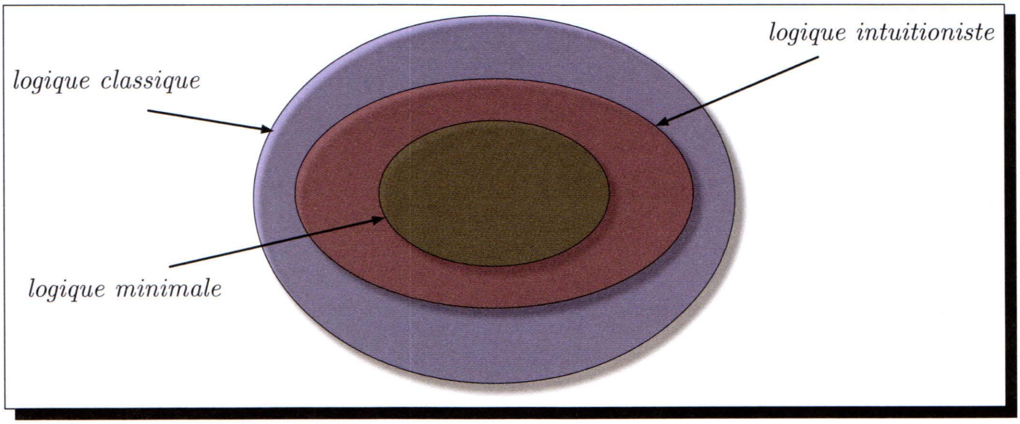
Exemple 156 un modèle de Kripke de la logique minimale dans lequel $\neg\neg(\neg\neg P \to P)$ n'est pas réalisé.

(1) (a) $\beta \nVdash P$ par définition,
   (b) d'où $\beta \Vdash \neg P$.
   (c) Mais également $\beta \Vdash \neg\neg P$ puisque $\beta \Vdash \bot$.
   (d) Mais alors $\beta \nVdash \neg\neg P \to P$.
   (e) Par conséquent $\beta \Vdash \neg(\neg\neg P \to P)$,
   (f) et toujours à cause du fait que $\beta \Vdash \bot$, on obtient $\beta \Vdash \neg\neg(\neg\neg P \to P)$.

(2) (a) $\alpha \nVdash P$ et $\beta \nVdash P$ par définition,
   (b) d'où $\alpha \Vdash \neg P$.
   (c) Mais $\alpha \nVdash \neg\neg P$ puisque $\alpha \nVdash \bot$.
   (d) On a aussi $\alpha \nVdash \neg\neg P \to P$ pour la raison que $\beta \Vdash \neg\neg P$ et $\beta \nVdash P$.
   (e) Par conséquent $\alpha \Vdash \neg(\neg\neg P \to P)$ puisqu'à la fois $\alpha \nVdash \neg\neg P \to P$ et $\beta \nVdash \neg\neg P \to P$.
   (f) d'où $\alpha \nVdash \neg\neg(\neg\neg P \to P)$ puisqu'à la fois $\alpha \Vdash \neg(\neg\neg P \to P)$ et $\alpha \nVdash \bot$.



Cela montre qu'il existe un nœud du modèle qui ne force pas la formule $\neg\neg(\neg\neg P \to P)$. Par conséquent, en utilisant le théorème de complétude de la logique minimale, on obtient directement que $\neg\neg(\neg\neg P \to P)$ n'est pas un théorème de la logique minimale. Comme nous avions montré que cette même formule était un théorème de la logique intuitionniste, nous savons donc que le séquent $\vdash \neg\neg(\neg\neg P \to P)$ est prouvable en logique intuitionniste mais pas en logique minimale. Ce qui prouve que la logique minimale forme un sous-ensemble strict de la logique intuitionniste, elle-même strictement inclue dans la logique classique. Plus précisément, si l'on appelle logique classique (resp. intuitionniste, minimale) l'ensemble des formules qui sont des théorèmes – c'est-à-dire des formules prouvables sans hypothèse – de la logique classique (resp. intuitionniste, minimale), alors nous obtenons le schéma suivant :



Pour aller plus avant :

Nous renvoyons le lecteur qui désirerait en savoir plus sur les modèles de Kripke des logiques intuitionniste et minimale, au manuel de René David, Karim Nour et Christophe Raffalli : *"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* [DNR04]. Il trouvera également quelques éléments dans les ouvrages suivants : *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00], *"Proof Theory"* de Gaisi Takeuti [Tak13] et *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02].

---

5 Le Calcul des Séquents

***Résumé* № 20** *Le Calcul des Séquents repose sur la notion de séquent. Mais contrairement à la Déduction Naturelle qui mettait en jeu des séquents de la forme $\Gamma \vdash \phi$ – où ϕ était une formule et Γ un ensemble de formules –, le Calcul des Séquents symétrise la notion de séquent qui prend la forme $\Gamma \vdash \Delta$, où Δ est également un ensemble de formules. Un tel séquent s'interprète comme* "la conjonction des formules de Γ prouve la disjonction des formules de Δ".
A l'exception de la règle de coupure, chacune des règles est une règle d'introduction, que ce soit à gauche ou à droite du symbole de séquent. La logique intuitionniste se retrouve en Calcul des Séquents en ce qu'elle ne conserve des démonstrations que les seules qui ne font jamais qu'intervenir qu'une seule formule – à contraction près – à droite du symbole de séquent.
La règle de coupure peut être omise – au prix de démonstrations généralement beaucoup plus longues – résultat qui permet de montrer la consistance du Calcul Propositionnel : une contradiction ne peut être démontrée sans hypothèse.

※

Le Calcul des Séquents est postérieur de quelques années à la Déduction Naturelle. Son intérêt consiste non seulement à rendre compte de la notion de démonstration, mais, plus encore que la Déduction Naturelle, à en dégager les propriétés mathématiques essentielles.

Ce faisant, le Calcul des Séquents s'éloigne du cararctère naturel des démonstrations telles qu'elles apparaîssaient avec la Déduction Naturelle. Il n'y a plus vraiment de preuves de théorèmes ou de déductions de formules. Il ne reste qu'un jeu sur les séquents, moins adapté à la construction de preuve qu'à la description de ces constructions.

Les deux différences principales, avec la Déduction Naturelle sont, d'une part, que la partie droite des séquents n'est plus constituée d'une seule formule conclusion mais d'un ensemble fini de formules, et d'autre part, que les règles d'élimination sont remplacées par des règles d'introduction à gauche, rendant ainsi le système de démonstration totalement symétrique, avec des règles d'introduction à droite et à gauche, se répondant en miroir.

Définition 157 *Un séquent (noté $\Gamma \vdash \Delta$) est un couple où :*

- *Γ est un ensemble fini de formules, appelé la partie gauche du séquent,*
- *Δ est également un ensemble fini de formules, appelé la partie droite du séquent.*

Remarque 158 Intuitivement, un séquent $\Gamma \vdash \Delta$ où $\Gamma = \{\phi_0, \ldots, \phi_n\}$ et $\Delta = \{\psi_0, \ldots, \psi_k\}$ est interprété comme $\bigwedge_{0 \le i \le n} \phi_i \vdash \bigvee_{0 \le j \le k} \psi_j$.

La partie gauche est donc une conjonction d'hypothèses comme dans la Déduction Naturelle, mais la partie droite doit être vue comme une disjonction de conclusions plutôt qu'une seule conclusion. Ainsi, la conjonction vide d'hypothèse est interprétée comme le vrai, alors que la disjonction vide de conclusion est interprétée comme le faux. Conformément à cela, le séquent $\vdash \Delta$ signifie $(\psi_0 \vee \psi_1 \vee \ldots \vee \psi_k)$, alors que le séquent $\Gamma \vdash$ signifie $(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n) \longrightarrow \perp$, c'est-à-dire $\neg(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n)$. Pour finir, le séquent " $\vdash$", qui signifie "vrai implique faux", est interprété comme l'absurde (il correspond au séquent $\vdash \perp$ de la Déduction Naturelle).

Les règles du Calcul des Séquents

Les règles du Calcul des Séquents sont très proches de celles de la Déduction Naturelle. Elles conservent en particulier le fait que d'un ensemble de *prémisses* (il peut y en avoir 0,1 ou 2), on déduit un séquent *conclusion* et elles sont représentées avec les prémisses au-dessus d'une barre horizontale et la conclusion en dessous. De même, les règles d'introduction de la Déduction Naturelle sont conservées. Elles deviennent des règles d'*introduction à droite.* Les règles d'élimination sont remplacées par des règles d'*introduction à gauche.*

On retrouve également une règle pour les axiomes, des règles logiques et des règles structurelles. Mais chose nouvelle, une règle de coupure est introduite :

$$\frac{\Gamma \vdash \phi, \Delta \qquad \Gamma', \phi \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ {\scriptstyle cut}$$

Cette notion de coupure correspond à la partie non mécanique de l'activité démonstrative. C'est elle qui permet l'utilisation d'énoncés généraux, de principes que l'on démontre une fois pour toute et que l'on applique ensuite à des cas particuliers. Ceci est une pratique courante des mathématiques où l'on fait grand usage de ces démonstrations indirectes. On démontre une formule ϕ d'hypothèses Γ en se servant d'un résultat général ψ qu'on sait déduire de ces mêmes hypothèses Γ et dont on montre qu'il entraîne ϕ. En Déduction Naturelle, cela correspond aux deux prémisses $\Gamma \vdash \psi$ et $\psi \vdash \phi$ desquelles on déduit $\Gamma \vdash \phi$. La propriété générale ψ est intervenue dans la démonstration telle un messager qui n'a de valeur que transitoire. Elle permet de relier Γ à ϕ, puis, une fois cette opération réalisée, elle disparaît. Les coupures évitent ainsi de devoir refaire des démonstrations complètes pour chaque cas particulier, permettant de s'appuyer sur des démonstrations plus générales.

Le problème qui apparaît alors est que cette règle de coupure permet de faire disparaître hypothèses et conclusion. Comment alors être certain qu'on ne peut pas dès lors faire apparaître le séquent vide ($\vdash$) ? C'est une question grave, car si tel était le cas, nous nous retrouverions avec un système de démonstration qui prouverait l'absurde, et donc prouverait n'importe quoi. Un tel système serait bon à jeter aux oubliettes et à nous renvoyer à nos chères études...

A cause du remplacement des règles d'élimination par des règles d'introduction à gauche, les règles logiques du Calcul des Séquents ne permettent pas d'élimination. C'est la raison pour laquelle on introduit cette règle de coupure qui permet de rétablir la transitivité dans les déductions : si l'on a prouvé avec l'hypothèse A que B et avec l'hypothèse B que C, alors on a prouvé que C avec l'hypothèse A. Cette règle de coupure est donc extrêmement naturelle. Elle correspond à la manière habituelle dont les raisonnements se déroulent.

Exemple 159 Une preuve en Calcul des Séquents du tiers exclu $\vdash \phi \vee \neg\phi$:

$$\dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}\ {\scriptstyle ax}}{\vdash \phi, \neg\phi}\ {\scriptstyle \neg_d}}{\vdash \phi \vee \neg\phi}\ {\scriptstyle \vee_d}$$

Calcul des Séquents

Axiomes

$$\frac{}{\phi \vdash \phi}\ {\scriptstyle ax} \qquad\qquad \frac{}{\bot \vdash}\ {\scriptstyle \bot_g}$$

Règles logiques

$$\frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta}\ {\scriptstyle \wedge_g} \qquad\qquad \frac{\Gamma \vdash \phi, \Delta \qquad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta,}\ {\scriptstyle \wedge_d}$$

$$\frac{\Gamma, \phi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta}\ {\scriptstyle \vee_g} \qquad\qquad \frac{\Gamma \vdash \phi, \psi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta}\ {\scriptstyle \vee_d}$$

$$\frac{\Gamma \vdash \phi, \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \to \psi \vdash \Delta}\ {\scriptstyle \to_g} \qquad\qquad \frac{\Gamma, \phi \vdash \psi, \Delta}{\Gamma \vdash \phi \to \psi, \Delta}\ {\scriptstyle \to_d}$$

$$\frac{\Gamma \vdash \phi, \Delta}{\Gamma, \neg\phi \vdash \Delta}\ {\scriptstyle \neg_g} \qquad\qquad \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \neg\phi, \Delta}\ {\scriptstyle \neg_d}$$

Règles structurelles

$$\frac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \Delta}\ {\scriptstyle aff_g} \qquad\qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \phi, \Delta}\ {\scriptstyle aff_d}$$

$$\frac{\Gamma, \phi, \phi \vdash \Delta}{\Gamma, \phi \vdash \Delta}\ {\scriptstyle ctr_g} \qquad\qquad \frac{\Gamma \vdash \phi, \phi, \Delta}{\Gamma \vdash \phi, \Delta}\ {\scriptstyle ctr_d}$$

Règle de coupure

$$\frac{\Gamma \vdash \phi, \Delta \qquad \Gamma', \phi \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ {\scriptstyle cut}$$

FIGURE 3.4 – Règles du Calcul des Séquents en logique classique.

Exemple 160 Une preuve en Calcul des Séquents de $\vdash \phi \to \neg\neg\phi$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\phi, \neg\phi \vdash}\,{\scriptstyle \neg_g}}{\phi \vdash \neg\neg\phi}\,{\scriptstyle \neg_d}}{\vdash \phi \to \neg\neg\phi}\,{\scriptstyle \to_d}$$

Exemple 161 Une preuve de l'élimination des doubles négations $\vdash \neg\neg\phi \to \phi$ en Calcul des Séquents :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\vdash \phi, \neg\phi}\,{\scriptstyle \neg_d}}{\neg\neg\phi \vdash \phi}\,{\scriptstyle \neg_g}}{\vdash \neg\neg\phi \to \phi}\,{\scriptstyle \to_d}$$

Exemple 162 Une preuve en Calcul des Séquents de la contraposition $\neg\psi \to \neg\phi \vdash \phi \to \psi$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\psi \vdash \psi}\,{\scriptstyle ax}}{\vdash \neg\psi, \psi}\,{\scriptstyle \neg_d}}{\phi \vdash \neg\psi, \psi}\,{\scriptstyle aff_g} \qquad \dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\phi, \neg\phi \vdash}\,{\scriptstyle \neg_g}}{\phi, \neg\phi \vdash \psi}\,{\scriptstyle aff_d}}{\neg\psi \to \neg\phi, \phi \vdash \psi}\,{\scriptstyle \to_g}}{\neg\psi \to \neg\phi \vdash \phi \to \psi}\,{\scriptstyle \to_d}$$

Exemple 163 Une preuve en Calcul des Séquents du troisième axiome du système de Hilbert – voir page 188 – $\vdash (\neg\psi \to \neg\phi) \to ((\neg\psi \to \phi) \to \psi)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\psi \vdash \psi}\,{\scriptstyle ax}}{\vdash \neg\psi, \psi}\,{\scriptstyle \neg_d}}{\neg\psi \to \neg\phi \vdash \neg\psi, \psi}\,{\scriptstyle aff_g} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\psi \vdash \psi}\,{\scriptstyle ax}}{\vdash \neg\psi, \psi}\,{\scriptstyle \neg_d}}{\phi \vdash \neg\psi, \psi}\,{\scriptstyle aff_g} \qquad \dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}}{\phi, \neg\phi \vdash}\,{\scriptstyle \neg_g}}{\phi, \neg\phi \vdash, \psi}\,{\scriptstyle aff_d}}{\neg\psi \to \neg\phi, \phi \vdash \psi}\,{\scriptstyle \to_g}}{\neg\psi \to \neg\phi, \neg\psi \to \phi \vdash \psi}\,{\scriptstyle \to_g}}{\neg\psi \to \neg\phi \vdash (\neg\psi \to \phi) \to \psi}\,{\scriptstyle \to_d}}{\vdash (\neg\psi \to \neg\phi) \to ((\neg\psi \to \phi) \to \psi)}\,{\scriptstyle \to_d}$$

Arrêtons-nous un instant sur les Exemples 160 et 161. La différence majeure entre les deux formules $\phi \longrightarrow \neg\neg\phi$ et $\neg\neg\phi \longrightarrow \phi$ – qui sont pourtant très semblables – est que la première est prouvable en logique intuitionniste alors que la seconde ne l'est pas. Si l'on regarde de près les deux preuves, nous devons bien admettre que nous avons fait quasiment la même chose dans l'une et l'autre. A la petite différence tout de même que dans la première preuve, nous avons d'abord effectué une introduction de la négation à droite avant d'effectuer la même introduction de la négation, mais à gauche cette fois. Alors que dans la seconde démonstration, nous avons d'abord effectué l'introduction de la négation à gauche avant celle de droite.

C'est que les logiques intuitionniste et minimale se trouvent avoir chacune une caractérisation extrêmement simple en Calcul des Séquents.

Théorème 164 *la logique intuitionniste est la version du Calcul des Séquents dont les règles sont restreintes aux séquents avec au plus une formule à droite, la contraction à droite étant considérée comme implicite.*

La table de ces règles est présentée dans la Figure 3.5, dans laquelle le symbole Δ tient lieu d'un ensemble contenant *au plus* une unique formule.

Théorème 165 *la logique minimale est la version du Calcul des Séquents diminuée de la règle de l'affaiblissement droit*[6] *et dont les règles sont restreintes aux séquents avec au plus une formule à droite*[7].

Preuve des Théorèmes 164 *et* 165 : Nous renvoyons ici encore le lecteur vers le manuel [DNR04], ainsi que [Bus98] [TvD88] *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00], [Tak13]. ⊣ 164 & 165

Exemple 166 Une preuve en Calcul des Séquents de $\vdash \neg\neg(\neg\neg\phi \to \phi)$:

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$\scriptstyle ax$}
\UnaryInfC{$\phi \vdash \phi$}
\RightLabel{$\scriptstyle aff\ g$}
\UnaryInfC{$\phi, \neg\neg\phi \vdash \phi$}
\RightLabel{$\scriptstyle \to\ d$}
\UnaryInfC{$\phi \vdash \neg\neg\phi \to \phi$}
\AxiomC{}
\RightLabel{$\scriptstyle ax$}
\UnaryInfC{$\neg\neg\phi \to \phi \vdash \neg\neg\phi \to \phi$}
\RightLabel{$\scriptstyle \neg\ g$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi), \neg\neg\phi \to \phi \vdash$}
\RightLabel{$\scriptstyle cut$}
\BinaryInfC{$\neg(\neg\neg\phi \to \phi), \phi \vdash$}
\RightLabel{$\scriptstyle \neg\ d$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi) \vdash \neg\phi$}
\RightLabel{$\scriptstyle \neg\ g$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi), \neg\neg\phi \vdash$}
\RightLabel{$\scriptstyle aff\ d$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi), \neg\neg\phi \vdash \phi$}
\RightLabel{$\scriptstyle \to\ d$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi) \vdash \neg\neg\phi \to \phi$}
\RightLabel{$\scriptstyle \neg\ g$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi), \neg(\neg\neg\phi \to \phi) \vdash$}
\RightLabel{$\scriptstyle ctr\ g$}
\UnaryInfC{$\neg(\neg\neg\phi \to \phi) \vdash$}
\RightLabel{$\scriptstyle \neg\ d$}
\UnaryInfC{$\vdash \neg\neg(\neg\neg\phi \to \phi)$}
\end{prooftree}
$$

6. Si l'on y songe, la règle de l'affaiblissement droit n'est pas autre chose que la règle de l'absurde intuitionniste.
7. La contraction à droite n'est ici pas considérée comme implicite.

Calcul des Séquents

Axiomes

$$\frac{}{\phi \vdash \phi}\, ax \qquad \frac{}{\bot \vdash}\, \bot_g$$

Règles logiques

$$\frac{\Gamma, \phi, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta}\, \wedge_g \qquad \frac{\Gamma \vdash \phi \qquad \Gamma \vdash \psi}{\Gamma \vdash \phi \wedge \psi}\, \wedge_d$$

$$\frac{\Gamma, \phi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta}\, \vee_g \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\, \vee_{d1} \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\, \vee_{d2}$$

$$\frac{\Gamma \vdash \phi \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \to \psi \vdash \Delta}\, \to_g \qquad \frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\, \to_d$$

$$\frac{\Gamma \vdash \phi}{\Gamma, \neg\phi \vdash}\, \neg_g \qquad \frac{\Gamma, \phi \vdash}{\Gamma \vdash \neg\phi}\, \neg_d$$

Règles structurelles

$$\frac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \Delta}\, \mathit{aff}_g \qquad \frac{\Gamma \vdash}{\Gamma \vdash \phi}\, \mathit{aff}_d$$

$$\frac{\Gamma, \phi, \phi \vdash \Delta}{\Gamma, \phi \vdash \Delta}\, ctr_g$$

Règle de coupure

$$\frac{\Gamma \vdash \phi \qquad \Gamma', \phi \vdash \Delta}{\Gamma, \Gamma' \vdash, \Delta}\, cut$$

FIGURE 3.5 – Règles du Calcul des Séquents en logique intuitionniste.

Exemple 167 Une preuve en Calcul des Séquents du premier axiome du système de Hilbert - voir page 188 - $\vdash \phi \rightarrow (\psi \rightarrow \phi)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}{\scriptstyle ax}}{\phi, \psi \vdash \phi}{\scriptstyle aff_g}}{\phi \vdash \psi \rightarrow \phi}{\scriptstyle \rightarrow_d}}{\vdash \phi \rightarrow (\psi \rightarrow \phi)}{\scriptstyle \rightarrow_d}$$

Exemple 168 Une preuve en Calcul des Séquents du second axiome du système de Hilbert - voir page 188 - $\vdash (\phi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \theta))$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\phi \vdash \phi}{\scriptstyle ax}}{\psi \rightarrow \theta, \phi \vdash \phi}{\scriptstyle aff_g} \quad \dfrac{\dfrac{\dfrac{}{\psi \vdash \psi}{\scriptstyle ax} \quad \dfrac{}{\theta \vdash \theta}{\scriptstyle ax}}{\psi, \psi \rightarrow \theta \vdash \theta}{\scriptstyle \rightarrow_g} \quad \dfrac{\dfrac{}{\phi \vdash \phi}{\scriptstyle ax} \quad \dfrac{}{\psi \vdash \psi}{\scriptstyle ax}}{\phi \rightarrow \psi, \phi \vdash \psi}}{\psi \rightarrow \theta, \phi \rightarrow \psi, \phi \vdash \theta}{\scriptstyle cut}}{\phi \rightarrow (\psi \rightarrow \theta), \phi \rightarrow \psi, \phi \vdash \theta}{\scriptstyle \rightarrow_g}}{\phi \rightarrow (\psi \rightarrow \theta), \phi \rightarrow \psi \vdash \phi \rightarrow \theta}{\scriptstyle \rightarrow_d}}{\phi \rightarrow (\psi \rightarrow \theta) \vdash (\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \theta)}{\scriptstyle \rightarrow_d}}{\vdash (\phi \rightarrow (\psi \rightarrow \theta)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \theta))}{\scriptstyle \rightarrow_d}$$

Ainsi, dans l'Exemple 160, sur chaque nœud de l'arbre de preuve, il n'y a jamais qu'au plus une formule à droite du symbole de séquent, alors que dans l'Exemple 161, il y a un nœud de l'arbre de preuve qui en contient deux et, dans l'Exemple 159, exactement trois nœuds de l'arbre de preuve de $\phi \vee \neg\phi$ en contiennent deux, dont l'un des trois n'en contient en réalité qu'une "à contraction près". Dans l'exemple 166, chaque nœud de l'arbre de preuve ne contient qu'au plus une formule à droite du symbole de séquent, par contre la règle de l'affaiblissement droit est utilisée, ce qui fait que cette preuve se situe dans le cadre de la logique intuitionniste mais pas de la logique minimale.

5.1 L'élimination des coupures

La règle de coupure en Calcul des Séquents correspond à la règle suivante en Déduction Naturelle :

$$\dfrac{\Gamma, \phi \vdash \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}{\scriptstyle cut}$$

Pour être plus précis, elle correspond donc, en Déduction Naturelle, à l'introduction de l'implication suivie aussitôt de son élimination :

$$\dfrac{\dfrac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\,{\scriptstyle \to_i} \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\,{\scriptstyle \to_e}$$

C'est une règle absolument essentielle pour rendre compte de la manière dont nous raisonnons. En effet, la plupart des raisonnements que nous faisons consistent à utiliser des conclusions de raisonnements antérieurs comme hypothèses pour de nouvelles démonstrations, hypothèses que par ailleurs, nous faisons disparaître sur la base du fait que nous les avons démontrées. De manière presque caricaturale, les raisonnements de la vie courante prennent la forme suivante : nous montrons que si nous avons A alors nous avons B, et par ailleurs que si nous avons B, alors nous avons C. Nous déduisons de cela qu'avec l'hypothèse A nous avons C. La conclusion intermédiaire B a disparu, mais elle était nécessaire pour atteindre C à partir de A. "Si je veux réussir cet examen, il faut que je puisse répondre correctement à des questions du même type que celles qui se trouvent dans les feuilles d'exercices distribuées chaque semaine. Or, une bonne manière de répondre à ce genre de question, c'est de s'y préparer en faisant les exercices régulièrement. Donc, si je veux réussir l'examen, il est bien que je m'y prépare en rendant une feuille d'exercices chaque semaine".

Pour le dire autrement, la règle de coupure correspond à l'utilisation de principes abstraits et généraux dans les raisonnements. Cela est particulièrement frappant dans l'activité mathématique : avec certaines hypothèses, on prouve une propriété générale, puis on prouve que le résultat souhaité est une conséquence de cette propriété générale. Cette dernière n'apparaît plus dans le résultat final, mais elle lui aura pourtant servi de tremplin.

Théorème 169 (Elimination des coupures) *S'il existe, en Calcul des Séquents classique (resp. intuitionniste), une preuve du séquent $\Gamma \vdash \Delta$, alors il existe une preuve en Calcul des Séquents classique (resp. intuitionniste) de ce séquent sans utilisation de la règle de coupure.*

Preuve du Théorème 169 : La preuve est longue et fastidieuse. Encore une fois nous renvoyons le lecteur vers d'autres ouvrages tels que [DNR04] [Bus98] [TvD88] [TS00] [Tak13]. $\dashv$ 169

Ce théorème extrêmement important justifie à lui seul la mise sur pied du Calcul des Séquents. Il affirme que l'on peut toujours se passer de la règle de coupure pour obtenir un séquent prouvable en logique classique. Mais, si l'on peut faire fi de la règle de coupure, cela signifie que tout séquent $\Gamma \vdash \Delta$ prouvable peut l'être par l'utilisation des seuls axiomes, règles logiques et règles structurelles. La preuve de ce théorème n'est pas vraiment difficile mais longue et fastidieuse puisqu'il faut remplacer dans une preuve donnée chaque utilisation de la règle de coupure par d'autres règles logiques.

Ce résultat a deux conséquences majeures :

Corollaire 170 *Le séquent " $\vdash$" n'est pas prouvable en logique classique.*

Rappelons que le séquent " $\vdash$" est intuitivement interprété par le vrai entraîne le faux. Il correspond à $\vdash \bot$ en Déduction Naturelle. On peut voir ainsi directement, par utilisation des règles d'affaiblissement, que si $\vdash$ était prouvable en Calcul des Séquents, alors n'importe lequel des séquents $\Gamma \vdash \Delta$ le serait également. La conséquence serait que toute la théorie de la démonstration s'écroulerait comme un château de carte. Il est absolument primordial que l'on ne puisse pas prouver ce séquent qui entraîne une absurdité généralisée, le non-sens absolu, en un mot le chaos le plus inextricable.

Preuve du Corollaire 170 : La preuve est immédiate : s'il existait une preuve de ce séquent en Calcul des Séquents, il en existerait également une qui se ferait sans utilisation de la règle de coupure. Or, toutes les autres règles introduisent une formule soit à droite, soit à gauche, soit des deux côtés à la fois. La seule règle qui permet de faire disparaître une formule est la règle de contraction, mais celle-ci ne fait pas disparaître une formule, elle ne fait disparaître qu'une des occurrences multiples d'une formule. Il est donc immédiat qu'il n'y a pas de preuve sans coupure du séquent " $\vdash$". Par application du théorème d'élimination des coupures, il n'y a donc pas de preuve (avec ou sans coupure) du séquent " $\vdash$". La Théorie de la démonstration est sauve.

$\dashv$ 170

Corollaire 171 (Propriété de la sous-formule) *Si le séquent $\Gamma \vdash \Delta$ est prouvable en logique classique (resp. en logique intuitionniste), alors il existe une preuve en logique classique (resp. en logique intuitionniste) de ce séquent dans laquelle n'apparaîssent que des séquents constitués de sous-formules des formules de Γ et de Δ.*

Preuve du Corollaire 171 : Par application du théorème de l'élimination des coupures, il existe une preuve sans coupure de $\Gamma \vdash \Delta$. Or, une telle preuve satisfait les conditions souhaitées. Cela se vérifie immédiatement règle par règle, par induction sur la hauteur d'une preuve sans coupure.

$\dashv$ 171

Une conséquence de la propriété de la sous-formule est qu'une preuve d'une disjonction en logique intuitionniste passe nécessairement par une preuve d'un des termes de la disjonction :

$$\vdash_i \phi \vee \psi \quad \text{si et seulement si} \quad \Big(\vdash_i \phi \text{ ou } \vdash_i \psi \Big).$$

Ainsi, par exemple, lorsqu'on prouve une instance du tiers exclu de la forme $\Gamma \vdash_i \phi \vee \neg\phi$ en logique intuitionniste, c'est parce qu'on a été capable soit de prouver $\Gamma \vdash_i \phi$, soit de prouver $\Gamma \vdash_i \neg\phi$, ce qui bien sûr n'est pas le cas en logique classique où $\Gamma \vdash_i \phi \vee \neg\phi$ est une conséquence immédiate du principe du tiers exclu.

Une conséquence majeure de la propriété de la sous-formule, qui elle-même repose directement sur l'élimination des coupures, est de permettre, tout particulièrement en logique intuitionniste, une recherche de preuve automatique. On peut ainsi mettre en place des "prouveurs automatiques" dont la tâche est la production mécanique de preuves, comme par exemple les preuves de programmes. Le caractère nécessairement abstrait des preuves par coupures étant oublié, ces machines recherchent des preuves, certes plus longues mais aussi plus simples dans le fait qu'elles ne font appel qu'aux sous-formules des formules du séquent qu'il s'agit de prouver.

5.2 Traduction de Gödel-Kolmogorov

Entre logique classique, intuitionniste et minimale, la logique minimale est la moins expressive des trois. Pourtant, il existe pour chaque formule ϕ une formule ϕ^g qui soit équivalente

– en logique classique ! – à ϕ et telle que ϕ^g est prouvable en logique minimale si ϕ est prouvable en logique classique.

On peut donc se passer de la logique classique et intuitionniste, à condition d'accepter d'effectuer, pour toute formule, la traduction qui suit.

Définition 172 (Traduction de Gödel-Kolmogorov) *Soit ϕ une formule du Calcul Propositionnel. La traduction de Gödel-Kolmogorov de ϕ (notée ϕ^g) est la formule définie par induction sur la hauteur de ϕ de la façon suivante :*

(1) $\bot^g = \bot$;

(2) $P^g = \neg\neg P$, *(P variable prop.)* ;

(3) $(\neg\phi)^g = \neg\phi^g$;

(4) $(\phi \wedge \psi)^g = \phi^g \wedge \psi^g$;

(5) $(\phi \vee \psi)^g = \neg\neg\,(\phi^g \vee \psi^g)$;

(6) $(\phi \longrightarrow \psi)^g = \phi^g \longrightarrow \psi^g$.

Notation 173 *Pour Γ un ensemble de formules du Calcul Propositionnel, Γ^g désigne l'ensemble des traductions de Gödel-Kolmogorov des formules de Γ :*

$$\Gamma^g = \{\phi^g \mid \phi \in \Gamma\}.$$

Théorème 174 *Pour tous Γ et ϕ, respectivement un ensemble de formules et une formule :*

$$\Gamma \vdash_c \phi \text{ ssi } \Gamma^g \vdash_m \phi^g.$$

Preuve du Théorème 174 : Nous renvoyons le lecteur à l'ouvrage de René David, Karim Nour et Christophe Raffalli : *"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* [DNR04], ainsi qu'à [Tak13][TS00].

$\dashv$ 174

Exemple 175 La traduction de Gödel-Kolmogorov de $P \vee \neg P$ donne :

$$(P \vee \neg P)^g = \neg\neg\,(\neg\neg P \vee \neg\neg\neg P).$$

Alors que $\vdash P \vee \neg P$ n'est prouvable qu'en logique classique, $\vdash (P \vee \neg P)^g$ est prouvable en logique minimale :

$$\AxiomC{}\RightLabel{ax}\UnaryInfC{$P \vdash P$}\RightLabel{$\neg_d$}\UnaryInfC{$\vdash P, \neg P$}\RightLabel{$\vee_d$}\UnaryInfC{$\vdash P \vee \neg P$}\DisplayProof$$

$$\AxiomC{}\RightLabel{ax}\UnaryInfC{$\neg\neg P \vdash \neg\neg P$}\RightLabel{$\vee_{d1}$}\UnaryInfC{$\neg\neg P \vdash \neg\neg P \vee \neg\neg\neg P$}\RightLabel{$\neg_g$}\UnaryInfC{$\neg\,(\neg\neg P \vee \neg\neg\neg P), \neg\neg P \vdash$}\RightLabel{$\neg_d$}\UnaryInfC{$\neg\,(\neg\neg P \vee \neg\neg\neg P) \vdash \neg\neg\neg P$}\RightLabel{$\vee_{d2}$}\UnaryInfC{$\neg\,(\neg\neg P \vee \neg\neg\neg P) \vdash \neg\neg P \vee \neg\neg\neg P$}\RightLabel{$\neg_g$}\UnaryInfC{$\neg\,(\neg\neg P \vee \neg\neg\neg P), \neg\,(\neg\neg P \vee \neg\neg\neg P) \vdash$}\RightLabel{$ctr_g$}\UnaryInfC{$\neg\,(\neg\neg P \vee \neg\neg\neg P) \vdash$}\RightLabel{$\neg_d$}\UnaryInfC{$\vdash \neg\neg\,(\neg\neg P \vee \neg\neg\neg P)$}\DisplayProof$$

Exemple 176 La traduction de Gödel-Kolmogorov de $\neg\neg P \to P$ donne : $\neg\neg\neg P \to \neg\neg P$.

La formule de l'élimination des doubles négations : $\vdash \neg\neg P \to P$ n'est prouvable qu'en logique classique, alors que sa traduction de Gödel-Kolmogorov $\vdash (\neg\neg P \to P)^g$ est prouvable en logique minimale :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$\scriptstyle ax$}
\UnaryInfC{$P \vdash P$}
\RightLabel{$\scriptstyle \neg_d$}
\UnaryInfC{$\vdash P, \neg P$}
\RightLabel{$\scriptstyle \neg_g$}
\UnaryInfC{$\neg\neg P \vdash P$}
\RightLabel{$\scriptstyle \to_d$}
\UnaryInfC{$\vdash \neg\neg P \to P$}
\end{prooftree}
\qquad
\begin{prooftree}
\AxiomC{}
\RightLabel{$\scriptstyle ax$}
\UnaryInfC{$\neg P \vdash \neg P$}
\RightLabel{$\scriptstyle \neg_g$}
\UnaryInfC{$\neg\neg P, \neg P \vdash$}
\RightLabel{$\scriptstyle \neg_d$}
\UnaryInfC{$\neg P \vdash \neg\neg\neg P$}
\RightLabel{$\scriptstyle \neg_g$}
\UnaryInfC{$\neg\neg\neg\neg P, \neg P \vdash$}
\RightLabel{$\scriptstyle \neg_d$}
\UnaryInfC{$\neg\neg\neg\neg P \vdash \neg\neg P$}
\RightLabel{$\scriptstyle \to d$}
\UnaryInfC{$\vdash \neg\neg\neg\neg P \to \neg\neg P$}
\end{prooftree}
$$

Exemple 177 La contraposition : $\neg Q \longrightarrow \neg P \vdash P \longrightarrow Q$ n'est prouvable qu'en logique classique – voir Exemple 162 – alors que sa traduction de Gödel-Kolmogorov

$$(\neg Q \longrightarrow \neg P)^g \vdash (P \longrightarrow Q)^g = \neg\neg\neg Q \longrightarrow \neg\neg\neg P \vdash \neg\neg P \longrightarrow \neg\neg Q$$

est prouvable en logique minimale :

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{$\scriptstyle ax$}
\UnaryInfC{$\neg Q \vdash \neg Q$}
\RightLabel{$\scriptstyle \neg_d$}
\UnaryInfC{$\neg Q, \neg\neg Q \vdash$}
\RightLabel{$\scriptstyle \neg_g$}
\UnaryInfC{$\neg Q \vdash \neg\neg\neg Q$}
\RightLabel{$\scriptstyle aff_g$}
\UnaryInfC{$\neg\neg\neg P, \neg Q \vdash \neg\neg\neg Q$}
\AxiomC{}
\RightLabel{$\scriptstyle ax$}
\UnaryInfC{$\neg\neg P \vdash \neg\neg P$}
\RightLabel{$\scriptstyle \neg_g$}
\UnaryInfC{$\neg\neg\neg P, \neg\neg P \vdash$}
\RightLabel{$\scriptstyle aff_g$}
\UnaryInfC{$\neg Q, \neg\neg\neg P, \neg\neg P \vdash$}
\RightLabel{$\scriptstyle ctr_g$}
\BinaryInfC{$\neg Q, \neg\neg\neg P, \neg\neg\neg Q \longrightarrow \neg\neg\neg P, \neg\neg P, \neg Q \vdash$}
\RightLabel{$\scriptstyle ctr_g$}
\UnaryInfC{$\neg\neg\neg P, \neg\neg\neg Q \longrightarrow \neg\neg\neg P, \neg\neg P, \neg Q \vdash$}
\RightLabel{$\scriptstyle \to_g$}
\UnaryInfC{$\neg\neg\neg Q \longrightarrow \neg\neg\neg P, \neg\neg P, \neg Q \vdash$}
\RightLabel{$\scriptstyle \neg_d$}
\UnaryInfC{$\neg\neg\neg Q \longrightarrow \neg\neg\neg P, \neg\neg P \vdash \neg\neg Q$}
\RightLabel{$\scriptstyle \to d$}
\UnaryInfC{$\neg\neg\neg Q \longrightarrow \neg\neg\neg P \vdash \neg\neg P \longrightarrow \neg\neg Q$}
\end{prooftree}
$$

Pour aller plus avant :

A nouveau, nous renvoyons le lecteur qui désirerait s'aventurer plus loin dans le domaine du Calcul des Séquents, au manuel de René David, Karim Nour et Christophe Raffalli : *"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* [DNR04], ainsi qu'aux ouvrages *"Proof Theory"* de Gaisi Takeuti [Tak13] et *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00]. Le lecteur particulièrement motivé pourra également consulter les ouvrages *"Le point aveugle, tome 1 : vers la perfection"* de Jean-Yves Girard [Gir06] ou *"Proofs and types"* de Jean-Yves Girard, Paul Taylor et Yves Lafont [GTL89], bien que leurs contenus correspondent plutôt à la logique dont nous traiterons dans la troisième partie de cet ouvrage [8].

---

8. La partie Logique du 1er ordre.

Deuxième partie

Logique Modale

Préambule

– *Now what is the message there?*
– *The message is that there are known "knowns."*
– *There are things we know that we know.*
– *There are known unknowns.*
– *That is to say there are things that we now know we don't know.*
– *But there are also unknown unknowns.*
– *There are things we do not know we don't know.*
– *So when we do the best we can and we pull all this information together, and we then say well that's basically what we see as the situation, that is really only the known knowns and the known unknowns.*
– *And each year, we discover a few more of those unknown unknowns.*

Donald Rumsfeld[1]

Qu'est-ce que la logique modale ?

Le Calcul Propositionnel est une logique fruste, d'utilisation restreinte et pour tout dire, de pouvoir expressif très limité. Une des manières d'étendre le champ d'application du Calcul propositionnel consiste à lui adjoindre des opérateurs de modalité. Ainsi complété, le Calcul (ou Logique) Propositionnel(le) se transforme en Logique Modale. Ces opérateurs de modalité fonctionnent comme autant de conditions particulières d'appréhension de formules. Par exemple, étant donnée une formule du Calcul Propositionnel ϕ, nous pourrons écrire $\Box\phi$, ou aussi $\Diamond\phi$. opérateurs de modalité sont ces symboles $\Box$, ou $\Diamond$ qui se lisent respectivement `carré` ou bien `boîte` pour le premier et `losange` ou `diamant` pour le second. Les deux formules ainsi constituées : $\Box\phi$ et $\Diamond\phi$ correspondent alors à deux modes différents sur lesquels sont compris ce que *raconte* la formule ϕ.

Chacun de ces deux modes donne naissance à une formule de la logique modale qui est différente de la simple formule ϕ. Ainsi présenté, un opérateur de modalité n'apparaît pas fort différent d'un connecteur logique. Qu'est-ce qui distingue par exemple $\Box$ ou $\Diamond$ de la négation $\neg$? Tous trois semblent être des connecteurs unaires, c'est-à-dire des symboles qui, placés devant une formule quelconque, servent à créer une nouvelle formule. Qu'est ce qui distingue $\Box\phi$ de $\neg\phi$ par exemple ? Et bien, d'un point de vue syntaxique, pas grand chose.

9. Conférence de presse au quartier général des forces de l'OTAN, Bruxelles, le 6 juin 2002. `http://www.nato.int/docu/speech/2002/s020606g.htm`.

Par contre, d'un point de vue sémantique, plusieurs choses les séparent. La manière dont le connecteur $\neg$ est interprété est identique quels que soient les modèles, quelles que soient les théories. Il en est de même des connecteurs binaires $\vee, \wedge, \longrightarrow, \longleftrightarrow$. Bien sûr, cela dépend de la logique dans laquelle on se place. En logique classique, $\neg\phi$ est vraie si et seulement si ϕ est fausse, alors que nous avons vu qu'en logique intuitionniste, l'on pouvait très bien n'avoir ni ϕ ni $\neg\phi$ de satisfaites. C'était entre autres le cas dans les modèles qui ne satisfaisaient pas le tiers exclu $(\phi \vee \neg\phi)$. Mais bon gré mal gré, il s'agissait toujours de la négation d'une formule, même si la négation au sens classique différait quelque peu de la négation au sens intuitionniste.

Tandis qu'avec les opérateurs de modalité, l'interprétation de $\Box$ et $\Diamond$ peut très bien se référer respectivement à la nécessité et la contingence, ou à la connaissance et la croyance, ou encore à des exécutions de programmes informatiques, ou tout simplement à des conditions temporelles comme le passé et le futur.

Dès lors, on pourra interpréter $\Box\phi$ comme voulant dire *"il est nécessaire que ϕ"* et $\Diamond\phi$ signifiera alors *"il est possible que ϕ"*. Nous pourrons ainsi dire *"il est nécessaire de porter des lunettes de protection"* ou bien *"il est possible de porter des lunettes de protection"*. Dans un autre contexte, on comprendra $\Box\phi$ comme *"je sais que ϕ"*, par contraste avec $\Diamond\phi$ qui se pensera comme *"je crois que ϕ"* : *"je sais que vous portez habituellement des lunettes de protection"*, ou bien *"je crois que vous portez habituellement des lunettes de protection"*. Enfin dans un troisième sens, nous pourrons entendre $\Box\phi$ comme *"ϕ est obligatoire"* et $\Diamond\phi$ comme *"ϕ est permis"* : *"il est obligatoire de porter des lunettes de protection"*, ou bien *"il est permis de porter des lunettes de protection"*.

Par conséquent, nous voyons apparaître un lien de dualité entre $\Box$ et $\Diamond$. Par exemple, si l'on dit qu'il est nécessaire que $\neg\phi$, cela signifie que quoi que l'on fasse, ϕ ne peut avoir lieu. Autrement dit, s'il est nécessaire que $\neg\phi$, alors il n'est pas possible que ϕ. L'inverse est également vrai : si ϕ n'est tout simplement pas possible, alors il est nécessaire que $\neg\phi$. Il en résulte qu'affirmer qu'*"il est possible que ϕ"* revient à dire qu'*"il n'est pas nécessaire que $\neg\phi$"*. Nous verrons donc l'équivalence entre les deux formules $\neg\Box\neg\phi$ et $\Diamond\phi$. Cela vaudra pour toutes les interprétations possibles de ces deux opérateurs de modalité. Ainsi, si je dis que *"je crois que ϕ"*, cela reviendra à dire qu'*"il est faux que je sache que $\neg\phi$"*. En fait, l'un des opérateurs se définit aisément en fonction de l'autre et bien souvent, nous ne considérerons $\Diamond\phi$ que comme une notation pour $\neg\Box\neg\phi$, ce qui facilitera grandement les preuves.

Nous pourrons également répéter ce processus et donc, à partir des formules $\Box\phi$ et $\Diamond\phi$, construire par exemple les formules $\Box\Box\phi$ ou $\Box\Diamond\phi$, voire encore $\Box\Diamond\Box\phi$ qui diront chacune respectivement *"il est nécessaire qu'il soit nécessaire que ϕ"*, ou *"il est nécessaire qu'il soit possible que ϕ"*, ou bien encore *"il est nécessaire qu'il soit possible qu'il soit nécessaire que ϕ"*.

Pour compliquer encore un peu plus les choses, alors que les connecteurs sont en nombres finis – par ailleurs extrêmement réduits – les opérateurs de modalité pourront parfois apparaître en très grands nombres, voire en nombres infinis. Nous pourrons par exemple utiliser $[i]$ ou $\langle i\rangle$ pour désigner respectivement ce que sait ou ce que croit la personne i. Cela permettra de parler de ce que sait Anne, de ce que croit Bertrand, ou de ce que sait Chloé.

Plus intéressant encore, avec de nombreux types de modalités comme $[i]$ et $\langle i\rangle$ (pour des indices i choisis dans un ensemble à dessein), nous pourrons dire *"Anne croit que Bertrand sait que Chloé croit que Anne sait que la roue avant du vélo est crevée"* en écrivant $\langle A\rangle[B]\langle C\rangle[A]\phi$, où ϕ sera la formule du Calcul Propositionnel qui nous informe que la roue avant du vélo est crevée. Bien sûr, nous pourrons à loisir utiliser les connecteurs logiques de la logique propositionnelle et ainsi former une formule comme

$$([B]\neg\langle C\rangle\phi \longrightarrow (\langle B\rangle[A]\phi \wedge \langle C\rangle[B]\psi))$$

qui dira que *"si Bertrand sait que Chloé ne croit pas que la roue avant du vélo est crevée, alors à la fois Bertrand croit que Anne sait que la roue avant du vélo est crevée et Chloé croit que Bertrand sait que le nécessaire de réparation se trouve dans le placard de l'entrée"* (pour autant que ψ signifie : *"le nécessaire de réparation se trouve dans le placard de l'entrée"*).

La seconde différence majeure par rapport au Calcul Propositionnel sera la mise à jour de "systèmes" de logique modale. Chacun de ces systèmes fonctionnent comme une théorie particulière, adaptée à l'interprétation des opérateurs de modalités que nous souhaiterons prendre en compte. Il y aura ainsi par exemple un système adapté à l'emploi d'opérateurs épistémiques comme `savoir` et `croire`, un autre pour des opérateurs temporels, etc.

La dernière chose qui différera du Calcul Propositionnel classique viendra de l'aspect sémantique. Tout en travaillant dans une logique "classique" – dans laquelle par exemple le tiers exclu et l'élimination des doubles négations seront satisfaits – les modèles des différents systèmes mis à jour seront du genre de ceux employés pour la logique intuitionniste : les *modèles de Kripke*. Ce sont d'ailleurs ces modèles qui ont d'abord été introduits par Saul Kripke à la fin des années cinquante et au début des années soixante, dans le cadre de la logique modale, qui ont ensuite été utilisés à profit dans celui des logiques intuitionnistes.

Encore une fois, nous insistons sur la portée de l'opposition entre syntaxe et sémantique. Pour les différents systèmes de la logique modale, comme pour le Calcul Propositionnel, une notion de preuve ou démonstration existe, que ce soit sous forme d'un système de déduction à la Hilbert, de Déduction Naturelle ou de Calcul des Séquents. Le *sens*, à proprement parler, des formules que nous utiliserons se situe dans cet écart entre les deux. Mais cet entre-deux ne peut faire sens que s'il jouit également d'un théorème de complétude au même titre que celui du Calcul Propositionnel. (En fait au même titre que les trois théorèmes de complétude qui sont ceux de la logique classique, la logique intuitionniste et la logique minimale).

Or, pendant longtemps, divers systèmes de logique modale coexistaient sans sémantique appropriée, du moins sans sémantique suffisamment claire et précise pour pouvoir justifier d'un théorème de complétude. Les modèles de Kripke, également appelés *modèles relationnels*, ou encore *sémantique des mondes possibles* – mais qui sont en fait d'un strict point de vue mathématique de simples graphes dirigés coloriés – ont révolutionné la logique modale.

En route vers les mondes possibles

***Résumé* № 21** *Des enfants sont sortis jouer et certains se sont salis. Chacun peut voir qui de ses frères ou sœurs est propre ou sale, mais personne ne peut se regarder soi-même... On étudie ce que savent ou croient possibles les uns et les autres.* ※

Un exemple de logique modale appliquée : la logique épistémique et les "enfants sales" [FHMV95] [10]

Trois frères et sœurs d'une même famille – Alice, Bob et Chloé – ont très envie de sortir jouer dehors, dans la nature. Malheureusement la pluie a rendu le sol boueux. Après avoir supplié leur maman de bien vouloir les laisser sortir, celle-ci abdique tout en les prévenant :

– *"Le sol est détrempé, il y a de la boue partout. Je veux bien que vous sortiez jouer mais à la condition que vous fassiez en sorte de ne pas vous salir."*

– *"Oui, on fera attention."* Répondent en cœur les trois enfants.

Mais les enfants se comportent comme des enfants et si chacun est très attentif à sa propre personne, il ou elle ne manque pas pour autant d'essayer de faire trébucher son petit frère ou sa petite sœur dans la boue afin qu'il ou elle se fasse gronder.

Chose étonnante, les enfants qui se salissent ne le font que sur leur *front*, en sorte qu'ils ne peuvent voir directement cette partie de leurs corps et ainsi savoir s'ils sont propres ou sales. Mais *a contrario* si un enfant est sale et ne peut donc pas voir sa figure pour le savoir, chacun de ses frères et sœur peut tout à fait le savoir en regardant simplement son front à lui.

Il est l'heure, les enfants rentrent, aucun enfant n'a communiqué avec ses autres frères et sœur au sujet de la saleté de son front. Plus encore, les enfants rentrent dans le vestibule où ne se trouve pas le moindre miroir. Désormais, les enfants restent silencieux, ils ne communiquent pas non plus entre eux par le moyen de mimiques ou de codes gestuels préalablement convenus. Les enfants se regardent mutuellement mais ne pipent mot.

Il va de soi que dans cette situation, un enfant donné qui est sale ne peut savoir qu'il est sale. Par contre, chaque autre enfant sait que cet enfant est sale puisqu'il le voit.

10. Cette section est très largement inspirée du premier chapitre du livre : Ronald Fagin, Joseph Y. Halpern, Yoram Moses, Moshe Y. Vardi, *Reasoning about knowledge*, The MIT Press, 1995.

Ensuite, le père rentre et voit ses trois enfants – Alice, Bob et Chloé – silencieux dans le vestibule. Il leur tient alors ces propos :

– *"L'un au moins de vous trois est sale."*

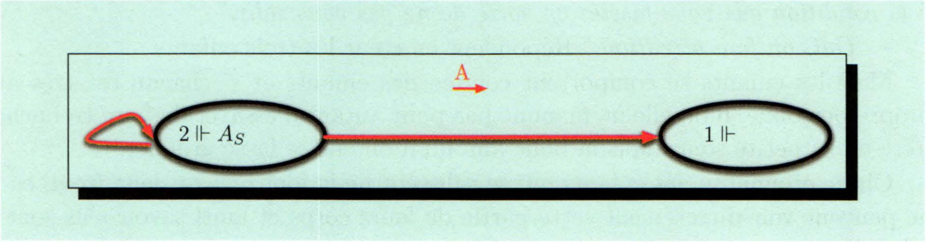
Puis il ajoute :

– *"Lequel d'entre vous sait qu'il – ou elle – est sale ?"*

Nous allons considérer différentes situations possibles que nous appellerons des mondes possibles.

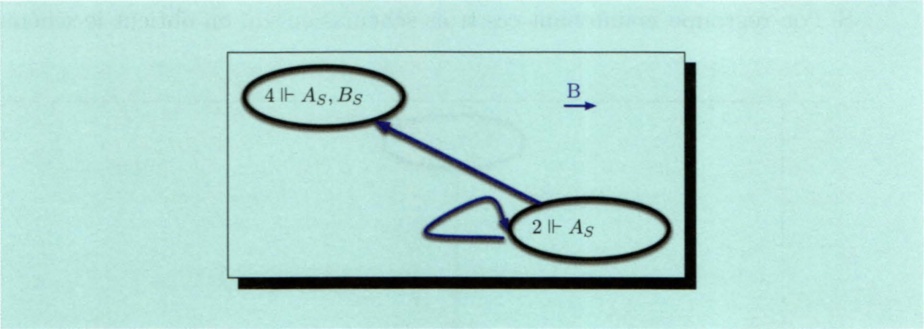
Seule Alice est sale Regardons ce qui se passe tout d'abord avant que le père n'ait parlé et ce, du point de vue de chacun des enfants.

Du point de vue d'Alice : Alice sait que Bob et Chloé sont propres. Elle considère possible qu'elle soit propre. Elle considère possible qu'elle soit sale. De son point de vue, il y a donc deux mondes possibles et elle ne sait pas particulièrement dans lequel elle se trouve. Nous pouvons représenter cela par le schéma qui suit. Chacun des cercles représente un monde possible. Dans le cercle situé à droite, il s'agit du monde $\boxed{1}$ dans lequel aucun enfant n'est sale. Le cercle situé à gauche représente le monde possible $\boxed{2}$ dans lequel seule Alice est sale. C'est effectivement dans le monde $\boxed{2}$ que se trouve Alice mais elle ne le sait pas. La notation $2 \Vdash A_s$ signifie que dans le monde $\boxed{2}$, le fait que Alice soit sale est *réalisé*. Le fait que nous n'écrivions pas $2 \Vdash B_s$ ni $2 \Vdash C_s$ signifie que dans ce monde $\boxed{2}$, Bob et Chloé sont tous les deux propres. Ainsi la notation $1 \Vdash$ signifie que dans le monde $\boxed{1}$ aucun enfant n'est sale.



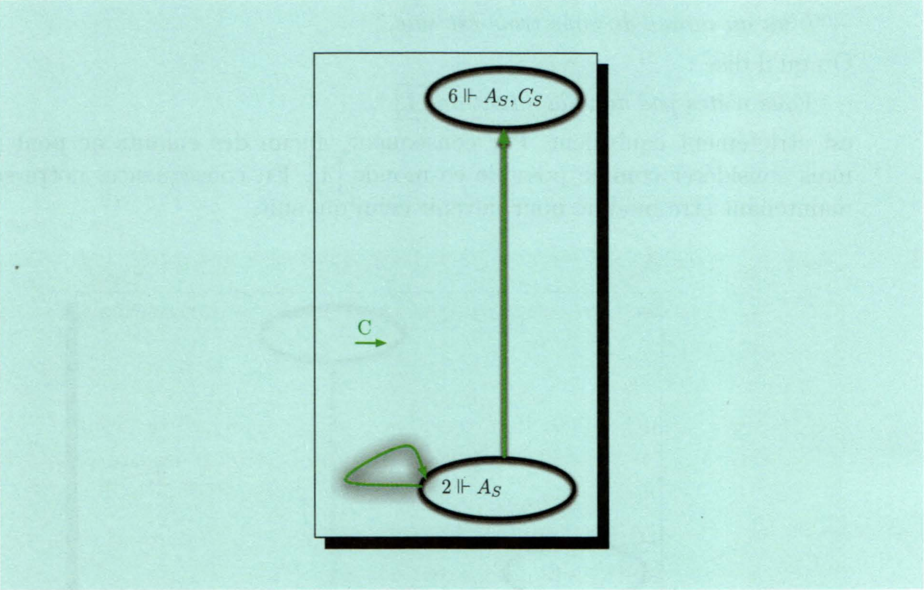
Les flèches rouges qui relient ces mondes possibles sont au nombre de deux. Chacune part du monde $\boxed{2}$. L'une y retourne alors que l'autre part vers le monde $\boxed{1}$. Chacune de ces flèches indique quel est pour Alice le monde qu'elle considère possible à partir du monde $\boxed{2}$. Ainsi l'on voit que dans la situation $\boxed{2}$, Alice considère possible le monde $\boxed{2}$ et également le monde $\boxed{1}$.

Du point de vue de Bob : Bob sait qu'Alice est sale et que Chloé est propre. Par contre il ne sait pas s'il est propre ou sale. Il considère donc possibles les deux mondes qui apparaissent dans le schéma qui suit : le monde $\boxed{2}$ dans lequel seule Alice est sale, et le monde $\boxed{4}$ dans lequel Alice et lui sont sales et Chloé est propre.



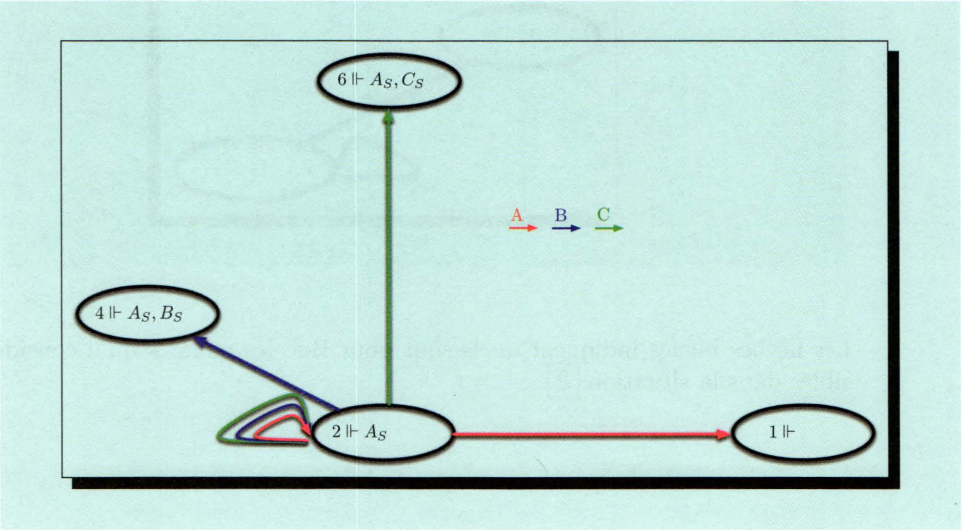
Les flèches bleues indiquent quels sont pour Bob les mondes qu'il considère possibles dans la situation $\boxed{2}$.

Du point de vue de Chloé : Chloé sait qu'Alice est sale et que Bob est propre. Par contre, elle ne sait pas si elle est propre ou sale. Elle considère donc possibles les deux mondes qui apparaissent dans le schéma qui suit : le monde $\boxed{2}$ dans lequel seule Alice est sale, et le monde $\boxed{6}$ dans lequel Alice et elle sont sales alors que Bob est propre.



Les flèches vertes cette fois indiquent quels sont – pour Chloé – les mondes qu'elle considère possibles lorsqu'elle se retrouve dans la situation $\boxed{2}$.

Si l'on regroupe maintenant ces trois schémas en un, on obtient le schéma qui suit :



Restons un instant sur ce schéma et regardons ce qui évolue lorsque le père entre en scène et déclare :

– *"L'un au moins de vous trois est sale."*

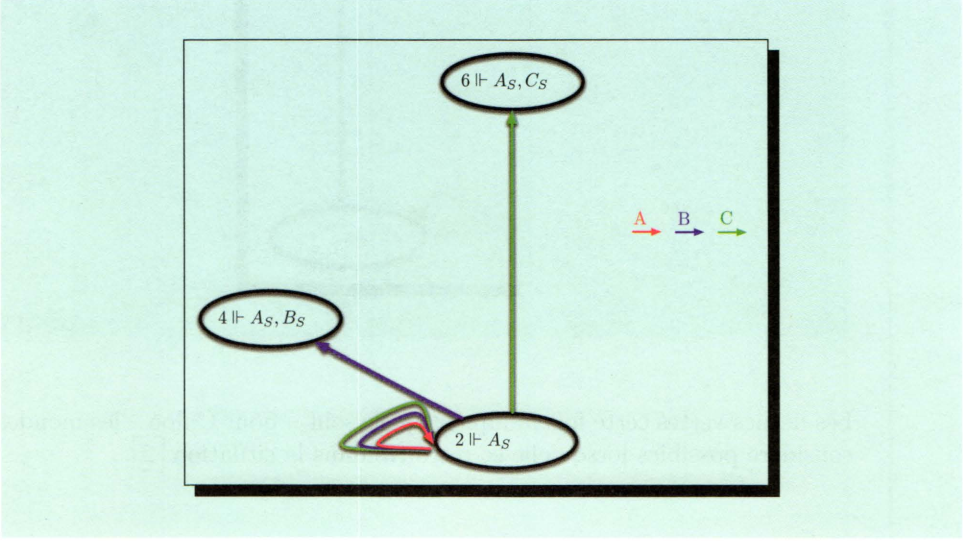
Immédiatement, l'information qui est communiquée par le père aux trois enfants rend caduque le fait de croire possible le monde $\boxed{1}$ dans lequel aucun enfant n'est sale. Effectivement que le père dise :

– *"L'un au moins de vous trois est sale."*

Ou qu'il dise :

– *"Vous n'êtes pas dans la situation* $\boxed{1}$*."*

est strictement équivalent. Par conséquent, aucun des enfants ne peut plus désormais considérer comme possible ce monde $\boxed{1}$. En conséquence, notre schéma doit maintenant être modifié pour devenir celui qui suit.



Désormais, lorsque le père pose la question :
– *"Lequel d'entre vous sait qu'il – ou elle – est sale ?"*

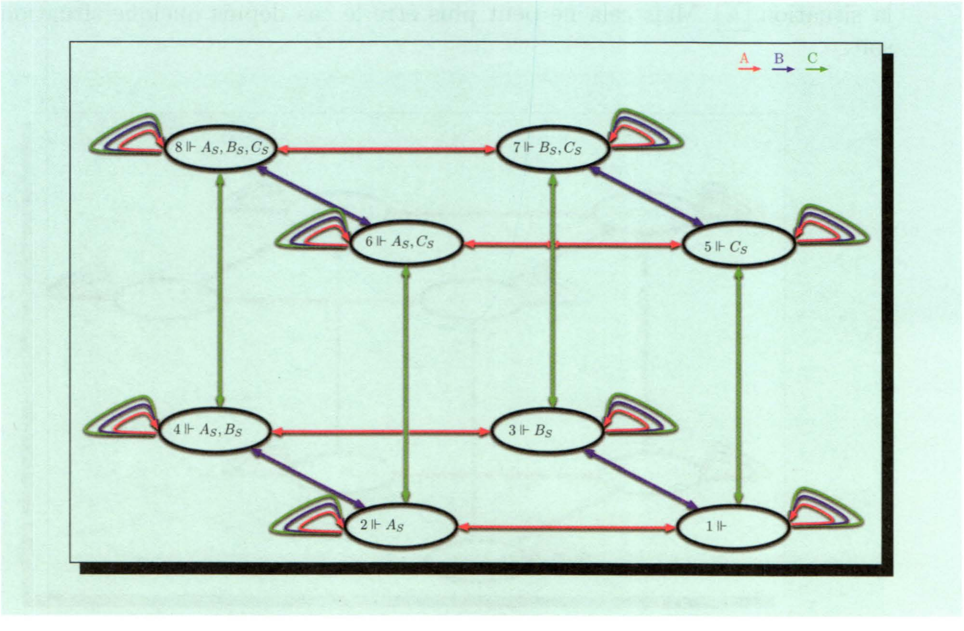
Bob et Chloé considèrent chacun deux mondes possibles. Ce ne sont pas les mêmes pour Bob et pour Chloé, mais chacun d'eux considère possible un monde dans lequel il – ou elle – est sale et un second dans lequel il – ou elle – est propre.

Par contre , si l'on s'attache maintenant au point de vue d'Alice, on remarque qu'elle ne considère plus possible qu'un seul monde. Précisément celui dans lequel elle est le seul enfant sale. En conséquence Alice *sait* qu'elle est sale et va donc répondre positivement à la question de son père.

Alice s'est donc déclarée sale. Mais que pouvons nous dire de Bob et de Chloé ? Est-ce que maintenant Bob et Chloé sont persuadés d'être tous les deux propres ? Effectivement c'est le cas. Mais pourquoi cela ?

Que s'est-t-il passé depuis que le père est entré et a communiqué l'information selon laquelle il y avait au moins un enfant qui était sale ? A première vue, il semble que l'information nouvelle est qu'Alice est sale puisqu'elle vient de se déclarer comme telle. Mais ni Bob ni Chloé n'avaient besoin de la déclaration d'Alice pour savoir cela. Chacun d'eux pouvait en effet très bien se rendre compte par lui-même qu'Alice était sale. C'est donc qu'une chose plus importante s'est déroulée lorsqu'Alice s'est déclarée sale. L'information qu'Alice leur a communiquée n'est en fait pas seulement celle selon laquelle elle est sale, mais également celle selon laquelle *Alice sait*, qu'Alice est sale. Comment donc Alice peut-elle savoir qu'elle est sale ? La seule manière de résoudre cela c'est de considérer qu'Alice ne voit que deux visages propres et par conséquent en infère qu'elle est la seule enfant qui soit sale.

Si nous reprenons la modélisation que nous avions mise en œuvre pour tenter de résoudre ce dilemme, nous nous apercevons très rapidement que celle-ci était trop particulière, trop restrictive. Nous allons au contraire nous attacher à la modélisation la plus générale, telle qu'elle apparaît dans le schéma ci-après.



Nous voyons tout de suite qu'il y a huit mondes possibles, puisque chaque enfant peut être propre ou sale et qu'il y a en tout trois enfants. Nous obtenons ainsi $2 \times 2 \times 2 = 8$ situations possibles. Ainsi par exemple, dans le monde $\boxed{1}$, tous les enfants sont propres, alors que dans le monde $\boxed{8}$, tous les enfants sont sales et dans le monde $\boxed{7}$, Bob et Chloé sont sales mais Alice est propre. Ensuite, entre deux mondes $\boxed{a}$ et $\boxed{b}$, il existe une flèche rouge de $\boxed{a}$ vers $\boxed{b}$ si dans la situation $\boxed{a}$ Alice considère possible le monde $\boxed{b}$. Par conséquent, il y a une flèche rouge du monde $\boxed{a}$ vers le monde $\boxed{b}$ si ou bien le monde $\boxed{b}$ n'est autre que le monde $\boxed{a}$ – Alice considère toujours possible la situation réelle dans laquelle elle se trouve – ou bien si le monde $\boxed{b}$ ne diffère du monde $\boxed{a}$ que par le fait que dans le monde $\boxed{a}$, Alice est sale mais qu'elle est propre dans le monde $\boxed{b}$, ou bien l'inverse – Alice est propre en $\boxed{a}$ mais sale en $\boxed{b}$.

Les flèches bleues sont définies de la même manière que les flèches rouges, mais en prenant le parti de Bob au lieu d'Alice. Et finalement les flèches vertes sont celles qui correspondent aux mondes que considère Chloé dans une situation donnée.

Ainsi dans le monde $\boxed{5}$, Alice considère possible les deux mondes $\boxed{5}$ et $\boxed{6}$, alors que Bob considère possible les deux mondes $\boxed{5}$ et $\boxed{7}$, tandis que Chloé considère possible les situations $\boxed{5}$ et $\boxed{1}$.

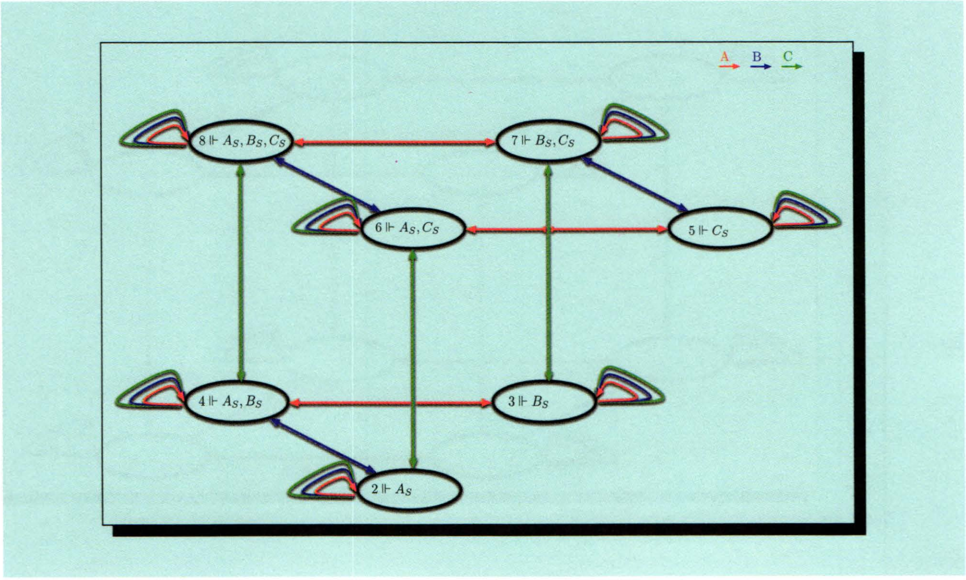
Que se passe-t-il maintenant une fois que le père est entré ? L'information qu'il communique :

– *"L'un au moins de vous trois est sale."*

est équivalent à :

– *"Vous n'êtes pas dans la situation* $\boxed{1}$*."*

Donc ce monde possible, $\boxed{1}$ n'existe plus. Il disparaît ainsi que les flèches qui menaient à lui, car une flèche qui menait de la situation $\boxed{a}$ au monde $\boxed{1}$ signifiait simplement que l'enfant indiqué par la couleur de la flèche considérait possible ce monde-ci depuis la situation $\boxed{a}$. Mais cela ne peut plus être le cas depuis quelque situation que ce soit.



Afin d'utiliser pleinement la modélisation que nous avons mise en place – et que nous appellerons un *modèle de Kripke* – nous allons introduire deux *opérateurs de modalité* pour chaque enfant. Ces opérateurs sont les suivants :

$$[A], \langle A \rangle, [B], \langle B \rangle, [C], \langle C \rangle.$$

Il y en a de deux types : les carrés ($[A], [B], [C]$) et les losanges ($\langle A \rangle, \langle B \rangle, \langle C \rangle$). Ces opérateurs de modalité servent à former des formules d'un nouveau genre par rapport au Calcul Propositionnel. Ainsi, si ϕ est une formule du Calcul Propositionnel, alors $[A]\phi$ sera une formule de la logique modale – épistémique en l'occurrence – que nous interpréterons par "*Alice sait que ϕ*". De même $\langle A \rangle\phi$ sera également une formule de la logique épistémique que nous interpréterons par "*Alice croît possible que ϕ*".

Bien évidemment, nous n'allons pas en rester là. Nous allons considérer que les formules de la logique épistémique sont toutes les formules du Calcul Propositionnel, qu'elle sont également closes par conjonctions, disjonctions, implications et doubles implications et par les opérations : à partir de ϕ, obtenir $[A]\phi$, $[B]\phi$, $[C]\phi$ ainsi que $\langle A \rangle\phi$, $\langle B \rangle\phi$, $\langle C \rangle\phi$.

Ainsi représentée de manière arborescente, une formule de la logique modale qui nous intéresse ici – à savoir avec les opérateurs de modalité $[A], \langle A \rangle, [B], \langle B \rangle, [C], \langle C \rangle$ – est un arbre dont toutes les feuilles sont des variables propositionnelles et dont tous les autres nœuds sont soit des connecteurs logiques, soit des opérateurs de modalité. Chaque branchement de l'arbre est soit unaire, soit binaire, en fonction précisément de l'arité du connecteur ou de l'opérateur en jeu. La hauteur d'une formule θ (notée $ht(\theta)$) est donnée par la longueur de s(a/es) plus longue(s) branche(s). Ainsi, une formule de hauteur 0 est une variable propositionnelle. Une formule de hauteur $n+1$ est soit de la forme qui suit – avec ϕ une formule de hauteur n :

$$\begin{array}{c} \neg \\ | \\ \phi \end{array}, \quad \begin{array}{c} [A] \\ | \\ \phi \end{array}, \quad \begin{array}{c} [B] \\ | \\ \phi \end{array}, \quad \begin{array}{c} [C] \\ | \\ \phi \end{array}, \quad \begin{array}{c} \langle A \rangle \\ | \\ \phi \end{array}, \quad \begin{array}{c} \langle B \rangle \\ | \\ \phi \end{array}, \quad \begin{array}{c} \langle C \rangle \\ | \\ \phi \end{array}$$

soit de l'une des quatre formes suivantes – avec le maximum des hauteurs de ϕ et de ψ qui vaut n :

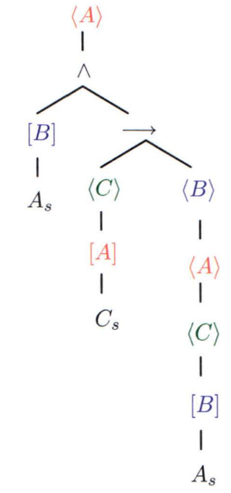
$$\begin{array}{c} \vee \\ \diagup \ \diagdown \\ \phi \quad \psi \end{array}, \quad \begin{array}{c} \wedge \\ \diagup \ \diagdown \\ \phi \quad \psi \end{array}, \quad \begin{array}{c} \longrightarrow \\ \diagup \ \diagdown \\ \phi \quad \psi \end{array}, \quad \begin{array}{c} \longleftrightarrow \\ \diagup \ \diagdown \\ \phi \quad \psi \end{array}$$

Par exemple la formule :

$$\begin{array}{c} \langle C \rangle \\ | \\ [B] \\ | \\ A_s \end{array}$$

signifie que Chloé croit possible que Bob sache qu'Alice est sale.

Et la formule



signifie qu'Alice croit possible qu'à la fois Bob sache qu'Alice est sale et que si Chloé croit possible qu'Alice sache que Chloé est sale, alors Bob croit possible qu'Alice croit possible que Chloé croit possible que Bob sache qu'Alice est sale.

Comment allons-nous utiliser de telles formules ? Et bien nous allons nous situer dans un monde possible et nous allons déterminer si cette formule est vraie ou non dans ce monde. Pour cela, savoir si une négation, conjonction, disjonction, implication ou double implication est vraie – on dit *réalisée* – ou non dans un monde possible ne varie pas par rapport au calcul propositionnel. La seule chose qui change d'un point de vue syntaxique, ce sont ces nouveaux opérateurs de modalité. Il nous faut donc expliquer quand est-ce qu'une formule de la forme $[A]\phi$, $[B]\phi$, $[C]\phi$, $\langle A\rangle\phi$, $\langle B\rangle\phi$, $\langle C\rangle\phi$ est réalisée dans un monde $\boxed{a}$.

L'idée est simple : une formule de la forme $\langle A\rangle\phi$, $\langle B\rangle\phi$, $\langle C\rangle\phi$ est réalisée dans un monde $\boxed{a}$ s'il existe une flèche correspondant à l'enfant en question – rouge pour Alice, bleue pour Bob et verte pour Chloé – qui mène de ce monde $\boxed{a}$ vers un monde $\boxed{b}$ dans lequel ϕ est réalisée. Ainsi dans le monde $\boxed{8}$, $\langle A\rangle A_s$ est réalisé – ce que l'on note $8 \Vdash \langle A\rangle A_s$ – car il y a une flèche rouge qui part du monde $\boxed{8}$ et atteint le monde $\boxed{8}$, monde dans lequel Alice est sale. De même dans le monde $\boxed{8}$, la formule $\langle A\rangle\langle B\rangle(\neg A_s \wedge \neg B_s)$ est réalisée car :

- il y a une flèche rouge qui part de $\boxed{8}$ et atteint $\boxed{7}$,
- du monde $\boxed{7}$ vers le monde $\boxed{5}$ il y a une flèche bleue,
- dans le monde $\boxed{5}$, à la fois Alice et Bob sont tous les deux propres.

Autrement dit, $8 \Vdash \langle A\rangle\langle B\rangle(\neg A_s \wedge \neg B_s)$ parce qu'il y a une flèche rouge de $\boxed{8}$ vers $\boxed{7}$ et le monde $\boxed{7}$ vérifie $7 \Vdash \langle B\rangle(\neg A_s \wedge \neg B_s)$ parce qu'il y a une flèche bleue de $\boxed{7}$ vers $\boxed{5}$ et que $5 \Vdash \neg A_s \wedge \neg B_s$.

Par contre, le monde $\boxed{8}$ ne réalise pas $\langle C\rangle\neg A_s$, puisque les deux flèches vertes qui partent du monde $\boxed{8}$ ne permettent d'atteindre que les mondes $\boxed{4}$ et $\boxed{8}$ qui tous deux réalisent le fait qu'Alice est sale.

Une formule de la forme $[A]\phi$, $[B]\phi$, $[C]\phi$ est réalisée dans un monde $\boxed{a}$ si *tous les mondes* atteignables par une flèche respectivement rouge, bleue, verte – suivant l'enfant en question – depuis le monde $\boxed{\text{a}}$ réalisent la formule ϕ. Ainsi dans le monde $\boxed{8}$, $[A]B_s$ est réalisée car les flèches rouges qui partent de ce monde mènent soit vers le monde $\boxed{8}$ soit vers le monde $\boxed{7}$ et chacun de ces deux mondes réalise le fait que Bob est sale, Cce que l'on note $8 \Vdash [A]B_s$.

Par contre, le monde $\boxed{8}$ ne réalise pas $[A]A_s$ puisque le monde $\boxed{7}$ ne réalise pas le fait qu'Alice soit sale.

On peut remarquer tout de suite que dans n'importe quel monde $\boxed{\text{a}}$ on a les équivalences suivantes :

- $a \Vdash \neg[A]\phi$ si et seulement si $a \Vdash \langle A\rangle\neg\phi$
  Pour Alice, ne pas savoir quelque chose est équivalent à croire possible le contraire de cette chose.
- $a \Vdash [A]\phi$ si et seulement si $a \Vdash \neg\langle A\rangle\neg\phi$
  Pour Alice, savoir quelque chose est identique à ne pas croire possible le contraire de cette chose.
- $a \Vdash \neg[A]\neg\phi$ si et seulement si $a \Vdash \langle A\rangle\phi$
  Pour Alice, croire possible quelque chose, cela revient à dire qu'elle ne sait pas le contraire de cette chose.

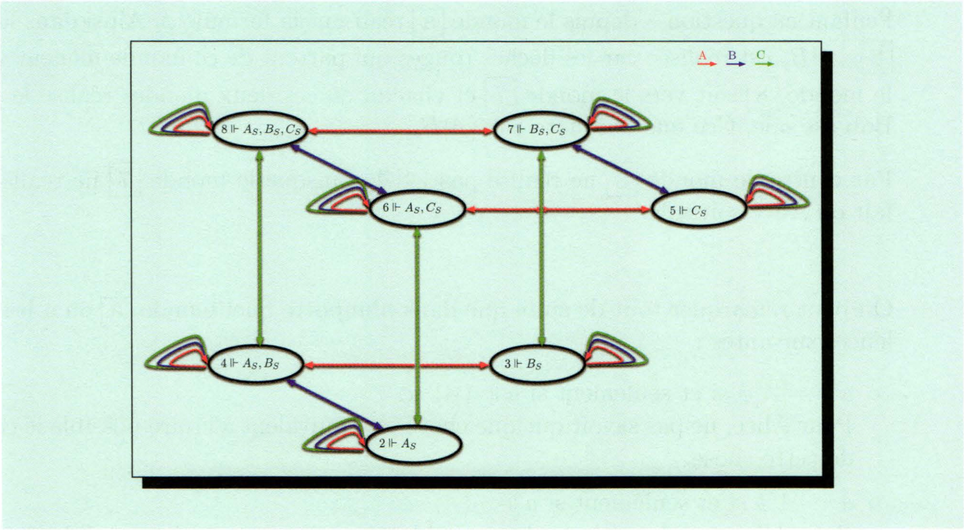
On a bien sûr les mêmes équivalences pour Bob et Chloé :

- $a \Vdash \neg[B]\phi$ si et seulement si $a \Vdash \langle B\rangle\neg\phi$
- $a \Vdash [B]\phi$ si et seulement si $a \Vdash \neg\langle B\rangle\neg\phi$
- $a \Vdash \neg[B]\neg\phi$ si et seulement si $a \Vdash \langle B\rangle\phi$
- $a \Vdash \neg[C]\phi$ si et seulement si $a \Vdash \langle C\rangle\neg\phi$
- $a \Vdash [C]\phi$ si et seulement si $a \Vdash \neg\langle C\rangle\neg\phi$
- $a \Vdash \neg[C]\neg\phi$ si et seulement si $a \Vdash \langle C\rangle\phi$

Arrêtons-nous un instant sur ce que nous venons de voir. Si je sais quelque chose, c'est que cette chose est vraie dans n'importe lequel des mondes que je considère possible (à partir du monde dans lequel je me trouve). Si au contraire une chose est réalisée dans un monde que je considère possible mais ne l'est pas dans un autre, alors je ne sais pas cette chose, puisque je crois possible qu'elle soit mais aussi qu'elle ne soit pas. De même, si je ne considère pas quelque chose comme possible, alors cela revient à dire que je sais la négation de cette chose.

Il est grand temps maintenant de revenir à notre modèle de Kripke qui rend compte des différents mondes possibles et de leurs interactions. Intéressons-nous à ce qui se passe une fois que le père a prononcé la phrase fatidique :

– *"L'un au moins de vous trois est sale."*



Le monde $\boxed{1}$ a disparu. On remarque les trois faits suivants :

- Dans le monde $\boxed{2}$ Alice sait qu'elle est sale : $2 \Vdash [A]A_s$.
- Dans le monde $\boxed{3}$ Bob sait qu'il est sale : $3 \Vdash [B]B_s$.
- Dans le monde $\boxed{5}$ Chloé sait qu'elle est sale : $5 \Vdash [C]C_s$.

Rappelons-nous que la situation réelle est en fait celle où seule Alice est sale et qu'Alice a déclaré à son père qu'elle savait qu'elle était sale. Si nous faisons un pas de plus, que peuvent en conclure Bob et Chloé ?

Tout d'abord attachons-nous à Bob. Bob ne sait pas s'il se trouve dans le monde $\boxed{2}$ ou dans le monde $\boxed{4}$. Effectivement, dans chacun de ces mondes, il sait qu'à la fois Alice est sale et Chloé est propre [11]. Et dans chacun également, il considère possible qu'il soit lui-même sale et il considère également possible qu'il soit propre [12].

Par contre, ce qui distingue le monde $\boxed{2}$ du monde $\boxed{4}$ est le fait que dans le monde $\boxed{2}$, Alice sait qu'elle est sale : $2 \Vdash [A]A_s$. Alors que dans le monde $\boxed{4}$, Alice considère possible le fait qu'elle soit propre : $4 \Vdash \langle A\rangle\neg A_s$. Précisément, il y a une flèche rouge qui part du monde $\boxed{4}$ pour aller vers le monde $\boxed{3}$ dans lequel Bob est le seul qui soit sale. En conclusion, Bob ne sait pas s'il se trouve dans le monde $\boxed{2}$ ou dans la situation $\boxed{4}$ avant qu'il entende Alice déclarer qu'elle sait qu'elle est sale. Bob a donc l'information qu'il se trouve dans un monde dans lequel Alice sait qu'elle est sale. Cela ne peut pas être le monde $\boxed{4}$, c'est donc qu'il se trouve dans le monde $\boxed{2}$.

Si nous regardons maintenant ce qui se passe pour Chloé, nous allons voir que son cas est tout à fait semblable à celui de Bob. En effet, Chloé hésite entre la situation $\boxed{2}$ et la situation $\boxed{6}$. Comme nous venons de le voir, dans le monde $\boxed{2}$, Alice sait qu'elle est sale – $2 \Vdash [A]A_s$ – mais dans le monde $\boxed{6}$, Alice ne le sait pas – $6 \Vdash \langle A\rangle\neg A_s$ – puisqu'elle considère possible le monde $\boxed{5}$ dans lequel seule Chloé est sale. Chloé en

11. Les deux énoncés $2 \Vdash [B](A_s \wedge \neg C_s)$ et $4 \Vdash [B](A_s \wedge \neg C_s)$ sont en effet tous deux réalisés.

12. Les deux énoncés $2 \Vdash \langle B\rangle B_s \wedge \langle B\rangle\neg B_s$ et $4 \Vdash \langle B\rangle B_s \wedge \langle B\rangle\neg B_s$ sont aussi tous deux réalisés.

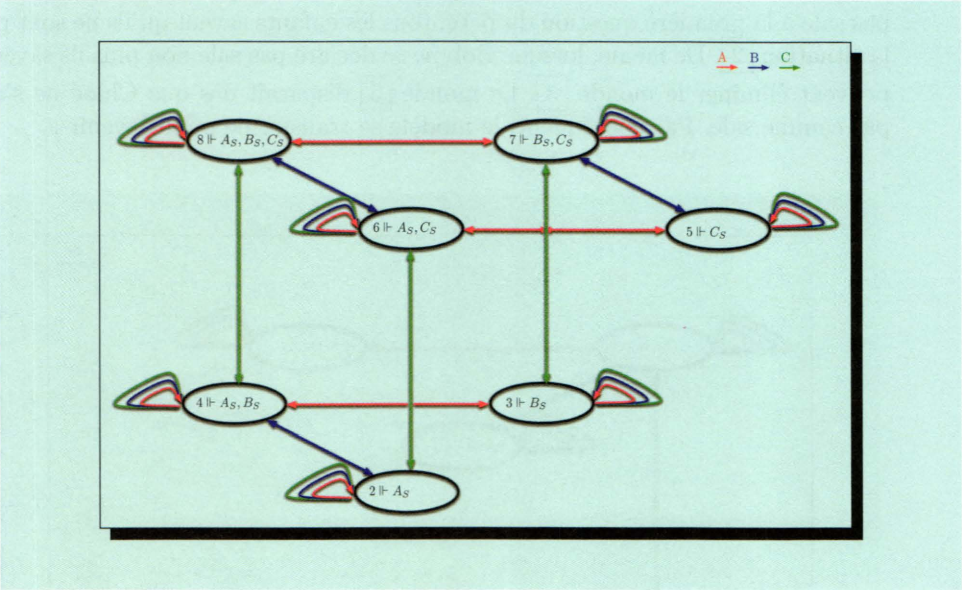
déduit donc qu'elle se trouve dans le monde $\boxed{2}$ dès qu'elle entend Alice déclarer à son père qu'elle sait qu'elle est sale.

Imaginons maintenant une autre situation :

Seuls Alice et Bob sont sales Dans ce cas là, après que le père ait proféré la phrase sempiternelle :

– *"L'un au moins de vous trois est sale."*

Chacun sait que la situation $\boxed{1}$ n'est pas celle dans laquelle il – ou elle – se trouve.



Mais Alice voit que Bob est sale et Bob voit qu'Alice est sale également. Tous les deux savent par contre que Chloé n'est pas sale. Donc Alice hésite entre la situation $\boxed{3}$ et la situation $\boxed{4}$, alors que Bob reste indéterminé par rapport aux deux mondes $\boxed{2}$ et $\boxed{4}$.

Lorsque le père pose pour la première fois la question :

– *"Lequel d'entre vous sait qu'il – ou elle – est sale ?"*

On voit clairement que les trois affirmations suivantes sont vérifiées :

- $4 \Vdash \neg[A]A_s$,
- $4 \Vdash \neg[B]B_s$,
- $4 \Vdash \neg[C]C_s$.

Donc aucun d'entre eux ne peut se déclarer sale.

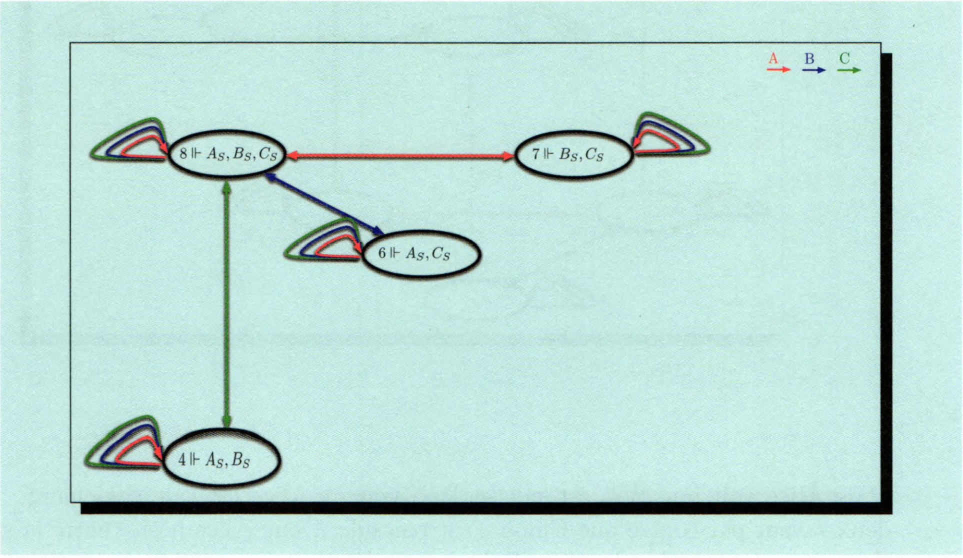
Par contre, le fait qu'aucun enfant ne se déclare sale apporte une nouvelle information. A savoir : Alice sait qu'elle est dans un monde dans lequel Bob ne sait pas qu'il est sale. Et Bob sait également qu'il se trouve dans une situation où Alice ne sait pas qu'elle est sale. Mais si Bob hésitait auparavant entre les situations $\boxed{4}$ et $\boxed{2}$, il constate désormais que $4 \Vdash \neg[A]A_s$ mais que par contre $2 \nVdash \neg[A]A_s$. Donc Bob en déduit qu'il se trouve dans le monde $\boxed{4}$. De même pour Alice, elle remarque que $4 \Vdash \neg[B]B_s$ alors que $3 \nVdash \neg[B]B_s$, elle en déduit donc qu'elle se trouve dans le monde $\boxed{4}$.

Ainsi, lorsque le père pose pour la seconde fois la question :

– *"Lequel d'entre vous sait qu'il – ou elle – est sale ?"*

Alice et Bob se déclarent en cœur tous les deux sales.

Une autre manière de voir la même chose consiste à dire que lorsqu'Alice ne se déclare pas sale à la première question du père, tous les enfants savent qu'ils ne sont pas dans la situation $\boxed{2}$. De même, lorsque Bob ne se déclare pas sale non plus ils savent qu'ils peuvent éliminer le monde $\boxed{3}$. Le monde $\boxed{5}$ disparaît dès que Chloé ne s'annonce pas comme sale. Par conséquent, le modèle se transforme pour devenir :



On voit clairement que seule Chloé ne peut pas déterminer si elle est propre ou sale.

Imaginons maintenant une troisième situation.

Alice, Bob et Chloé sont tous sales Ici encore est proférée la sentence introductive :

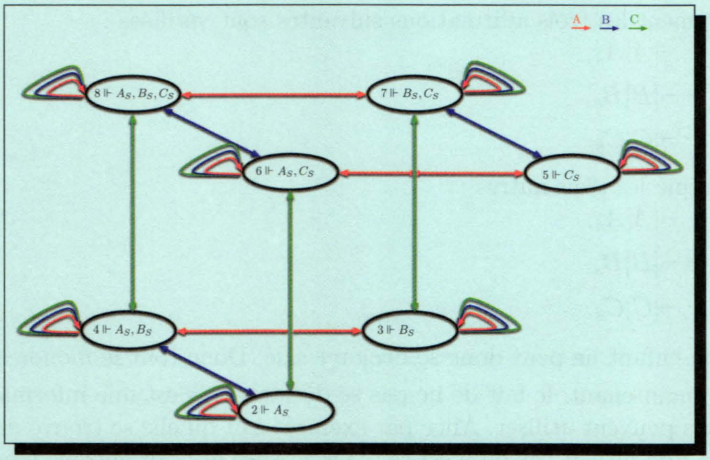
– *"L'un au moins de vous trois est sale"*,

chacun sait que la situation $\boxed{1}$ n'est pas celle dans laquelle il – ou elle – se trouve.

Chacun voit que les deux autres sont sales. Alice hésite donc entre les mondes $\boxed{7}$ et $\boxed{8}$; Bob hésite entre $\boxed{6}$ et $\boxed{8}$ et Chloé quant à elle hésite entre $\boxed{4}$ et $\boxed{8}$.

Lorsque le père pose pour la première fois la question :

– *"Lequel d'entre vous sait qu'il – ou elle – est sale ?"*



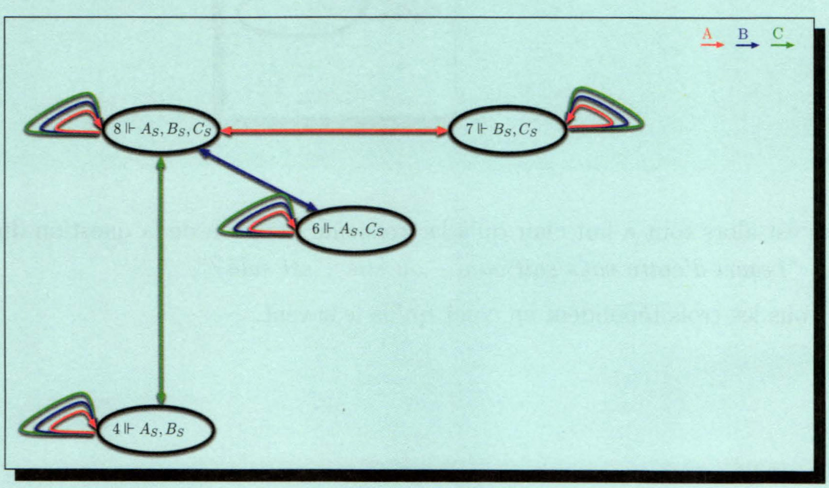
On voit clairement que les trois affirmations suivantes sont vérifiées :

- $8 \Vdash \neg[A]A_s$,
- $8 \Vdash \neg[B]B_s$,
- $8 \Vdash \neg[C]C_s$.

Mais également les affirmations ci-dessous :

- $7 \Vdash \neg[A]A_s$,
- $6 \Vdash \neg[B]B_s$,
- $4 \Vdash \neg[C]C_s$.

Donc aucun d'entre eux ne peut se déclarer sale à la première question du père. Cela donne une information supplémentaire à chaque enfant. Ils peuvent éliminer les mondes $\boxed{2}$, $\boxed{3}$ et $\boxed{5}$. Chacun se retrouve donc avec le modèle ci-après.



Que se passe-t-il maintenant à la seconde question posée par le père ?
Clairement les trois affirmations suivantes sont vérifiées :

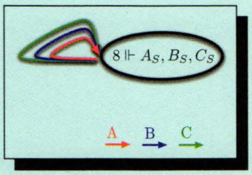
- $8 \Vdash \neg[A]A_s$,
- $8 \Vdash \neg[B]B_s$,
- $8 \Vdash \neg[C]C_s$.

Ainsi que les trois autres :

- $7 \Vdash \neg[A]A_s$,
- $6 \Vdash \neg[B]B_s$,
- $4 \Vdash \neg[C]C_s$.

Aucun enfant ne peut donc se déclarer sale. Donc tout le monde se tait.
Mais maintenant, le fait de ne pas se déclarer sale est une information que les autres enfants peuvent utiliser. Alice par exemple sait qu'elle se trouve dans un monde dans lequel Bob ne sait pas qu'il est sale. Or si Alice hésitait entre le monde $\boxed{8}$ et le monde $\boxed{7}$, elle peut tout de suite se rendre compte que le monde $\boxed{7}$ ne réalise pas le fait que Bob ne sache pas qu'il est sale : $7 \Vdash [B]B_s$. Par conséquent, Alice se retrouve immédiatement dépossédée de ce monde $\boxed{7}$, il ne lui reste pas d'autre alternative que d'être dans le monde $\boxed{8}$. De même pour Bob, l'hésitation entre les mondes $\boxed{8}$ et $\boxed{6}$ est résolue puisque le monde $\boxed{6}$ réalise que Chloé sait qu'elle est sale – de même pour Alice d'ailleurs – donc le fait que $6 \Vdash [C]C_s$ alors que Chloé ne s'est pas déclarée sale permet à Bob de déduire qu'il se trouve bien dans le monde $\boxed{8}$. Finalement, pour que Chloé se départisse du monde $\boxed{4}$, il lui suffit de remarquer que $4 \Vdash [B]B_s$ et que Bob ne s'est pas déclaré.
A ce point, chacun est persuadé que les mondes $\boxed{4}$, $\boxed{6}$ et $\boxed{7}$ ne correspondent pas à la situation actuelle.

Le modèle se transforme alors en :

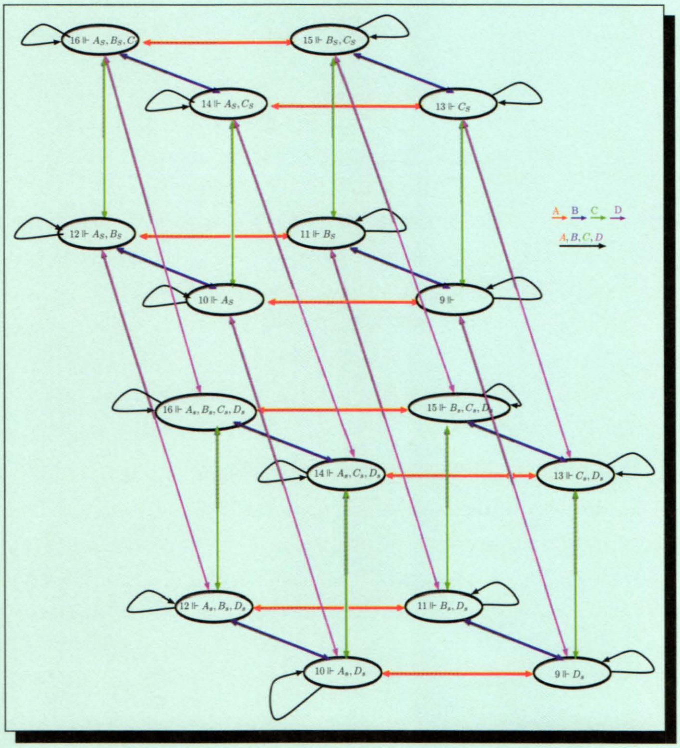


Il est alors tout à fait clair qu'à la troisième itération de la question du père :
– *“Lequel d'entre vous sait qu'il – ou elle – est sale ?”*

Tous les trois répondent en cœur qu'ils le savent.

Exemple 178

S'il y avait quatre enfants au lieu de trois, le processus serait de même nature, le modèle de Kripke de départ serait celui ci-dessous.



Pour aller plus avant :

L'exemple des "enfants sales" est emprunté à l'excellent ouvrage *"Reasoning about knowledge"* des auteurs Ronald Fagin, Joseph Y. Halpern, Yoram Moses et Moshe Y. Vardi [FHMV95], lui même adapté d'un article de Jon Barwise [Bar81] dans lequel se trouve l'exemple du *"the puzzle of the dirty children"* qui est lui-même une variante du problème des femmes infidèles (*"unfaithtful wifes"*) du livre *"A mathematician's miscellany"* de John Edensor Littlewood [Lit53]. Le lecteur particulièrement intéressé à cet exemple et au traitement logique de la connaissance trouvera une mine d'information dans l'ouvrage *"Reasoning about knowledge"* sus-cité [FHMV95] et sera également certainement intrigué par *"Reasoning about uncertainty"* de Joseph Y. Halpern [Hal03].

Chapitre 4

Syntaxe

1 Le langage

***Résumé* № 22** *Le langage de la Logique Modale comporte quatre ingrédients : les variables propositionnelles –* $P_0, P_1, P_2, P_3, P_4, \ldots$*, les connecteurs modaux –* $[0]$*,* $[1]$*,* $[2]$*,* $[3]$*,* $[4]$*,… et* $\langle 0\rangle$*,* $\langle 1\rangle$*,* $\langle 2\rangle$*,* $\langle 3\rangle$*,* $\langle 4\rangle$*,…, les connecteurs logiques –* $\neg, \vee, \wedge, \longrightarrow, \longleftrightarrow$ *– ainsi que les parenthèses fermante et ouvrante –) et (. Les connecteurs modaux fonctionnent comme des opérateurs unaires (ils permettent de construire une formule sur la base d'une autre).* ※

Le langage de la Logique Modale est constitué de quatre groupes de symboles différents : les variables propositionnelles, les connecteurs logiques, les parenthèses et les opérateurs modaux.

1.1 Les variables propositionnelles

Tout comme dans le cadre du Calcul Propositionnel, les variables propositionnelles sont représentées par des symboles non ambigus qui les distinguent des connecteurs et des opérateurs modaux, et bien évidemment également des parenthèses. Le but étant toujours que la lecture d'une formule ne soit pas équivoque mais univoque, qu'il n'y ait aucune ambiguïté.

Tout à fait traditionnellement, nous utiliserons des lettres majuscules pour dénoter les variables propositionnelles $(P, Q, R, \ldots)$. Et lorsque nous souhaiterons en utiliser une infinité, nous adjoindrons un indice entier $(P_0, P_1, P_2, \ldots)$. Il est entendu qu'il ne s'agit là que d'une convention. L'important pour démarrer cette définition du langage de la logique modale est de se donner un ensemble infini de symboles appelés variables propositionnelles, et de faire en sorte par la suite de ne jamais employer l'un de ces symboles pour dénoter autre chose qu'une variable propositionnelle. Nous utiliserons la notation VAR pour désigner l'*ensemble des variables propositionnelles* suivant :

$$VAR = \{P, Q, R, \ldots, P_0, P_1, P_2, P_3, P_4, \ldots\}$$

1.2 Les connecteurs logiques

Dans le cadre du Calcul Propositionnel, nous utilisions 5 connecteurs dont 4 étaient binaires et un seul unaire. Nous avions vu qu'il était possible, en particulier, de définir sur cette base 16 connecteurs binaires différents. Mais également, par ailleurs, que toute formule écrite avec ces 5 connecteurs admettait une formule équivalente qui ne comportait que les connecteurs $\neg$ et $\wedge$, ou encore une autre avec les seuls $\neg$ et $\vee$. Nous avions également remarqué qu'il existe deux connecteurs binaires - les barres de Sheffer disjonctive et conjonctive - qui permettent, chacune séparément, d'engendrer, à équivalence près, toutes les formules possibles. Il est donc, en quelque sorte, arbitraire de choisir tels connecteurs plutôt que tels autres pour autant que l'on se donne un système complet.

Nous conservons les cinq connecteurs que nous avions introduits dans le cadre du Calcul Propositionnel, auxquels sont adjoints les deux seuls connecteurs 0-aires : $\top$, $\bot$. Le fait que ce soient des connecteurs 0-aires signifient qu'ils ne relient (connectent) aucune formule à une autre. Alors que le connecteur binaire $\wedge$ a besoin de deux formules ϕ et ψ pour en former une troisième $(\phi \wedge \psi)$, ou que le connecteur unaire $\neg$ n'en a besoin que d'une $(\neg\phi)$, ces connecteurs 0-aires n'en ont besoin d'aucune. Ils sont en ce sens extrêmement rudimentaires mais se révéleront très utiles par la suite.

Nous nous donnons donc les sept symboles suivants :

$$\top, \bot, \neg, \vee, \wedge, \longrightarrow, \longleftrightarrow$$

(1) $\top$ est appelé symbole de *tautologie*, on le prononce simplement "Té", ou "top" ou encore "true",

(2) $\bot$ est appelé symbole de *contradiction*, on le prononce "Té inversé", mais plus généralement *"bottom"*.

(3) $\neg$ est appelé symbole de *négation*, on le prononce "non".

(4) $\vee$ est appelé symbole de *disjonction*, on le prononce "ou".

(5) $\wedge$ est appelé symbole de *conjonction*, on le prononce "et".

(6) $\longrightarrow$ est appelé symbole d'*implication*, on le prononce "implique".

(7) $\longleftrightarrow$ est appelé symbole de *double implication*, ou encore parfois symbole d'*équivalence*, on le prononce "si et seulement si" ou encore "équivaut à".

L'intérêt de ces connecteurs est de mettre en "connection" un certain nombre de formules pour en obtenir une formule nouvelle. Les deux premiers de ces symboles $(\top)$ et $(\bot)$ sont des connecteurs *zéro-aires*, le troisième $(\neg)$ est un connecteur *unaire*, les quatre restants sont des connecteurs *binaires*.

1.3 Les parenthèses

Il s'agit simplement de la parenthèse fermante et de la parenthèse ouvrante :

$$) \;,\; ($$

Nous les ferons intervenir dans différentes tailles afin de faciliter la lecture, mais *stricto sensu*, elles ne sont que deux. Elles ne serviront d'ailleurs que pour une présentation linéaire du langage.

1.4 Les opérateurs de modalité

Il s'agit de symboles opérants comme des connecteurs unaires : à partir d'une formule, chacun d'eux permet de construire une nouvelle formule. A l'origine, il n'y en avait qu'un : "$\Box$" ; auquel s'est adjoint son dual : "$\Diamond$". Puis il est devenu nécessaire d'en considérer plusieurs, voire même une infinité.

Ainsi, les symboles que nous utiliserons pour les opérateurs de modalité seront généralement :

$$[i], \langle i \rangle$$

où l'ensemble des indices i varie sur un ensemble I que l'on pourra identifier par commodité à l'ensemble des entiers $\mathbb{N}$. Mais lorsque, par exemple dans le cadre de la logique épistémique, nous voudrons parler de ce que sait Bob, ou de ce que croit possible Alice, nous nous permettrons d'écrire $[Bob], respectivement\langle Alice\rangle$, ou également $[B], \langle A\rangle$, au lieu de $[1], \langle 0\rangle$, tout en pensant que l'indice 1 se rapporte à Bob et l'indice 0 à Anne. Nous nous permettrons ce genre d'abus exactement de la même manière que dans le Calcul Propositionnel, nous avions défini les variables propositionnelles comme des lettres P, Q, R possiblement indicées, mais utilisions parfois A, B comme nom de variables.

Ici encore, nous ferons intervenir ces symboles dans différentes tailles afin d'en faciliter la lecture.

De plus, lorsque nous ne serons intéressés que par un seul indice, au lieu d'écrire $[0], \langle 0\rangle$, nous omettrons cet indice et écrirons simplement $[], \langle\rangle$ et pour des raisons purement esthétiques, ces symboles prendront la forme de $\Box$ pour $[]$ et $\Diamond$ pour $\langle\rangle$.

Ainsi le langage $\mathcal{L}$ de la *Logique Modale* est l'ensemble suivant :

$$\begin{aligned}
\mathcal{L} &= VAR \cup \{\top, \bot, \neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\} \cup \{), (\} \cup \{[i] : i \in \mathbb{N}\} \cup \{\langle i\rangle : i \in \mathbb{N}\} \\
&= \{P, Q, R, \ldots, P_0, P_1, P_2, P_3 \ldots\} \cup \{\top, \bot, \neg, \vee, \wedge, \longrightarrow, \longleftrightarrow\} \cup \{), (\} \\
&\qquad \cup \{[i] : i \in \mathbb{N}\} \cup \{\langle i\rangle : i \in \mathbb{N}\} \\
&= \{P, Q, R, \ldots, P_0, P_1, P_2, P_3 \ldots, \top, \bot, \neg, \vee, \wedge, \longrightarrow, \longleftrightarrow,), \\
&\qquad (, [0], [1], [2], [3], \ldots, \langle 0\rangle, \langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \ldots\}.
\end{aligned}$$

2 Les formules

***Résumé* № 23** *Les formules de la logique modale sont des arbres dont les feuilles sont des variables propositionnelles et tous les autres nœuds sont ou bien des connecteurs logiques, ou bien des opérateurs de modalité. Chaque branchement de l'arbre est soit unaire, soit binaire, en fonction précisément de l'a-rité du connecteur en jeu. Dans le cas des opérateurs de modalité, le branchement est toujours unaire. La hauteur d'une formule* θ *(notée* $ht(\theta)$*) est donnée par la longueur de sa (ses) plus longue(s) branche(s). Ainsi une formule de hauteur 0 est une variable propositionnelle. Une formule de hauteur* $n+1$ *est soit de la forme qui suit – avec* ϕ *une formule de hauteur* n *:*

$$\begin{array}{c}\neg\\ |\\ \phi\end{array} \qquad \begin{array}{c}[i]\\ |\\ \phi\end{array} \qquad \begin{array}{c}\langle i\rangle\\ |\\ \phi\end{array}$$

soit de l'une des quatre formes suivantes – avec le maximum des hauteurs de ϕ *et de* ψ *qui vaut* n *:*

$$\begin{array}{ccc} & \vee & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \wedge & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longrightarrow & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longleftrightarrow & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}.$$

La profondeur modale d'une formule ϕ *est le plus grand nombre d'opérateurs de modalité rencontré sur une branche.* ※

Les formules de la logique modale sont construites de manière tout à fait similaire à celles du Calcul Propositionnel. D'ailleurs chaque formule du Calcul Propositionnel est également une formule de la logique modale. Cette dernière est simplement plus vaste du fait de l'adjonction des opérateurs de modalité. La différence, du point de vue syntaxique, provient donc de ce que l'on dispose en quelque sorte de deux types nouveaux d'"opérateurs unaires" qui viennent s'adjoindre au connecteur de négation : $[i]$ et $\langle i\rangle$.

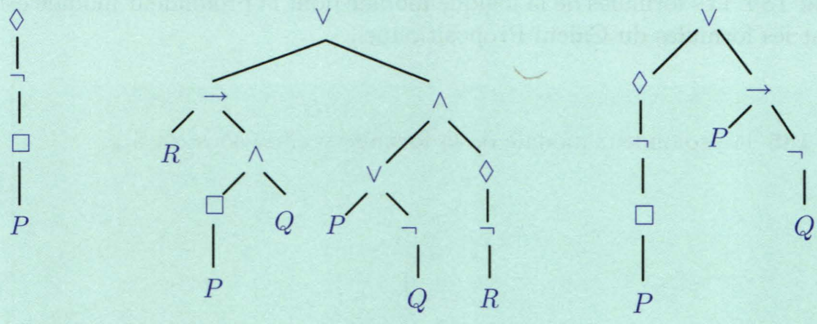
Définition 179 *L'ensemble* $\mathcal{F}$ des formules de la Logique Modale *est le plus petit ensemble d'arbre qui :*

- *contient chaque arbre réduit à sa racine qui est une variable propositionnelle.*
- *chaque fois qu'il contient des formules* ϕ *et* ψ*, contient également les formules suivantes :*

$$\begin{array}{c}[i]\\ |\\ \phi\end{array}, \quad \begin{array}{c}\langle i\rangle\\ |\\ \phi\end{array}, \quad \begin{array}{c}\neg\\ |\\ \phi\end{array}, \quad \begin{array}{ccc} & \vee & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \wedge & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longrightarrow & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longleftrightarrow & \\ \diagup & & \diagdown \\ \phi & & \psi\end{array}$$

On définit la hauteur d'une formule comme étant la longueur de sa plus longue branche – ou de ses plus longues branches lorsqu'il y en a plusieurs.

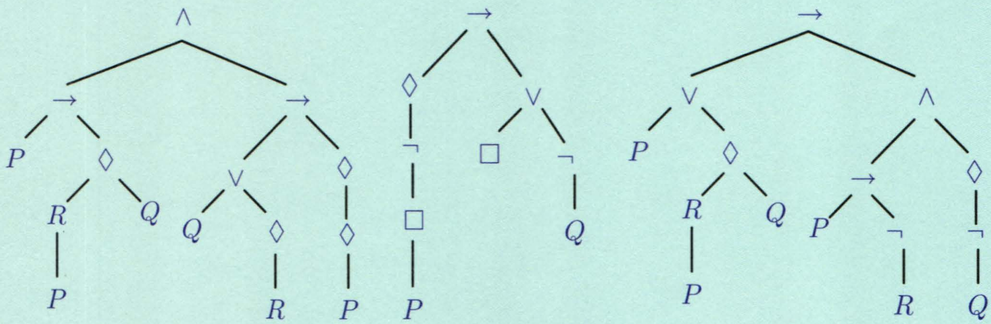
Exemple 180 Trois formules, la première de hauteur 3, les deux suivantes de hauteur 4 :



Remarques 181

- Les nœuds d'une formule sont de deux sortes : les feuilles et les autres. Aux feuilles se trouvent uniquement des variables propositionnelles. Aux autres nœuds se trouvent des connecteurs logiques ou des opérateurs de modalité.
- La longueur minimale d'une formule est 0. Les seules formules de longueur 0 sont celles constituées d'une simple variable propositionnelle. La longueur maximale qu'une formule peut atteindre n'existe pas. Nous verrons plus loin qu'il existe non seulement des formules de toutes longueurs, mais aussi que, d'un point de vue sémantique, il existe des formules de toutes longueurs irréductibles à des formules de longueurs moindres.

Exemple 182 Pourquoi ces arbres ne représentent-ils pas des formules de la logique modale ? [1]



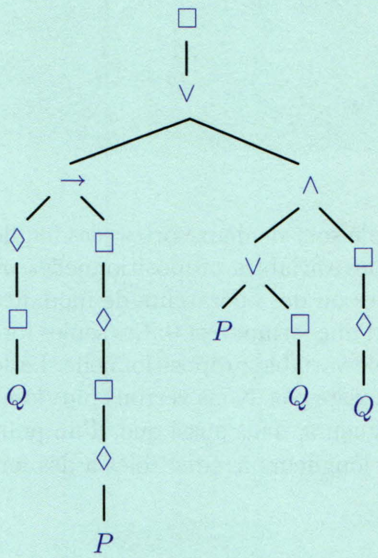
1. (1) $\diamond$ n'est pas un opérateur binaire ; (2) $\square$ n'est pas une variable ; (3) R est une variable.

En plus de la hauteur d'une formule, on définit également sa profondeur modale qui témoigne de son éloignement par rapport aux formules du Calcul Propositionnel.

Définition 183 *La profondeur modale d'une formule ϕ est le plus grand nombre d'opérateurs modaux que possède une branche de ϕ.*

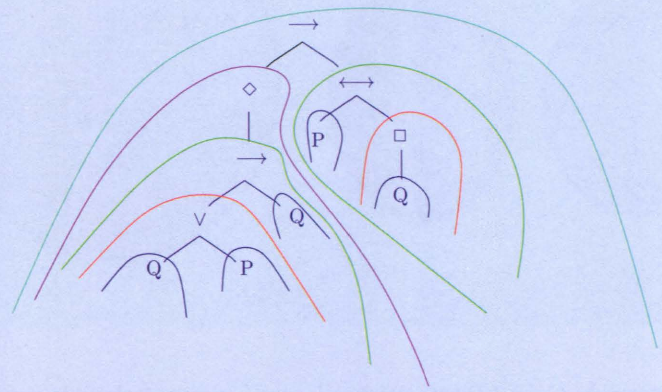
Remarque 184 Les formules de la logique modale dont la profondeur modale est nulle sont précisément les formules du Calcul Propositionnel.

Exemple 185 la profondeur modale de la formule ϕ ci-dessous est 5 :



3 Les sous-formules

Résumé № 24 *Une sous-formule d'une formule ϕ est un sous-arbre de ϕ dont l'un des nœuds de ϕ est la racine.*



※

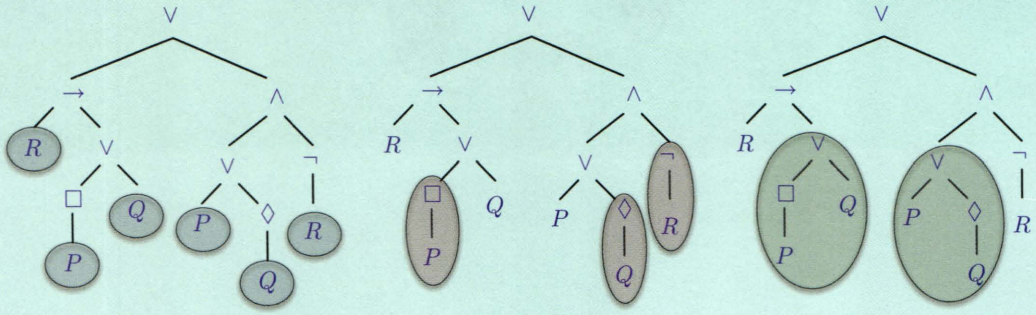
Une formule de la logique modale étant un arbre de nature semblable à celui qui définit une formule du Calcul Propositionnel, les sous-formules d'une formule de la logique modale ne sont par nature pas différentes de celles rencontrées dans le cadre du Calcul Propositionnel.

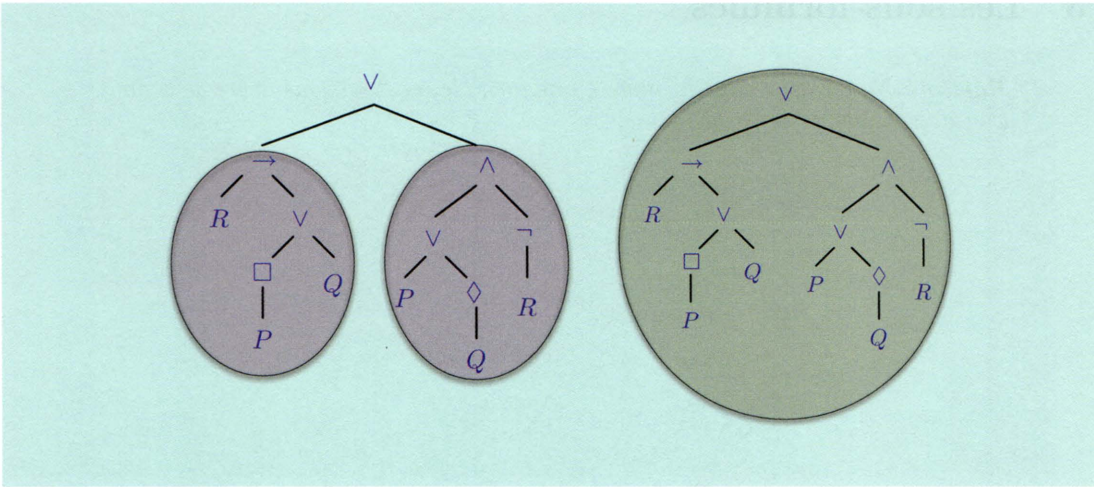
Définition 186 *Une sous-formule d'une formule ϕ est un sous-arbre de ϕ engendré par un nœud de ϕ.*

Cette définition signifie à la fois qu'en pointant un nœud quelconque de la formule ϕ, on obtient une sous-formule de ϕ, mais aussi que cet agissement est le seul qui permette de pointer l'un de ses nœuds et de ne garder de la formule ϕ que ce nœud-ci et tous ses descendants. On obtient ainsi une nouvelle formule dont le nœud pointé est la racine.

Remarque 187 Par construction, une formule est construite à partir de ses sous-formules. Elle ne tient debout que parce que ses sous-formules la soutiennent. C'est bien sûr le cas pour les formules de hauteur 0, qui sont elles-mêmes leurs uniques sous-formules. Les formules de hauteur strictement positive ne sont quant à elles que l'articulation au moyen de connecteurs ou d'opérateurs modaux de formules de hauteur strictement plus petites.

Exemple 188 Les sous-formules de hauteurs respectives $0, 1, 2, 3, 4$ d'une même formule ϕ.

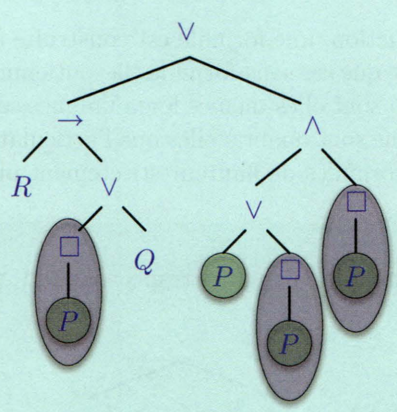




Comme dans le cas du Calcul Propositionnel, une formule ψ donnée peut avoir plusieurs occurrences comme sous-formule d'une formule ϕ.

Exemple 189 Dans la formule ci-dessous :

- la sous-formule P possède 4 occurrences ;
- la sous-formule $\begin{array}{c}\Box\\ |\\ P\end{array}$ possède 3 occurrences.



4 La linéarisation d'une formule

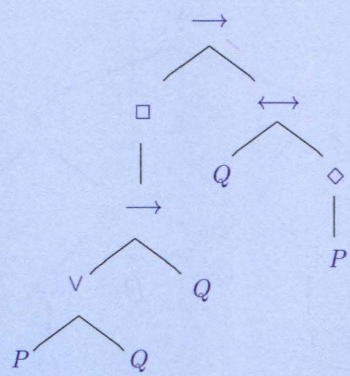
Résumé № 25 *L'écriture d'une formule sous forme linéaire consiste à transfomer :*

$$\overset{\langle i\rangle}{\underset{\phi}{|}},\quad \overset{[i]}{\underset{\phi}{|}},\quad \overset{\neg}{\underset{\phi}{|}},\quad \overset{\vee}{\underset{\phi\quad\psi}{\diagup\diagdown}},\quad \overset{\wedge}{\underset{\phi\quad\psi}{\diagup\diagdown}},\quad \overset{\longrightarrow}{\underset{\phi\quad\psi}{\diagup\diagdown}},\quad \overset{\longleftrightarrow}{\underset{\phi\quad\psi}{\diagup\diagdown}}$$

en respectivement

$$\langle i\rangle\overline{\phi},\quad [i]\overline{\phi},\quad \neg\overline{\phi},\quad (\overline{\phi}\vee\overline{\psi}),\quad (\overline{\phi}\wedge\overline{\psi}),\quad (\overline{\phi}\longrightarrow\overline{\psi}),\quad (\overline{\phi}\longleftrightarrow\overline{\psi})$$

où $\overline{\phi}$ et $\overline{\psi}$ sont elles-mêmes écrites sous forme linéaire. Les variables propositionnelles étant inchangées de leur écriture sous forme d'arbre (P) à celle linéaire ($\overline{P}$).
Ainsi :



se linéarise en : $(\Box((P\vee Q)\longrightarrow Q)\longrightarrow(Q\longleftrightarrow\Diamond P)).$ ※

Tout comme dans le Calcul Propositionnel, les formules – qui sont des arbres – admettent une présentation sous forme linéaire. Cette linéarisation des formules de la logique modale s'effectue de manière similaire à celle des formules du Calcul Propositionnel puisqu'il suffit d'ajouter aux règles précédemment introduites celles touchant aux opérateurs de modalité.

Définition 190 *Soit θ une formule, la linéarisation de θ (notée $\overline{\theta}$) est définie par induction sur la hauteur de θ.*

ht(θ)**=0** *: dans ce cas $\theta=\overline{\theta}=P$ pour une certaine variable propositionnelle P.*

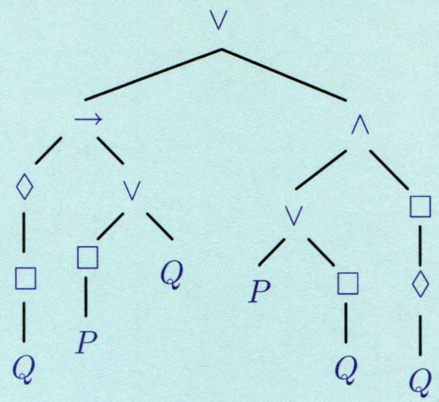
ht(θ)**>0** *:*

- *si* $\theta=\overset{\vee}{\underset{\phi\quad\psi}{\diagup\diagdown}}$ *alors* $\overline{\theta}=(\overline{\phi}\vee\overline{\psi})$,
- *si* $\theta=\overset{\longrightarrow}{\underset{\phi\quad\psi}{\diagup\diagdown}}$ *alors* $\overline{\theta}=(\overline{\phi}\longrightarrow\overline{\psi})$,
- *si* $\theta=\overset{\wedge}{\underset{\phi\quad\psi}{\diagup\diagdown}}$ *alors* $\overline{\theta}=(\overline{\phi}\wedge\overline{\psi})$,
- *si* $\theta=\overset{\longleftrightarrow}{\underset{\phi\quad\psi}{\diagup\diagdown}}$ *alors* $\overline{\theta}=(\overline{\phi}\longleftrightarrow\overline{\psi})$,

- $\circ$ *si* $\theta = \begin{array}{c}[i]\\ | \\ \phi\end{array}$ *alors* $\overline{\theta} = [i]\overline{\phi}$,
- $\circ$ *si* $\theta = \begin{array}{c}\neg\\ | \\ \phi\end{array}$ *alors* $\overline{\theta} = \neg\overline{\phi}$,
- $\circ$ *si* $\theta = \begin{array}{c}\langle i\rangle\\ | \\ \phi\end{array}$ *alors* $\overline{\theta} = \langle i\rangle\,\overline{\phi}$,

Comme dans le cadre du Calcul Propositionnel, l'écriture linéaire d'une formule peut très rapidement devenir embarrassante. Dès qu'il y a beaucoup de parenthèses, il devient difficile de repérer le connecteur qui est à la racine de l'arbre, même si en comptant attentivement les parenthèses ouvrantes et fermantes, on retrouve ce connecteur.

Exemple 191 Linéarisation $\overline{\phi}$ de la formule ϕ suivante :



$$\overline{\phi} = \Big((\Diamond\Box Q \longrightarrow (\Box P \vee Q)) \vee ((P \vee \Box Q) \wedge \Box\Diamond Q)\Big).$$

Remarques 192

- $\circ$ La hauteur d'une formule ϕ qui serait présentée de manière linéaire peut également être définie par :
  (1) Si ϕ est une variable propositionnelle, alors $ht\,(\phi) = 0$
  (2) Si ϕ n'est une variable propositionnelle, alors
    (a) si $\phi = (\psi_1 \vee \psi_2)$ alors $ht\,(\phi) = 1 + \max\{ht\,(\psi_1)\,, ht\,(\psi_2)\}$
    (b) si $\phi = (\psi_1 \wedge \psi_2)$ alors $ht\,(\phi) = 1 + \max\{ht\,(\psi_1)\,, ht\,(\psi_2)\}$
    (c) si $\phi = (\psi_1 \longrightarrow \psi_2)$ alors $ht\,(\phi) = 1 + \max\{ht\,(\psi_1)\,, ht\,(\psi_2)\}$
    (d) si $\phi = (\psi_1 \longleftrightarrow \psi_2)$ alors $ht\,(\phi) = 1 + \max\{ht\,(\psi_1)\,, ht\,(\psi_2)\}$
    (e) si $\phi = \neg\psi$ alors $ht\,(\phi) = 1 + ht\,(\psi)$
    (f) si $\phi = \Box\psi$ alors $ht\,(\phi) = 1 + ht\,(\psi)$
    (g) si $\phi = \Diamond\psi$ alors $ht\,(\phi) = 1 + ht\,(\psi)$.

- La profondeur modale d'une formule ϕ qui serait présentée de manière linéaire peut également être définie par induction sur la hauteur de ϕ :

(1) Si $ht(\phi) = 0$ alors $p_f(\phi) = 0$

(2) Si $ht(\phi) > 0$ alors

(a) si $\phi = (\psi_1 \vee \psi_2)$ alors $p_f(\phi) = \max\{p_f(\psi_1), p_f(\psi_2)\}$

(b) si $\phi = (\psi_1 \wedge \psi_2)$ alors $p_f(\phi) = \max\{p_f(\psi_1), p_f(\psi_2)\}$

(c) si $\phi = (\psi_1 \longrightarrow \psi_2)$ alors $p_f(\phi) = \max\{p_f(\psi_1), p_f(\psi_2)\}$

(d) si $\phi = (\psi_1 \longleftrightarrow \psi_2)$ alors $p_f(\phi) = \max\{p_f(\psi_1), p_f(\psi_2)\}$

(e) si $\phi = \neg\psi$ alors $p_f(\phi) = p_f(\psi)$

(f) si $\phi = \Box\psi$ alors $p_f(\phi) = 1 + p_f(\psi)$

(g) si $\phi = \Diamond\psi$ alors $p_f(\phi) = 1 + p_f(\psi)$.

Exemple 193 La hauteur de la formule sous forme linéaire ci-dessous est 9, sa profondeur modale est 5 :

$$(\Diamond((\Box\Diamond(R \wedge \Box\Diamond P) \vee Q) \wedge (P \longrightarrow Q)) \longrightarrow \Diamond((\Diamond\Diamond(R \wedge \Box\Box R) \longrightarrow Q) \wedge (P \longrightarrow Q))).$$

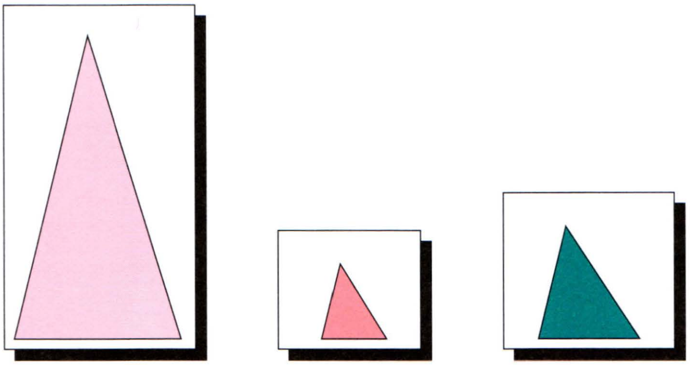
5 Les substitutions

Très souvent, nous aurons besoin de remplacer, à l'intérieur d'une formule, une sous-formule par une autre. Par exemple, lorsque nous aurons acquis la certitude qu'une sous-formule comme $(\Box P \wedge \neg\Diamond P)$ est une contradiction, il sera utile de remplacer dans la formule :

$$(\Box Q \longrightarrow (\Box P \wedge \neg\Diamond P))$$

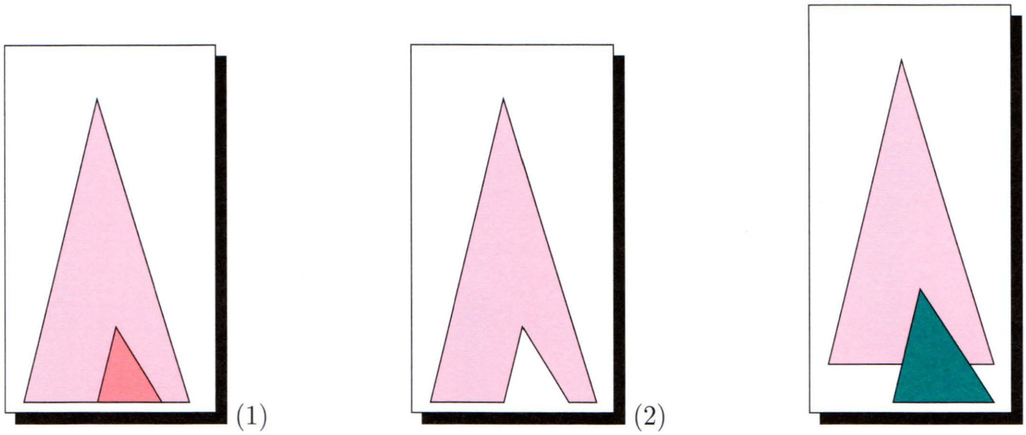
la seule occurrence de cette sous-formule par une formule plus simple qui lui soit équivalente. En l'occurrence, nous aimerions remplacer $(\Box P \wedge \neg\Diamond P)$ par $\perp$, pour obtenir $(\Box Q \longrightarrow \perp)$.

Cette notion de remplacement s'appelle la substitution. Elle consiste en une manipulation sur les arbres. Ci-dessous des diagrammes représentant les formules ϕ, ψ et θ :



ϕ ψ θ

On souhaite remplacer une occurrence particulière de ψ dans la formule ϕ par θ.



(1) (2) (3)

(1) Position de l'occurrence particulière de ψ à l'intérieur de ϕ.

(2) On retire l'occurrence de la sous-formule ψ de la formule ϕ.

(3) On la remplace par la formule θ et on obtient la nouvelle formule dont l'arbre de décomposition est ci-dessous.

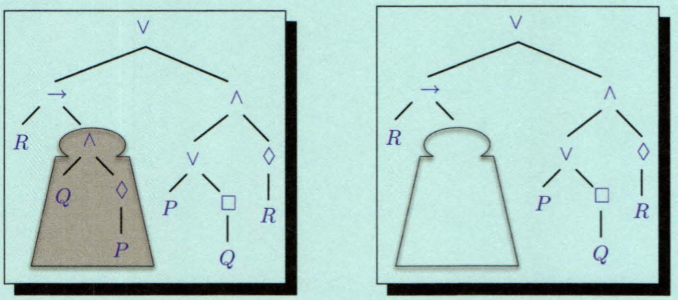
Remplacer toutes les occurrences de la sous-formule ψ par la formule θ consiste non pas à répéter cette opération, mais à effectuer d'abord le retrait de toutes les occurrences de ψ, et ensuite remplacer chacune de celles-ci par θ . Cette opération s'appelle la *substitution uniforme.*

Notation 194 *Soient ϕ, ψ, θ trois formules, on note :*

$$\phi[\theta/\psi]$$

la substitution uniforme de la formule θ à toutes les occurrences de ψ dans ϕ.

Exemple 195 Substitution de $(\Box P \vee Q)$ à $(Q \wedge \Diamond P)$:



Exemple 196 Quelques exemples de substitutions uniformes.

(1) $(P \vee \neg P)[\Box P/P] = (\Box P \vee \neg \Box P)$

(2) $(P \longrightarrow Q)[\Box Q/Q] = (P \longrightarrow \Box Q)$

(3) $(P \longrightarrow (P \longrightarrow Q))[\Box Q/(P \longrightarrow Q)] = (P \longrightarrow \Box Q)$.

Pour aller plus avant :

Le lecteur qui souhaite creuser la partie syntaxe de la logique modale trouvera matière à nourrir sa curiosité dans les livres *"Modal logic : an introduction to its syntax and semantics"* de Nino B. Cocchiarella et Max A. Freund [CF08], dans *"Modal logic : an introduction"* de Brian F. Chellas [Che80], ou encore dans le livre plus récent *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03].

Pour une lecture plus approfondie encore, il y a l'excellent ouvrage *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02], ainsi que le *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06] et le cours de Johan van Benthem *"Modal Logic for Open Minds"* [vB10].

Le lecteur qui recherche une approche plus particulièrement destinée à des philosophes pourra consulter avec intérêt *"Modal logics and Philosophy"* ou *"Possible worlds"*, tous deux de Rod Girle [Gir00, Gir03], *"Modal logic for philosophers"* de James W. Garson [Gar06] ou encore *"Possibilities and paradox : An introduction to modal and many-valued logicphilosophers"* de Jc Beall et Bas C van Fraassen [BvF03].

Chapitre 5

Sémantique

1 Avant-propos

***Résumé* № 26** *La sémantique de la Logique Modale repose sur la notion de* modèle de Kripke *qui se décompose en deux éléments :*

(1) Le graphe proprement dit. Il s'appelle système de transition et forme le cadre sur lequel s'articulent les différents mondes possibles. Ces derniers sont représentés par les nœuds du graphe, leurs articulations sont déterminées par les flèches qui les relient.

(2) La valuation qui désigne l'attribution à chaque monde possible des variables propositionnelles qui sont vérifiées en ce nœud. La valuation est celle qui permet donc de donner la valeur vrai ou faux – réalisable ou non – à une variable dans un monde donné.

※

L'interprétation des formules de la Logique Modale repose sur la notion de *modèle de Kripke*. Mais si les modèles de Kripke dont il s'agit ici sont les mêmes que ceux qui servent de sémantique à la logique intuitionniste, ils sont néanmoins utilisés de manière classique. Ainsi, les interprétations de la négation ou de l'implication seront tout à fait traditionnelles et non pas intuitionnistes.

La notion de modèle de Kripke rejoint en fait deux autres terminologies équivalentes. Nous aurons donc à notre disposition les trois notions suivantes qui se réfèrent toutes aux mêmes objets, mais avec des saveurs particulières :

(1) modèle de Kripke,

(2) graphe dirigé coloré,

(3) système de transition étiqueté.

En effet, les modèles de Kripke font intervenir des *graphes dirigés*, c'est-à-dire des nœuds reliés entre eux par des flèches. Ils sont dits *dirigés* car les flèches ont un sens, une direction. Le coloriage dont il est question dans l'appellation *graphe coloré* n'est autre que la caractérisation, pour chacun des nœuds du graphe, de celles parmi les variables propositionnelles étudiées qui sont vraies en ces nœuds. La notion de coloriage est donc plus imagée que réelle. Il ne s'agit pas réellement de colorier en vert, bleu ou jaune le nœud d'un graphe, mais de lui attribuer une certaine caractéristique – précisément celle qui nous intéresse – qui est de savoir quelles sont les variables qui sont vraies en ce nœud. La troisième notion, celle de *système de transition étiqueté*, nous rapproche de l'informatique. Les transitions dont il s'agit sont celles qui régissent les changements d'état de la machine. Un ordinateur peut en effet être perçu comme une machine qui recèle un très grand nombre d'états possibles. De manière imagée, chacun de ces états représente une sorte d'état *psychologique* qui conditionne son comportement face à ce qui lui est proposé. Or ce qui est proposé à un ordinateur – qui se trouve donc dans un certain état – c'est de lire une lettre qui est soit la lettre "0" soit la lettre "1", de remplacer celle-ci soit par la lettre "0" soit par la lettre "1", puis de se déplacer pour continuer sa lecture soit vers la droite, soit vers la gauche, et enfin de changer d'état. Deux états différents entraînant généralement des comportements différents, exactement comme lorsque devant une même situation, un même individu réagira d'une certaine manière s'il est *très énervé*, mais d'une toute autre manière si ce matin-là il est d'humeur *joviale et décontractée*. Ce sont précisément ces changements successifs d'états que le système de transition modélise. Un état est ici à la fois la donnée d'un nœud et de sa couleur.

2 systèmes de transition

***Résumé* № 27** *Un* système de transition *est un graphe dirigé. C'est un ensemble de nœuds reliés (ou non) par des flèches.* ※

Le cadre des modèles de Kripke est formé par les *systèmes de transition* qui ne sont rien d'autre que des graphes dirigés.

Définition 197 *Soient I un ensemble non vide, un système de transition étiqueté par I (ou de signature I) est une structure relationnelle (un graphe dirigé étiqueté)*

$$\mathcal{S} = (N, A)$$

où

(1) N est un ensemble non vide dont les éléments sont appelés nœuds,

(2) A est un ensemble de relations binaires sur N indicées par I ($A = \{A_i \subseteq N \times N \mid i \in I\}$).

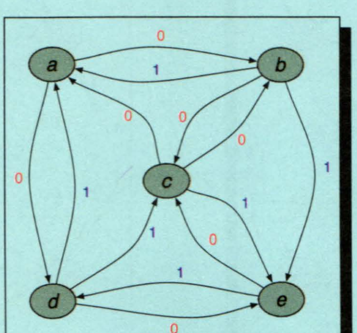
Remarque 198

(1) Les éléments de A_i s'appellent "arêtes d'étiquettes i". On écrira resp. $a \xrightarrow{i} b$ ou $a \overset{i}{\not\to} b$ pour dire qu'il y a une arête d'étiquette i de a vers b, ou pour dire qu'il n'y a pas de telle arête.

(2) Lorsque la signature d'un système de transition est un singleton (par exemple $I = \{i\}$), l'étiquette de chaque flèche étant identique, elle sera omise. On écrit alors $a \to b$ sans mention de l'étiquette au lieu de $a \xrightarrow{i} b$.

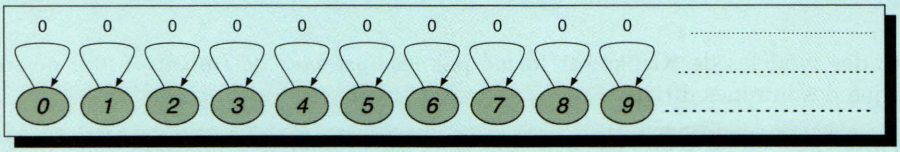
(3) Les éléments de N sont appelés nœuds en référence au fait qu'un système de transition a une nature de graphe. Mais suivant l'utilisation que nous ferons de ces systèmes de transition, ces nœuds pourront prendre le nom d'*états*, d'*instants*, voire de *mondes possibles* ou encore de *situations*.

Exemple 199 Un système de transition avec $\{0, 1\}$ pour signature et cinq nœuds dénotés a, b, c, d, e



Exemple 200 Un système de transition avec $I = \{0\}$ pour signature et $\mathbb{N}$ comme ensemble de nœuds.

Il y a simplement une flèche d'un nœud vers lui-même.



Nous nous intéresserons par la suite à trois propriétés essentielles des systèmes de transition – autrement dit des graphes dirigés. Ce sont en fait des propriétés de la relation binaire associée :

(1) réflexivité : tout élément est en relation avec lui-même ($a \xrightarrow{i} a$) ;

(2) symétrie : toute flèche est bi-directionnelle ($a \xrightarrow{i} b$ si et seulement si $b \xrightarrow{i} a$) ;

(3) transitivité : tout chemin a son raccourci (si $a \xrightarrow{i} b$ et $b \xrightarrow{i} c$, alors $a \xrightarrow{i} c$).

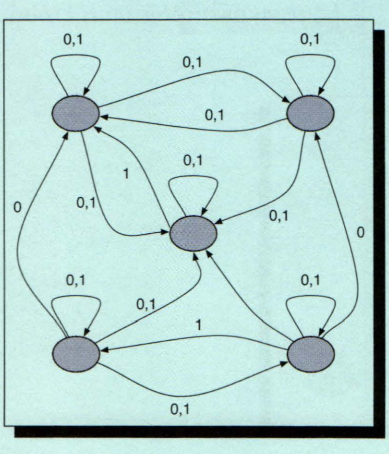
Définition 201 *Un sytème de transition $\mathcal{S} = (N, A)$ (avec $A = \{A_i \subseteq N \times N \mid i \in I\}$) est dit*

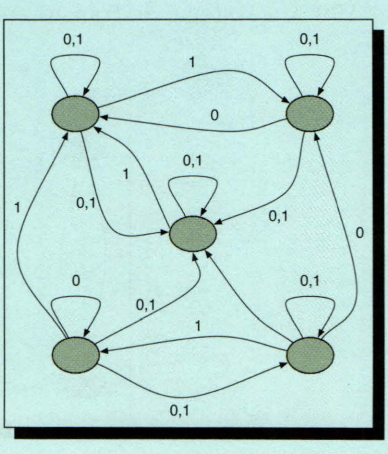
(1) réflexif *si, pour tous $i \in I$ et pour tous $a \in N$, il vérifie $a \xrightarrow{i} a$;*

(2) symétrique *si, pour tous $i \in I$ et pour tous $a, b \in N$, dès qu'il vérifie $a \xrightarrow{i} b$, il vérifie aussi $b \xrightarrow{i} a$;*

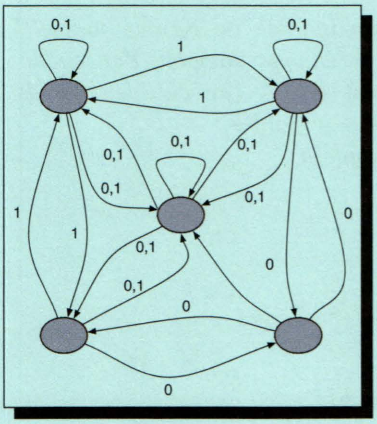
(3) transitif *si, pour tous $i \in I$ et pour tous $a, b, c \in N$, dès qu'il vérifie à la fois $a \xrightarrow{i} b$ et $b \xrightarrow{i} c$, il vérifie aussi $a \xrightarrow{i} c$.*

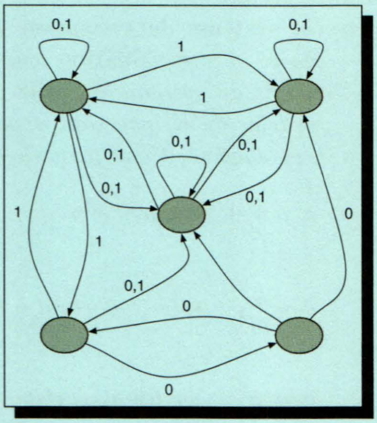
Exemple 202 Un système de transition réflexif et un qui ne l'est pas.



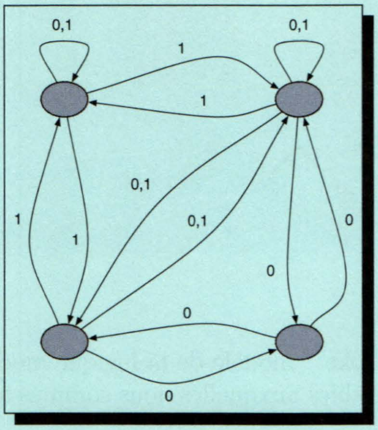


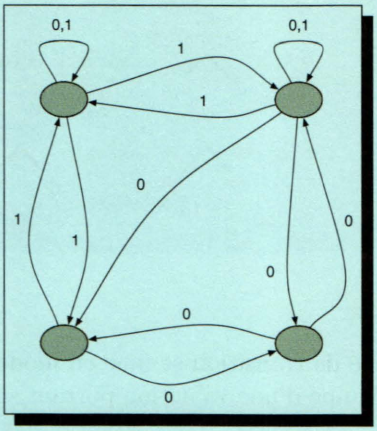
Exemple 203 Un système de transition symétrique et un qui ne l'est pas.





Exemple 204 Un système de transition transitif et un qui ne l'est pas.





3 Valuation et évaluation

Résumé № 28

- *Un* système de transition *devient un* modèle de Kripke *lorsqu'il est équipé d'une* valuation *qui associe à chaque variable l'ensemble des nœuds du système où cette variable est vérifiée* (forcée). *Les nœuds des modèles de Kripke sont appelés* mondes possibles.
- *L'évaluation d'une formule en un monde a :*
  - $a \Vdash \begin{array}{c}\neg\\ |\\ \phi\end{array}$ *ssi* $a \not\Vdash \phi$;
  - $a \Vdash \begin{array}{c}[i]\\ |\\ \phi\end{array}$ *ssi* $b \Vdash \phi$ *(tout* b *t.q.* $a \xrightarrow{i} b$*)* ;
  - $a \Vdash \begin{array}{c}\langle i\rangle\\ |\\ \phi\end{array}$ *ssi* $b \Vdash \phi$ *(existe* b *t.q.* $a \xrightarrow{i} b$*)* ;
  - $a \Vdash \begin{array}{c}\vee\\ \diagup\;\diagdown\\ \phi\quad\psi\end{array}$ *ssi* $a \Vdash \phi$ ou $a \Vdash \psi$;
  - $a \Vdash \begin{array}{c}\wedge\\ \diagup\;\diagdown\\ \phi\quad\psi\end{array}$ *ssi* $a \Vdash \phi$ et $a \Vdash \psi$;
  - $a \Vdash \begin{array}{c}\longrightarrow\\ \diagup\;\diagdown\\ \phi\quad\psi\end{array}$ *ssi* $a \not\Vdash \phi$ ou $a \Vdash \psi$;
  - $a \Vdash \begin{array}{c}\longleftrightarrow\\ \diagup\;\diagdown\\ \phi\quad\psi\end{array}$ *ssi* $a \Vdash \begin{array}{c}\longrightarrow\\ \diagup\;\diagdown\\ \phi\quad\psi\end{array}$ et $a \Vdash \begin{array}{c}\longrightarrow\\ \diagup\;\diagdown\\ \psi\quad\phi\end{array}$.

※

Un système de transition se mue en modèle de Kripke – modèle de la logique modale – dès qu'il est équipé d'une valuation portant sur les variables auxquelles nous sommes intéressés.

Définition 205 *Soient I un ensemble non vide, $\mathcal{S} = (N, A)$ un système de transition étiqueté par I, une valuation (ou distribution de valeurs de vérité) sur ce système de transition S est une fonction :*

$$\begin{array}{rccc} \mathcal{V}: & VAR & \longrightarrow & \mathcal{P}(N) \\ & P & \mapsto & \{a \mid a \Vdash P\} \end{array}$$

Intuitivement, une valuation $\mathcal{V}$ indique pour chaque nœud du système de transition, quelles sont les variables qui sont satisfaites en ce nœud. Le seul but d'une valuation est d'indiquer pour chaque nœud quelles sont les variables qui sont forcées en ce nœud. Ainsi une définition qui, au lieu d'associer à chaque variable l'ensemble des nœuds où cette variable est forcée, aurait associé à chaque nœud l'ensemble des variables qui sont forcées en ce nœud, produirait rigoureusement le même effet.

Définition 206 *Etant fixés :*

(1) $\mathcal{S} = (N, A)$ *un système de transition étiqueté par un ensemble non vide* I*,*

(2) $\mathcal{V}$ *une valuation sur* $\mathcal{S}$*,*

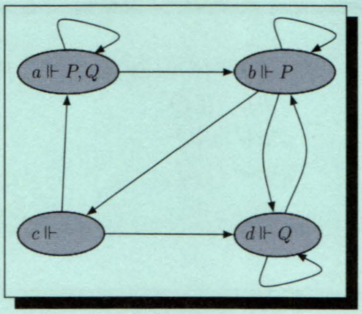
(3) $a \in N$*,*

(4) ϕ *une formule de la logique modale dont les opérateurs modaux sont indicés par des éléments de* I*,*

La satisfaction de la formule ϕ *au nœud* a *(au sein de* $\mathcal{S}$ *et pour la valuation* $\mathcal{V}$*) est notée* $a \Vdash \phi$ *et se définit par induction sur la hauteur de* ϕ *:*

- $a \Vdash \top$ *et* $a \nVdash \bot$
- $a \Vdash P$ *si et seulement si* $a \in \mathcal{V}(P)$ *(pour une variable* P *quelconque)*
- $a \Vdash \neg\phi$ *si et seulement si* $a \nVdash \phi$
- $a \Vdash (\phi \vee \psi)$ *si et seulement si* $(a \Vdash \phi$ ou $a \Vdash \psi)$
- $a \Vdash (\phi \wedge \psi)$ *si et seulement si* $(a \Vdash \phi$ et $a \Vdash \psi)$
- $a \Vdash (\phi \longrightarrow \psi)$ *si et seulement si* $(a \nVdash \phi$ ou $a \Vdash \psi)$
- $a \Vdash (\phi \longleftrightarrow \psi)$ *si et seulement si* $((a \Vdash \phi$ et $a \Vdash \psi)$ ou $(a \nVdash \phi$ et $a \nVdash \psi))$
- $a \Vdash [i]\phi$ *si et seulement si pour tout* b*, si* $a \xrightarrow{i} b$ *alors* $b \Vdash \phi$
- $a \Vdash \langle i \rangle\phi$ *si et seulement si il existe* b *tel que* $a \xrightarrow{i} b$ *et* $b \Vdash \phi$*.*

Exemple 207 Dans le schéma ci-dessous, le système de transition comprend quatre nœuds (a, b, c, d), les variables propositionnelles considérées sont P et Q et la valuation est définie par $\mathcal{V}(P) = \{a, b\}$, $\mathcal{V}(Q) = \{a, d\}$.



- $a \Vdash P$
- $a \Vdash (P \wedge \Box P)$
- $a \nVdash \Diamond\neg P$
- $b \Vdash P$
- $b \nVdash Q$
- $b \Vdash \Diamond Q$
- $c \Vdash \Box Q$
- $c \nVdash \Box P$
- $c \Vdash \Box\Box(P \vee Q)$
- $c \Vdash \Diamond\Diamond\Diamond\neg(P \vee Q)$
- $d \Vdash Q$
- $d \nVdash \Box P$
- $d \Vdash \Diamond\Diamond Q$
- $d \Vdash \Diamond\Box\Diamond\neg P$.

Remarque 208

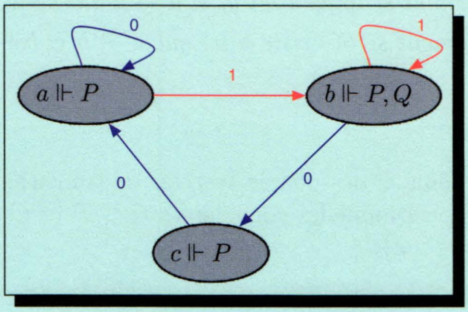
(1) La satisfaction d'une formule en un nœud d'un système de transition équipé d'une valuation $\mathcal{V}$ dépend bien évidemment de ces trois ingrédients. Ainsi on utilisera la notation $\langle S, \mathcal{V}, a \rangle \Vdash \phi$ pour le dénoter.

(2) Dans le cas où ϕ n'est qu'une formule du Calcul Propositionnel, la satisfaction de cette formule au nœud a n'est pas autre chose que la satisfaction de cette formule dans un modèle du Calcul Propositionnel muni de la distribution de valeurs de vérité induite par $\mathcal{V}$. A savoir, P est vraie dans le monde a si et seulement si $a \in \mathcal{V}(P)$.

(3) S'il n'existe pas de nœud b tel que $a \xrightarrow{i} b$, alors quelle que soit la formule ϕ, $a \Vdash \langle i \rangle \phi$ est toujours fausse. Autrement dit, $a \nVdash \langle i \rangle \phi$.

(4) Par contre, s'il n'existe pas de nœud b tel que $a \xrightarrow{i} b$, alors $a \Vdash [i]\phi$ est toujours vraie quelque soit la formule ϕ. En effet, la condition pour que $a \Vdash [i]\phi$ soit vérifiée repose sur le fait que (pour un nœud b quelconque) si $a \xrightarrow{i} b$ est attesté ; alors $b \Vdash \phi$. Mais la condition $a \xrightarrow{i} b$ n'est jamais vérifiée, donc l'implication "si…, alors…" est vraie.

Exemple 209 Dans le schéma ci-dessous, le système de transition comprend trois nœuds (a, b, c), les variables propositionnelles sont P et Q et la valuation est définie par $\mathcal{V}(P) = \{a, b, c\}$, $\mathcal{V}(Q) = \{b\}$.



- $a \Vdash P$
- $a \Vdash (P \longrightarrow [0]P)$
- $a \nVdash \langle 1 \rangle \neg P$
- $b \Vdash P$
- $b \Vdash (P \wedge ([0]P \wedge [0][0]P))$
- $b \nVdash \langle 0 \rangle Q$
- $c \nVdash [0]Q$
- $c \Vdash [1]Q$
- $c \Vdash [0][1](P \wedge Q)$
- $c \Vdash ([0][1][0]\psi \longleftrightarrow \psi)$.

Pour aller plus avant :

Pour des références traitant de l'approche classique de la sémantique, nous renvoyons le lecteur vers les ouvrages suivants : *"An introduction to non-classical logic"* de Graham Priest [Pri01], *"Modal logic : an introduction to its syntax and semantics"* de Nino B. Cocchiarella et Max A. Freund [CF08], *"Modal logic : an introduction"* de Brian F. Chellas [Che80], *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03], ainsi que *"Modal logic"* de Alexander Chagrov et Michael Zakharyaschev [CZ97] et *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02].

Pour une approche plus proche de la philosophie : *"Modal logic for philosophers"* de James W. Garson [Gar06], ainsi que les deux ouvrages de Rod Girle : *"Modal logics and Philosophy"* [Gir00] et *"Possible worlds"* [Gir03].

---

4 Jeux d'évaluation

***Résumé* № 29** *L'évaluation d'une formule ϕ en un nœud a d'un modèle de Kripke $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ est présentée comme la résolution d'un jeu : $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a \rangle, \phi)$. Ce jeu comporte deux joueurs – le* **V**érificateur *et le* **F**alsificateur *– qui opèrent des choix de bifurcation sur l'arbre de la formule ϕ en fonction des connecteurs logiques de celle-ci, ainsi que des trajets à l'intérieur du modèle de Kripke $\mathcal{M}$, en fonction des opérateurs modaux que cette formule renferme.*

Le jeu est identique au jeu d'évaluation des formules du Calcul Propositionnel, à la différence que lorsqu'un opérateur modal est rencontré, le **V**érificateur *(s'il s'agit de $\langle i \rangle$)et le* **F**alsificateur *(s'il s'agit de $[i]$) choisissent également un monde "c" accessible depuis le monde "b" dans lequel il se trouve à ce moment de la partie (i.e., $b \xrightarrow{i} c$).*

Une partie se termine lorsqu'une feuille de la formule est atteinte. Elle est gagnée par le **V**érificateur *si cette feuille correspond à une variable propositionnelle forcée dans le monde dans lequel il se trouve à cette étape. Autrement, elle est gagnée par son adversaire.*

On vérifie $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi$ si et seulement si le **V**érificateur *possède une stratégie gagnante dans le jeu $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a \rangle, \phi)$.* ※

Etant donné un système de transition $\mathcal{S}$, une valuation $\mathcal{V}$, un nœud a et une formule ϕ, $a \Vdash \phi$ revient à déterminer lequel des deux joueurs possède une stratégie gagnante dans un jeu qui reprend trait pour trait les règles du jeu d'évaluation d'une formule du Calcul Propositionnel dans un modèle, et en ajoute simplement deux pour prendre en compte le cas des opérateurs modaux. Ce jeu, noté $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a \rangle, \phi)$, est le *jeu d'évaluation* de la logique modale. C'est un jeu fini à deux joueurs et à information parfaite. Par conséquent, c'est un jeu qui est déterminé.

Définition 210 *Soient ϕ une formule dont tous les connecteurs logiques sont parmi $\{\neg, \vee, \wedge\}$, I un ensemble non vide, $\mathcal{S} = (N, A)$ un système de transition étiqueté par I et équipé d'une valuation $\mathcal{V}$, enfin $a \in N$ un nœud. Le jeu d'évaluation $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a \rangle, \phi)$ est défini comme suit :*

(1) il comprend deux joueurs appelés **V**érificateur *et* **F**alsificateur*. Le* **V**érificateur *(**V**) cherche à montrer que la formule est forcée au nœud a, alors que le* **F**alsificateur *(**F**) au contraire cherche à montrer qu'elle ne l'est pas.*

Les coups de ces deux joueurs consistent à choisir des positions de la forme (b, ψ), où ψ est une sous-formule de la formule apparaissant au coup précédent (la formule de départ étant ϕ), et $b \in N$ est un nœud du graphe (le nœud de départ étant a).

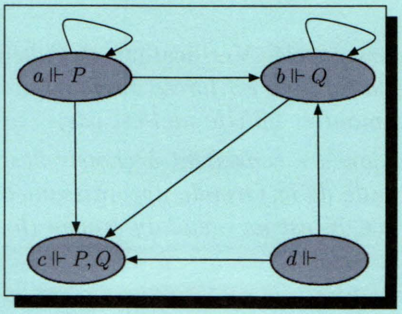
(2) Tout cela en respectant les règles suivantes :

si la position actuelle du jeu est...	*c'est au tour de...*	*le jeu continue avec...*
$(b, (\varphi_0 \vee \varphi_1))$	**V** *choisit* $j \in \{0,1\}$	(b, φ_j)
$(b, (\varphi_0 \wedge \varphi_1))$	**F** *choisit* $j \in \{0,1\}$	(b, φ_j)
$(b, \neg\varphi)$	**F** *et* **V** *échangent leurs rôles*	(b, φ)
$(b, \langle i \rangle \varphi)$	**V** *choisit* c *tel que* $b \xrightarrow{i} c$	(c, φ)
$(b, [i]\varphi)$	**F** *choisit* c *tel que* $b \xrightarrow{i} c$	(c, φ)
(b, φ) $\varphi \in \{\top, \bot\} \cup VAR$	*personne*	*le jeu s'arrête,* **V** *gagne ssi* $b \Vdash \varphi$

(3) La condition de gain apparaît une fois la partie terminée. Celle-ci s'arrête nécessairement sur une position de la forme (b, P), $(b, \bot)$, ou encore $(b, \top)$. Si la position est $(b, \bot)$, **F** *gagne, et si elle est $(b, \top)$,* **V** *l'emporte. Finalement, dans le cas d'une variable propositionnelle,* **V** *gagne si $b \Vdash P$ et* **F** *gagne si $b \nVdash P$.*

Remarque 211 Il est important de remarquer que lorsqu'un joueur ne peut choisir un monde possible, alors ce joueur perd la partie ! Cette règle du jeu est nécessaire pour que dans un monde *"a"* dont aucune flèche pour l'agent i ne part, les formules de la forme $[i]\phi$ soient réalisées et celles de la forme $\langle i \rangle \phi$ ne soient pas réalisées.

Exemple 212 Soit $\langle \mathcal{S}, \mathcal{V} \rangle$ le modèle de Kripke suivant :



(1) Un exemple de partie dans le jeu $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a\rangle, \Box(\Diamond P \vee (\neg Q \wedge P)))$:
   (a) **F** choisit le nœud c, on continue donc en c avec $(\Diamond P \vee (\neg Q \wedge P))$.
   (b) **V** choisit la seconde partie de la disjonction, on continue en c avec $(\neg Q \wedge P)$.
   (c) **F** choisit la première partie de la conjonction, on continue en c avec $\neg Q$.
   (d) **V** et **F** échangent leurs rôles, on continue en c avec Q.
   (e) Stop. Puisque $c \Vdash Q$, le **V**érificateur actuel gagne la partie[1].

(2) Un exemple de partie dans le jeu $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, d\rangle, \Box(\Diamond P \vee (\neg Q \wedge P)))$:
   (a) **F** choisit de déplacer le jeu au nœud b, on continue en b avec $(\Diamond P \vee (\neg Q \wedge P))$.
   (b) **V** choisit la première partie de la disjonction, on continue en b avec $\Diamond P$.
   (c) **V** choisit de déplacer le jeu au nœud c, on continue en c avec P.
   (d) Stop. Puisque $c \Vdash P$, **V** l'emporte.

(3) Un exemple de partie dans le jeu $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, c\rangle, \Box(\Diamond P \vee (\neg Q \wedge P)))$:
   (a) **F** ne peut déplacer le jeu du nœud c, donc **F** perd la partie et **V** l'emporte.

1. Mais comme les joueurs ont échangé leurs rôles un nombre impair de fois, le **V**érificateur actuel n'est autre que le **F**alsificateur du début. Ainsi, le **F**alsificateur au début de la partie l'emporte.

Théorème 213 *Soient ϕ une formule dont tous les connecteurs logiques sont parmi $\{\neg, \vee, \wedge\}$, I un ensemble non vide, $\mathcal{S} = (N, A)$ un système de transition étiqueté par I et équipé d'une valuation $\mathcal{V}$, enfin $a \in N$ un nœud,*

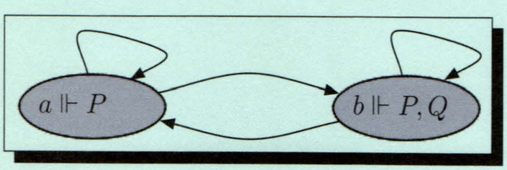
$$\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi \textit{ ssi } \mathbf{V} \textit{ a une stratégie gagnante dans } \mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a\rangle, \phi)\,.$$

Preuve du Théorème 213 : La preuve est par induction sur la hauteur de la formule ϕ. On montre simultanément que :

- si $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi$ alors **V** a une stratégie gagnante dans $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a\rangle, \phi)$,
- si $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \neg\phi$ alors **F** a une stratégie gagnante dans $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a\rangle, \phi)$.

$\dashv$ 213

Exemple 214 Soit $\langle \mathcal{S}, \mathcal{V}\rangle$ le modèle de Kripke suivant :



Une stratégie gagnante pour **V** dans le jeu $\mathbb{E}v\,(\langle \mathcal{S}, \mathcal{V}, a\rangle, \Diamond(\Box\Diamond P \vee \Diamond\Box Q))$

(1) **V** choisit de déplacer le jeu au nœud b, on continue en b avec $(\Box\Diamond P \vee \Diamond\Box Q)$.

(2) **V** choisit la première partie de la disjonction, le jeu continue en b avec $\Box\Diamond P$.

(3) (a) Si **F** choisit de rester au nœud b, on continue en b avec $\Diamond P$.

(A) **V** choisit de déplacer le jeu au nœud a, et **V** gagne puisque $a \Vdash P$.

(b) Si **F** choisit déplacer le jeu au nœud a, on continue en a avec $\Diamond P$.

(A) **V** choisit de rester au nœud a, et donc l'emporte puisque $a \Vdash P$.

Pour aller plus avant :

Pour retrouver l'approche théorique des jeux de la sémantique de la logique modale, le lecteur pourra se reporter aux ouvrages *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06] et *"Modal Logic for Open Minds"* de Johan van Benthem [vB10], ainsi qu'à l'article de Johan van Benthem *"Logic and Game Theory : Close Encounters of the Third Kind"* [vB03].

---

5 Modèles et classes, vérité et validité

***Résumé* № 30**

- *Un* modèle $\mathcal{M}$ *de la logique modale (*modèle de Kripke*) est la donnée d'un système de transition muni d'une valuation :*

$$\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle.$$

- *Une formule* ϕ *est* vraie *dans un modèle* $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ *si elle est forcée en chacun des nœuds du système de transition :*

$$\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi.$$

- *Une formule* ϕ *est* valide *dans un système de transition* $\mathcal{S}$ *si elle est* vraie *dans chacun des modèles construits sur ce système de transition :*

$$\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi.$$

- *Si une formule* ϕ *est* valide *dans tout système de transition* $\mathcal{S}$ *d'une* classe de modèles $\mathscr{C}$*, on le note :*

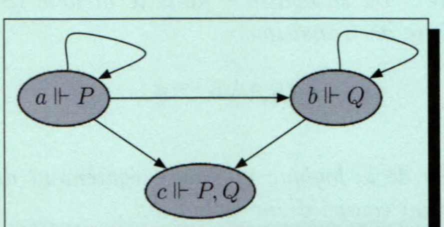
$$\mathscr{C} \Vdash^{\forall a, \forall \mathcal{V}} \phi.$$

※

Définition 215 *Soient* ϕ *une formule,* I *un ensemble non vide,* $\mathcal{S} = (N, A)$ *un système de transition étiqueté par* I*,* a *un nœud de* $\mathcal{S}$ *et* $\mathcal{V}$ *une valuation, on définit les relations suivantes :*

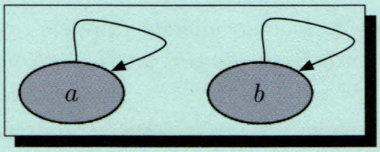
$\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi$	*si et seulement si*	*pour chaque nœud* $a', \langle \mathcal{S}, \mathcal{V}, a' \rangle \Vdash \phi$
$\langle \mathcal{S}, a \rangle \Vdash^{\forall \mathcal{V}} \phi$	*si et seulement si*	*pour toutes valuations* $\mathcal{V}'$, $\langle \mathcal{S}, \mathcal{V}', a \rangle \Vdash \phi$
$\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi$	*si et seulement si*	*pour tous nœuds* a' *et toutes valuations* $\mathcal{V}'$, $\langle \mathcal{S}, \mathcal{V}', a' \rangle \Vdash \phi$.

Exemple 216 Un système de transition $\mathcal{S}$ équipé de la valuation $\mathcal{V}$:



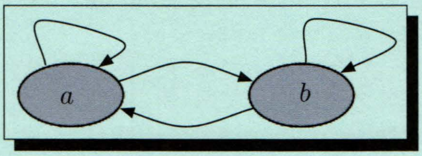
- $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} (P \vee Q)$
- $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} (P \vee \neg P)$
- $\langle \mathcal{S}, \mathcal{V} \rangle \nVdash^{\forall a} (P \longrightarrow Q)$
- $\langle \mathcal{S}, \mathcal{V} \rangle \nVdash^{\forall a} (\Box P \longrightarrow \Diamond P)$
- $\langle \mathcal{S}, \mathcal{V} \rangle \nVdash^{\forall a} (P \longrightarrow \Box P)$
- $\langle \mathcal{S}, \mathcal{V} \rangle \nVdash^{\forall a} (\Box P \longleftrightarrow P)$

Exemple 217 Soit $\mathcal{S}$ le système de transition suivant :



- $\mathcal{S} \nVdash^{\forall a, \forall \mathcal{V}} P$
- $\mathcal{S} \nVdash^{\forall a, \forall \mathcal{V}} \Box P$
- $\mathcal{S} \nVdash^{\forall a, \forall \mathcal{V}} \Diamond P$
- $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (\Diamond P \longrightarrow P)$
- $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (P \longrightarrow \Box P)$
- $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (\Box P \longrightarrow P)$

Exemple 218 Soit $\mathcal{T}$ le système de transition suivant :



- $\mathcal{T} \nVdash^{\forall a, \forall \mathcal{V}} P$
- $\mathcal{T} \nVdash^{\forall a, \forall \mathcal{V}} (P \longrightarrow \Box P)$
- $\mathcal{T} \nVdash^{\forall a, \forall \mathcal{V}} \Box P$
- $\mathcal{T} \Vdash^{\forall a, \forall \mathcal{V}} (\Box P \longrightarrow P)$
- $\mathcal{T} \Vdash^{\forall a, \forall \mathcal{V}} (\Box\Box P \longrightarrow P)$
- $\mathcal{T} \Vdash^{\forall a, \forall \mathcal{V}} (\Box P \longrightarrow \Box\Box P)$

Définition 219 *Un* modèle *de la logique modale – également dénommé* modèle de Kripke *– est un système de transition équipé d'une valuation :*

$$\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle.$$

Une formule ϕ est vraie – ou satisfaite – dans le modèle $\langle \mathcal{S}, \mathcal{V} \rangle$ – si elle est forcée en chacun des nœuds du système de transition :

$$\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi.$$

Définition 220 *Un* modèle *de la logique modale – également dénommé* modèle de Kripke *– est un système de transition équipé d'une valuation :*

$$\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle.$$

Une formule ϕ est vraie *– ou* satisfaite *– dans le modèle $\langle \mathcal{S}, \mathcal{V} \rangle$ – si elle est forcée en chacun des nœuds du système de transition :*

$$\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi.$$

Remarques 221

(1) La notion de vérité dans un modèle de Kripke est une notion globale, elle prend en compte l'ensemble des nœuds du système de transition ; par opposition à la notion de vérité locale – celle qui statue sur l'état des choses en un nœud. Ainsi, par exemple une formule de la forme $\phi \vee \psi$ est vraie localement si et seulement si l'une des deux formules est vraie localement :

$$\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi \vee \psi \text{ si et seulement si } \Big(\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi \text{ ou } \langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \psi\Big).$$

Par contre, il en va tout autrement de la validité globale de cette même formule :

$$\langle \mathcal{S}, \mathcal{V}\rangle \Vdash^{\forall a} \phi \vee \psi \text{ n'implique pas } \Big(\langle \mathcal{S}, \mathcal{V}\rangle \Vdash^{\forall a} \phi \text{ ou } \langle \mathcal{S}, \mathcal{V}\rangle \Vdash^{\forall a} \psi\Big).$$

Un contre exemple immédiat est fourni par la formule $P \vee \neg P$ avec le système de transition $\mathcal{S}$ équipé de la valuation $\mathcal{V}$ de l'exemple 214. Il est clair que $\langle \mathcal{S}, \mathcal{V}\rangle \Vdash^{\forall a}$ $Q \vee \neg Q$, par contre $b \Vdash Q$ alors que $a \Vdash \neg Q$, donc $\langle \mathcal{S}, \mathcal{V}\rangle \nVdash^{\forall a} Q$ et $\langle \mathcal{S}, \mathcal{V}\rangle \nVdash^{\forall a} \neg Q$.

(2) On retrouve les modèles du Calcul Propositionnel si l'on se restreint aux systèmes de transition qui ne comportent qu'un seul nœud. En effet, une formule ϕ de profondeur modale nulle est une formule du Calcul Propositionnel (et réciproquement). Soit $\mathcal{M}$ un modèle du Calcul Propositionnel défini par la distribution de valeur de vérité $\delta_{\mathcal{M}}$ qui associe aux variables apparaissant dans ϕ la valeur 1 lorsqu'elles sont vraies dans $\mathcal{M}$ et 0 lorsqu'elles sont fausses[2]. La formule ϕ est vraie dans $\mathcal{M}$ (noté $\mathcal{M} \models \phi$) si et seulement si cette même formule ϕ est vraie dans le système de transition $\mathcal{S}_{\mathcal{M}} = (N, A)$, où $N = \{a\}$ et $A = \emptyset$, équipé de la valuation $\mathcal{V}_{\delta_{\mathcal{M}}}$ défini par : $\mathcal{V}_{\delta_{\mathcal{M}}}(P) = \{a\}$ si et seulement si $\delta_{\mathcal{M}}(P) = 1$ et $\mathcal{V}_{\delta_{\mathcal{M}}}(P) = \emptyset$ si et seulement si $\delta_{\mathcal{M}}(P) = 0$. Ce qui s'écrit :

$$\mathcal{M} \models \phi \text{ si et seulement si } \langle \mathcal{S}, \mathcal{V}_{\delta_{\mathcal{M}}}\rangle \Vdash^{\forall a} \phi.$$

Définition 222 *Soient ϕ une formule de la logique modale et $\mathcal{S}$ un système de transition. La formule ϕ est* valide *dans le système de transition $\mathcal{S}$ si :*

$$\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi.$$

Remarque 223 La notion de validité se distingue de la notion locale de vérité. Une formule de la forme $\phi \vee \psi$ peut être valide dans le système de transition $\mathcal{S}$ sans que ni ϕ ni ψ ne le soit. En effet, si nous considérons la formule $P \vee \neg P$, cette formule sera valide dans tout système de transition, quels que soient le nombre de ses nœuds et les arêtes entre ceux-ci. Par contre, dès que ce système possède plus d'un nœud, il suffit de considérer une valuation qui assigne le premier nœud à la variable P mais non le second, pour obtenir un modèle dans lequel ni P ni $\neg P$ ne seront globalement (en tous nœuds) vraies.

Proposition 224 *Soient ϕ une formule de* profondeur modale nulle, *$\mathcal{S} = (N, A)$ un système de transition. Les affirmations suivantes sont équivalentes :*

(1) $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi$,

(2) il existe $a \in N$ tel que $\langle \mathcal{S}, a\rangle \Vdash^{\forall \mathcal{V}} \phi$,

(3) pour $\mathcal{T} = (\{a\}, \emptyset)$, $\langle \mathcal{T}, a\rangle \Vdash^{\forall \mathcal{V}} \phi$,

(4) ϕ est une tautologie du Calcul Propositionnel.

2. $\delta_{\mathcal{M}}(P) = 1$ si et seulement si $\mathcal{M} \models P$.

Preuve de la Proposition 224 : La preuve s'effectue directement en montrant la suite des implications (1)$\longrightarrow$(2), (2)$\longrightarrow$(3), (3)$\longrightarrow$(4) et (4)$\longrightarrow$(1). La circularité nous fournissant immédiatement les implications inverses - ainsi par exemple, (2)$\longrightarrow$(1) découle de (2)$\longrightarrow$(3)$\longrightarrow$(4)$\longrightarrow$(1) – nous obtenons dès lors les équivalences voulues.

- Les implications (1)$\longrightarrow$(2) et (2)$\longrightarrow$(3) sont immédiates.
- Pour montrer (3)$\longrightarrow$(4), nous allons montrer $\neg$(4)$\longrightarrow$ $\neg$(3), c'est-à-dire montrer la contraposée. Nous supposons que ϕ n'est pas une tautologie du Calcul Propositionnel. Il existe donc un modèle $\mathcal{M}$ dans lequel cette formule est fausse. Nous équipons alors le système de transition $\mathcal{T} = (\{a\}, \emptyset)$ de la valuation suivante : pour chacune des variables propositionnelles P apparaissant dans ϕ, $a \in \mathcal{V}(P)$ si et seulement si $\mathcal{M} \models P$. Par simple définition de la satisfaction locale d'une formule, il apparaît immédiatement que :

$$\langle \mathcal{T}, \mathcal{V}, a\rangle \Vdash \phi \text{ si et seulement si } \mathcal{M} \models \phi.$$

  Or, comme il n'y a qu'un nœud dans le système $\mathcal{T}$, il s'ensuit que :

$$\langle \mathcal{T}, \mathcal{V}, a\rangle \Vdash \phi \text{ si et seulement si } \langle \mathcal{T}, , \mathcal{V}\rangle \Vdash^{\forall a} \phi.$$

  Notre hypothèse étant $\mathcal{M} \not\models \phi$, nous en déduisons à la fois $\langle \mathcal{T}, \mathcal{V}, a\rangle \nVdash \phi$ et $\langle \mathcal{T}, \mathcal{V}\rangle \nVdash \phi$. Ce qui montre $\mathcal{T} \nVdash^{\forall a, \forall \mathcal{V}} \phi$.
- Pour montrer (4)$\longrightarrow$(1), nous allons également passer par la contraposée et montrer $\neg$(1)$\longrightarrow$ $\neg$(4). Nous supposons que la relation $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi$ n'est pas satisfaite, et donc qu'il existe une valuation $\mathcal{V}$ et un nœud a tel que $\langle \mathcal{S}, \mathcal{V}, a\rangle \nVdash \phi$. On définit le modèle du Calcul Propositionnel $\mathcal{M}$ par $\mathcal{M} \models P$ si et seulement si $a \in \mathcal{V}(P)$, et ce pour chaque variable propositionnelle apparaissant dans ϕ. On a donc que $\mathcal{M} \not\models \phi$. Par conséquent, ϕ n'est pas une tautologie.

$\dashv$ 224

Exemple 225 Soient I un singleton, $\mathcal{S} = (N, A)$ un système de transition **réflexif**[3], pour toute formule ϕ la relation suivante est vérifée :

$$\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (\Box\phi \longrightarrow \phi).$$

En effet, si un nœud a quelconque, pour une valuation quelconque, vérifie $a \Vdash \Box\phi$, alors par définition, pour tout b tel que $a \to b$, $b \Vdash \phi$. Puisque $\mathcal{S}$ est réflexif, a est lui-même l'un de ces "b" et donc $a \Vdash \Box\phi$.

3. Pour tout nœud $a \in N$, $a \to a$.

L'exemple suivant est en quelque sorte la réciproque de ce que nous venons de voir. A savoir, nous venons de trouver une formule qui est valide dans tous les systèmes de transition réflexifs. Nous allons voir qu'en fait cette formule n'est valide que dans ces seuls systèmes de transition réflexifs et que par conséquent, elle les caractérise.

Exemple 226 Soient I un singleton, $\mathcal{S} = (N, A)$ un système de transition étiqueté par I. Si pour toute formule ϕ la relation suivante est vérifée :

$$\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (\Box\phi \longrightarrow \phi),$$

alors

$$\mathcal{S} \text{ est } \textbf{réflexif}.$$

En effet, supposons que $\mathcal{S}$ ne soit pas réflexif. Il s'en suit qu'il existe un nœud a tel que $a \not\to a$. Soient $\phi = P$ une formule de hauteur 0 et $\mathcal{V}$ une valuation telle que $b \in \mathcal{V}(P)$ si et seulement si $a \to b$. Par définition de $\mathcal{V}$, $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box P$, mais pourtant $\langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash P$ et donc $\langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash (\Box P \longrightarrow P)$. Cela prouve ainsi que $\mathcal{S} \nVdash^{\forall a, \forall \mathcal{V}} (\Box\phi \longrightarrow \phi)$, ce qui contredit l'hypothèse.

Nous venons en fait de démontrer le résultat qui suit.

Lemme 227 *Pour tout système de transition $\mathcal{S}$, les affirmations suivantes sont équivalentes :*

(1) $\mathcal{S}$ *est* réflexif.

(2) Pour toute formule ϕ, $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (\Box\phi \longrightarrow \phi)$.

Preuve du Lemme 227 : L'Exemple 225 prouve (1)$\Rightarrow$ (2) et l'Exemple 226 prouve (1)$\Leftarrow$ (2).

$\dashv$ 227

Nous venons de voir que les formules de la forme $\Box\phi \longrightarrow \phi$ caractérisaient en quelque sorte les systèmes de transition qui sont réflexifs. Nous allons maintenant considérer l'implication inverse et nous demander s'il existe une propriété des systèmes de transition que les formules de la forme $\phi \longrightarrow \Box\phi$ caractérisent.

Exemple 228 Convenons d'appeler **famélique** tout système de transition qui satisfait :

$$\text{si } a \to b \text{ alors } a = b.$$

Un système de transition $\mathcal{S}$ muni de la valuation $\mathcal{V}$ satisfait la formule $\phi \longrightarrow \Box\phi$ au nœud a, si, lorsque de $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi$, il s'en suit $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\phi$. Autrement dit, dès qu'une formule est satisfaite en un nœud elle doit être satisfaite en chacun des successeurs de ce nœud.

(1) Cela ne pose évidemment pas de problème si tout nœud n'a soit pas de successeur, soit n'a que lui-même comme successeur.

(2) Mais dans le cas où il existe un nœud a qui possède un successeur b différent de lui-même, alors il suffit de considérer la formule $\phi = P$ ainsi qu'une valuation $\mathcal{V}$ qui vérifie simplement $a \in \mathcal{V}(P)$, et $b \notin \mathcal{V}(P)$, pour obtenir :

- $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi$
- $\langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash \Box\phi$
- $\langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash \phi \longrightarrow \Box\phi$.

Nous avons ainsi montré :

Lemme 229 *Pour tout système de transition $\mathcal{S}$, les affirmations suivantes sont équivalentes :*

(1) $\mathcal{S}$ *est* famélique[4].

(2) Pour toute formule ϕ, $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} (\phi \longrightarrow \Box\phi)$.

Preuve du Lemme 229 : (1)$\Rightarrow$ (2) est traité dans l'Exemple 228(1) ; (1)$\Leftarrow$ (2) est traité dans l'Exemple 228(2). $\dashv$ 229

Plus généralement, nous serons amenés à nous intéresser non pas simplement à un système de transition particulier, mais à une collection de tels systèmes que nous appellerons une *classe de systèmes de transition.* De telles collections ne seront pas nécessairement finies. Par contre, elles seront toujours définies par des moyens finis comme des propriétés de théorie des graphes ou bien des propriétés relationnelles communes.

Notation 230 *Soient* ϕ *une formule,* $\mathscr{C}$ *une classe de systèmes de transition,*

$$\mathscr{C} \Vdash \phi \textit{ si et seulement si } \text{pour tout } \mathcal{S} \in \mathscr{C}, \quad \mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi.$$

Pour le dire en un mot, la notation $\mathscr{C} \Vdash \phi$ désigne le fait que ϕ est valide ($\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi$) dans tout système de transition $\mathcal{S}$ de la classe $\mathscr{C}$.

Exemple 231 Soit $\mathscr{C}$, la classe de tous les systèmes de transition.

$$\mathscr{C} \Vdash \Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q).$$

En effet, soient $\mathcal{S}$ un système de transition, a un nœud de $\mathcal{S}$ et $\mathcal{V}$ une valuation quelconque.

Si

$$\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Box(P \longrightarrow Q),$$

alors pour tout b tel que $a \to b$,

$$\langle \mathcal{S}, \mathcal{V}, b\rangle \Vdash P \longrightarrow Q.$$

Pour montrer

$$\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Box P \longrightarrow \Box Q$$

il suffit de supposer

$$\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Box P$$

et de montrer

$$\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Box Q.$$

Or,

$$\text{si } \langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Box P, \text{ alors } \langle \mathcal{S}, \mathcal{V}, b\rangle \Vdash P \quad (\text{tous } b \text{ tel que } a \to b).$$

4. Un système de transition est dit *famélique* si pour chacun de ses nœuds a, on a si $a \to b$ alors $a = b$.

Comme par hypothèse

$$\langle \mathcal{S}, \mathcal{V}, b \rangle \Vdash P \longrightarrow Q,$$

nous en déduisons

$$\langle \mathcal{S}, \mathcal{V}, b \rangle \Vdash Q.$$

Comme cela est vrai de n'importe quel nœud b tel que $a \rightarrow b$, nous en déduisons

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box Q.$$

Exemple 232 Soit $\mathscr{C}_{tr.}$ la classe de tous les systèmes de transition **transitifs**

$$\mathscr{C}_{tr.} \Vdash \Box\phi \longrightarrow \Box\Box\phi$$

En effet, soient $\mathcal{S}$ un système de transition *transitif* quelconque, $\mathcal{V}$ une valuation et a un nœud.

Si

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\phi,$$

alors pour tout nœud b tel que $a \rightarrow b$,

$$\langle \mathcal{S}, \mathcal{V}, b \rangle \Vdash \phi.$$

Pour montrer

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\Box\phi,$$

il suffit de montrer que pour tout c tel qu'il existe b vérifiant $a \rightarrow b$ et $b \rightarrow c$, on a

$$\langle \mathcal{S}, \mathcal{V}, c \rangle \Vdash \phi.$$

Or puisque $\mathcal{S}$ est transitif, $a \rightarrow b$ et $b \rightarrow c$ implique $a \rightarrow c$. D'où $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\phi$ entraîne

$$\langle \mathcal{S}, \mathcal{V}, c \rangle \Vdash \phi.$$

Exemple 233 Considérons une classe quelconque $\mathscr{C}$ qui vérifie pour toute formule ϕ :

$$\mathscr{C} \Vdash \Box\phi \longrightarrow \Box\Box\phi.$$

Cela entraîne que tous les systèmes de transition de $\mathscr{C}$ sont *transitifs*.

En effet, supposons qu'il existe un système de transition non transitif $\mathcal{S}$ appartenant à $\mathscr{C}$. Soient a, b, c trois nœuds de $\mathcal{S}$ tels que $a \rightarrow b$, $b \rightarrow c$ et $a \not\rightarrow c$. Soit $\mathcal{V}$ une valuation qui vérifie $d \in \mathcal{V}(P)$ si et seulement si $a \rightarrow d$. Pour $\phi = P$, nous obtenons donc à la fois :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\phi \text{ et } \langle \mathcal{S}, \mathcal{V}, c \rangle \nVdash \phi$$

ce qui montre :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\phi \text{ et } \langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash \Box\Box\phi$$

d'où

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \not\Vdash \Box\phi \longrightarrow \Box\Box\phi$$

et donc

$$\mathscr{C} \Vdash \Box\phi \longrightarrow \Box\Box\phi.$$

Lemme 234 *Pour tout système de transition $\mathcal{S}$, les affirmations suivantes sont équivalentes :*

(1) $\mathcal{S}$ *est* transitif[5].

(2) Pour toute formule ϕ, $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \Box\phi \longrightarrow \Box\Box\phi$.

Preuve du Lemme 234 : (1)$\Rightarrow$ (2) est traité dans l'Exemple 232 ; (1)$\Leftarrow$ (2) est traité dans l'Exemple 233. $\dashv$ 234

Exemple 235 On nomme **dense** un système de transition qui vérifie pour tous nœuds a, c : si $a \to c$, alors il existe b tel que $a \to b$ et $b \to c$. La classe de tous les systèmes de transition *denses* – notée $\mathscr{C}_{dense}$ – est “caractérisée” par les formules de la forme $\Box\Box\phi \longrightarrow \Box\phi$ au sens où :

$$\mathscr{C}_{dense} \Vdash \Box\Box\phi \longrightarrow \Box\phi.$$

En effet, prenons $\mathcal{S} \in \mathscr{C}_{dense}$, a un nœud de $\mathcal{S}$ et $\mathcal{V}$ une valuation quelconque. Supposons que $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\Box\phi$ est vérifié et montrons que $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\phi$ l'est également. Pour cela, soit c quelconque qui vérifie $a \to c$. Il nous faut montrer $\langle \mathcal{S}, \mathcal{V}, c \rangle \Vdash \phi$. Or, $\mathcal{S}$ étant dense, il existe b tel que $a \to b$ et $b \to c$. Par conséquent, l'hypothèse $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box\Box\phi$ entraîne aussitôt $\langle \mathcal{S}, \mathcal{V}, c \rangle \Vdash \phi$.

Exemple 236 Si pour toute formule ϕ, $\mathcal{T}$ vérifie

$$\mathcal{T} \Vdash^{\forall a, \forall \mathcal{V}} \Box\Box\phi \longrightarrow \Box\phi,$$

alors $\mathcal{T} \in \mathscr{C}_{dense}$.

Supposons que $\mathcal{T}$ vérifie $\mathcal{T} \Vdash^{\forall a, \forall \mathcal{V}} \Box\Box\phi \longrightarrow \Box\phi$ pour n'importe quelle formule ϕ bien que $\mathcal{T}$ ne soit pas dense. Il existe donc deux nœuds a et c tels que $a \to c$ mais pourtant aucun b ne vérifie à la fois $a \to b$ et $b \to c$. Considérons $\mathcal{V}$ la valuation définie par $d \in \mathcal{V}(P)$ si et seulement si $d \neq c$. Il s'en suit que

$$\text{si } \langle \mathcal{T}, \mathcal{V}, c \rangle \not\Vdash P \text{ alors } \langle \mathcal{T}, \mathcal{V}, a \rangle \not\Vdash \Box P,$$

et pourtant,

$$\langle \mathcal{T}, \mathcal{V}, a \rangle \Vdash \Box\Box P.$$

D'où

$$\langle \mathcal{T}, \mathcal{V}, a \rangle \not\Vdash \Box\Box P \longrightarrow \Box P.$$

ce qui contredit l'hypothèse.

5. Un système de transition est *transitif* lorsque pour tous nœuds a, b, c, si $a \to b$ et $b \to c$ alors, $a \to c$.

Lemme 237 *Pour tout système de transition $\mathcal{S}$, les affirmations suivantes sont équivalentes :*

(1) $\mathcal{S}$ est dense[6].

(2) Pour toute formule ϕ, $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \Box\phi \longrightarrow \Box\Box\phi$.

Preuve du Lemme 237 : (1)$\Rightarrow$ (2) est traité dans l'Exemple 235 ; (1)$\Leftarrow$ (2) est traité dans l'Exemple 236. $\dashv$ 237

On définit les notations suivantes :

Notation 238 *Soient Γ un ensemble de formules, $\mathcal{S}$ un système de transition, $\mathcal{V}$ une valuation sur $\mathcal{S}$, a un nœud de N, $\mathscr{C}$ une classe de systèmes de transition, on écrit :*

- $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Gamma$ *si et seulement si pour toute formule* $\phi \in \Gamma$, $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi$
- $\langle \mathcal{S}, a\rangle \Vdash^{\forall \mathcal{V}} \Gamma$ *si et seulement si pour toute formule* $\phi \in \Gamma$, $\langle \mathcal{S}, a\rangle \Vdash^{\forall \mathcal{V}} \phi$
- $\langle \mathcal{S}, \mathcal{V}\rangle \Vdash^{\forall a} \Gamma$ *si et seulement si pour toute formule* $\phi \in \Gamma$, $\langle \mathcal{S}, \mathcal{V}\rangle \Vdash^{\forall a} \phi$
- $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \Gamma$ *si et seulement si pour toute formule* $\phi \in \Gamma$, $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi$
- $\mathscr{C} \Vdash \Gamma$ *si et seulement si pour toute formule* $\phi \in \Gamma$, $\mathscr{C} \Vdash \phi$.

Les deux dernières notations sont les plus importantes. L'énoncé $\mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \Gamma$ signifie que $\mathcal{S}$ est un système de transition tel qu'en tous nœuds et quelle que soit la valuation considérée, il satisfait ce que "raconte Γ". C'est donc par sa seule forme que ce système de transition vérifie ce que "dit" Γ. Plus généralement $\mathscr{C} \Vdash \Gamma$ énonce le même genre d'affirmation mais pour une classe de systèmes de transition toute entière au lieu d'un seul représentant. En ce sens, la plus grande classe $\mathscr{C}$ qui vérifie $\mathscr{C} \Vdash \Gamma$ octroie une espèce de caractérisation par la seule forme des graphes de ce que "relate" Γ.

Pour aller plus avant :

Au sujet de la caractérisation de classes de systèmes de transition par des formules particulières, nous renvoyons le lecteur au très abordable *"Modal logic for philosophers"* de James W. Garson [Gar06], ainsi qu'aux ouvrages *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03] et *"Modal logic : an introduction"* de Brian F. Chellas [Che80]. Pour une lecture plus avancée : *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02] et *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06].

---

6. Un système de transition est *dense* lorsque pour tous nœuds a, c, si $a \to c$, alors il existe b tel que $a \to b$ et $b \to c$.

6 Conséquences sémantiques

Résumé № 31

- *Une formule* ϕ *est* conséquence sémantique globale *d'un ensemble de formules* Γ*, restreinte à une classe de modèles* $\mathcal{MOD}$ *:*

$$\Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi$$

si pour tout modèle $\langle \mathcal{S}, \mathcal{V} \rangle \in \mathcal{MOD}$,

$$\textit{si } \langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \Gamma, \textit{ alors } \langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi.$$

- *Une formule* ϕ *est* conséquence sémantique locale *d'un ensemble de formules* Γ*, restreinte à une classe de modèles* $\mathcal{MOD}$ *:*

$$\Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi$$

si pour tout modèle $\langle \mathcal{S}, \mathcal{V} \rangle \in \mathcal{MOD}$ *et tout nœud* a,

$$\textit{si } \langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Gamma, \textit{ alors } \langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi.$$

※

La notion de conséquence sémantique est différente en deux points de ce qu'elle est dans le Calcul Propositionnel. Tout d'abord, elle est restreinte à une classe de modèles de Kripke – le plus souvent à une classe de systèmes de transition et par extension à la classe de tous les modèles de Kripke qu'elle génére – au lieu d'être applicable à tous les modèles indistinctement de leurs formes. Ensuite, il se trouve deux acceptions de la notion de conséquence sémantique. La première est globale, la seconde est locale.

Définition 239 (Conséquence sémantique globale) *Soient* I *un ensemble non vide,* ϕ *une formule,* Γ *un ensemble de formules, toutes ces formules ne comportant que des opérateurs modaux indicés par les éléments de* I*, et* $\mathcal{MOD}$ *une classe de modèles, c'est-à-dire de systèmes de transition associés à des valuations.*

$$\phi \textit{ est une } \text{conséquence sémantique globale} \textit{ de } \Gamma \textit{ (noté } \Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi)$$
$$\textit{si et seulement si}$$
$$\textit{pour tout modèle } \langle \mathcal{S}, \mathcal{V} \rangle \in \mathcal{MOD}, \quad \textit{si } \langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \Gamma \textit{ alors } \langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi.$$

La notion de conséquence sémantique globale dit simplement qu'une formule est conséquence d'un ensemble de formules - que l'on pourra regarder comme des hypothèses - si chaque fois que ces hypothèses sont vraies dans un modèle de la classe considérée, alors cette formule est également vraie dans ce modèle.

Cette conséquence sémantique s'appelle globale car elle ne se réfère en rien aux nœuds particuliers. Elle regarde la vérité en sa globalité. En cela, elle est plus grossière que la notion de conséquence sémantique locale que nous définissons maintenant.

Définition 240 (Conséquence sémantique locale) *Soient* I *un ensemble non vide,* ϕ *une formule,* Γ *un ensemble de formules, toutes ne comportant que des opérateurs modaux indicés par les éléments de* I*, et* $\mathcal{MOD}$ *une classe de modèles.*

ϕ *est une* conséquence sémantique locale *de* Γ *(noté* $\Gamma \Vdash_{\mathcal{MOD}} \phi$*)*
si et seulement si
pour tout modèle $\langle \mathcal{S}, \mathcal{V} \rangle \in \mathcal{MOD}$*, et tout nœud* $a \in N$ *:* si $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Gamma$ *alors* $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi$.

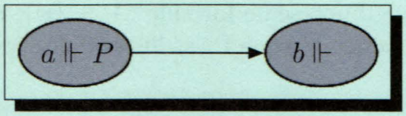
La conséquence sémantique locale est plus forte que la conséquence sémantique globale au sens où, pour une classe de modèles $\mathcal{MOD}$, si $\Gamma \Vdash_{\mathcal{MOD}} \phi$ alors $\Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi$. L'inverse est généralement faux comme le montre l'exemple suivant.

Exemple 241 Pour $\mathcal{MOD}$ la classe de tous les modèles, $\Gamma = \{P\}$ et $\phi = \Box P$, on a

$$\Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi.$$

En effet, considérons un modèle quelconque $\langle \mathcal{S}, \mathcal{V} \rangle$ qui vérifie $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \Gamma$. Autrement dit, $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash P$ est vrai de tout nœud a. En particulier, pour tout nœud b tel que $a \to b$, la relation $\langle \mathcal{S}, \mathcal{V}, b \rangle \Vdash P$ est vérifiée, d'où tout nœud a vérifie $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Box P$.

Par contre, $\Gamma \Vdash_{\mathcal{MOD}} \phi$ est trivialement faux puisque dans le modèle suivant on a $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash P$ et $\langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash \Box P$.



Il y a pourtant un lien simple entre ces deux notions de conséquence sémantique. Pour l'établir, nous avons besoin de la notation suivante.

Notation 242 *Soit* ϕ *une formule et* $n \in \mathbb{N}$*, on écrit :*

- $\Box^n \phi$ *pour*
  - ϕ *si* $n = 0$
  - $\underbrace{\Box \ldots \Box\Box}_{n} \phi$ *si* $n > 0$
- $\Diamond^n \phi$ *pour*
  - ϕ *si* $n = 0$
  - $\underbrace{\Diamond \ldots \Diamond\Diamond}_{n} \phi$ *si* $n > 0$.

Proposition 243 *Soient* ϕ *une formule,* Γ *un ensemble de formules et* $\mathcal{MOD}$ *la classe de tous les modèles,*

$$\Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi \text{ si et seulement si } \{\Box^n \psi \mid n \in \mathbb{N},\ \psi \in \Gamma\} \Vdash_{\mathcal{MOD}} \phi.$$

Preuve de la Proposition 243 :

($\Longleftarrow$) Soient $\mathcal{S} = (N, A)$ un système de transition et $\mathcal{V}$ une valuation qui vérifient $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \Gamma$. Montrons alors que $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi$. Soit a un nœud quelconque. Puisque a est quelconque et que $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Gamma$, il s'en suit que tout nœud b de N vérifie $\langle \mathcal{S}, \mathcal{V}, b \rangle \Vdash \Gamma$. En particulier, cela vaut pour tous les nœuds b qui sont atteignables en empruntant un nombre fini d'arêtes. En conséquence $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \{\Box^n \psi \mid n \in \mathbb{N},\ \psi \in \Gamma\}$. Et ceci vaut également pour tout nœud a du modèle $\langle \mathcal{S}, \mathcal{V} \rangle$. Dès lors, en appliquant l'hypothèse, on obtient $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi$, ce qui démontre le résultat souhaité.

($\Longrightarrow$) Procédons par la contraposée. Montrons que si $\{\Box^n\psi \mid n \in \mathbb{N},\ \psi \in \Gamma\} \not\Vdash_{\mathcal{MOD}} \phi$, alors $\Gamma \not\Vdash^{\forall a}_{\mathcal{MOD}} \phi$. Soient donc $\mathcal{S} = (N, A)$ un système de transition, $\mathcal{V}$ une valuation et $a \in N$ un nœud, tels que $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \{\Box^n\psi \mid n \in \mathbb{N},\ \psi \in \Gamma\}$ alors que $\langle \mathcal{S}, \mathcal{V}, a\rangle \not\Vdash \phi$. Formons le système de transition $\mathcal{T}$ induit par $\mathcal{S}$ au nœud a défini de la manière suivante : $\mathcal{T} = (N', A')$, où N' est l'ensemble des nœuds que l'on peut atteindre depuis a en empruntant un nombre fini d'arêtes de A, et A' les arêtes induites. Précisément :

$$N' = \{b \in N \mid \text{ il existe } n \in \mathbb{N}, \text{ il existe } a_0, a_1, \ldots, a_n \in N \quad a = a_0 \to a_1 \ldots \to a_n = b\}$$

et A' défini comme l'ensemble des arêtes de A qui relient deux nœuds de N'. Ce système de transition $\mathcal{T}$ muni de la valuation $\mathcal{V}'$ définie pour tout $b \in N'$ par $b \in \mathcal{V}'(P)$ si et seulement si $b \in \mathcal{V}(P)$, est un modèle $\langle \mathcal{T}, \mathcal{V}'\rangle$ qui vérifie par construction $\langle \mathcal{T}, \mathcal{V}'\rangle \Vdash^{\forall a} \psi$ pour chaque formule ψ de Γ. Cela entraîne donc $\langle \mathcal{T}, \mathcal{V}'\rangle \Vdash^{\forall a} \Gamma$. Pourtant le nœud a vérifie $\langle \mathcal{T}, \mathcal{V}', a\rangle \not\Vdash \phi$, ce qui contredit $\Gamma \Vdash^{\forall a}_{\mathcal{MOD}} \phi$.

$\dashv$ 243

Remarque 244

(1) Si Γ n'est composé que d'une seule formule : $\Gamma = \{\psi\}$, on écrira $\psi \Vdash^{\forall a}_{\mathcal{MOD}} \phi$ au lieu de $\{\psi\} \Vdash^{\forall a}_{\mathcal{MOD}} \phi$. De même, lorsque Γ est l'ensemble vide, on écrira $\Vdash^{\forall a}_{\mathcal{MOD}} \phi$ au lieu de $\emptyset \Vdash^{\forall a}_{\mathcal{MOD}} \phi$.

(2) Si $\mathcal{MOD}$ désigne la classe de tous les mdoèles, ϕ et ψ sont deux formules telles que $\psi \Vdash^{\forall a}_{\mathcal{MOD}} \phi$, alors tout modèle dans lequel ψ est vraie est également un modèle dans lequel ϕ est vraie. Autrement dit, si $\mathcal{MOD}_\psi$ et $\mathcal{MOD}_\phi$ désignent respectivement tous les modèles dans lesquels ψ est vraie et tous ceux dans lesquels ϕ est vraie, alors $\psi \Vdash^{\forall a}_{\mathcal{MOD}} \phi$ est équivalent à l'inclusion $\mathcal{MOD}_\psi \subseteq \mathcal{MOD}_\phi$. En conséquence, si à la fois $\psi \Vdash^{\forall a}_{\mathcal{MOD}} \phi$ et $\phi \Vdash^{\forall a}_{\mathcal{MOD}} \psi$ sont toutes deux vérifées, alors $\mathcal{MOD}_\psi = \mathcal{MOD}_\phi$.

Deux questions apparaissent dès lors :

(1) Quelles sont les formules qui sont vraies dans tous les modèles ?

(2) Comment caractériser deux modèles qui se comportent de la même manière vis à vis de la logique modale ?

Nous répondrons à la première de ces questions un peu plus tard. Pour l'instant, nous allons nous intéresser à la seconde en clarifiant tout d'abord ce que nous entendons par le fait que deux modèles *se comportent de la même manière*. Nous voulons dire qu'ils sont indiscernables par la logique modale. Cela signifie qu'il n'est pas possible de trouver une formule qui soit vraie dans l'un et fausse dans l'autre. Il n'est pas possible de les distinguer à l'aide d'une formule. Autrement dit, ils vérifient tous les deux exactement les mêmes formules.

7 Modèles : théories et équivalence

Résumé № 32

- *La théorie d'un modèle de Kripke $\mathcal{M}$ est l'ensemble de toutes les formules vraies dans ce modèle :*

$$Th_{\mathcal{M}} = \{\phi \mid \langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi\}.$$

- *Deux modèles $\mathcal{M}$ et $\mathcal{N}$ sont équivalents ($\mathcal{M} \equiv \mathcal{N}$) s'ils ont la même théorie :*

$$Th_{\mathcal{M}} = Th_{\mathcal{N}}.$$

※

La théorie d'un modèle désigne ce que "raconte" un modèle. Elle comporte deux déclinaisons suivant qu'on la regarde globalement ou localement.

Définition 245 (Théorie d'un modèle) *Soit $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ un modèle de la logique modale dont les arêtes du système de transition sont étiquetées par I.*

On appelle théorie du modèle $\langle \mathcal{S}, \mathcal{V} \rangle$ l'ensemble de toutes les formules dont les opérateurs modaux sont indicés par des éléments de I qui sont vraies dans ce modèle :

$$Th_{\mathcal{M}} = \{\phi \mid \langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi\}.$$

La théorie d'un modèle est donc composée de toutes les formules qui décrivent ce modèle. Deux modèles sont distinguables par la logique modale s'ils n'ont pas la même théorie. Et deux modèles qui possèdent la même théorie racontent exactement la même chose, même s'ils sont différents par ailleurs. Car leur différence, si elle existe, n'est pas du ressort de la logique modale.

Définition 246 (Théorie locale d'un modèle) *Soit $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ un modèle de la logique modale dont les arêtes du système de transition sont étiquetées par I et a un nœud de N.*

On appelle théorie locale du modèle $\langle \mathcal{S}, \mathcal{V} \rangle$ au nœud a l'ensemble de toutes les formules dont les opérateurs modaux sont indicés par des éléments de I qui sont vraies dans ce modèle :

$$Th_{(\mathcal{M},a)} = \{\phi \mid \langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi\}.$$

Cette notion de théorie locale renvoie simplement à la notion de satisfaction en un nœud particulier.

Définition 247 (Modèles équivalents) *Soient I un ensemble non vide $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$, $\mathcal{N} = \langle \mathcal{T}, \mathcal{W} \rangle$ deux modèles de la logique modale dont les arêtes des systèmes de transition $\mathcal{S} = (N, A)$ et $\mathcal{T} = (M, B)$ sont toutes les deux étiquetées par I ; $a \in N$ et $b \in M$ deux nœuds.*

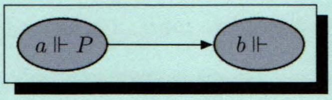
(1) $\mathcal{M}$ et $\mathcal{N}$ sont équivalents *s'ils ont la même théorie :*

$$\mathcal{M} \equiv \mathcal{N} \text{ si et seulement si } Th_{\mathcal{M}} = Th_{\mathcal{N}}.$$

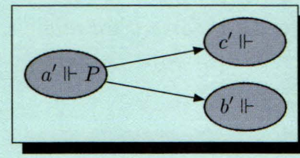
(2) $(\mathcal{M}, a)$ et $(\mathcal{N}, b)$ sont localement équivalents *s'ils partagent la même théorie locale :*

$$(\mathcal{M}, a) \equiv (\mathcal{N}, b) \text{ si et seulement si } Th_{(\mathcal{M},a)} = Th_{(\mathcal{N},b)}.$$

Exemple 248 Les deux modèles suivants sont équivalents ($\mathcal{M} \equiv \mathcal{N}$)



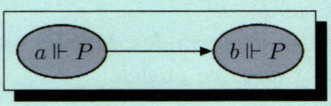
Le modèle $\mathcal{M}$.



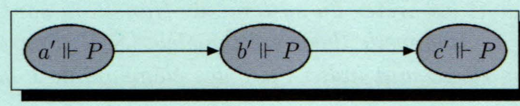
Le modèle $\mathcal{N}$.

Par ailleurs, $(\mathcal{M}, a) \equiv (\mathcal{N}, a')$, $(\mathcal{M}, b) \equiv (\mathcal{N}, b')$, $(\mathcal{M}, b) \equiv (\mathcal{N}, c')$. Nous verrons plus tard comment, à l'aide d'un jeu, reconnaître que ces modèles sont localement équivalents.

Exemple 249 Les deux modèles suivants ne sont pas équivalents :



Le modèle $\mathcal{M}$.



Le modèle $\mathcal{N}$.

La formule $\Box\Box\neg P$ est vraie dans $\mathcal{M}$ car pour chacun des deux nœuds a et b. Le **F**alsificateur perd l'unique partie du jeu d'évaluation de la formule $\Box\Box\neg P$ en ce nœud, tout simplement parce que le **F**alsificateur ne peut effectuer les deux déplacements requis par les deux symboles " $\Box\Box$". Alors que dans le modèle $\mathcal{N}$, cette formule est fausse puisque $a \nVdash \Box\Box\neg P$ (le **F**alsificateur avance nécessairement jusqu'en c' où il l'emporte puisque $c' \Vdash P$. Par contre, les relations équivalences suivantes sont vérifiées :

$$(\mathcal{M}, a) \equiv (\mathcal{N}, b') \text{ et } (\mathcal{M}, b) \equiv (\mathcal{N}, c').$$

8 Bisimulation

***Résumé* № 33** *Etant donnés deux mondes a et b provenant de deux modèles $\mathcal{M}$ et $\mathcal{N}$, on définit le jeu – à deux joueurs mais dont la longueur peut être infinie – de bisimulation* $\mathbb{B}\mathrm{is}((\mathcal{M},a),(\mathcal{N},b))$*, de manière à ce que le joueur* Duplicateur *ait une stratégie gagnante dans ce jeu si et seulement si* $(\mathcal{M},a) \equiv (\mathcal{N},b)$. ※

Imaginons deux modèles de Kripke $\mathcal{M}$ et $\mathcal{N}$, et pour chaque modèle, un nœud particulier m pour $\mathcal{M}$ et n pour $\mathcal{N}$. Imaginons finalement deux personnes qui vivent l'une au monde possible m de $\mathcal{M}$ et l'autre qui réside au monde n de $\mathcal{N}$. Bien que ces deux personnes n'habitent pas du tout au même endroit, il est fort possible qu'elles ne puissent pourtant le distinguer tant qu'elle n'en reste qu'au niveau de la logique modale. Il se peut en effet que depuis le monde m, tout paraisse exactement identique à ce que l'on perçoit depuis le monde n. Pour le dire autrement, il se peut que m et n soient comme deux univers parallèles dont les nuances sont impénétrables pour les personnes qui vivent en ces mondes. Bien sûr, pour quelqu'un qui est à l'extérieur de ces systèmes, il est évident qu'il y a là deux modèles de Kripke qui peuvent également être radicalement différents [7], mais pour celui qui réside à l'intérieur d'un modèle de Kripke, rien d'autre que ce seul modèle existe. Cette notion, qui permet de dire que deux mondes sont tellement semblables qu'on ne peut pas les différencier sans pour autant qu'ils soient identiques, s'appelle *l'indiscernabilité*. Deux mondes sont indiscernables s'il n'existe pas de formule qui soit vraie dans l'un et fausse dans l'autre. Ils satisfont les même formules – de la logique modale – il n'est donc pas possible de les distinguer, bien qu'ils soient pourtant différents.

Nous allons proposer un jeu à deux joueurs et information parfaite – appelé jeu de *bisimulation* – qui est défini en sorte que le joueur appelé *Duplicateur* possède une statégie gagnante si et seulement si les deux mondes – associés à leurs modèles respectifs – qui interviennent dans le jeu sont *bisimilaires*. Or, précisément, ce que caractérise la notion de bisimilarité est le fait d'être indiscernables. Au lieu de devoir en passer par toutes les formules possibles de la logique modale afin de déterminer si deux mondes sont ou non indiscernables, nous allons disposer d'un moyen beaucoup plus pratique : le jeu de bisimulation, qui se révèlera être une aubaine pour le discernement.

Définition 250 *Soient I un ensemble non vide, $\mathcal{M} = \langle \mathcal{S},\mathcal{V}\rangle$, $\mathcal{N} = \langle \mathcal{T},\mathcal{W}\rangle$ deux modèles de la logique modale dont les arêtes des systèmes de transition $\mathcal{S} = (N,A)$ et $\mathcal{T} = (M,B)$ sont toutes les deux étiquetées par I ; $a \in N$ et $b \in M$ deux nœuds.*

Le jeu de bisimulation $\mathbb{B}\mathrm{is}((\mathcal{M},a),(\mathcal{N},b))$ *est défini comme suit :*

(1) il comprend deux joueurs appelés Duplicateur *et* Corrupteur. *Le* Duplicateur *(*$\mathbf{D}_{up}$*) cherche à montrer que les deux modèles sont localement bisimilaires, alors que le* Corrupteur *(*$\mathbf{C}_{or}$*) au contraire cherche à montrer qu'ils ne le sont pas.*

Les coups de ces deux joueurs consistent à choisir des nœuds dans les systèmes de transition. Les nœuds de départ étant a dans $\mathcal{S}$ et b dans $\mathcal{T}$.

7. L'un peut être fini alors que l'autre est infini, par exemple.

(2) A chaque tour, lorsque les positions sont a' et b' des nœuds respectivement de N et M :

- $\mathbf{C}_{or}$ *choisit d'abord de jouer dans $\mathcal{S}$ ou dans $\mathcal{T}$.*

  (a) Si $\mathbf{C}_{or}$ choisit de jouer dans $\mathcal{S}$, il produit $i \in I$ et $a'' \in N$ tel que $a' \xrightarrow{i} a''$, et $\mathbf{D}_{up}$ répond en produisant $b'' \in M$ tel qu'à la fois $b' \xrightarrow{i} b''$ et pour toute variable propositionnelle P :

  $$\langle \mathcal{S}, \mathcal{V}, a'' \rangle \Vdash P \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b'' \rangle \Vdash P.$$

  (b) Si $\mathbf{C}_{or}$ choisit de jouer dans $\mathcal{T}$, il produit $i \in I$ et $b'' \in M$ tel que $b' \xrightarrow{i} b''$, et $\mathbf{D}_{up}$ répond en produisant $a'' \in N$ tel que à la fois $a' \xrightarrow{i} a''$ et pour toute variable propositionnelle P :

  $$\langle \mathcal{S}, \mathcal{V}, a'' \rangle \Vdash P \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b'' \rangle \Vdash P.$$

(3) (a) S'il existe une variable propositionnelle P telle que la position initiale vérifie

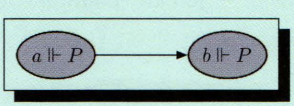
$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash P \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \nVdash P,$$

alors $\mathbf{C}_{or}$ l'emporte.

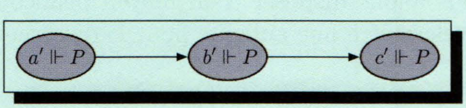
(b) Si un joueur ne peut plus avancer alors ce joueur perd la partie.

(c) Si la partie est infinie, alors $\mathbf{D}_{up}$ l'emporte.

Exemple 251 Etant donnés les modèles de Kripke $\mathcal{M}$ et $\mathcal{N}$ ci-dessous, une partie dans le jeu de bisimulation $\mathbb{Bis}((\mathcal{M}, a), (\mathcal{N}, a'))$ peut se présenter sous la forme suivante :



Le modèle $\mathcal{M}$.



Le modèle $\mathcal{N}$.

Le corrupteur ($\mathbf{C}_{or}$) possède une stratégie gagnante :

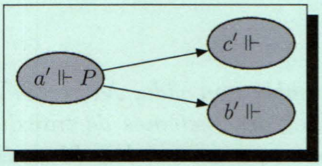
(1) $\mathbf{C}_{or}$ choisit de jouer dans $\mathcal{N}$ et produit b'.

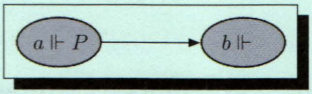
(2) $\mathbf{D}_{up}$ n'a pas d'autre option que de choisir b.

(3) $\mathbf{C}_{or}$ choisit à nouveau de jouer dans $\mathcal{N}$ et produit c' mais,

(4) $\mathbf{D}_{up}$ perd car il ne peut plus avancer.

Exemple 252 Dans le jeu de bisimulation $\mathbb{B}\mathrm{is}((\mathcal{M}, a'), (\mathcal{N}, a))$





Le modèle $\mathcal{N}$.

Le modèle $\mathcal{M}$.

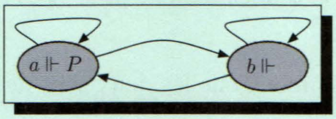
$\mathbf{D}_{up}$ possède une stratégie gagnante qui consiste :

(1) si $\mathbf{C}_{or}$ choisit b', ou c', à choisir b ;

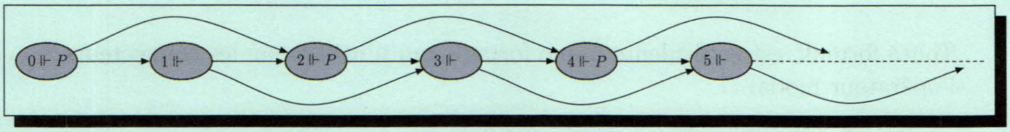
(2) si $\mathbf{C}_{or}$ choisit b, à choisir par exemple b' ;

De la sorte, le corrupteur ne peut jouer son deuxième coup et perd la partie.

Exemple 253 Soit le jeu de bisimulation $\mathbb{B}\mathrm{is}((\mathcal{M}, a), (\mathcal{N}, 0))$



Le modèle $\mathcal{M}$.



Le modèle $\mathcal{N}$.

Le modèle $\mathcal{N}$ est défini par :

- l'ensemble des nœuds est $\mathbb{N}$,
- pour tout $n \in \mathbb{N}$ deux arêtes : $n \to n+1$ et $n \to n+2$,
- $2n \Vdash P$ et $2n+1 \nVdash P$.

$\mathbf{D}_{up}$ possède une stratégie gagnante qui consiste à tout moment de la partie :

(1) si $\mathbf{C}_{or}$ joue dans $\mathcal{N}$ et choisit n, à choisir a si n est pair et b sinon.

(2) si $\mathbf{C}_{or}$ joue dans $\mathcal{M}$ et choisit a, à choisir à partir de la position n dans $\mathcal{N}$
   - $n+1$ si n est impair,
   - $n+2$ si n est pair.

(3) si $\mathbf{C}_{or}$ joue dans $\mathcal{M}$ et choisit b, à choisir à partir de la position n dans $\mathcal{N}$
   - $n+2$ si n est impair,
   - $n+1$ si n est pair.

De la sorte, le jeu continue indéfiniment, entraînant la défaite du corrupteur.

Définition 254 *Soit $\mathcal{S} = (N, A)$ un système de transition étiqueté par un ensemble non vide I, $\mathcal{S}$ est à* branchement fini, *si pour tout élément $i \in I$, pour tout nœud $a \in N$, $\{b \in N \mid a \xrightarrow{i} b\}$ est fini.*

Théorème 255 (Henessy-Millner) *Soient I un ensemble non vide, $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$, $\mathcal{N} = \langle \mathcal{T}, \mathcal{W} \rangle$ deux modèles de la logique modale dont les arêtes des systèmes de transition $\mathcal{S} = (N, A)$ et $\mathcal{T} = (M, B)$ sont toutes les deux étiquetées par I ; $a \in N$ et $b \in M$ deux nœuds. On suppose en outre que $\mathcal{S}$ et $\mathcal{T}$ sont à branchement fini.*

$(\mathcal{M}, a) \equiv (\mathcal{N}, b)$ *si et seulement si* $\mathbf{D}_{up}$ *a une stratégie gagnante dans* $\mathbb{B}\mathtt{is}\left((\mathcal{M}, a), (\mathcal{N}, b)\right)$.

Nous rappelons que deux modèles sont localement équivalents – noté $(\mathcal{M}, a) \equiv (\mathcal{N}, b)$ – s'ils ont la même théorie locale :

$$\mathtt{Th}_{(\mathcal{M},a)} = \{\phi \mid \langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi\} = \{\phi \mid \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \phi\} = \mathtt{Th}_{(\mathcal{N},b)}.$$

Autrement dit, ces deux modèles sont localement équivalents si, pour toute formule ϕ,

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \phi.$$

Preuve du Théorème 255 : Nous montrons les deux sens de la double implication :

($\Longleftarrow$) On montre, par induction sur sa hauteur, que pour toute formule ϕ,

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \phi.$$

Toute formule est équivalente à une formule qui n'utilise que les connecteurs $\neg, \wedge$ et l'opérateur modal $\Box$:

- $\phi_0 \vee \phi_1$ est équivalente à $\neg(\neg\phi_0 \wedge \neg\phi_1)$
- $\phi_0 \longrightarrow \phi_1$ est équivalente à $\neg(\phi_0 \wedge \neg\phi_1)$
- $\phi_0 \longleftrightarrow \phi_1$ est équivalente à $\neg(\neg\phi_0 \wedge \neg\phi_1) \wedge \neg(\neg\phi_1 \wedge \neg\phi_0)$
- $\langle i \rangle\varphi$ est équivalente à $\neg[i]\neg\varphi$.

Nous pourrons donc supposer que ϕ ne comporte que les connecteurs $\neg, \wedge$ et l'opérateur modal $[i]$.

(1) Si la hauteur de ϕ est nulle, alors il est clair que :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \top \text{ et } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \top, \text{ et par ailleurs } \langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash \bot \text{ et } \langle \mathcal{T}, \mathcal{W}, b \rangle \nVdash \bot.$$

Lorsque ϕ est une variable propositionnelle P, la définition même des conditions du jeu, associée au fait que $\mathbf{D}_{up}$ a une stratégie gagnante dans $\mathbb{B}\mathtt{is}\left((\mathcal{M}, a), (\mathcal{N}, b)\right)$, vérifie

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash P \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash P.$$

(2) Soit ϕ de hauteur $n + 1$, trois cas apparaissent :

(a) $\phi = \phi_0 \vee \phi_1$: la hauteur de ϕ_0 et celle de ϕ_1 sont toutes deux inférieures à $n + 1$. L'hypothèse d'induction s'applique donc à elles deux. Alors, puisque $\mathbf{D}_{up}$ a une stratégie gagnante dans $\mathbb{B}\mathrm{is}((\mathcal{M}, a), (\mathcal{N}, b))$ nous avons à la fois :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi_0 \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \phi_0$$

et

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi_1 \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \phi_1.$$

D'où l'on déduit que :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \phi_0 \vee \phi_1 \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \phi_0 \vee \phi_1.$$

(b) $\phi = \neg\varphi$: la hauteur de φ est n, par conséquent l'hypothèse d'induction s'applique à φ. Ainsi, puisque $\mathbf{D}_{up}$ a une stratégie gagnante dans $\mathbb{B}\mathrm{is}((\mathcal{M}, a), (\mathcal{N}, b))$ nous avons :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \varphi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \varphi$$

qui donne immédiatement :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \neg\varphi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash \neg\varphi.$$

(c) $\phi = [i]\varphi$. la hauteur de φ est n, par conséquent l'hypothèse d'induction s'applique à φ. Remarquons préalablement que :

(A) soit a et b ont tous les deux au moins un successeur le long d'une flèche étiquetée i (il existe a' et b' tels que $a \xrightarrow{i} a'$ et $b \xrightarrow{i} b'$).

(B) soit a et b n'ont pas de successeurs par i (il n'existe ni a', ni b' tels que $a \xrightarrow{i} a'$ et $b \xrightarrow{i} b'$). Dans ce cas, on note que $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash [i]\varphi$ et $\langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash [i]\varphi$ sont trivialement vérifiés tous les deux et donc également :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash [i]\varphi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash [i]\varphi.$$

(C) Le cas où a aurait un successeur a' tel que $a \xrightarrow{i} a'$, mais qu'il n'existerait pas de b' tel que $b \xrightarrow{i} b'$ est impossible puisque si $\mathbf{C}_{or}$ choisit précisément ce nœud a', $\mathbf{D}_{up}$ est incapable de répondre et perd la partie, ce qui contredit le fait qu'il possède une stratégie gagnante.

(D) Le cas où b aurait un successeur b' tel que $b \xrightarrow{i} b'$, mais qu'il n'existerait pas de a' tel que $a \xrightarrow{i} a'$ est identique au précédent *mutatis mutandis*.

Il ressort de cette étude préalable que nous n'avons qu'à considérer le cas (2)((c))(A). Deux sous-cas apparaissent :

(i) si $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash [i]\varphi$, alors pour tout nœud a' tel que $a \xrightarrow{i} a'$, $\langle \mathcal{S}, \mathcal{V}, a' \rangle \Vdash \varphi$. Soit un nœud b' quelconque tel que $b \xrightarrow{i} b'$. Considérons la partie du jeu $\mathbb{B}\mathrm{is}((\mathcal{M}, a), (\mathcal{N}, b))$ dans laquelle le premier coup de $\mathbf{C}_{or}$ choisit précisément ce nœud b' et $\mathbf{D}_{up}$ répond en appliquant sa stratégie gagnante et choisit a'. Dans le jeu $\mathbb{B}\mathrm{is}((\mathcal{M}, a'), (\mathcal{N}, b'))$, $\mathbf{D}_{up}$ possède toujours une stratégie gagnante, par conséquent, par application de l'hypothèse d'induction, nous obtenons :

$$\langle \mathcal{S}, \mathcal{V}, a' \rangle \Vdash \varphi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b' \rangle \Vdash \varphi$$

Ce qui montre que $\langle \mathcal{T}, \mathcal{W}, b' \rangle \Vdash \varphi$. Comme b' était quelconque, nous obtenons :

$$\langle \mathcal{T}, \mathcal{W}, b \rangle \Vdash [i]\varphi.$$

(ii) $\langle \mathcal{S}, \mathcal{V}, a \rangle \nVdash [i]\varphi$, alors il existe un nœud a' tel que $a \xrightarrow{i} a'$ et $\langle \mathcal{S}, \mathcal{V}, a' \rangle \nVdash \varphi$. Considérons la partie du jeu $\mathbb{B}\mathbb{i}\mathbb{s}\,((\mathcal{M}, a), (\mathcal{N}, b))$ dans laquelle $\mathbf{C}_{or}$ choisit précisément ce nœud a' au premier coup. $\mathbf{D}_{up}$ répond en appliquant sa stratégie gagnante et choisit un nœud b' tel que $b \xrightarrow{i} b'$. Comme dans le jeu $\mathbb{B}\mathbb{i}\mathbb{s}\,((\mathcal{M}, a'), (\mathcal{N}, b'))$, $\mathbf{D}_{up}$ possède toujours une stratégie gagnante, il nous suffit d'appliquer l'hypothèse d'induction pour obtenir :

$$\langle \mathcal{S}, \mathcal{V}, a' \rangle \Vdash \varphi \text{ si et seulement si } \langle \mathcal{T}, \mathcal{W}, b' \rangle \Vdash \varphi$$

Ce qui montre que $\langle \mathcal{T}, \mathcal{W}, b' \rangle \nVdash \varphi$. Par conséquent :

$$\langle \mathcal{T}, \mathcal{W}, b \rangle \nVdash [i]\varphi.$$

Remarquons que l'hypothèse sur le caractère fini du branchement des systèmes de transition n'a pas été utilisée pour démontrer ce sens de la double implication.

($\Longrightarrow$) Il suffit de montrer que si deux nœuds a et b quelconques vérifient $(\mathcal{M}, a) \equiv (\mathcal{N}, b)$, alors :

(1) cette position initiale du jeu $\mathbb{B}\mathbb{i}\mathbb{s}\,((\mathcal{M}, a), (\mathcal{N}, b))$ n'est pas immédiatement perdue pour $\mathbf{D}_{up}$ et

(2) quelque soit le coup initial $a' \in N$ de $\mathbf{C}_{or}$, $\mathbf{D}_{up}$ peut répondre par $b' \in M$ tel que $(\mathcal{M}, a') \equiv (\mathcal{N}, b')$.

(3) Et symétriquement si $\mathbf{C}_{or}$ choisit $b' \in M$, $\mathbf{D}_{up}$ peut répondre par $a' \in N$ tel que $(\mathcal{M}, a') \equiv (\mathcal{N}, b')$.

En montrant cela, on construit une stratégie pour $\mathbf{D}_{up}$ dans le jeu $\mathbb{B}\mathbb{i}\mathbb{s}\,((\mathcal{M}, a), (\mathcal{N}, b))$ qui n'atteint toujours que des positions engendrant des modèles locaux équivalents, donc en particulier vérifiant les mêmes variables propositionnelles. Ainsi, soit le jeu s'arrête parce que $\mathbf{C}_{or}$ ne peut plus avancer, soit il continue indéfiniment. Dans les deux cas, $\mathbf{D}_{up}$ l'emporte. Cette stratégie est alors une stratégie gagnante pour $\mathbf{D}_{up}$ dans $\mathbb{B}\mathbb{i}\mathbb{s}\,((\mathcal{M}, a), (\mathcal{N}, b))$.

Nous montrons donc que :

(1) la position initiale du jeu $\mathbb{B}\mathbb{i}\mathbb{s}\,((\mathcal{M}, a), (\mathcal{N}, b))$ n'est pas immédiatement perdue pour $\mathbf{D}_{up}$. Cela est faux si $\mathbf{C}_{or}$ peut avancer alors que $\mathbf{D}_{up}$ ne le peut pas. Procédons par l'absurde et supposons que ce soit le cas. Si $\mathbf{C}_{or}$ peut avancer, c'est que pour un certain $i \in I$, il existe soit un successeur de a, soit un successeur de b, mais pas les deux. Par symétrie, supposons qu'il existe a' tel que $a \xrightarrow{i} a'$ mais aucun nœud b' tel que $b \xrightarrow{i} b'$. Dans ce cas-là, il suffit de considérer la formule $\langle i \rangle (P \vee \neg P)$ pour obtenir la contradiction suivante :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \langle i \rangle (P \vee \neg P) \text{ mais pourtant } \langle \mathcal{T}, \mathcal{W}, b \rangle \nVdash \langle i \rangle (P \vee \neg P).$$

(2) Montrons également que quelque soit le coup initial $a' \in N$ de $\mathbf{C}_{or}$, $\mathbf{D}_{up}$ peut répondre par $b' \in M$ tel que $(\mathcal{M}, a') \equiv (\mathcal{N}, b')$.

Là encore procédons par l'absurde, et imaginons que $\mathbf{C}_{or}$ choisit a' tel que $a \xrightarrow{i} a'$, et que pour tout b' tel que $b \xrightarrow{i} b'$ nous avons $(\mathcal{M}, a') \not\equiv (\mathcal{N}, b')$. Puisque $\mathcal{N}$ est à branchement fini, il n'existe qu'un nombre fini de nœuds b' tels que $b \xrightarrow{i} b'$: $b'_0, b'_1, \ldots, b'_k$. Pour chaque $j \in \{0, 1, \ldots, k\}$, on choisit une formule ϕ_j telle que :

$$\langle \mathcal{S}, \mathcal{V}, a' \rangle \Vdash \phi_j \text{ et } \langle \mathcal{T}, \mathcal{W}, b'_j \rangle \nVdash \phi_j.$$

Cela est clairement toujours possible puisque $(\mathcal{M}, a') \not\equiv (\mathcal{N}, b'_j)$ implique qu'il existe une formule φ telle que $\langle \mathcal{S}, \mathcal{V}, a' \rangle \Vdash \varphi$ si et seulement si $\langle \mathcal{T}, \mathcal{W}, b' \rangle \nVdash \varphi$. En posant soit $\phi_j = \varphi$, soit $\phi_j = \neg\varphi$ on obtient la formule ϕ_j souhaitée.

Finalement, il suffit de considérer la formule $(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_k)$ et voir que :

$$\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \langle i \rangle(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_k) \text{ alors que } \langle \mathcal{T}, \mathcal{W}, b \rangle \nVdash \langle i \rangle(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_k).$$

ce qui bien sûr contredit l'hypothèse.

(3) Le cas où $\mathbf{C}_{or}$ choisit $b' \in M$, mais $\mathbf{D}_{up}$ ne peut répondre par $a' \in N$ tel que $(\mathcal{M}, a') \equiv (\mathcal{N}, b')$ est bien évidemment symétrique.

$\dashv$ 255

Pour aller plus avant :

La notion de bisimulation est très naturelle, elle remonte à la notion philosophique des *"indiscernables"*, puisqu'elle consiste à se poser la question de la distinction de deux modèles par une formule. Le fait de pouvoir discerner cela au moyen d'un jeu trouve son origine dans les jeux d'Ehrenfeucht-Fraïssé qui permettre de résoudre le même genre de problème, mais pour une logique différente : la logique du 1$^{\text{er}}$ordre. Au début de la seconde moitié du XX$^{\text{ème}}$siècle, Roland Fraïssé avait mis au point une méthode dite de *"va et vient"* permettant de tester si deux structures sont *"élémentairement équivalentes"*, c'est-à-dire indiscernables au moyen de la logique du 1$^{\text{er}}$ordre [Fra50]. Quelques années plus tard, Andrzej Ehrenfeucht a reformulé cette technique au moyen d'un jeu [Ehr61]. C'est ce même jeu qui est considéré ici, mais dans le cadre de la logique modale, dont on verra qu'elle forme en fait une sous-partie de la logique du 1$^{\text{er}}$ordre (dans laquelle elle est interprétable) ; la notion de bisimulation jouant elle-même un rôle clé dans la définition de de cette "sous-partie". Pour plus de détails sur ce sujet, nous renvoyons le lecteur vers les ouvrages *"First steps in modal logic"* de Sally Popkorn [Pop94], *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02] et *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06]. Pour les jeux d'Ehrenfeucht-Fraïssé nous recommandons tout particulièrement l'excellent *"Elements of finite model theory"* de Leonid Libkin [Lib04].

Chapitre 6

Systèmes logiques

1 Logiques de classes

***Résumé* № 34** *La logique d'une classe de systèmes de transition $\mathscr{C}$ est*

$$Log_{\mathscr{C}} = \{\phi \mid \textit{pour tout } \mathcal{S} \in \mathscr{C}, \;\; \mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi\}.$$

※

Dès lors que nous avons défini les systèmes de transition comme sémantique adéquate pour notre syntaxe, la première question qui vient à l'esprit est celle de déterminer quelles sont toutes les formules qui sont valides pour la classe de tous les systèmes de transition. Plus précisément, en Calcul Propositionnel, les formules qui sont vraies dans tous les modèles sont appelées tautologies et sont par ailleurs obtenues grâce à l'application de règles de déduction à des axiomes, que ce soit dans le cadre de systèmes de déduction à la Hilbert, ou dans celui de la Déduction Naturelle ou encore dans celui du Calcul des Séquents. La question que nous posons dans le cadre de la logique modale est la même. Quelles sont ces formules qui sont valides partout, en tout nœud, d'un système de transition quelconque pour une valuation quelconque ?

Cela signifie que nous considérons la classe $\mathscr{C}$ de tous les systèmes de transition et nous aimerions savoir quelles sont les formules ϕ, telles que quel que soit le système de transition $\mathcal{S}$ muni d'une valuation quelconque $\mathcal{V}$ et en un nœud quelconque a, vérifient $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi$.

Un premier début de réponse consiste à dire que ce sont au moins toutes les formules qui sont des tautologies du Calcul Propositionnel. C'est-à-dire que toute formule de profondeur modale nulle qui est une tautologie du Calcul Propositionnel sera nécessairement forcée dans tout nœud de n'importe quel modèle, peu importe quels sont les successeurs de ce nœud, puisque l'absence d'opérateur de modalité limite la satisfaction ou non de cette formule en un nœud à ce seul nœud. Mais sont-ce là toutes les formules qui sont valides en tout système de transition ? Loin s'en faut ! Car nous avons de nombreuses formules de logique modale qui ne sont pas des formules du Calcul Propositionnel mais pourtant forcées en tout nœud de tout modèle. Par exemple, la formule $\Box(P \vee \neg P)$ est clairement forcée en tout nœud puisque la formule $P \vee \neg P$ est une tautologie du Calcul Propositionnel, qui est donc elle-même forcée en tout nœud.

Avant d'étudier cela plus en détail nous commençons par une définition :

Définition 256 *Soit $\mathscr{C}$ une classe de systèmes de transition. On appelle logique de la classe $\mathscr{C}$, la classe de toutes les formules qui sont valides dans tous les systèmes de transition de $\mathscr{C}$:*

$$\mathtt{Log}_{\mathscr{C}} = \{\phi \mid \textit{pour tout } \mathcal{S} \in \mathscr{C},\ \ \mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi\}.$$

Notre question devient : quelle est la logique de la classe de tous les systèmes de transition ? Comme nous l'avons rapidement vu, cette logique doit contenir toutes les formules du Calcul Propositionnel qui sont des tautologies (comme par exemple $P \longleftrightarrow P$, ou $P \vee \neg P$). Par ailleurs, si elle contient une formule quelconque ϕ, elle devra contenir aussi toutes les substitutions uniformes $\phi[\psi/P]$ d'une *variable de cette formule* par une formule quelconque ψ – par exemple $\psi \longleftrightarrow \psi$ ou $\psi \vee \neg\psi$. Attention, nous ne parlons pas de n'importe quelle forme de substitution, mais uniquement des substitutions uniformes, c'est-à-dire de celles qui substituent une formule à toutes les occurrences d'une variable et non pas des substitutions qui porteraient sur certaines seulement des occurrences d'une variable, ou pire encore, celles qui substitueraient une fomule à une sous-formule quelconque au lieu d'une simple variable.

Là encore, la raison de la présence dans cette logique de toutes les substitutions uniformes opérées sur des variables est naturelle. Si une formule ϕ est valide dans un système de transition donné $\mathcal{S}$, alors elle est vraie dans tout modèle $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ issu de ce système de transition. La satisfaction de ϕ en un nœud donné a est donc indépendante de la valuation $\mathcal{V}$. Donc, que P soit vraie ou fausse, la formule ϕ est forcée au nœud a. Par conséquent, que ψ soit vraie ou fausse, la satisfaction de la formule $\phi[\psi/P]$ ne varie pas.

Une autre chose à considérer est ce qu'on appelle la *généralisation* d'une formule, ou encore sa *nécessitation*. Si la formule ϕ est vraie dans un modèle, elle est forcée en tout nœud de ce modèle. Par conséquent la formule $\Box\phi$ est elle aussi forcée en tout nœud. En effet, pour que $\Box\phi$ ne soit pas forcé en un nœud, il faudrait qu'il existe un successeur de ce nœud qui ne force pas ϕ, ce qui n'est pas le cas.

En dernier lieu, il faut également admettre que la logique de la classe de tous les systèmes de transition soit close par *modus ponens*. Cela signifie que si $\phi \longrightarrow \psi$ et ϕ sont toutes deux des formules valides dans tout système de transition, alors la formule ψ l'est également.

Pour résumer ce que nous venons de dire, la logique de la classe de tous les systèmes de transition contient toutes les tautologies du Calcul Propositionnel, auxquelles il faut encore ajouter la formule permettant de passer de $\Box$ à $\Diamond$: $\Diamond P \longleftrightarrow \neg\Box\neg P$. Cette logique est en plus de cela close par substitution uniforme, close par généralisation et close par *modus ponens*. Pourtant, nous verrons que ce n'est pas tout. Cette logique est encore plus large que cela. La logique de la classe de tous les systèmes de transition contient encore d'autres formules.

Une fois que nous aurons correctement caractérisé cette logique, nous allons l'enrichir étapes par étapes en ajoutant d'autres formules, obtenant ainsi des logiques de plus en plus riches mais qui auront pour effet de réduire la classe des systèmes de transition qu'elles caractériseront. La question devient alors : existe-t-il une classe de systèmes de transition bien définie qui corresponde à chacune de ces extensions de notre logique de la classe de tous les systèmes de transition ?

2 Axiomatique et systèmes de déduction

Résumé № 35

- *Un* axiome *est une formule.*
- *Un* système formel *est un ensemble d'axiomes.*
- *Les formules qui se* déduisent *d'un système formel* **S** *sont celles obtenues à partir des axiomes qui constituent* **S**, *par application des règles suivantes :*

  - modus ponens,
  - *substit. uniforme,*
  - *nécessitation.*

- *On note* $\vdash_{\mathbf{S}} \phi$ *le fait que* ϕ *se déduit de* **S**.
- *On écrit* $\Gamma \vdash_{\mathbf{S}} \phi$ *s'il existe* $\psi_0, \psi_1, \ldots, \psi_n \in \Gamma$ *telles que* $\vdash_{\mathbf{S}} (\psi_0 \wedge \psi_1 \wedge \ldots \wedge \psi_n) \longrightarrow \phi$.

※

Pour mener à bien ce programme, nous avons besoin de définir la manière dont nous allons *enrichir* les différentes logiques que nous rencontrerons. Nous allons le faire sur une base purement syntaxique, et pour cela nous introduisons les notions suivantes.

Définition 257

(1) Un axiome est une formule.

(2) Un système formel est un ensemble d'axiomes.

Pourquoi alors parler de système formel et d'axiome au lieu d'employer simplement les mots d'ensemble de formules et de formule ? C'est que la notion d'axiome fait référence à une formule, mais une formule qui tient un rôle particulier dans une preuve. De même, un système formel représente un ensemble de formules qui forment le cadre de cette preuve.

Ce que nous venons de dire réclame quelques précisions sur ce que nous entendons par *preuve* en logique modale. L'idéal serait d'avoir une notion de preuve du type Déduction Naturelle ou Calcul des Séquents. Malheureusement, le monde de la Logique Modale est moins rose que celui du Calcul Propositionnel. Les systèmes de déduction auxquels nous allons devoir faire appel sont des systèmes de Hilbert. Il existe pourtant, pour certaines logiques particulières, des systèmes de déduction du type que nous souhaiterions, mais ce n'est pas le cas pour la logique modale en générale. Si nous voulions insister fermement sur la partie démonstrative de chacune des ces logiques, nous introduirions très certainement ces différentes versions de Calcul des Séquents, mais notre propos n'est pas de nous attarder sur la théorie de la démonstration de la logique modale. Voila la raison pour laquelle nous nous contentons de système à la Hilbert, gracieux dans leur simplicité mais peu commode d'emploi, tout en renvoyant le lecteur curieux vers le livre *"Gentzen calculi for modal propositional logic"* de Francesca Poggiolesi [Pog10].

Définition 258 *Soient* I *un ensemble non vide,* ϕ *une formule et* **S** *un système formel. Une preuve de la formule* φ *dans le système formel* **S** *est une suite finie de formules* $\langle \varphi_0, \varphi_1, \ldots, \varphi_n \rangle$ *telle que :*

- $\varphi_n = \varphi$

- *chaque* φ_l *vérifie l'une des quatre conditions suivantes :*
  (1) φ_l *est un axiome de* $\mathbf{S}$. *(*$\varphi_l \in \mathbf{S}$*),*

  (2) φ_l *est obtenue à partir de l'application de la règle du* modus ponens *à deux formules d'indices inférieurs* φ_j *et* φ_k $(j, k < l)$. *i.e.* $\varphi_j = (\varphi_k \longrightarrow \varphi_l)$.

  (3) φ_l *est obtenue par* substitution uniforme *d'une variable* P *quelconque par une formule* θ *quelconque dans une formule d'indice inférieur* φ_k $(k < l)$. *i.e.* $\varphi_l = \varphi_k[\theta/P]$.

  (4) φ_l *est obtenue à partir de l'application de la règle dite de généralisation ou de nécessitation appliquée à une formule d'indice inférieur* φ_j $(j < l)$. *i.e.* $\varphi_l = [i]\varphi_j)$, *pour une valeur* $i \in I$ *quelconque.*

Exemple 259 Si $\mathbf{S}$ désigne l'ensemble des tautologies du Calcul Propositionnel, alors la suite

$$\langle P \longrightarrow (P \vee \neg P), \Diamond Q \longrightarrow (\Diamond Q \vee \neg \Diamond Q), \Box(\Diamond Q \longrightarrow (\Diamond Q \vee \neg \Diamond Q)), \Box(\Diamond \phi \longrightarrow (\Diamond \phi \vee \neg \Diamond \phi))\rangle$$

est une preuve de $\Box(\Diamond \phi \longrightarrow (\Diamond \phi \vee \neg \Diamond \phi))$ dans ce système, puisque :

(1) $\varphi_0 = P \longrightarrow (P \vee \neg P)$ est une tautologie du Calcul Propositionnel et donc un axiome du système formel $\mathbf{S}$,

(2) $\varphi_1 = \Diamond Q \longrightarrow (\Diamond Q \vee \neg \Diamond Q)$ est le résultat de la substitution de la formule $\Diamond Q$ à P dans φ_0 : $\Diamond Q \longrightarrow (\Diamond Q \vee \neg \Diamond Q) = P \longrightarrow (P \vee \neg P)[\Diamond Q/P]$,

(3) $\varphi_2 = \Box(\Diamond Q \longrightarrow (\Diamond Q \vee \neg \Diamond Q))$ est obtenue à partir de φ_1 par généralisation,

(4) $\varphi_3 = \Box(\Diamond \phi \longrightarrow (\Diamond \phi \vee \neg \Diamond \phi))$ est obtenue par substitution de la formule ϕ à Q dans φ_2.

Exemple 260

Si $\mathbf{S}$ désigne l'ensemble des tautologies du Calcul Propositionnel auquel on ajoute la formule $P \longrightarrow \Diamond P$, alors la suite

$$\langle \varphi_0, \varphi_1, \varphi_2, \varphi_3, \varphi_4, \varphi_5, \varphi_6, \varphi_7, \varphi_8, \varphi_9, \varphi_{10}, \varphi_{11}, \varphi_{12}, \varphi_{13}\rangle$$

décrite ci-dessous est une preuve de $\Box(\phi \longrightarrow \Diamond\Diamond\phi)$ dans ce système :

(1) $\varphi_0 = A \longrightarrow (B \longrightarrow (A \wedge B))$ est une tautologie du Calcul Propositionnel et donc un axiome du système formel $\mathbf{S}$.

(2) $\varphi_1 = (P \longrightarrow \Diamond P) \longrightarrow (B \longrightarrow ((P \longrightarrow \Diamond P) \wedge B))$ est obtenue par substitution de $P \longrightarrow \Diamond P$ à A dans φ_0.

(3) $\varphi_2 = (P \longrightarrow \Diamond P) \longrightarrow ((\Diamond P \longrightarrow \Diamond\Diamond P) \longrightarrow ((P \longrightarrow \Diamond P) \wedge (\Diamond P \longrightarrow \Diamond\Diamond P)))$ est obtenue par substitution de $(\Diamond P \longrightarrow \Diamond\Diamond P)$ à B dans φ_1.

(4) $\varphi_3 = P \longrightarrow \Diamond P$ est un axiome.

(5) $\varphi_4 = (\Diamond P \longrightarrow \Diamond\Diamond P) \longrightarrow ((P \longrightarrow \Diamond P) \wedge (\Diamond P \longrightarrow \Diamond\Diamond P))$ est obtenue par *modus ponens* à partir de φ_2 et φ_3.

(6) $\varphi_5 = \Diamond P \longrightarrow \Diamond\Diamond P$ est obtenue par *substitution* de $\Diamond P$ à P dans φ_3.

(7) $\varphi_6 = (P \longrightarrow \Diamond P) \wedge (\Diamond P \longrightarrow \Diamond\Diamond P)$ est obtenue par *modus ponens* à partir de φ_4 et φ_5.

(8) $\varphi_7 = ((A' \longrightarrow B') \wedge (B' \longrightarrow C')) \longrightarrow (A' \longrightarrow C')$ est un axiome.

(9) $\varphi_8 = (P \longrightarrow B' \wedge B' \longrightarrow C') \longrightarrow (P \longrightarrow C')$ est obtenue par *substitution* de P à A' dans φ_7.

(10) $\varphi_9 = (P \longrightarrow \Diamond P \wedge \Diamond P \longrightarrow C') \longrightarrow (P \longrightarrow C')$ est obtenue par *substitution* de $\Diamond P$ à B' dans φ_8.

(11) $\varphi_{10} = (P \longrightarrow \Diamond P \wedge \Diamond P \longrightarrow \Diamond\Diamond P) \longrightarrow (P \longrightarrow \Diamond\Diamond P)$ est obtenue par *substitution* de $\Diamond\Diamond P$ à C' dans φ_9.

(12) $\varphi_{11} = P \longrightarrow \Diamond\Diamond P$ est obtenue par *modus ponens* à partir de φ_6 et φ_{10}.

(13) $\varphi_{12} = \phi \longrightarrow \Diamond\Diamond\phi$ est obtenue par *substitution* à partir de φ_{11}.

(14) $\varphi_{13} = \Box(\phi \longrightarrow \Diamond\Diamond\phi)$ est obtenue par *nécessitation* à partir de φ_{12}.

Cette présentation des preuves sous forme linéaire n'est ni gracieuse ni plaisante à lire. Nous lui préférerons une présentation sous forme d'arbres. Ainsi, les deux preuves des deux exemples précédents deviendront :

Supposons que **S** désigne l'ensemble des tautologies du Calcul Propositionnel.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{P \longrightarrow (P \vee \neg P)}\,ax}{\Diamond Q \longrightarrow (\Diamond Q \vee \neg\Diamond Q)}\,sub.}{\Box(\Diamond Q \longrightarrow (\Diamond Q \vee \neg\Diamond Q))}\,nec.}{\Box(\Diamond\phi \longrightarrow (\Diamond\phi \vee \neg\Diamond\phi))}\,sub.$$

Supposons que **S** désigne l'ensemble des tautologies du Calcul Propositionnel augmentée de la formule $P \longrightarrow \Diamond P$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A \longrightarrow (B \longrightarrow (A \wedge B))}\,ax}{(P \longrightarrow \Diamond P) \longrightarrow (B \longrightarrow ((P \longrightarrow \Diamond P) \wedge B))}\,sub}{(P \longrightarrow \Diamond P) \longrightarrow ((\Diamond P \longrightarrow \Diamond\Diamond P) \longrightarrow ((P \longrightarrow \Diamond P) \wedge (\Diamond P \longrightarrow \Diamond\Diamond P)))}\,sub \qquad \dfrac{}{P \longrightarrow \Diamond P}\,ax}{(\Diamond P \longrightarrow \Diamond\Diamond P) \longrightarrow ((P \longrightarrow \Diamond P) \wedge (\Diamond P \longrightarrow \Diamond\Diamond P))}\,mod.p. \qquad \dfrac{\dfrac{}{P \longrightarrow \Diamond P}\,ax}{\Diamond P \longrightarrow \Diamond\Diamond P}\,sub.}{(P \longrightarrow \Diamond P) \wedge (\Diamond P \longrightarrow \Diamond\Diamond P)}\,mod.p. \qquad \dfrac{\dfrac{}{((A' \longrightarrow B') \wedge (B' \longrightarrow C')) \longrightarrow (A' \longrightarrow C')}\,ax}{(P \longrightarrow \Diamond P \wedge \Diamond P \longrightarrow \Diamond\Diamond P) \longrightarrow (P \longrightarrow \Diamond\Diamond P)}\,sub.\ \times 3}{\dfrac{\dfrac{P \longrightarrow \Diamond\Diamond P}{\phi \longrightarrow \Diamond\Diamond\phi}\,sub.}{\Box(\phi \longrightarrow \Diamond\Diamond\phi)}\,nec.}\,mod.p.$$

Nous étendons la notion de preuve d'une formule dans un système formel par celle de preuve avec hypothèses. Avec un système de démonstration "à la Hilbert", cela se définit comme suit.

Définition 261 *Soit* $\mathbf{S}$ *un système formel et* Γ *un ensemble de formules appelées hypothèses, on écrit :*

$$\Gamma \vdash_{\mathbf{S}} \phi$$

s'il existe un ensemble fini de formules $\{\psi_0, \psi_1, \ldots, \psi_n\} \subseteq \Gamma$ *tel que la formule*

$$(\psi_0 \wedge \psi_1 \wedge \ldots \wedge \psi_n) \longrightarrow \phi$$

puisse être prouvée dans le système formel $\mathbf{S}$*. Autrement dit le séquent*

$$\vdash_{\mathbf{S}} (\psi_0 \wedge \psi_1 \wedge \ldots \wedge \psi_n) \longrightarrow \phi$$

est vérifié pour un nombre fini de formules bien choisies de Γ*.*

Lorsque $\Gamma = \emptyset$, nous retrouvons bien évidemment la notion de preuve dans un système formel. Lorsque l'ensemble Γ des hypothèses est lui-même fini ($\Gamma = \{\theta_0, \theta_1, \ldots, \theta_k\}$), alors la condition $\Gamma \vdash_{\mathbf{S}} \phi$ revient à dire que $\vdash_{\mathbf{S}} (\theta_0 \wedge \theta_1 \wedge \ldots \wedge \theta_k) \longrightarrow \phi$.

Remarque 262 Cette notion de déduction – à l'intérieur d'un système formel $\mathbf{S}$ – au moyen d'un ensemble d'hypothèses Γ ne doit pas être confondue avec celle présentée dans le cadre de la logique propositionnelle. En effet, prouver le séquent $\phi \vdash_{\mathbf{S}} \psi$ ne consiste pas à "ajouter" la formule ϕ aux axiomes dont on dispose pour ensuite tenter d'atteindre la formule ψ grâce aux règles de *modus ponens*, substitution uniforme et nécessitation, mais bien à prouver la formule $\phi \longrightarrow \psi$ sur la base des seuls axiomes. La première version – semblable en cela à ce qui se passe en logique propositionnelle – permettrait de prouver $\phi \vdash_{\mathbf{S}} \Box\phi$ par simple application de la règle de nécessitation à "l'hypothèse ϕ", alors que la seconde version – qui est celle que nous adoptons – nécessite de montrer $\vdash_{\mathbf{S}} \phi \longrightarrow \Box\phi$. Nous verrons, par exemple, lorsque nous aurons l'appui du théorème de complétude forte pour le système $\mathbf{K}$ – présenté dans la section à venir – que la formule $P \longrightarrow \Box P$ n'est pas prouvable dans ce système formel, et par conséquent nous avons $P \nvdash_{\mathbf{K}} \Box P$.

Pour aller plus avant :

Nous renvoyons le lecteur vers le livre de Francesca Poggiolesi *"Gentzen calculi for modal propositional logic"* [Pog10], ainsi qu'au chapitre intitulé "Modal Proof Theory" dans le *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06]. Pour la partie uniquement "systèmes de Hilbert" de la théorie de la démonstration pour la logique modale, le lecteur peut se reporter à *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02].

---

3 Le système K

Résumé № 36 *Le système* **K** *contient uniquement :*

(1) les tautologies du Calcul Propositionnel,

(2) la formule "K" := $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$,

(3) la formule "Dual" := $\Diamond P \longleftrightarrow \neg\Box\neg P$.

※

Le premier système formel que nous rencontrons est un système minimal en ce qu'il est validé dans tout modèle.

Définition 263 *Le système* **K** *est le plus petit système formel qui contient :*

(1) chaque formule de profondeur modale nulle qui est une tautologie du Calcul Propositionnel,

(2) (K) $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$,

(3) (dual) $\Diamond P \longleftrightarrow \neg\Box\neg P$.

Remarque 264

(1) Chaque tautologie du Calcul Propositionnel est forcée en tout nœud de tout système de transition, et ce quell que soit la valuation considérée.

(2) L'axiome (K) est clairement valide dans tous les systèmes de transition. Plus précisément encore, pour tout modèle $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ et tout nœud a, si $a \Vdash \Box(P \longrightarrow Q)$ et $a \Vdash \Box P$, cela signifie que pour tout nœud b tel que $a \to b$, $b \Vdash P \longrightarrow Q$ et $b \Vdash P$, par conséquent $b \Vdash Q$ et donc $a \Vdash \Box Q$.

(3) Cet axiome (K) est appelé axiome de *distribution* car il permet de distribuer l'opérateur modal $\Box$ à l'intérieur de l'implication. Exactement comme la multiplication se distribue par rapport à l'addition dans $a \cdot (b + c) = (a \cdot b + a \cdot c)$.

(4) L'axiome (*dual*) est simplement là pour permettre d'utiliser l'opérateur modal $\Diamond$. Il est valide dans tout système de transition.

Ce système formel **K** n'est pourtant pas, en l'état, suffisamment riche pour contenir toutes les formules valides dans tous les modèles quels qu'ils soient. Pour cela, il faudrait également considérer toutes les substitutions uniformes possibles qui pourraient être effectuées, entre autres, dans la formule (K). Cela signifie que nous devrions prendre les formules de la forme :

$$\Box(\psi \longrightarrow \phi) \longrightarrow (\Box\psi \longrightarrow \Box\phi)$$

mais aussi bien d'autres encore. C'est pour cette raison que nous passons maintenant des systèmes formels aux logiques modales.

4 Logique modale normale

***Résumé* № 37** *Une logique modale normale $\mathbb{L}$ est un système formel satisfaisant :*

(1) $\mathbf{K} \subseteq \mathbb{L}$ *et*

(2) $\mathbb{L}$ *est clos par déduction (pour toute ϕ, si $\vdash_{\mathbb{L}} \phi$ alors $\phi \in \mathbb{L}$).*

※

Définition 265 *Une logique modale normale est un ensemble de formules qui contient le système formel* $\mathbf{K}$ *suivant :*

(1) *chaque tautologie du Calcul Propositionnel,*

(2) *(K)* $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$

(3) *(dual)* $\Diamond P \longleftrightarrow \neg\Box\neg P$

et qui est clos par :

(1) modus ponens

$$\frac{\phi \qquad \phi \longrightarrow \psi}{\psi}\ {\scriptstyle mod.p.}$$

(2) substitution uniforme

$$\frac{\phi}{\phi[\theta/P]}\ {\scriptstyle subst.}$$

(3) nécessitation

$$\frac{\phi}{\Box\phi}\ {\scriptstyle nec.}$$

Remarque 266 (1) Toute logique modale normale contient chaque formule ϕ prouvable dans le système formel $\mathbf{K}$. Autrement dit, si $\vdash_{\mathbf{K}} \phi$ alors ϕ fait partie de toute logique modale normale.

(2) Une autre manière de définir une logiques modale normale $\mathbb{L}$ serait de dire qu'elle contient toutes les formules ϕ telles que $\vdash_{\mathbf{S}} \phi$, où $\mathbf{S}$ vaut pour un système formel bien choisi qui contient le système $\mathbf{K}$ ($\mathbf{K} \subseteq \mathbf{S}$).

(3) La plus petite logique modale normale est donc celle construite sur la base du système formel $\mathbf{K}$. Notons-la $\mathbb{L}_{\mathbf{K}}$. La relation entre la logique normale $\mathbb{L}_{\mathbf{K}}$ et le système formel $\mathbf{K}$ qui l'engendre est immédiate :

$$\phi \in \mathbb{L}_{\mathbf{K}} \quad \text{si et seulement si} \quad \vdash_{\mathbf{K}} \phi.$$

Pour aller plus avant :

Au sujet du système **K** et des logiques modale normales, nous renvoyons le lecteur vers le très abordable *"Modal logic for philosophers"* de James W. Garson [Gar06], mais également vers les plus exigeants *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03], ainsi que *"Modal logic : an introduction"* de Brian F. Chellas [Che80] et également *"Modal logic : an introduction to its syntax and semantics"* de Nino B. Cocchiarella et Max A. Freund [CF08].

Pour un point de vue plus avancé, nous conseillons également le *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06] et le *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02].

Le lecteur intéressé à la fois aux logiques modales normales et "non-nomales" lira avec intérêt les ouvrages suivants très accessibles : *"Modal logics and Philosophy"* de Rod Girle [Gir00] et *"An introduction to non-classical logic"* de Graham Priest [Pri01].

5 Quelques axiomes usuels

***Résumé* № 38**

- (K) $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$
- (D) $\Box P \longrightarrow \Diamond P$
- (T) $\Box P \longrightarrow P$
- (B) $P \longrightarrow \Box\Diamond P$
- (4) $\Box P \longrightarrow \Box\Box P$
- (5) $\Diamond P \longrightarrow \Box\Diamond P$.

※

Nous présentons quelques formules ultra-classiques de la logique modale. Chacune de ces formules sert à produire, seule ou en combinaison avec d'autres, un système formel. C'est pourquoi nous les qualifions d'axiomes.

Définition 267 *Quelques formules notoires de la logique modale :*

- (K) $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$
- (D) $\Box P \longrightarrow \Diamond P$
- (T) $\Box P \longrightarrow P$
- (B) $P \longrightarrow \Box\Diamond P$
- (4) $\Box P \longrightarrow \Box\Box P$
- (5) $\Diamond P \longrightarrow \Box\Diamond P$

Remarque 268

(1) La formule (D) dit en quelque sorte que si quelque chose est nécessaire (pour autant que $\Box$ soit interprété comme modalité de nécessité), alors cette même chose doit être possible. Ou dans le cadre d'une logique déontique, que quelque chose qui est obligatoire doit être permise. Ou bien, dans une logique épistémique, que si je sais P, alors il est faux que je sache $\neg P$. Ou encore dans une logique doxastique, que si je crois que P, alors il est faux que je crois que $\neg P$.

Ceci dit, en dehors de ces interprétations, la formule (D) dit précisément que le système de transition qui la valide n'admet *pas d'impasse*. Autrement dit, les arêtes doivent être non bornées à droite. Cela signifie que si $\mathcal{S} = (N, A)$ est un système de transition qui valide (D), alors quel que soit le nœud $a \in N$, il existe $a_1, a_2, a_3, \ldots$ tels que $a \to a_1 \to a_2 \to a_3 \ldots$. Bien évidemment, il peut y avoir multiple répétition parmi les nœuds $a_1, a_2, a_3, \ldots$; l'essentiel est qu'aucun chemin le long de ces arêtes ne mène à un nœud dépourvu d'arête. Pour le dire encore autrement, un système de transition valide la formule (D) si et seulement si pour tout nœud a il existe un nœud b tel que $a \to b$.

(2) La formule (T) dit que si quelque chose est nécessaire, alors cette même chose est. Dans le cadre d'une logique déontique, que ce qui est obligatoire est. Dans celui d'une logique épistémique, que si je sais P, alors P est avéré. Ou encore dans celui d'une logique doxastique, que si je crois que P, alors P est également avéré.

Par ailleurs, nous avons vu qu'un système de transition valide la formule (T) si et seulement si ce système est *réflexif*.

(3) La formule (B) dit que si quelque chose est le cas, alors il est nécessaire que cette même chose soit possible. Dans le cadre d'une logique déontique, que ce qui est, est obligatoirement permis. Dans celui d'une logique épistémique, que si P est avéré, alors je sais que je ne sais pas $\neg P$. Ou encore dans celui d'une logique doxastique, que si P est avéré, alors je crois que je ne crois pas $\neg P$.

Si nous regardons ce que dit cette formule d'un système de transition, nous nous apercevons qu'un système quelconque valide la formule (B) si et seulement si pour tout couple de nœuds a et b, si $a \to b$ alors $b \to a$. Autrement dit, le système est *symétrique*. Nous pouvons rapidement contrôler cela :

- si $\mathcal{S}$ est symétrique et si pour une valuation donnée $a \Vdash P$, alors soit il n'existe pas de nœud b tel que $a \to b$, auquel cas $P \longrightarrow \Box\Diamond P$ est trivialement vérifié, soit il existe un tel nœud b, auquel cas quel que soit le nœud c, tel que $a \to c$, il existe également une arête $c \to a$, ce qui suffit à satisfaire $a \Vdash P \longrightarrow \Box\Diamond P$, puisque pour tout choix du Falsificateur à partir de a, le **V**érificateur peut ensuite immédiatement revenir en a et l'emporter car, par hypothèse, $a \Vdash P$.
- Inversement, s'il existe deux nœuds a et b tels que $a \to b$ mais $b \not\to a$, il suffit de considérer une valuation telle que $a \Vdash P$ et $c \Vdash \neg P$ pour tout nœud c, tel que $b \to c$ pour obtenir $a \not\Vdash P \longrightarrow \Box\Diamond P$.

(4) La formule (4) dit que si quelque chose est nécessaire, alors cette même chose est nécessairement nécessaire. Ou bien, si elle est obligatoire, il est obligatoire qu'elle le soit. Son intérêt est néanmoins mieux perçu lorsqu'on l'interprète dans le cadre d'une logique épistémique. En effet, la formule (4) énonce que si je sais P, alors je sais que je sais P. C'est-à-dire que dès que l'on sait quelque chose, on sait aussitôt qu'on le sait. Et donc transitivement, on sait que l'on sait que l'on sait... Autrement dit, avec la formule (4) nous décrivons des agents parfaitement rationnels.

Par ailleurs, du point de vue de l'interprétation sous forme de validité dans des systèmes de transition, nous avons vu que cette formule caractérise précisément les systèmes de transition dont le graphe est *transitif* : pour tous nœuds a, b, c, si $a \to b$ et $b \to c$, alors $a \to c$. Ce qui s'exprime également par s'il existe un chemin de a vers x, alors il existe une arête de a vers x.

(5) La formule (5) dit que s'il n'est pas nécessaire que quelque chose ne soit pas, alors cela est nécessaire. Ou bien, si quelque chose est permise, alors il est obligatoire qu'elle soit permise. Néanmoins, cette formule retire sa pertinence de la logique épistémique, puisqu'elle signifie dans ce contexte que si je ne sais pas quelque chose, alors je sais que je ne le sais pas. Mieux encore, dans le cadre doxastique, elle témoigne du fait que si je ne crois pas quelque chose, alors je crois que je ne le crois pas. L'interprétation épistémique décrit un agent parfaitement conscient de ce qu'il ne sait pas, alors que celle doxastique présente un agent complètement conscient de ce à quoi il ne croit pas.

Si nous regardons maintenant les systèmes de transition que décrit la formule (5), nous nous apercevons qu'ils vérifient la propriété suivante :

$$\text{si } a \to c \text{ et } a \to b, \text{ alors } b \to c.$$

On appelle *euclidiens* les graphes qui vérifient cette propriété.

- si un système de transition est euclidien, alors la formule (5) est vérifiée en tout nœud a, puisque s'il existe un nœud c tel que $a \to c$ et $c \Vdash P$, alors pour tout nœud b tel que $a \to b$, il existe bien un nœud d, tel que $b \to d$ et $d \Vdash P$. En effet, il suffit de prendre $d = c$, puisque le caractère euclidien du graphe nous assure que de $a \to c$ et $a \to b$ nous obtenons $b \to c$.

- Inversement, si un système de transition n'est pas euclidien, alors la formule (5) n'est pas vérifiée en un nœud a de ce système. En effet, s'il existe des nœuds a, b, c, avec $a \to c$ et $a \to b$, mais pas d'arête $b \to c$, alors il suffit de considérer une valuation telle que $c \Vdash P$ et pour tout nœud $d \neq c$, $d \nVdash P$. Nous obtenons alors $a \Vdash \Diamond P$ puisque $c \Vdash P$, mais comme il n'y a pas d'arête de $b \to c$, $b \nVdash \Diamond P$ et par conséquent $a \nVdash \Box\Diamond P$.

(6) Si nous prenons ensemble la formule (5) et la formule (T), alors tout se passe comme si nous ne regardions que les systèmes de transition qui sont à la fois *euclidiens et réflexifs*. La conjonction de ces deux propriétés est en fait équivalente à la conjonction des trois suivantes : *réflexivité, symétrie et transitivité*. Autrement dit, un graphe euclidien et réflexif est en fait ni plus ni moins qu'un graphe dans lequel la relation d'accessibilité est une relation d'équivalence. Examinons cela plus en détail.

(a) Pour cela supposons tout d'abord que nous avons un graphe euclidien et réflexif et montrons que ce graphe est également :

réflexif : c'est immédiat,

symétrique : comme le graphe est réflexif, pour tout nœud a nous avons une arête de a vers lui-même ($a \to a$), par conséquent si nous avons une arête $a \to b$, le caractère euclidien nous donne une arête $b \to a$,

transitif : si nous avons deux arêtes, $a \to b$ et $b \to c$, comme nous savons dès lors que le graphe est symétrique, nous avons une arête $b \to a$, et donc en utilisant le caractère euclidien, nous retrouvons une arête $a \to c$.

(b) Supposons maintenant que nous possédons un graphe réflexif, symétrique et transitif et montrons que ce graphe est également :

réflexif : c'est immédiat,

euclidien : si nous avons deux arêtes, $a \to b$ et $a \to c$, alors la symétrie donne une arête $b \to a$ et ensuite la transitivité permet de récupérer une arête $b \to c$.

6 Quelques systèmes formels et logiques usuelles

Résumé № 39

(1) $\mathbf{KD} := \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P\}$

(2) $\mathbf{KB} := \mathbf{K} \cup \{P \longrightarrow \Box\Diamond P\}$

(3) $\mathbf{KT} := \mathbf{K} \cup \{\Box P \longrightarrow P\}$

(4) $\mathbf{K4} := \mathbf{K} \cup \{\Box P \longrightarrow \Box\Box P\}$

(5) $\mathbf{KB4} := \mathbf{K} \cup \{P \longrightarrow \Box\Diamond P, \Box P \longrightarrow \Box\Box P\}$

(6) $\mathbf{KD4} := \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P, \Box P \longrightarrow \Box\Box P\}$

(7) $\mathbf{KDB} := \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P, P \longrightarrow \Box\Diamond P\}$

(8) $\mathbf{KTB} := \mathbf{K} \cup \{\Box P \longrightarrow P, P \longrightarrow \Box\Diamond P\}$

(9) $\mathbf{S4} := \mathbf{KT4} := \mathbf{K} \cup \{\Box P \longrightarrow P, \Box P \longrightarrow \Box\Box P\}$

(10) $\mathbf{S5} := \mathbf{KT5} := \mathbf{K} \cup \{\Box P \longrightarrow P, \Diamond P \longrightarrow \Box\Diamond P\}$

※

Par la suite, nous donnerons le même nom au système formel et à la logique qu'il induit. Ces systèmes formels **S**, seront tous des extensions du système **K**. Par conséquent, présenter un système formel **S** c'est *ipso facto* présenter la logique du même nom puisqu'elle ne consiste qu'en la clôture de ce système formel **S** par les règles de *modus ponens*, *substitution uniforme* et *nécessitation*.

Définition 269 *Quelques systèmes formels notoires de la logique modale et les logiques normales qu'ils induisent :*

(1) **K** *: le plus petit système formel qui contient :*

(a) chaque tautologie du Calcul Propositionnel,

(b) $(K)\quad \Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$

(c) $(dual)\quad \Diamond P \longleftrightarrow \neg\Box\neg P$

(2) $\mathbf{KD}$: $\mathbf{K} \cup \{(D)\} = \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P\}$

(3) $\mathbf{KB}$: $\mathbf{K} \cup \{(B)\} = \mathbf{K} \cup \{P \longrightarrow \Box\Diamond P\}$

(4) $\mathbf{KT}$: $\mathbf{K} \cup \{(T)\} = \mathbf{K} \cup \{\Box P \longrightarrow P\}$

(5) $\mathbf{K4}$: $\mathbf{K} \cup \{(4)\} = \mathbf{K} \cup \{\Box P \longrightarrow \Box\Box P\}$

(6) $\mathbf{KB4}$: $\mathbf{K} \cup \{(B), (4)\} = \mathbf{K} \cup \{P \longrightarrow \Box\Diamond P, \Box P \longrightarrow \Box\Box P\}$

(7) $\mathbf{KD4}$: $\mathbf{K} \cup \{(D), (4)\} = \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P, \Box P \longrightarrow \Box\Box P\}$

(8) $\mathbf{KDB}$: $\mathbf{K} \cup \{(D), (B)\} = \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P, P \longrightarrow \Box\Diamond P\}$

(9) **KTB** : $\mathbf{K} \cup \{(T), (B)\} = \mathbf{K} \cup \{\Box P \longrightarrow P, P \longrightarrow \Box\Diamond P\}$

(10) $\mathbf{S4} = \mathbf{KT4}$: $\mathbf{K} \cup \{(T), (4)\} = \mathbf{K} \cup \{\Box P \longrightarrow P, \Box P \longrightarrow \Box\Box P\}$

(11) $\mathbf{S5} = \mathbf{KT5}$: $\mathbf{K} \cup \{(T), (5)\} = \mathbf{K} \cup \{\Box P \longrightarrow P, \Diamond P \longrightarrow \Box\Diamond P\}$

Notation 270 *Soient* $\mathbf{S}$ *et* $\mathbf{S'}$ *deux systèmes formels,* ϕ *une formule quelconque,* $\mathbf{S} \leq \mathbf{S'}$ *si et seulement si* $\vdash_{\mathbf{S}} \phi \longrightarrow \vdash_{\mathbf{S'}} \phi$.

Remarque 271

(1) Cette relation est bien évidemment réflexive ($\mathbf{S} \leq \mathbf{S}$) et transitive[1].

(2) On lit $\mathbf{S} \leq \mathbf{S'}$: $\mathbf{S}$ se réduit à $\mathbf{S'}$. Cela signifie que tout ce qui peut être prouvé à l'aide de $\mathbf{S}$ peut également l'être avec $\mathbf{S'}$.

Cette relation est une relation de comparaison, plus précisément, une relation de réduction. Si $\mathbf{S}$ se réduit à $\mathbf{S'}$, cela veut dire que $\mathbf{S}$ est en quelque sorte moins compliqué que $\mathbf{S'}$ puisque le second permet d'exprimer au moins autant que ce que fait le premier. Tout ce qui est prouvable par $\mathbf{S}$ l'est aussi par $\mathbf{S'}$.

Il est aussi important de remarquer que si $\mathbf{S}$ se réduit à $\mathbf{S'}$, cela signifie que $\mathbf{S}$ permet de prouver au moins autant de formules (appelées théorèmes) que $\mathbf{S'}$ et par conséquent, que la classe des systèmes de transition dans lesquels toutes ces formules prouvables dans $\mathbf{S'}$ sont valides est incluse dans celle des systèmes de transition qui tous valident les formules prouvables dans $\mathbf{S}$.

Autrement dit, si $\mathscr{C}_{\mathbf{S}}$, $\mathscr{C}_{\mathbf{S'}}$ désignent respectivement la classe de tous les systèmes de transition qui valident $\mathbf{S}$ et $\mathbf{S'}$:

$$\mathbf{S} \leq \mathbf{S'} \text{ si et seulement si } \mathscr{C}_{\mathbf{S'}} \subseteq \mathscr{C}_{\mathbf{S}}.$$

(3) Lorsque $\mathbf{S}$ et $\mathbf{S'}$ contiennent tous les deux le système formel $\mathbf{K}$, les logiques modales normales qu'ils engendrent ($\mathbb{L}_{\mathbf{S}}$ et $\mathbb{L}_{\mathbf{S'}}$) vérifient la relation suivante :

$$\mathbf{S} \leq \mathbf{S'} \text{ si et seulement si } \mathbb{L}_{\mathbf{S}} \subseteq \mathbb{L}_{\mathbf{S'}}.$$

Proposition 272

(1) $\mathbf{K} \leq \mathbf{K4}$, $\mathbf{K} \leq \mathbf{KB}$, $\mathbf{K} \leq \mathbf{KD}$, $\mathbf{K4} \leq \mathbf{KB4}$, $\mathbf{KB} \leq \mathbf{KB4}$, $\mathbf{K} \leq \mathbf{KT}$

(2) $\mathbf{KD} \leq \mathbf{KT}$

(3) $\mathbf{KD} \leq \mathbf{KDB}$, $\mathbf{KD} \leq \mathbf{KD4}$, $\mathbf{KDB} \leq \mathbf{KTB}$, $\mathbf{KD4} \leq \mathbf{KT4} = \mathbf{S4}$

(4) $\mathbf{S4} = \mathbf{KT4} \leq \mathbf{KT5} = \mathbf{S5}$

(5) $\mathbf{KB4} \leq \mathbf{KT5} = \mathbf{S5}$

1. Si $\mathbf{S} \leq \mathbf{S'}$ et $\mathbf{S'} \leq \mathbf{S''}$ alors $\mathbf{S} \leq \mathbf{S''}$.

Preuve de la Proposition 272 :

(1) Ces réductions sont toutes immédiates.

(2) Pour montrer que **KD** se réduit à **KT**, il suffit de montrer que la formule (D) peut être prouvée grâce au système **KT**. C'est-à-dire : $\vdash_{\mathbf{KT}} \Box P \longrightarrow \Diamond P$.

$$\dfrac{\dfrac{}{\Box P \longrightarrow P}\,\textit{ax.} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Box P \longrightarrow P}\,\textit{ax.}}{\Box\neg P \longrightarrow \neg P}\,\textit{subst.} \quad \dfrac{\dfrac{\dfrac{}{(A \longrightarrow \neg B) \longrightarrow (B \longrightarrow \neg A)}\,\textit{ax.}}{(\Box\neg P \longrightarrow \neg B) \longrightarrow (B \longrightarrow \neg\Box\neg P)}\,\textit{subst.}}{(\Box\neg P \longrightarrow \neg P) \longrightarrow (P \longrightarrow \neg\Box\neg P)}\,\textit{subst.}}{P \longrightarrow \neg\Box\neg P}\,\textit{mod.p.}}{P \longrightarrow \Diamond P}\,\textit{dual} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{(B \longrightarrow C) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C))}\,\textit{ax.}}{(B \longrightarrow C) \longrightarrow ((\Box P \longrightarrow B) \longrightarrow (\Box P \longrightarrow C))}\,\textit{subst..}}{(P \longrightarrow C) \longrightarrow ((\Box P \longrightarrow P) \longrightarrow (\Box P \longrightarrow C))}\,\textit{subst..}}{(P \longrightarrow \Diamond P) \longrightarrow ((\Box P \longrightarrow P) \longrightarrow (\Box P \longrightarrow \Diamond P))}\,\textit{subst..}}{(\Box P \longrightarrow P) \longrightarrow (\Box P \longrightarrow \Diamond P)}\,\textit{mod.p.}}{\Box P \longrightarrow \Diamond P}\,\textit{mod.p.}$$

En regroupant les étapes de substitution, cette même preuve pourra être présentée comme suit :

$$\dfrac{\dfrac{}{\Box P \longrightarrow P}\,\textit{ax.} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Box P \longrightarrow P}\,\textit{ax.}}{\Box\neg P \longrightarrow \neg P}\,\textit{subst.} \quad \dfrac{\dfrac{}{(A \longrightarrow \neg B) \longrightarrow (B \longrightarrow \neg A)}\,\textit{ax.}}{(\Box\neg P \longrightarrow \neg P) \longrightarrow (P \longrightarrow \neg\Box\neg P)}\,\textit{subst.}}{P \longrightarrow \neg\Box\neg P}\,\textit{mod.p.}}{P \longrightarrow \Diamond P}\,\textit{dual} \quad \dfrac{\dfrac{}{(B \longrightarrow C) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C))}\,\textit{ax.}}{(P \longrightarrow \Diamond P) \longrightarrow ((\Box P \longrightarrow P) \longrightarrow (\Box P \longrightarrow \Diamond P))}\,\textit{subst..}}{(\Box P \longrightarrow P) \longrightarrow (\Box P \longrightarrow \Diamond P)}\,\textit{mod.p.}}{\Box P \longrightarrow \Diamond P}\,\textit{mod.p.}$$

(3) Ces réductions sont elles aussi toutes immédiates.

(4) Pour montrer que $\mathbf{KTB} \leq \mathbf{KT5} = \mathbf{S5}$, il suffit de montrer que la formule (B) peut être prouvée grâce au système **KT5**. C'est-à-dire : $\vdash_{\mathbf{S5}} P \longrightarrow \Box\Diamond P$.
Nous allons procéder en deux temps. Tout d'abord, nous allons montrer que $\vdash_{\mathbf{KT}} P \longrightarrow \Diamond P$; ce qui montre également que $\vdash_{\mathbf{KT5}} P \longrightarrow \Diamond P$. Puis nous allons montrer que $\vdash_{\mathbf{S5}} P \longrightarrow \Box\Diamond P$ en utilisant ce résultat intermédiaire. En fait, $P \longrightarrow \Box\Diamond P$ n'est qu'un autre nom pour la formule (T). En réalité, nous avons plus précisément $\vdash_{\mathbf{KT}} (P \longrightarrow \Diamond P) \longleftrightarrow (\Box P \longrightarrow P)$, cependant nous ne prouvons ci-dessous que le coté ($\longleftarrow$) de l'implication.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Box P \longrightarrow P}\,\textit{ax.}}{\Box\neg P \longrightarrow \neg P}\,\textit{subst..} \quad \dfrac{\dfrac{}{(A \longrightarrow \neg B) \longrightarrow (B \longrightarrow \neg A)}\,\textit{ax.}}{(\Box\neg P \longrightarrow \neg P) \longrightarrow (P \longrightarrow \neg\Box\neg P)}\,\textit{subst..}}{P \longrightarrow \neg\Box\neg P}\,\textit{mod.p.}}{P \longrightarrow \Diamond P}\,\textit{dual}$$

$$\dfrac{\dfrac{}{P \longrightarrow \Diamond P}\,\textit{th.} \quad \dfrac{\dfrac{}{\Diamond P \longrightarrow \Box\Diamond P}\,\textit{ax.} \quad \dfrac{\dfrac{}{(B \longrightarrow C) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C))}\,\textit{ax.}}{(\Diamond P \longrightarrow \Box\Diamond P) \longrightarrow ((P \longrightarrow \Diamond P) \longrightarrow (P \longrightarrow \Box\Diamond P))}\,\textit{subst..}}{(P \longrightarrow \Diamond P) \longrightarrow (P \longrightarrow \Box\Diamond P)}\,\textit{mod.p.}}{P \longrightarrow \Box\Diamond P}\,\textit{mod.p.}$$

(5) Pour montrer que $\mathbf{S4} \leq \mathbf{S5}$, c'est-à-dire $\mathbf{KT4} \leq \mathbf{KT5}$, il suffit de montrer que la formule (4) peut être prouvée avec le système **KT5**. C'est-à-dire : $\vdash_{\mathbf{S5}} \Box P \longrightarrow \Box\Box P$.
Nous allons procéder en plusieurs temps.

(a) Tout d'abord, nous montrons : $\vdash_{\mathbf{S5}} \Box P \longrightarrow \Box\Diamond\Box P$

$$\dfrac{\dfrac{\dfrac{}{P \longrightarrow \Diamond P}\,\textit{th.} \quad \dfrac{\dfrac{}{\Diamond P \longrightarrow \Box\Diamond P}\,\textit{ax.} \quad \dfrac{\dfrac{}{(B \longrightarrow C) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C))}\,\textit{ax.}}{(\Diamond P \longrightarrow \Box\Diamond P) \longrightarrow ((P \longrightarrow \Diamond P) \longrightarrow (P \longrightarrow \Box\Diamond P))}\,\textit{subst..}}{(P \longrightarrow \Diamond P) \longrightarrow (P \longrightarrow \Box\Diamond P)}\,\textit{mod.p.}}{P \longrightarrow \Box\Diamond P}\,\textit{mod.p.}}{\Box P \longrightarrow \Box\Diamond\Box P}\,\textit{subst..}$$

(b) Nous montrons ensuite : $\vdash_{\mathbf{S5}} \Diamond\Box P \longrightarrow \Box P$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Diamond P \longrightarrow \Box\Diamond P}\,ax.}{\neg\Box\neg P \longrightarrow \neg\Diamond\Box\neg P}\,dual \quad \dfrac{\dfrac{}{(\neg A \longrightarrow \neg B) \longrightarrow (B \longrightarrow A)}\,ax.}{(\neg\Box\neg P \longrightarrow \neg\Diamond\Box\neg P) \longrightarrow (\Diamond\Box\neg P \longrightarrow \Box\neg P)}\,subst..}{\Diamond\Box\neg P \longrightarrow \Box\neg P}\,mod.p.}{\Diamond\Box\neg\neg P \longrightarrow \Box\neg\neg P}\,subst..}{\Diamond\Box P \longrightarrow \Box P}\,elim.\neg\neg$$

(c) Nous montrons encore : $\vdash_{\mathbf{S5}} \Box\Diamond\Box P \longrightarrow \Box\Box P$

$$\dfrac{\dfrac{\dfrac{}{\Diamond\Box P \longrightarrow \Box P}\,th.}{\Box(\Diamond\Box P \longrightarrow \Box P)}\,nec. \quad \dfrac{\dfrac{}{\Box(A \longrightarrow B) \longrightarrow (\Box A \longrightarrow \Box B)}\,ax.}{\Box(\Diamond\Box P \longrightarrow \Box P) \longrightarrow (\Box\Diamond\Box P \longrightarrow \Box\Box P)}\,subst..}{\Box\Diamond\Box P \longrightarrow \Box\Box P}\,mod.p.$$

(d) Nous montrons finalement : $\vdash_{\mathbf{S5}} \Box P \longrightarrow \Box\Box P$

$$\dfrac{\dfrac{}{\Box P \longrightarrow \Box\Diamond\Box P}\,th. \quad \dfrac{\dfrac{}{\Box\Diamond\Box P \longrightarrow \Box\Box P}\,th. \quad \dfrac{\dfrac{}{(B \longrightarrow C) \longrightarrow ((A \longrightarrow B) \longrightarrow (A \longrightarrow C))}\,ax.}{(\Box\Diamond\Box P \longrightarrow \Box\Box P) \longrightarrow ((\Box P \longrightarrow \Box\Diamond\Box P) \longrightarrow (\Box P \longrightarrow \Box\Box P))}\,subst..}{(\Box P \longrightarrow \Box\Diamond\Box P) \longrightarrow (\Box P \longrightarrow \Box\Box P)}\,mod.p.}{\Box P \longrightarrow \Box\Box P}\,mod.p.$$

(6) Pour montrer que **KB4** $\leq$ **S5** , il faut montrer deux choses :

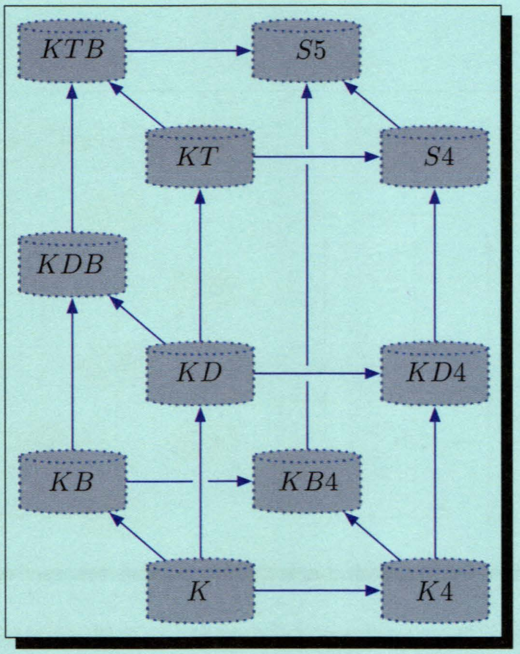
(a) la formule (4) peut être prouvée avec le système **S5**. C'est-à-dire : $\vdash_{\mathbf{S5}} \Box P \longrightarrow \Box\Box P$. Cela a été vu lors de la réduction de **S4** à **S5**.

(b) la formule (B) peut être prouvée avec le système **S5**. C'est-à-dire : $\vdash_{\mathbf{S5}} P \longrightarrow \Box\Diamond P$. Cela a également été traité plus haut lorsque nous avons montré que **KTB** $\leq$ **S5**

Une conséquence immédiate de ces deux remarques est que puisque d'une part **KB4** $\leq$ **S5** et d'autre part **KTB** $\leq$ **S5**, il en ressort que **KTB4** $\leq$ **S5**.

$\dashv$ 272

En conséquence, si l'on marque d'une flèche de **S** vers **S′** le fait que la relation **S** $\leq$ **S′** est avérée, on obtient la figure de l'exemple suivant.



Une flèche d'un système formel vers un autre dénote la réduction du premier au second.

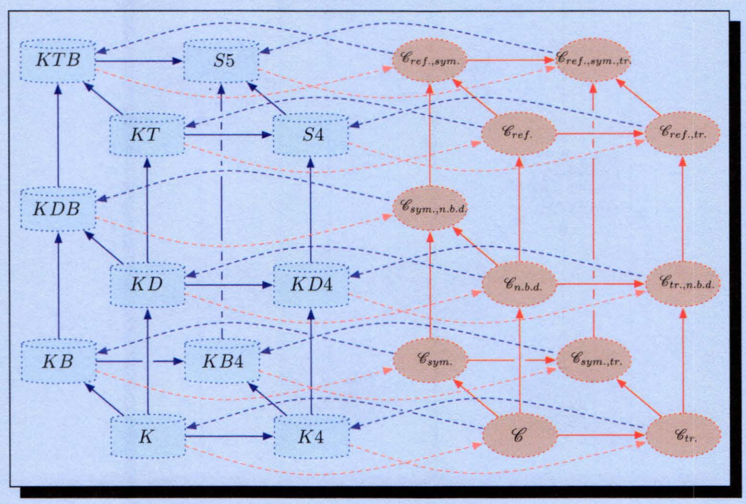
Pour aller plus avant :

Afin de retrouver dans un cadre plus avancé les extensions du système **K** que nous présentons ici, le lecteur pourra se reporter à l'ouvrage de Patrick Blackburn, Maarten de Rijke et Yde Venema intitulé *"Modal logic"* [BdRV02]. Pour des ouvrages plus abordables, le lecteur est invité à porter son attention vers *"Modal logic : an introduction"* de Brian F. Chellas [Che80] ou *"Modal logic : an introduction to its syntax and semantics"* de Nino B. Cocchiarella et Max A. Freund [CF08], ainsi que *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03]. Pour une approche d'accès plus facile encore, nous conseillons *"Modal logic for philosophers"* de James W. Garson [Gar06], *"Modal logics and Philosophy"* de Rod Girle [Gir00] ou encore *"An introduction to non-classical logic"* de Graham Priest [Pri01].

---

7 Les théorèmes de complétude

Résumé № 40



- *La relation entre systèmes formels* $\mathbf{S} \longrightarrow \mathbf{S}'$ *indique que pour toute formule* ϕ*, si* $\vdash_{\mathbf{S}} \phi$ *alors* $\vdash_{\mathbf{S}'} \phi$*.*
- *La relation entre classes de modèles* $\mathscr{C} \longrightarrow \mathscr{C}'$ *représente l'inclusion inverse* ($\mathscr{C} \supseteq \mathscr{C}'$)*.*
- *La relation* $\mathscr{C} \dashrightarrow \mathbf{S}$ *signifie : pour tout ensemble de formules* $\Gamma \cup \{\phi\}$*, si* $\Gamma \models_{\mathscr{C}} \phi$ *alors* $\Gamma \vdash_{\mathbf{S}} \phi$*.*
- *La relation* $\mathbf{S} \dashrightarrow \mathscr{C}$ *signifie : pour tout ensemble de formules* $\Gamma \cup \{\phi\}$*, si* $\Gamma \vdash_{\mathbf{S}} \phi$ *alors* $\Gamma \models_{\mathscr{C}} \phi$*.*

※

Convenons de la notation suivante pour décrire la conséquence locale sémantique.

Notation 273 *Soient* $\mathscr{C}$ *une classe de systèmes de transition,* ϕ *une formule et* Γ *un ensemble de formules. On écrit :*

$$\Gamma \models_{\mathscr{C}} \phi.$$

si pour tout système de transition $\mathcal{S} \in \mathscr{C}$*, toute valuation* $\mathcal{V}$ *et tout nœud* a*,*

$$\text{si } \langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Gamma \text{ alors } \langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi.$$

Nous rappelons que $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Gamma$ signifie que pour toute formule ψ de Γ, $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \psi$. Lorsque Γ est vide, nous utiliserons simplement la notation $\models_{\mathscr{C}} \phi$ qui signifie que la formule ϕ est valide – à la fois localement et globalement – dans tous les modèles issus de la classe $\mathscr{C}$.

Définition 274 *Soient $\mathscr{C}$ une classe de systèmes de transition et $\mathbb{L}$ une logique modale normale, $\mathbb{L}$ est solide par rapport à la classe $\mathscr{C}$ (noté $\mathscr{C}$-solide) si pour toute formule ϕ et pour tout système de transition $\mathcal{S}$ de la classe $\mathscr{C}$,*

$$\textit{si } \vdash_{\mathbb{L}} \phi \textit{ alors } \mathcal{S} \Vdash^{\forall a, \forall \mathcal{V}} \phi.$$

Il ressort de cette définition que si une logique modale normale $\mathbb{L}$ est *solide* par rapport à une classe $\mathscr{C}$, et qu'il se trouve par ailleurs un système de transition $\mathcal{S}$ de cette classe, muni d'une valuation $\mathcal{V}$, qui ne valide pas une formule ϕ en un nœud a ($\langle \mathcal{S}, \mathcal{V}, a\rangle \nVdash \phi$), alors cette formule n'est pas prouvable.

Muni de cette notation, le fait que $\mathbb{L}$ soit solide par rapport à la classe $\mathscr{C}$ s'exprime par le fait que pour toute formule ϕ, si $\vdash_{\mathbb{L}} \phi$ alors $\models_{\mathscr{C}} \phi$.

Notation 275 *Nous utilisons les abréviations suivantes pour désigner :*

(1) $\mathscr{C}$: la classe de tous les systèmes de transition

(2) $\mathscr{C}_{tr.}$: la classe de tous les systèmes de transition transitifs

(3) $\mathscr{C}_{n.b.d.}$: la classe de tous les systèmes de transition non bornés à droite

(4) $\mathscr{C}_{tr.,n.b.d.}$: la classe de tous les systèmes de transition transitifs et non bornés à droite

(5) $\mathscr{C}_{ref.}$: la classe de tous les systèmes de transition réflexifs

(6) $\mathscr{C}_{ref.,tr.}$: la classe de tous les systèmes de transition réflexifs et transitifs

(7) $\mathscr{C}_{sym.}$: la classe de tous les systèmes de transition symétriques

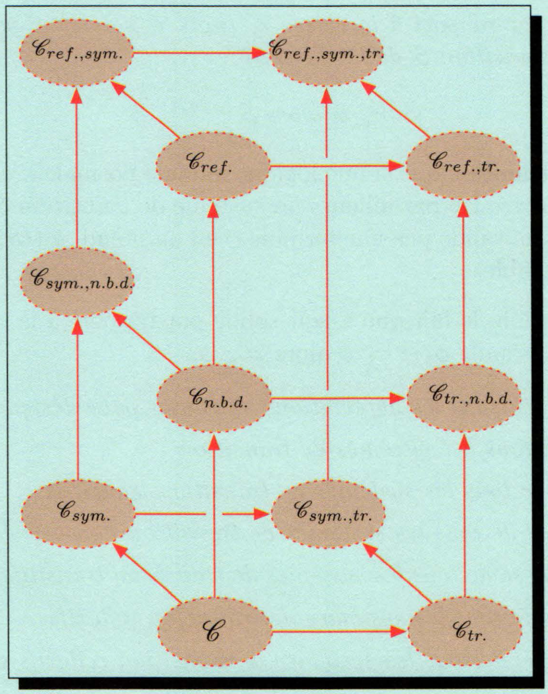
(8) $\mathscr{C}_{sym.,tr.}$: la classe de tous les systèmes de transition symétriques et transitifs

(9) $\mathscr{C}_{sym.,n.b.d.}$: la classe de tous les systèmes de transition symétriques et non bornés à droite

(10) $\mathscr{C}_{ref.,sym.}$: la classe de tous les systèmes de transition réflexifs et symétriques

(11) $\mathscr{C}_{ref.,sym.,tr.}$: la classe de tous les systèmes de transition réflexifs, symétriques et transitifs

Exemple 276 Ces classes se distribuent comme indiqué dans la figure suivante où une flèche d'une classe vers une autre ($\mathscr{C} \to \mathscr{C}'$) indique que la seconde est contenue dans la première ($\mathscr{C}' \subseteq \mathscr{C}$).



A chacune de ces onze classes, nous allons faire correspondre une logique modale normale qui se trouve être solide pour cette classe.

Théorème 277 (solidité) *Soit ϕ une formule quelconque.*

(1) si $\vdash_{\mathbf{K}} \phi$, alors $\models_{\mathscr{C}} \phi$

(2) si $\vdash_{\mathbf{K4}} \phi$, alors $\models_{\mathscr{C}_{tr.}} \phi$

(3) si $\vdash_{\mathbf{KD}} \phi$, alors $\models_{\mathscr{C}_{n.b.d.}} \phi$

(4) si $\vdash_{\mathbf{KD4}} \phi$, alors $\models_{\mathscr{C}_{tr.,n.b.d.}} \phi$

(5) si $\vdash_{\mathbf{KT}} \phi$, alors $\models_{\mathscr{C}_{ref.}} \phi$

(6) si $\vdash_{\mathbf{S4}} \phi$, alors $\models_{\mathscr{C}_{ref.,tr.}} \phi$

(7) si $\vdash_{\mathbf{KB}} \phi$, alors $\models_{\mathscr{C}_{sym.}} \phi$

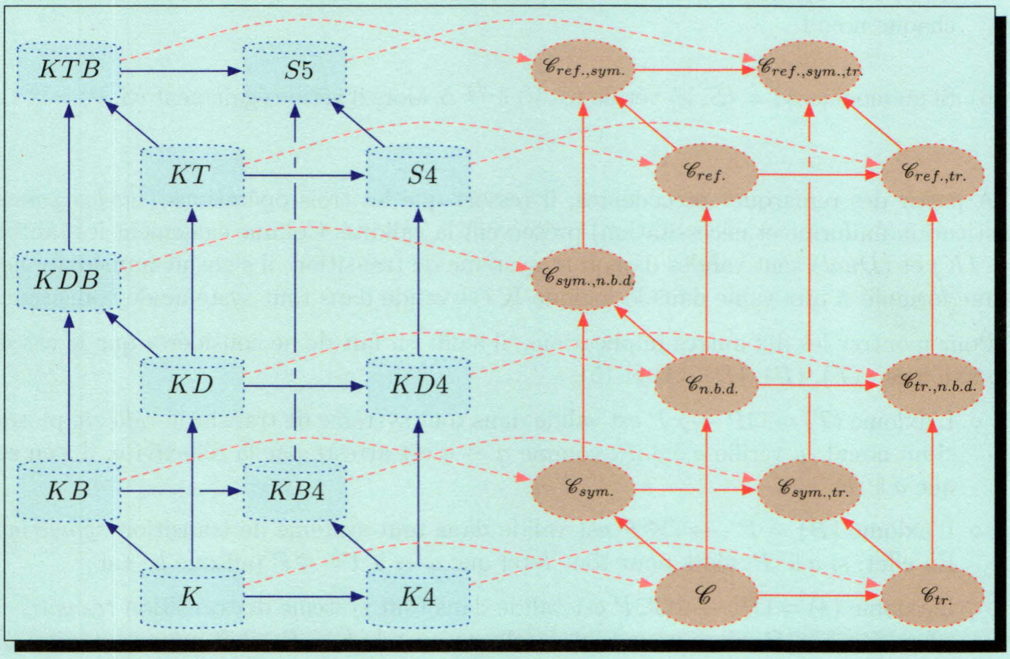
(8) si $\vdash_{\mathbf{KB4}} \phi$, alors $\models_{\mathscr{C}_{sym.,tr.}} \phi$

(9) si $\vdash_{\mathbf{KDB}} \phi$, alors $\models_{\mathscr{C}_{sym.,n.b.d.}} \phi$

(10) si $\vdash_{\mathbf{KTB}} \phi$, alors $\models_{\mathscr{C}_{ref.,sym.}} \phi$

(11) si $\vdash_{\mathbf{S5}} \phi$, alors $\models_{\mathscr{C}_{ref.,sym.,tr.}} \phi$

Exemple 278 On note par une flèche "$\mathbf{X} \to \mathscr{C}_x$", la relation de solidité : "si $\vdash_{\mathbf{X}} \phi$, alors $\models_{\mathscr{C}_x} \phi$".



Preuve du Théorème 277 :

La preuve de chacun de ces onze cas s'effectue par induction sur la longueur de la preuve de $\vdash_{\mathbb{L}} \phi$ dans la logique considérée. La longueur minimale étant bien entendu 1, puisqu'il ne s'agit dans ce cas que de considérer que ϕ est un axiome.

Quelques remarques préalables très générales :

(1) Toute tautologie du Calcul Propositionnel ϕ satisfait $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi$, quels que soient le système de transition $\mathcal{S}$, la valuation $\mathcal{V}$ et le nœud a.

(2) $(dual) = \Diamond P \longleftrightarrow \neg\Box\neg P$ est trivialement vérifié dans tout modèle. (Le fait que le ***Vérificateur*** choisisse est rigoureusement la même chose que de dire : les joueurs échangent leurs rôles, puis le ***Falsificateur*** choisit, et les joueurs échangent à nouveau leurs rôles).

(3) $(K) = \Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$ est vérifié dans tout modèle et en tout nœud, comme nous l'avons vu lors de son introduction.

(4) Si un modèle $\mathcal{M} = \langle \mathcal{S}, \mathcal{V}\rangle$ vérifie en un nœud a, à la fois $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \psi$ et $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \psi \longrightarrow \phi$, alors (par définition de l'interprétation de l'implication) il vérifie également $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \phi$.

(5) Si un système de transition $\mathcal{S}$ vérifie en un nœud a, à la fois $\langle \mathcal{S}, a \rangle \Vdash^{\forall \mathcal{V}} \phi$, alors il vérifie également $\langle \mathcal{S}, a \rangle \Vdash^{\forall \mathcal{V}} \phi[\theta/P]$ pour n'importe quelle formule θ. En effet, si $\langle \mathcal{S}, a \rangle \Vdash^{\forall \mathcal{V}} \phi$ est vérifié, cela signifie que la satisfaction de ϕ au nœud a est totalement indépendante de la valeur de vérité que prend la variable P en un nœud quelconque de $\mathcal{S}$. Elle est donc également indépendante de la valeur que prend la formule θ en chaque nœud.

(6) Si un modèle $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ vérifie $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \phi$, alors il vérifie également $\langle \mathcal{S}, \mathcal{V} \rangle \Vdash^{\forall a} \Box\phi$.

A partir des remarques précédentes, il ressort que les trois opérations (*modus ponens*, substitution uniforme et nécessitation) préservent la validité. Comme également les tautologies, (K) et $(Dual)$ sont valides dans tout système de transition, il s'ensuit immédiatement qu'une formule ϕ prouvable dans la logique **K** est valide dans tout système de transition.

Pour montrer les dix autres implications, il suffit en fait de ne considérer que le cas des cinq axiomes : (T), (B), (D), (4) et (5).

- L'axiome $(T) = \Box P \longrightarrow P$ est valide dans tout système de transition *réflexif*, puisque si un nœud a vérifie $a \Vdash \Box P$, comme $a \rightarrow a$ est attesté par la réflexivité, il s'en suit que $a \Vdash P$.
- L'axiome $(B) = P \longrightarrow \Box\Diamond P$ est valide dans tout système de transition *symétrique*. En effet, si $a \Vdash P$, alors pour tout b tel que $a \rightarrow b$, $b \Vdash \Diamond P$ puisque $b \rightarrow a$.
- L'axiome $(4) = \Box P \longrightarrow \Box\Box P$ est valide dans tout système de transition *transitif*. En effet, si $a \Vdash \Box P$, alors pour tout b tel que $a \rightarrow b$, $b \Vdash P$, d'où pour tout c tel que $a \rightarrow b \rightarrow c$, $c \Vdash P$ puisque $a \rightarrow c$ est vérifié par la transitivité.
- L'axiome $(D) = \Box P \longrightarrow \Diamond P$ est valide dans tout système de transition *non bornés à droite* - ou *n.b.d.* en abrégé - c'est-à-dire tout système de transition dans lequel il n'existe aucun nœud d'où ne parte aucune flèche. Ou pour le dire encore d'une troisième manière, un système de transition est *n.b.d.* précisément lorsqu'aucun chemin dans le graphe ne peut mener à une impasse. Dès lors, le fait que tout système de transition valide $\Box P \longrightarrow \Diamond P$ devient une trivialité.
- L'axiome $(5) = \Diamond P \longrightarrow \Box\Diamond P$ est valide dans tout système de transition *euclidien*, c'est-à-dire tel que si $a \rightarrow b$ et $a \rightarrow c$ alors $c \rightarrow b$. Si un nœud a vérifie $a \Vdash \Diamond P$, alors il existe un nœud b, tel que $b \Vdash P$. Soit maintenant un nœud c quelconque tel que $a \rightarrow c$, puisque le système de transition est euclidien et à la fois $a \rightarrow b$ et $a \rightarrow c$ sont vérifiés, et donc $c \rightarrow b$ est également satisfait, ce qui donne $c \Vdash \Diamond P$.

  Par ailleurs, nous avons déjà montré qu'un graphe est à la fois *réflexif* et *euclidien* si et seulement si il est *réflexif*,*symétrique* et *transitif*[2].

Il suffit dès lors de prendre en considération les axiomes modaux intervenant dans chacune des onze logiques modales normales pour obtenir les résultats de solidité des logiques en question par rapport aux classes de systèmes de transition qui leur correspondent.

$\dashv$ 277

2. cf. Remarque 268(6).

Définition 279 *Soient $\mathscr{C}$ une classe de systèmes de transition et $\mathbb{L}$ une logique modale normale,*

(1) $\mathbb{L}$ est faiblement complète par rapport à la classe $\mathscr{C}$ (noté $\mathscr{C}$-faiblement complète) si pour toute formule ϕ

$$\text{si } \models_{\mathscr{C}} \phi \text{ alors } \vdash_{\mathbb{L}} \phi.$$

(2) $\mathbb{L}$ est fortement complète par rapport à la classe $\mathscr{C}$ (noté $\mathscr{C}$-fortement complète, ou plus simplement $\mathscr{C}$-complète) si pour toute formule ϕ et tout ensemble de formules Γ

$$\text{si } \Gamma \models_{\mathscr{C}} \phi \text{ alors } \Gamma \vdash_{\mathbb{L}} \phi.$$

Remarque 280

(1) En passant par la contraposée, la notion de faible complétude s'exprime par :

$$\text{si } \nvdash_{\mathbb{L}} \phi \text{ alors } \not\models_{\mathscr{C}} \phi.$$

(2) Et celle de complétude au sens fort revient à dire :

$$\text{si } \Gamma \nvdash_{\mathbb{L}} \phi \text{ alors } \Gamma \not\models_{\mathscr{C}} \phi.$$

Théorème 281 (forte complétude) *Soient ϕ une formule et Γ un ensemble de formules.*

(1) si $\Gamma \models_{\mathscr{C}} \phi$ alors $\Gamma \vdash_{\mathbf{K}} \phi$

(2) si $\Gamma \models_{\mathscr{C}_{tr.}} \phi$ alors $\Gamma \vdash_{\mathbf{K4}} \phi$

(3) si $\Gamma \models_{\mathscr{C}_{n.b.d.}} \phi$ alors $\Gamma \vdash_{\mathbf{KD}} \phi$

(4) si $\Gamma \models_{\mathscr{C}_{tr.,n.b.d.}} \phi$ alors $\Gamma \vdash_{\mathbf{KD4}} \phi$

(5) si $\Gamma \models_{\mathscr{C}_{ref.}} \phi$ alors $\Gamma \vdash_{\mathbf{KT}} \phi$

(6) si $\Gamma \models_{\mathscr{C}_{ref.,tr.}} \phi$ alors $\Gamma \vdash_{\mathbf{S4}} \phi$

(7) si $\Gamma \models_{\mathscr{C}_{sym.}} \phi$ alors $\Gamma \vdash_{\mathbf{KB}} \phi$

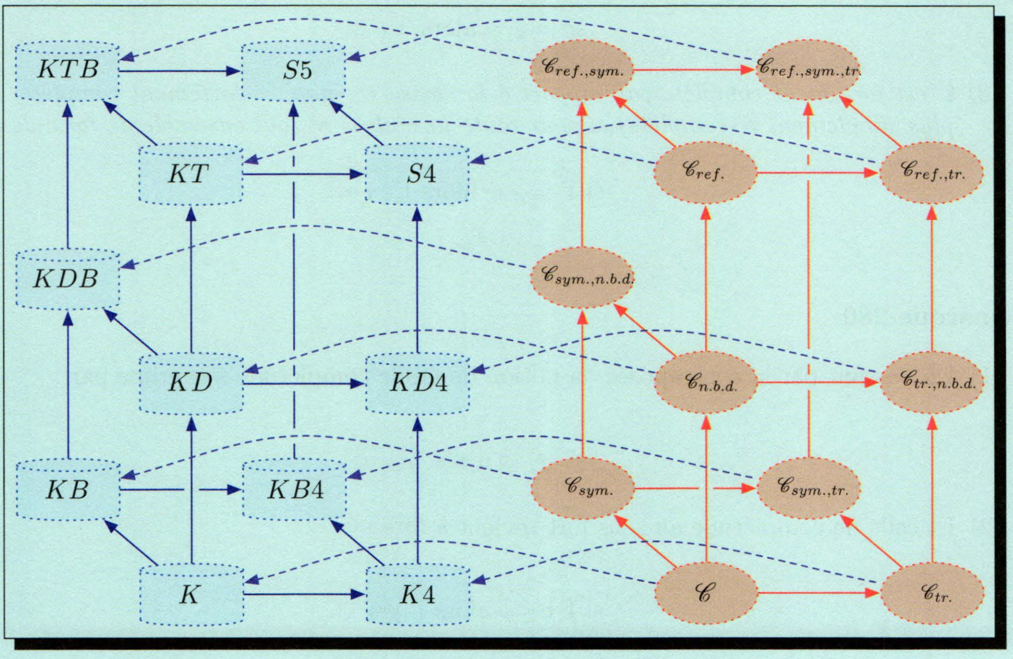
(8) si $\Gamma \models_{\mathscr{C}_{sym.,tr.}} \phi$ alors $\Gamma \vdash_{\mathbf{KB4}} \phi$

(9) si $\Gamma \models_{\mathscr{C}_{sym.,n.b.d.}} \phi$ alors $\Gamma \vdash_{\mathbf{KDB}} \phi$

(10) si $\Gamma \models_{\mathscr{C}_{ref.,sym.}} \phi$ alors $\Gamma \vdash_{\mathbf{KTB}} \phi$

(11) si $\Gamma \models_{\mathscr{C}_{ref.,sym.,tr.}} \phi$ alors $\Gamma \vdash_{\mathbf{S5}} \phi$

Exemple 282 On note par une flèche "$\mathscr{C}_x \to \mathbf{X}$" la relation de forte complétude : "si $\Gamma \models_{\mathscr{C}_x} \phi$ alors $\Gamma \vdash_{\mathbf{X}} \phi$".



La manière abrupte de prouver ce théorème serait de considérer n'importe quel système de transition d'une classe donnée, une formule valide dans ce système de transition avec Γ pour hypothèses et de produire une preuve de ϕ dans la logique correspondante.

Ce n'est pas du tout ce que nous allons faire. Bien au contraire, *ces résultats de complétude vont chacun se ramener à la production d'un seul modèle.* Avant de voir cela, nous avons besoin d'une définition et d'un résultat simple transformant la complétude en la recherche de ce modèle.

Définition 283 *Soient* $\mathbf{S}$ *un système formel et* Γ *un ensemble de formules,*

$$\Gamma \text{ est } \mathbf{S}\text{-consistant} \quad \text{si et seulement si} \quad \Gamma \nvdash_{\mathbf{S}} \bot.$$

Dans le cas contraire, Γ est dit $\mathbf{S}$-inconsistant.

Lemme 284 *Soient* $\mathscr{C}$ *une classe de systèmes de transition,* $\mathbb{L}$ *une logique modale normale,*

$$\begin{gathered} \mathbb{L} \text{ est } \mathscr{C}\text{-(fortement) complète} \\ \text{si et seulement si} \\ \text{pour tout } \Gamma \subseteq \mathbb{L} \text{ qui est } \mathbb{L}\text{-consistant, il existe } \mathcal{S} \in \mathscr{C},\ \mathcal{V} \text{ et } a \text{ tels que } \langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Gamma. \end{gathered}$$

Preuve du Lemme 284 : Il y a deux sens à cette preuve :

($\Rightarrow$) puisque $\mathbb{L}$ est $\mathscr{C}$-complète, un ensemble de formules quelconque qui est $\mathbb{L}$-consistant $\Gamma \subseteq \mathbb{L}$ est nécessairement satisfaisable par un système de transition de la classe $\mathscr{C}$. En effet, si ce n'était le cas, l'expression $\Gamma \models_{\mathscr{C}} \bot$ serait vraie, mais alors nous pourrions en déduire $\Gamma \vdash_{\mathbb{L}} \bot$ en utilisant la $\mathscr{C}$-complétude de $\mathbb{L}$.

($\Leftarrow$) nous montrons la contraposée. C'est-à-dire : si $\mathbb{L}$ n'est pas $\mathscr{C}$-complète alors il existe $\Gamma \subseteq \mathbb{L}$, $\mathbb{L}$-consistant tel que quels que soient $\mathcal{S} \in \mathscr{C}$, $\mathcal{V}$ et a, $\langle \mathcal{S}, \mathcal{V}, a \rangle \not\Vdash \Gamma$.

Soit donc Γ un ensemble de formules et ϕ une formule tels que $\Gamma \models_{\mathscr{C}} \phi$ mais $\Gamma \not\vdash_{\mathbb{L}} \phi$. Il apparaît dès lors que $\Gamma \cup \{\neg\phi\} \not\vdash_{\mathbb{L}} \bot$ est vérifié, car sinon $\Gamma \cup \{\neg\phi\} \vdash_{\mathbb{L}} \bot$ entraînerait $\Gamma \vdash_{\mathbb{L}} \neg\phi \longrightarrow \bot$ puis, en passant par la contraposée, $\Gamma \vdash_{\mathbb{L}} \phi$. Par conséquent $\Gamma \cup \{\neg\phi\}$ est $\mathbb{L}$-consistant et pourtant, pour tout système de transition $\mathbf{S} \in \mathscr{C}$, $\mathcal{V}$ et a, $\langle \mathcal{S}, \mathcal{V}, a \rangle \not\Vdash \Gamma \cup \{\neg\phi\}$.

$\dashv$ 284

Notre problème de démontrer les théorèmes de complétude (un pour chacune des onze logiques normales que nous considérons) revient donc, étant donné un ensemble de formules Γ $\mathbb{L}$-consistant, à celui de chercher un modèle $\langle \mathcal{S}, \mathcal{V} \rangle$ - dont le système de transition fait partie de la classe considérée - et un nœud a tel que $\langle \mathcal{S}, \mathcal{V}, a \rangle \Vdash \Gamma$.

En fait, nous n'allons pas chercher un modèle au hasard, mais nous allons à chaque fois regarder un modèle particulier que nous appellerons le *modèle canonique*. Comment, d'ailleurs, pourrions-nous chercher un modèle au hasard ? Ce qui est néanmoins étonnant, c'est que ce modèle ne sera pas constitué de "véritables individus" (comme des vaches ou des assiettes, ou encore des nombrils) mais de ce que nous avons sous la main. Précisément, qu'avons-nous sous la main ? Vraiment tout proche, nous n'avons que des formules, puisque nous baignons dans la syntaxe. Or précisément, il nous faudrait trouver toute autre chose : un modèle. Et bien, au risque de jouer les rabats joie, nous allons décrire un modèle dans lequel le système de transition sera constitué d'ensemble de formules. C'est là la suprême astuce de la sémantique : tourner la syntaxe à son profit. Etonnant non ?!

Définition 285 *Soient $\mathbb{L}$ une logique modale et Γ un ensemble de formules,*

$$\Gamma \textit{ est maximal } \mathbb{L}\textit{-consistant si et seulement si } \Gamma \not\vdash_{\mathbb{L}} \bot \textit{ et pour tout ensemble } \Gamma \subsetneq \Gamma', \; \Gamma' \vdash_{\mathbb{L}} \bot.$$

Remarque 286 Si Γ est maximal $\mathbb{L}$-consistant, alors :

- $\mathbb{L} \subseteq \Gamma$
- Γ est clos par *modus ponens.*
- Pour toute formule ϕ,
$$\phi \in \Gamma \text{ ou } \neg\phi \in \Gamma.$$
- Pour toutes formules ϕ, ψ,
$$\phi \vee \psi \in \Gamma \text{ si et seulement si } \phi \in \Gamma \text{ ou } \psi \in \Gamma.$$

Lemme 287 (Lindenbaum) *Si Γ est $\mathbb{L}$-consistant, alors il existe Γ_{max} maximal $\mathbb{L}$-consistant tel que $\Gamma \subseteq \Gamma_{max}$.*

Preuve du Lemme 287 : Soit $(\phi_n)_{n\in\mathbb{N}}$ une énumération de toutes les formules. On définit :

- $\Gamma_0 = \Gamma$
- $\Gamma_{n+1} = \begin{cases} \Gamma_n \cup \{\phi_n\} \text{ si } \Gamma_n \cup \{\phi_n\} \nvdash_{\mathbb{L}} \bot \\ \Gamma_n \cup \{\neg\phi_n\} \text{ sinon} \end{cases}$
- $\Gamma_{max} = \bigcup_{n\in\mathbb{N}} \Gamma_n$
- Γ_{max} est $\mathbb{L}$-consistant, car sinon il existerait un plus petit entier n tel que $\Gamma_{n+1} \vdash_{\mathbb{L}} \bot$. Dans ce cas, nous aurions $\Gamma_n \cup \{\phi_n\} \vdash_{\mathbb{L}} \bot$ et $\Gamma_n \cup \{\neg\phi_n\} \vdash_{\mathbb{L}} \bot$, d'où, en utilisant le raisonnement par l'absurde, nous obtenons à la fois $\Gamma_n \vdash_{\mathbb{L}} \neg\phi_n$ et $\Gamma_n \vdash_{\mathbb{L}} \phi_n$. Cela conduit à $\Gamma_n \vdash_{\mathbb{L}} \bot$, contredisant le fait que par minimalité de l'entier n, Γ_n est $\mathbb{L}$-consistant.
- Γ_{max} est maximal, car sinon il existerait Γ' $\mathbb{L}$-consistant tel que $\Gamma_{max} \subsetneq \Gamma'$. Si tel était le cas, soit ψ une formule quelconque telle que $\psi \in \Gamma' \setminus \Gamma_{max}$. Cette formule apparaît dans l'énumération $(\phi_n)_{n\in\mathbb{N}}$ de toutes les formules. Ainsi, il existe un entier n tel que $\psi = \phi_n$. Par construction de Γ_{max}, puisque $\phi_n \notin \Gamma_{max}$, $\Gamma_n \cup \{\phi_n\} \vdash_{\mathbb{L}} \bot$ est vérifié. Et donc $\Gamma_{max} \cup \{\phi_n\} \vdash_{\mathbb{L}} \bot$ ce qui entraîne $\Gamma' \vdash_{\mathbb{L}} \bot$, contredisant le caractère $\mathbb{L}$-consistant de Γ'.

$\dashv$ 287

Définition 288 *Soit $\mathbb{L}$ une logique modale, le modèle canonique $\mathcal{M}_{\mathbb{L}}$ est défini par $\mathcal{M}_{\mathbb{L}} = \langle N_{\mathbb{L}}, A_{\mathbb{L}}, \mathcal{V}_{\mathbb{L}}\rangle$:*

(1) $N_{\mathbb{L}} = \{\Gamma \mid \Gamma \text{ maximal } \mathbb{L}\text{−consistant}\}$.

(2) $A_{\mathbb{L}}$ défini par $\Gamma \to \Gamma'$ si et seulement si pour toute formule ϕ, si $\phi \in \Gamma'$ alors $\Diamond\phi \in \Gamma$. i.e. $\Gamma \supseteq \{\Diamond\phi \ : \phi \in \Gamma'\}$.

(3) $\mathcal{V}_{\mathbb{L}}$ défini par $\mathcal{V}_{\mathbb{L}}(P) = \{\Gamma \in N_{\mathbb{L}} \mid P \in \Gamma\}$. i.e., $\Gamma \Vdash P$ si et seulement si $P \in \Gamma$.

Lemme 289 ($\to$ et $\Box$) *Soit $\mathbb{L}$ une logique modale normale et $\mathcal{M}_{\mathbb{L}} = \langle N_{\mathbb{L}}, A_{\mathbb{L}}, \mathcal{V}_{\mathbb{L}}\rangle$ le modèle canonique associé à $\mathbb{L}$. Pour tout nœud $\Gamma, \Gamma' \in N_{\mathbb{L}}$, on a :*

$$\Gamma \to \Gamma' \text{ si et seulement si pour toute formule } \psi, \text{ si } \Box\psi \in \Gamma \text{ alors } \psi \in \Gamma'$$

Preuve du Lemme 289 :

($\Longrightarrow$) Nous raisonnons par l'absurde et supposons donc $\Box\psi \in \Gamma$ et $\psi \notin \Gamma'$. Par maximale $\mathbb{L}$-consistance de Γ', il s'ensuit que $\neg\psi \in \Gamma'$. Par définition de l'arête $\Gamma \to \Gamma'$, $\Diamond\neg\psi \in \Gamma$ et puisque Γ est consistant, $\neg\Diamond\neg\psi \notin \Gamma$, d'où $\Box\psi \notin \Gamma$, contradiction.

($\Longleftarrow$) Soit $\psi \in \Gamma'$. Nous raisonnons par l'absurde et supposons $\Diamond\psi \notin \Gamma$. Alors par maximale $\mathbb{L}$-consistance $\neg\Diamond\psi \in \Gamma$, par conséquent $\neg\Diamond\neg\neg\psi \in \Gamma$ et donc $\Box\neg\psi \in \Gamma$. Par hypothèse $\Box\neg\psi \in \Gamma$ entraîne $\neg\psi \in \Gamma'$, ce qui contredit la $\mathbb{L}$-consistance de Γ'.

$\dashv$ 289

Lemme 290 ($\to$ et $\Diamond$) *Soit $\mathbb{L}$ une logique modale normale et $\mathcal{M}_{\mathbb{L}} = \langle N_{\mathbb{L}}, A_{\mathbb{L}}, \mathcal{V}_{\mathbb{L}}\rangle$ le modèle canonique associé à $\mathbb{L}$.*

Pour tout nœud $\Gamma, \Gamma' \in N_{\mathbb{L}}$,

$$\text{si } \Diamond\phi \in \Gamma \text{ alors il existe } \Gamma' \text{ tel que } \Gamma \to \Gamma' \text{ et } \phi \in \Gamma'.$$

Preuve du Lemme 290 : Supposons $\Diamond\phi \in \Gamma$, on obtient Γ' de la manière suivante. On construit tout d'abord $\Theta = \{\phi\} \cup \{\psi \mid \Box\psi \in \Gamma\}$. Cet ensemble Θ est consistant car sinon il existerait $\psi_1, \ldots, \psi_k \in \Theta$ tels que :

$$\vdash_{\mathbb{L}} (\psi_1 \wedge \ldots \wedge \psi_k) \longrightarrow \neg\phi.$$

Par nécessitation on obtient :

$$\vdash_{\mathbb{L}} \Box((\psi_1 \wedge \ldots \wedge \psi_k) \longrightarrow \neg\phi)$$

et par distributivité (c'est-à-dire l'utilisation de l'axiome (K)) :

$$\vdash_{\mathbb{L}} \Box(\psi_1 \wedge \ldots \wedge \psi_k) \longrightarrow \Box\neg\phi.$$

Puisque dans toute logique normale,

$$\vdash_{\mathbb{L}} (\Box\psi_1 \wedge \ldots \wedge \Box\psi_k) \longrightarrow \Box(\psi_1 \wedge \ldots \wedge \psi_k).$$

On aboutit ainsi à :

$$\vdash_{\mathbb{L}} (\Box\psi_1 \wedge \ldots \wedge \Box\psi_k) \longrightarrow \Box\neg\phi.$$

Par conséquent $\Gamma \vdash_{\mathbb{L}} \Box\neg\phi$, ce qui implique $\Box\neg\phi \in \Gamma$ par maximalité, et donc également $\neg\Diamond\phi \in \Gamma$. Cela conduit à montrer la $\mathbb{L}$-inconsistance de Γ, puisque par hypothèse $\Diamond\phi \in \Gamma$ est vérifié, c'est donc une contradiction.

Comme nous venons de monter que l'ensemble $\Theta = \{\phi\} \cup \{\psi \mid \Box\psi \in \Gamma\}$ est $\mathbb{L}$-consistant, il suffit de prendre pour Γ' l'ensemble Θ_{max} maximal $\mathbb{L}$-consistant, donné par le lemme de Lindenbaum (Lemme 287), tel que $\Theta \subseteq \Theta_{max}$.

$\dashv$ 290

Lemme 291 (vérité) *Soit $\mathbb{L}$ une logique modale normale et $\mathcal{M}_{\mathbb{L}} = \langle N_{\mathbb{L}}, A_{\mathbb{L}}, \mathcal{V}_{\mathbb{L}}\rangle$ le modèle canonique associé à $\mathbb{L}$. Pour tout nœud $\Gamma \in N_{\mathbb{L}}$,*

$$\langle \mathcal{M}_{\mathbb{L}}, \Gamma\rangle \Vdash \phi \iff \phi \in \Gamma.$$

Preuve du Lemme 291 : La preuve s'effectue par induction sur la hauteur de la formule ϕ.

- si $ht(\phi) = 0$, alors $\phi = \bot$ ou $\phi = \top$ ou ϕ est une variable propositionnelle. Dans ce dernier cas, $\Gamma \Vdash \phi$ si et seulement si $\phi \in \Gamma$ est la définition même de la valuation $\mathcal{V}_{\mathbb{L}}$.
- si $ht(\phi) = n + 1$ alors :
  - si $\phi = \neg\psi$ alors $\Gamma \Vdash \neg\psi$ si et seulement si $\Gamma \nVdash \psi$. Par hypothèse d'induction :

    $$\Gamma \nVdash \psi \iff \psi \notin \Gamma.$$

    Par maximalité de Γ, on obtient $\neg\psi \in \Gamma$.
  - si $\phi = (\phi_1 \vee \phi_2)$ alors :

    $$\Gamma \Vdash (\phi_1 \vee \phi_2) \iff \Gamma \Vdash \phi_1 \text{ ou } \Gamma \Vdash \phi_2.$$

    Par hypothèse d'induction :

    $$\Gamma \Vdash \phi_1 \iff \phi_1 \in \Gamma$$

et

$$\Gamma \Vdash \phi_2 \iff \phi_2 \in \Gamma.$$

Par maximalité de Γ :

$$\phi_1 \in \Gamma \text{ ou } \phi_2 \in \Gamma \iff (\phi_1 \vee \phi_2) \in \Gamma.$$

- si $\phi = (\phi_1 \wedge \phi_2)$ alors :

$$\Gamma \Vdash (\phi_1 \wedge \phi_2) \iff \Gamma \Vdash \phi_1 \text{ et } \Gamma \Vdash \phi_2.$$

Par hypothèse d'induction :

$$\Gamma \Vdash \phi_1 \iff \phi_1 \in \Gamma$$

et

$$\Gamma \Vdash \phi_2 \iff \phi_2 \in \Gamma.$$

Or, par $\mathbb{L}$-consistance :

$$\phi_1 \in \Gamma \text{ et } \phi_2 \in \Gamma \iff (\phi_1 \wedge \phi_2) \in \Gamma.$$

- si $\phi = (\phi_1 \longrightarrow \phi_2)$. Ce cas se déduit facilement de $\neg\phi_1 \vee \phi_2$. En effet :

$$\begin{aligned}
\Gamma \Vdash \phi_1 \longrightarrow \phi_2 &\iff \Gamma \Vdash \neg\phi_1 \vee \phi_2 \\
&\iff \Gamma \Vdash \neg\phi_1 \text{ ou } \Gamma \Vdash \phi_2 \\
&\iff \neg\phi_1 \in \Gamma \text{ ou } \phi_2 \in \Gamma \\
&\iff \neg\phi_1 \vee \phi_2 \in \Gamma \\
&\iff \phi_1 \longrightarrow \phi_2 \in \Gamma.
\end{aligned}$$

- si $\phi = \phi_1 \longleftrightarrow \phi_2$. Ce cas se déduit facilement de $\phi_1 \longrightarrow \phi_2 \wedge \phi_2 \longrightarrow \phi_1$. En effet :

$$\begin{aligned}
\Gamma \Vdash \phi_1 \longleftrightarrow \phi_2 &\iff \Gamma \Vdash (\phi_1 \longrightarrow \phi_2) \wedge (\phi_2 \longrightarrow \phi_1) \\
&\iff \Gamma \Vdash \phi_1 \longrightarrow \phi_2 \text{ et } \Gamma \Vdash \phi_2 \longrightarrow \phi_1 \\
&\iff \phi_1 \longrightarrow \phi_2 \in \Gamma \text{ et } \phi_2 \longrightarrow \phi_1 \in \Gamma \\
&\iff (\phi_1 \longrightarrow \phi_2) \wedge (\phi_2 \longrightarrow \phi_1) \in \Gamma \\
&\iff \phi_1 \longleftrightarrow \phi_2 \in \Gamma.
\end{aligned}$$

- si $\phi = \Diamond\psi$, alors :

$$\Gamma \Vdash \Diamond\psi \iff \text{il existe } \Gamma',\ \Gamma \to \Gamma' \text{ et } \Gamma' \Vdash \psi.$$

Or, par hypothèse d'induction :

$$\Gamma' \Vdash \psi \iff \psi \in \Gamma'.$$

Finalement, par définition de la relation $\Gamma \to \Gamma'$ et par le Lemme 290 :

$$\psi \in \Gamma' \iff \Diamond\psi \in \Gamma.$$

- si $\phi = \Box\psi$ alors $\Gamma \Vdash \Box\psi$ se déduit de $\Gamma \Vdash \neg\Diamond\neg\psi$.
  En effet :

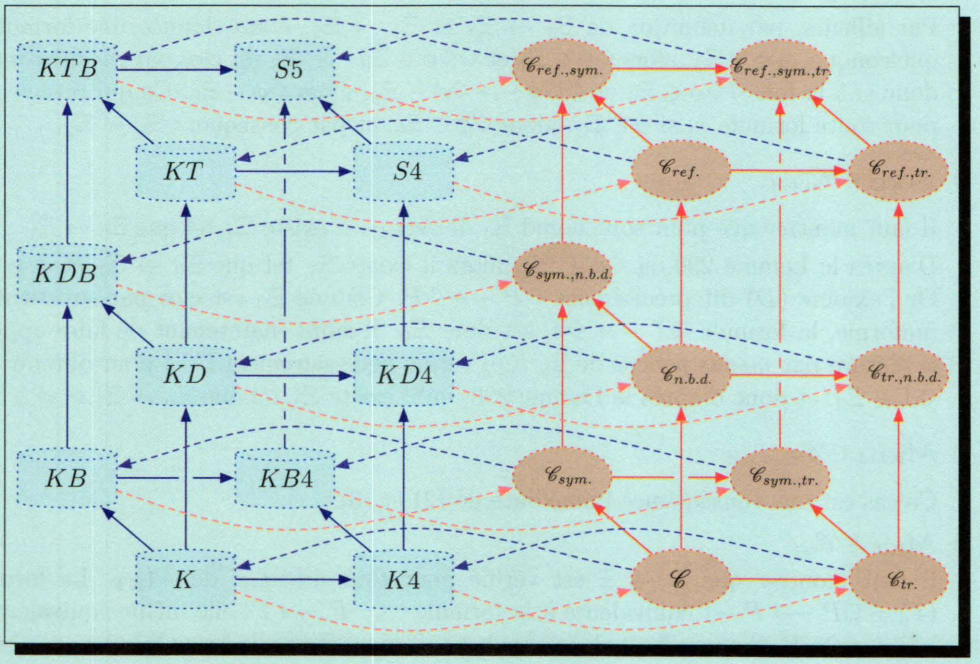
$$\Gamma \Vdash \Box\psi \iff \Gamma \Vdash \neg\Diamond\neg\psi \iff \neg\Diamond\neg\psi \in \Gamma \iff \Box\psi \in \Gamma$$

(par maximal $\mathbb{L}$-consistance).

$\dashv$ 291

Nous sommes finalement en mesure de prouver le Théorème 281, qui stipule que chacune des onze logiques modales normales que nous considérons dans ce chapitre est fortement complète. Pour cela, nous allons à chaque fois nous intéresser au modèle canonique de chacune de ces logiques.

Exemple 292 Dans ce schéma, une flèche "$\mathbf{X} \to \mathscr{C}_x$" indique "$\vdash_{\mathbf{X}} \phi$ entraîne $\models_{\mathscr{C}_x} \phi$" ; une flèche "$\mathscr{C}_x \to \mathbf{X}$", indique "si $\Gamma \models_{\mathscr{C}_x} \phi$ alors $\Gamma \vdash_{\mathbf{X}} \phi$".



Preuve du Théorème 281 : Par le Lemme 284, $\mathbb{L}$ est $\mathscr{C}$-(fortement) complète ssi pour tout $\Gamma \subseteq \mathbb{L}$, $\mathbb{L}$-consistant, il existe $\mathcal{S} \in \mathscr{C}$, $\mathcal{V}$ et a tels que $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Gamma$. Il suffit donc, pour chacune des onze logiques ($\mathbb{L}$) considérées, à partir d'un ensemble de formules $\Gamma \subseteq \mathbb{L}$, $\mathbb{L}$-consistant, de trouver un modèle $\mathcal{M} = \langle \mathcal{S}, \mathcal{V}\rangle$ et un nœud a de ce modèle tels que $\langle \mathcal{S}, \mathcal{V}, a\rangle \Vdash \Gamma$ et $\mathcal{S} \in \mathscr{C}$.

A chaque fois le modèle que nous allons choisir est le modèle canonique $\mathcal{M}_{\mathbb{L}} = \langle N_{\mathbb{L}}, A_{\mathbb{L}}, \mathcal{V}_{\mathbb{L}}\rangle$ associé à la logique $\mathbb{L}$ considérée. Pour un nœud a, nous allons prendre un ensemble Γ' maximal $\mathbb{L}$-consistant qui vérifie $\Gamma \subseteq \Gamma'$. Nous prendrons ainsi par exemple $\Gamma' = \Gamma_{max}$. Par le Lemme 291, on obtient $\langle \mathcal{M}_{\mathbb{L}}, \Gamma'\rangle \Vdash \phi$ si et seulement si $\phi \in \Gamma'$. En conséquence, puisque $\Gamma \subseteq \Gamma'$, il ressort que $\langle \mathcal{M}_{\mathbb{L}}, \Gamma'\rangle \Vdash \Gamma$.

La seule chose qu'il reste à prouver à chaque fois est que le modèle canonique est bien construit sur la base d'un système de transition de la classe $\mathscr{C}$ considérée. Dans ce qui suit, nous écrivons $\mathcal{M} \in \mathscr{C}$ pour dire que le système de transition sur lequel est construit le modèle $\mathcal{M}$ est dans la classe $\mathscr{C}$ (un modèle n'est qu'un système de transition muni d'une valuation).

(1) $\mathcal{M}_{\mathbf{K}} \in \mathscr{C}$: il n'y a vraiment rien à montrer dans ce cas-ci, puisque $\mathscr{C}$ désigne la classe de tous les systèmes de transition.

(2) $\mathcal{M}_{\mathbf{K4}} \in \mathscr{C}_{tr.}$
Il faut montrer que pour tout nœud Ξ_0, Ξ_1, Ξ_2 de $\mathcal{M}_{\mathbf{K4}}$, si $\Xi_0 \to \Xi_1$ et $\Xi_1 \to \Xi_2$ alors $\Xi_0 \to \Xi_2$.
La formule $(4) = \Box P \longrightarrow \Box\Box P$ est équivalente à la formule $\neg\Diamond\neg P \longrightarrow \neg\Diamond\neg\neg\Diamond\neg P$, elle-même équivalente à $\Diamond\Diamond\neg P \longrightarrow \Diamond\neg P$. Comme à la fois $\Diamond\Diamond\neg P \longrightarrow \Diamond\neg P \in \Gamma$ et $\Diamond\Diamond\neg P \longrightarrow \Diamond\neg P \in \Xi_0$, et comme Ξ_0 est clos par substitution uniforme, $\Diamond\Diamond\neg\neg\phi \longrightarrow \Diamond\neg\neg\phi$ appartient à Ξ_0. Et donc chaque formule $\Diamond\Diamond\phi \longrightarrow \Diamond\phi$ appartient à Ξ_0.
Par ailleurs, par définition de $\Xi_0 \to \Xi_1$ et $\Xi_1 \to \Xi_2$, étant donnée une formule ϕ quelconque, si $\phi \in \Xi_2$, alors $\Diamond\phi \in \Xi_1$ et $\Diamond\Diamond\phi \in \Xi_0$. Or, Ξ_0 est clos par *modus ponens*, donc si à la fois $\Diamond\Diamond\phi \in \Xi_0$ et $\Diamond\Diamond\phi \longrightarrow \Diamond\phi \in \Xi_0$, alors $\Diamond\phi \in \Xi_0$. Ce qui prouve que pour toute formule ϕ, si $\phi \in \Xi_2$, alors $\Diamond\phi \in \Xi_0$, et par conséquent $\Xi_0 \to \Xi_2$.

(3) $\mathcal{M}_{\mathbf{KD}} \in \mathscr{C}_{n.b.d.}$

Il faut montrer que pour tout nœud Ξ_0 de $\mathcal{M}_{\mathbf{KD}}$, il existe Ξ_1 tel que $\Xi_0 \to \Xi_1$.
D'après le Lemme 290, si $\Diamond\phi \in \Xi_0$, alors il existe Ξ_1 tel que $\Xi_0 \to \Xi_1$ et $\phi \in \Xi_1$. Or l'axiome (D) dit précisément $\Box P \longrightarrow \Diamond P$. Comme Ξ_0 est clos par substitution uniforme, la formule $\Box\top \longrightarrow \Diamond\top$ est dans Ξ_0. Il suffit maintenant de faire appel à la clôture par *modus ponens* de Ξ_0 (qui vérifie nécessairement $\Box\top$) pour obtenir que $\Diamond\top \in \Xi_0$, et donc d'après le Lemme 290, qu'il existe Ξ_1 tel que $\Xi_0 \to \Xi_1$ et $\phi \in \Xi_1$.

(4) $\mathcal{M}_{\mathbf{KD4}} \in \mathscr{C}_{tr.,n.b.d.}$

Ce cas est une conséquence immédiate de (2) et (3).

(5) $\mathcal{M}_{\mathbf{KT}} \in \mathscr{C}_{ref.}$
Il faut montrer que $\Xi \to \Xi$ est vérifié pour tout nœud Ξ de $\mathcal{M}_{\mathbf{KT}}$. La formule $(T) = \Box P \longrightarrow P$ est équivalente à la formule $\neg\Diamond\neg P \longrightarrow P$, elle-même équivalente à $\neg P \longrightarrow \Diamond\neg P$. Comme Ξ est clos par substitution uniforme, la formule $\neg\neg\phi \longrightarrow \Diamond\neg\neg\phi$ est dans Ξ (et ce pour toute formule ϕ). Par conséquent $\phi \longrightarrow \Diamond\phi$ est également dans Ξ. Finalement, comme Ξ est clos par *modus ponens*, pour toute formule ϕ, si $\phi \in \Xi$, alors $\Diamond\phi \in \Xi$, ce qui est la condition nécessaire à la relation $\Xi \to \Xi$.

(6) $\mathcal{M}_{\mathbf{S4}} \in \mathscr{C}_{ref.,tr.}$

Ce cas est une conséquence immédiate de (2) et (5).

(7) $\mathcal{M}_{\mathbf{KB}} \in \mathscr{C}_{sym.}$

Il faut montrer que pour tout couple de nœuds Ξ_0, Ξ_1 de $\mathcal{M}_{\mathbf{KB}}$, si $\Xi_0 \to \Xi_1$ alors $\Xi_1 \to \Xi_0$. Pour cela, il faut montrer que pour toute formule ϕ, si $\phi \in \Xi_0$ alors $\Diamond\phi \in \Xi_1$. Or (B) est l'axiome $P \longrightarrow \Box\Diamond P$. Comme Ξ_0 est clos par substitution uniforme, toutes les formules $\phi \longrightarrow \Box\Diamond\Phi$ sont dans Ξ_0 et donc par clôture par *modus ponens* de θ_0, il apparaît que pour tout $\phi \in \Xi_0$, l'appartenance $\Box\Diamond\Phi \in \Xi_0$ est vérifiée. D'après le

Lemme 289, si $\Xi_0 \to \Xi_1$ alors pour toute formule ψ, si $\Box\psi \in \Xi_0$ alors $\psi \in \Xi_1$. Il retourne donc que pour toute formule $\phi \in \Xi_0$, $\Diamond\Phi \in \Xi_1$. Ce qui est exactement la condition nécessaire pour définir $\Xi_1 \to \Xi_0$.

(8) $\mathcal{M}_{\mathbf{KB4}} \in \mathscr{C}_{sym.,tr.}$

Ce cas est une conséquence immédiate de (2) et (7).

(9) $\mathcal{M}_{\mathbf{KDB}} \in \mathscr{C}_{sym.,n.b.d.}$

Ce cas est une conséquence immédiate de (3) et (7).

(10) $\mathcal{M}_{\mathbf{KTB}} \in \mathscr{C}_{ref.,sym.}$

Ce cas est une conséquence immédiate de (5) et (7).

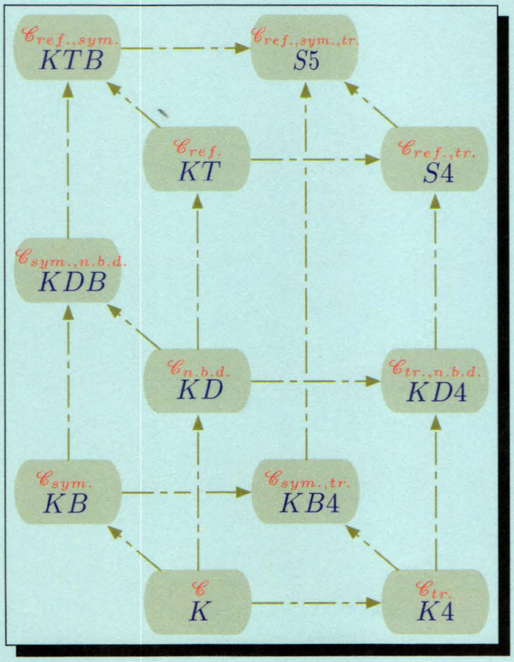
(11) $\mathcal{M}_{\mathbf{S5}} \in \mathscr{C}_{ref.,sym.,tr.}$

Si l'on se souvient que $\vdash_{\mathbf{S5}} P \longrightarrow \Box\Diamond P$ et $\vdash_{\mathbf{S5}} \Box P \longrightarrow \Box\Box P$, alors ce cas devient une conséquence immédiate de (2), (5) et (7).

$\dashv$ 281

Pour terminer ce chapitre, nous présentons dans l'exemple qui suit les correspondances entre systèmes logiques et classes de systèmes de transition.

Exemple 293 La représentation suivante présente la correspondance entre une logique (ou le système formel l'engendrant) et la classe de système de transition pour laquelle solidité et forte complétude sont avérées.



Pour aller plus avant :

Le lecteur intéressé aux résultats de complétude pour les logiques normales pourra se reporter aux ouvrages suivants : *"Modal logic for philosophers"* de James W. Garson [Gar06], *"Modal logic : an introduction to its syntax and semantics"* de Nino B. Cocchiarella et Max A. Freund [CF08], *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03] et, dans une moindre mesure, *"Modal logic : an introduction"* de Brian F. Chellas [Che80].

Pour une lecture plus poussée, il y a l'excellent *"Modal logic"* de Patrick Blackburn, Maarten de Rijke et Yde Venema [BdRV02], ainsi que le *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06].

Chapitre 7

Logiques aléthique, déontique, épistémiques, temporelles, etc.

***Résumé* № 41**

(1) Logique Déontique *(Logique de l'obligation/permission)*
KD : $\mathbf{K} \cup \{(D)\} = \mathbf{K} \cup \{\Box P \longrightarrow \Diamond P\}$.

(2) Logique Aléthique *(Logique de la nécessité/possibilité)*
KTB : $\mathbf{K} \cup \{(T), (B)\} = \mathbf{K} \cup \{\Box P \longrightarrow P, P \longrightarrow \Box\Diamond P\}$.

(3) Logique Epistémique *(Logique de la connaissance)*
S5 = **KT5** : $\mathbf{K} \cup \{(T), (5)\} = \mathbf{K} \cup \{\Box P \longrightarrow P, \Diamond P \longrightarrow \Box\Diamond P\}$.

(4) Logique Temporelle *(Logique du temps discret)*
K4 : $\mathbf{K} \cup \{(4)\} = \mathbf{K} \cup \{\Box P \longrightarrow \Box\Box P\}$.

(5) Logique de la Prouvabilité *(Logique de Gödel-Löb)*
K4GL : $\mathbf{K} \cup \{(4)\} \cup \{(GL)\} =$
$\mathbf{K} \cup \{\Box P \longrightarrow \Box\Box P, \Box(\Box P \longrightarrow P) \longrightarrow \Box P\}$.

※

La logique modale peut être utilisée pour rendre compte des modalités du discours. Ainsi, comme nous l'avons vu, la boîte peut être utilisée pour exprimer le fait qu'un agent sait quelque chose. Le dual de la boîte – le losange – exprimera dès lors le fait que cet agent croit possible cette même chose. D'autres emplois sont courants. Parmi eux, nous en distinguerons deux dans lesquels ni la boîte ni le losange n'est rattaché à un agent. Le premier est celui qui donne la *logique aléthique* : la boîte est interprétée comme l'opérateur de nécessité ; et par conséquent le losange comme celui de possibilité. Le second est celui qui engendre la *logique déontique* : la boîte se rapporte à l'obligation et le losange à la permission.

Ces trois logiques modales différentes donnent lieu entre autre à des carrés des oppositions – semblables à celui d'Aristote. Attardons-nous un instant sur ces différents carrés et leurs significations.

1 La logique aléthique

La logique modale est dite *aléthique* lorsque les modalités sont utilisées pour traduire la nécessité et la possibilité.

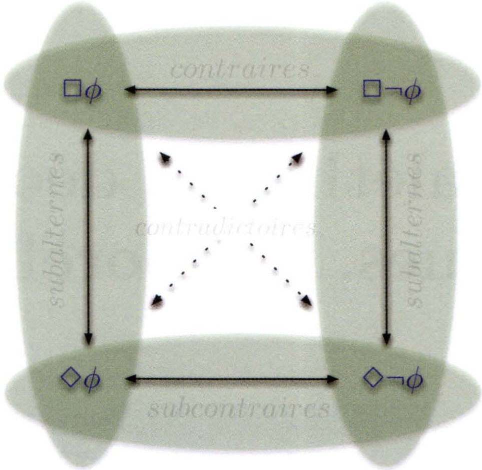


FIGURE 7.1 – Carré des oppositions.

Dans cette logique les différentes formules intervenant dans le carré des oppositions se traduisent par :

- $\Box\phi$: ϕ est nécessaire
- $\neg\Box\phi$: ϕ est contingent [1]
- $\Diamond\phi$: ϕ est possible
- $\neg\Diamond\phi$: ϕ est impossible.

Il existe différentes variantes des logiques aléthiques [2]. Nous choisissons ici de considérer une version de la logique aléthique pour laquelle chaque nœud (a) d'un modèle de Kripke la réalisant doive satisfaire $\mathbf{K} \cup \{\Box P \longrightarrow P, P \longrightarrow \Box\Diamond P\}$. Traduit en mots, cela se dit :

- $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$: "*s'il est nécessaire que P entraîne Q, alors si P est nécessaire, alors Q est nécessaire également*" ;
- $\Box P \longrightarrow P$:"*si P est nécessaire, alors P est réalisé* [3]" ;
- $P \longrightarrow \Box\Diamond P$:"*si P est réalisé, alors il est nécessaire que P soit possible*".

On peut discuter des raisons pour lesquelles on devrait être assujetti à prendre en compte une formule comme $P \longrightarrow \Box\Diamond P$ lorsque l'on souhaite interpréter l'opérateur modal "$\Box$" par la nécessité. Il n'est peut-être pas clair que "*si quelque chose est réalisée, alors il est nécessaire que cette même chose soit possible*". Pourtant, si nous considérons les équivalences suivantes :

$$\begin{aligned} P \longrightarrow \Box\Diamond P &\equiv P \longrightarrow \neg\Diamond\neg\neg\Box\neg P \\ &\equiv P \longrightarrow \neg\Diamond\Box\neg P. \end{aligned}$$

1. Ou plus exactement ϕ n'est pas nécessaire. Car dire que ϕ est contingent présuppose que ϕ est possible. La contingence de ϕ s'énoncerait donc plutôt $\Diamond\phi \wedge \neg\Box\phi$.
2. Nous renvoyons le lecteur vers [Gir00] ainsi qu'à la bibliographie qui est indiquée dans cet ouvrage. Ici nous choisissons de regarder **KTB** : $\mathbf{K} \cup \{(T), (B)\}$.
3. Sous-entendu, dans le monde actuel.

L'énoncé "*si quelque chose est réalisée, alors il est nécessaire que cette même chose soit possible*" se transforme alors en l'énoncé logiquement équivalent "*si quelque chose est réalisée, alors il n'est pas possible que son contraire soit nécessaire*".

Demandons-nous maintenant ce que signifie, en termes de structure des mondes possibles, la contrainte de devoir valider $\Box P \longrightarrow P$ et $P \longrightarrow \Box\Diamond P$ pour une classe de systèmes de transition.

- Un monde possible (a) réalise $\Box P \longrightarrow P$, signifie si P est nécessaire, alors P est réalisé dans le monde dans lequel nous nous trouvons actuellement. Et ce pour n'importe quelle chose que puisse dénoter P. Autrement dit, le système de transition se doit d'être réflexif.
- De même, demander à ce que tout monde possible (a) réalise $P \longrightarrow \Box\Diamond P$ signifie que le système de transition est symétrique.

La classe des systèmes de transition auquel cette logique se restreint est donc celle des systèmes de transition qui sont à la fois réflexifs et symétriques.

Nous retrouvons donc la classe de systèmes de transition $\mathscr{C}_{ref.,sym.}$ pour laquelle le système **KTB** $:= \mathbf{K} \cup \{\Box P \longrightarrow P, P \longrightarrow \Box\Diamond P\}$ vérifiait précisément : $\Gamma \models_{\mathscr{C}_{ref.,sym.}} \phi$ ssi $\Gamma \vdash_{\mathbf{KTB}} \phi$.

Arrêtons nous sur un des exemples les plus fameux et qui remonte à l'origine même de la logique aléthique. Dans *De l'interprétation* (19a30-33), Aristote écrit :

"*Nécessairement il y aura demain une bataille navale ou il n'y en aura pas. Mais il n'est pas nécessaire qu'il y ait demain une bataille navale, pas plus qu'il n'est nécessaire qu'il n'y en ait pas. Mais qu'il y ait ou qu'il n'y ait pas demain une bataille navale, voilà qui est nécessaire.*" [Ari70]

En posant B pour " *il y aura demain une bataille navale*", ces trois assertions se laissent aisément traduire par les formules qui suivent, le monde α de la figure 7.2 forçant la seconde d'entre elles.

(1) $\Box(B \vee \neg B)$; (2) $\neg\Box B \wedge \neg\Box\neg B$; (3) $\Box(B \vee \neg B)$.

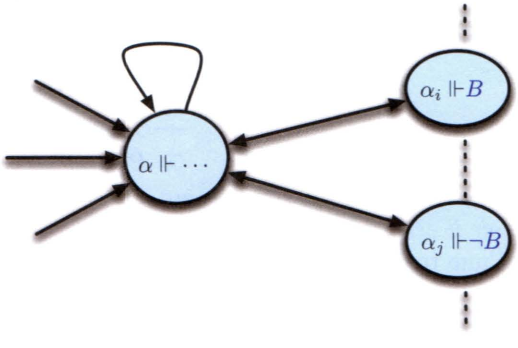


FIGURE 7.2 – Dans le monde α il n'est pas nécessaire qu'il y ait demain une bataille navale, pas plus qu'il n'est nécessaire qu'il n'y en ait pas.

2 La logique déontique

Dans cette logique il s'agit de rendre compte d'énoncés qui portent sur l'obligation d'effectuer quelque chose ou simplement de sa permission.

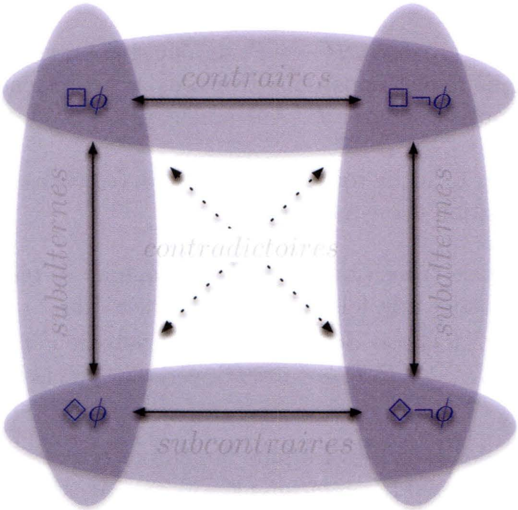


FIGURE 7.3 – Carré des oppositions de la logique déontique.

Les quatre formule du carré des oppositions se traduisent donc par :

- $\Box\phi$: ϕ est obligatoire
- $\neg\Box\phi$: ϕ est facultatif (optionnel)
- $\Diamond\phi$: ϕ est permis
- $\neg\Diamond\phi$: ϕ est interdit.

La logique déontique standard doit vérifier $\mathbf{K} \cup \{\Box P \longrightarrow \Diamond P\}$.

- $\Box(P \longrightarrow Q) \longrightarrow (\Box P \longrightarrow \Box Q)$: "*si P entraîne Q est obligatoire, alors si P est obligatoire, alors Q est obligatoire également*";
- La formule $(D) = \Box P \longrightarrow \Diamond P$ signifie : "*si quelque chose est obligatoire, alors cette chose est permise*". Ou, pour le dire autrement, si l'on remarque que l'on a les équivalences suivantes :
$$\begin{aligned} \Box P \longrightarrow \Diamond P &\equiv \neg\Box P \vee \Diamond P \\ &\equiv \neg\neg\Diamond\neg P \vee \Diamond P \\ &\equiv \Diamond\neg P \vee \Diamond P. \end{aligned}$$
Alors la formule (D) s'exprime au travers de $\Diamond\neg P \vee \Diamond P$ par "*soit il est permis de faire une chose, soit il est permis de ne pas la faire*".
Ou, pour le dire d'une troisième manière, en utilisant les équivalences suivantes :
$$\begin{aligned} \Diamond\neg P \vee \Diamond P &\equiv \neg\Box\neg\neg P \vee \neg\Box\neg P \\ &\equiv \neg\Box P \vee \neg\Box\neg P \\ &\equiv \neg(\Box P \wedge \Box\neg P). \end{aligned}$$
La formule (D) s'exprime encore par "*ne peuvent être obligatoire à la fois une chose et son contraire*". Ou de manière équivalente : "*quelque chose et son contraire ne peuvent être toutes deux interdites*".

$$\begin{aligned}\neg(\Box P \wedge \Box\neg P) &\equiv \neg(\neg\Diamond\neg P \wedge \neg\Diamond\neg\neg P)\\ &\equiv \neg(\neg\Diamond\neg P \wedge \neg\Diamond P)\\ &\equiv \neg(\neg\Diamond P \wedge \neg\Diamond\neg P).\end{aligned}$$

Du point de vue sémantique, une telle logique correspond à la classe $\mathscr{C}_{n.b.d.}$ des systèmes de transition dans lesquels pour tout monde α, il existe une transition qui parte de α vers un monde β – autrement dit, aucun monde n'est une impasse. Un monde qui serait une impasse est un monde dans lequel rien ne serait permis, puisqu'il ne satisferait aucune formule de la forme $\Diamond\phi$. Nous avons donc l'équivalence entre syntaxe et sémantique suivante :

$$\Gamma \models_{\mathscr{C}_{n.b.d.}} \phi \text{ ssi } \Gamma \vdash_{\mathbf{KD}} \phi.$$

Différents paradoxes apparents découlent de cette formalisation de l'obligation et de la permission [Gir00]. Chacun montre soit que cette approche est insuffisante, soit que le paradoxe réside dans le manque d'adéquation entre le langage naturel et les formules de la logique déontique. Nous en mentionnons simplement deux : Le paradoxe de Ross qui peut s'énoncer sous la forme *"s'il est permis d'écrire un livre, il est alors permis d'écrire un livre ou d'en plagier un"* si l'on parle de permission, ou lorsqu'on parle d'obligation par *"s'il est obligatoire de payer ses achats à la caisse du supermarché, alors il est obligatoire de payer ses achats à la caisse du supermarché ou d'assassiner la caissière"* [Ros44]. Pour autant que le second énoncé se traduise par une formule de la forme $\Box P \longrightarrow \Box(P \vee Q)$, il est prouvable sans hypothèse dans cette logique déontique, donc également vérifié en tout nœud de tout modèle de Kripke non borné à droite. Néanmoins, est-ce que l'impression de paradoxe ne provient pas de ce qu'un locuteur écoutant cette dernière phrase, l'entend en fait comme *"s'il est obligatoire de payer ses achats à la caisse du supermarché, alors il est soit obligatoire de payer ses achats à la caisse du supermarché, soit obligatoire d'assassiner la caissière"* – $\Box P \longrightarrow (\Box P \vee \Box Q)$? Ce qui est évidemment invalidé par de très nombreux modèles.

Concernant le paradoxe de Ross, une seconde remarque est que la formule $\Box P \longrightarrow (\Box P \vee \Box Q)$ est logiquement équivalente à la formule $\neg\Diamond\neg P \longrightarrow \neg\Diamond(\neg P \wedge \neg Q)$ qui se traduirait par : *"s'il est interdit de voler le supermarché, alors il est interdit de voler le supermarché et de laisser la caissière en vie"*. On voit à nouveau que lorsqu'on entend cette dernière phrase, on glisse très facilement vers *"s'il est interdit de voler le supermarché, il est non seulement interdit de voler le supermarché mais également de laisser la caissière en vie"*, sous-entendant que ces deux activités sont interdites au même titre.

Un second paradoxe apparent concerne la "violabilité" de l'obligation : pour qu'une action soit obligatoire, il doit être possible de ne pas perpétrer cette action. Sinon à quoi bon rendre celle-ci obligatoire si de toutes façons il n'est pas possible de lui échapper. Ce paradoxe apparent s'exprime dès lors par : *"s'il est logiquement impossible que ϕ soit fausse, alors il est logiquement impossible que ϕ soit obligatoire."* En conséquence *"il est logiquement impossible que $\top$ soit obligatoire"*. Autrement dit, ce qui est universellement valide ne peut être également obligatoire car on ne peut y échapper. C'est le cas précisément de la vérité.

Néanmoins, le caractère paradoxale de cette assertion semble reposer sur un glissement de sens entre trois notions pourtant très différentes : l'implication logique, la nécessité et l'obligation. Le principe de "violabilité" de l'obligation repose sur la *possibilité/nécessité* de sa non réalisation, alors que l'implication logique fait intervenir une *nécessité/possibilité* d'un tout autre type. Tout se passe comme s'il y avait trois types de nécessité différentes qui se retrouvent ici mêlées : la *"nécessité logique"* – qui repose sur la notion de démonstration ou d'universalité via le théorème de complétude –, la *"nécessité aléthique"* – qui s'oppose à la *"la possibilité effective"* –, la *"nécessité déontique"* – autrement dit *"l'obligation"* qui s'oppose à *"la permission"*.

3 Les logiques épistémiques

Les logiques épistémiques s'intéressent à des énoncés portant sur le fait de savoir quelque chose ou de la croire simplement possible. Un agent peut très bien *"croire possible"* quelque chose sans que cette chose soit effectivement possible. Simplement cet agent ne sait pas que cette chose est impossible. Il peut ainsi par exemple croire tout à fait possible que les parents de Barack Obama soient encore tous deux en vie, pour la raison que cet agent n'a pas reçu d'information sur leurs décès. Il est donc envisageable de *"croire possible"* l'*"impossible"*.

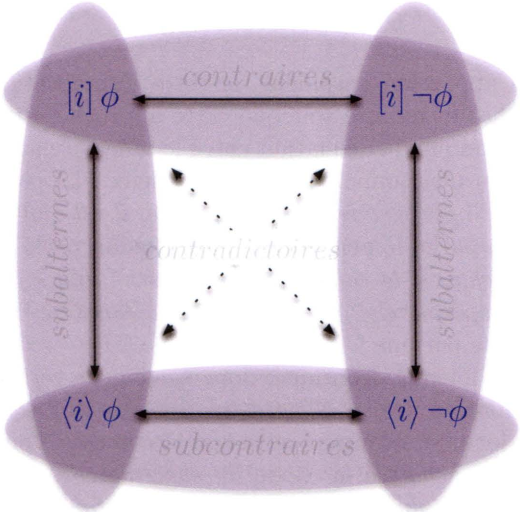


FIGURE 7.4 – Carré des oppositions.

Les quatre formules du carré des oppositions se traduisent par :

- $[i]\phi$: l'agent i sait que ϕ
- $\neg[i]\phi$: l'agent i ne sait pas que ϕ
- $\langle i\rangle\phi$: l'agent i croit possible ϕ
- $\neg\langle i\rangle\phi$: l'agent i ne croit pas possible ϕ.

En fait, il n'existe pas une logique épistémique mais plusieurs. Cette variété des manières de rendre compte de la connaissance se sépare de prime abord en deux groupes en fonction du caractère logiquement omniscient ou non de l'agent épistémique. Un agent qui connait toutes les conséquences logiques des vérités logiques est dit *"fortement logiquement omniscient"*. Si ce n'est pas le cas, on parle alors d'un agent *"faiblement logiquement omniscient"*; et toute la question revient à définir la portée exacte de ce qu'il peut effectivement déduire.

Mais même si l'on s'accorde le postulat de ne considérer que des agents idéaux, en quelque sorte parce qu'ils sont *"fortement logiquement omniscients"*, il reste encore des différences notoires d'une logique épistémique à l'autre. Nous ne présentons ici – et de manière très succincte – que les deux logiques $\mathbf{S_4}$ et $\mathbf{S_5}$.

- Pour la logique épistémique $\mathbf{S_5}$, il est nécessaire que dans tous les mondes possibles soient vérifiées $\mathbf{K} \cup \{[i]P \longrightarrow P, \neg[i]P \longrightarrow [i]\neg[i]P\}$. Autrement dit, il faut que dans un monde quelconque (a) $[i]P \longrightarrow P$ soit réalisé – c'est-à-dire que si l'agent i sait que P, alors P est vrai dans ce monde a. Mais aussi que soit réalisé $\neg[i]P \longrightarrow [i]\neg[i]P$,

ce qui signifie que si l'agent i ne sait pas quelque chose, alors il sait qu'il ne sait pas cette chose. On appelle ce pré-requis le principe d'*introspection négative.*
L'agent de la logique $\mathbf{S_5}$ est une sorte d'agent idéal qui a non seulement accès à toutes les conséquences logiques de ce qui est et de ce qu'il connait, mais également qui fait porter sa connaissance non seulement sur ce dont il a connaissance, mais aussi sur ce qu'il ne sait pas. C'est en somme une espèce d'agent pour lequel l'accès à la connaissance est maximal, sans qu'il ne sache pour autant tout.
La logique $\mathbf{S_5}$ correspond à une sémantique dans laquelle la relation d'accessibilité vérifie des propriétés très fortes, puisqu'elle est une relation d'équivalence :

$$\vdash_{\mathbf{S5}} \phi \text{ ssi } \models_{\mathscr{C}_{ref.,sym.,tr.}} \phi.$$

- Il en va autrement de la logique épistémique $\mathbf{S_4}$. Il est nécessaire que soient vérifiées les mêmes formules que pour la logique $\mathbf{S_5}$, à l'exception notoire de celle exprimant *"l'introspection négative"* qui se voit ici remplacée par *"l'introspection positive"* signifiant que si l'agent i sait quelque chose, alors il sait qu'il le sait et qui s'énonce par $[i]P \longrightarrow [i][i]P$.
  L'agent de la logique $\mathbf{S_4}$ est une sorte d'agent idéal mais qui possède un accès restreint à la connaissance. Il est idéal en ce qu'il conserve une omniscience logique totale. Mais il peut par exemple très bien vivre dans un monde dans lequel Barack Obama n'a pas de sœur [4], donc dans lequel il ne sait pas que Barack Obama a une sœur et pourtant il ne sait pas lui-même qu'il ne sait pas que Barack Obama a une sœur. Il peut ainsi croire possible qu'il sait que Barack Obama a bien une sœur, alors que par ailleurs il ne sait pas qu'il a une sœur. Autrement dit, l'agent de la logique $\mathbf{S_4}$ peut tout à fait croire possible qu'il sait quelque chose que par ailleurs il ne sait pas – ce qui n'est manifestement pas le cas de l'agent de la logique $\mathbf{S_5}$. La raison de cela réside dans les limitations de son pouvoir d'*"introspection négative"*, qui est par contre sans borne pour l'agent de la logique $\mathbf{S_5}$.
  La logique $\mathbf{S_4}$ correspond à une sémantique dans laquelle la relation d'accessibilité est réflexive et transitive mais pas nécessairement symétrique. En d'autres termes, il ne lui manque que la symétrie pour être une relation d'équivalence :

$$\vdash_{\mathbf{S4}} \phi \text{ ssi } \models_{\mathscr{C}_{ref.,tr.}} \phi.$$

4 Les logiques temporelles

Les logiques temporelles sont nombreuses. Elles intéressent à la fois le philosophe et l'informaticien. Le philosophe regarde deux types de temporalité, l'une dirigée vers le passé, l'autre vers l'avenir. Pour l'informaticien, les logiques temporelles permettent de décrire des propriétés que peut ou non satisfaire une machine informatique au cours du temps : Cette machine va-t-elle atteindre à un moment dans le futur un état considéré comme *"bons"*, ou bien va-t-elle toujours éviter des états qui sont *"néfastes"*?

4. Barack Obama a bien effectivement une demi-sœur, mais il n'a pas de sœur – ni de frère d'ailleurs – pour autant.

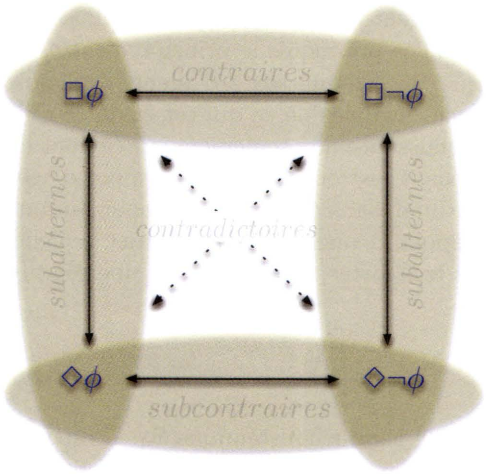


FIGURE 7.5 – Carré des oppositions.

Dans tous les cas des logiques temporelles, le temps auquel on s'intéresse est un temps *"discret"* par opposition au temps *"continu"* des physiciens. Une temporalité discrète est comme une succession de monde possibles tels qu'entre un instant t et un instant t' plus éloigné, il n'y a qu'un nombre fini d'instants différents, alors que dans une conception continue du temps, il y a une infinité d'instants entre t et $t' > t$. A remarquer que le temps discret est réellement le temps dans lequel évolue un processeur informateur, puisqu'il fonctionne avec une horloge qui découpe le temps en pulsations, comme le ferait un cœur artificiel. Sauf que ce cœur bat vraiment très vite. Lorsqu'on parle par exemple d'un processeur avec une fréquence d'horloge de 5.5 GHz (GigaHerz), il s'agit d'une machine pour laquelle chaque seconde est divisée en 5.5 milliards d'entités – comme un cœur qui battrait à 330 milliards de pulsations par minutes.

Le temps discret des logiques temporelles prend soit une forme linéaire, comme dans la figure 7.6, soit une forme arborescente comme dans la figure 7.7.

En tous cas, ce qu'on demande au minimum à la relation d'accessibilité, c'est de satisfaire la transitivité. Elle est donc implicite dans les schémas que nous avons présentés : s'il y a une flèche du monde (a) vers le monde (b) et du monde (b) vers le monde (c), alors il y a une flèche de (a) vers (c). Nous avons simplement omis ces flèches pour des raisons de lisibilité. Le système logique minimal correspondant aux logiques temporelles est donc **K4**, puisque nous avons l'équivalence suivante :

$$\Gamma \vdash_{\mathbf{K4}} \phi \text{ ssi } \Gamma \models_{\mathscr{C}_{tr.}} \phi.$$

Le futur d'un monde est l'ensemble des mondes qui lui sont accessibles. Comme la réflexivité n'est pas réclamée, le monde actuel ne fait pas partie du futur à proprement parlé.

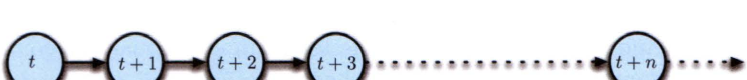


FIGURE 7.6 – Temps linéaire.

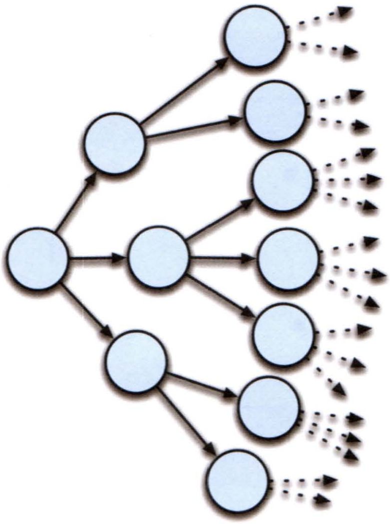


FIGURE 7.7 – Temps arborescent.

Les quatre formules du carré des oppositions se traduisent par :
- $\Box\phi$: ϕ sera toujours vérifiée.
- $\neg\Box\phi$: ϕ ne sera pas toujours vérifiée.
- $\Diamond\phi$: ϕ sera vérifiée à un certain moment.
- $\neg\Diamond\phi$: ϕ ne sera jamais vérifiée.

Dans une telle logique, on peut donc exprimer des énoncés tels que :
- $P \wedge \Box P$: les êtres humains existent actuellement et existeront toujours.
- $\Diamond\Box\neg P$: il y aura un moment dans le futur à partir duquel les êtres humains n'existeront plus jamais.
- $\Diamond(\neg P \wedge \Diamond P)$: il y aura un moment dans le futur où les êtres humains n'existeront pas, mais un moment ultérieur où ils existeront à nouveau.

On peut de la même manière parler du passé. On peut également parler à la fois du passé et du futur. Il suffit pour cela d'introduire deux types d'opérateurs : $[F]$ et $\langle F\rangle$ pour le futur et $[P]$ et $\langle P\rangle$ pour le passé. On retrouve alors de cette manière le fameux opérateur binaire *"until"* des informaticiens qui se définit par $\phi U \psi$: ϕ arrive à tout instant jusqu'à ce que ψ arrive. Cela se traduit dans le formalisme ci-dessus par $[F](\neg\psi \wedge \neg\langle P\rangle\psi) \longrightarrow \phi$ – si ni dans l'instant présent, ni dans un instant passé ψ s'est réalisé, je vois actuellement ϕ se réaliser – ou de manière équivalente : $[F](\neg\psi \wedge [P]\neg\psi) \longrightarrow \phi$ – à chaque instant, tant que je n'ai pas vu ψ se réaliser, je vois ϕ se réaliser.

5 La logique de Gödel-Löb, la logique de la prouvabilité

Il y a différentes logiques de la prouvabilité, celle de Gödel-Löb constituant néanmoins un élément central. L'idée de base est d'interpréter "$\Box\phi$" comme signifiant *"la formule ϕ est prouvable"*. Le fait de pouvoir parler, au sein d'une logique de la prouvabilité, de cette logique remonte aux théorèmes d'incomplétude de Gödel. Pour ces théorèmes, Gödel travaillait dans le cadre de l'arithmétique – de l'arithmétique de Peano (cf. Exemple 399 page 436) très

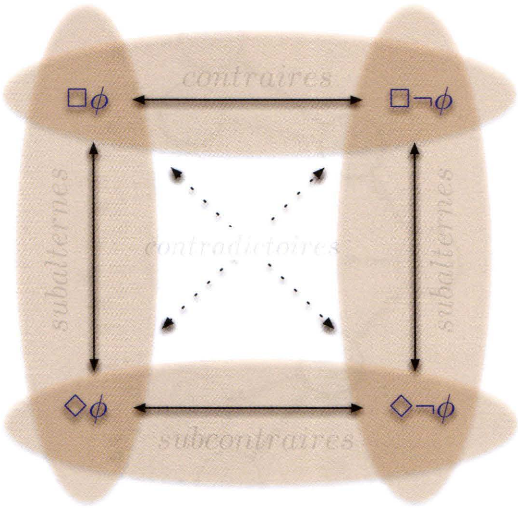


FIGURE 7.8 – Carré des oppositions.

exactement – donc les objets dont parlaient les formules qu'il manipulait était des nombres. Or si un nombre est très différent d'une formule, il est néanmoins possible de rapporter les formules à des nombres : de les *"coder par des nombres"*. La façon la plus immédiate de voir cela est d'écrire cette formule au moyen de son traitement de texte favori – LaTex, Word, etc. – puis de prendre le fichier ainsi constitué. Ce fichier n'est en fait qu'une suite relativement longue $u_0u_1 \dots u_k$ composée uniquement de *"0"* et de *"1"*. De mettre ensuite un *"1"* au début de cette suite : $1u_0u_1 \dots u_k$ et le tour est joué : à partir de la formule, un nombre – entier naturel – est obtenu qui représente le *"code"* de cette formule. Ainsi, les formules de l'arithmétique qui ne parlent que de nombres, peuvent aussi parler de formules de l'arithmétique au moyen de leurs codes. De la même manière que l'on peut coder des formules par des entiers, on peut également coder des arbres de preuves par des entiers[5]. Dès lors une formule peut très bien parler du fait qu'une autre formule est démontrable puisqu'il s'agit de dire qu'il existe un entier possédant les propriétés qui le caractérisent comme étant le code d'une preuve de cette formule. C'est d'ailleurs précisément ce que fait la formule "$\Box\phi$".

Le premier théorème d'incomplétude de Gödel s'appuie sur le fait que pour une formule ϕ, si l'on peut démontrer – dans le cadre de l'arithmétique de Peano formalisée en logique du 1$^{\text{er}}$ ordre[6] – la formule $\neg\Box\phi \longleftrightarrow \phi$, alors la formule ϕ n'est pas démontrable. En faisant un pas de plus et considérant une formule qui dit d'elle-même qu'elle n'est pas démontrable, Gödel obtient que cette formule n'est pas prouvable alors qu'elle est pourtant *"vraie"*.

Si l'on remplace maintenant la formule $\neg\Box\phi \longleftrightarrow \phi$ par la formule $\Box\phi \longleftrightarrow \phi$, la question naturelle devient : que peut-on dire de ces formules ϕ telles que l'on peut prouver le sens difficile de $\Box\phi \longleftrightarrow \phi$, c'est-à-dire $\Box\phi \longrightarrow \phi$?

5. Un arbre de preuve rédigé au moyen de LaTeX par exemple, correspond à un fichier informatique au même titre qu'une formule. Il suffit à nouveau de regarder le fichier engendré par ce traitement de texte, placer un *"1"* au début pour obtenir le nombre désiré.

6. Voir le chapitre III.

La réponse réside dans le théorème de Löb qui dit que ces formules ne sont autres que celles qui sont prouvables – dans l'arithmétique de Peano – ce qui s'énonce :

$$\Box(\Box\phi \longrightarrow \phi) \longrightarrow \Box\phi.$$

La logique de la prouvabilité de Gödel-Löb consiste à partir du système **K** – il est à noter que la formule $(K) = \Box(\phi \longrightarrow \psi) \longrightarrow (\Box\phi \longrightarrow \Box\psi)$ ne décrit rien d'autre que le *modus ponens*[7] – et de lui adjoindre l'axiome $(4) = \Box P \longrightarrow \Box\Box P$ – qui dit que si j'ai une preuve de P alors j'ai une preuve du fait que j'ai une preuve de P – ainsi que le théorème de Löb $(GL) = \Box(\Box P \longrightarrow P) \longrightarrow \Box P$.

Les quatre formules du carré des oppositions se traduisent par :

- $\Box\phi$: ϕ est prouvable.
- $\neg\Box\phi$: ϕ n'est pas prouvable.
- $\Diamond\phi$: $\neg\phi$ n'est pas prouvable.
- $\neg\Diamond\phi$: $\neg\phi$ est prouvable.

Cette logique ne fait pas partie des logiques normales que nous avons étudiées. Pourtant, si nous dénotons par $\mathscr{C}_{tr.,b.d.}$ la classe des modèles de Kripke qui sont à la fois transitifs et vérifient qu'il n'existe pas de suite infinie de la forme

$$a_0 \rightarrow a_1 \rightarrow a_2 \rightarrow \ldots \rightarrow a_n \rightarrow a_{n+1} \rightarrow \ldots,$$

on obtient le théorème de complétude ci-dessous [BPV99] :

$$\Gamma \vdash_{\mathbf{K4GL}} \phi \text{ ssi } \Gamma \models_{\mathscr{C}_{tr.,b.d.}} \phi.$$

Pour aller plus avant :

Le lecteur intéressé en particulier à la logique épistémique trouvera un très grand intérêt à l'ouvrage collectif *"Reasoning about knowledge"* de Ronald Fagin, Joseph Y. Halpern, Yoram Moses, Moshe Y. Vardi *Reasoning about knowledge* [FHMV95]. (Cette lecture pourra le conduire à s'intéresser à un second ouvrage qui dépasse néanmoins très largement le cadre de notre investigation : *"Reasoning about uncertainty"* de Joseph Y. Halpern [Hal03].

Le lecteur pourra également regarder de manière plus anecdotique les livres de Brian F. Chellas *"Modal logic : an introduction"* [Che80] pour le chapitre sur la logique déontique et *"An introduction to non-classical logic"* de Graham Priest [Pri01] pour sa partie sur les logiques temporelles.

Les logiques épistémique, temporelle, déontique, aléthique et d'autres encore se retrouvent dans les ouvrages abordables que sont *"Modal logics and Philosophy"* de Rod Girle [Gir00], *"Modal logic for philosophers"* de James W. Garson [Gar06], *"Modal Logic for Open Minds"* de Johan van Benthem [vB10], ainsi que dans le plus abrupt *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06].

La logique de la probabilité se trouve mentionnée dans les trois derniers ouvrages cités, mais le lecteur désireux d'en savoir plus pourra se reporter aux écrits suivants : le déjà ancien *"The logic of provability"*, de George S. Boolos [Boo95], *"Provability, Complexity, Grammars"* de Lev D Beklemishev, Mati R. Pentus et Nikolai K. Vereshchagin [BPV99] et le plus récent *"Provability logic"*, de Sergei N Artemov et Lev D Beklemishev [AB05].

---

7. Si j'ai une preuve de $\phi \longrightarrow \psi$ et une preuve de ϕ, alors j'ai une preuve de ψ.

Chapitre 8

Un soupçon de logique modale quantifiée

1 Une syntaxe restreinte

***Résumé* № 42** *On ajoute des quantificateurs à la logique modale. Pour cela les formules atomiques que sont les variables propositionnelles sont remplacées par des formules de la forme $P(x)$ ou $P(c)$, où P désigne une propriété que satisfont ou non des individus appelés "éléments". Les formules sont des arbres semblables à ceux qui constituaient les formules de la logique modale excepté pour :*

(1) ***Les feuilles****, qui au lieu d'être de la forme P, Q, R, etc. sont de la forme $P(x)$, $Q(y)$, $R(c)$, etc. où "P, Q, R" désignent des propriétés qui sont attribuées soit à des variables – comme "x" et "y" – soit à des constantes – comme "c".*

(2) ***Les nœuds*** *– autres que les feuilles – qui en plus de pouvoir être de la forme $\wedge, \vee, \longrightarrow, \longleftrightarrow$ avec deux descendants, ou de la forme $\neg, \Box, \Diamond, [i], \langle i \rangle$ avec un descendant, peuvent également être de la forme $\exists x$, $\forall y$ – où "x" et "y" sont des variables quelconques – avec un seul descendant.*

(3) Pour toute feuille de la forme $P(x)$ où "x" est une variable, il existe un ***unique nœud*** *de la forme "$\exists x$" ou "$\forall x$" sur la branche qui mène de la racine à cette feuille.*

※

Ce chapitre ne présente pas la *logique modale quantifiée* dans toute son ampleur. Il se veut simplement un pont entre la logique modale et la logique du 1$^{\text{er}}$ordre afin de permettre d'accéder en douceur au processus de quantification. Le lecteur enthousiasmé par cette extension de la logique modale pourra se reporter en fin de chapitre pour des indications bibliographiques.

1.1 Le langage

Le langage de la logique modale quantifiée restreinte à laquelle nous allons nous intéresser, ressemble fortement à celui de la logique modale. A l'exception des variables propositionnelles, on y retrouve tous les ingrédients de la logique modale construite sur le Calcul Propositionnel : les connecteurs binaires "$\wedge$, $\vee$, $\longrightarrow$, $\longleftrightarrow$", le connecteur unaire "$\neg$" ainsi que les opérateurs de modalité"$[i]$" et "$\langle i\rangle$". Les variables propositionnelles disparaissent et sont remplacées par des objets plus compliqués : les "*formules atomiques*". Au même titre que les variables propositionnelles forment le niveau zéro de toute formule – elles en sont les feuilles – les formules atomiques forment la base de toute formule de la logique modale quantifiée restreinte. Dans la syntaxe restreinte que nous retenons ici, ces formules atomiques sont de deux sortes :

(1) $P(x)$ (2) $P(c)$

Ces formules atomiques doivent se comprendre comme l'attribution d'une certaine propriété – en l'occurrence la propriété "P" – à une variable – désignée par "x" – dans le premier cas, et à une constante – désignée par "c" – dans le second cas. La différence entre variable et constante, comme on peut s'y attendre, est qu'une variable "ça varie", alors qu'une constante "ça reste constant" et par conséquent "ça ne varie pas". La distinction entre les deux deviendra claire lorsque nous aborderons la section consacrée à la sémantique. Pour l'instant il est simplement essentiel que nous distinguions bien entre les *variables* – que nous noterons le plus souvent par les lettres "x", "y" ou "z", ou encore les lettres "x_0", "x_1",..., "x_n",... ; et les symboles de constantes que nous noterons "c" ou encore "c_0", "c_1", "c_2"...

Aux formules atomiques s'ajoutent également les quantificateurs existentiel et universel :

(1) le quantificateur existentiel :"$\exists$" (2) le quantificateur universel :"$\forall$"

Ces quantificateurs n'apparaissent jamais seuls. Ils précèdent toujours une variable. On les verra dès lors se présenter soit sous la forme "$\exists x$", soit sous la forme "$\forall y$". Mais en aucun cas sous la forme "$\exists c$" ni sous la forme "$\forall c$" car les quantificateurs opèrent sur des variables et jamais sur des constantes.

Définition 294 *On appelle* signature *d'un langage de la logique modale quantifiée restreinte $\mathcal{L}$, l'ensemble des symboles de constante et des symboles de priorités que ce langage comporte.*

1.2 Les formules

Définition 295 *Soit $\mathcal{F}$' le plus petit ensemble d'arbres qui*

- *contient chaque arbre réduit à sa racine qui est une formule atomique, et*
- *chaque fois qu'il contient des formules ϕ et ψ contient également les formules suivantes :*

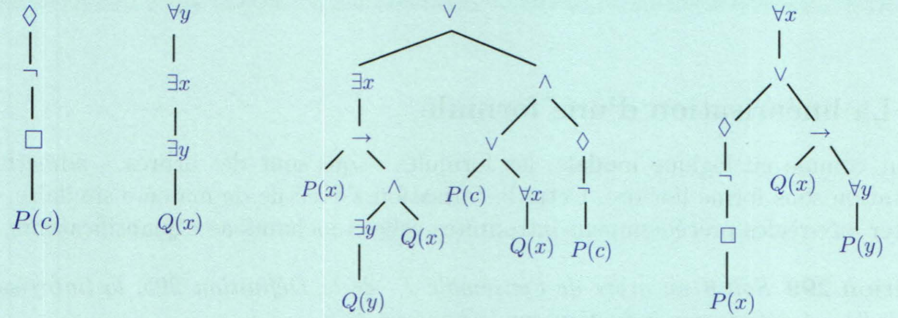
$$\begin{array}{c}[i]\\ |\\ \phi\end{array}, \quad \begin{array}{c}\exists x\\ |\\ \phi\end{array}, \quad \begin{array}{c}\forall x\\ |\\ \phi\end{array}, \quad \begin{array}{c}\langle i\rangle\\ |\\ \phi\end{array}, \quad \begin{array}{c}\neg\\ |\\ \phi\end{array}, \quad \begin{array}{ccc} & \vee & \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \wedge & \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longrightarrow & \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longleftrightarrow & \\ \phi & & \psi\end{array}.$$

L'ensemble $\mathcal{F}$ des formules de la Logique Modale quantifiée restreinte *est l'ensemble de tous les arbres T de $\mathcal{F}$' qui vérifient la propriété suivante :*

- *Pour toute variable x, si $P(x)$ est une feuille de T, alors sur la branche de T qui va de cette feuille à la racine, il existe un unique nœud qui soit de la forme "$\exists x$" ou "$\forall x$".*

De manière usuelle, on définit la hauteur d'une formule comme étant la longueur de sa plus longue branche – ou de ses plus longues branches lorsqu'il y en a plusieurs.

Exemple 296 Trois formules, les deux premières de hauteur 3, les deux suivantes de hauteur 5 :

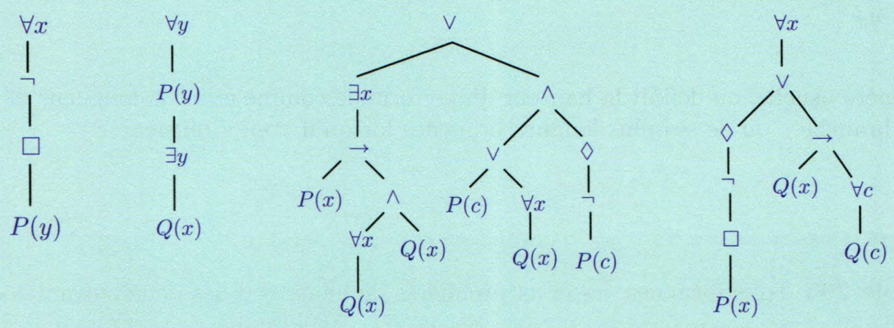


Remarques 297

- D'après notre définition nous pouvons tout à fait avoir des formules de la forme

Même si nous verrons qu'une telle formule est équivalente à la formule $Q(c)$ et que par conséquent les quantificateurs qu'elle contient sont tout à fait inutiles.

Exemple 298 Pourquoi ces arbres ne représentent-ils pas des formules de la logique modale quantifiée restreinte ? [1]



1.3 La linéarisation d'une formule

Tout comme en logique modale, les formules – qui sont des arbres – admettent une présentation sous forme linéaire. Cette linéarisation s'effectue de manière similaire. Il suffit d'ajouter aux règles précédemment introduites celles touchants aux quantificateurs.

Définition 299 *Soit θ un arbre de l'ensemble $\mathcal{F}$' de la Définition 295, la linéarisation de θ (notée $\overline{\theta}$) est définie par induction sur la hauteur de θ.*

ht(θ)**=0** *: dans ce cas θ est une formule atomique soit de la forme $P(c)$, soit de la forme $P(x)$. Dans ce cas $\theta = \overline{\theta} = P(c)$ ou bien $\theta = \overline{\theta} = P(x)$.*

ht(θ)**>0** *:*

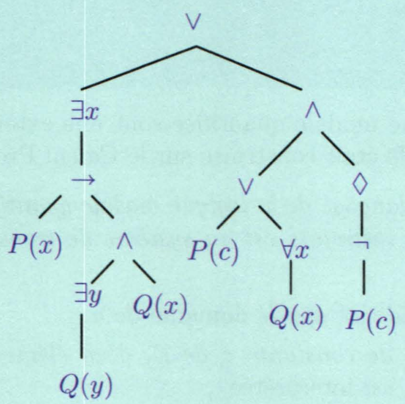
- *si* $\theta = \begin{array}{c}\vee\\ \diagup\diagdown\\ \phi \quad \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \vee \overline{\psi})$,
- *si* $\theta = \begin{array}{c}\langle i\rangle\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \langle i\rangle\,\overline{\phi}$,
- *si* $\theta = \begin{array}{c}\wedge\\ \diagup\diagdown\\ \phi \quad \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \wedge \overline{\psi})$,
- *si* $\theta = \begin{array}{c}\neg\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \neg\overline{\phi}$,
- *si* $\theta = \begin{array}{c}\longrightarrow\\ \diagup\diagdown\\ \phi \quad \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \longrightarrow \overline{\psi})$,
- *si* $\theta = \begin{array}{c}\exists x\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \exists x\overline{\phi}$,
- *si* $\theta = \begin{array}{c}\longleftrightarrow\\ \diagup\diagdown\\ \phi \quad \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \longleftrightarrow \overline{\psi})$,
- *si* $\theta = \begin{array}{c}\forall x\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \forall x\overline{\phi}$,
- *si* $\theta = \begin{array}{c}[i]\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = [i]\overline{\phi}$.

1.
on ne trouve ni $\exists y$ ni $\forall y$ sur l'unique branche qui va de $P(y)$ à la racine ;
on ne trouve ni $\exists x$ ni $\forall x$ sur l'unique branche qui va de $Q(x)$ à la racine ;
sur l'unique branche qui va de l'occurrence la plus à gauche de $Q(x)$ à la racine il y a à la fois $\exists x$ et $\forall x$;
on trouve un nœud $\forall c$.

Exemple 300 La formule ϕ suivante :

se linéarise sous la forme $\overline{\phi} = \neg\exists x \neg\forall z Q(c)$.

Exemple 301 Linéarisation $\overline{\phi}$ de la formule ϕ suivante :



$$\overline{\phi} = \Big(\exists x \Big(P(x) \longrightarrow (\exists y Q(y) \wedge Q(x))\Big) \vee \Big((P(c) \vee \forall x Q(x)) \wedge \Diamond\neg P(c)\Big)\Big).$$

2 Sémantique

Résumé № 43

(1) Les modèles de la logique modale sont des modèles de Kripke *dans lesquels chaque monde possible a est constitué de :*

(a) un domaine *:= un ensemble non vide d'objets, noté $|a|$;*

(b) Pour chaque symbole de constante c *du langage, un élément du domaine de a par lequel* c *est* interprété *:=* c^a *;*

(c) Pour chaque symbole de propriété P du langage, l'interprétation de cette propriété := l'ensemble $P^a \subseteq |a|$ des éléments qui satisfont la propriété P.

(2) L'évaluation d'une formule en un monde a d'un modèle $\mathcal{M}$ s'effectue au moyen d'un jeu d'évaluation identique à celui de la logique modale excepté lorsque $\exists x\phi$ (resp. $\forall x\phi$) est rencontré, auquel cas le **V***érificateur (resp. le* **F***alsificateur) choisit un élément e du monde dans lequel on se trouve et le jeu se poursuit avec ϕ dans laquelle e remplace x. Le jeu se termine lorsqu'on atteint une "formule" atomique de la forme $P(\mathsf{c})$ où $P(e)$, dont le modèle indique si elle est vérifiée ou non, désignant ainsi le vainqueur.*

※

Les modèles de la logique modale quantifiée sont une extension des modèles de Kripke de la logique modale (qui elle était construite sur le Calcul Propositionnel).

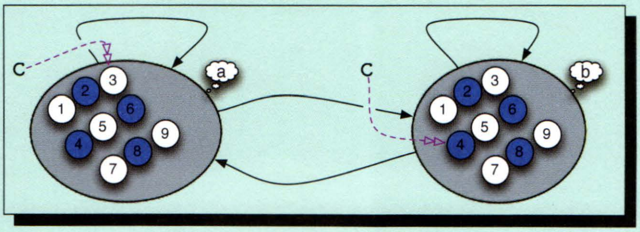
Définition 302 *Soit $\mathcal{L}$ un langage de la logique modale quantifiée. Un modèle de Kripke de la logique modale quantifiée restreinte est un système de transition $\mathcal{S}$ dont chaque nœud " a" est la donnée :*

(1) d'un ensemble non vide $|a|$ appelé domaine *de a ;*

(2) pour chaque symbole de constante c *de $\mathcal{L}$, d'un élément* c^a *du domaine de a (par lequel cette constante est* interprétée*) ;*

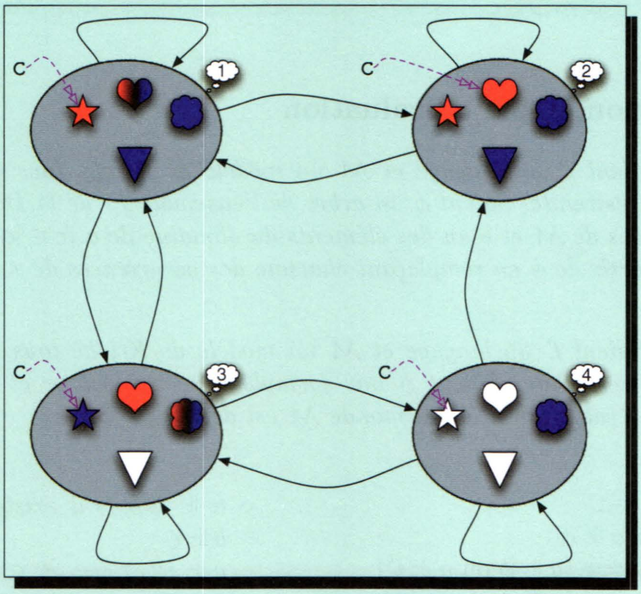
(3) Pour chaque symbole de propriété P de $\mathcal{L}$, d'un ensemble $P^a \subseteq |a|$ (l'ensemble des éléments qui satisfont cette propriété).

Exemple 303 Un modèle de Kripke de la logique modale quantifiée avec pour signature le symbole de constante c et le symbole de propriété P. Dans chacun des 2 mondes possibles a et b, les éléments qui vérifient la propriété P sont coloriés en bleu.



On voit que dans chacun des mondes a et b, ce sont les nombres pairs qui vérifient la propriété P. Dans le premier monde le symbole de constante c est interprétée par ③ ($\mathsf{c}^a =$ ③), alors que dans le second monde c est interprétée par ④ ($\mathsf{c}^b =$ ④).

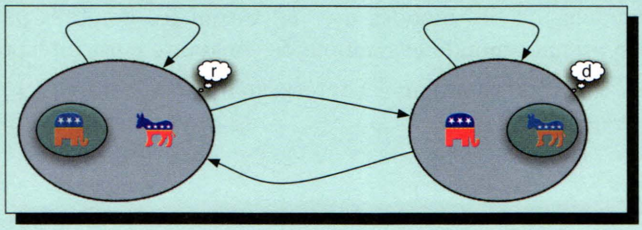
Exemple 304 Un modèle de Kripke de la logique modale quantifiée avec pour signature le symbole de constante c et les symboles de propriété P et Q. Dans chacun des 4 mondes possibles $1, 2, 3, 4$ les éléments qui vérifient la propriété P sont coloriés en rouge, ceux qui vérifient la propriété Q sont coloriés en bleu.



On voit ainsi que l'élément  satisfait la propriété P dans les mondes $1, 2$ et 3. Ce même élément satisfait la propriété Q dans le seul monde 1. Alors que l'élément  satisfait la propriété P dans le monde 3, et la propriété Q dans tous les mondes.

Le symbole de constante c est interprété par  dans les mondes $1, 3$ et 4, mais par  dans le monde 3.

Exemple 305 Un modèle de Kripke de la logique modale quantifiée avec pour signature le seul symbole de propriété P. Chacun des deux mondes possibles r et d a pour domaine les deux éléments  et . Dans le monde r, seul  vérifie la propriété P ; alors que dans le monde d, seul  vérifie P.



On pourra penser que les deux éléments représentent les prochains candidats républicain et démocrate à l'élection présidentielle ; la propriété P caractérisant le fait de devenir président. Dans le monde r (pour "républicain") le candidat républicain emporte les élections, alors que dans le monde d (pour "démocrate") c'est le candidat démocrate qui l'emporte.

2.1 Satisfaction et jeu d'évaluation

Notation 306 *Soient $\mathcal{L}$ un langage et $\mathcal{M}$ un modèle de Kripke tous deux de la logique modale quantifiée restreinte. Soient ϕ un arbre de l'ensemble $\mathcal{F}$' de la Définition 295, a un des mondes possibles de $\mathcal{M}$ et e un des éléments du domaine de a ($e \in |a|$). On note $\phi[e/x]$ l'arbre obtenu à partir de ϕ en remplaçant chacune des occurrences de x par e.*

Définition 307 *Soient $\mathcal{L}$ un langage et $\mathcal{M}$ un modèle de Kripke tous deux de la logique modale quantifiée restreinte. Soient ϕ une formule de cette logique et a un des mondes possibles de $\mathcal{M}$. L'évaluation de ϕ au monde $\mathcal{M}$ est définit par :*

- $a \Vdash \top$ *et* $a \nVdash \bot$
- $a \Vdash \neg\phi \iff a \nVdash \phi$
- $a \Vdash (\phi \vee \psi) \iff (a \Vdash \phi$ ou $a \Vdash \psi)$
- $a \Vdash (\phi \wedge \psi) \iff (a \Vdash \phi$ et $a \Vdash \psi)$
- $a \Vdash (\phi \longrightarrow \psi) \iff (a \nVdash \phi$ ou $a \Vdash \psi)$
- $a \Vdash (\phi \longleftrightarrow \psi) \iff (a \Vdash \phi$ ssi $a \Vdash \psi)$
- $a \Vdash [i]\phi$ *si pour tout* b *t.q.* $a \xrightarrow{i} b$, $b \Vdash \phi$
- $a \Vdash \langle i \rangle \phi$ *s'il existe* b *t.q.* $a \xrightarrow{i} b$ *et* $b \Vdash \phi$
- $a \Vdash P(\mathsf{c}) \iff \mathsf{c}^a \in P^a$ *(c constante)*
- $a \Vdash P(e) \iff e \in P^a$ *(pour $e \in |a|$)*
- $a \Vdash \exists x\phi$ *s'il existe* $e \in |a|$, $a \Vdash \phi[e/x]$
- $a \Vdash \forall x\phi$ *si pour tout* $e \in |a|$, $a \Vdash \phi[e/x]$.

La satisfaction d'une formule se décline également sous la forme d'un jeu d'évaluation très semblable à celui qui a cours en logique modale. Ce jeu à deux joueurs et à information parfaite est fini. Par conséquent, c'est un jeu qui est déterminé.

Définition 308 *Soient $\mathcal{L}$ un langage et $\mathcal{M}$ un modèle de Kripke tous deux de la logique modale quantifiée restreinte. Soient ϕ une formule de cette logique dont les connecteurs sont parmi $\{\neg, \vee \wedge\}$ et a un des mondes possibles de $\mathcal{M}$. Le jeu d'évaluation $\mathbb{E}v(\langle \mathcal{M}, a \rangle, \phi)$ comprend deux joueurs appelés* **V**érificateur *et* **F**alsificateur. *Il est défini comme suit*[2] *:*

2. Dans le tableau, la lettre b désigne un des mondes du modèle $\mathcal{M}$.

si la position actuelle du jeu est...	*c'est au tour de...*	*le jeu continue avec...*
$(b, (\varphi_0 \lor \varphi_1))$	**V** *choisit* $j \in \{0, 1\}$	(b, φ_j)
$(b, (\varphi_0 \land \varphi_1))$	**F** *choisit* $j \in \{0, 1\}$	(b, φ_j)
$(b, \neg\varphi)$	**F** *et* **V** *échangent leurs rôles*	(b, φ)
$(b, \langle i \rangle \varphi)$	**V** *choisit* c *tel que* $a \xrightarrow{i} c$	(c, φ)
$(b, [i]\varphi)$	**F** *choisit* c *tel que* $a \xrightarrow{i} c$	(c, φ)
$(b, \exists x\varphi)$	**V** *choisit* $e \in \|b\|$	$(c, \varphi[e/x])$
$(b, \forall x\varphi)$	**F** *choisit* $e \in \|b\|$	$(c, \varphi[e/x])$
$(b, P(\mathsf{c}))$	*Stop*	**V** *gagne ssi* $\mathsf{c}^b \in P^b$
$(b, P(e))$	*Stop*	**V** *gagne ssi* $e \in P^b$

Remarque 309

(1) Tout comme dans le cadre de la logique modale, il est important de remarquer que lorsqu'un joueur ne peut choisir un monde possible, ce joueur perd alors la partie ! Cette règle du jeu est nécessaire pour que dans un monde *"a"* dont aucune flèche pour l'agent i ne parte les formules de la forme $[i]\phi$ soient réalisées et celles de la forme $\langle i \rangle \phi$ ne le soient pas.

(2) La sémantique que nous avons adoptée a cela d'étrange qu'un élément du domaine peut être choisi dans un monde, puis ce même élément peut faire partie d'une formule atomique qui sera évaluée dans un monde dans lequel cet élément a disparu. C'est par exemple le cas avec la formule $\exists x \Diamond P(x)$. Imaginons qu'elle soit évaluée au monde a, que le **V**érificateur y choisisse l'élément e, puis se déplace dans le monde b dans lequel cet élément n'existe pas. La formule $P(e)$ ne sera pas vérifiée en b puisque $e \notin P^b$.
Le plus souvent, on cherche à éliminer ce cas de figure. Pour cela, on renforce la définition de modèle de Kripke en ajoutant une hypothèse sur les domaines : on demande à ce que pour tous mondes a, b tels que b soit accessible depuis a, le domaine de b contienne le domaine de a :

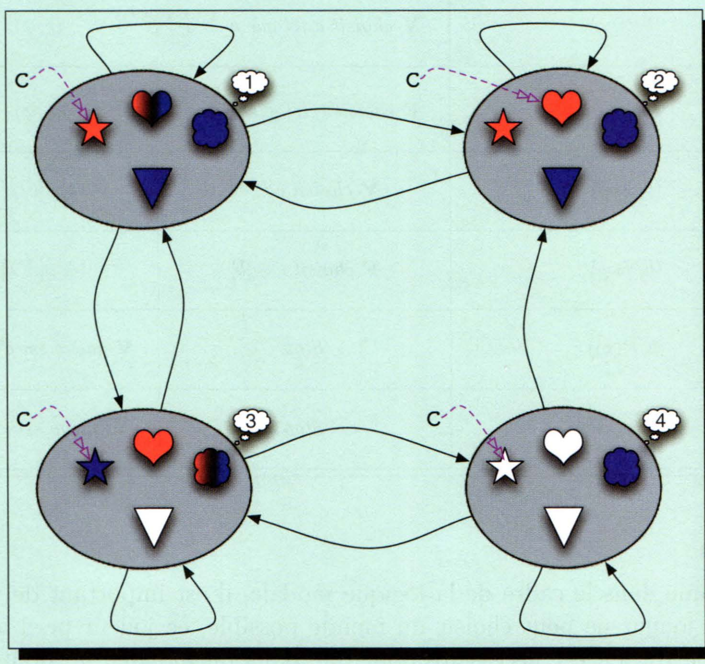
$$a \xrightarrow{i} b \Longrightarrow |a| \subseteq |b|.$$

(3) Une hypothèse encore plus forte sur les domaines consiste à exiger que ceux-ci soient constants. Dèslors, les domaines de chacun des mondes possibles d'un modèle de

Kripke sont tous identiques. Cela correspond, par exemple dans le cas de la logique épistémique, à exiger que les domaines soient connaissance commune parmi les agents.

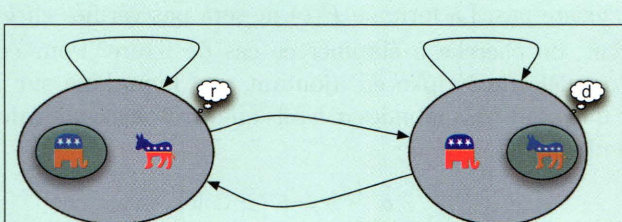
Exemple 310 Le modèle de Kripke de la logique modale quantifiée ci-dessous – où les éléments vérifiant la propriété P, resp. Q, sont coloriés en rouge, resp. en bleu – on vérifie :

- $1 \Vdash \exists x(P(x) \wedge Q(x))$
- $2 \Vdash \exists x P(x) \wedge \exists y \neg P(y)$
- $3 \Vdash \exists x\big(Q(x) \wedge \Diamond P(x)\big)$
- $3 \Vdash \forall x \Diamond Q(x)$
- $3 \nVdash \Diamond \forall x Q(x)$
- $4 \Vdash \Box \exists x Q(x)$
- $4 \nVdash \exists x \Box Q(x)$
- $1 \Vdash \Diamond P(\mathsf{c}) \wedge \Diamond Q(\mathsf{c})$
- $3 \Vdash \Diamond \neg P(\mathsf{c}) \wedge \Diamond \neg Q(\mathsf{c})$



Exemple 311 Dans le modèle ci-dessous :

- $r \Vdash \Box \exists x P(x)$
- $r \nVdash \exists x \Box P(x)$
- $d \Vdash \Box \exists x P(x)$
- $d \nVdash \exists x \Box P(x)$



Formule de Barcan

Nous allons nous pencher sur une formule qui a suscité de nombreuses controverses dans le monde philosophique. En termes de sémantique des mondes possibles, la validité universelle de cette formule implique que tous les objets qui existent dans quelque monde possible que ce soit – accessible depuis le monde réel – existent également dans le monde réel. Autrement dit, les domaines des mondes possibles restent constants et ne croissent pas.

$$\forall x \Box \phi \to \Box \forall x \phi.$$

"Si toute chose est nécessairement ϕ, alors il est nécessaire que chaque chose soit ϕ".

Cette formule est équivalente à la formule suivante :

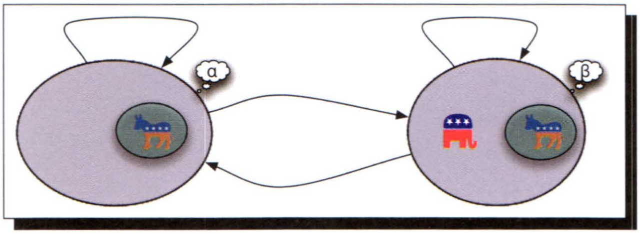
$$\Diamond \exists x \phi \to \exists x \Diamond \phi.$$

"S'il est possible qu'il existe quelque chose satisfaisant ϕ, alors il existe quelque chose qui possiblement satisfait ϕ".

On vérifiera aisément que

(1) dans les modèles de Kripke dont les domaines sont constants, la formule de Barcan est vraie en tout monde.

(2) Par contre, ce n'est pas toujours le cas si les domaines ne sont pas constants, quand bien même ils respecteraient la règle d'inclusion $a \xrightarrow{i} b \Longrightarrow |a| \subseteq |b|$, comme le montre l'exemple suivant.



On a en effet, $\alpha \Vdash \forall x \Box P(x)$, mais $\alpha \nVdash \forall x \Box \phi \to \Box \forall x \phi$.

Les désignateurs rigides

On dit qu'un symbole de constante c est un *désignateur rigide* lorsque ce symboles de constante est interprétée par le même élément dans chacun des mondes possibles. Un célèbre exemple tiré de la littérature philosophique montre qu'il est parfois nécessaire de considérer des désignateurs qui ne sont pas rigides.

- La planète Vénus était dénommée "étoile sur soir" (*Hesperus*) car c'était le premier astre à luire à l'ouest, lorsque le soleil se couche. Mais était également dénommée "étoile sur matin" (*Phosphorus*) pour être la dernière à disparaitre à l'est au petit matin.
- Les astronomes de l'antiquité ne savaient pas que ces deux étoiles n'en faisaient qu'une. En l'occurrence une représentation en terme de modèle de Kripke du monde antique et du monde moderne se doit d'interpréter les deux symboles de constantes $\mathsf{c}_{Hesperus}$ et $\mathsf{c}_{Phosphorus}$ par deux éléments distincts dans le monde antique, mais par le même élément dans le monde moderne.

Pour aller plus avant :

Comme nous l'avons précisé au début de ce chapitre, nous nous sommes intéressé à une version extrêmement restrictive de la logique modale quantifiée. Lecteur qui souhaiterait retrouver une version *"light"* de la logique modale quantifiée pourra lire avec intérêt *"A new introduction to modal logic"* de Max J. Cresswell et George E. Hughes [CH03] ou picorer quelques idées dans *"An introduction to non-classical logic"* de Graham Priest [Pri01].

Le lecteur qui souhaiterait par contre se confronter à la logique modale quantifiée dans toute sa plénitude trouvera matière à nourrir sa réflexion dans *"Modal logics and Philosophy"* de Rod Girle [Gir00], *"Modal Logic for Open Minds"* de Johan van Benthem [vB10] et tout particulièrement dans *"Modal logic for philosophers"* de James W. Garson [Gar06]. Il trouvera également une mine d'information dans le le très ardu *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06].

Ce chapitre étant le moyen d'introduire le lecteur à la quantification,

Le lecteur notera que la quantification introduite dans ce chapitre ne porte que soit sur un individu, soit sur tous les individus, alors que dans le langage courant on utilise des expressions comme "il y a des hommes qui encerclent la maison" pour lesquelles aucun des quantificateurs "$\exists$" ou "$\forall$" ne conviennent. Le lecteur intrigué par cette question consultera avec profit l'ouvrage *"Plural predication"* de Thomas J. McKay [McK06].

Troisième partie

Logique du 1er ordre

Chapitre 9

Préambule

L'idée de la *logique du 1er ordre*, encore appelée *Logique des Prédicats* ou même *Calcul des Prédicats*, trouve ses origines dans la notion de quantification. Prenons comme exemple l'un des syllogismes les plus classiques :

Tous les hommes sont mortels,
Socrate est un homme,
donc Socrate est mortel

Il est quasi impossible de rendre compte de ce raisonnement avec les moyens mis à notre disposition par le Calcul Propositionnel. Les deux raisons essentielles sont :

(1) Chacun des trois énoncés fait référence à certaines propriétés (l'humanité et le fait d'être mortel) qui sont attribuées soit à Socrate, soit aux hommes en général. Or, en Calcul Propositionnel, une variable ne peut pas permettre d'énoncer une propriété que l'on peut attribuer à une personne tout d'abord et à une autre ensuite. Le fait que Socrate soit mortel sera traduit par P et le fait que tous les hommes soient mortels par Q. Ce faisant, on perd l'essentiel de ce raisonnement.

(2) Les deux dernières assertions attribuent des propriétés au personnage Socrate, alors que la première le fait non pas en visant une personne particulière, mais toutes les personnes qui satisfont la propriété d'être humain.

Si l'on voulait interpréter ce raisonnement dans le cadre de la théorie naïve des ensembles, on considérerait deux ensembles : $H^{\mathcal{M}}$ pour l'ensemble des hommes (ou, pour le dire autrement, $H^{\mathcal{M}}$ pour la relation unaire "être un homme") et $M^{\mathcal{M}}$ pour l'ensemble des êtres mortels. Puis, on considérerait un élément s pour Socrate. Ce raisonnement devenant :

$H^{\mathcal{M}} \subseteq M^{\mathcal{M}}$,
$Socrate \in H^{\mathcal{M}}$,
donc $Socrate \in M^{\mathcal{M}}$

Mais on voit bien que dans cette présentation, la quantification universelle (*tous les hommes...*) est implicite. Car dire $H^{\mathcal{M}} \subseteq M^{\mathcal{M}}$, c'est dire que tous les éléments qui sont dans $H^{\mathcal{M}}$ sont dans $M^{\mathcal{M}}$.

La logique du 1er ordre répond à ces deux exigences. Un tel raisonnement sera formalisé de la manière suivante :

(1) de manière syntaxique par la formule :

$$\Big(\forall x\ (\mathsf{H}(x) \longrightarrow \mathsf{M}(x))\ \wedge\ \mathsf{H}(\mathsf{s})\Big)\ \longrightarrow\ \mathsf{M}(\mathsf{s})$$

ou encore en Déduction Naturelle :

$$\forall x\ (\mathsf{H}(x) \longrightarrow \mathsf{M}(x)),\ \mathsf{H}(\mathsf{s})\ \vdash\ \mathsf{M}(\mathsf{s})$$

(2) de manière sémantique, par la donnée d'un modèle $\mathcal{M}$ dont les éléments sont l'ensemble $|\mathcal{M}|$ des êtres vivants, dans lequel les symboles de relation unaire H et M seront interprétés respectivement par les relations unaires , $H^{\mathcal{M}}$ et $M^{\mathcal{M}}$, et le symbole de constante s sera interprété par l'individu Socrate.

1 Une première approche

Afin d'entrer plus avant dans la logique du 1er ordre, nous allons définir un modèle particulier qui nous permettra de présenter les différents ingrédients de cette logique.

Intéressons-nous donc aux étudiants présents dans l'auditoire. L'ensemble de ces étudiants forme ce que l'on appelle le *domaine* de notre modèle. C'est celui sur lequel nos variables pourront... euh ! Comment dire ?.. C'est cela, oui : varier ! Cela signifie que lorsque nous écrirons $\exists x\phi$, nous voudrons dire qu'il existe un étudiant dans cet auditoire qui vérifie ce que raconte ϕ. Et lorsque nous écrirons $\forall x\phi$, cela signifiera que tous les étudiants de l'auditoire vérifient ϕ. Le domaine que nous avons choisi est homogène, il ne comporte que des étudiants. Mais cela n'est pas nécessaire. En toute généralité, un domaine est un ensemble de tout et n'importe quoi. Il peut très bien contenir des pommes et des poires, des nombres et des sentiments, des livres et des idées abstraites, y compris les objets mêmes de la logique (mais ça c'est une autre histoire).

Les formules de la logique du 1er ordre vont donc raconter des choses à propos des étudiants. Pour ce faire, examinons rapidement quelles sont les propriétés – que vérifie ou non un étudiant – sur lesquelles nous souhaitons nous arrêter. En guise d'exemple prêtons une oreille discrète et écoutons ce que disent les étudiants d'eux-mêmes :

- Il y en a un qui travaille dur, mais il ne passera pas.
- Il y en a un qui n'est jamais là, par contre il passera.
- Tu as remarqué qu'Armand avait les yeux bleus ?
- Oui, et Béatrice a les yeux verts.
- Non ! Béatrice a les yeux marrons.
- En fait, elle a les yeux à la fois verts et marrons.
- Armand est en HEC n'est-ce pas ?
- Oui, et Béatrice est en philo.
- Mais Béatrice, elle n'a pas de laptop. Armand en a un, lui.
- Armand, il est plein aux as.
- Ouais. Mais n'empêche que c'est pas un vantard, Armand.
- Béatrice non plus !
- Ouais. Mais Béatrice, elle est exceptionnelle.
- D'ailleurs, Béatrice c'est la plus grande de tous les étudiants de philo.

– Ouais, et Armand ce n'est pas le plus gros de tous les étudiants de HEC.
– Par contre Béatrice n'est pas plus grande qu'Armand.
– Il y a au moins un étudiant de HEC qui la dépasse.
– Elle n'est pas plus riche qu'Armand non plus.
– Oui, mais elle est plus sympa.
– Et aussi plus jolie !
– En tout cas, Armand il travaille moins que Charles-Edouard et il est bien meilleur.
– Ils n'ont pas le même âge.
– Par contre Armand et Béatrice ; ils ont le même âge tous les deux.
– Ceci-dit Charles-Edouard est amoureux de Béatrice.
– Ouais, mais Béatrice, elle, elle ne l'aime pas du tout.

On y reconnaît aisément les propriétés suivantes que nous notons comme des relations unaires :

(1) $P_{\text{travailler dur}}(\_)$	(5) $P_{\text{avoir les yeux verts}}(\_)$	(9) $P_{\text{avoir un laptop}}(\_)$
(2) $P_{\text{réussir l'examen}}(\_)$	(6) $P_{\text{avoir les yeux marrons}}(\_)$	(10) $P_{\text{être riche}}(\_)$
(3) $P_{\text{être régulier au cours}}(\_)$	(7) $P_{\text{être en HEC}}(\_)$	(11) $P_{\text{être vantard}}(\_)$
(4) $P_{\text{avoir les yeux bleus}}(\_)$	(8) $P_{\text{être en philo}}(\_)$	(12) $P_{\text{être exceptionnel}}(\_)$.

On y reconnaît aussi les relations binaires suivantes :

(1) $R_{\text{être plus grand que}}(\_,\_)$	(4) $R_{\text{être plus sympa que}}(\_,\_)$	(7) $R_{\text{travailler moins que}}(\_,\_)$
(2) $R_{\text{être plus gros que}}(\_,\_)$	(5) $R_{\text{être plus joli que}}(\_,\_)$	(8) $R_{\text{avoir le même âge que}}(\_,\_)$
(3) $R_{\text{être plus riche que}}(\_,\_)$	(6) $R_{\text{être meilleur que}}(\_,\_)$	(9) $R_{\text{être amoureux de}}(\_,\_)$.

On reconnaît aussi, au milieu des étudiants, trois personnes qui ont été singularisées. Il y a Béatrice, Armand et Charles-Edouard. Bien sûr, chaque étudiant possède un prénom et une identité. Mais eux seuls peuvent être nommés grâce au vocabulaire dont nous disposons. Nous dirons que les mots "*Béatrice*", "*Armand*" et "*Charles-Edouard*" fonctionnent comme des *symboles de constantes*. Ce sont comme des marqueurs qui permettent dans le langage d'identifier certains éléments de notre domaine. Nous les notons comme des symboles de constantes :

(1) c_A	(2) c_B	(3) c_C

– Il y en a un qui travaille dur, mais il ne passera pas.

$$\exists x(P_{\text{travailler dur}}(x) \wedge \neg P_{\text{réussir l'examen}}(x)).$$

– Il y en a un qui n'est jamais là, par contre il passera.

$$\exists x(\neg P_{\text{être régulier au cours}}(x) \wedge P_{\text{réussir l'examen}}(x)).$$

– Tu as remarqué qu'Armand avait les yeux bleus ?

$$P_{\text{avoir les yeux bleus}}(\mathsf{c}_\mathsf{A}).$$

– Oui, et Béatrice a les yeux verts.

$$P_{\text{avoir les yeux verts}}(\mathsf{c}_\mathsf{B}).$$

– Non ! Béatrice a les yeux marrons.

$$P_{\textsf{avoir les yeux marrons}}(\mathsf{c_B}).$$

– En fait, elle a les yeux à la fois verts et marrons.

$$\Big(P_{\textsf{avoir les yeux verts}}(\mathsf{c_B}) \wedge P_{\textsf{avoir les yeux marrons}}(\mathsf{c_B})\Big).$$

– Armand est en HEC n'est-ce pas ?

$$P_{\textsf{être en HEC}}(\mathsf{c_A}).$$

– Oui, et Béatrice est en philo.

$$P_{\textsf{être en philo}}(\mathsf{c_B}).$$

– Mais Béatrice, elle n'a pas de laptop. Armand en a un, lui.

$$\Big(\neg P_{\textsf{avoir un laptop}}(\mathsf{c_B}) \wedge P_{\textsf{avoir un laptop}}(\mathsf{c_A})\Big).$$

– Armand, il est plein aux as.

$$P_{\textsf{être riche}}(\mathsf{c_A}).$$

– Ouais. Mais n'empêche que c'est pas un vantard, Armand.

$$\neg P_{\textsf{être vantard}}(\mathsf{c_A}).$$

– Béatrice non plus !.

$$\neg P_{\textsf{être vantard}}(\mathsf{c_B}).$$

– Ouais. Mais Béatrice, elle est exceptionnelle.

$$P_{\textsf{être exceptionnel}}(\mathsf{c_B}).$$

– D'ailleurs, Béatrice c'est la plus grande de tous les étudiants de philo.

$$\forall x\Big(P_{\textsf{être en philo}}(x) \longrightarrow R_{\textsf{être plus grand que}}(\mathsf{c_B}, x)\Big).$$

– Ouais, et Armand ce n'est pas le plus gros de tous les étudiants de HEC.

$$\neg\forall x\Big(P_{\textsf{être en HEC}}(x) \longrightarrow R_{\textsf{être plus gros}}(\mathsf{c_A}, x)\Big)$$
$$\equiv$$
$$\exists x\neg\Big(P_{\textsf{être en HEC}}(x) \longrightarrow R_{\textsf{être plus gros}}(\mathsf{c_A}, x)\Big)$$
$$\equiv$$
$$\exists x\neg\Big(\neg P_{\textsf{être en HEC}}(x) \vee R_{\textsf{être plus gros}}(\mathsf{c_A}, x)\Big)$$
$$\equiv$$
$$\exists x\Big(\neg\neg P_{\textsf{être en HEC}}(x) \wedge \neg R_{\textsf{être plus gros}}(\mathsf{c_A}, x)\Big)$$
$$\equiv$$
$$\exists x\Big(P_{\textsf{être en HEC}}(x) \wedge \neg R_{\textsf{être plus gros}}(\mathsf{c_A}, x)\Big).$$

– Par contre Béatrice n'est pas plus grande qu'Armand.

$$\neg R_{\text{être plus grand}}(\mathsf{c_B}, \mathsf{c_A})\Big).$$

– Il y a au moins un étudiant de HEC qui la dépasse.

$$\exists x\Big(P_{\text{être en HEC}}(x) \wedge R_{\text{être plus grand}}(x, \mathsf{c_B})\Big).$$

– Elle n'est pas plus riche qu'Armand non plus.

$$\neg R_{\text{être plus riche}}(\mathsf{c_B}, \mathsf{c_A}).$$

– Oui mais elle est plus sympa.

$$R_{\text{être plus sympa}}(\mathsf{c_B}, \mathsf{c_A}).$$

– Et aussi plus jolie !

$$R_{\text{être plus joli}}(\mathsf{c_B}, \mathsf{c_A}).$$

– En tout cas, Armand il travaille moins que Charles-Edouard et il est bien meilleur.

$$\Big(R_{\text{travailler moins}}(\mathsf{c_A}, \mathsf{c_C}) \wedge R_{\text{être meilleur}}(\mathsf{c_A}, \mathsf{c_C})\Big).$$

– Ils n'ont pas le même âge.

$$\neg R_{\text{avoir le même âge}}(\mathsf{c_A}, \mathsf{c_C}).$$

– Par contre Armand et Béatrice ; ils ont le même âge tous les deux.

$$R_{\text{avoir le même âge}}(\mathsf{c_A}, \mathsf{c_B}).$$

– Ceci-dit Charles-Edouard est amoureux de Béatrice.

$$R_{\text{être amoureux}}(\mathsf{c_C}, \mathsf{c_B}).$$

– Ouais, mais Béatrice, elle. Elle ne l'aime pas du tout.

$$\neg R_{\text{être amoureux}}(\mathsf{c_B}, \mathsf{c_C}).$$

On remarque avec intérêt que la négation d'une formule du type $\exists x\Big(P(x) \wedge P'(x)\Big)$ – qui signifie qu'il existe un élément qui satisfait les deux propriétés $P(\_)$ et $P'(\_)$ – est équivalente aux deux formules suivantes :

$$(1)\ \forall x\Big(P(x) \longrightarrow \neg P'(x)\Big) \qquad\qquad (2)\ \forall x\Big(P'(x) \longrightarrow \neg P(x)\Big).$$

En effet :

$$\begin{aligned}
\neg\exists x\Big(P(x) \wedge P'(x)\Big) &\equiv \forall x \neg\Big(P(x) \wedge P'(x)\Big) \\
&\equiv \forall x\Big(\neg P(x) \vee \neg P'(x)\Big) \equiv \forall x\Big(P(x) \longrightarrow \neg P'(x)\Big) \\
&\equiv \forall x\Big(\neg P'(x) \vee \neg P(x)\Big) \equiv \forall x\Big(P'(x) \longrightarrow \neg P(x)\Big).
\end{aligned}$$

Ces deux formules : $\forall x\big(P(x) \longrightarrow \neg P'(x)\big)$ et $\forall x\big(P'(x) \longrightarrow \neg P(x)\big)$ disent respectivement que tout élément qui satisfait la première propriété ne satisfait pas la seconde, et que tout élément qui satisfait la seconde ne satisfait pas la première. Ces deux expressions disent toutes les deux qu'aucun élément ne satisfait à la fois les deux propriétés, puisque quand il satisfait l'une, il ne satisfait pas l'autre.

Revenons un instant aux syllogismes. Les syllogismes permettaient la quantification. Mais celle-ci prenait toujours l'une des deux formes suivantes :

(1) $\forall x\Big(P_{\textsf{être grec}}(x) \longrightarrow P_{\textsf{être homme}}(x)\Big)$, (2) $\exists x\Big(P_{\textsf{être grec}}(x) \wedge P_{\textsf{être athénien}}(x)\Big)$,

que les propriétés soient positives ou négatives. En outre, on y trouvait l'usage de symboles de constantes comme dans l'exemple Socrate est un homme que l'on exprimera par :

$$P_{\textsf{être homme}}(\mathsf{c}_{\textsf{Socrate}}).$$

Avec la quantification telle que nous l'utilisons, nous pouvons intriquer les différents niveaux de quantifications. Nous pouvons ainsi dire $\exists x\phi$ qui signifie qu'il existe un étudiant qui vérifie ce que raconte ϕ. Mais ϕ elle-même peut faire intervenir une quantification. Par exemple :

(1) $\exists x \exists y R_{\textsf{aimer}}(x, y)$

il y a un étudiant qui en aime un autre (possiblement lui-même !)

(2) $\forall x \forall y R_{\textsf{aimer}}(x, y)$

tous les étudiants s'aiment (les uns les autres)

(3) $\exists x \forall y R_{\textsf{aimer}}(x, y)$

il existe un étudiant qui aime tous les autres (y compris lui-même !)

(4) $\forall x \exists y R_{\textsf{aimer}}(x, y)$

tout étudiant aime quelqu'un d'autre (possiblement lui-même !)

(5) $\exists y \forall x R_{\textsf{aimer}}(x, y)$

il existe un étudiant que tout le monde aime (y compris lui-même !)

(6) $\forall y \exists x R_{\textsf{aimer}}(x, y)$

tout étudiant est aimé par quelqu'un (possiblement lui-même !)

Lorsqu'une variable est dans le "champ" d'un quantificateur, on dit qu'elle est *liée* par ce quantificateur. Ainsi par exemple dans :

$$\forall y \exists x R_{\textsf{aimer}}(x, y)$$

la variable x est liée par le quantificateur existentiel, alors que la variable y l'est par le quantificateur universel. Mais qu'en est-il de la variable x dans la formule suivante :

$$\forall x \forall y \exists x R_{\textsf{aimer}}(x, y)?$$

On convient que c'est toujours le dernier quantificateur (dans le sens de la lecture linéaire gauche–droite) qui la lie. En l'occurrence, c'est donc le quantificateur existentiel et non pas le quantificateur universel. On verra plus loin que la représentation des formules sous forme d'arbres permet de définir cela plus joliment.

Une variable qui n'est pas liée est appelée *libre*. En quelque sorte, elle fait ce qu'elle veut. Une formule qui comporte une variable libre n'est ni vraie ni fausse dans un modèle. Pour déterminer sa valeur de vérité, il faut "remplacer" la variable libre par un élément du domaine. Autrement dit, une telle formule détermine l'ensemble des éléments du modèle pour lesquelles elle devient vraie. Ainsi par exemple, une formule à une variable libre suivante :

$$\Big(P_{\text{être en HEC}}(x) \wedge R_{\text{être plus gros}}(\mathsf{c}_{\mathsf{A}}, x)\Big)$$

parle de x qui est en HEC et qui est moins gros qu'Armand. L'ensemble des étudiants qui satisfont cette formule est tous ceux qui sont en HEC et qu'Armand dépasse sur la balance :

$$\Big\{x \text{ est étudiant } : \Big(P_{\text{être en HEC}}(x) \wedge R_{\text{être plus gros}}(\mathsf{c}_{\mathsf{A}}, x)\Big)\Big\}.$$

Une formule à deux variables libres détermine un ensemble de couples d'étudiants. Par exemple, la formule suivante :

$$\Big(P_{\text{être en HEC}}(x) \wedge P_{\text{être en philo}}(y) \wedge R_{\text{aimer}}(x, y)\Big)$$

détermine l'ensemble des couples d'étudiants dont le premier est en HEC, le second en philosophie et tels que le premier aime le second.

$$\Big\{(x, y) \in \{\text{étudiants}\} \times \{\text{étudiants}\} \ : \Big(P_{\text{être en HEC}}(x) \wedge P_{\text{être en philo}}(y) \wedge R_{\text{aimer}}(x, y)\Big)\Big\}.$$

2 Au cœur de la logique du 1^er^ ordre

Nous sommes partis d'un modèle et nous avons étudié quelques "formules", afin de tenter à la fois de comprendre ce qu'elles signifiaient et de déterminer leur véracité ou non dans notre modèle. Mais à la vérité, ces formules n'en étaient pas ! Elles avaient l'aspect de formules, elles en avaient le goût, mais ce n'étaient pas des formules. Pourquoi cela ?
Parce qu'une formule ne fait intervenir que des *symboles* (de relation, de constante,....) et non leurs interprétations comme le fait le modèle.
Ainsi :

$$\forall x\Big(P(x) \longrightarrow R(\mathsf{c}, x)\Big)$$

est une formule. Elle fait intervenir un symbole de constante (c), un symbole de relation unaire (P) et un symbole de relation binaire (R).

$$\forall x\Big(P_{\text{être en HEC}}(x) \longrightarrow R_{\text{être plus sympa}}(\mathsf{c}_{\mathsf{A}}, x)\Big)$$

est en quelque sorte *l'interprétation* de cette formule dans le modèle particulier que nous avons choisi. Elle signifie qu'Armand est le plus sympa des étudiants qui sont en HEC.

Si nous considérons un autre modèle, par exemple celui dans lequel le domaine de base est composé des peintures modernes, c est interprété par *la danse* de Matisse, P par la propriété être un tableau de Jackson Pollock, et R par la relation être antérieur à. La signification de cette formule devient alors :

$$\forall x\Big(P_{\text{être un Pollock}}(x) \longrightarrow R_{\text{être antérieur à}}(\mathsf{c}_{\text{danse}}, x)\Big).$$

Une formule est donc un pur objet formel. Par exemple :

- $\forall x\Big(P(x) \longrightarrow R(\mathsf{c}, x)\Big)$;
- $\Big(\forall x(\mathsf{H}(x) \longrightarrow \mathsf{M}(x)) \wedge \mathsf{H}(\mathsf{s})\Big) \longrightarrow \mathsf{M}(\mathsf{s})$.

Alors que les “formules” ci-dessous n’en sont que des *interprétations* particulières.

- $\forall x\Big(P_{\text{être un Pollock}}(x) \longrightarrow R_{\text{être antérieur à}}(\mathsf{c}_{\text{danse}}, x)\Big)$;
- $\forall x\Big(P_{\text{être en HEC}}(x) \longrightarrow R_{\text{être plus sympa}}(\mathsf{c}_{\mathsf{A}}, x)\Big)$;
- $\Big(\forall x\ (H_{\text{omme}}(x) \longrightarrow M_{\text{ortel}}(x))\ \wedge\ H_{\text{omme}}(\mathsf{s}_{ocrate})\Big)\ \longrightarrow\ M_{\text{ortel}}(\mathsf{s}_{ocrate})$;
- $\Big(\forall x\ (H_{\text{ibou}}(x) \longrightarrow M_{\text{alin}}(x))\ \wedge\ H_{\text{ibou}}(\mathsf{s}_{tan})\Big)\ \longrightarrow\ M_{\text{alin}}(\mathsf{s}_{tan})$;
- $\Big(\forall x\ (H_{\text{ypermarché}}(x) \longrightarrow M_{\text{oche}}(x))\ \wedge\ H_{\text{ypermarché}}(\mathsf{s}_{par})\Big)\ \longrightarrow\ M_{\text{oche}}(\mathsf{s}_{par})$.

Par interprétations particulières, il faut entendre que la formule prend un sens nouveau lorsqu’elle est “plongée” dans un modèle. Elle prend corps, elle prend chair, elle s’incarne et cesse de n’être que ce squelette dénué de vie. Le modèle est donc un objet qui fournit non seulement des éléments sur lesquels les variables “varient”, mais aussi un “habit” pour chacun des symboles de constantes et des symboles de relations.

Ainsi au lieu d’écrire :

$$\forall x\Big(P_{\text{être en HEC}}(x) \longrightarrow R_{\text{être plus sympa}}(\mathsf{c}_{\mathsf{A}}, x)\Big)$$

on écrira simplement :

$$\mathcal{M} \models \forall x\Big(P(x) \longrightarrow R(c, x)\Big).$$

Mais on indiquera que dans le modèle $\mathcal{M}$ les éléments sont des étudiants, $P(\_)$ est interprété par la propriété $P_{\text{être en HEC}}(\_)$, $R(\_,\_)$ est interprété par la relation binaire $R_{\text{être plus sympa}}(\_,\_)$ et finalement c_{A} désigne un étudiant particulier (Armand). On dira précisément :

- le domaine de $\mathcal{M}$ (noté $|\mathcal{M}|$) est l’ensemble des étudiants de cet auditoire,
- l’interprétation de $P(\_)$ dans $\mathcal{M}$ (noté $P^{\mathcal{M}}$) est précisément $P_{\text{être en HEC}}(\_)$,
- l’interprétation de $R(\_,\_)$ dans $\mathcal{M}$ (noté $R^{\mathcal{M}}$) est $R_{\text{être plus sympa}}(\_,\_)$,
- l’interprétation de c dans $\mathcal{M}$ (noté $\mathsf{c}^{\mathcal{M}}$) est c_{A}.

Et plutôt qu’écrire :

$$\forall x\Big(P_{\text{être en HEC}}(x) \longrightarrow R_{\text{être plus sympa}}(\mathsf{c}_{\mathsf{A}}, x)\Big)$$

On écrira simplement :

$$\langle|\mathcal{M}|, P^{\mathcal{M}}, R^{\mathcal{M}}, \mathsf{c}^{\mathcal{M}}\rangle \models \forall x\Big(P(x) \longrightarrow R(c, x)\Big)$$

ou même :

$$\mathcal{M} \models \forall x\big(P(x) \longrightarrow R(c, x)\big).$$

En conséquence, si $\mathcal{N}$ désigne le modèle défini par :

- le domaine de $\mathcal{N}$ (noté $|\mathcal{N}|$) est l'ensemble des peintures modernes,
- l'interprétation de $P(\_)$ dans $\mathcal{M}$ (noté $P^{\mathcal{N}}$) est précisément $P_{\text{être un Pollock}}(\_)$,
- l'interprétation de $R(\_,\_)$ dans $\mathcal{M}$ (noté $R^{\mathcal{N}}$) est $R_{\text{être antérieur à}}(\_,\_)$,
- l'interprétation de c dans $\mathcal{M}$ (noté $\mathsf{c}^{\mathcal{N}}$) est $\mathsf{c}_{\text{danse}}$.

Nous écrirons :

$$\langle |\mathcal{N}|, P^{\mathcal{N}}, R^{\mathcal{N}}, c^{\mathcal{N}} \rangle \models \forall x \Big(P(x) \longrightarrow R(c,x) \Big)$$

ou même :

$$\mathcal{N} \models \forall x \Big(P(x) \longrightarrow R(c,x) \Big)$$

pour dire :

$$\forall x \Big(P_{\text{être un Pollock}}(x) \longrightarrow R_{\text{être antérieur à}}(\mathsf{c}_{\text{danse}}, x) \Big).$$

Une formule qui n'a pas de variable libre est appelée une *formule close.*

Ce sont les formules closes qui vont constituer les théories. La grande question étant :

Mon énoncé (précisé sous forme de formule close) ϕ est-il une conséquence de la théorie T ?

Là encore, les deux notions différentes de conséquence (sémantique et syntaxique) vont se correspondre.

- La notion de conséquence sémantique notée $T \models \phi$ dit que ϕ est vraie dans tous les modèles qui satisfont (toutes les formules de) la théorie T.
- La notion de conséquence syntaxique notée $T \vdash \phi$ dit qu'il existe une preuve de ϕ.

Ce qui est remarquable, c'est qu'une preuve est un objet fini (comme par exemple un arbre de preuve), alors que les modèles qui satisfont une théorie sont en général en nombre infini. Pourtant les deux se correspondent puisque :

$$T \vdash \phi \text{ si et seulement si } T \models \phi.$$

Ce qui est équivalent à dire

$$T \nvdash \phi \text{ si et seulement si } T \not\models \phi.$$

L'on voit que la bonne façon de montrer qu'un énoncé (ϕ) n'est pas conséquence d'un ensemble d'hypothèses (T), c'est de trouver un malheureux modèle qui satisfait les hypothèses (T) mais non la conclusion (ϕ). C'est précisément ce que l'on appelle un *contre-exemple.*

Chapitre 10

Syntaxe

1 Le langage

Résumé № 44 *Un langage $\mathcal{L}$ de la logique du* 1^er^ ordre *est composé de deux parties différentes :*

(1) les invariants *de $\mathcal{L}$:*

(a) les variables : $v_0, v_1, v_2, \dots, v_n, \dots$;

(b) les connecteurs logiques : $\neg$, $\vee$, $\wedge$, $\longrightarrow$, $\longleftrightarrow$:

(c) les quantificateurs : $\forall$, $\exists$;

(2) la signature *de $\mathcal{L}$:*

(a) un ensemble de symboles de constantes : $\{\mathtt{c}_0, \mathtt{c}_1 \dots\}$;

(b) un ensemble de symboles de fonctions de différentes arités : $\{f_0, f_1, \dots\}$;

(c) un ensemble de symboles de relations de différentes arités : $\{R_0, R_1, \dots\}$.

※

Plutôt que de parler du langage de la logique du 1$^{\text{er}}$ ordre, on devrait parler *des* langages de la logique du 1$^{\text{er}}$ ordre, car il y en a en fait une infinité, tous construits sur le même schéma. On utilise pourtant le terme langage du *1erordre* en un sens générique – c'est-à-dire pour désigner le cadre général de ces différents langages de la logique du 1$^{\text{er}}$ ordre. Nous verrons plus loin les raisons de ce qualificatif.

Définition 312 *Le langage de la logique du* 1$^{\text{er}}$ordre *est un ensemble $\mathcal{L}$ composé de deux parties différentes :*

(1) la première est commune à tous les langages du 1er ordre, elle ressemble beaucoup au langage du Calcul Propositionnel. Elle est constituée :

(a) d'un ensemble infini de symboles de variables (ou encore appelés variables tout court) :

$$\mathcal{V} = \{v_0, v_1, v_2, \dots, v_n, \dots\}$$

(Pour plus de lisibilité, on notera souvent ces variables $x, y, z \ldots$).

(b) *des connecteurs logiques :*

$$\neg,\ \vee,\ \wedge,\ \longrightarrow,\ \longleftrightarrow$$

(c) *des quantificateurs :*

(A) *le quantificateur universel :*

$$\forall$$

(B) *le quantificateur existentiel :*

$$\exists$$

(2) *la seconde partie est propre à chaque langage particulier. Elle comporte :*

(a) *un ensemble de symboles de constantes (ou encore appelés constantes tout court) :*

$$\{\mathsf{c}_0, \mathsf{c}_1, \ldots\}$$

(b) *un ensemble de symboles de fonctions de différentes arités (*attention, ce sont bien des symboles de fonctions et pas des fonctions*) :*

$$\{f_0, f_1, \ldots\}$$

(c) *un ensemble de symboles de relations de différentes arités (*attention, ce sont bien des symboles de relations et pas des relations*) :*

$$\{R_0, R_1, \ldots\}$$

Remarques 313

(1) L'*égalité* est une relation binaire particulière. Pour des commodités de lecture, on notera $x = y$ et non $R_=(x, y)$. On ne la confondra pas avec les autres symboles de relation pour la raison que son interprétation dans un modèle sera contrainte, au contraire de toute autre relation binaire. Pour cela, on parle de *langage égalitaire* lorsque le symbole d'égalité fait partie de $\mathcal{L}$ et de *langage non égalitaire* lorsque l'égalité n'en fait pas partie.

(2) Nous pourrions nous passer des symboles de fonction. En effet, nous pourrions utiliser le graphe d'une fonction (qui est une relation binaire) à la place de celle-ci. Ainsi, soit $f\ E \longrightarrow F$ une fonction, posons $G_f = \{(x, y) \in E \times F :\ y = f(x)\}$. Au lieu d'écrire, par exemple $P(f(x))$ (où P est un symbole de relation unaire) pour dire que tous les termes se trouvant être l'image d'un élément de E par f vérifient aussi la propriété P, nous pourrions tout aussi bien écrire $P(y) \wedge G_f(x, y)$. Pourtant, il y a une raison fondamentale à l'utilisation des symboles de fonctions. Hormis le fait que les fonctions interviennent naturellement dans la pratique quotidienne ; elles nous seront absolument nécessaires lorsqu'il s'agira de prouver le théorème de complétude (Théorème 439). Il nous faudra alors construire un modèle de toute pièce à partir de rien d'autre que les objets syntaxiques dont nous disposerons. Fort heureusement, parmi ces objets, nous aurons à notre disposition les symboles de constantes et symboles de fonctions qui nous donneront des *termes* grâce auxquels nous pourrons vraiment démarrer la construction de notre modèle.

On parle de symboles de fonction et de symboles de relations et non pas de fonctions ou de relations pour la simple raison qu'aucun domaine n'est spécifié ni pour les symboles de fonctions ni pour les symboles de relations. Pour être plus précis, dès que nous aborderons la sémantique de la logique du 1er ordre, nous verrons qu'un symbole de fonction est quelque chose qui sera interprété comme une véritable fonction, un symbole de relation comme une véritable relation, en respectant, chaque fois, les arités de chacuns.

2 Les termes du langage

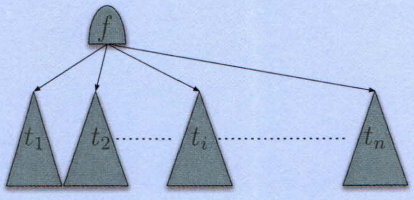
Résumé № 45 *L'ensemble* $T_{\mathcal{L}}$ *des* termes du langage $\mathcal{L}$ *est le plus petit ensemble tel que :*

- *les variables* $v_0, v_1, v_2, \ldots \in T_{\mathcal{L}}$ *;*
- *les symboles de constantes* $\mathsf{c}_0, \mathsf{c}_1 \ldots \in T_{\mathcal{L}}$ *;*
- *pour chaque symbole de fonction d'arité n " f" de* $\mathcal{L}$*,*

$$t_1, \ldots, t_n \in T_{\mathcal{L}} \Longrightarrow f(t_1, \ldots, t_n) \in T_{\mathcal{L}}.$$

On définit l'arbre de décomposition d'un terme $t \in T_{\mathcal{L}}$ *par :*

- *si* $t = v_i$ *ou* $t = \mathsf{c}$*, alors l'arbre se confond avec le terme.*
- *si* $t = f(t_1, \ldots, t_n)$*, alors l'arbre est*



La hauteur de l'arbre est la longueur de sa (ses) plus longue(s) branche(s).

※

Définition 314 *Soit* $\mathcal{L}$ *un langage du 1*er*ordre. L'ensemble* $T_{\mathcal{L}}$ *des* termes du langage $\mathcal{L}$ *est le plus petit ensemble qui :*

- *contient les variables et les symboles de constantes,*
- *pour chaque f, symbole de fonction d'arité n du langage* $\mathcal{L}$*, chaque fois qu'il contient les termes* $t_1, \ldots, t_n$*, il contient également le terme* $f(t_1, \ldots, t_n)$*.*

Exemple 315 Soit $\mathcal{L}$ le langage qui ne contient que le symbole de constante "c", le symbole de fonction unaire "f" et le symbole de fonction binaire "g".

(1) les énoncés suivants sont des termes du langage $\mathcal{L}$:

- c
- $g(c, c)$
- $g(\mathsf{c}, g(\mathsf{c}, \mathsf{c}))$
- $f(\mathsf{c})$
- $f(f(\mathsf{c}))$
- $f(g(\mathsf{c}, g(\mathsf{c}, \mathsf{c})))$
- $g\Big(f(f(\mathsf{c})), g\Big(f(f(\mathsf{c})), f(f(\mathsf{c}))\Big)\Big).$

(2) Quelques exemples qui ne sont pas des termes du langage $\mathcal{L}$:

- $f(\mathsf{c})\mathsf{c}$
- $g(f(\mathsf{c}))$
- $f(f(\mathsf{c}, g(\mathsf{c}, f)))$
- $g(\mathsf{c})$
- $g(f, g(\mathsf{c}, \mathsf{c}))$
- $f(f(\mathsf{c}).$

La définition que nous venons de donner est une définition par *le haut*. Elle consiste à engendrer l'ensemble de tous les termes comme l'intersection de toutes les classes qui vérifient une certaine propriété. En l'occurrence, cette propriété est de contenir les symboles de constantes et de variables et d'être *close* pour les symboles de fonctions (en appliquant un symbole de fonction à une suite de termes de même longueur que l'arité du symbole de fonction, on ne sort pas de l'ensemble des termes).

Nous allons définir la hauteur d'un terme par induction sur la formation de celui-ci. Il est clair que l'ensemble des termes est exactement l'ensemble qui contient les termes de toutes hauteurs finies.

Définition 316 *Soient $\mathcal{L}$ un langage du 1erordre et t un terme de ce langage. La hauteur de t notée $(ht(t))$ est définie par :*

- *si t est un symbole de constante ou bien un symbole de variable, alors $ht(t) = 0$.*
- *si $t = f(t_1, \ldots, t_n)$, alors $ht(t) = 1 + \max\Big(ht(t_1), \ldots, ht(t_n)\Big)$.*

Exemple 317 Soit $\mathcal{L}$ le langage qui ne contient que le symbole de constante c, le symbole de fonction unaire f et le symbole de fonction g.

(1) $ht(\mathsf{c}) = 0$

(2) $ht(f(\mathsf{c})) = 1$

(3) $ht(g(\mathsf{c}, \mathsf{c})) = 1$

(4) $ht(f(f(\mathsf{c}))) = 2$

(5) $ht(g(\mathsf{c}, g(\mathsf{c}, \mathsf{c}))) = 2$

(6) $ht(f(g(\mathsf{c}, g(\mathsf{c}, \mathsf{c})))) = 3$

(7) $ht(g(f(f(\mathsf{c})), g(f(f(\mathsf{c})), f(f(\mathsf{c}))))) = 4$.

2.1 L'arbre de décomposition d'un terme

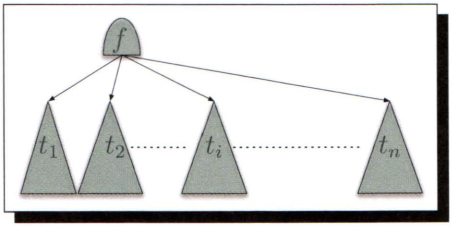
Chaque terme d'un langage du 1er ordre peut être présenté sous forme d'arbre. Les avantages de ce mode de représentation sont multiples. Il permet de lire le terme de manière beaucoup plus efficace que ne l'autorise sa présentation linéaire. La hauteur du terme correspond à la longueur de la plus longue branche de cet arbre. Et finalement, chacun des sous-termes est directement accessible par les sous-arbres.

Définition 318 *L'arbre T_t de décomposition d'un terme t est défini par induction sur la hauteur de ce terme :*

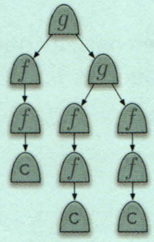
(1) Si $ht(t) = 0$, T_t est alors simplement l'arbre constitué d'un seul nœud[1] :

1. On rappelle que dans ce cas, t est soit une constante soit une variable.

(2) Si $ht(t) = k+1$, alors non seulement t est de la forme $t = f(t_1, \ldots, t_n)$, mais encore T_t est l'arbre dont la racine est le symbole de fonction f, d'où partent exactement n branches, la $i^{ème}$ menant à l'arbre de décomposition du terme t_i.



Exemple 319 Arbre de décomposition du terme $g\Big(f(f(\mathsf{c})), g\big(f(f(\mathsf{c})), f(f(\mathsf{c}))\big)\Big)$:



Ce terme a pour hauteur 4.

Remarques 320 La hauteur d'un terme correspond exactement à la longueur de la plus longue branche de son arbre de décomposition. Cela se démontre par induction sur la hauteur des termes.

2.2 Les substitutions dans les termes

Définition 321 *Soient $x_1, x_2, \ldots, x_k$ des variables deux à deux distinctes, et $t, t_1, t_2, \ldots, t_k$ des termes, on définit le terme $t_{[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]}$ comme étant le résultat de la substitution des termes t_i aux variables x_i dans le terme t. Cela se définit proprement par induction sur la hauteur de t comme suit :*

(1) si $ht(t) = 0$ alors :

(a) si t est un symbole de constante ou bien une variable différente de $x_1, x_2, \ldots, x_k$:

$$t_{[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]} = t$$

(b) si t est une variable x_i :

$$t_{[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]} = t_i$$

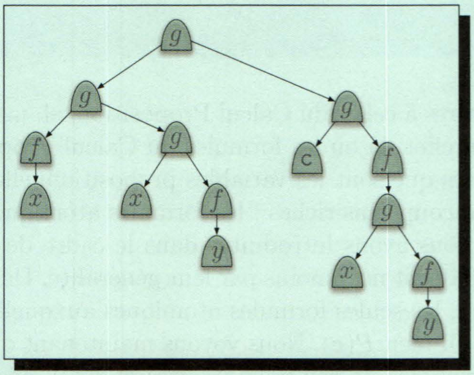
(2) si $ht(t) = n+1$, alors t est de la forme $t = f(u_1, \ldots, u_n)$, chaque u_i étant un terme de hauteur au plus n (l'un d'entre eux étant de hauteur exactement n) et

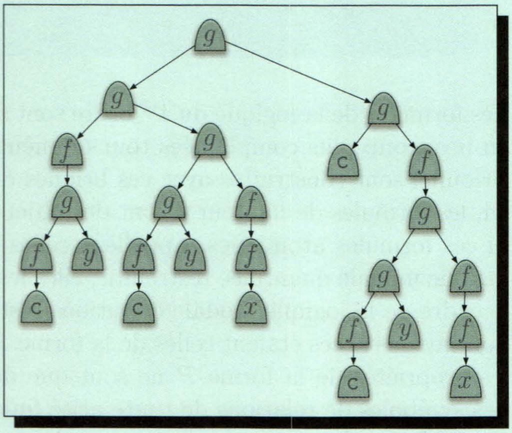
$$t_{[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]} \;=\; f(u_{1[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]}, \ldots, u_{n[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]}).$$

Exemple 322 Considérons le terme $g\Bigg(g\Big(f(x), g\big(x, f(y)\big)\Big), g\bigg(\mathsf{c}, f\Big(g\big(x, f(y)\big)\Big)\bigg)\Bigg)$ et opérons la substitution du terme $g(f(\mathsf{c}), y)$ à la variable x et celle du terme $f(x)$ à la variable y :

$$g(g(f(x), g(x, f(y))), g(\mathsf{c}, f(g(x, f(y)))))_{[g(f(\mathsf{c}),y))/x, f(x)/y]}$$
$$=$$
$$g(g(f(g(f(\mathsf{c}), y))), g(g(f(\mathsf{c}), y)), f(f(x)))), g(\mathsf{c}, f(g(g(f(\mathsf{c}), y)), f(f(x))))).$$

Le même exemple mais présenté sous forme d'arbre de décomposition :





3 Les formules

***Résumé* № 46** *Etant donné un langage $\mathcal{L}$ de la logique du* 1^er ordre, *les $\mathcal{L}$-formules sont des arbres dont les feuilles sont des* formules atomiques *et les autres nœuds des connecteurs logiques. Ainsi, θ est une $\mathcal{L}$-formule si :*

(1) Soit θ est une formule atomique, i.e., de la forme $R(t_1, \ldots, t_n)$ où :

(a) R est un symbole de relation de $\mathcal{L}$ d'arité n ;

(b) $t_1, \ldots, t_n$ sont des termes de $\mathcal{L}$.

(2) soit θ est de la forme :

$$\begin{array}{c}\neg\\ |\\ \phi\end{array},\quad \begin{array}{c}\exists x\\ |\\ \phi\end{array},\quad \begin{array}{c}\forall x\\ |\\ \phi\end{array},\quad \begin{array}{c}\vee\\ \diagup\diagdown\\ \phi\quad\psi\end{array},\quad \begin{array}{c}\wedge\\ \diagup\diagdown\\ \phi\quad\psi\end{array},\quad \begin{array}{c}\longrightarrow\\ \diagup\diagdown\\ \phi\quad\psi\end{array},\quad \begin{array}{c}\longleftrightarrow\\ \diagup\diagdown\\ \phi\quad\psi\end{array}.$$

pour des formules ϕ et ψ.

※

Les formules de la logique du 1^er ordre sont similaires à celles du Calcul Propositionnel, mais en beaucoup plus compliquées tout de même. En effet, là où les formules du Calcul Propositionnel sont construites avec ces briques de bases que sont les variables propositionnelles, ici, les formules de hauteur 0 sont des objets beaucoup plus riches : les formules atomiques. Si ces formules atomiques rappellent celles que nous avons introduites dans le cadre de la logique modale quantifiée restreinte ; elles les surpassent néanmoins par leur généralité. Dans le cadre de la logique modale quantifiée restreinte, les seules formules atomiques auxquelles nous avions accès étaient celles de la forme $P(x)$ ou bien $P(\mathsf{c})$. Nous voyons maintenant que les propriétés de la forme P ne sont que des symboles de relations unaires et qu'il existe des symboles de relations de toute arité finie. Par ailleurs, les termes que nous considérions (variables ou constantes) ne sont que des termes de hauteur 0, alors qu'il existe des termes de toute hauteur. Nous allons donc définir la notion de formule atomique de manière somme toute similaire à $P(x)$ ou bien $P(\mathsf{c})$, mais en autorisant des symboles de relations d'arité quelconque ainsi que des termes de hauteur quelconque.

Définition 323 *Soit $\mathcal{L}$ un langage du 1^er ordre, l'ensemble des* formules atomiques *de ce langage est constitué de toutes les suites de symboles de la forme :*

$$R(t_1, \ldots, t_n)$$

où :

(1) R est un symbole de relation d'arité n,

(2) $t_1, \ldots, t_n$ sont des termes du langage $\mathcal{L}$.

Intuitivement, une formule atomique, tout comme une variable propositionnelle, est quelque chose susceptible de vérité ou de fausseté. Elle joue en fait le même rôle que la variable propositionnelle : c'est une brique de base qui peut être vraie ou fausse. Mais à la différence de la variable propositionnelle qui se présente comme un bloc indécomposable, une formule atomique est composée d'un symbole de relation (que l'on interprétera comme une véritable relation, donc comme quelque chose qui affirme une propriété ou une relation entre des objets) muni de termes (ces termes forment une manière détournée d'atteindre un objet, puisqu'ils le circonscrivent aux moyens de fonctions de fonctions de fonctions de...... fonctions de constantes ou de variables).

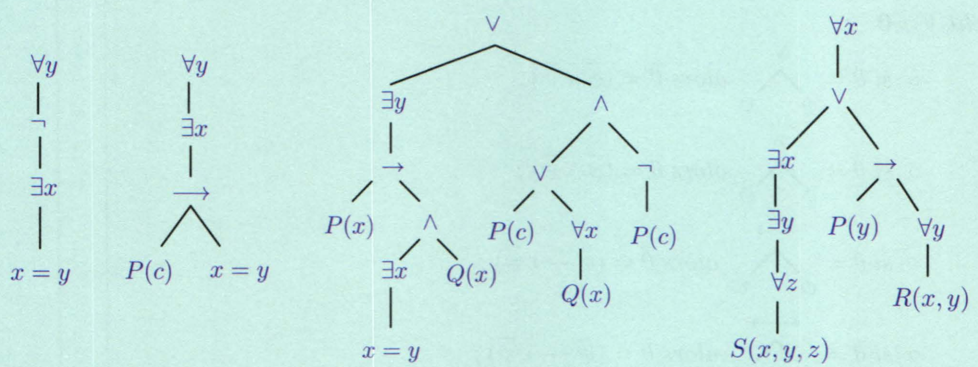
Définition 324 *L'ensemble* $\mathcal{F}$ *des* formules de la Logique du 1[er] ordre *est le plus petit ensemble qui :*

- *contient chaque arbre réduit à sa racine qui est une* formule atomique, *et*
- *chaque fois qu'il contient des formules* ϕ *et* ψ *contient également – pour chaque variable* x *– les formules suivantes :*

La hauteur d'une formule est la longueur de sa plus longue branche – ou de ses plus longues branches lorsqu'il y en a plusieurs.

Il est à remarquer qu'il n'y a plus de condition particulière portant sur l'existence de quantificateur dans les formules admettant des variables dans leurs formules atomiques, comme c'était le cas dans la Définition 324 des formules de la logique quantifiée restreinte.

Exemple 325 Trois formules, les deux premières de hauteur 3, les deux suivantes de hauteur 5 :



4 La linéarisation d'une formule

Résumé № 47 *L'écriture d'une formule sous forme linéaire consiste à transfomer :*

$$\begin{array}{c}\neg\\ \mid\\ \phi\end{array} ; \quad \begin{array}{c}\exists x\\ \mid\\ \phi\end{array} ; \quad \begin{array}{c}\forall x\\ \mid\\ \phi\end{array} ; \quad \begin{array}{ccc} & \vee & \\ \phi & & \psi\end{array} ; \quad \begin{array}{ccc} & \wedge & \\ \phi & & \psi\end{array} ; \quad \begin{array}{ccc} & \longrightarrow & \\ \phi & & \psi\end{array} ; \quad \begin{array}{ccc} & \longleftrightarrow & \\ \phi & & \psi\end{array} ;$$

en respectivement

$$\neg\overline{\phi} \ ; \ \exists x\overline{\phi} \ ; \ \forall x\overline{\phi} \ ; \ (\overline{\phi} \vee \overline{\psi}) \ ; \ (\overline{\phi} \wedge \overline{\psi}) \ ; \ (\overline{\phi} \longrightarrow \overline{\psi}) \ ; \ (\overline{\phi} \longleftrightarrow \overline{\psi}).$$

où $\overline{\phi}$ et $\overline{\psi}$ désignent respectivement les linéarisations de ϕ et de ψ ; la linéarisation des formules atomiques restant inchangée. ※

Tout comme dans les logiques précédemment étudiées, les formules de la logique du 1^{er} ordre admettent une présentation sous forme linéaire.

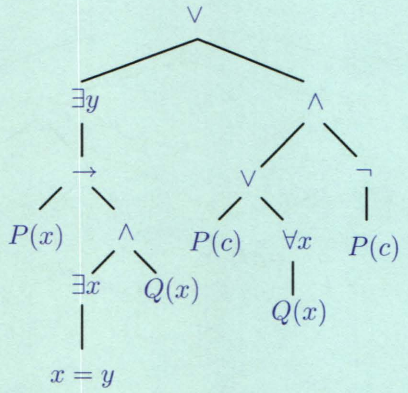
Définition 326 *Soit $\theta \in \mathcal{F}$ une formule de la logique du 1^{er} ordre. La linéarisation de la formule θ (notée $\overline{\theta}$) est définie par induction sur la hauteur de θ.*

$ht(\theta)$=0 *: dans ce cas θ est une formule atomique de la forme $R(t_1, \ldots, t_k)$, auquel cas $\theta = \overline{\theta} = R(t_1, \ldots, t_k)$.*

$ht(\theta)$>0 *:*

- *si* $\theta = \begin{array}{ccc} & \vee & \\ \phi & & \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \vee \overline{\psi})$;
- *si* $\theta = \begin{array}{ccc} & \wedge & \\ \phi & & \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \wedge \overline{\psi})$;
- *si* $\theta = \begin{array}{ccc} & \longrightarrow & \\ \phi & & \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \longrightarrow \overline{\psi})$;
- *si* $\theta = \begin{array}{ccc} & \longleftrightarrow & \\ \phi & & \psi\end{array}$ *alors* $\overline{\theta} = (\overline{\phi} \longleftrightarrow \overline{\psi})$;
- *si* $\theta = \begin{array}{c}\neg\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \neg\overline{\phi}$;
- *si* $\theta = \begin{array}{c}\exists x\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \exists x\overline{\phi}$;
- *si* $\theta = \begin{array}{c}\forall x\\ \mid\\ \phi\end{array}$ *alors* $\overline{\theta} = \forall x\overline{\phi}$.

Exemple 327 Linéarisation $\overline{\phi}$ de la formule ϕ suivante :



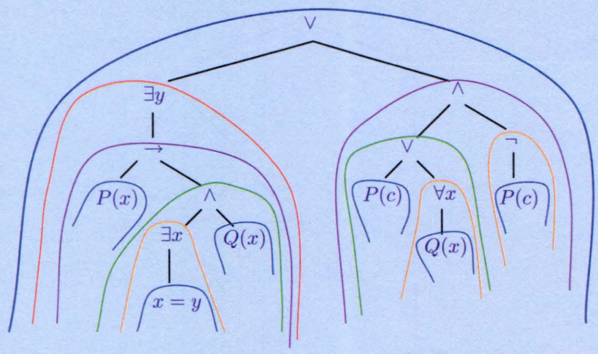
$$\overline{\phi} = \Big(\exists y\ \big(P(x) \longrightarrow (\exists x\ x = y \wedge Q(x))\big) \vee \big((P(\mathsf{c}) \vee \forall x\ Q(x)) \wedge \neg P(\mathsf{c})\big)\Big).$$

Exemple 328 On considère le langage $\mathcal{L}$ composé de P et R comme symboles de relations respectivement unaire et binaire, ainsi que du symbole de fonction unaire f et du symbole de constante c.

- Les suites de symboles de $\mathcal{L}$ ci-dessous sont des formules (sous forme linéaire) :
  - $P(\mathsf{c})$;
  - $(P(x) \wedge R(\mathsf{c}, x))$;
  - $\exists y\ (P(x) \wedge R(\mathsf{c}, x))$;
  - $\neg\neg P(f(f(\mathsf{c})))$;
  - $\forall x\ (P(x) \wedge R(\mathsf{c}, x))$;
  - $(\neg P(\mathsf{c}) \wedge \neg\neg(P(x) \wedge (R(f(x), f(\mathsf{c})) \longrightarrow P(y))))$;
  - $\neg\neg(\neg R(\mathsf{c}, \mathsf{c}) \longleftrightarrow \neg\neg(\neg R(x, x) \wedge (\neg P(f(f(x))) \longrightarrow \neg\neg P(\mathsf{c}))))$.
- Par contre, les suites suivantes n'en sont pas :
  - $P(P)$;
  - $R(P(\mathsf{c}), x)$;
  - $\exists y\ (P(x)\exists x\ \wedge R(\mathsf{c}, x))$.
  - $P(x)\neg(P(x) \wedge P(\mathsf{c}))$;
  - $\forall \mathsf{c}\ (P(x) \wedge R(\mathsf{c}, x))$;

5 Les sous-formules

Résumé № 48 *Une sous-formule d'une formule ϕ est un sous-arbre de ϕ dont l'un des nœuds de ϕ est la racine.*



※

Chaque formule qui n'est pas atomique est construite par récurrence, en agençant d'autres formules appelées *sous-formules.*

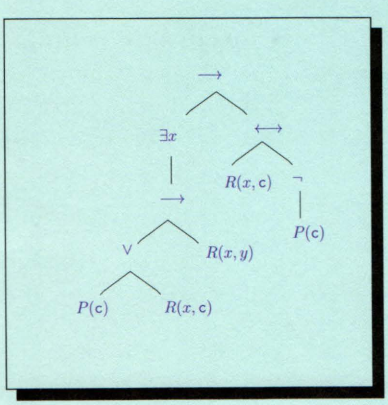
Définition 329 *Une sous-formule d'une formule ϕ est un sous-arbre de ϕ engendré par un nœud de ϕ.*

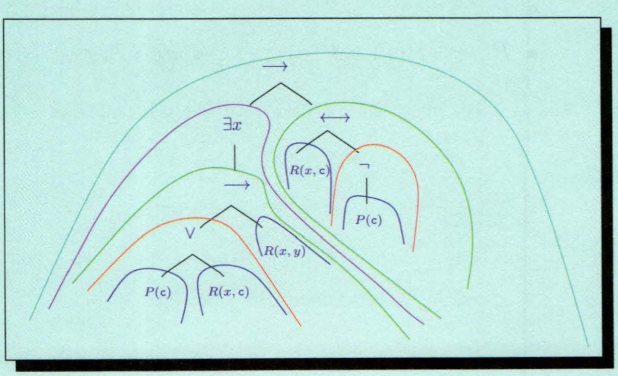
Cela signifie qu'on obtient une sous-formule de ϕ en pointant l'un de ses nœuds et en ne gardant de la formule ϕ que ce nœud-ci ainsi que tous ses descendants.

Exemple 330 Considérons la formule

$$\Big(\exists x\ \big((P(\mathsf{c}) \vee R(x,\mathsf{c})) \longrightarrow R(x,y)\big) \longrightarrow (R(x,\mathsf{c}) \longleftrightarrow \neg P(\mathsf{c}))\Big)$$

qui est la linéarisation de la formule ci-dessous :





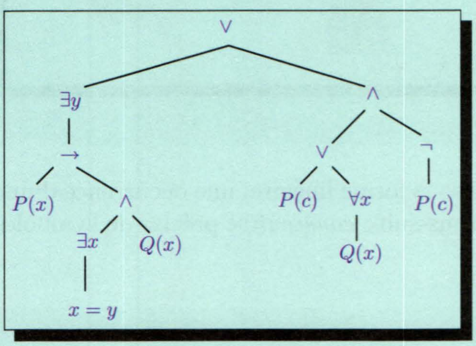
Dans le dessin de droite, les sous-arbres matérialisés par des traits de couleur correspondent aux sous-formules de différentes hauteurs :

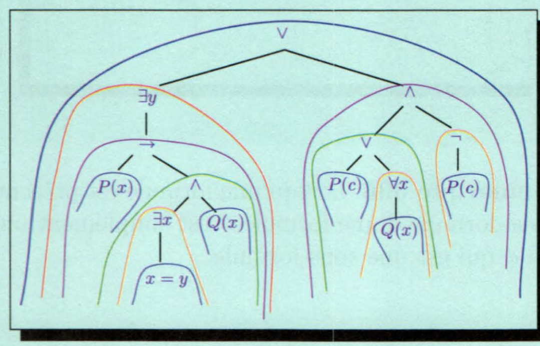
$$\text{bleu foncé} \rightsquigarrow 0,\ \text{rouge} \rightsquigarrow 1\,;\ \text{vert} \rightsquigarrow 2\,;\ \text{violet} \rightsquigarrow 3\,;\ \text{bleu clair} \rightsquigarrow 4.$$

Exemple 331 La formule

$$\Big(\exists y \ \big(P(x) \longrightarrow (\exists x \ x = y \vee Q(x))\big) \vee \big((P(\mathsf{c}) \wedge \forall x \ Q(x)) \wedge \neg P(\mathsf{c})\big)\Big)$$

est la linéarisation de la formule ci-dessous à gauche, ses sous-formules étant ci-dessous à droite :





Remarque 332 Lorsqu'une formule est présentée sous forme linéaire, une sous-formule d'une formule ϕ devient une suite **consécutive** de symboles de ϕ qui est elle-même une formule.

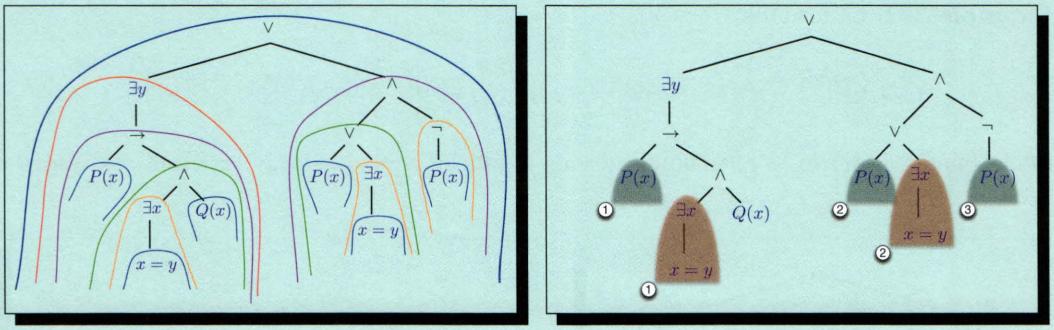
Exemple 333 Considérons la fomule $\phi = \forall x \ \big(P(x) \wedge R(c, x)\big)$.

- Les suites de symboles suivants sont des sous-formules de ϕ :
  - $P(x)$
  - $R(\mathsf{c}, x)$
  - $\big(P(x) \wedge R(\mathsf{c}, x)\big)$
  - $\forall x \ \big(P(x) \wedge R(\mathsf{c}, x)\big)$
- Par contre les suites suivantes n'en sont pas :
  - P
  - $R(\mathsf{c}, x$
  - $P(x)\wedge$
  - $\forall x$
  - $\forall x \ (P(x)$
  - $\forall x \ P(x)$

  (Seule la dernière est bien une formule, mais elle n'est pas une suite consécutive de symboles de ϕ.)

Remarque 334 Une formule donnée peut apparaître à plusieurs reprises comme sous-formule d'une même formule ϕ. On distingue chacune de ces "apparitions" comme autant d'occurrence de la sous-formule.

Exemple 335 La formule ϕ ci-dessous, dont les sous-formules sont matérialisées par des traits de couleur, possède deux sous-formules ayant plusieurs occurrences : $P(x)$ et $\exists x\ x = y$.



Remarque 336 Lorsqu'une formule est présentée sous forme linéaire, une occurrence d'une sous-formule d'une formule ϕ est simplement une sous-suite *consécutive* précise de symboles de ϕ qui est une sous-formule.

Exemple 337 Soit

$$\phi = \Big(\big((\neg P(x) \vee P(y)) \wedge \neg(\neg P(x) \vee P(y))\big) \wedge \big((\neg P(x) \vee P(y)) \longrightarrow \neg P(x)\big)\Big),$$

Clairement, $(\neg P(x) \vee P(y))$ est une sous-formule de ϕ. Il y a trois occurrences de $(\neg P(x) \vee P(y))$ dans ϕ notées 1, 2, 3 ci-dessous :

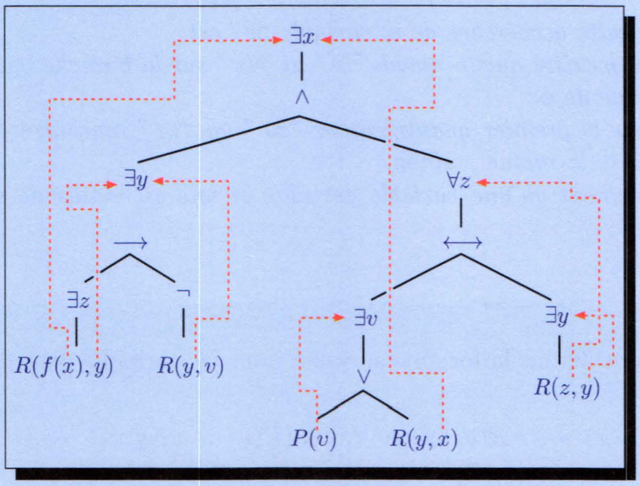
$$\Big(\big(\underbrace{(\neg P(x) \vee P(y))}_{1} \wedge \neg \underbrace{(\neg P(x) \vee P(y))}_{2}\big) \wedge \big) \underbrace{(\neg P(x) \vee P(y))}_{3} \longrightarrow \neg P(x)\big)\Big)$$

Il y a également 3 occurrences de $P(y)$, 4 occurrences de $\neg P(x)$ et 4 occurrences de $P(x)$.

6 Variables libres et variables liées

Résumé № 49

- *Une occurrence d'une variable x est* liée *par le premier nœud $\exists x$ ou $\forall x$ rencontré en remontant vers la racine.*
- *Une occurrence d'une variable qui n'est pas* liée *est* libre
- *Une variable est* libre *si elle possède une occurrence* libre.
- *Une formule est* close *si elle ne contient aucune variable libre.*
- *Si les variables libres de ϕ sont parmi $x_1, \ldots, x_n$, la* clôture universelle *de ϕ est la formule : $\forall x_1 \cdots \forall x_n\ \phi$.*



※

La quantification fait porter le poids du quantificateur sur une variable. On ne quantifie d'ailleurs que sur des variables, jamais sur d'autres termes. De la sorte, nous pouvons être amenés à dire que la nature même d'une variable est de se trouver sous la portée d'un quantificateur. Variables et quantificateurs forment les deux cotés d'un même objet de pensée. Il n'y a pas de quantification sans objet sur lequel cette quantification est censée s'exercer. Et la symbolisation de tels objets constitue la nature même de la variable. Inversement, une variable est quelque chose qui, comme son nom l'indique, doit varier, doit pouvoir prendre, en droit, différentes valeurs. Indiquer la portée de cette variation est précisément la raison d'être du quantificateur.

Or, les formules sont construites par induction. On construit d'abord la formule ϕ avant la formule $\exists x\ \phi$. Cela revient à dire que l'on construit d'abord des formules dans lesquelles les variables sont libres de tout lien à quelque quantificateur que ce soit.

Par ailleurs, dans la formule $\forall x\ \exists x\ P(x)$, il y a deux quantifications qui portent toutes deux sur la même variable, en l'occurrence : x. Laquelle de ces deux quantifications est la bonne ? De même, dans la formule $(P(x) \wedge \exists x\ P(x))$, la première occurrence de la variable x n'a pas le même poids que la dernière. La dernière se trouve sous la portée d'un quantificateur existentiel, la première est libre. Finalement, les deux formules $P(x)$ et $P(y)$ sont différentes, comme le sont également les deux formules $\exists x\ P(x)$ et $\exists y\ P(y)$. Mais ces dernières sont plus proches l'une de l'autre que les deux premières, la raison intuitive étant que lorsqu'on veut signifier qu'il existe un objet qui satisfait la propriété P, peut importe que l'on désigne cet objet par x ou par y, la variable n'est qu'un nom transitoire.

Pour toutes ces raisons, nous sommes maintenant amenés à distinguer les variables qui tombent sous la coupe d'une quantification et celles qui ne le sont pas. Plus précisément, nous allons distinguer parmi les différentes occurrences des variables, celles qui sont sous la portée d'un quantificateur (nous les appelerons *liées*) et celles qui ne le sont pas (que nous appellerons *libres*).

Définition 338 *Soient ϕ une formule de la logique du 1er ordre, $R(t_1, \ldots, t_n)$ l'une des feuilles de ϕ et x une occurrence d'une variable qui apparaît dans l'un des termes $t_1, \ldots, t_n$.*

- *On dit que cette occurrence de la variable "x" est*
  - libre *s'il n'existe aucun nœud "$\exists x$" ni "$\forall x$" sur la branche qui va de cette feuille à la racine de ϕ ;*
  - liée *– par le premier quantificateur "$\exists x$" ou "$\forall x$" rencontré en remontant de la feuille vers la racine – sinon.*
- *On dit également qu'une variable est libre si une au moins de ces occurrences est libre.*

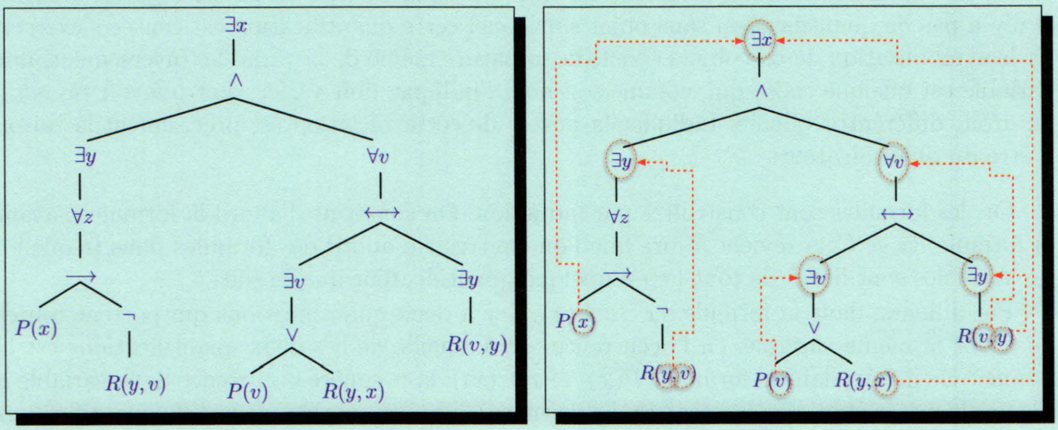
Exemple 339 Considérons la formule suivante dont les variables sont v, x, y, z :

$$\exists x \left(\exists y\ \forall z\ \big(P(x) \longrightarrow \neg R(y,v)\big)\ \wedge\ \forall v\Big(\exists v\big(P(v)\ \vee\ R(y,x)\big)\ \longleftrightarrow\ \exists y\ R(v,y)\Big)\right).$$

Colorions les occurrences de variables libres en vert, et liées en rouge :

$$\exists x \left(\exists y\ \forall z\ \big(P(x) \longrightarrow \neg R(y,v)\big)\ \wedge\ \forall v\Big(\exists v\big(P(v)\ \vee\ R(y,x)\big)\ \longleftrightarrow\ \exists y\ R(v,y)\Big)\right).$$

On se convainc beaucoup plus aisément en regardant la formule sous forme d'arbre :



6.1 Formules closes et clôture universelle

Définition 340 *Une variable libre dans une formule est une variable qui admet au moins une occurrence libre dans cette formule.*

Définition 341 *Une formule est* close *si elle ne contient aucune variable libre.*

Dans le meilleur des mondes possibles, nous voudrions n'employer que des formules closes. Pour cela, nous avons un bon moyen de traiter les formules qui ne le sont pas. Nous les transformons en formules closes en prenant la clôture universelle :

Définition 342 *Soit ϕ une formule dont les variables libres sont parmi $v_1, \ldots, v_n$, la clôture universelle de ϕ est la formule :*

$$\forall v_1 \, \forall v_2 \, \ldots \forall v_n \; \phi.$$

Remarque 343 L'ordre dans lequel on considère les variables libres n'a guère d'importance. Cela repose sur le fait que la sémantique de la logique du 1^{er} ordre interprète de la même manière la formule $\forall x \; \forall y \; \phi$ et $\forall y \; \forall x \; \phi$. La même remarque valant également pour le quantificateur existentiel : $\exists x \; \exists y \; \phi$ et $\exists y \; \exists x \; \phi$. Ces deux formules seront interprétées rigoureusement de la même manière. Mais cette remarque n'est plus valable lorsqu'on a une alternance de quantificateur : il ne faut surtout pas confondre $\forall x \; \exists y \; \phi$ et $\exists y \; \forall x \; \phi$. Intuitivement, $\forall x \; \exists y \; \phi$ signifie que pour chaque x, on peut choisir un y tel que la propriété, dont ϕ est chargée de rendre compte, est vraie. Alors que $\exists y \; \forall x \; \phi$ signifie que l'on peut choisir un y pour lequel la propriété ϕ va être vérifiée pour tous les x…

7 Substitutions dans les formules

***Résumé* № 50**

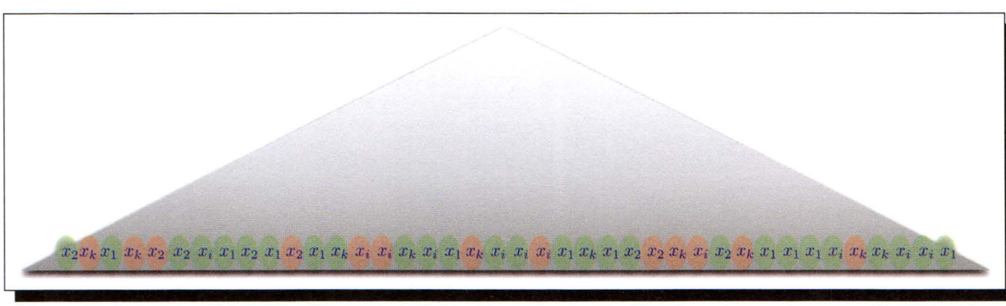
- *Substituer un terme t à une variable x à l'intérieur d'une formule ϕ, signifie remplacer chacune des occurrences* libres *de cette variable par le terme t. On obtient ainsi la formule $\phi_{[t/x]}$.*
- *Ce procédé se généralise, en un procédé simultané, à un nombre fini quelconque de termes et de variables.*

※

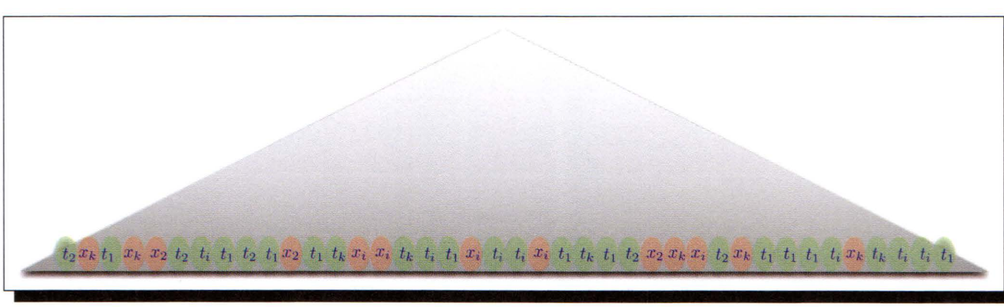
Nous avons vu précédemment (2.2) comment, à l'intérieur d'un terme, substituer des termes à des variables. Nous faisons maintenant un pas de plus : nous substituons toujours des termes à des variables, mais désormais nous le faisons à l'intérieur d'une formule. Cela semble aller de soi. Pourtant, il faut prêter attention à n'effectuer cette substitution que pour les seules occurrences des variables qui sont libres.

Définition 344 *Soient $\mathcal{L}$ un langage de la logique du 1er ordre, ϕ une formule, $x_1, x_2, \ldots, x_k$ des variables deux à deux distinctes, et $t, t_1, t_2, \ldots, t_k$ des termes de $\mathcal{L}$. La substitution des termes t_i $(1 \leq i \leq k)$ aux occurrences libres de chacune des variables respectives x_i $(1 \leq i \leq k)$ constitue la formule $\phi_{[t_1/x_1, t_2/x_2, \ldots, t_k/x_k]}$ obtenue en :*

(1) repérant les occurrences libres des variables $x_1, \ldots, x_n$:



(2) puis substituant simultanément *aux seules occurrences libres des variables $x_1, \ldots, x_n$, les termes $t_1, \ldots, t_n$:*



Cette définition a l'avantage d'être "visuellement" bien comprise. En effet, pour repérer quelles sont les occurrences libres des variables $x_1, \ldots, x_n$, il suffit de remonter le long de l'arbre de ϕ depuis la feuille dans laquelle se trouve la variable en question, jusqu'à la racine, à la recherche d'un quantificateur la liant. La substitution proprement dite consiste ensuite à "arracher" *simultanément* les occurrences libres des variables $x_1, \dots, x_n$ et les remplacer par les termes $t_1, \dots, t_n$.

Cette définition est généralement présentée comme suit, à partir de la forme linéaire des formules. Le lecteur pourra se convaincre que les deux définitions sont équivalentes, mais que la suivante est nettement moins intuitive.

Définition 345 (alternative linéaire) *Soient ϕ une formule, $x_1, x_2, \dots, x_k$ des variables deux à deux distinctes, et $t, t_1, t_2, \dots, t_k$ des termes, on définit la formule $\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]}$ comme étant le résultat de la substitution de chacun des termes t_i $(1 \leq i \leq k)$ aux occurrences libres de chacune des variables respectives x_i $(1 \leq i \leq k)$ dans la formule ϕ. La définition procède par induction sur la hauteur de ϕ.*

(1) si $ht(\phi) = 0$ alors $\phi = R(u_1, \dots, u_n)$ où $u_1, \dots, u_n$ sont des termes :

$$R(u_1, \dots, u_n)_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} = R(u_{1[t_1/x_1, t_2/x_2, \dots, t_k/x_k]}, \dots, u_{n[t_1/x_1, t_2/x_2, \dots, t_k/x_k]})$$

(Le lecteur se reportera à la Définition 321 pour la substitution dans les termes.)

(2) si $\phi = \neg\psi$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \neg\ \psi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]};$$

(3) si $\phi = (\psi_0 \vee \psi_1)$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \Big(\psi_{0[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} \vee \psi_{1[t_1/x_1, t_2/x_2, \dots, t_k/x_k]}\Big);$$

(4) si $\phi = (\psi_0 \wedge \psi_1)$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \Big(\psi_{0[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} \wedge \psi_{1[t_1/x_1, t_2/x_2, \dots, t_k/x_k]}\Big);$$

(5) si $\phi = (\psi_0 \longrightarrow \psi_1)$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \Big(\psi_{0[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} \longrightarrow \psi_{1[t_1/x_1, t_2/x_2, \dots, t_k/x_k]}\Big);$$

(6) si $\phi = (\psi_0 \longleftrightarrow \psi_1)$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \Big(\psi_{0[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} \longleftrightarrow \psi_{1[t_1/x_1, t_2/x_2, \dots, t_k/x_k]}\Big);$$

(7) si $\phi = \exists x\ \psi$, avec $x \notin \{x_1, x_2, \dots, x_k\}$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \exists x\ \psi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]};$$

(8) si $\phi = \forall x\ \psi$, avec $x \notin \{x_1, x_2, \dots, x_k\}$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \forall x\ \psi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]};$$

(9) si $\phi = \exists x_i\ \psi$, avec $x_i \in \{x_1, x_2, \dots, x_k\}$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \exists x_i\ \psi_{[t_1/x_1, t_2/x_2, \dots, t_{i-1}/x_{i-1}, t_{i+1}/x_{i+1}, \dots, t_k/x_k]};$$

(10) si $\phi = \forall x_i\ \psi$, avec $x_i \in \{x_1, x_2, \dots, x_k\}$:

$$\phi_{[t_1/x_1, t_2/x_2, \dots, t_k/x_k]} := \forall x_i\ \psi_{[t_1/x_1, t_2/x_2, \dots, t_{i-1}/x_{i-1}, t_{i+1}/x_{i+1}, \dots, t_k/x_k]}.$$

Exemple 346 Considérons la formule suivante dont les variables sont v, x, y :

$$\phi := \exists x \left(\exists y \; (P(x) \longrightarrow \neg R(y,v)) \; \wedge \; \forall v \Big(\exists v \big(P(v) \; \vee \; R(y, f(x)) \big) \; \longleftrightarrow \; \exists y \; R(v,y) \Big) \right).$$

opérons la substitution du terme $f(\mathsf{c})$ à la variable v et du terme c à la variable y : $\phi_{[f(\mathsf{c})/v,\ \mathsf{c}/y]}$.

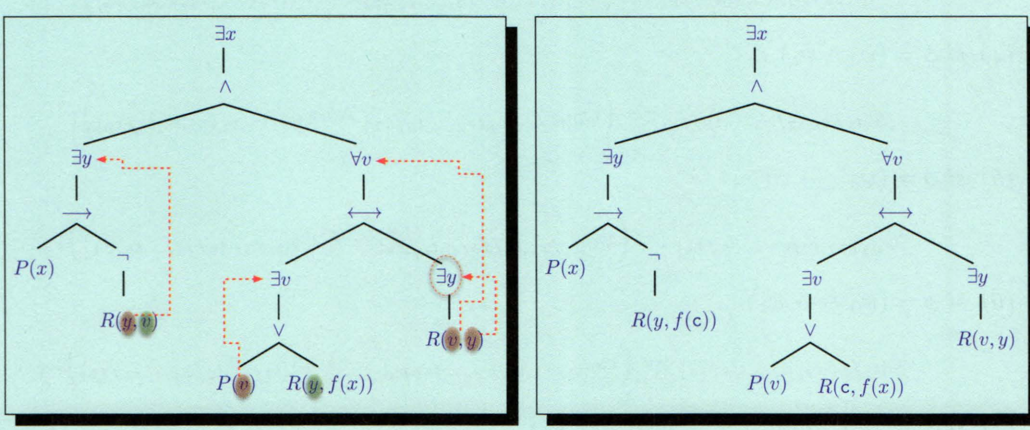
Pour cela, distinguons, en vert, les occurrences de ces deux variables qui sont libres et, en rouge, celles qui sont liées :

$$\phi := \exists x \left(\exists y \; (P(x) \longrightarrow \neg R(y,v)) \; \wedge \; \forall v \Big(\exists v \big(P(v) \; \vee \; R(y, f(x)) \big) \; \longleftrightarrow \; \exists y \; R(v,y) \Big) \right).$$

Nous obtenons :

$$\phi_{[f(\mathsf{c})/v,\ \mathsf{c}/y]}$$
$$:=$$
$$\exists x \left(\exists y \; (P(x) \longrightarrow \neg R(y, f(\mathsf{c}))) \; \wedge \; \forall v \Big(\exists v \big(P(v) \; \vee \; R(\mathsf{c}, f(x)) \big) \; \longleftrightarrow \; \exists y \; R(v,y) \Big) \right).$$

On se convainc beaucoup plus aisément en regardant la formule sous forme d'arbre.



7.1 Capture de variables

L'un des problèmes lorsque l'on fait de la substitution, c'est que des variables qui sont libres dans un terme peuvent être capturées par un quantificateur présent dans la formule dans laquelle elles prennent place. C'est le cas par exemple si nous considérons la formule $\phi = \exists x \; \neg x = y$ (qui signifie qu'il existe un élément qui n'est pas y) et que nous substituons le terme x à la variable y dans cette formule. Nous obtenons alors $\phi_{[x/y]}$ devient $\exists x \; \neg x = x$ qui signifie tout à fait autre chose, puisqu'elle dit qu'il existe un élément qui n'est pas lui-même, ce qui sera bien évidemment impossible à réaliser. Par contre si nous effectuons cette même substitution du terme x à la variable y dans la formule $\psi = \exists z\ \neg z = y$ – dont la signification est rigoureusement identique à la formule ϕ – nous obtenons $\psi_{[x/y]}$ devient $\exists z\ \neg z = x$ qui conserve le sens initial.

Pour cette raison nous veillerons à éviter la capture de variable et pour ce faire nous opérerons comme suit :

Avant de substituer les termes $t_1, \ldots, t_n$ aux occurrences libres des variables $x_1, \ldots, x_n$ dans la formule ϕ, il conviendra :

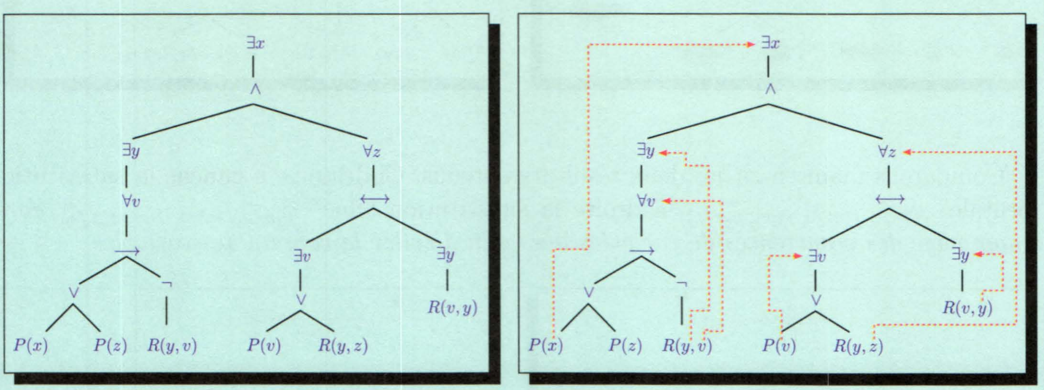
(1) d'effectuer la liste $v_1, \ldots, v_k$ de toutes les variables de la formule ϕ qui possèdent au moins l'une de leurs occurrences liées ;

(2) de choisir des nouvelles variables $z_1, \ldots, z_k$ qui n'apparaissent ni dans ϕ, ni dans les termes $t_1, \ldots, t_n$;

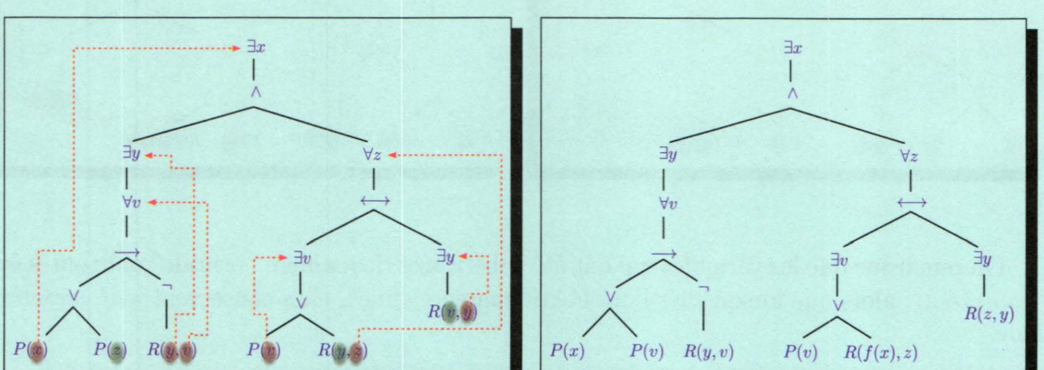
(3) puis, pour chaque variable v_i ($1 \leq i \leq k$), de remplacer chaque *occurrence liée* de v_i par z_i ainsi que chaque nœud $\exists v_i$ par $\exists z_i$ et chaque nœud $\forall v_i$ par $\forall z_i$;

(4) enfin, d'effectuer la substitution souhaitée.

Exemple 347 Considérons la formule ϕ à gauche ci-dessous dont les variables sont v, x, y, z, et repérons à droite les occurrences des variables qui sont liées :



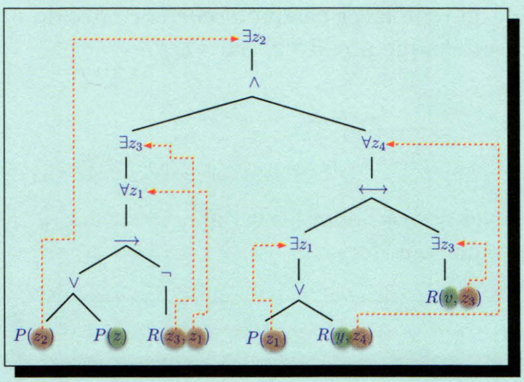
Effectuons tout d'abord la substitution "brutale" $\phi_{[z/v, f(c)/x, f(x)/y, v/z]}$:

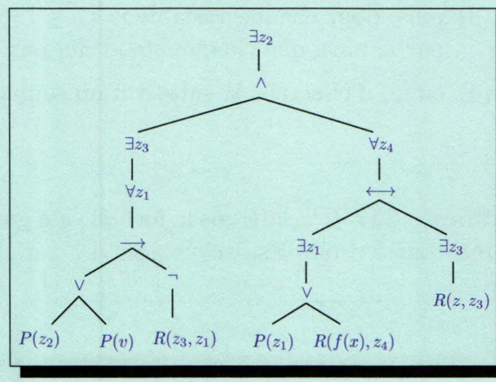


Effectuons maintenant la même substitution, mais en prenant soin d'éviter la *capture des variables*. Pour cela, renommons les variables dont les occurrences sont liées et effectuons les remplacements suivants :

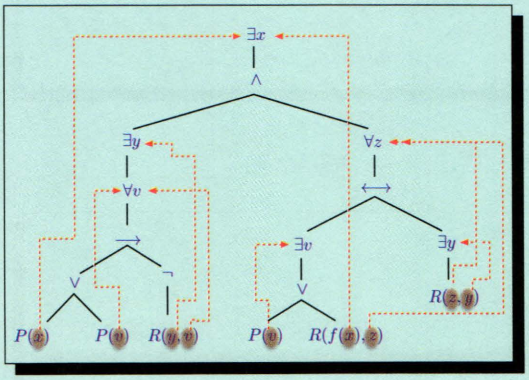
occ. liée $\rightsquigarrow$ n^{velle} *var.*	*quantif.* $\exists$	*quantif.* $\forall$
$v \rightsquigarrow z_1$	$\exists v \rightsquigarrow \exists z_1$	$\forall v \rightsquigarrow \forall z_1$
$x \rightsquigarrow z_2$	$\exists x \rightsquigarrow \exists z_2$	$\forall x \rightsquigarrow \forall z_2$
$y \rightsquigarrow z_3$	$\exists y \rightsquigarrow \exists z_3$	$\forall y \rightsquigarrow \forall z_3$
$z \rightsquigarrow z_4$	$\exists z \rightsquigarrow \exists z_4$	$\forall z \rightsquigarrow \forall z_4$

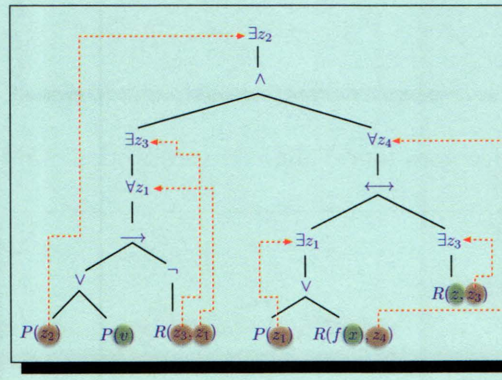
Cela donne la formule à gauche ci-dessous. Puis effectuons les substitutions souhaitées pour obtenir la formule ci-dessous à droite :





Comparons maintenant les deux résultats obtenus. Ci-dessous, à gauche la substitution "brutale" $\phi_{[z/v, f(\mathtt{c})/x, f(x)/y, v/z]}$, à droite la substitution "fine" $\phi_{[z/v, f(\mathtt{c})/x, f(x)/y, v/z]}$ *après renommage des occurrences de variables liées afin d'éviter la capture des variables* :





On remarque que les variables qui ont été substituées de manière "brutale" ont toutes été "*capturées*"; alors que lorsqu'elles l'ont été de manière "fine", elles conservent leur caractère *libre*.

Pour aller plus avant :

La syntaxe de la logique du 1^er^ ordre se retrouve dans de très nombreux livres. Parmi les ouvrages relativement faciles d'accès, nous recommandons particulièrement l'excellent *"An introduction to elementary logic"* de Wilfrid Hodges [Hod01]. Sont également recommandables car très accessibles *"Logic For Dummies"* de Mark Zegarelli [Zeg10], ainsi que l'*"Introduction à la logique"* de Jean Leroux [Ler98] ou les *"Eléments de logique contemporaine"* de François Lepage [Lep01].

Par ailleurs, la logique du 1^{er} ordre joue un rôle central en mathématiques, il n'est donc point étonnant de la retrouver très largement détaillée dans tous les ouvrages dont le titre comporte *"logique mathématique"*, *"mathematical logic"*, *"mathematische Logik"*, etc. Ceci dit, la syntaxe y est toujours exposée de manière linéaire : les termes sont des expressions linéaires, de même que les formules. Les formules telles que nous les présentons sous forme d'arbres, représentent dans ces ouvrages ce qu'ils appellent les *"arbres de décomposition"* des formules introduites de manière linéaire.

De ces ouvrages qui traitent de logique mathématique, nous recommandons tout particulièrement, parmi les ouvrages en français, *"Logique mathématique, tome 1 : Calcul propositionnel; algèbre de Boole; calcul des prédicats"* de René Cori et Daniel Lascar [CLK03a], *"Introduction à la logique"* d'André Delessert [Del88] et *"Eléments de logique mathématique : théorie des modèles"* de Georg Kreisel et Jean-Louis Krivine [KK67]. En allemand, on trouve le fameux manuel *"Einführung in die mathematische Logik"* de Heinz-Dieter Ebbinghaus, Jörg Flum et Wolfgang Thomas [EFT78]. En anglais, le choix est vaste. Nous retenons : *"A mathematical introduction to logic"* de Herbert B. Enderton [End72], *"A friendly introduction to mathematical logic"* de Christopher C. Leary [Lea99], *"Introduction to mathematical logic"* de Mendelson Mendelson [Men97], *"Mathematical logic : a first course"* de Joel W. Robbin [Rob69] et *"Mathematical logic"* de George Tourlakis [Tou11b].

Parmi les ouvrages anciens, le lecteur trouvera particulièrement plaisant de s'immerger dans *"Mathematical logic"*, de Joseph R. Shoenfield [Sho67], *"Introduction to Mathematical Logic"* d'Alonzo Church [Chu96], *"Mathematical Logic"* de Stephen C. Kleene [Kle67], ainsi que l'*"Introduction à la logique"* d'Alfred Tarski [Tar69]. Dans une perspective cette fois totalement historique, au lecteur qui souhaiterait se plonger dans les linéaments de la mise en place de la logique du 1^{er} ordre, nous recommandons tout particulièrement l'ouvrage *"From Freege to Gödel : A Source Book in Mathematical Logic, 1879-1931"* de Jean van Heijenoort [vH77].

Chapitre 11

Sémantique

1 Les modèles de la logique du 1^er^ ordre

***Résumé* № 51** *Etant donné un langage $\mathcal{L}$, un modèle $\mathcal{M}$ de la logique du 1^er^ ordre est une $\mathcal{L}$-structure qui se compose :*

- *d'un ensemble non vide appelé domaine de base (noté $M = |\mathcal{M}|$) sur lequel "varient" les variables.*
- *pour chaque symbole de constante c de $\mathcal{L}$, un élément $\mathsf{c}^{\mathcal{M}} \in M$;*
- *pour chaque symbole de fonction f de $\mathcal{L}$, une fonction $f^{\mathcal{M}} : M^n \longrightarrow M$ (où n désigne l'arité de f).*
- *pour chaque symbole de relation R de $\mathcal{L}$, une relation $R^{\mathcal{M}} \subseteq M^n$ (où n désigne l'arité de R).*

※

Les formules de la logique du 1^er^ ordre ne signifient rien en particulier. Afin de pouvoir les utiliser, il faut leur donner un sens. Ces formules sont des suites de symboles qui, d'une part, rappellent celles du Calcul Propositionnel, et d'autre part, ne sont que des symboles de fonctions, des symboles de relations et des quantificateurs. Donner un sens à de telles suites de signes, c'est tout d'abord interpréter ces symboles de relations par de "vraies" relations, ces symboles de fonctions par de "vraies" fonctions. Mais pour cela, il nous faut un domaine sur lequel agissent ces relations et ces fonctions. Ce domaine est aussi rendu nécessaire pour la bonne compréhension de l'usage des quantificateurs. Que ce soit le quantificateur universel ou le quantificateur existentiel, tous deux s'occupent de variables qui, comme leur nom l'indique, *varient* sur un domaine. Ce domaine constitue en quelque sorte l'univers des objets auxquels on s'intéresse. Cela peut être un univers extrêmement restreint, limité même à un seul élément. Mais celui-ci peut être aussi un vaste ensemble d'objets disparates, voire même un ensemble contenant une infinité d'objets, comme c'est le cas dans la plupart des structures qui intéressent les mathématiciens.

Nous voyons ainsi que la première différence majeure entre le Calcul Propositionnel et la logique du 1^er^ ordre réside dans la taille du domaine des modèles considérés. Dans le cadre du Calcul Propositionnel, les modèles ne comportent comme ensemble de base que l'ensemble à deux éléments $\{0, 1\}$ - qui symbolisent le vrai par 1 et le faux par 0. A l'opposé, dans la logique du 1^er^ ordre, les ensembles de base des modèles peuvent être rigoureusement n'importe quel ensemble non vide. Ce peut être aussi bien l'ensemble des individus de la planète que les atomes d'un morceau de sucre, les plaisanteries de Groucho Marx, les madeleines de Proust, les écrits de Platon, les nombres entiers, les nombres réels, les flocons de neige sur lesquels j'ai skié l'hiver dernier...

Définition 348 *Soit $\mathcal{L}$ un langage du 1er ordre dont la signature est composé :*

(1) des symboles de relations : $R_1, \ldots, R_k$;

(2) des symboles de fonctions : $f_1, \ldots, f_l$;

(3) des symboles de constantes : $\mathsf{c}_1, \ldots, \mathsf{c}_m$.

Un modèle $\mathcal{M}$ de la logique du 1er ordre (également appelé une $\mathcal{L}$-structure, ou encore une $\mathcal{L}$-réalisation) est une suite :

$$\mathcal{M} \;=\; \langle M, \mathsf{c}_1^{\mathcal{M}}, \ldots, \mathsf{c}_m^{\mathcal{M}}, f_1^{\mathcal{M}}, \ldots, f_l^{\mathcal{M}}, R_1^{\mathcal{M}}, \ldots, R_k^{\mathcal{M}} \rangle$$

où

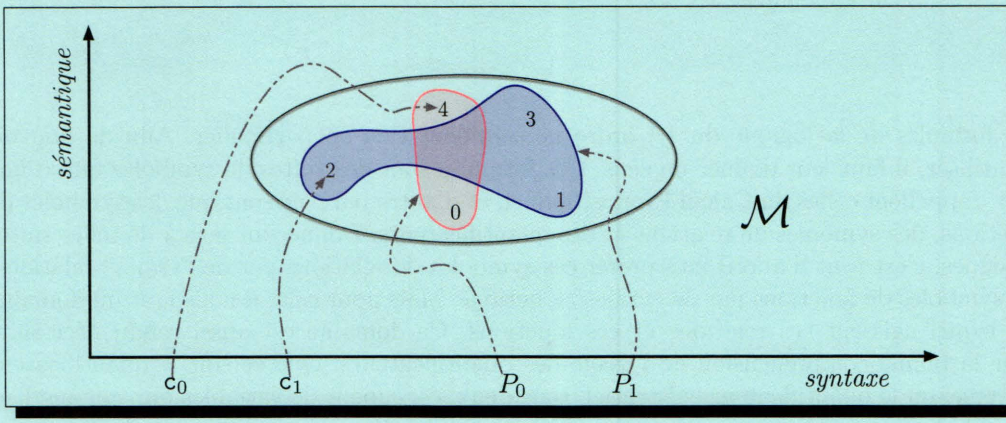
(1) M est un ensemble non vide, appelé ensemble de base *ou* domaine *du modèle ;*

(2) $\mathsf{c}_i^{\mathcal{M}}$ est un élément du domaine ($\mathsf{c}_i^{\mathcal{M}} \in M$) ;

(3) $f_i^{\mathcal{M}}$ est une fonction n_i-aire[1] de M dans M ($f_i : M^{n_i} \longrightarrow M$) ;

(4) $R_i^{\mathcal{M}}$ est une relation n_i-aire[2] sur M ($R_i^{\mathcal{M}} \subseteq M^{n_i}$).

Exemple 349 Considérons le langage qui contient deux symboles de constantes : c_0 et c_1, ainsi que deux symboles de relation unaire P_0 et P_1. Un modèle à cinq éléments peut être représenté par la figure ci-dessous.



Le domaine contient les entiers de 0 à 4, le symbole de constante c_0 est interprété par l'entier 4, le symbole de constante c_1 est interprété par l'entier 2. Le symbole de relation P_0 est interprété comme le sous-ensemble $\{0, 4\}$, et finalement P_1 est interprété comme le sous-ensemble $\{1, 2, 3\}$.

1. n_i désignant l'arité du symbole de fonction f_i, pour chaque $i \in \{1, \ldots l\}$.
2. n_i désignant l'arité du symbole de relation R_i, pour chaque $i \in \{1, \ldots m\}$.

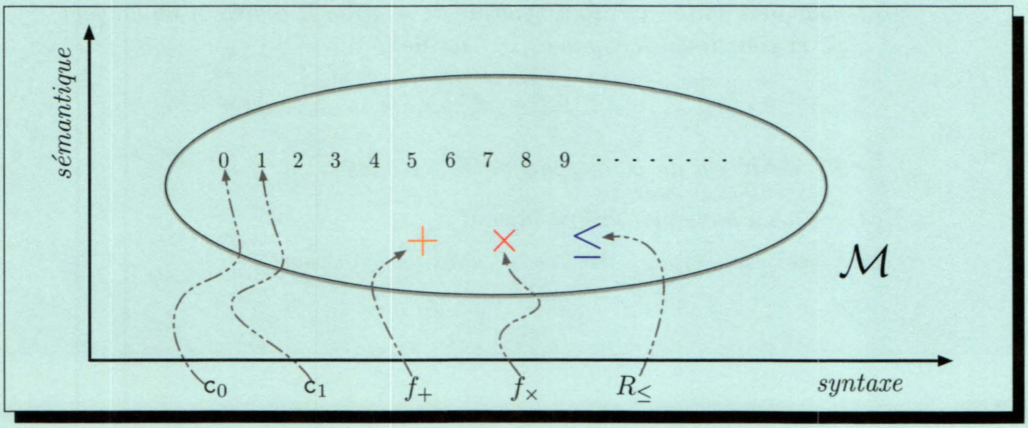
Exemple 350 Considérons le langage qui contient deux symboles de constante c_0 et c_1, deux symboles de fonctions binaires f_+ et $f_\times$, ainsi qu'un symbole de relation binaire $R_\leq$. Le modèle ci-dessous représente ce qu'on appelle généralement l'*arithmétique.*

(1) le domaine (M) de ce modèle est constitué de tous les entiers naturels ($\mathbb{N}$). C'est donc un ensemble infini ;

(2) c_0 est interprété par l'élément 0 et c_1 est interprété par l'élément 1. Autrement dit $\mathsf{c}_0^{\mathcal{M}} = 0$ et $\mathsf{c}_1^{\mathcal{M}} = 1$;

(3) f_+ est interprétée par l'addition et $f_\times$ par la multiplication : $f_+^{\mathcal{M}}$ est la fonction qui vérifie $f_+^{\mathcal{M}}(x,y) = x + y$ et $f_\times^{\mathcal{M}}$ celle qui vérifie $f^{\mathcal{M}}(x,y)_\times = x \times y$;

(4) $R_\leq$ est interprété par la relation d'ordre usuelle sur les entiers : $(a,b) \in R_\leq^{\mathcal{M}}$ ssi $a \leq b$.



2 Homomorphisme, isomorphisme et plongement

***Résumé* № 52** *Pour un langage du 1erordre $\mathcal{L}$ et $\mathcal{M}$, $\mathcal{N}$ deux $\mathcal{L}$-structures,*

(1) $\varphi : M \longrightarrow N$ est un homomorphisme de $\mathcal{M}$ dans $\mathcal{N}$ si :

(a) pour tout symbole de constante c de $\mathcal{L}$,

$$\varphi(\mathsf{c}^{\mathcal{M}}) = \mathsf{c}^{\mathcal{N}};$$

(b) pour tout entier n et tout symbole de fonction f d'arité n du langage $\mathcal{L}$, et pour tous éléments $a_1, \ldots, a_n$ de $|\mathcal{M}|$:

$$\varphi\left(f^{\mathcal{M}}(a_1, \ldots, a_n)\right) = f^{\mathcal{N}}\left(\varphi(a_1), \ldots, \varphi(a_n)\right);$$

(c) pour tout entier n et tout symbole de relation R d'arité n du langage $\mathcal{L}$, et pour tous éléments $a_1, \ldots, a_n$ de $|\mathcal{M}|$:

$$(a_1, \ldots, a_n) \in R^{\mathcal{M}} \implies (\varphi(a_1), \ldots, \varphi(a_n)) \in R^{\mathcal{N}}.$$

(2) $\varphi : M \longrightarrow N$ est un isomorphisme de $\mathcal{M}$ dans $\mathcal{N}$ si

(a) φ est un homomorphisme injectif *;*

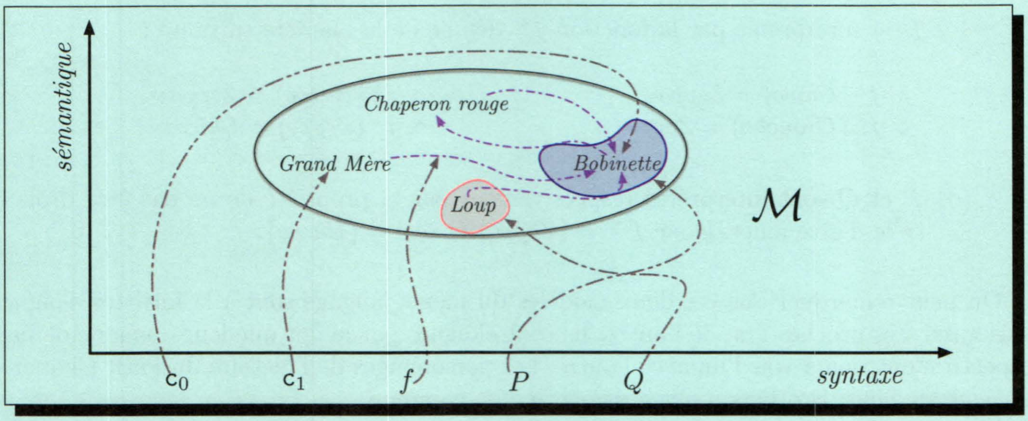
(b) "$\Longrightarrow$" est remplacé par "$\longleftrightarrow$" dans la définition (1)(c).

※

Lorsqu'on a différents modèles d'un même langage, il est souvent intéressant de les comparer. Les notions d'homomorphisme et d'isomorphisme sont une réponse à cette exigence comparative. Mais commençons par un exemple.

Exemple 351 Considérons le langage qui contient deux symboles de constante : c_0 et c_1, deux symboles de relation unaires P et Q, ainsi qu'un symbole de fonction unaire f. Nous allons donner deux modèles différents ($\mathcal{M}$ et $\mathcal{N}$) de ce langage. Mais ces modèles ne seront pourtant différents que par les "noms" des éléments ainsi que les "noms" des interprétations des symboles de constante, de fonction et de relation.

(1) Le modèle $\mathcal{M}$:



(a) le domaine (M) de ce modèle est l'ensemble contenant quatre éléments suivant : {*Chaperon rouge, Loup, Grand-Mère, Bobinette*} ;

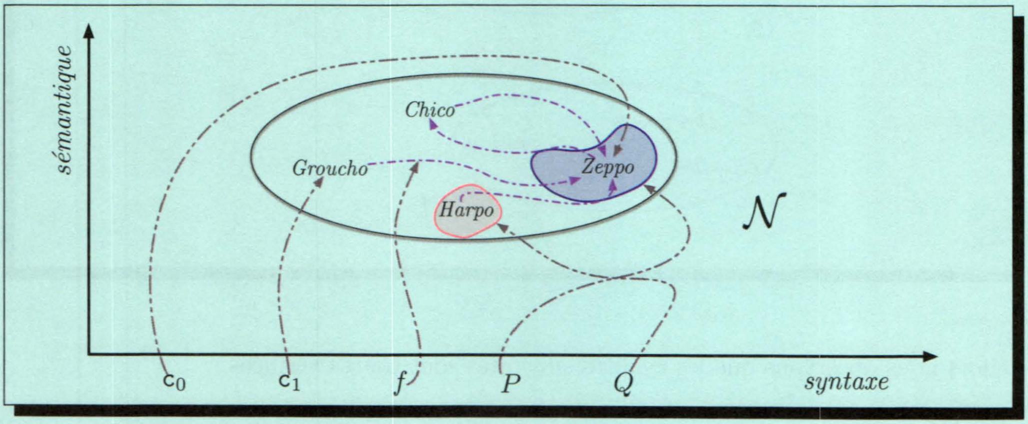
(b) c_0 est interprété par l'élément *Bobinette*. C'est-à-dire $c_0^{\mathcal{M}}$ =*Bobinette*; Et c_1 est interprété par l'élément *Grand-Mère*. C'est-à-dire $c_1^{\mathcal{M}}$ =*Grand-Mère*;

(c) f est interprétée par la fonction $f^{\mathcal{M}}$ définie par :

- $f^{\mathcal{M}}$(*Chaperon rouge*) = *Bobinette*,
- $f^{\mathcal{M}}$(*Grand-Mère*) = *Bobinette*,
- $f^{\mathcal{M}}$(*Loup*) = *Bobinette*,
- $f^{\mathcal{M}}$(*Bobinette*) = *Chaperon rouge*;

(d) P et Q sont interprétés respectivement par la propriété d'être inanimé et d'être assoiffé de sang. Donc $P^{\mathcal{M}}$ = {*Bobinette*} et $Q^{\mathcal{M}}$ = {*Loup*}.

(2) Le modèle $\mathcal{N}$:



(a) le domaine (M) de ce modèle est l'ensemble contenant les quatre Marx Brothers : {*Chico, Harpo, Groucho, Zeppo*} ;

(b) c_0 est interprété par l'élément *Zeppo*. C'est-à-dire $\mathsf{c}_0^{\mathcal{N}}$ =*Zeppo* ; Et c_1 est interprété par l'élément *Groucho*. C'est-à-dire $\mathsf{c}_1^{\mathcal{N}}$ =*Groucho* ;

(c) f est interprétée par la fonction $f^{\mathcal{N}}$ définie de la manière suivante :

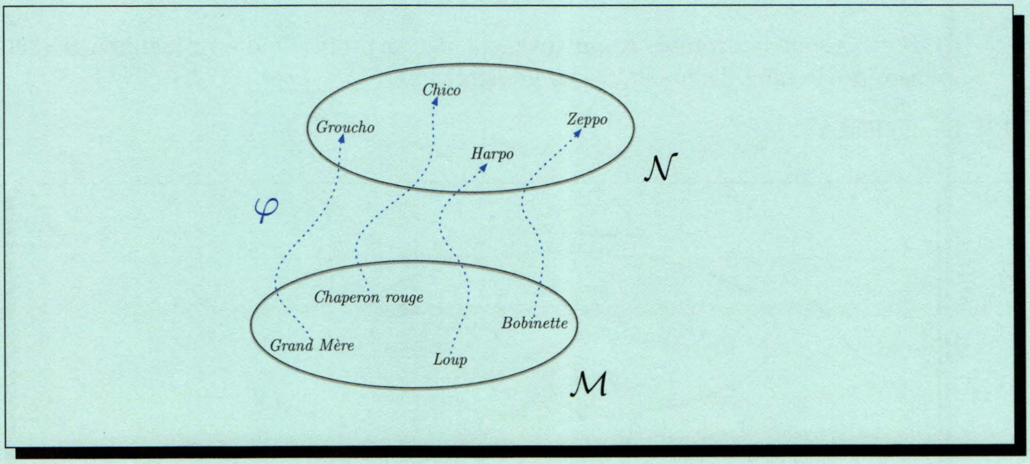
- $f^{\mathcal{N}}(\mathit{Chico}) = \mathit{Zeppo}$;
- $f^{\mathcal{N}}(\mathit{Harpo}) = \mathit{Zeppo}$;
- $f^{\mathcal{N}}(\mathit{Groucho}) = \mathit{Zeppo}$;
- $f^{\mathcal{N}}(\mathit{Zeppo}) = \mathit{Chico}$;

(d) P et Q sont interprétés respectivement par la propriété de ne pas être drôle et celle d'être muet. Donc $P^{\mathcal{N}} = \{\mathit{Zeppo}\}$ et $Q^{\mathcal{N}} = \{\mathit{Harpo}\}$.

On peut remarquer que ces deux modèles du même langage sont à la fois très éloignés, mais aussi très proches l'un de l'autre. Ils sont éloignés par le fait que leur domaine de base respectif n'ont rien à voir l'un avec l'autre. Les personnages de l'histoire du Petit Chaperon rouge et les Marx Brothers n'ont *a priori* rien en commun.

Mais pourtant, ces deux modèles sont plus proches que ne le laisse penser la disparité de leur domaine. En effet, tout porte à croire que *la Grand-Mère* et *Groucho Marx* ont le même rôle *par rapport aux interprétations des symboles du langage*. De même, *le Loup* et *Harpo*, *le Chaperon rouge* et *Chico*, et finalement *la Bobinette* et *Zeppo* ont des rôles tout à fait similaires dans les deux modèles.

Cela signifie qu'avec les interprétations du langage que nous avons dans un modèle et dans l'autre, *la Grand-Mère*, *le Loup*, *le Chaperon rouge* et *la Bobinette* ont exactement entre eux les mêmes relations que *Groucho Marx*, *Harpo*, *Chico* et *Zeppo*. Ou, pour le dire plus précisément, si nous considérons la bijection φ de M vers N indiquée dans le schéma ci-dessous :

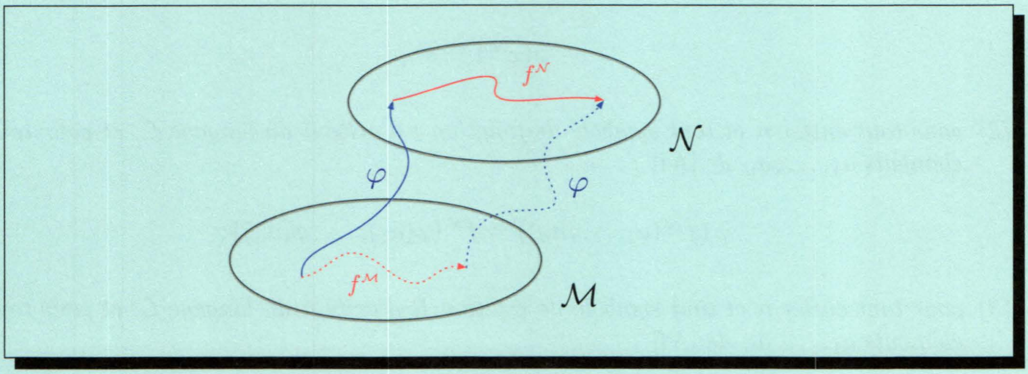


alors nous observons que les égalités suivantes sont toutes vérifiées :

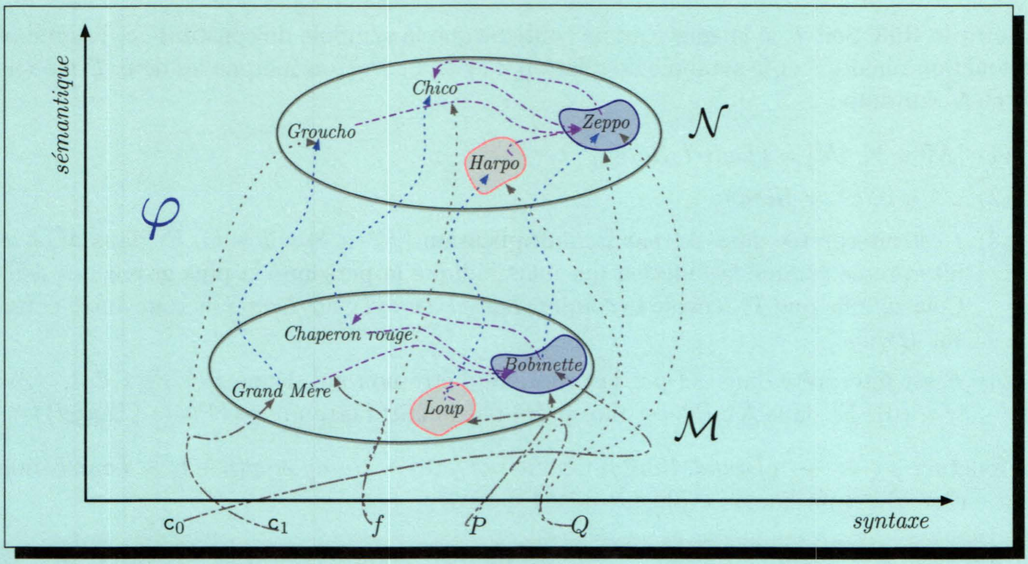
(1) $\mathsf{c}_0^{\mathcal{N}} = \varphi(\mathsf{c}_0^{\mathcal{M}})$ (2) $\mathsf{c}_1^{\mathcal{N}} = \varphi(\mathsf{c}_1^{\mathcal{M}})$ (3) pour chaque $a \in |\mathcal{M}|$:

- $a \in P^{\mathcal{M}} \Leftrightarrow \varphi(a) \in P^{\mathcal{N}}$
- $a \in Q^{\mathcal{M}} \Leftrightarrow \varphi(a) \in Q^{\mathcal{N}}$
- $\varphi(f^{\mathcal{M}}(a)) = f^{\mathcal{N}}(\varphi(a))$

cette dernière égalité est illustrée dans la figure ci-dessous, où le trajet en trait plein et celui en pointillé coïncident.



Tout cela se résume dans la figure qui suit :



On dit de deux tels modèles qu'ils sont *isomorphes*. Cela signifie qu'ils sont vraiment identiques, au changement de noms près. En effet, il n'est pas de manière de les distinguer par le langage. Le *Loup* et *Harpo*, par exemple, vérifient exactement les mêmes propriétés, eu égard aux interprétations de celles-ci dans leurs modèles respectifs.

Deux modèles isomorphes sont comme deux univers parfaitement équivalents. On ne peut les distinguer qu'en regardant le noms des éléments. Entre autres, deux modèles isomorphes vérifient exactement les mêmes formules du langage en question. Il n'est donc pas possible de les distinguer à l'aide d'une formule qui serait vraie dans l'un et fausse dans l'autre. Leurs différences sont inexprimables, elle sont *indiscibles* dans le langage.

Définition 352 *Soient $\mathcal{L}$ un langage du 1er ordre et $\mathcal{M}$, $\mathcal{N}$ deux $\mathcal{L}$-modèles,*
Un homomorphisme de $\mathcal{M}$ dans $\mathcal{N}$ est une fonction φ de M dans N qui vérifie :

(1) pour tout symbole de constante c de $\mathcal{L}$,

$$\varphi(\mathsf{c}^{\mathcal{M}}) = \mathsf{c}^{\mathcal{N}};$$

(2) pour tout entier n et tout symbole de fonction f d'arité n du langage $\mathcal{L}$, et pour tous éléments $a_1, \ldots, a_n$ de $|\mathcal{M}|$:

$$\varphi\left(f^{\mathcal{M}}(a_1, \ldots, a_n)\right) = f^{\mathcal{N}}\left(\varphi(a_1), \ldots, \varphi(a_n)\right);$$

(3) pour tout entier n et tout symbole de relation R d'arité n du langage $\mathcal{L}$, et pour tous éléments $a_1, \ldots, a_n$ de $|\mathcal{M}|$:

$$\textit{si } (a_1, \ldots, a_n) \in R^{\mathcal{M}} \textit{ alors } (\varphi(a_1), \ldots, \varphi(a_n)) \in R^{\mathcal{N}}.$$

Exemple 353 Soit $\mathcal{L}$ le langage qui ne contient que le symbole de constante c, le symbole de fonction binaire f et le symbole de relation d'arité 1 : P. Considérons les deux $\mathcal{L}$-modèles $\mathcal{M}$ et $\mathcal{N}$ suivants :

(1) $|\mathcal{M}| = \mathbb{N}$, $|\mathcal{N}| = \{\textit{Laurel}, \textit{Hardy}\}$

(2) $\mathsf{c}^{\mathcal{M}} = 0$, $\mathsf{c}^{\mathcal{N}} = \textit{Hardy}$;

(3) f est interprétée dans $\mathcal{M}$ par la multiplication ($f^{\mathcal{M}}(a, b) = a \times b$). Et dans $\mathcal{N}$, f est interprétée comme la fonction qui nous indique la personne la plus grosse des deux. Cela signifie que $f^{\mathcal{N}}$ envoie le couple (*Laurel*, *Laurel*) sur *Laurel* et tout autre couple sur *Hardy*.

(4) P est interprété dans $\mathcal{M}$ par la propriété d'être non nul. Donc $P^{\mathcal{M}} = \{1, 2, 3, \ldots\} = \mathbb{N} \setminus \{0\}$. Et dans $\mathcal{N}$, $P^{\mathcal{N}}$ est interprété par le fait d'être mince ($P^{\mathcal{N}} = \{\textit{Laurel}\}$).

La fonction $\varphi : \mathbb{N} \longrightarrow \{\textit{Laurel}, \textit{Hardy}\}$ définie par $\varphi(0) = \textit{Hardy}$ et $\varphi(n+1) = \textit{Laurel}$ (pour tout entier n) est un homomorphisme de $\mathcal{M}$ dans $\mathcal{N}$.

La fonction $\psi : \{\textit{Laurel}, \textit{Hardy}\} \longrightarrow \mathbb{N}$ définie par $\psi(\textit{Hardy}) = 0$ et $\psi(\textit{Laurel}) = 1$ est également un homomorphisme de $\mathcal{N}$ dans $\mathcal{M}$.

Ainsi, un homomorphisme d'une structure dans une autre est une fonction qui envoie les éléments de la première dans la seconde, tout en *respectant* les constantes, les fonctions et les relations de ces deux structures. L'image toute entière de la première structure par l'homomorphisme est comme une copie de cette première structure dans la seconde. C'est pourtant une copie imparfaite puisque rien n'indique que l'homomorphisme soit injectif. Et, en effet, dans la plupart des cas, les homomorphismes ne sont pas injectifs, comme c'est le cas dans l'exemple précédent. Si l'on veut s'approcher un peu plus de l'idée d'image fidèle de la première structure dans la seconde, il faut alors ajouter la condition d'injectivité et renforcer la dernière condition par une équivalence à la place d'une simple implication.

Définition 354 *Soient $\mathcal{L}$ un langage du 1^er^ ordre et $\mathcal{M}$, $\mathcal{N}$ deux $\mathcal{L}$-modèles. Un* plongement *$\mathcal{M}$ dans $\mathcal{N}$ est un homomorphisme φ de M dans N qui vérifie les deux conditions supplémentaires suivantes :*

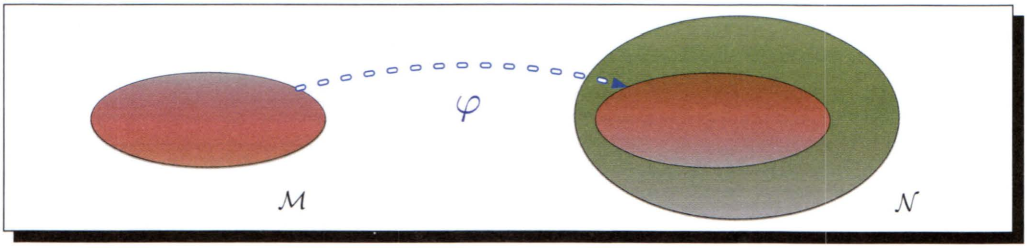
(1) φ est injectif ;

(2) pour tout entier n et tout symbole de relation R d'arité n du langage $\mathcal{L}$, et pour tous éléments $a_1, \ldots, a_n$ de $|\mathcal{M}|$:

$$(a_1, \ldots, a_n) \in R^{\mathcal{M}} \text{ si et seulement si } (\varphi(a_1), \ldots, \varphi(a_n)) \in R^{\mathcal{N}}.$$

Exemple 355 Dans l'exemple précédent, l'homomorphisme $\psi : \{Laurel, Hardy\} \longrightarrow \mathbb{N}$ est un plongement de $\mathcal{N}$ dans $\mathcal{M}$. Alors que l'homomorphisme $\varphi : \mathbb{N} \longrightarrow \{Laurel, Hardy\}$ n'est pas un plongement pour la raison qu'il n'est pas injectif.

Le plongement d'un modèle dans un autre détermine une copie conforme du premier modèle dans le second. En effet, l'injectivité du plongement implique que l'image du premier modèle dans le second forme une sous-structure du second modèle, parfaitement semblable au premier modèle, au changement de nom près. On a donc l'image indiquée dans la figure ci-dessous.



Pour être plus précis, dans l'image ci-dessus, l'image du domaine de $\mathcal{M}$ par le plongement forme un sous-modèle de $\mathcal{N}$ qui est isomorphe à $\mathcal{M}$. Cela signifie que cette image est une copie conforme du modèle de départ, une copie qui "vit" dans le modèle $\mathcal{N}$ et qui en forme donc une partie, une restriction : la restriction de toutes les interprétations des symboles de constantes, de fonctions, de relations, au domaine image du domaine de $\mathcal{M}$.

Définition 356 *Soient $\mathcal{L}$ un langage du 1^er^ ordre et $\mathcal{M}$, $\mathcal{N}$ deux $\mathcal{L}$-modèles,*
Un isomorphisme *de $\mathcal{M}$ dans $\mathcal{N}$ est un plongement* surjectif *de M dans N.*

Remarques 357

(1) Si φ est un isomorphisme de $\mathcal{M}$ dans $\mathcal{N}$, alors la fonction réciproque de φ (notée φ^{-1}) est un isomorphisme de $\mathcal{N}$ dans $\mathcal{M}$.

(2) On dit que $\mathcal{M}$ et $\mathcal{N}$ sont isomorphes, lorsqu'il existe un isomorphisme de l'un vers l'autre. Dans l'exemple 351, les deux modèles en question sont isomorphes. Dire que deux modèles sont isomorphes, cela signifie qu'ils sont infiniment proches, eu égard au langage à partir duquel ces modèles sont constitués. Le langage concrétise l'accessibilité à ces modèles. En fait, les modèles n'ont pas d'existence hors du langage

qu'ils réalisent. C'est par le langage, en tant qu'il véhicule leurs interprétations, qu'ils prennent corps. Donc, dire que deux modèles sont isomorphes, cela signifie qu'ils sont deux fois la même réalisation du langage *aux noms près des interprétations*. Si l'on oublie le nom des objets des deux domaines, ainsi que le nom des interprétations des différents symboles du langage, ces deux modèles n'en sont qu'un. Ils représentent, en fait, tous les deux le même monde, le même univers. Ce qui permet de les distinguer n'est que du ressort de la dénomination. Ou, pour le dire encore autrement, deux modèles isomorphes représentent la même structure logique, les éléments de l'un et de l'autre fonctionnant les uns par rapport aux autres rigoureusement de la même façon dans un modèle comme dans l'autre. Les relations structurelles sont identiques dans les deux modèles.

(3) La notion d'isomorphisme permet entre autre de rendre compte de manière formelle de la notion de métaphore. Une métaphore "transporte" le sens d'un univers imaginaire dans un autre, de la même manière que l'isomorphisme "transporte" la structure d'un modèle dans un autre.

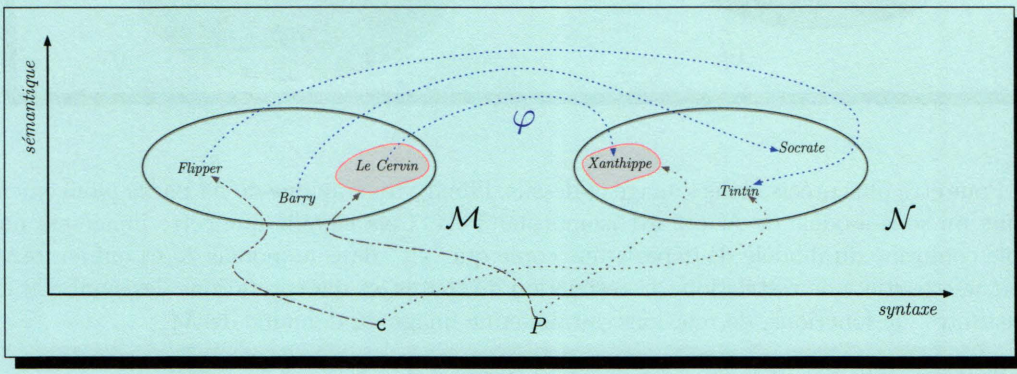
Exemple 358 Soit $\mathcal{L}$ le langage qui ne contient que le symbole de constante c et le symbole de relation P d'arité 1. Considérons les deux $\mathcal{L}$-modèles $\mathcal{M}$ et $\mathcal{N}$ suivants :

(1) $|\mathcal{M}| = \{$*Barry, Le Cervin, Flipper*$\}$, $|\mathcal{N}| = \{$*Xanthippe, Tintin, Socrate*$\}$.

(2) $\mathsf{c}^{\mathcal{M}} =$ *Flipper*, $\mathsf{c}^{\mathcal{N}} =$ *Tintin*.

(3) P est interprété dans $\mathcal{M}$ par la propriété d'être un sommet alpin et dans $\mathcal{N}$, par le fait d'être acariâtre. ($P^{\mathcal{M}} = \{$*Le Cervin*$\}$ et $P^{\mathcal{N}} = \{$*Xanthippe*$\}$).

Ces deux modèles sont isomorphes, comme indiqué dans la figure ci-dessous.



Bien sûr, pour que ces deux modèles ne soient plus isomorphes, il nous suffirait de les enrichir par des interprétations différentes de nouveaux symboles du langage. Mais pour cela, il faudrait également enrichir le langage lui-même. Nous voyons donc que la richesse du langage est un outil essentiel pour permettre de discerner les différents univers qui se présentent à nous.

En ce sens, il y a deux directions possibles en logique :

(1) Soit nous partons d'un langage formel, sur la base duquel nous constituons une théorie pour ensuite la confronter aux modèles possibles.

(2) Mais nous pouvons également procéder en sens inverse. Nous partons d'un modèle que nous cherchons à décrire. Nous nous donnons alors un langage dont les interprétations adhèrent au mieux à la structure de ce modèle tel que nous le percevons et grâce auquel nous explicitons la théorie de ce modèle, autrement dit, la nature de sa structure.

Pour aller plus avant :

Les notions d'homomorphisme, d'isomorphisme et de plongement sont parmi les premiers linéaments de la *"théorie des modèles"* qui est la partie de la logique dédiée à l'étude des relations qu'entretiennent les modèles entre eux. Le lecteur qui souhaiterait étendre le champs de ses connaissances dans cette direction regardera avec grand intérêt le livre *"A Shorter Model Theory"* de Wilfrid Hodges [Hod97].

Pour des ouvrages à la fois plus conséquents et dirigés avant tout vers les mathématiques, il y a *"Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles"* de René Cori et Daniel Lascar [CLK03b], *"Eléments de logique mathématique : théorie des modèles"* de Georg Kreisel et Jean-Louis Krivine [KK67], *"Introduction to model theory"* de Philipp Rothmaler [Rot00] et *"Models and games"* de Jouko Väänänen [Vää11].

Pour une approche sans concession, nous recommandons les plus difficiles *"Cours de théorie des modèles : une introduction à la Logique mathématique contemporaine"* de Bruno Poizat [Poi85], *"Model theory : an introduction"* de David Marker [Mar02], ainsi que *"Model theory"* de Chen C. Chang et H. Jerome Keisler [CK90].

Une approche différente consiste à se restreindre aux seuls modèles finis. Cette *"théorie des modèles finis"* est différente, mais les notions essentielles s'y retrouvent dans un cadre peut-être plus abordable. Nous conseillons sur ce point les livres *"Elements of finite model theory"* de Leonid Libkin [Lib04], ainsi que *"Finite model theory"* de Heinz-Dieter Ebbinghaus et Jörg Flum [EF05].

---

3 Satisfaction des formules dans une $\mathcal{L}$-structure

***Résumé* № 53** *L'évaluation d'une formule close ϕ ne comportant que les connecteurs $\neg, \vee, \wedge$ en une $\mathcal{L}$-structure $\mathcal{M}$ s'effectue au moyen d'un jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi)$ dans lequel deux joueurs – le* **V**érificateur *et le* **F**alsificateur *– opèrent :*

- *des choix de bifurcation le long de l'arbre de la formule ϕ :*
  - *le* **V**érificateur *choisit aux bifurcations de type "$\vee$" et*
  - *le* **F**alsificateur *choisit aux bifurcations de type "$\wedge$";*
- *des choix d'éléments du domaine $|\mathcal{M}|$:*
  - *le* **V**érificateur *choisit $a_i \in |\mathcal{M}|$ aux nœuds de type "$\exists x_i$" et*
  - *le* **F**alsificateur *choisit $a_i \in |\mathcal{M}|$ aux nœuds de type "$\forall x_i$";*
- *la partie s'arrête lorsqu'une feuille[a] $R(t_1, \ldots, t_n)$ est atteinte. Les variables $x_1, \ldots, x_k$ des termes $t_1, \ldots, t_n$ sont remplacées par les choix des éléments $a_1, \ldots, a_k$ des joueurs. Le* **V**érificateur *gagne si $\left(t_1^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]}, \ldots, t_k^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]}\right) \in R^{\mathcal{M}}$; le* **F**alsificateur *l'emporte sinon.*

$\mathcal{M} \models \phi$ *si le* **V**érificateur *possède une strat. gagn. dans* $\mathbb{E}v\,(\mathcal{M}, \phi)$.

※

a. Une feuille est nécessairement une formule atomique de la forme $R(t_1, \ldots, t_n)$.

3.1 Evaluation sous forme classique

Nous avons pour l'instant des formules du côté syntaxique et des modèles du côté sémantique. Il nous faut créer le lien entre les deux. Il nous reste donc à évaluer les formules dans les modèles, c'est-à-dire à préciser les conditions de vérité des formules dans les modèles, ce que l'on appelle la satisfaction des formules. La satisfaction d'une formule dans un modèle se fait tout naturellement par induction sur la hauteur de cette formule. Mais si les différents symboles du langage que sont les symboles de constantes, de fonctions et de relations ont bien une interprétation dans le modèle, il n'en est pas de même quant aux variables. Les variables n'ont aucune interprétation dans le modèle. Une variable n'est pas consignée à un élément du modèle comme l'est la constante. Une variable n'est attachée à aucun élément du domaine du modèle. Elle est libre comme l'air, c'est d'ailleurs pour cela qu'on l'appelle variable : parce qu'elle varie. Comme une variable est par nature changeante, il va falloir l'empêcher de varier, c'est-à-dire la fixer sur une valeur pour arriver à évaluer une formule dans laquelle cette variable est libre.

Il est à garder en mémoire que nous ne serons ultimement interessés que par les formules closes, c'est-à-dire celles qui n'ont précisément pas de variables libres. Alors pourquoi dès lors se préoccuper des variables libres ? La raison est simple et évidente : puisque nous souhaitons définir la satisfaction d'une formule par induction sur sa hauteur, nous serons nécessairement amenés à considérer les sous-formules de cette formule. Or, les sous-formules d'une formule close ne sont généralement pas closes ($\exists x\ \forall y\ f(x) = y$ est close mais ni $\forall y\ f(x) = y$, ni $f(x) = y$ ne sont closes).

Définition 359 *Soient $\mathcal{L}$ un langage du 1^{er} ordre, $\mathcal{M}$ un $\mathcal{L}$-modèle, t un terme du langage dont les variables sont parmi $x_1, \ldots, x_n$ et $\{a_1, \ldots, a_n\} \subseteq |\mathcal{M}|$.*

On définit $t^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]}$ l'interprétation du terme t dans la $\mathcal{L}$-structure $\mathcal{M}$, lorsque les variables $x_1, \ldots, x_n$ sont respectivement remplacées par $a_1, \ldots, a_n$ *:*

- *si $t = x_i$, alors $t^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]} = a_i$*
- *si $t = \mathsf{c}$ (un symbole de constante de $\mathcal{L}$), alors $t^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]} = \mathsf{c}^{\mathcal{M}}$*
- *si $t = f(t_1, \ldots, t_k)$, alors $t^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]} = f^{\mathcal{M}}(t_1^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]}, \ldots, t_k^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]})$.*

Définition 360 *Soient $\mathcal{L}$ un langage du 1^{er} ordre, $\mathcal{M}$ un $\mathcal{L}$-modèle, ϕ une formule dont les variables libres sont parmi $x_1, \ldots, x_n$ et $a_1, \ldots, a_n$ des éléments du domaine de $\mathcal{M}$.*

On note $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ le fait que la formule ϕ est satisfaite dans la $\mathcal{L}$-structure $\mathcal{M}$, lorsque les variables $x_1, \ldots, x_n$ sont respectivement remplacées par $a_1, \ldots, a_n$. *Cela se définit par induction sur la hauteur de ϕ par :*

- *si $\phi = R(t_1, \ldots, t_k)$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\left(t_1^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]}, \ldots, t_k^{\mathcal{M}[a_1/x_1,\ldots,a_n/x_n]}\right) \in R^{\mathcal{M}}$$

- *si $\phi = \neg\psi$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \not\models \psi$$

- *si $\phi = (\phi_0 \vee \phi_1)$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_0 \quad \textbf{ou} \quad \mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_1$$

- *si $\phi = (\phi_0 \wedge \phi_1)$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_0 \quad \textbf{et} \quad \mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_1$$

- *si $\phi = (\phi_0 \longrightarrow \phi_1)$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \not\models \phi_0 \quad \textbf{ou} \quad \mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_1$$

- *si $\phi = (\phi_0 \longleftrightarrow \phi_1)$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_0 \quad \textbf{ssi} \quad \mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi_1$$

- *si $\phi = \exists x\ \psi$ avec $x \notin \{x_1, \ldots, x_n\}$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\textbf{il existe } \textit{un élément } a \in |\mathcal{M}| \textit{ tel que } \mathcal{M}, a/x, a_1/x_1, \ldots, a_n/x_n \models \psi$$

- *si $\phi = \forall x\ \psi$ avec $x \notin \{x_1, \ldots, x_n\}$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\textbf{pour tout } \textit{élément } a \in |\mathcal{M}|, \quad \mathcal{M}, a/x, a_1/x_1, \ldots, a_n/x_n \models \psi$$

- *si $\phi = \exists x_i\ \psi$, alors $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi$ si et seulement si*

$$\textbf{il existe } a \in |\mathcal{M}| \textit{ tel que } \mathcal{M}, a_1/x_1, \ldots, a_{i-1}/x_{i-1}, a/x_i, a_{i+1}/x_{i+1}, \ldots, a_n/x_n \models \psi$$

- *si* $\phi = \forall x_i\ \psi$, *alors* $\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \ \vDash \phi$ *si et seulement si*

$$\textbf{pour tout } a \in |\mathcal{M}|, \quad \mathcal{M}, a_1/x_1, \ldots, a_{i-1}/x_{i-1}, a/x_i, a_{i+1}/x_{i+1}, \ldots, a_n/x_n \ \vDash \psi.$$

Remarques 361

(1) Si la formule ϕ est close, la satisfaction de ϕ dans le modèle $\mathcal{M}$ se note simplement $\mathcal{M} \vDash \phi$.

(2) La définition de la satisfaction de la formule ϕ dans la $\mathcal{L}$-structure $\mathcal{M}$ lorsque les variables $x_1, \ldots, x_n$ sont respectivement remplacées par $a_1, \ldots, a_n$, ne dépend absolument pas de l'ordre dans lequel on considère ces variables.

(3) La définition de la satisfaction d'une formule de la logique du 1^er ordre n'est somme toute pas très éloignée de celle que l'on rencontre en Calcul Propositionnel. La validité reposant sur les connecteurs logiques est finalement la même. La différence majeure vient de la quantification. C'est elle qui rend nécessaire ces objets plutôt complexes que sont les formules atomiques. Mais la satisfaction d'une formule atomique s'avère plus simple qu'il n'y paraît : elle repose sur le fait de savoir si des éléments du modèles sont ou ne sont pas dans une certaine relation.

Définition 362 *Soient $\mathcal{L}$ un langage du 1^er ordre, $\mathcal{M}$ une $\mathcal{L}$-structure et ϕ une formule dans ce langage,*

$$\mathcal{M} \textit{ est un } \text{modèle} \textit{ de } \phi \textit{ si et seulement si } \mathcal{M} \vDash \phi.$$

Exemple 363 Reprenons le modèle $\mathcal{M}$ de l'exemple 351 :

(1) $\mathcal{M} \vDash P(\mathsf{c}_0)$, car $\mathsf{c}_0^{\mathcal{M}} = \textit{Bobinette}$ et $\textit{Bobinette} \in P^{\mathcal{M}}$.

(2) $\mathcal{M} \nvDash \forall x\ P(x)$, car, par exemple, *le Loup* $\notin P^{\mathcal{M}}$.

(3) $\mathcal{M} \vDash \forall x\ (P(x) \lor P(f(x)))$, car l'élément *Bobinette* satisfait la propriété $P^{\mathcal{M}}$, et les trois autres ont comme image par $f^{\mathcal{M}}$ l'élément *Bobinette*.

(4) $\mathcal{M} \nvDash \exists x\ (P(x) \land P(f(x)))$, car le seul élément qui satisfasse la propriété $P^{\mathcal{M}}$ est *Bobinette*, or son image par $f^{\mathcal{M}}$ est *Le Chaperon rouge* qui ne satisfait malheureusement pas cette propriété.

(5) $\mathcal{M} \nvDash (\exists x\ \forall y\ ((Q(y) \land P(f(x))) \longrightarrow \neg P(y)) \longleftrightarrow P(\mathsf{c}_1))$.
Car $\mathcal{M} \nvDash P(\mathsf{c}_1)$, alors que $\mathcal{M} \vDash \exists x\ \forall y\ ((Q(y) \land P(f(x))) \longrightarrow \neg P(y))$. Pour voir que $\mathcal{M} \vDash \exists x\ \forall y\ ((Q(y) \land P(f(x))) \longrightarrow \neg P(y))$, il suffit de prendre *Bobinette* comme valeur pour x. La valeur de $(Q(y) \land P(f(x)))$ est alors toujours fausse indépendamment du choix de y, et donc $((Q(y) \land P(f(x))) \longrightarrow \neg P(y))$ est toujours vraie.

Nous allons maintenant proposer un modèle, donc un langage particulier, ainsi qu'une formule qui rende compte précisément du syllogisme suivant :

Tous les hommes sont mortels ;
Socrate est un homme ;
donc Socrate est mortel.

Pour cela, la manière de rendre compte des propriétés d'être mortel ou d'être un homme (que l'on considérera comme celle d'être un humain) consiste à les interpréter comme des relations unaires. Par conséquent, ces propriétés, vues comme des relations unaires, sont l'interprétation de symboles de relation unaire.

L'individu Socrate est un des objets du domaine, le fait qu'il soit dénommé ainsi nécessite de prendre dans le langage un symbole de constante qui désigne cet individu précis.

Quant au domaine, nous avons le choix, il dépend simplement de la manière dont nous interprétons ce dont parle ce syllogisme. S'agit-il des objets sur terre à ce moment-là ? Ou bien de tous les objets de l'univers ? Uniquement des hommes ? La manière dont nous percevons la signification des arguments de ce syllogisme détermine le domaine du modèle que nous considérerons.

Exemple 364 Considérons le langage $\mathcal{L}$ qui contient deux symboles de prédicat unaire H et M, ainsi que le symbole de constante s. Définissons le modèle $\mathcal{M}$ de la manière suivante :

(1) $|\mathcal{M}|$ = *l'ensemble des choses sur terre à l'époque de Socrate* ;

(2) $H^{\mathcal{M}}$ = *l'ensemble des êtres humains* ;

(3) $M^{\mathcal{M}}$ = *l'ensemble des choses mortelles* ;

(4) $s^{\mathcal{M}}$ = *Socrate.*

Les différentes parties de ce syllogisme s'interprètent de la manière suivante :

(1) $\mathsf{H}(\mathsf{s})$: *Socrate est un homme*,

(2) $\mathsf{M}(\mathsf{s})$: *Socrate est mortel* (*est un mortel*),

(3) $\forall x\ \big(\mathsf{H}(x) \longrightarrow \mathsf{M}(x)\big)$: *Tout être humain est mortel* (*pour toute chose, si cette chose est humaine, alors elle est mortelle*),

(4) $\Big(\forall x\ \big(\mathsf{H}(x) \longrightarrow \mathsf{M}(x)\big) \wedge \mathsf{H}(\mathsf{s})\Big)$: *Tout être humain est mortel, et Socrate est un homme*,

(5) $\Big(\big(\forall x\ (\mathsf{H}(x) \longrightarrow \mathsf{M}(x)\big) \wedge \mathsf{H}(\mathsf{s})\Big) \longrightarrow \mathsf{M}(\mathsf{s})$: *si, à la fois, tout être humain est mortel et Socrate est un homme, alors Socrate est mortel.*

Exemple 365 Reprenons le langage de l'exemple précédant, mais changeons de modèle, en prenant par exemple :

(1) $|\mathcal{N}|$ = *l'ensemble des personnages de cartoons* ;

(2) $H^{\mathcal{N}}$ = *l'ensemble des super héros* ;

(3) $M^{\mathcal{N}}$ = *l'ensemble des personnages doués de pouvoirs extraordinaires*;

(4) $s^{\mathcal{N}}$ = *Spiderman.*

On obtient, comme signification des différentes formules suivantes :

(1) $\mathsf{H}(\mathsf{s})$: *Spiderman est un super héros,*

(2) $\mathsf{M}(\mathsf{s})$: *Spiderman possède des pouvoirs extraordinaires,*

(3) $\forall x\ \big(\mathsf{H}(x) \longrightarrow \mathsf{M}(x)\big)$: *Tout super héros possède des pouvoirs extraordinaires,*

(4) $\Big(\forall x\ \big(\mathsf{H}(x) \longrightarrow \mathsf{M}(x)\big) \wedge \mathsf{H}(\mathsf{s})\Big)$: *Tout super héros possède des pouvoirs extraordinaires, et Spiderman est un super héros,*

(5) $\Big(\big(\forall x\ (\mathsf{H}(x) \longrightarrow \mathsf{M}(x)\big) \wedge \mathsf{H}(\mathsf{s})\Big) \longrightarrow \mathsf{M}(\mathsf{s})$: *si, à la fois, tout super héros possède des pouvoirs extraordinaires et Spiderman est un super héros, alors Spiderman possède des pouvoirs extraordinaires.*

Remarque 366 Lorsque nous voulons exprimer le fait qu'il existe un individu x satisfaisant la propriété P qui satisfait également la propriété Q, la bonne formulation est

$$\exists x\ \big(P(x) \wedge Q(x)\big).$$

Par contre, lorsque nous voulons dire que tous les individus satisfaisant la propriété P satisfont aussi la propriété Q, la bonne formulation devient

$$\forall x\ \big(P(x) \longrightarrow Q(x)\big).$$

Et non pas $\forall x\ \big(P(x) \wedge Q(x)\big)$, qui signifie que tous les individus satisfont les deux propriétés en question.

Définition 367 *Soient $\mathcal{L}$ un langage du 1er ordre et ϕ, ψ deux formules dans ce langage,*

On dit que ces deux formules sont équivalentes (noté $\phi \equiv \psi$) si et seulement si elles ont exactement les mêmes modèles.

$$\phi \equiv \psi \text{ ssi pour toute } \mathcal{L}\text{-structure } \mathcal{M}, \quad (\mathcal{M} \vDash \phi \text{ ssi } \mathcal{M} \vDash \psi)\,.$$

Deux formules équivalentes sont indiscernables par un quelconque modèle. Il n'existe pas de modèle dans lequel l'une serait vraie et l'autre fausse. Autrement dit, d'un point de vue sémantique, ces formules sont identiques.

Remarque 368 Pour tout langage $\mathcal{L}$ et toute formule ϕ, il existe au moins une formule ψ (en fait une infinité) telle que

- ψ ne contient aucun des deux connecteurs logiques $\longrightarrow$ et $\longleftrightarrow$.
- $\phi \equiv \psi$.

Il suffit en effet de remarquer que, d'une part

$$(\phi_0 \longrightarrow \phi_1) \equiv (\neg\phi_0 \vee \phi_1)$$

et d'autre part

$$(\phi_0 \longleftrightarrow \phi_1) \equiv ((\phi_0 \wedge \phi_1) \vee (\neg\phi_0 \wedge \neg\phi_1)).$$

3.2 Evaluation par les jeux

Nous allons présenter la satisfaction d'une formule de la logique du 1^{er} ordre dans un modèle, au moyen d'un jeu d'évaluation semblable à celui que nous avons utilisé dans le cadre du Calcul Propositionnel. En fait, ce jeu d'évaluation est en quelque sorte une extension de celui du Calcul Propositionnel.

Mais avant de définir ce jeu, et afin d'en simplifier grandement les règles, convenons de ne jouer celui-ci qu'avec des formules ne contenant que $\wedge$ et $\vee$ comme connecteurs logiques binaires. Cela ne pose pas de problème puisque nous savons, par la remarque 368, que toute formule est équivalente à une formule de cette forme.

On se donne donc tout d'abord un langage du 1^{er} ordre $\mathcal{L}$, puis une $\mathcal{L}$-structure $\mathcal{M}$ et une formule ϕ écrite dans le langage $\mathcal{L}$. Le *jeu d'évaluation* $\mathbb{E}v\,(\mathcal{M}, \phi)$ est un jeu fini à deux joueurs et à information parfaite, ce qui permet de rendre compte de la satisfaction ou non de la formule ϕ dans la $\mathcal{L}$-structure $\mathcal{M}$. Les règles de ce jeu sont très proches de celles du jeu d'évaluation décrit dans le cadre du Calcul Propositionnel. Comme ce jeu est un cas particulier des jeux finis à deux joueurs et à information parfaite, il est déterminé. L'un des deux joueurs possède une stratégie gagnante. Nous verrons que l'existence d'une stratégie gagnante pour un joueur correspond exactement à la satisfaisabilité de la formule ϕ dans la $\mathcal{L}$-structure $\mathcal{M}$.

Définition 369 *Soient $\mathcal{L}$ un langage du 1^{er} ordre, ϕ une formule* close *dont tous les connecteurs logiques sont parmi $\{\neg, \vee, \wedge\}$ et $\mathcal{M}$ une $\mathcal{L}$-structure,*

Le jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi)$ est défini comme suit :

(1) il comprend deux joueurs appelés **V**érificateur *et* **F**alsificateur. *Le* **V**érificateur *(**V**) cherche à montrer que la formule est satisfaite dans la $\mathcal{L}$-structure ($\mathcal{M} \models \phi$), alors que le but du* **F**alsificateur *(**F**) est, au contraire, de montrer que cette formule est fausse ($\mathcal{M} \not\models \phi$).*

Les coups de ces deux joueurs consistent à choisir des sous-formules en respectant les règles suivantes :

si la position actuelle du jeu est...	*c'est au tour de...*	*le jeu continue avec...*
$\varphi_0 \vee \varphi_1$	**V** *choisit* $j \in \{0,1\}$	φ_j
$\varphi_0 \wedge \varphi_1$	**F** *choisit* $j \in \{0,1\}$	φ_j
$\neg\varphi$	**F** *et* **V** *échangent leurs rôles*	φ
$\exists x_i \varphi$	**V** *choisit* $a_i \in \lvert\mathcal{M}\rvert$	$\varphi[a_i/x_i]$
$\forall x_i \varphi$	**F** *choisit* $a_i \in \lvert\mathcal{M}\rvert$	$\varphi[a_i/x_i]$
$R(t_1,\ldots,t_k)_{[a_1/x_1,\ldots,a_n/x_n]}$	*Stop*	**V** *gagne ssi* $\mathcal{M}, a_1/x_1,\ldots,a_n/x_n \models R(t_1,\ldots,t_k)$

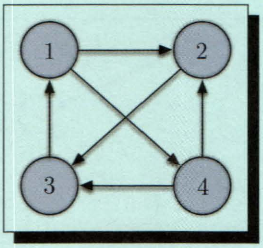
(2) La condition de gain de la partie apparaît une fois celle-ci terminée, c'est-à-dire lorsque la sous-formule en jeu n'est plus qu'une formule atomique $R(t_1,\ldots,t_k)_{[a_1/x_1,\ldots,a_n/x_n]}$. A noter que les règles du jeu sont faites afin que – partant d'une formule close – on aboutisse nécessairement à une formule atomique qui ne contienne aucune variable (puisque chaque variable a été, au cours de la partie, remplacée par un élément du modèle)[3]*. Le joueur* **V** *gagne si $R(t_1,\ldots,t_k)$ est satisfaite dans la $\mathcal{L}$-structure étendue $\mathcal{M}, a_1/x_1,\ldots,a_n/x_n$ ($\mathcal{M}, a_1/x_1,\ldots,a_n/x_n \models R(t_1,\ldots,t_k)$), et* **F** *l'emporte dans le cas contraire.*

Remarque 370 Dans la définition des coups de ce jeu, lorsque la formule à décomposer est de la forme $\exists x\ \psi$ ou bien $\forall x\ \psi$, il faut bien prendre garde que l'élément du domaine que choisit le joueur dont c'est le tour de jouer (le ***Vérificateur*** dans le cas d'un quantificateur existentiel et le ***Falsificateur*** dans le cas d'un quantificateur universel) ne remplace que les occurrences libres de la variable en question. Dans les deux cas, la partie continue avec $\psi_{[a/x]}$. Ainsi, par exemple, pour la formule $\forall x\ \exists x\ \psi$, le joueur ***Falsificateur*** choisit $a \in |\mathcal{M}|$ et la partie continue avec $(\exists x\ \psi)_{[a/x]}$ qui n'est autre que $\exists x\ \psi$ puisqu'il n'y a aucune occurrence libre de la variable x dans cette formule. Ensuite, le joueur ***Vérificateur*** choisit $b \in |\mathcal{M}|$ et la partie continue avec $\psi_{[b/x]}$. On voit donc que le coup du joueur ***Falsificateur*** n'a strictement aucune incidence sur le déroulement de la partie, c'est un coup pour rien.

3. Pour être parfaitement précis, il faudrait dire non pas que nous remplaçons une variable x_i par un élément a_i du modèle, mais que nous remplaçons x_i par un *nouveau* symbole de constante $\mathtt{c}_{a_i}$, dont l'interprétation est précisement l'élément a_i, et la formule à laquelle nous nous arrêtons est en fait de la forme $R(t_1,\ldots,t_k)_{[\mathtt{c}_{a_1}/x_1,\ldots,\mathtt{c}_{a_n}/x_n]}$.

Exemple 371 Considérons le langage qui ne contient qu'un symbole de relation binaire E, la formule $\forall x \forall y\, (E(x,y) \ \vee\ \exists z(E(x,z) \ \wedge\ E(z,y)))$, et le modèle $\mathcal{M}$ défini par :

- $|\mathcal{M}| = \{1,2,3,4\}$,
- $E^{\mathcal{M}}$ est définie par $(a,b) \in E^{\mathcal{M}}$ si et seulement s'il existe une flèche de a vers b dans le graphe ci-dessous :



Un exemple de partie dans le jeu $\mathbb{E}v\Big(\mathcal{M}, \forall x \forall y\big(E(x,y) \ \vee\ \exists z(E(x,z) \ \wedge\ E(z,y))\big)\Big)$:

joueur	coup	la partie continue avec
F	prend 2	$\forall y\, (E(2,y) \ \vee\ \exists z(E(2,z) \ \wedge\ E(z,y)))$
F	prend 4	$E(2,4) \ \vee\ \exists z(E(2,z) \ \wedge\ E(z,4))$
V	choisit	$\exists z(E(2,z) \ \wedge\ E(z,4))$
V	prend 3	$E(2,3) \ \wedge\ E(3,4)$
F	choisit	$E(3,4)$
	Stop	**F** gagne.

Exemple 372 Considérons le langage qui contient un symbole de relation unaire P, un symbole de relation binaire R et un symbole de fonction unaire f, la formule $\forall x\, \Big(P(x) \ \vee\ \exists y\, R\big(f(x),y\big)\Big)$, et le modèle $\mathcal{M}$ défini par :

- $|\mathcal{M}| = \{Laurel, Hardy\}$,
- $P^{\mathcal{M}}$ est définie par la propriété d'être mince ($P^{\mathcal{M}} = \{Laurel\}$),
- $R^{\mathcal{M}}$ est définie par $(a,b) \in R^{\mathcal{M}}$ ssi b est plus gros que a – i.e. $R^{\mathcal{M}} = \{(Laurel, Hardy)\}$.
- $f^{\mathcal{M}}$ échange les partenaires : $f^{\mathcal{M}}(Laurel) = Hardy$ et $f^{\mathcal{M}}(Hardy) = Laurel$.

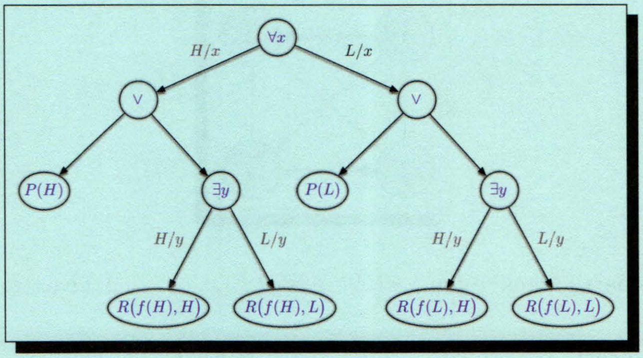
A des fins de concision, nous noterons par la suite L pour *Laurel* et H pour *Hardy*.

Un exemple de partie dans le jeu $\mathbb{E}v\Big(\mathcal{M}, \forall x\, \Big(P(x) \ \vee\ \exists y\, R\big(f(x),y\big)\Big)\Big)$:

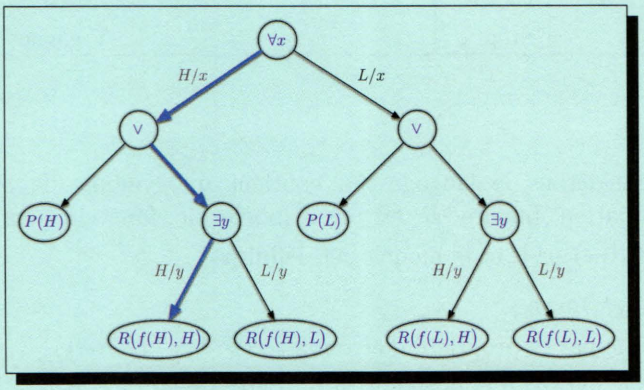
joueur	coup	la partie continue avec
F	prend Hardy	$(P(H) \ \vee\ \exists y\, R(f(H),y))$
V	choisit	$\exists y\, R(f(H),y)$
V	prend Hardy	$R(f(H),H)$
	Stop	**V** gagne

Considérons maintenant l'arbre de jeu associé à ce jeu :

$$\mathbb{E}v\,(\mathcal{M}, \forall x\ (P(x)\ \vee\ \exists y\ R(f(x), y)))$$

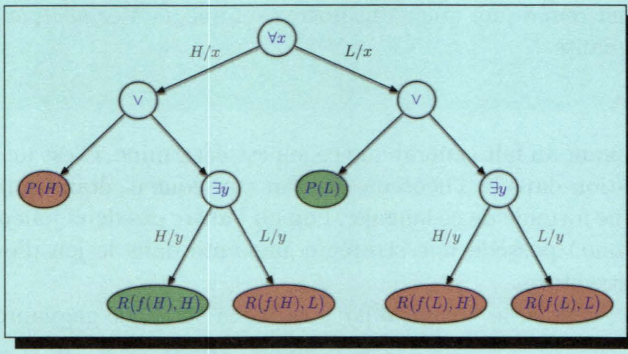


On remarque que les branches ont une longueur maximale de 3, ce qui correspond à la hauteur de la formule. Sur cet arbre, dessinons en bleu la partie que nous venons de jouer :



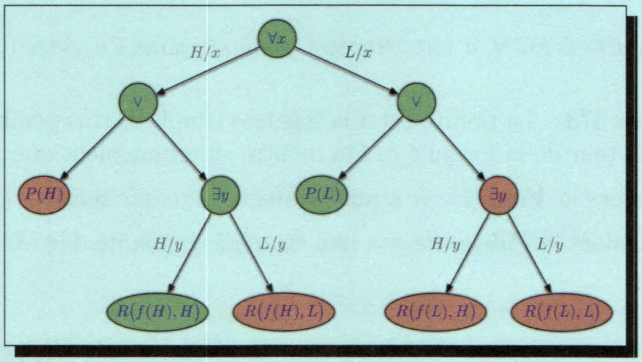
Cette partie est gagnante pour le joueur **V**érificateur puisqu'elle se termine par la formule atomique $R(f(H), H)$ qui est satisfaite dans cette structure. En effet, $f^{\mathcal{M}}(H) = L$ et $(L, H) \in R^{\mathcal{M}}$.

Nous pouvons également calculer lequel des deux joueurs possède une stratégie gagnante dans ce jeu. L'algorithme consiste à remonter le long des branches de l'arbre de jeu en coloriant les nœuds en fonction du joueur qui possède une stratégie gagnante à partir de la position indiquée par le nœud. Nous commençons par colorier les feuilles de l'arbre en fonction du joueur qui possède une stratégie gagnante à ce stade (c'est-à-dire celui qui l'emporte car la partie est finie à ce stade).



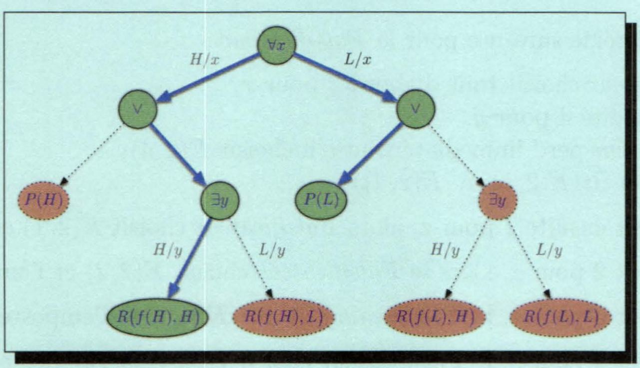
Les nœuds coloriés en vert désignent les positions à partir desquels le *Vérificateur* possède une stratégie gagnante, ceux en rouge vérifient la même propriété mais pour le *Falsificateur.*

On remonte ensuite le long des branches de manière croissante, suivant la hauteur des sous-formules, en appliquant la règle suivante : on colorie un nœud en rouge si ce nœud est pour le joueur ***Falsificateur*** et qu'il y a au moins un fils de ce nœud qui est rouge, ou bien si ce nœud est pour le joueur *Vérificateur* et tous les fils de ce nœud sont rouges.



On aboutit ainsi à colorier la racine. Dans notre exemple, la racine est verte, ce qui indique que le joueur *Vérificateur* possède une stratégie gagnante dans ce jeu.

Une stratégie gagnante pour le *Vérificateur* est indiquée dans la figure ci-dessous par les seules flèches bleues :



On peut également remarquer que, dans notre exemple, le ***Vérificateur*** ne possède qu'une unique stratégie gagnante.

Revenons maintenant au fait général que ce jeu est déterminé. C'est un cas particulier des jeux dont il est question dans le Théorème 75. Par conséquent, étant donnés un langage $\mathcal{L}$, une $\mathcal{L}$-structure et une formule de ce langage, l'un ou l'autre des deux joueurs (le ***Vérificateur*** ou bien le ***Falsificateur***) possède une stratégie gagnante dans le jeu d'évaluation de cette formule dans cette structure.

Dans l'exemple ci-dessus, le ***Vérificateur*** possède la stratégie gagnante suivante :

- si le ***Falsificateur***, au premier coup, choisit $(P(A) \ \vee\ \exists y\ R(f(A), y))$, il suffit au ***Vérificateur*** de choisir ensuite $\exists y\ R(f(A), y)$, puis à nouveau $R(f(A), A)$ pour l'emporter.
- si, au contraire, le ***Falsificateur*** choisit, au premier coup, $(P(E) \ \vee\ \exists y\ R(f(E), y))$, il suffit au ***Vérificateur*** de choisir ensuite $P(E)$ pour l'emporter.

En fait, les règles de ce jeu sont définies pour que l'on obtienne le résultat majeur suivant :

Théorème 373

$$\mathcal{M} \models \phi \text{ ssi } \mathbf{V} \text{ a une stratégie gagnante dans } \mathbb{E}v\,(\mathcal{M}, \phi)\,.$$

Preuve du Théorème 373 : La preuve est à la fois très simple et très pénible. Elle se fait par induction sur la hauteur de la formule ϕ. On montre simultanément que :

- si $\mathcal{M} \models \phi$, alors le ***Vérificateur*** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi)$, et
- si $\mathcal{M} \models \neg\phi$, alors le ***Falsificateur*** a une stratégie gagnante dans $\mathbb{E}v\,(\mathcal{M}, \phi)$.

$\dashv$ 373

Ainsi, si l'on reprend l'exemple 372, la formule $\forall x\ (P(x) \ \vee\ \exists y\ R(f(x), y))$ est satisfaite dans le modèle $\mathcal{M}$, puisque le joueur ***Vérificateur*** possède une stratégie gagnante dans le jeu $\mathbb{E}v\,(\mathcal{M}, \forall x\ (P(x) \ \vee\ \exists y\ R(f(x), y)))$.

Inversement, dans l'exemple 371, la formule $\forall x \forall y\,(E(x, y) \ \vee\ \exists z(E(x, z) \ \wedge\ E(z, y)))$ n'est pas satisfaite dans la structure $\mathcal{M}$. En effet, considérons le jeu d'évaluation :

$$\mathbb{E}v\,(\mathcal{M}, \forall x \forall y\,(E(x, y) \ \vee\ \exists z(E(x, z) \ \wedge\ E(z, y))))$$

et indiquons la stratégie suivante pour le ***Falsificateur*** :

- Le ***Falsificateur*** choisit tout d'abord 2 pour x,
- Il choisit ensuite 4 pour y.
- Le ***Vérificateur*** perd immédiatement s'il choisit $E(2, 4)$.
- Et s'il choisit $\exists z(E(2, z) \ \wedge\ E(z, 4))$:
  - s'il choisit ensuite 1 pour z, alors ***Falsificateur*** choisit $E(2, 1)$ et l'emporte,
  - s'il choisit 2 pour z, alors le ***Falsificateur*** choisit $E(2, 2)$ et l'emporte,
  - s'il choisit 3 pour z, le ***Falsificateur*** choisit $E(3, 4)$ et l'emporte,
  - s'il choisit 4 pour z, le ***Falsificateur*** choisit $E(4, 4)$ et l'emporte aussi.

Nous venons d'exhiber une stratégie gagnante pour le joueur ***Falsificateur***. Cela prouve donc que cette formule n'est pas satisfaite dans cette structure.

Remarques 374

(1) En toute généralité, le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$ est un jeu de longueur finie : le nombre de coups joués par les deux joueurs est fini. Cela tient au fait qu'à chaque coup, une sous-formule (*mutatis mutandis*) est choisie. Toute formule étant une suite finie de symboles, cela implique un nombre fini de sous-formules. Le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$ s'arrête donc après un temps fini. Par contre, contrairement aux jeux d'évaluation que nous avons rencontrés dans le cadre du Calcul Propositionnel, l'arbre de jeu n'est pas forcément un objet fini. En effet, il suffit que la $\mathcal{L}$-structure $\mathcal{M}$ ait un nombre infini d'éléments de base et que la formule considérée comporte une variable, pour que le choix de substituer un élément du modèle à cette variable soit infini.

Considérons par exemple le modèle $\mathcal{M}$ de l'arithmétique tel que présenté dans l'exemple 350 et la formule $\phi = \exists x R_{\leq}(x, x)$. Ce jeu est trivial : le joueur ***Vérificateur*** choisit une valeur n pour x, puis le jeu s'arrête et l'on regarde si $n \leq n$ est vérifié (ce qui est évidemment le cas). L'arbre de jeu a donc une hauteur 1 (sa plus longue branche a une longueur 1), mais pourtant cet arbre possède une infinité de branches : une pour chaque choix d'un entier n par le ***Vérificateur***.

(2) Tout jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$ est déterminé. L'un des deux joueurs possède une stratégie gagnante. L'existence d'une stratégie gagnante pour un joueur ou pour l'autre décide de la validité ou de la non validité de cette formule ϕ dans le modèle $\mathcal{M}$. Pour autant, il n'est pas nécessairement facile de déterminer lequel des deux joueurs possède une stratégie gagnante. C'est non seulement difficile parce que cela peut prendre du temps lorsque le modèle est suffisement compliqué et fini, mais c'est souvent impossible pratiquement lorsque le modèle est infini.

Pour avoir une idée de cette difficulté, il suffit de considérer le modèle de l'arithmétique et une formule quelconque ϕ écrite dans ce langage. Décider lequel des deux joueurs possède une stratégie gagnante dans le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$, c'est résoudre le problème de savoir si la formule ϕ est vraie dans le modèle $\mathcal{M}$. C'est donc décider pour une formule quelconque de l'arithmétique si elle est vraie ou non. Si l'on songe qu'il a fallu 350 ans pour prouver le théorème de Fermat (qui est un énoncé parfaitement formalisable dans le langage de l'arithmétique), on a une idée de la difficulté du problème général de déterminer le gagnant dans le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$. Pour le dire autrement, si nous pouvions aisément déterminer lequel des joueurs possède une stratégie gagnante dans le jeu $\mathbb{E}v\,(\mathcal{M}, \phi)$, nous pourrions alors facilement décider de tout problème arithmétique. Or il reste encore un grand nombre de questions majeures non résolues dans ce domaine...

Un simple exemple : la conjecture de Goldbach (tout nombre pair plus grand que 2 est la somme de deux nombres premiers) est un énoncé très simple de l'arithmétique qui reste ouvert (personne n'a encore apporté de solution positive ou négative à cet énoncé). Et il en existe des milliers comme celui-là ! Mais revenons à la conjecture de Goldbach, pour plus de simplicité, imaginons que nous enrichissons le langage de l'arithmétique avec un symbole de prédicat Pr que l'on interprète par "être un nombre premier". Le jeu associé à cette conjecture consiste à ce que :

(a) ***Falsificateur*** choisit un nombre pair $2n$,

(b) ***Vérificateur*** choisit un nombre a,

(c) ***Vérificateur*** choisit un nombre b,

(d) ***Falsificateur*** choisit parmi $Pr(a)$, $Pr(b)$ et $a \cdot b = 2n$

Il est tout à fait évident que le ***Falsificateur*** a une stratégie gagnante dans ce jeu si et seulement si la conjecture de Goldbach est fausse. En effet, dans ce cas il existe bien un nombre pair $2n$ qui ne la satisfait pas et il suffit au ***Falsificateur*** de choisir ce nombre, les choix de a et b par le ***Vérificateur*** entraînant *ipso facto*, ou bien le fait que l'un des deux (a ou b) n'est pas premier, ou bien que le produit de a par b n'est pas égal au nombre $2n$.

Pour aller plus avant :

La sémantique usuelle de la logique du 1er ordre se retrouve dans de très nombreux ouvrages, au contraire de l'approche théorique des jeux que nous avons privilégiée ici et qui est absente de la quasi totalité des manuels. Nous renvoyons le lecteur tout particulièrement vers le livre *"An introduction to elementary logic"* de Wilfrid Hodges [Hod01], mais aussi sans discernement particulier vers tous les ouvrages proposés à la page 395.

---

4 Où l'on revoit les isomorphismes

Résumé № 54

- *Si deux $\mathcal{L}$-structures sont isomorphes, elles vérifient dès lors les mêmes formules de $\mathcal{L}$.*
- *La réciproque est généralement fausse.*

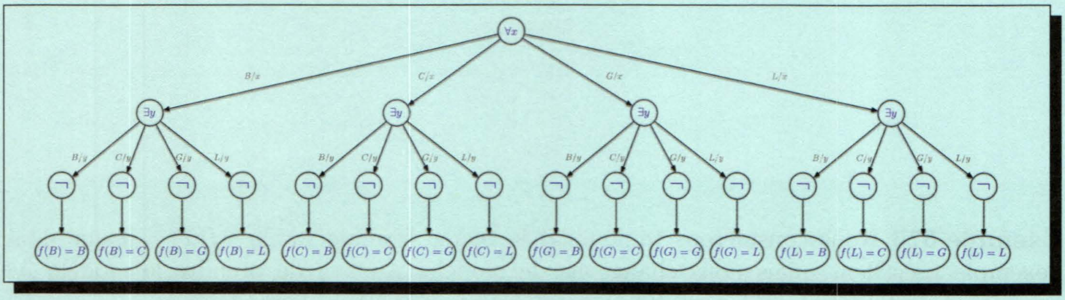
※

Nous allons commencer cette section par deux exemples. Il s'agit d'évaluer à chaque fois la même formule mais dans des modèles différents dont nous avons montré précédemment qu'ils étaient isomorphes. Nous allons remarquer que les jeux d'évaluations associés à cette même formule dans le premier modèle et dans le second sont étonnamment semblables. Ils ont en fait la même structure, le même squelette. Ils ne varient que par le changement des noms des éléments des domaines considérés lorsqu'on passe d'un modèle à l'autre. Une conséquence de cette quasi identité des deux jeux sera que le joueur qui possèdera une stratégie gagnante sera le même dans un jeu et dans l'autre. Et donc la formule aura exactement la même valeur de vérité dans les deux modèles.

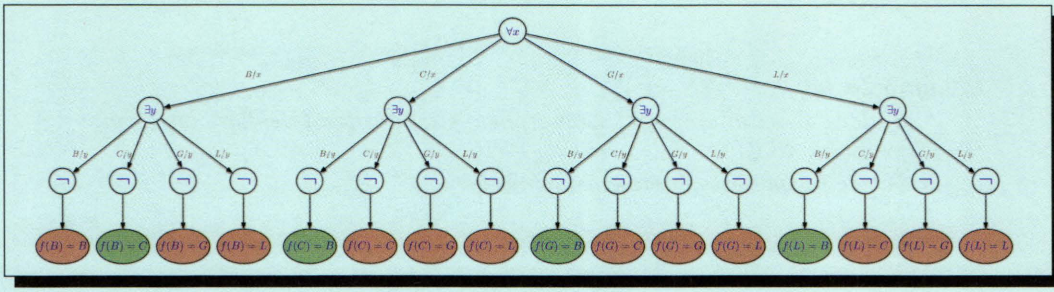
Exemple 375 Soient $\mathcal{M}$ le modèle présenté dans l'exemple 351 page 400, ainsi que ϕ la formule $\forall x\ \exists y\ \neg f(x) = y$. Pour plus de concision, on notera :

- B pour la *Bobinette*
- C pour le petit *Chaperon rouge*
- G pour la *Grand-Mère*
- L pour le grand méchant *Loup*.

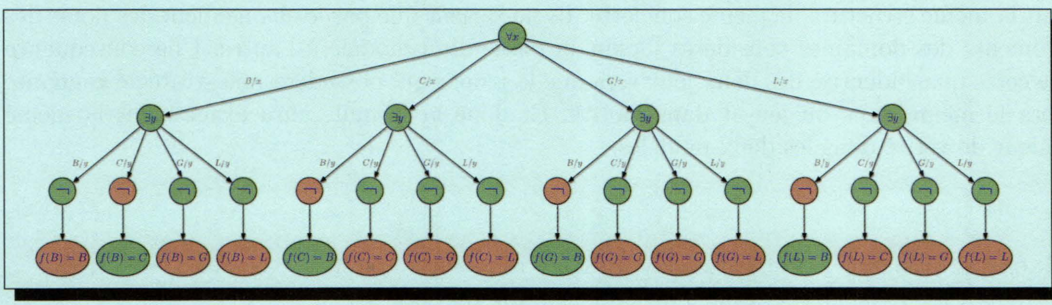
L'arbre de jeu associé au jeu d'évaluation $\mathbb{E}v\,(\mathcal{M}, \phi)$ est le suivant :



Nous colorions maintenant en vert les formules atomiques qui sont vraies dans le modèle $\mathcal{M}$ et en rouge celles qui sont fausses.



Nous colorions ensuite les feuilles en fonction du vainqueur : rouge pour le ***Falsificateur*** et vert pour le ***Vérificateur***.



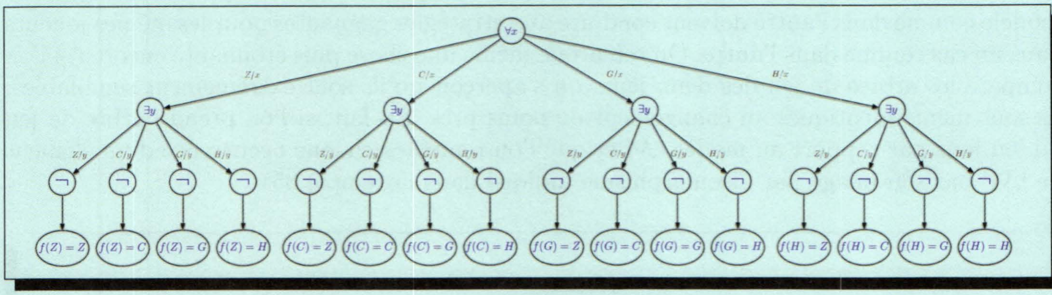
Nous voyons que le ***Vérificateur*** possède une stratégie gagnante dans ce jeu. La formule $\forall x \; \exists y \; \neg f(x) = y$ est donc vraie dans ce modèle.

Exemple 376 Nous considérons toujours ϕ la même formule $\forall x \; \exists y \; \neg f(x) = y$ que dans l'exemple précédent, mais nous changeons de modèle. Au lieu de prendre le modèle $\mathcal{M}$ présenté dans l'exemple 351 page 400, nous prenons cette fois-ci le modèles $\mathcal{N}$.

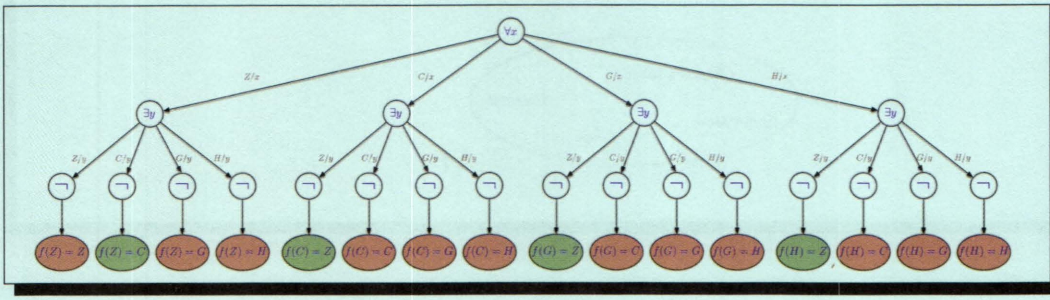
Pour plus de concision nous écrivons :

- C pour *Chico*,
- G pour *Groucho*,
- H pour *Harpo*,
- Z pour *Zeppo*.

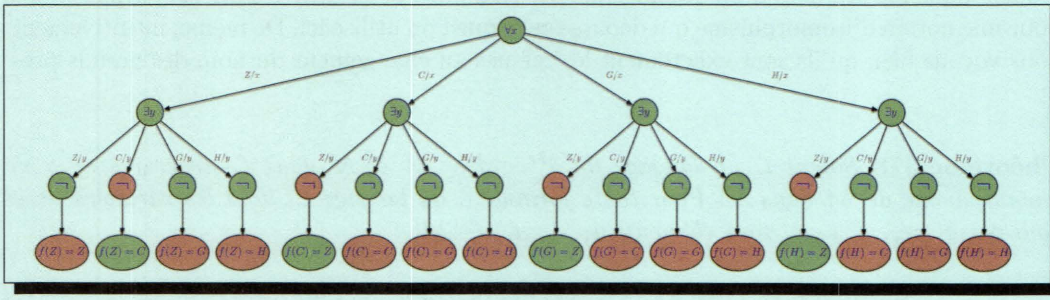
L'arbre de jeu associé au jeu d'évaluation $\mathbb{E}v\left(\mathcal{M}, \phi\right)$ est présenté ci-dessous. Il est à noté qu'il est identique à celui étudié dans l'exemple précédent, si l'on fait exception des noms des éléments du domaine.



Nous colorions maintenant en vert les formules atomiques qui sont vraies dans le modèle $\mathcal{N}$ et en rouge celles qui sont fausses.

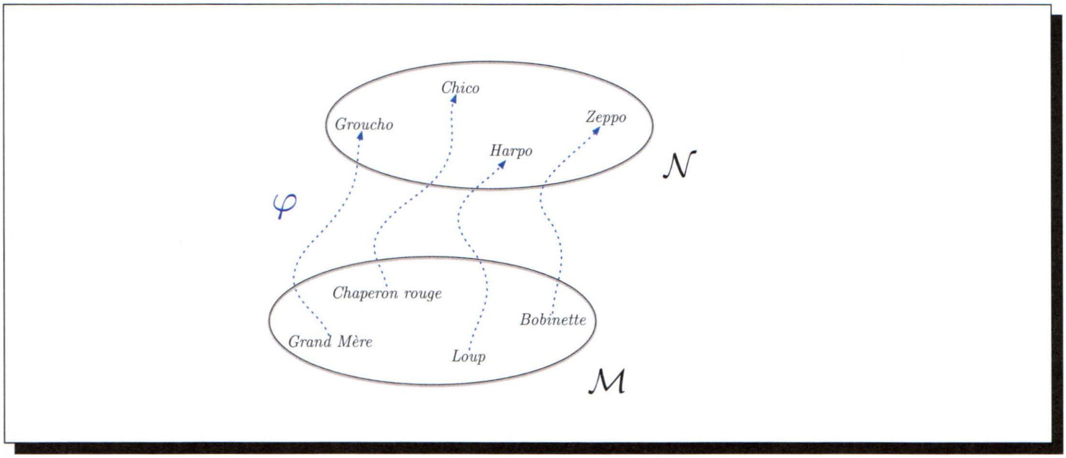


Pour chaque autre feuille, nous colorions ensuite celle-ci en fonction de celui qui possède une stratégie gagnante si la partie débutait ici : rouge pour le ***Falsificateur*** et vert pour le ***Vérificateur***.



Nous voyons que le ***Vérificateur*** possède une stratégie gagnante dans ce jeu. Il en découle que la formule $\forall x \; \exists y \; \neg f(x) = y$ est vraie dans le modèle $\mathcal{N}$.

Remarque 377 Nous venons de considérer deux jeux d'évaluation différents. Dans ces deux jeux, la formule était la même, ce qui changeait était le modèle. Or, nous savons que ces deux modèles sont isomorphes. Et nous avons obtenu une stratégie gagnante pour le même joueur dans les deux cas. Est-ce un hasard ? Non ! Lorsque deux modèles sont isomorphes, ils vérifient exactement les mêmes formules. Par conséquent, les jeux d'évalutation dans un modèle comme dans l'autre doivent conduire aux stratégies gagnantes pour les mêmes joueurs dans un cas comme dans l'autre. On remarque même une chose plus étonnante encore : si l'on compare les arbres de jeu des deux jeux, on s'aperçoit qu'ils sont extrêmement semblables, ils sont même identiques au changement de noms près. En fait, si l'on prend l'arbre de jeu du jeu joué par rapport au modèle $\mathcal{M}$ et que l'on remplace chaque occurrence d'un élément de $|\mathcal{M}|$ par son image par l'isomorphisme indiqué dans l'exemple 351 :



on obtient alors exactement l'arbre de jeu d'évaluation joué par rapport au modèle $\mathcal{N}$. Cela indique également qu'une stratégie pour un joueur dans le premier jeu peut être recopiée dans le second jeu. En particulier, une stratégie gagnante pour un joueur dans le premier jeu est "transformée par l'isomorphisme" en une stratégie gagnante pour le même joueur dans le second jeu. Plus exactement, l'isomorphisme transporte tout l'arbre de jeu du premier modèle dans l'arbre de jeu du second modèle. Ainsi, les deux arbres sont *isomorphes*, mais pour une notion d'isomorphisme qui dépasse celle que l'on utilise ici. De même, intuitivement, nous voyons bien qu'ils sont exactement les mêmes au changement du nom des nœuds près.

Théorème 378 *Soient $\mathcal{L}$ un langage du 1er ordre, $\mathcal{M}$ et $\mathcal{N}$ deux $\mathcal{L}$-structures et φ un isomorphisme de $\mathcal{M}$ dans $\mathcal{N}$. Pour toute formule ϕ du langage $\mathcal{L}$, dont les variables libres sont parmi $x_1, \ldots, x_n$ et tous éléments $a_1, \ldots, a_n \in |\mathcal{M}|$:*

$$\mathcal{M}, a_1/x_1, \ldots, a_n/x_n \models \phi \textit{ ssi } \mathcal{N}, \varphi(a_1)/x_1, \ldots, \varphi(a_n)/x_n \models \phi.$$

Preuve du Théorème 378 : La preuve – aussi simple que fastidieuse – se déroule par induction sur la hauteur de la formule ϕ. Si l'on pense la notion de validité ou de fausseté de la formule ϕ dans les structures $\mathcal{M}$ et $\mathcal{N}$ en terme d'existence d'une stratégie gagnante pour un joueur dans les jeux d'évaluation sous-jacents respectifs. La preuve consiste à jouer les deux jeux en parallèle : au choix d'un élément a par un joueur dans le jeu associé à $\mathcal{M}$, correspond le choix de $\varphi(a)$ par ce même joueur dans le jeu associé à $\mathcal{N}$. Et inversement, au choix d'un élément b par un joueur dans le jeu associé à $\mathcal{N}$, correspond le choix de $\varphi^{-1}(b)$ par ce même joueur dans le jeu associé à $\mathcal{M}$. $\dashv$ 378

A contrario, deux $\mathcal{L}$-structures qui vérifient les mêmes formules du langage $\mathcal{L}$ ne sont pas nécessairement isomorphes. *A priori*, ce résultat semble plus simple que le précédent puisqu'il suffit de ne présenter qu'un seul *contre-exemple* pour témoigner de sa véracité. Néanmoins, procurer un tel contre-exemple consiste à mettre à disposition deux modèles différents qui satisfont exactement les mêmes formules, bien qu'ils ne soient pas isomorphes. Or il n'est pas aisé de montrer que deux modèles satisfont exactement les mêmes formules – on appelle cela être *élémentairement équivalent* – car il est bien sûr illusoire de pouvoir passer en revue chacune de celles-ci. De même, montrer que deux modèles ne sont pas isomorphes n'est pas si simple, surtout lorsqu'ils satisfont exactement les mêmes formules, puisque c'est comme dire qu'ils sont indiscernables – par une formule – bien qu'ils soient pourtant intrinsèquement différents (et pas seulement à un changement de nom près). Nous donnons cependant un tel contre-exemple au travers de l'exemple qui suit, mais sans la preuve formelle qu'il convient. Celle-ci serait en effet à la fois beaucoup trop longue pour ce chapitre et trop ambitieuse pour cet ouvrage.

Exemple 379 On considère un langage $\mathcal{L}$ qui ne comporte, en plus de l'égalité, qu'un unique symbole de relation binaire noté $<$. Pour des raisons évidentes, on convient de noter $x < y$ au lieu de $<(x, y)$.

Un modèle de la théorie des ordres denses sans premiers ni derniers éléments est une $\mathcal{L}$-structure qui vérifie chacune des formules – dénommées axiomes – qui suivent :

(1) $\forall x \neg\, x < x$

(2) $\forall x \forall y \neg\, (x < y \;\wedge\; y < x)$

(3) $\forall x \forall y \forall z \; \big((x < y \wedge y < z) \longrightarrow x < z\big)$

(4) $\forall x \forall y \; (x < y \vee y < x \vee x = y)$

(5) $\forall x \forall z \; \big(x < z \longrightarrow \exists y \; (x < y \wedge y < z)\big)$

(6) $\forall y \exists x \; x < y$

(7) $\forall x \exists y \; x < y$.

Les formules (1)-(3) décrivent le fait que $<$ est une relation d'ordre. Plus précisément, ces formules expriment que la relation $<$ est :

(1) *irréflexive* (2) *antisymétrique* (3) *transitive.*

Les formules (4) et (5) stipulent que $<$ représente respectivement :

(4) *un ordre total* (5) *un ordre dense.*

Un ordre est dit total lorsque deux éléments quelconques sont toujours comparables (s'ils sont différents, alors l'un est strictement plus petit que l'autre) et dense lorsqu'entre deux éléments distincts, il en existe toujours un troisième.

Les formules (6) et (7) expriment finalement que l'ordre $<$ ne comporte pas :

(6) *de plus petit élément* (7) *de plus grand élément.*

Il est clair que la structure formée par les entiers naturels ($\mathbb{N}$) équipés de l'ordre usuel sur les entiers satisfait bien les axiomes (1)-(4) et également (7). Par contre, elle ne satisfait ni (5) (puisqu'entre 0 et 1 il n'y a aucun entier) ni (6) (puisque 0 constitue un élément minimal).

Par contre, la structure $\mathcal{R}$ formée par les réels ($\mathbb{R}$) équipés de l'ordre usuel sur les réels, ainsi que la structure $\mathcal{Q}$ formée par les nombre rationnels ($\mathbb{Q}$) équipés cette fois-ci de l'ordre usuel sur les rationnels satisfont toutes deux l'entier des axiomes (1)-(7).

On remarque évidemment qu'il ne peut y avoir de modèle vérifiant ces axiomes dont le domaine soit fini – puisqu'entre deux éléments distincts il y en a toujours un troisième, donc un quatrième, puis un cinquième, etc. Là où les choses commencent à devenir intéressantes, c'est lorsqu'on s'aperçoit que deux modèles quelconques de cette théorie des ordres denses sans premier ni dernier éléments satisfont toujours exactement les mêmes formules. Nous ne pouvons établir ici ce résultat qui nécessitent des méthodes qui dépassent très largement le cadre de cet ouvrage. Nous renvoyons à des ouvrages tels que [CLK03b, KK67, Mar02, Sho67].

Par ailleurs, les deux modèles que nous venons d'indiquer – $\mathcal{Q}$ et $\mathcal{R}$ – ne sont pas isomorphes. La raison de cela réside dans le fait qu'il n'existe simplement pas de *bijection* entre les deux domaines de ces modèles. Il n'y a pas de bijection entre les nombres rationnels et les nombres réels. Ces derniers sont en réalité *trop nombreux*. Autrement dit, bien que l'ensemble des réels et celui des rationnels soient tous deux infinis, ils n'ont pas la même taille : l'un est plus grand que l'autre. Pour des preuves, nous renvoyons vers [Mos94, Kun11, Tou11a, SV02, HJ99, CLK03b, Sho67].

Les deux modèles $\mathcal{Q}$ et $\mathcal{R}$ sont donc équivalents (ils satisfont les mêmes formules) sans être pour autant isomorphes, ce qui contredit la réciproque du Théorème 378.

Pour aller plus avant :

Que deux modèles isomorphes satisfassent exactement les mêmes formules et soient donc indiscernables au regard du langage utilisé, cela participe des bases de la *"théorie des modèles"*, tout comme les notions d'homomorphisme et de plongement que nous avions vu plus haut. Nous ne pouvons donc que réitérer ici les conseils prodigués à la page 407.

---

5 Formules logiquement équivalentes

Résumé № 55

- *Deux formules ϕ et ψ du langage $\mathcal{L}$ sont* logiquement équivalentes *(noté $\phi \equiv \psi$) si elles sont satisfaites dans les mêmes $\mathcal{L}$-structures.*

※

Maintenant que nous avons à disposition la valeur de vérité d'une formule dans un modèle, nous pouvons regarder, pour une formule donnée, l'ensemble de ses modèles. Bien sûr, ce travail s'effectue toujours à langage fixé. On commence par se donner un langage $\mathcal{L}$ et c'est par rapport à ce langage qu'à la fois les modèles et la formule sont considérés. Il est évident que lorsqu'on ne regarde qu'une formule à la fois, on peut très bien considérer que le langage en question n'est composé que des symboles – de constante, de fonction et de relation – qui interviennent dans la formule. Et lorsqu'on regarde non plus une formule, mais un ensemble de formules (ce que nous appelons une théorie), le langage en question peut être restreint à la réunion des ensembles de symboles – de constante, de fonction et de relation – de chaque formule.

L'ensemble des modèles d'une formule, c'est-à-dire l'ensemble des $\mathcal{L}$-structures dans laquelle cette formule est vraie, constitue en quelque sorte sa carte d'identité sémantique. La signification d'une formule constitue en effet l'ensemble de ses modèles. Ainsi, deux formules qui n'ont pas la même signification n'auront pas les mêmes modèles. En particulier, on pourra trouver un modèle qui les distingue : un modèle dans lequel l'une est vraie alors que l'autre est fausse.

Comparer deux formules sur le plan sémantique consiste à chercher ce qui les différencie ; ce qui, au niveau de leurs interprétations, permet de les distinguer. Autrement dit, cela revient à consulter le catalogue de tous les modèles possibles de ces deux formules et tenter de trouver, parmi eux, ceux qui les opposent. S'il n'existe pas de tel modèle, alors ces formule sont dites équivalentes.

Définition 380 *Soient $\mathcal{L}$ un langage du 1^er^ ordre, ϕ, ψ deux formules* closes *de ce langage*

$$\phi \text{ et } \psi \text{ sont équivalentes ssi elles sont satisfaites dans les mêmes } \mathcal{L}\text{-structures.}$$

i.e.,

$$\phi \equiv \psi \text{ ssi pour tout modèle } \mathcal{M}, \Big(\mathcal{M} \vDash \phi \text{ ssi } \mathcal{M} \vDash \psi\Big).$$

Une conséquence immédiate de cette définition est que deux formules sont équivalentes précisément lorsque l'équivalence logique de ces deux formules est vérifiée dans tout modèle :

Corollaire 381 *Soient $\mathcal{L}$ un langage du 1^{er} ordre, ϕ, ψ deux formules* closes *dans ce langage,*

$$\phi \equiv \psi \text{ ssi pour toute } \mathcal{L}\text{-structure } \mathcal{M}, \quad \mathcal{M} \vDash (\phi \longleftrightarrow \psi).$$

Preuve du Corollaire 381 : Immédiate.

⊣ 381

Exemple 382 Considérons le langage $\mathcal{L}$ qui contient P et Q comme symboles de relation unaire, R comme symbole de relation binaire et c comme constante.

(1) (a) $\exists x\ (P(x) \wedge P(x)) \equiv \exists x\ P(x)$

(b) $\exists x\ \exists y\ (P(x) \vee P(y)) \equiv \exists x\ P(x)$

(c) $\neg\neg P(\mathsf{c}) \equiv P(\mathsf{c})$

(d) $\forall x\ \exists x\ P(x) \equiv \exists x\ P(x)$

(e) $\exists x\ (P(x) \longrightarrow Q(\mathsf{c})) \equiv (\exists x\ \neg P(x) \vee Q(\mathsf{c}))$

(f) $\exists x\ \forall y\ (P(x) \longrightarrow P(y)) \equiv \exists y\ \forall x\ (\neg P(y) \vee P(x))$.

(2) Les formules suivantes ne sont pas équivalentes :

(a) $\exists x\ P(x) \ \equiv\ \exists x\ Q(x)$; considérer un modèle $\mathcal{M}$ dans lequel $P^{\mathcal{M}} = \emptyset$ alors que $P^{\mathcal{M}} \neq \emptyset$;

(b) $(P(\mathsf{c}) \longrightarrow P(\mathsf{c}))$ et $P(\mathsf{c})$; considérer $\mathcal{M}$ dans lequel $\mathsf{c}^{\mathcal{M}} \notin P^{\mathcal{M}}$;

(c) $\exists x\ P(x)$ et $\forall x\ P(x)$; considérer $\mathcal{M}$ tel que $\emptyset \subsetneq P^{\mathcal{M}} \subsetneq |\mathcal{M}|$.

On généralise la notion d'équivalence sémantique aux formules en général (c'est-à-dire également à celles qui ne sont pas closes) en prenant la clôture universelle de ces formules.

Définition 383 *Soient $\mathcal{L}$ un langage du 1er ordre, ϕ, ψ deux formules de ce langage dont les variables libres sont parmi $x_1, \ldots, x_n$,*

$$\phi \equiv \psi \iff \Big(\textit{pour tout modèle } \mathcal{M},\ \ \mathcal{M} \models \forall x_1, \ldots, \forall x_n(\phi \longleftrightarrow \psi)\Big).$$

Remarque 384 La relation d'équivalence $\equiv$ est évidemment réflexive, symétrique et transitive. Comme son nom l'indique, c'est une relation d'équivalence.

Notation 385 *On utilisera les notations suivantes afin d'alléger le texte :*

(1) $(\phi_0 \wedge \phi_1 \wedge \phi_2 \wedge \ldots \wedge \phi_k)$ *ou bien* $\displaystyle\bigwedge_{0\leq i\leq k} \phi_i$ *à la place de* $(\phi_0 \wedge (\phi_1 \wedge (\phi_2 \wedge (\ldots \wedge \phi_k \underbrace{)))\ldots)}_{k}$.

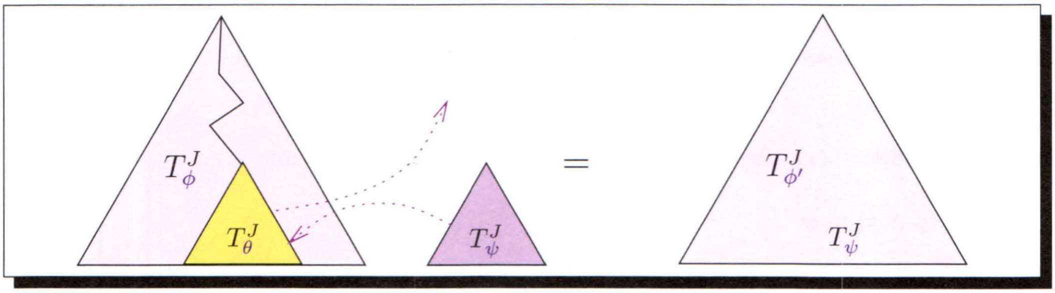
(2) $(\phi_0 \vee \phi_1 \vee \phi_2 \vee \ldots \vee \phi_k)$ *ou bien* $\displaystyle\bigvee_{0\leq i\leq k} \phi_i$ *au lieu de* $(\phi_0 \vee (\phi_1 \vee (\phi_2 \vee (\ldots \vee \phi_k \underbrace{)))\ldots)}_{k}$.

Proposition 386 *Soient $\mathcal{L}$ un langage du 1er ordre, ϕ, ψ et θ trois formules de ce langage. On suppose que ϕ est une formule close, que ψ n'a pas d'autres variables libres que celles de θ qui sont parmi $x_1, \ldots, x_n$.*

Si, pour toute $\mathcal{L}$-structure $\mathcal{M}$ et tout $a_1, \ldots, a_n \in |\mathcal{M}|$, $\psi_{[a_1/x_1,\ldots,a_n/x_n]} \ \equiv\ \theta_{[a_1/x_1,\ldots,a_n/x_n]}$, alors

$$\phi' \equiv \phi$$

où ϕ' est la formule obtenue à partir de ϕ en substituant ψ à θ.



Preuve de la Proposition 386 :

Cette preuve est relativement simple. Nous voulons montrer que ϕ et ϕ' sont équivalentes, c'est-à-dire qu'elles sont vraies dans les mêmes modèles. Si nous adoptons le point de vue des jeux d'évaluation, cela signifie que pour toute $\mathcal{L}$-structure $\mathcal{M}$, le même joueur possède une stratégie gagnante dans les deux jeux d'évaluation $\mathbb{E}v\,(\phi, \mathcal{M})$ et $\mathbb{E}v\,(\phi', \mathcal{M})$.

Supposons donc que le joueur **J** possède une stratégie gagnante σ dans le jeu $\mathbb{E}v\,(\phi, \mathcal{M})$. Nous allons décrire une stratégie gagnante τ pour ce même joueur dans le jeu $\mathbb{E}v\,(\phi', \mathcal{M})$. La stratégie τ consiste à suivre rigoureusement la stratégie σ, excepté lorsque la partie *entre* dans la sous-formule $\psi_{[a_1/x_1,\dots,a_n/x_n]}$ où $a_1, \dots, a_n$ sont les différents choix d'éléments du domaine effectués par les joueurs lors du début de la partie. Or, nous savons que le joueur **J** possède une stratégie gagnante dans le jeu d'évaluation $\mathbb{E}v\left(\theta_{[a_1/x_1,\dots,a_n/x_n]}, \mathcal{M}\right)$, donc par hypothèse, nous savons également que le joueur **J** possède une stratégie gagnante dans le jeu d'évaluation $\mathbb{E}v\left(\psi_{[a_1/x_1,\dots,a_n/x_n]}, \mathcal{M}\right)$. Il suffit alors d'appliquer cette dernière.

$\dashv$ 386

De manière tout à fait similaire au cas du Calcul Propositionnel, les équivalences suivantes sont aisément vérifiées :

Lemme 387

(1) Soient $\phi \equiv \phi'$ et $\psi \equiv \psi'$:

- $\neg\phi \equiv \neg\phi'$
- $(\phi \vee \psi) \equiv (\phi' \vee \psi')$
- $(\phi \wedge \psi) \equiv (\phi' \wedge \psi')$
- $(\phi \longrightarrow \psi) \equiv (\phi' \longrightarrow \psi')$
- $(\phi \longleftrightarrow \psi) \equiv (\phi' \longleftrightarrow \psi')$.

(2)
- $\neg\exists x\ \phi \equiv \forall x\ \neg\phi$
- $\neg\forall x\ \phi \equiv \exists x\ \neg\phi$.

(3) On suppose que y n'est pas une variable apparaissant dans ϕ :

- $\exists x\ \phi \equiv \exists y\ \phi_{[y/x]}$
- $\forall x\ \phi \equiv \forall y\ \phi_{[y/x]}$.

Preuve du Lemme 387 : Immédiate, laissée au lecteur.

$\dashv$ 387

Remarque 388 Nous retrouvons exactement les mêmes équivalences fondamentales que celles que nous avions dégagées dans le cadre du Calcul Propositionnel :

Exemples 389 (1) idempotence de la conjonction et disjonction :

(a) $(\phi \wedge \phi) \equiv \phi$ (b) $(\phi \vee \phi) \equiv \phi$

(2) commutativité de la conjonction, disjonction et double implication :

(a) $(\phi \vee \psi) \equiv (\psi \vee \phi)$ (b) $(\phi \wedge \psi) \equiv (\psi \wedge \phi)$ (c) $(\phi \longleftrightarrow \psi) \equiv (\psi \longleftrightarrow \phi)$

(3) associativité de la conjonction, de la disjonction et de la double implication :

(a) $((\phi \vee \psi) \vee \theta) \equiv (\phi \vee (\psi \vee \theta))$ (c) $((\phi \longleftrightarrow \psi) \longleftrightarrow \theta) \equiv (\phi \longleftrightarrow (\psi \longleftrightarrow \theta))$
(b) $((\phi \wedge \psi) \wedge \theta) \equiv (\phi \wedge (\psi \wedge \theta))$

(4) distributivité de la disjonction par rapport à la conjonction et réciproquement :

(a) $((\phi \vee (\psi \wedge \theta)) \equiv ((\phi \vee \psi) \wedge (\phi \vee \theta))$ (b) $((\phi \wedge (\psi \vee \theta)) \equiv ((\phi \wedge \psi) \vee (\phi \wedge \theta))$

(5) lois d'absorption :

(a) $(\phi \wedge (\phi \vee \psi)) \equiv \phi$ (b) $(\phi \vee (\phi \wedge \psi)) \equiv \phi$

(6) lois de De Morgan :

(a) $\neg(\phi \vee \psi) \equiv (\neg\phi \wedge \neg\psi)$ (b) $\neg(\phi \wedge \psi) \equiv (\neg\phi \vee \neg\psi)$

(7) contraposée, décomposition de l'implication et élimination des doubles négations :

(a) $(\phi \longrightarrow \psi) \equiv (\neg\psi \longrightarrow \neg\phi)$ (b) $(\phi \longrightarrow \psi) \equiv (\neg\phi \vee \psi)$ (c) $\neg\neg\phi \equiv \phi$.

Lorsque deux formules sont équivalentes, il arrive que l'une soit plus "simple" que l'autre, qu'elle soit plus facilement compréhensible. On peut dès lors se demander si l'on peut trouver pour chaque formule, une ou plusieurs formules qui lui soient équivalentes, mais qui nous siéent tout particulièrement. C'est là l'objet du chapitre suivant.

6 Formules sous formes prénexes

Résumé № 56

(1) Pour toute formule, il existe une formule équivalente sous forme prénexe :

$$\phi = Q_1 x_1, \ldots, Q_k x_k \ \psi$$

où

(a) chaque "Q_i" est soit "$\exists$" soit "$\forall$";

(b) ψ est une formule sans quantificateur.

(2) De plus, on peut exiger que ψ soit :

(a) sous forme normale conjonctive (FNC) :

$$\psi = \bigwedge_{1 \leq i \leq k} \Big(\bigvee_{1 \leq j \leq n_i} \varepsilon_{i,j} A_{i,j} \Big)$$

(b) ou sous forme normale disjonctive (FND) :

$$\psi = \bigvee_{1 \leq i \leq k} \Big(\bigwedge_{1 \leq j \leq n_i} \varepsilon_{i,j} A_{i,j} \Big).$$

(Avec $\varepsilon_{i,j} A_{i,j} = A_{i,j}$ ou $\varepsilon_{i,j} A_{i,j} = \neg A_{i,j}$; et $A_{i,j}$ des formules atomiques.)

※

Etant donnée une formule du 1^er^ ordre, parmi l'infinité des formules qui lui sont équivalentes, quels pourraient bien être les critères qui nous permettraient d'affirmer que l'une d'elle est "simple" ou plus parfaitement constituée ? La notion de *forme prénexe* est une première réponse. Elle consiste à dire que dans le jeu d'évaluation associé à une formule, les joueurs ont deux types de coups très différents : soit ils descendent le long de la formule – qu'ils échangent leur chapeau ou non – soit ils choisissent des éléments du domaine et ce, à chaque fois qu'ils rencontrent le quantificateur correspondant à leurs fonctions. Mais ne pourrait-on donc pas dissocier ces deux types de coups pour éviter qu'ils ne s'enchevêtrent ? Ne pourrait-on pas tout simplement commencer la partie en choisissant des représentants du domaine une bonne fois pour toute, pour ensuite ne se concentrer que sur les déplacement à l'intérieur de la formule le long des symboles "$\vee$", des "$\wedge$" et des "$\neg$" ? Ne pourrait-on pas non plus de surcroît faire en sorte que si le joueur rencontre un éventuel symbole de négation, ce ne soit que juste avant que le jeu ne stoppe ? Mieux encore, ne pourrait-on pas séparer les "$\vee$" des "$\wedge$" en sorte de ne rencontrer tout d'abord uniquement les premiers, puis uniquement les seconds ?

Ce chapitre est entièrement consacré à apporter une réponse affirmative à chacune des questions précédentes.

Définition 390 *Soient $\mathcal{L}$ un langage du 1^er^ ordre et ϕ une formule dans ce langage. ϕ est dite* sous forme prénexe *s'il existe des variables $x_1, \ldots, x_k$ ainsi que des quantificateurs*

$Q_1, \ldots, Q_k$ *et une formule* sans quantificateur ψ *tels que :*

$$\phi = Q_1 x_1, \ldots, Q_k x_k \psi.$$

De plus, ϕ *est dite sous forme prénexe* polie *si les variables* $x_1, \ldots, x_k$ *sont deux à deux distinctes.*

Théorème 391 *Soient* $\mathcal{L}$ *un langage du* 1^{er}*ordre,*

Pour toute formule ϕ *de ce langage, il existe une formule* ψ *de ce langage telle que :*

(1) ψ *est sous forme prénexe polie,*

(2) $\phi \equiv \psi$.

Preuve du Théorème 391 : La preuve se fait par induction sur la hauteur de la formule ϕ. Sans perte de généralité, on peut supposer que ϕ ne possède aucun des deux connecteurs "$\longrightarrow$" et "$\longleftrightarrow$".

(1) si $ht(\phi) = 0$, alors ϕ est une formule atomique, par conséquent sans quantificateur, et $\psi = \phi$ convient.

(2) Si $\phi = \neg\theta$, alors par hypothèse d'induction, $\theta \equiv \theta'$ avec θ' sous forme prénexe polie : $\theta' = Q_1 x_1 \ \ldots \ Q_k x_k \ \psi'$. Par conséquent, l'équivalence suivante est vérifiée : $\phi \equiv \neg \ Q_1 x_1 \ \ldots \ Q_k x_k \ \psi'$. Or, avec la convention $\bar{Q}_i$ est le quantificateur dual de Q_i (c'est-à-dire $\bar{\exists} = \forall$ et $\bar{\forall} = \exists$), on voit donc aisément que $Q_1 x_1 \ \ldots \ Q_k x_k \ \psi' \equiv \bar{Q}_1 x_1 \ \ldots, \bar{Q}_k x_k \ \neg \ \psi'$ et par conséquent $\phi \equiv \bar{Q}_1 x_1 \ \ldots, \bar{Q}_k x_k \ \neg \ \psi'$. Il suffit donc de prendre $\psi = \bar{Q}_1 x_1 \ \ldots, \bar{Q}_k x_k \ \neg \ \psi'$.

(3) Si $\phi = (\phi_0 \vee \phi_1)$, alors par hypothèse d'induction, $\phi_0 \equiv \phi'_0$ et $\phi_1 \equiv \phi'_1$ avec $\phi'_0 = Q_1 x'_1 \ \ldots \ Q_n x'_n \ \psi'_0$ et $\phi'_1 = Q'_1 x'_1 \ \ldots \ Q'_m x'_m \ \psi'_1$, où ψ'_0 et ψ'_1 sont sans quantificateurs. On se donne alors $n + m$ variables n'ayant aucune occurrence ni dans ψ'_0, ni dans ψ'_1 : $x_1, \ldots, x_n, y_1, \ldots, y_m$ et on pose :

$$\psi_0 = \psi'_{0[x_1/x'_1, \ldots, x_n/x'_n]} \text{ et } \psi_1 = \psi'_{1[y_1/y'_1, \ldots, y_m/y'_m]}$$

puis

$$\psi = Q_1 x_1 \ \ldots \ Q_n x_n, Q'_1 \ \ldots \ Q'_m \ (\psi_0 \vee \psi_1).$$

(4) Si $\phi = (\phi_0 \wedge \phi_1)$, alors ce cas est totalement similaire au cas précédent.

(5) Si $\phi = \exists x \ \theta$, alors, par hypothèse d'induction, $\theta \equiv \theta'$ avec θ' sous forme prénexe polie : $\theta' = Q_1 x_1 \ \ldots \ Q_k x_k \ \psi'$. Par conséquent :

   (a) si $x \notin \{x_1, \ldots, x_n\}$, il suffit de prendre $\psi = \exists x \ Q_1 x_1 \ldots \ Q_k x_k \ \psi'$,

   (b) si $x \in \{x_1, \ldots, x_n\}$, il suffit de prendre $\psi = Q_1 x_1 \ldots \ Q_k x_k \ \psi'$.

(6) Si $\phi = \forall x \ \theta$, alors ce cas est identique, *mutatis mutandis*, au précédent.

$\dashv$ 391

Remarques 392

(1) Nous retrouvons, avec la logique du 1er ordre, les mêmes notions de systèmes complets de connecteurs que nous avions vues dans le cadre du Calcul Propositionnel pour ce qui est des formules sans quantificateur. Par ailleurs, il est immédiat de voir qu'une formule de la forme $\forall x \ \phi$ est équivalente à la formule $\neg\exists x \ \neg\phi$, de même que $\exists x \ \phi$ est équivalente à $\neg\forall x \ \neg\phi$. Nous déduisons de cela que les systèmes suivants sont tous des systèmes complets de connecteurs et quantificateurs :

(a) $\{\neg, \vee, \exists\}$ (b) $\{\neg, \vee, \forall\}$ (c) $\{\neg, \wedge, \exists\}$ (d) $\{\neg, \wedge, \forall\}$.

(2) En combinant ce que nous venons de dire avec le résultat du Théorème 391, nous voyons que toute formule ϕ est équivalente à une formule sous forme prénexe $Q_1x_1, \ldots, Q_kx_k\psi$ d'une part, la partie sans quantificateur de la formule (ψ) pouvant être supposée ne comportant que les seuls connecteurs $\vee, \wedge$ et $\neg$, d'autre part. Dès lors, en utilisant les lois de De Morgan, nous pouvons pousser les négations à l'intérieur de la formule ψ de manière à obtenir une formule équivalente ψ' qui ne comporte des symboles de négation que devant les formules atomiques.

Nous pouvons ensuite utiliser la distributivité de la disjonction par rapport à la conjonction et inversement, de manière à obtenir une formule ψ'' équivalente à ψ' (et donc équivalente à ψ) qui soit, au choix, sous forme normale conjonctive ou disjonctive.

6.1 Formes normales

Définition 393 *Une formule* ϕ sans quantificateur *est sous forme normale disjonctive (en abrégé* FND*), s'il existe :*

(1) un entier $k \geq 1$,

(2) des entiers $n_1, \ldots, n_k$,

(3) et pour chaque $i \in \{1, 2, \ldots, k\}$ *il existe*

(a) n_i *formules atomiques :* $A_{i,j_1}, \ldots, A_{i,j_{n_i}}$,

(b) n_i *éléments :* $\varepsilon_{i,j_1}, \ldots, \varepsilon_{i,j_{n_i}}$ *parmi* $\{\neg, \not\neg\}$[4]

tels que :

$$\phi = \bigvee_{1 \leq i \leq k} \Big(\bigwedge_{1 \leq j \leq n_i} \varepsilon_{i,j} A_{i,j} \Big).$$

Elle est dite sous forme normale conjonctive (en abrégé FNC*), si elle vérifie les conditions (1), (2) et (3) ci-dessus et s'écrit :*

$$\phi = \bigwedge_{1 \leq i \leq k} \Big(\bigvee_{1 \leq j \leq n_i} \varepsilon_{i,j} A_{i,j} \Big).$$

Proposition 394 *Pour toute formule* sans quantificateur ϕ *il existe :*

(1) $\phi_\vee$ *sous FND telle que* $\phi \equiv \phi_\vee$ *et*

(2) $\phi_\wedge$ *sous FNC telle que* $\phi \equiv \phi_\wedge$.

Preuve de la Proposition 394 : Immédiate par induction sur la hauteur de la formule ϕ.

$\dashv$ 394

En combinant ce résultat avec celui sur les formes prénexes, nous obtenons un résultat de forme normale sur les formules de la logique du 1[er] ordre :

4. Par convention, pour toute formule ψ, on a $\not\neg\psi = \psi$.

Théorème 395 *Pour toute formule ϕ il existe :*

(1) des variables $x_1, \ldots, x_k$,

(2) des quantificateurs $Q_1, \ldots, Q_k$,

(3) des formules sans quantificateur, *respectivement sous FND et FNC, $\phi_\vee$ et $\phi_\wedge$ telles que :*

$$\phi \;\equiv\; Q_1x_1, \ldots, Q_kx_k\ \phi_\vee \;\equiv\; Q_1x_1, \ldots, Q_kx_k\ \phi_\wedge.$$

Les formules $Q_1x_1, \ldots, Q_kx_k\ \phi_\vee$ et $Q_1x_1, \ldots, Q_kx_k\ \phi_\wedge$ sont dites respectivement forme prénexe disjonctive *et* forme prénexe conjonctive.

Preuve du Théorème 395 : Immédiate à partir du Théorème 391, et de la proposition 394. $\dashv$ 395

Il est particulièrement intéressant de remarquer que le jeu d'évaluation associer à la formule $Q_1x_1, \ldots, Q_kx_k\ \phi_\vee$ consiste tout d'abord à choisir k éléments dans le domaine du modèle considéré – et cela en fonction de la nature des quantificateurs impliqués – puis le **V**érificateur choisit (la valeur i) avant de laisser la main au **F**alsificateur qui choisit à son tour (la valeur j) puis le jeu stoppe – avec éventuellement un unique changement de chapeau si $\varepsilon_{i,j}$ représente le symbole de négation – avec la formule atomique $A_{i,j}$ dans laquelle les variables avaient été remplacées par les k éléments choisis en début de partie. C'est donc un jeu particulièrement simple. Celui associé à la formule duale $Q_1x_1, \ldots, Q_kx_k\ \phi_\wedge$ est tout à fait semblable, à la différence près que lors des déplacements le long de $\phi_\wedge$, c'est d'abord le **F**alsificateur qui a la main, avant de la laisser au **V**érificateur.

7 Conséquence sémantique et théories

***Résumé* № 57**

(1) Une théorie $\mathcal{T}$ de $\mathcal{L}$ est un ensemble de formules closes de $\mathcal{L}$.

(2) Si $\mathcal{M}$ est une $\mathcal{L}$-structure, $\mathcal{T}$ est satisfaite dans $\mathcal{M}$ (noté $\mathcal{M} \models \mathcal{T}$) si pour toute formule $\psi \in \mathcal{T}$:

$$\mathcal{M} \models \phi.$$

(3) Une formule ϕ de $\mathcal{L}$ est conséquence[a] de $\mathcal{T}$ (noté $\mathcal{T} \models \phi$) si pour toute $\mathcal{L}$-structure $\mathcal{M}$:

$$\mathcal{M} \models \mathcal{T} \implies \mathcal{M} \models \phi.$$

※

a. Au sens sémantique.

Nous rappelons que de manière imagée, une formule se comporte comme une phrase du langage vernaculaire. Cette comparaison se poursuit avec les notions de livre ou de discours, tous deux perçus comme des ensembles de phrases. L'équivalent logique du livre ou du discours est la *théorie*. Une théorie n'est donc pas autre chose qu'un ensemble (fini ou même infini) de formules. Mais comme toujours avec la logique du 1$^{\text{er}}$ ordre, le langage dans lequel sont écrites les formules de cette théorie est préalablement fixé.

Définition 396 *Une théorie $\mathcal{T}$ de la logique du 1$^{\text{er}}$ ordre est un ensemble de formules d'un langage $\mathcal{L}$ donné. On parle également d'une $\mathcal{L}$-théorie.*

La sémantique associée à la notion de théorie rejoint celle que nous avons développée dans le cadre du Calcul Propositionnel : on interprète une théorie comme on interpète les formules qui la constituent.

Définition 397 *Soient $\mathcal{L}$ un langage du 1$^{\text{er}}$ ordre, $\mathcal{T}, \mathcal{T}'$ deux $\mathcal{L}$-théories ϕ une formule du langage $\mathcal{L}$ et $\mathcal{M}$ une $\mathcal{L}$-structure ,*

(1) $\mathcal{T}$ est satisfaite *dans $\mathcal{M}$, ou encore $\mathcal{M}$ est un modèle de $\mathcal{T}$, noté $\mathcal{M} \vDash \mathcal{T}$ ssi pour toute formule $\phi \in \mathcal{T}$ $\mathcal{M} \vDash \phi$.*

(2) $\mathcal{T}$ est consistante, *(encore appelé* satisfaisable, *ou même parfois* non-contradictoire[5]*) ssi il existe au moins une $\mathcal{L}$-structure $\mathcal{M}$ tel que $\mathcal{M} \vDash \mathcal{T}$.*

(3) $\mathcal{T}$ est inconsistante *(ou encore parfois* contradictoire*) ssi $\mathcal{T}$ n'est pas satisfaisable. Par conséquent, si pour toute $\mathcal{L}$-structure $\mathcal{M}$, il existe une formule $\phi_{\mathcal{M}} \in \mathcal{T}$ qui n'est pas vérifiée dans $\mathcal{M}$ ($\mathcal{M} \nvDash \phi_{\mathcal{M}}$).*

5. *Consistance* et *non-contradiction* sont deux aspects de la notion de *cohérence* d'une théorie. Nous réserverons le terme de *consistance* à la notion sémantique de la cohérence (intuitivement une théorie est *consistante* si elle consiste en quelque chose, si elle témoigne de quelque chose de palpable, comme un modèle qui la vérifie) et celui de *non-contradiction* à la notion syntaxique de la cohérence (intuitivement une théorie est *non-contradictoire* si elle ne dit pas une chose et son contraire, si l'on ne peut parvenir à prouver une contradiction).

(4) ϕ *est une* conséquence logique *de* $\mathcal{T}$ *(ou plus simplement* ϕ *est* conséquence *de* $\mathcal{T}$*), noté* $\mathcal{T} \models \phi$*, ssi tout modèle de* $\mathcal{T}$ *est un modèle de* ϕ*. Autrement dit, pour toute* $\mathcal{L}$*-structure* $\mathcal{M}$*, si* $\mathcal{M} \models \mathcal{T}$ *alors* $\mathcal{M} \models \phi$*.*

(5) $\mathcal{T}$ *et* $\mathcal{T}'$ *sont deux théories équivalentes ssi elles ont exactement les mêmes modèles.*

Exemple 398 Soit $\mathcal{L}$ le langage qui contient deux symboles de relations unaires : P, Q ainsi qu'un symbole de relation binaire R. Les $\mathcal{L}$-théories suivantes sont toutes équivalentes :

(1) $\mathcal{T}_1 = \{\neg\exists x\ \exists y\ (P(x) \wedge Q(y)),\ \exists x\ \forall y\ (P(x) \wedge R(x,y)),\ \forall x\ P(x)\}$

(2) $\mathcal{T}_2 = \{\forall x\ \forall y\ \neg(P(x) \wedge Q(y)),\ \exists x\ \forall y\ (P(x) \wedge R(x,y)),\ \forall x\ P(x)\}$

(3) $\mathcal{T}_3 = \{\forall x\ \forall y\ (P(x) \longrightarrow \neg Q(y)),\ \exists x\ \forall y\ R(x,y),\ \forall x\ P(x)\}$

(4) $\mathcal{T}_4 = \{\forall x\ P(x),\ \forall x\ \neg Q(x),\ \exists x\ \forall y\ R(x,y)\}$.

L'idée qui se cache derrière la notion de théories équivalentes est que ces théories représentent des manières différentes de dire la même chose. Deux théories sont équivalentes s'il n'existe pas de modèle capable de les distinguer. Si l'on considère les théories d'un point de vue sémantique – et c'est d'ailleurs ce que nous faisons lorsque nous nous attachons à l'équivalence des théories – la signification d'une théorie est l'ensemble de ses modèles. Dire que deux théories sont équivalentes, c'est dire qu'elles ont la même signification. Elles forment toutes deux une description des mêmes mondes possibles.

Exemple 399 [Arithmétique de Peano]

Soit $\mathcal{L} = \{\mathsf{c}_0, f_s, f_+, f_\times, =\}$ où c_0 est un symbole de constante, f_s est un symbole de fonction unaire et $f_+, f_\times$ sont des symboles de fonction binaires. La théorie de Peano $\mathcal{T}_\mathcal{P}$ est l'ensemble *infini* de formules contenant :

(1) $\forall x\ \neg f_s(x) = \mathsf{c}_0$

(2) $\forall x\ \exists y\ (\neg x = \mathsf{c}_0 \longrightarrow f_s(y) = x$

(3) $\forall x\ \forall y\ (f_s(x) = f_s(y) \longrightarrow x = y)$

(4) $\forall x\ f_+(x, \mathsf{c}_0) = x$

(5) $\forall x\ \forall y\ \Big(f_+(x, f_s(y)) = f_s(f_+(x,y))\Big)$

(6) $\forall x\ f_\times(x, \mathsf{c}_0) = \mathsf{c}_0$

(7) $\forall x\ \forall y\ \Big(f_\times(x, f_s(y)) = f_+(f_\times(x,y), x)\Big)$

(8) Pour toute formule $\phi_{[x_0, x_1, \ldots, x_n]}$ (formules dont toutes les variables libres sont parmi $x_0, x_1, \ldots, x_n$), la formule suivante fait aussi partie de $\mathcal{T}_\mathcal{P}$.

$$\forall x_0\ \forall x_1\ \ldots\ \forall x_n\ \Big(\big(\phi_{[\mathsf{c}_0/x_0]}\ \wedge\ \forall x_0\ (\phi \longrightarrow \phi_{[f_s(x_0)/x_0]})\big) \longrightarrow \forall x_0\ \phi\Big).$$

Remarques 400

(1) Cette théorie s'appelle l'axiomatique de Peano. Il est très important de remarquer qu'elle contient un nombre infini de formules (encore appelées axiomes). En effet, le cas (8) n'est pas un axiome à proprement parler, mais un *schéma d'axiomes*, il propose autant d'axiomes qu'il y a de formules de ce langage. Et il y a bien évidemment une infinité de formules pouvant être écrites avec ce langage.

(2) Cette théorie admet un modèle très naturel, c'est d'ailleurs pour rendre compte de l'arithmétique qu'elle fut mise au point. Ce modèle $\mathcal{N}$ a pour domaine de base $\mathbb{N}$ (l'ensemble des entiers naturels), $\mathsf{c}_0^{\mathcal{N}} = 0$, $f_s^{\mathcal{N}}$ est la fonction successeur ($f_s^{\mathcal{N}}(n) = n+1$), $f_+^{\mathcal{N}}$ et $f_\times^{\mathcal{N}}$ sont respectivement l'addition et la multiplication. On appelle ce modèle le modèle standard de l'arithmétique.

Il est tout à fait évident que les sept premiers axiomes sont trivialement satisfaits dans ce modèle. Quant au schéma d'axiome (8), il exprime le schéma d'induction. Il est nécessaire pour toutes les preuves par induction en arithmétique.

(3) Ce modèle s'appelle le *modèle standard* de l'arithmétique. Mais existe-t-il d'autres modèles ? Nous allons voir dans la section suivante qu'il existe effectivement d'autres modèles de l'arithmétique. On les appelles les *modèles non standards.* Ils se comportent exactement comme le *modèle standard* lorsqu'on les regarde de l'intérieur, c'est-à-dire lorsqu'on les regarde avec les moyens de la logique du 1$^{\text{er}}$ ordre muni du langage ci-dessus. Plus précisément, ce qui distingue un *modèle non standard* du *modèle standard* ne peut être exprimé par une formule du 1$^{\text{er}}$ ordre. Par contre, lorsqu'on les regarde de l'extérieur, ils n'ont pas les mêmes éléments dans leur domaine de base. Et cette différence n'est pas simplement une différence de dénomination – il serait facile, par exemple, de substituer au domaine de base $\mathbb{N}$, un ensemble qui soit en bijection avec celui-ci (par exemple l'ensemble M des suites finies ne contenant que la lettre a, ou encore plus simplement l'ensemble des mots construits sur l'alphabet ne contenant que la lettre a : $\{\varepsilon, a, aa, aaa, aaaa, \ldots\}$, où ε désigne le mot vide, c'est-à-dire le mot de longueur 0). A partir d'une bijection entre domaines de base : φ de $\mathbb{N}$ dans M définie par $\varphi(n) = \underbrace{aa\ldots a}_{n}$, il est aisé de construire un modèle $\mathcal{M}$ dont le domaine de base est précisément M et l'interprétation des différents symboles du langage est exactement ce qu'il faut pour que la bijection φ soit un isomorphisme :

(a) $\mathsf{c}_0^{\mathcal{M}} = \varepsilon$

(b) $f_s^{\mathcal{M}}(\underbrace{aa\ldots a}_{n}) = \underbrace{aa\ldots a}_{n+1}$

(c) $f_+^{\mathcal{M}}(\underbrace{aa\ldots a}_{n}, \underbrace{aa\ldots a}_{m}) = \underbrace{aa\ldots a}_{n+m}$

(d) $f_\times^{\mathcal{M}}(\underbrace{aa\ldots a}_{n}, \underbrace{aa\ldots a}_{m}) = \underbrace{aa\ldots a}_{n\cdot m}$.

Mais précisément, ces deux modèles sont isomorphes, le modèle $\mathcal{M}$ n'est finalement que le modèle standard dans lequel nous avons changé le nom des éléments. L'élément n prenant le nom du mot de n lettres $\underbrace{aa\ldots a}_{n}$.

Or, les *modèles non standards* ne sont pas des modèles isomorphes au *modèle standard*, ils ne sont pas construits sur la base d'un simple renommage des éléments du domaine de base. Ils contiennent une *copie* du *modèle standard* dont les éléments sont appelés *entiers standards*, mais également d'autres éléments, différents des entiers standards, qui sont de ce fait dénommés *"entiers non standards"*.

Exemple 401 Soit $\mathcal{L} = \{P_0, P_1, P_2, R, c\}$ où P_0, P_1, P_2 sont des symboles de relation unaires, R est un symbole de relation binaire et c une constante. Les théories suivantes sont toutes inconsistantes. Elles sont donc aussi toutes équivalentes.

(1) $\mathcal{T}_1 = \{\forall x\ P_0(x),\ \forall x\ (P_0(x) \longrightarrow P_1(x)),\ (P_2(\mathsf{c}) \longrightarrow \neg P_1(\mathsf{c})),\ \forall x\ (P_2(x) \vee \neg P_0(x))\}$

(2) $\mathcal{T}_2 = \{\exists x\ P_0(x),\ \forall x\ (P_0(x) \longrightarrow P_2(x)),\ \forall x\ (P_0(x) \longrightarrow \neg P_2(x))\}$

(3) $\mathcal{T}_3 = \{\exists x\ (P_0(\mathsf{c}) \wedge \neg P_1(x)),\ \forall x\ P_1(x),\ \neg\exists x\ P_0(x)\}$

(4) $\mathcal{T}_4 = \{\forall x\ R(\mathsf{c}, x),\ \forall x\ \exists\ \neg R(x, y),\ \forall x\ \exists y\ \neg R(x, y),\ \neg R(\mathsf{c}, \mathsf{c})\}$

(5) $\mathcal{T}_5 = \{\forall x\ (R(\mathsf{c}, x) \vee \neg P_0(x)),\ P_0(\mathsf{c}),\ \neg R(\mathsf{c}, \mathsf{c})\}$.

Une théorie inconsistante est une théorie qui n'a pas de modèle. Elle n'a donc pas de signification, elle ne décrit, à proprement parler, rien. Elle ne parle de rien, ou plus exactement, elle parle, mais pour ne rien dire. A noter tout de même qu'une théorie inconsistante parle beaucoup, si l'on entend par là toutes les conséquences logiques (sémantiques) d'une telle théorie. Puisque toute formule est conséquence logique d'une théorie inconsistante, une telle théorie dit tout, absolument tout, mais cela n'a aucune signification. C'est d'ailleurs précisément le fait de pouvoir tout dire (toute chose et son contraire) qui rend absurde toute interprétation.

Exemple 402 Soit $\mathcal{L} = \{P,\ Q, R, c\}$ où $P,\ Q$ sont des symboles de relation unaires, R est un symbole de relation binaire et c une constante. On considère la théorie suivante :

$$\mathcal{T} = \{\forall x\ (P(x) \vee \neg Q(x)),\ \neg(P(\mathsf{c}) \wedge Q(\mathsf{c})),\ \exists x\ (Q(x) \wedge R(\mathsf{c}, x))\}.$$

On a :

(1) $\mathcal{T} \models\ \neg Q(\mathsf{c})$

(2) $\mathcal{T} \not\models\ \forall x\ P(x)$

(3) $\mathcal{T} \models\ \forall x\ (Q(x) \vee \neg Q(x))$

(4) $\mathcal{T} \not\models\ \exists x\ \wedge R(x, \mathsf{c})$

(5) $\mathcal{T} \models\ \exists x\ Q(x)$.

La notion de conséquence logique constitue la version sémantique de la déduction. Une formule est conséquence logique d'une théorie si elle est vraie partout où cette théorie est vraie. Il faudrait, en fait, parler de conséquence *logique sémantique* pour celle que nous venons de décrire et de conséquence *logique syntaxique* pour celle issue de la théorie de la démonstration.

Exemple 403 Soit $\mathcal{L}$ le langage qui ne contient que l'égalité. On considère les différentes théories suivantes ainsi que leurs modèles :

(1) $\mathcal{T}_1 = \{\forall x\ \forall y\ x = y\}$. Cette théorie n'admet pour modèle que des ensembles qui ne contiennent qu'un seul élément.

(2) $\mathcal{T}_2 = \{\exists x_1\ \exists x_2\ \neg x_1 = x_2\}$. Les modèles de cette théorie ont au moins deux éléments.

(3) $\mathcal{T}_3 = \{\exists x_1 \exists x_2 \neg x_1 = x_2,\ \exists x_1 \exists x_2 \exists x_3 \left(\neg x_1 = x_2 \wedge \neg x_1 = x_3 \wedge \neg x_2 = x_3\right)\}$. Les modèles de cette théorie ont au moins trois éléments.

(4) $\mathcal{T}_n = \{\exists x_1 \exists x_2 \neg x_1 = x_2, \ldots,\ \exists x_1 \ldots \exists x_n \bigwedge_{i \neq j} \neg x_i = x_j\}$.

Les modèles de cette théorie ont tous au moins n éléments distincts.

(5) $\mathcal{T}_\infty = \{\exists x_1 \ldots \exists x_n \bigwedge_{i \neq j} \neg x_i = x_j \mid n \in \mathbb{N}\}$.

Cette théorie contient une infinité de formules. Une formule pour chaque entier n, qui dit précisément qu'il existe n éléments distincts. On voit donc qu'aucun modèle de cette théorie ne peut avoir un nombre fini d'éléments. Les modèles de cette théorie sont tous les modèles dont le domaine contient une infinité d'éléments.

Définition 404 *Soit $\mathcal{L}$ un langage du 1er ordre. Une formule (respectivement une théorie) est dite (universellement valide) si elle est satisfaite dans n'importe quelle $\mathcal{L}$-structure.*

Remarques 405 Une conséquence immédiate des notions de théories équivalentes et de formules équivalentes est que si l'on remplace, dans une théorie $\mathcal{T}$ quelconque, chaque formule par une formule qui lui est logiquement équivalente, on obtient alors une théorie qui est elle-même équivalente à la théorie $\mathcal{T}$ d'origine. Dans le cas d'une théorie finie $\mathcal{T} = \{\phi_0, \phi_1, \ldots, \phi_k\}$, la théorie est équivalente à une théorie ne comportant qu'une unique formule : $\phi_\mathcal{T} = \left(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_k\right)$. Par conséquent, si $\mathcal{T}$ et $\mathcal{T}'$ sont deux théories finies telles que $\phi_\mathcal{T}$ et $\phi_{\mathcal{T}'}$ représentent la conjonction des formules respectivement de $\mathcal{T}$ et $\mathcal{T}'$, alors ces deux théories sont équivalentes ($\mathcal{T} \equiv \mathcal{T}'$) précisément lorsque ces formules sont équivalentes ($\phi_\mathcal{T} \equiv \phi_{\mathcal{T}'}$).

Plus généralement, nous avons les équivalences qui suivent :

(1) les énoncés suivants sont équivalents :
   - (a) $\mathcal{T}$ est *satisfaisable*
   - (b) pour toute $\mathcal{T}' \subseteq \mathcal{T}$, $\mathcal{T}'$ est *satisfaisable*
   - (c) il existe ϕ, $\mathcal{T} \not\models \phi$.

(2) les énoncés suivants sont équivalents :
   - (a) $\mathcal{T}$ est *inconsistante*
   - (b) pour ϕ quelconque, $\mathcal{T} \models \phi \wedge \neg\phi$
   - (c) pour *toute* ϕ, $\mathcal{T} \models \phi$
   - (d) pour ϕ *contradiction* quelconque, $\mathcal{T} \models \phi$
   - (e) pour toute $\mathcal{T} \subseteq \mathcal{T}'$, $\mathcal{T}'$ est *inconsistante*
   - (f) $\mathcal{T} \equiv \mathcal{F}^{cl}_\mathcal{L}$ (l'ensemble des formules closes de $\mathcal{L}$).

(3) les énoncés suivants sont équivalents :
   - (a) ϕ est *universellement valide*
   - (b) pour *toute théorie* $\mathcal{T}$, $\mathcal{T} \models \phi$
   - (c) $\emptyset \models \phi$.

(4) les énoncés suivants sont équivalents :
  (a) $\mathcal{T} \models \phi$
  (b) $\mathcal{T} \cup \{\neg\phi\}$ est *inconsistante*
  (c) il existe $\mathcal{T}' \subseteq \mathcal{T}$, $\mathcal{T}' \models \phi$.

(5) les énoncés suivants sont équivalents :
  (a) $\mathcal{T} \cup \{\phi\} \models \psi$
  (b) $\mathcal{T} \models (\phi \longrightarrow \psi)$.

Nous laissons au lecteur les preuves de chacune des équivalences mentionnées ci-dessus, qui sont de simples affaires de définition.

Il est tout à fait immédiat que si une théorie $\mathcal{T}$ est satisfaisable, alors cette théorie admet un modèle qui satisfait à son tour chacune des formules de $\mathcal{T}$, donc qui satisfait chacune des sous-théories $\mathcal{T}' \subseteq \mathcal{T}$ et en particulier chacune des sous-théories *finies* $\mathcal{T}' \subseteq \mathcal{T}$. En conséquence, si une théorie $\mathcal{T}$ est satisfaisable, alors chaque sous-théorie *finie* $\mathcal{T}' \subseteq \mathcal{T}$ est également *satisfaisable*. Par contre, la réciproque semble *a priori* complètement fausse : si chaque sous-théorie *finie* d'une théorie est *satisfaisable*, alors cette théorie toute entière admet aussi un modèle. En effet, on ne voit pas pourquoi le fait que chaque sous-partie *finie* de $\mathcal{T}$ soit satisfaisable entraînerait que $\mathcal{T}$ soit elle-même satisfaisable. C'est pourtant le cas. Ce résultat étonnant va nous occuper dans le chapitre à venir.

8 Le théorème de compacité et les entiers non standards

***Résumé* № 58** *Pour toute théorie $\mathcal{T}$ et formule ϕ :*
- $\mathcal{T}$ *est* satisfaisable *ssi chaque* $\mathcal{T}'$ finie $\subseteq \mathcal{T}$ *est* satisfaisable
- $\mathcal{T} \models \phi$ *ssi il existe* $\mathcal{T}'$ finie $\subseteq \mathcal{T}$, $\mathcal{T}' \models \phi$
- $\mathcal{T}$ *est inconsistante ssi il existe* $\mathcal{T}' \subseteq \mathcal{T}$, $\mathcal{T}'$ finie *et inconsistante.*

※

Si $\mathcal{T}$ est une $\mathcal{L}$-théorie telle que pour toute théorie $\mathcal{T}'$ *finie* $\subseteq \mathcal{T}$, il existe $\mathcal{M}'$ une $\mathcal{L}$-structure telle que $\mathcal{M}' \models \mathcal{T}'$, alors nous allons voir que la théorie $\mathcal{T}$ elle-même admet un modèle. Tout d'abord, il est clair que si $\mathcal{T}$ est satisfaisable, alors $\mathcal{T}$ admet un modèle et ce même modèle satisfait également chaque $\mathcal{T}' \subseteq \mathcal{T}$, donc en particulier chaque $\mathcal{T}'$ *finie* $\subseteq \mathcal{T}$. En conséquence, si $\mathcal{T}$ est *satisfaisable*, $\mathcal{T}$ est également *finement satisfaisable.*

Par contre, l'implication inverse semble à première vue fausse. Si chaque sous-théorie finie $\mathcal{T}' \subseteq \mathcal{T}$ admet un modèle, on ne voit pas comment il serait possible, à partir de ceux-ci, de construire un modèle qui satisfasse la théorie $\mathcal{T}$ tout entière ? Pourtant cela se peut.

Thèorème 406 (Thèorème de compacité – Gödel-Malcev) *Soient $\mathcal{L}$ un langage du 1^er^ ordre et $\mathcal{T}$ une théorie de ce langage,*

$$\mathcal{T} \textit{ est satisfaisable ssi } \mathcal{T} \textit{ chaque } \mathcal{T}' \textit{ finie } \subseteq \mathcal{T} \textit{ est satisfaisable .}$$

Ou, pour le dire autrement, $\mathcal{T}$ admet un modèle si et seulement si chaque théorie *finie* $\mathcal{T}' \subseteq \mathcal{T}$ admet un modèle. Ce théorème n'a d'intérêt que pour les théories infinies. Comme nous l'avons dit, il possède un sens évident de peu d'intérêt : si $\mathcal{T}$ est satisfaisable, alors $\mathcal{T}$ est finiement satisfaisable. Par contre, l'autre sens suscite un bien plus grand intérêt : le fait qu'il suffise qu'une théorie soit finiement satisfaisable pour qu'elle soit satisfaisable a de nombreuses applications.

Corollaire 407 *Soient $\mathcal{L}$ un langage du 1^er^ ordre, $\mathcal{T}$ une théorie de ce langage,*

$$\mathcal{T} \textit{ est inconsistante ssi il existe } \mathcal{T}' \subseteq \mathcal{T}, \mathcal{T}' \textit{inconsistante et finie.}$$

Preuve du Corollaire 407 : Du fait que "A si et seulement si B" étant une assertion équivalente à "$\neg A$ si et seulement si $\neg B$", il découle du théorème de compacité que $\mathcal{T}$ n'est pas satisfaisable si et seulement s'il existe $\mathcal{T}'$ finie $\subseteq \mathcal{T}$ qui soit inconsistante. ⊣ 407

Corollaire 408 *Soient $\mathcal{L}$ un langage du 1^er^ ordre, $\mathcal{T}$ et ϕ respectivement une théorie et une formule de ce langage,*

$$\mathcal{T} \models \phi \textit{ ssi il existe } \mathcal{T}' \subseteq \mathcal{T}, \mathcal{T}' \textit{ finie telle que } \mathcal{T}' \models \phi.$$

Preuve du Corollaire 408 : Nous avons vu à la page 440 que l'assertion "$\mathcal{T} \models \phi$" était équivalente à l'énoncé "$\mathcal{T} \cup \{\neg\phi\}$ est inconsistante". Par le Corollaire 407, nous savons que $\mathcal{T} \cup \{\neg\phi\}$ est inconsistante si et seulement si il existe $\mathcal{T}' \subseteq \mathcal{T} \cup \{\neg\phi\}$ qui soit à la fois finie et inconsistante. Il suffit de remarquer qu'indépendamment du fait que $\neg\phi$ appartienne ou non à la sous-théorie $\mathcal{T}'$, nous avons toujours que $\mathcal{T}' \cup \{\neg\phi\}$ est à la fois finie et inconsistante, ce qui est équivalent à dire que $\mathcal{T}'$ est une sous-théorie finie satisfaisant $\mathcal{T}' \models \{\phi\}$. ⊣ 408

Preuve du Théorème 406 : La preuve directe de ce théorème – celle qui donne son nom au théorème car elle utilise la propriété de compacité – nécessite l'utilisation d'arguments topologiques qui sont très loin des préoccupations de ce cours. On trouvera néanmoins cette preuve dans le *"Cours de théorie des modèles : une introduction à la Logique mathématique contemporaine"* ou dans la version anglaise de Bruno Poizat [Poi85, Poi00].

Une preuve directe est disponible en annexe (cf Chapitre 18 page 545). Elle utilise des outils de théorie des modèles à la fois magnifiques mais aussi malheureusement beaucoup trop avancés pour faire partie du corps de cet ouvrage – raison pour laquelle cette preuve est disponible en annexe.

Une dernière preuve découlera du théorème de complétude (Théorème 439, page 474). Cette preuve consistera à transférer le problème du champs sémantique dans le champs syntaxique où sa réponse sera alors très aisée (voir page 480). ⊣ 406

Dans l'exemple suivant, le fait que chaque sous-théorie finie ait un modèle est évident, mais la nature d'un modèle pour la théorie entière (que l'on déduit par théorème de compacité) est très intriguante. En effet, nous allons utiliser le théorème de compacité pour montrer qu'il existe (au moins) un modèle non standard de l'arithmétique.

Exemple 409 Nous reprenons ici la théorie $\mathcal{T}_{\mathcal{P}}$, présentée dans l'Exemple 399 et dénommée *arithmétique de Peano*. Nous construisons la théorie $\mathcal{T}_{\mathcal{P}}^{+}$ en ajoutant à la théorie $\mathcal{T}_{\mathcal{P}}$ une infinité de formules qui toutes ensembles disent qu'il existe un élément différent des entiers standards.

Le langage est donc $\mathcal{L} = \{\mathsf{c}, \mathsf{c}_0, f_s, f_+, f_\times, =\}$ où c et c_0 sont des symboles de constante, f_s est un symbole de fonction unaire et $f_+, f_\times$ sont des symboles de fonction binaires. La théorie $\mathcal{T}_{\mathcal{P}}^{+}$ est l'ensemble *infini* contenant :

(1) les axiomes de l'arithmétique de Peano :

(a) $\forall x \; \neg f_s(x) = \mathsf{c}_0$

(b) $\forall x \; \exists y \; (\neg x = \mathsf{c}_0 \longrightarrow f_s(y) = x)$

(c) $\forall x \; \forall y \; (f_s(x) = f_s(y) \longrightarrow x = y)$

(d) $\forall x \; f_+(x, \mathsf{c}_0) = x$

(e) $\forall x \; \forall y \; \Big(f_+(x, f_s(y)) = f_s(f_+(x,y))\Big)$

(f) $\forall x \; f_\times(x, \mathsf{c}_0) = \mathsf{c}_0$

(g) $\forall x \; \forall y \; \Big(f_\times(x, f_s(y)) = f_+(f_\times(x,y), x)\Big)$.

(h) Pour toute formule $\phi_{[x_0, x_1, \ldots, x_n]}$ (formules dont toutes les variables libres sont parmi $x_0, x_1, \ldots, x_n$), la formule suivante fait aussi partie de $\mathcal{T}_{\mathcal{P}}$.

$$\forall x_1 \; \ldots \; \forall x_n \; \Big(\big(\phi_{[\mathsf{c}_0/x_0]} \wedge \big(\forall x_0 \; \phi \longrightarrow \phi_{[f_s(x_0)/x_0]}\big)\big) \longrightarrow \forall x_0 \; \phi \Big).$$

(2) Et, pour chaque entier n, la formule $\neg\, c = \underbrace{f_s(f_s(\ldots(f_s}_{n}(c_0)\ldots))$ qui dit que la constante c ne peut pas être interprétée comme le $n^{\text{ème}}$ successeur de 0 (c'est-à-dire comme n).

Chaque sous-théorie finie $\mathcal{T}' \subseteq \mathcal{T}_{\mathcal{P}}^{+}$ est satisfaite dans le modèle standard. En effet, soit $\mathcal{T}' \subseteq \mathcal{T}_{\mathcal{P}}^{+}$ une sous-théorie finie. $\mathcal{T}'$ est la réunion d'un ensemble fini de formules de $\mathcal{T}_{\mathcal{P}}$ et d'un ensemble fini de formules de la forme $\neg\, c = \underbrace{f_s(f_s(\ldots(f_s}_{n}(c_0)\ldots))$.

Considérons $\mathcal{N}$ le modèle standard qui a pour domaine de base $\mathbb{N}$ et dans lequel $c_0^{\mathcal{N}} = 0$, $f_s^{\mathcal{N}}$ est la fonction successeur, $f_+^{\mathcal{N}}$ et $f_\times^{\mathcal{N}}$ sont respectivement l'addition et la multiplication. Il nous faut également une interprétation pour la constante c.

Pour cela, prenons n'importe quel entier n tel que la formule $\neg\, c = \overbrace{f_s(f_s(\ldots(f_s}^{n}(c_0)\ldots))$ *n'est pas* dans la théorie $\mathcal{T}'$ (il en existe nécessairement puisque $\mathcal{T}'$ est finie) et posons $c^{\mathcal{N}} = n$. Cette structure est clairement un modèle de $\mathcal{T}'$.

Par application du théorème de compacité, il existe donc un modèle $\mathcal{M}$ de $\mathcal{T}_{\mathcal{P}}^{+}$. Or, on voit aisément que ce modèle ne peut être le modèle standard puisque la constante c ne peut être interprétée par aucun des successeurs (finis) de 0 (l'élément du domaine par lequel on interprète c_0). Si l'on convient de dénommer entiers standards les éléments $c_0^{\mathcal{M}}$, $f_s^{\mathcal{M}}(c_0^{\mathcal{M}})$, $f_s^{\mathcal{M}}(f_s^{\mathcal{M}}(c_0^{\mathcal{M}}))$, ..., il apparaît que $c^{\mathcal{M}}$ n'est pas un entier standard.

Dans l'exemple précédent, un entier non standard se comporte exactement comme un entier, en ce sens qu'il intervient dans les opérations usuelles de l'arithmétique : il a un successeur, il peut être ajouté à tout entier, il peut être également multiplié à tout entier, mais il n'est aucun des entiers auxquels nous pensons.

Remarque 410 Aucun modèle non standard $\mathcal{M}$ de l'arithmétique n'est isomorphe au modèle standard. Cela résulte de la remarque que nous avons faite dans le cadre de l'exemple lui-même. S'il existait un tel isomorphisme, il enverrait $c_0^{\mathcal{M}}$ sur 0, puis $f_s^{\mathcal{M}}(c_0^{\mathcal{M}})$ sur 1, $f_s^{\mathcal{M}}(f_s^{\mathcal{M}}(c_0^{\mathcal{M}}))$ sur 2, etc. et il n'y aurait finalement aucun entier sur lequel envoyer $c^{\mathcal{M}}$...

Pour aller plus avant :

Le lecteur désirant retrouver la sémantique de la logique du 1er ordre dans un cadre bienveillant accueillera avec bonheur le livre *"An introduction to elementary logic"* de Wilfrid Hodges [Hod01]. Pour une approche plus poussée, nous recommandons, toujours du même auteur, *"A Shorter Model Theory"* de Wilfrid Hodges [Hod97]. Parmi les ouvrages beaucoup plus avancés mais passionnant, on trouve le *"Cours de théorie des modèles : une introduction à la Logique mathématique contemporaine"* de Bruno Poizat [Poi85], et les livres *"Model theory : an introduction"* de David Marker [Mar02] ainsi que *"Model theory"* de Chen C. Chang et H. Jerome Keisler [CK90]. Finalement, le lecteur exigeant pourra se référer aux ouvrages suivants dont le champs d'intérêt est toutefois restreint aux mathématiques : en allemand *"Einführung in die mathematische Logik"* de Heinz-Dieter Ebbinghaus, Jörg Flum et Wolfgang Thomas [EFT78], en anglais *"Mathematical logic,* de Joseph R. Shoenfield [Sho67] et *"A mathematical introduction to logic"* de Herbert B. Enderton [End72], en français *"Logique mathématique, tome 1 : Calcul Propositionnel; algèbre de Boole; calcul des prédicats"* de René Cori et Daniel Lascar [CLK03a].

Le nom le plus souvent évoqué lorsqu'on mentionne la sémantique de la logique du 1erordre est celui d'Alfred Tarski. Nous ne pouvons donc, pour clore ces recommandations, que chaleureusement conseiller son *"Introduction à la logique"* [Tar69], mais aussi *"Introduction to Metamathematics"* de Stephen C. Kleene [Kle52] et *"First-order logic"* de Raymond M. Smullyan [Smu95].

Le lecteur intrigué par l'arithmétique et ses modèles non standards pourra consulter *"An Introduction to the Theory of Numbers"* de Godfrey Harold Hardy et Edward Maitland Wright [HW79] ; *"Elements of number theory"* de John Stillwell [Sti03], ainsi que *"Models of Peano arithmetic"* de Richard Kaye [Kay91].

Chapitre 12

Traduction de la logique modale dans la logique du 1er ordre

***Résumé* № 59** *La logique modale admet une traduction en logique du 1er ordre qui consiste à associer :*

- *à chaque modèle $\mathcal{M}$ de la logique modale, un modèle $\mathcal{M}$ de la logique du 1er ordre ;*
- *à chaque formule modale ϕ, une formule du 1er ordre $\phi(x)$ ne comportant qu'une unique variable libre.*

Il ressort que les formules du du 1er ordre qui sont équivalentes à la traduction d'une formule modale sont exactement celles qui sont invariantes par bisimulation.

※

Dans ce chapitre nous allons traduire la logique modale en logique du 1er ordre. Cela consiste à faire la chose suivante :

(1) à chaque modèle $\mathcal{M}$ de la logique modale, on associe un modèle $\mathcal{M}$ de la logique du 1er ordre dont le domaine est constitué des mondes possibles du modèle de Kripke ;

(2) à chaque formule modale ϕ, on associe une formule de la logique du 1er ordre ne comportant qu'une unique variable libre $\phi(x)$

en sorte que pour tout monde possible a du modèle de Kripke $\mathcal{M}$:

$$a \Vdash \phi \text{ si et seulement si } \mathcal{M}, a/x \models \phi(x)$$

Pour cela, concentrons-nous tout d'abord sur ce qu'est un modèle de la logique modale. Un modèle de Kripke de la logique modale est un système de transition équipé d'une valuation (cf. Définition 219) : $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$. Un système de transition – étiqueté par I – est lui-même un graphe dirigé étiqueté (cf. Définition 197) $\mathcal{S} = (N, A)$.

Remarquons tout d'abord qu'un système de transition, en tant qu'il est une structure relationnelle, est évidemment un modèle de la logique du 1er ordre. En effet, l'ensemble N des nœuds du système – qui est un ensemble non vide – forme idéalement le domaine de base du modèle $\mathcal{M}$, et A, qui désigne un ensemble de relations binaires sur N indicées par I ($A = \{A_i \subseteq N \times N \mid i \in I\}$), induit tout naturellement autant de relations binaires qu'il y a d'éléments dans I. A chaque relation binaire A_i, on associe un symbole de relation binaire A_i dont l'interprétation dans dans $\mathcal{M}$ – dénotée $A_i^{\mathcal{M}}$ – est toute trouvée : $A_i^{\mathcal{M}} = A_i$.

Afin de caractériser le modèle de la logique modale $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ comme un modèle de la logique du 1er ordre, il nous reste à nous occuper de la valuation $\mathcal{V}$. *A priori* cela semble plus embêtant, car la valuation porte sur des variables propositionnelles qui sont des objets inexistants en logique du 1er ordre. Mais regardons les choses d'un peu plus près : par définition (cf. Définition 205) une valuation est une fonction :

$$\begin{array}{rccc} \mathcal{V}: & VAR & \longrightarrow & \mathcal{P}(N) \\ & P & \mapsto & \{a \mid a \Vdash P\} \end{array}$$

Elle associe donc à chaque variable propositionnelle P l'ensemble des mondes possibles qui satisfont P. Or, un ensemble de mondes possibles n'est rien d'autre qu'un sous-ensemble de l'ensemble des mondes possibles N, qui est lui-même le domaine de notre modèle $\mathcal{M}$: $|\mathcal{M}| = N$. Par ailleurs, un sous-ensemble du domaine de base d'un modèle s'exprime comme une relation unaire sur ce domaine. Dès lors, pour transposer la valuation du modèle de la logique modale dans celui de la logique du 1er ordre, il nous suffit, pour chaque variable propositionnelle considérée P, d'introduire un symbole de relation unaire P dont l'interprétation dans le modèle $\mathcal{M}$ n'est autre que l'ensemble des mondes possibles qui satisfont la variable propositionnelle P : $P^{\mathcal{M}} = \mathcal{V}(P)$.

Définition 411 *Soit $\mathcal{M} = \langle \mathcal{S}, \mathcal{V} \rangle$ un modèle de Kripke de la logique modale où $\mathcal{S} = (N, A)$ est un système de transition étiqueté par I – i.e. $A = \{A_i \subseteq N \times N \mid i \in I\}$ – et $\mathcal{V}$ est une valuation :*

$$\begin{array}{rccc} \mathcal{V}: & VAR & \longrightarrow & \mathcal{P}(N) \\ & P & \mapsto & \{a \mid a \Vdash P\} \end{array}$$

On associe à $\mathcal{M}$ le modèle de la logique du 1er ordre $\mathcal{M}$ défini de la manière suivante :

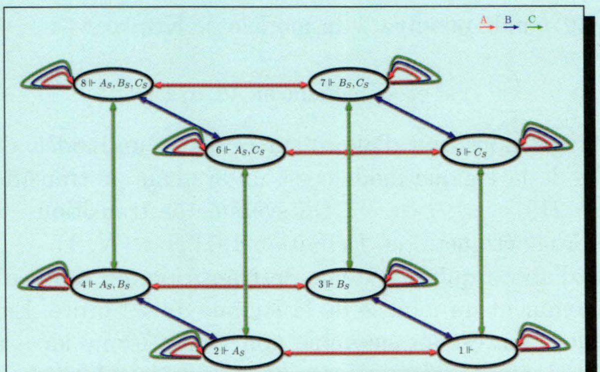
(1) La signature du langage du 1er ordre sur lequel est construit $\mathcal{M}$ ne comporte aucun symbole de constante ni de fonction, mais les seuls symboles de relations suivants :
- *pour chaque variable propositionnelle $P \in VAR$, un symbole de relation* unaire P ;
- *pour chaque $i \in I$, un symbole de relation* binaire A_i.

(2) Le domaine de $\mathcal{M}$ est $|\mathcal{M}| = N$;

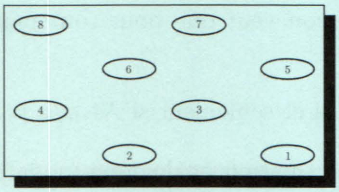
(3) L'interprétation de P dans $\mathcal{M}$ est $P^{\mathcal{M}} = \mathcal{V}(P)$;

(4) L'interprétation de A_i dans $\mathcal{M}$ est $A_i^{\mathcal{M}} = A_i$.

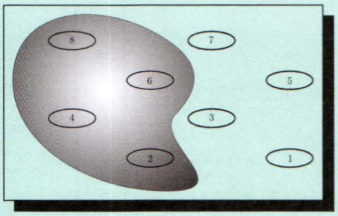
Exemple 412 Le modèle de Kripke $\mathcal{M}$ des enfants sales :

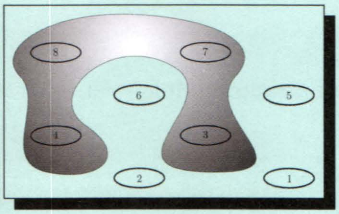


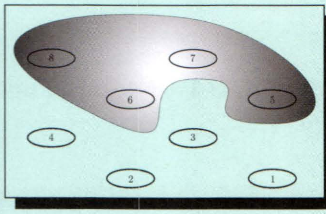
se traduit au 1$^{\text{er}}$ ordre par le modèle $\mathcal{M} = \langle N, A_s^{\mathcal{M}}, B_s^{\mathcal{M}}, C_s^{\mathcal{M}}, A^{\mathcal{M}}, B^{\mathcal{M}}, C^{\mathcal{M}}, \rangle$ suivant :
Le domaine de base est $N = \{1, 2, 3, 4, 5, 6, 7, 8\}$ représenté graphiquement par :



Les interprétations des relations unaires sont :

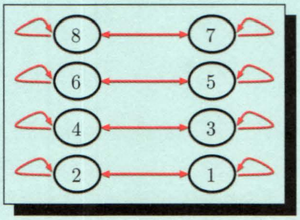


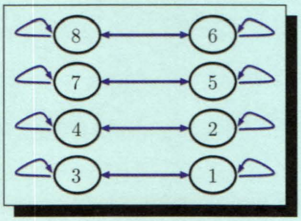


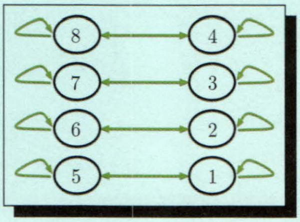


$A_s^{\mathcal{M}} = \{2, 4, 6, 8\}$ $B_s^{\mathcal{M}} = \{3, 4, 7, 8\}$ $C_s^{\mathcal{M}} = \{5, 6, 7, 8\}$

Les interprétations des relations binaires[1] sont représentées par les graphes suivants :







$A^{\mathcal{M}}$ $B^{\mathcal{M}}$ $C^{\mathcal{M}}$

Ensuite, à chaque formule modale ϕ, on associe une formule $\phi(x)$ de la logique du 1$^{\text{er}}$ ordre ne comportant qu'une seule et unique variable libre x.

Définition 413 *La traduction d'une formule de la logique modale ϕ en une formule $\phi(x)$ de la logique du 1er ordre est définie par récurrence sur la hauteur de ϕ :*
- *si $\phi = P$, alors $\phi = P(x)$*
- *si $\phi = \neg\psi$, alors $\phi(x) = \neg\psi(x)$*
- *si $\phi = (\psi_0 \vee \psi_1)$, alors $\phi(x) = (\psi_0(x) \vee \psi_1(x))$*
- *si $\phi = (\psi_0 \wedge \psi_1)$, alors $\phi(x) = (\psi_0(x) \wedge \psi_1(x))$*
- *si $\phi = (\psi_0 \longrightarrow \psi_1)$, alors $\phi(x) = (\psi_0(x) \longrightarrow \psi_1(x))$*
- *si $\phi = (\psi_0 \longleftrightarrow \psi_1)$, alors $\phi(x) = (\psi_0(x) \longleftrightarrow \psi_1(x))$*

1. *Stricto sensu*, ces relations binaires représentées sous forme de graphe forment les ensembles :
$A^{\mathcal{M}} = \{(1,1);(1,2);(2,1);(2,2);(3,3);(3,4);(4,3);(4,4);(5,5);(5,6);(6,5);(6,6);(7,7);(7,8);(8,7);(8,8)\}$,
$B^{\mathcal{M}} = \{(1,1);(1,3);(3,1);(3,3);(2,2);(2,4);(4,2);(4,4);(5,5);(5,7);(7,5);(7,7);(6,6);(6,8);(8,6);(8,8)\}$,
$C^{\mathcal{M}} = \{(1,1);(1,5);(5,1);(5,5);(2,2);(2,6);(6,2);(6,6);(3,3);(3,7);(7,3);(7,7);(4,4);(4,8);(8,4);(8,8)\}$.

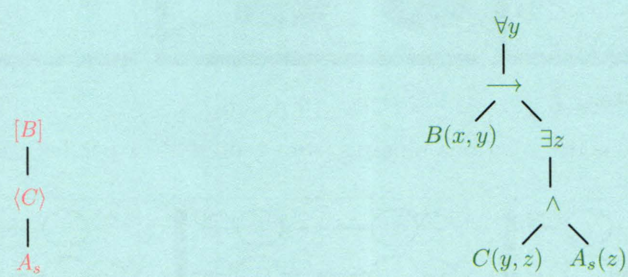
- *si* $\phi = \langle i \rangle \psi$, *alors* $\phi(x) = \exists y(A_i(x, y) \wedge \psi(y/x))$ [2]
- *si* $\phi = [i]\psi$, *alors* $\phi(x) = \forall y(A_i(x, y) \longrightarrow \psi(y/x))$ [2] .

Cette traduction est guidée par la sémantique de ces deux logiques. Elle représente exactement ce qui est nécessaire si l'on veut que pour tout monde possible a d'un modèle de Kripke $\mathcal{M}$, on obtienne :

$$a \Vdash \phi \text{ si et seulement si } \mathcal{M}, a/x \models \phi(x).$$

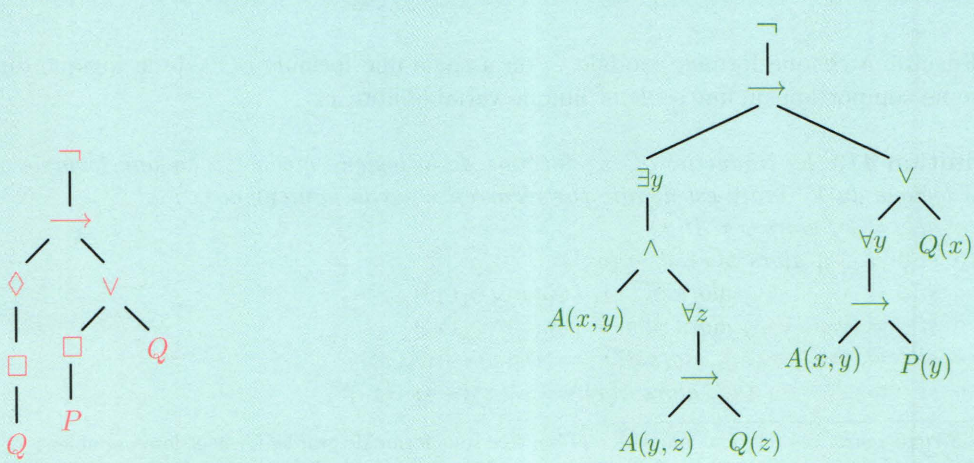
En particulier, dans un jeu d'évaluation en logique modale, une position de la forme $\langle i \rangle$ (respectivement $[i]$) correspond à un choix du **V**érificateur (respectivement du **F**alsificateur), de même que $\exists y$ (respectivement $\forall y$) correspond au choix du même joueur dans le jeu d'évaluation en logique du 1^er ordre.

Exemple 414 Ci-dessous, une formule modale ϕ et sa traduction $\phi(x)$ en logique du 1^er ordre.



$\phi = [B]\langle C \rangle A_s$ $\qquad$ $\phi(x) = \forall y\Big(B(x, y) \longrightarrow \exists z\big(C(y, z) \wedge A_s(z)\big)\Big).$

Exemple 415 Une formule modale et sa traduction en logique du 1^er ordre.



2. Où y est une nouvelle variable non présente dans $\psi(x)$.

La formule modale $\neg(\Diamond\Box Q \longrightarrow (\Box P \vee Q))$ est donc représentée par la formule du 1^er^ ordre

$$\neg\Big(\exists y\big(A(x,y) \wedge \forall z(A(y,z) \longrightarrow Q(z))\big) \longrightarrow \big(\forall y(A(x,y) \longrightarrow P(y)) \vee Q(x)\big)\Big).$$

Comme nous l'avons dit en introduction de ce chapitre, le but de cette traduction de la logique modale en logique du 1^er^ ordre est d'obtenir le résultat suivant :

Théorème 416 *Soit $\phi(x)$ la traduction en logique du 1^er^ ordre d'une formule de logique modale ϕ conformément à la Définition 413 et $\mathcal{M}$ la traduction en logique du 1^er^ ordre d'un modèle de Kripke de la logique modale $\mathcal{M}$ selon la Définition 411. Pour tout monde possible a de $\mathcal{M}$ on a :*

$$a \Vdash \phi \text{ si et seulement si } \mathcal{M}, a/x \models \phi(x).$$

Preuve du Théorème 416 : La preuve est immédiate par induction sur la hauteur de la formule ϕ et consiste à montrer que le même joueur possède une stratégie gagnante dans les deux jeux d'évaluations associés. $\dashv$ 416

Maintenant que nous savons que nous pouvons interpréter la logique modale dans la logique du 1^er^ ordre, la question se pose de la réciproque. Pouvons-nous interpréter la logique du 1^er^ ordre dans la logique modale. Plus simplement, est-il vrai que si nous considérons un langage du 1^er^ ordre qui ne comporte que des symboles de relation unaires $P_0, \dots, P_k$ et binaires $R_0, \dots, R_n$, nous pouvons trouver pour toute formule $\phi(x)$ et tout modèle $\mathcal{M}$ du 1^er^ordre construits sur ce langage, une formule φ tel que pour tout modèle $\mathcal{M}$ de la logique modale, dont $\mathcal{M}$ est la traduction selon la Définition 411, on ait pour tout élément a du domaine de $\mathcal{M}$:

$$a \Vdash \varphi \text{ si et seulement si } \mathcal{M}, a/x \models \phi(x)\,?$$

La réponse est en fait négative. Cela montre que la logique modale a un pouvoir expressif moindre que celui de la logique du 1^er^ ordre. Mieux encore, les formules de la logique du 1^er^ ordre, qui sont susceptibles d'être traduites en logique modale, peuvent être caractérisées précisément selon un résultat fameux de van Benthem [BvBW06]. Afin de présenter ce résultat, il nous faut nous attarder quelques instants sur la notion de formule du 1^er^ ordre *invariante par bisimulation* (cf. II.**5**.8).

Définition 417 *Soit un langage du 1^er^ ordre qui ne comporte que des symboles de relation unaires $P_0, \dots, P_k$ et binaires $R_0, \dots, R_n$ (et aucun symbole de fonction ni de constante) et $\phi(x)$ une formule sur ce langage. On dit que $\phi(x)$ est* invariante par bisimulation *si pour tous modèles du 1^er^ ordre $\mathcal{M}, \mathcal{N}$ sur ce langage formant la traduction en logique 1^er^ ordre des modèles de la logique modale $\mathcal{M}, \mathcal{N}$ et pour tous mondes possibles $a \in \mathcal{M}$ et $b \in \mathcal{N}$,*

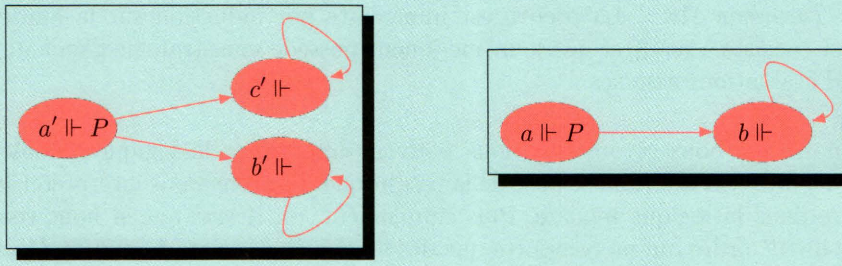
$$\text{si } \mathbf{D}_{up} \text{ possède une stratégie gagnante dans } \mathbb{B}\mathrm{is}\left((\mathcal{M},a),(\mathcal{N},b)\right), \text{ alors}$$

$$\mathcal{M}, a/x \models \phi(x) \text{ si et seulement si } \mathcal{N}, b/x \models \phi(x).$$

Une chose est claire : toute formule $\phi(x)$ qui est la traduction d'une formule de la logique modale ϕ est *invariante par bisimulation.* En effet, dire que le joueur $\mathbf{D}_{up}$ possède une stratégie gagnante dans le jeu $\mathbb{Bis}((\mathcal{M}, a), (\mathcal{N}, b))$ revient à dire que la théorie locale du modèle $\mathcal{M}$ au monde a est celle du modèle $\mathcal{N}$ au monde b sont identiques – ce qui se note $(\mathcal{M}, a) \equiv (\mathcal{N}, b)$. Or, si la formule ϕ est vraie au monde a, elle fait partie de la théorie locale de $\mathcal{M}$ au monde a et donc de la théorie locale de $\mathcal{N}$ au monde b – puisque $(\mathcal{M}, a) \equiv (\mathcal{N}, b)$ est vérifié – donc elle est vraie au monde b. Inversement et pour les mêmes raisons, si ϕ est vraie au monde b, elle est également vraie au monde a.

Par contre, comme montré dans l'Exemple 418, il existe des formules de la logique du 1er ordre qui ne sont pas *invariante par bisimulation.* Cela montre la stricte supériorité en matière de pouvoir expressif de la logique du 1er ordre sur la logique modale.

Exemple 418 Dans le jeu de bisimulation $\mathbb{Bis}((\mathcal{M}, a'), (\mathcal{N}, a))$



Le modèle $\mathcal{M}$ *Le modèle* $\mathcal{N}$.

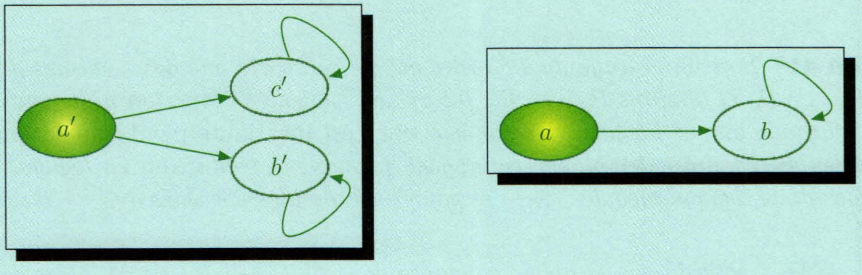
$\mathbf{D}_{up}$ possède une stratégie gagnante qui consiste :

(1) si $\mathbf{C}_{or}$ choisit b', ou c', à choisir b ;

(2) si $\mathbf{C}_{or}$ choisit b, à choisir indifféremment b' ou c' ;

De la sorte, pour chacun des coups suivants, le seul choix réel est celui de $\mathbf{C}_{or}$ de choisir de jouer dans $\mathcal{M}$ ou $\mathcal{N}$ puisque les déplacements des joueurs sont maintenant restreints aux seules deux boucles possibles à l'intérieur de $\mathcal{M}$ et de $\mathcal{N}$.

Il s'en suit que la partie se déroule de manièreinfinie et donc $\mathbf{D}_{up}$ l'emporte.



Le modèle $\mathcal{M}$ *Le modèle* $\mathcal{N}$.

Formellement, les modèles $\mathcal{M}$ et $\mathcal{N}$ sont définis par :
$\mathcal{M} = \langle M, A^{\mathcal{M}}, P^{\mathcal{M}} \rangle$ où $M = \{a', b', c'\}$ et

- $A^{\mathcal{M}} = \{(a', b'); (a', c'); (b', b'); (c', c')\}$
- $P^{\mathcal{M}} = \{a'\}$.

$\mathcal{N} = \langle N, A^{\mathcal{N}}, P^{\mathcal{N}} \rangle$ où $N = \{a, b\}$ et

- $A^{\mathcal{N}} = \{(a, b); (b, b)\}$
- $P^{\mathcal{N}} = \{a\}$.

On remarque alors :

$$\mathcal{M}, a'/x \models \exists y \exists z \Big((A(x,y) \wedge A(x,z)) \wedge \neg A(y,z) \Big)$$

$$\mathcal{N}, a/x \not\models \exists y \exists z \Big((A(x,y) \wedge A(x,z)) \wedge \neg A(y,z) \Big).$$

La formule $\exists y \exists z \Big((A(x,y) \wedge A(x,z)) \wedge \neg A(y,z) \Big)$ n'est donc pas *invariante par bisimulation.*

Théorème 419 (van Benthem) *Soit $\phi(x)$ une formule du 1er ordre ne contenant que x comme variable libre et dont les seuls termes sont réduits aux variables et ne comportent que des symboles de relation d'arité au plus 2.*

Les énoncés suivants sont équivalents :

(1) $\phi(x)$ est équivalente à la traduction en logique du 1er ordre d'une formule modale φ.

(2) $\phi(x)$ est invariante par bisimulation.

Preuve du Théorème 419 : Le sens (1) $\Longrightarrow$(2) de la preuve est facile et indiqué plus haut. Par contre le sens (2) $\Longrightarrow$(1) est plus difficile et nous renvoyons le lecteur vers [BvBW06, vB10]. $\dashv$ 419

Pour aller plus avant :

Si l'on y songe, le plongement de la logique modale dans la logique du 1er ordre est relativement évident. Cela est contraire au résultat de Johann van Benthem caractérisant à équivalence près les formules du 1er ordre qui dérivent de cette traduction de la logique modale. Nous renvoyons le lecteur qui désire en savoir plus au très ardu *"Handbook of modal logic"* de Patrick Blackburn, Johan van Benthem et Frank Wolter [BvBW06], ainsi qu'au plus abordable *"Modal Logic for Open Minds"* de Johan van Benthem [vB10]. Pour le lecteur qui se demanderait comment lier logique modale et logique du 1er ordre, nous recommandons *"First-order modal logic"* de Melvin Fitting et Richard L. Mendelsohn [FM98].

Chapitre 13

Théorie de la démonstration

Nous convenons d'omettre les parenthèses extérieures dans les formules. Ainsi, nous écrivons $\phi \wedge \psi$ à la place de $(\phi \wedge \psi)$, ou bien $\exists x\ \phi \longrightarrow (\phi \vee \neg\psi)$ au lieu de $(\exists x\ \phi \longrightarrow (\phi \vee \neg\psi))$.

Dans ce chapitre, nous développons la notion de preuve pour la logique du 1er ordre. Bien que cette logique soit beaucoup plus riche que le Calcul Propositionnel, les différents systèmes de démonstration qu'elle génère sont étrangement proches de ceux du Calcul Propositionnel. En fait, à la seule différence du traitement de la quantification, ils sont identiques.

Un système de démonstration pour la logique du 1er ordre doit permettre, comme c'était le cas pour le Calcul Propositionnel, d'aboutir à un théorème de complétude. Pour le dire autrement, un système de démonstration permet d'établir la *vérité syntaxique*, c'est-à-dire, étant donnée une théorie, de déduire par un jeu de réécriture les formules conséquences de cette théorie. En effet, à la notion de *conséquence logique sémantique* s'ajoute celle de *conséquence logique syntaxique*. Nous disons que la formule ϕ est une conséquence syntaxique de la théorie $\mathcal{T}$ si elle se déduit de $\mathcal{T}$ au moyen de règles d'un système de démonstration. On écrira $\mathcal{T} \vdash \phi$ lorsque la formule ϕ pourra être déduite de la théorie $\mathcal{T}$. Cette notion de *vérité syntaxique* ne fait pas intervenir les modèles. Pourtant, il est essentiel que les notions de *vérité syntaxique* et de *vérité sémantique* coïncident. Ce qui signifie que si la formule ϕ se déduit de la théorie $\mathcal{T}$ par des procédés syntaxiques, elle doit également être une conséquence logique sémantique de la théorie $\mathcal{T}$. Ce qui peut être déduit d'une théorie doit être vrai dans tous les modèles de cette théorie. Autrement dit, un système de démonstration doit vérifier le fait que $\mathcal{T} \vdash \phi$ implique $\mathcal{T} \models \phi$. Mais la réciproque est tout aussi nécessaire. Il est également important que $\mathcal{T} \models \phi$ entraîne $\mathcal{T} \vdash \phi$.

Cela signifie que le but d'un système de démonstration est d'obtenir le résultat suivant, appelé théorème de complétude, qui fait coïncider vérité syntaxique et vérité sémantique.

$$\mathcal{T} \models \phi \text{ si et seulement si } \mathcal{T} \vdash \phi.$$

Les différents systèmes de démonstration

Tout comme pour le Calcul Propositionnel , il existe trois grandes familles de systèmes de démonstration :

(1) les systèmes axiomatiques,

(2) la Déduction Naturelle,

(3) le Calcul des Séquents.

Les systèmes axiomatiques remontent au mathématicien allemand David Hilbert, tandis que la Déduction Naturelle et le Calcul des Séquents sont dûs à Gerhard Gentzen.

1 Les systèmes axiomatiques

***Résumé* № 60**

- *Les systèmes axiomatiques possèdent l'avantage de la concision, mais sont très éloignés de la pratique de la démonstration.*
- *Une démonstration de la formule ϕ à partir d'un ensemble d'hypothèses Γ est une suite $\langle \varphi_0, \varphi_1, \ldots, \varphi_n \rangle$, telle que $\varphi_n = \varphi$ et chaque φ_i vérifie l'une des trois conditions suivantes :*

(1) φ_i *est l'un des axiomes :*

- *Calcul Propositionnel :*

(a) $\theta \longrightarrow (\psi \longrightarrow \theta)$

(b) $(\theta \longrightarrow (\psi \longrightarrow \theta)) \longrightarrow ((\theta \longrightarrow \psi) \longrightarrow (\theta \longrightarrow \theta))$

(c) $(\neg\psi \longrightarrow \neg\phi) \longrightarrow ((\neg\psi \longrightarrow \phi) \longrightarrow \psi)$.

- *Quantification :*

(d) $\forall x\ \theta \longrightarrow \theta_{[t/x]}$

(e) $\forall x\ (\theta \longrightarrow \psi) \longrightarrow (\theta \longrightarrow \forall x\ \psi)$ [a].

- *Egalité :*

(f) $x = x$

(g) $x = y \longrightarrow (\phi[x/z] \longrightarrow \phi[y/z])$.

(2) φ_i *est une hypothèse* $(\varphi_i \in \Gamma)$ *;*

(3) φ_i *est obtenu à partir de l'application de la règle du* modus ponens *à deux formules d'indices inférieurs* φ_j *et* φ_k $(j, k < i)$.

※

a. Lorsque θ ne contient pas d'occurrence libre de la variable x.

Ces systèmes axiomatiques ont l'avantage de fournir une formalisation à la fois très simple de la notion de démonstration, mais aussi totalement inopérante quant à l'explication de ce qu'est une démonstration.

Afin de simplifier, nous allons nous contenter des formules écrites en utilisant comme connecteurs uniquement l'implication et la négation ("$\longrightarrow$" et "$\neg$") et comme quantificateur, le seul quantificateur universel ("$\forall$"). Il est clair que toute formule est équivalente à une formule de ce type.

Axiomes

- *Calcul Propositionnel :*

(1) $\theta \longrightarrow (\psi \longrightarrow \theta)$

(2) $(\theta \longrightarrow (\psi \longrightarrow \theta)) \longrightarrow ((\theta \longrightarrow \psi) \longrightarrow (\theta \longrightarrow \theta))$

(3) $(\neg\psi \longrightarrow \neg\phi) \longrightarrow ((\neg\psi \longrightarrow \phi) \longrightarrow \psi)$

- *Quantification :*

  (4) $\forall x\ \theta \longrightarrow \theta_{[t/x]}$

  (5) $\forall x\ (\theta \longrightarrow \psi) \longrightarrow (\theta \longrightarrow \forall x\ \psi)$ [1]
- *Egalité :*

  (6) $x = x$

  (7) $x = y \longrightarrow (\phi[x/z] \longrightarrow \phi[y/z])$.

Règle *Le seul* modus ponens *: de ϕ et $\phi \longrightarrow \psi$, on déduit ψ.*

Définition 420 *Une déduction de la formule φ à partir d'un ensemble de formules Γ, est une suite finie de formules $\langle \varphi_0, \varphi_1, \ldots, \varphi_n \rangle$ telle que :*

- *chaque φ_i vérifie l'une des trois conditions suivantes :*
  - *φ_i est un axiome,*
  - *φ_i est une hypothèse ($\varphi_i \in \Gamma$),*
  - *φ_i est obtenu à partir de l'application de la règle du* modus ponens *à deux formules d'indices inférieurs φ_j et φ_k ($j, k < i$).*
- *$\varphi_n = \varphi$.*

Exemple 421 Prenons comme ensemble d'hypothèses :

$$\Gamma = \{\forall x\ (P(x) \longrightarrow P(f_s(x))),\ P(y)\}.$$

Une démonstration de la formule $P(f_s(f_s(y)))$ dans ce système prend la forme suivante :

(1) $\forall x\ (P(x) \longrightarrow P(f_s(x))) \longrightarrow (P(y) \longrightarrow P(f_s(y)))$	(*axiome* (4))
(2) $\forall x\ (P(x) \longrightarrow P(f_s(x)))$	(*hypothèse*)
(3) $P(y) \longrightarrow P(f_s(y))$	(*modus ponens* 1-2)
(4) $P(y)$	(*hypothèse*)
(5) $P(f_s(y))$	(*modus ponens* 3-4)
(6) $\forall x\ (P(x) \longrightarrow P(f_s(x))) \longrightarrow (P(y) \longrightarrow P(f_s(y)))$	(*axiome* (4))
(7) $P(f_s(y)) \longrightarrow P(f_s(f_s(y)))$	(*modus ponens* 6-2)
(8) $P(f_s(f_s(y)))$	(*modus ponens* 7-5)

Remarque 422 Les systèmes axiomatiques ont les défauts de leurs qualités. Ils fournissent une notion de démonstration d'une étonnante simplicité, pour autant elle n'est en général pas du tout naturelle. La raison de cette simplicité réside dans le fait qu'une démonstration n'utilise toujours que les hypothèses d'origine. Il n'y a pas d'autre hypothèse de la déduction que les hypothèses précisées comme telles au commencement de la déduction. Il n'y a pas, au cours de la déduction, de nouvelles hypothèses qui sont introduites. Ou pour le dire autrement, les hypothèses d'une sous-déduction ne sont que les hypothèses de la déduction.

1. Lorsque θ ne contient pas d'occurrence libre de la variable x.

Pour aller plus avant :

Le lecteur que nos propos sur les systèmes “à la Hilbert” n'aurait pas éconduit pourra consulter avec profit le livre original de 1928 de Hilbert et Ackermann intitulé *“Grundzüge der Theoretischen Logik”* [HA28] ou encore sa traduction anglaise de 1950 : *“Principles of mathematical logic”* [HAL50]. Il pourra également retrouver ces systèmes dans *“Introduction to mathematical logic”* d'Elliot Mendelson [Men97], ainsi que *“Basic proof theory”* de Anne S. Troelstra et Helmut Schwichtenberg [TS00]. Le lecteur curieux sera également certainement intéressé par les considérations sur les systèmes “à la Hilbert” que tient Jean-Yves Girard dans *“Le point aveugle, tome 1 : vers la perfection”* [Gir06].

2 La Déduction Naturelle

Résumé № 61 *La Déduction Naturelle pour la logique du 1^er^ ordre est une simple extension de la Déduction Naturelle pour le Calcul Propositionnel au moyen des règles suivantes :*

$$\frac{\Gamma \vdash \phi_{[y/x]}{}^{a}}{\Gamma \vdash \forall x\ \phi}\ \forall i \qquad \frac{\Gamma \vdash \forall x\ \phi}{\Gamma \vdash \phi_{[t/x]}{}^{b}}\ \forall e$$

$$\frac{\Gamma \vdash \phi_{[t/x]}{}^{b}}{\Gamma \vdash \exists x\ \phi}\ \exists i \qquad \frac{\Gamma \vdash \exists x\ \phi \qquad \Gamma', \phi_{[y/x]} \vdash \psi^{\ c}}{\Gamma, \Gamma' \vdash \psi}\ \exists e$$

$$\frac{}{\vdash t = t^{\ b}}\ =i \qquad \frac{\Gamma \vdash \phi_{[t/x]} \qquad \Gamma' \vdash t = u}{\Gamma, \Gamma' \vdash \phi_{[u/x]}}\ =e$$

※

a. y sans occ. libre dans Γ, ϕ.
b. t un terme.
c. y sans occ. libre dans Γ', ϕ, ψ.

La méthode de Déduction Naturelle dans le cadre de la logique du 1^er^ ordre est très proche de celle élaborée pour le Calcul Propositionnel. Elle est bien sûr basée sur la notion de séquent. Nous y retrouvons dès lors les mêmes définitions de séquent (avec les hypothèses à gauche du symbole "$\vdash$", et la conclusion à sa droite), ainsi que de séquent prouvable ou démontrable.

Les règles de démonstration de la Déduction Naturelle pour la logique du 1^er^ ordre sont similaires à celles du Calcul Propositionnel, nous pourrions dire qu'elles sont pratiquement les mêmes. En effet, les règles pour la logique du 1^er^ ordre ne sont pas autre chose que les règles pour le Calcul Propositionnel, auxquelles sont rajoutées les règles chargées de gérer la quantification. Nous rappelons que ces règles constituent les briques de base permettant de construire les déductions. Une déduction formelle n'est pas autre chose qu'un assemblage fini de telles règles, assemblage généralement représenté sous forme d'un arbre.
Nous rappelons que chaque règle est composée :

- d'un ensemble de *prémisses* (il peut y en avoir 0,1,2, ou 3), chacune des prémisses étant un séquent.
- d'un séquent *conclusion* de la règle.
- d'une barre horizontale séparant les prémisses (en haut) de la conclusion (en bas). Et sur la droite de la barre, le nom de la règle est indiqué en abrégé.

Nous rappelons également qu'une règle peut se lire de deux manières :

- de haut en bas : si les prémisses sont prouvées alors la conclusion est également prouvée.
- de bas en haut : pour prouver la conclusion, il suffit de chercher à prouver les prémisses.

A chaque connecteur logique, ainsi qu'à chaque quantificateur correspondent deux types de règles.

(1) les règles d'*introduction* qui permettent de prouver une formule dont ce connecteur est l'opérateur principal.

(2) les règles d'*élimination* qui permettent d'utiliser dans les prémisses une formule ayant ce connecteur comme opérateur principal.

Nous oublions la double implication qui s'exprime par ailleurs très simplement à l'aide de l'implication et de la conjonction : la formule $\phi \longleftrightarrow \psi$ correspondant à $(\phi \longrightarrow \psi) \wedge (\psi \longrightarrow \phi)$.

Les règles

Nous retrouvons les mêmes règles que pour le Calcul Propositionnel, auxquelles s'ajoutent une règle d'introduction et une règle d'élimination pour chacun des deux quantificateurs.

Axiome

$$\frac{}{\phi \vdash \phi}\ {\scriptstyle ax}$$

C'est le point de départ de toute démonstration : si l'on prend la conclusion comme hypothèse, alors on obtient une preuve immédiate de la conclusion. Autrement dit, un séquent dans lequel la conclusion est également l'hypothèse est prouvable.

Introduction de la conjonction

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\ {\scriptstyle \wedge i}$$

Si l'on a montré ϕ sur la base de certaines hypothèses et, par ailleurs, ψ sur la base d'autres hypothèses, alors toutes ces hypothèses mises ensembles nous permettent de montrer $\phi \wedge \psi$.

Elimination de la conjonction

$$\frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ {\scriptstyle \wedge e_g} \qquad\qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ {\scriptstyle \wedge e_d}$$

Ces deux règles, qui disent que de $\phi \wedge \psi$ on peut déduire, d'une part ϕ et d'autre part ψ, sont intuitivement évidentes puisqu'une conjonction de deux formules est un énoncé "plus fort" que chacune des formules prises séparément.

Introduction de l'implication

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\ {\scriptstyle \to i}$$

Tout le sens de l'implication apparaît ici : pour prouver $\phi \longrightarrow \psi$, il suffit de prendre ϕ comme hypothèse et de prouver ψ. Ce qui est sous-tendu derrière l'usage même de l'implication est la notion de conséquence logique et donc de conclusion sur la base d'hypothèse. Ici se dévoile le fait que $\phi \longrightarrow \psi$ n'est réellement importante que lorsque la formule ϕ est attestée, et dans ce cas cette formule ne dit pas autre chose que la formule ψ est conséquence de ϕ.

Elimination de l'implication (*modus ponens*)

$$\frac{\Gamma \vdash \phi \rightarrow \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi} \rightarrow_e$$

Si l'on a prouvé ϕ, et, par ailleurs, $\phi \longrightarrow \psi$ alors on a prouvé ψ. Ce qui peut se dire encore : si l'on a montré $\phi \longrightarrow \psi$ qui est une formule disant que ψ est vérifié sous la condition ϕ, et que l'on a par ailleurs montré ϕ, alors l'hypothèse étant avérée, la condition en découle.

Introduction de la négation

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi} \neg_i$$

Si l'on obtient une contradiction en considérant à la fois Γ et ϕ, alors nous avons une preuve de la négation de ϕ sur la base des hypothèses Γ.

Elimination de la négation

$$\frac{\Gamma \vdash \neg\phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \bot} \neg_e$$

Si certaines hypothèses nous ont permis de montrer ϕ et d'autres $\neg\phi$, alors toutes ces hypothèses mises ensemble nous permettent d'obtenir une contradiction.

Introduction de la disjonction

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi} \vee i_g \qquad\qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi} \vee i_d$$

Prouver ϕ c'est prouver ϕ ou autre chose.

Elimination de la disjonction

$$\frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta} \vee e$$

La manière dont on utilise une preuve de la disjonction $\phi \vee \psi$ consiste à démontrer une formule θ avec ϕ comme hypothèse d'une part, puis encore cette même formule θ avec cette fois ψ comme hypothèse d'autre part. Comme on a montré que l'on a ou bien ϕ ou bien ψ, on a ainsi montré θ.

Introduction du quantificateur universel

$$\frac{\Gamma \vdash \phi_{[y/x]}\ ^{*}}{\Gamma \vdash \forall x\ \phi}\ {\scriptstyle \forall i}$$

*. y sans occurrence libre dans Γ, ϕ.

C'est une manière de dire que l'on s'intéresse aux occurrences libres de la variable x dans ϕ et que l'on ne souhaite faire aucune hypothèse particulière sur cette variable x. Elle peut apparaître dans Γ, mais si elle y apparait, alors c'est qu'elle y est liée. Tout se passe donc comme si cette variable n'apparaissait pas dans les hypothèses, puisqu'une variable liée peut tout à fait être renommée sans changer en rien la signification de la formule considérée.

Par conséquent, cette règle dit que si l'on a prouvé ϕ sans hypothèse particulière sur x, alors on a prouvé ϕ pour tout x, donc on a prouvé $\forall x\ \phi$.

Elimination du quantificateur universel

$$\frac{\Gamma \vdash \forall x\ \phi}{\Gamma \vdash \phi_{[t/x]}\ ^{\dagger}}\ {\scriptstyle \forall e}$$

†. t : un terme.

Si l'on a montré $\forall x\ \phi$, alors on a montré que ϕ valait lorsqu'on substituait n'importe quel terme aux occurrences libres de x. Intuitivement, les termes désignent les objets au sujet desquels parlent les formules. Si l'on a montré $\forall x\ \phi$, on a montré que la formule ϕ, en tant qu'elle parle de l'objet x, valait pour toute valeur que pouvait prendre cet objet x, donc en particulier, lorsque x prend la valeur t.

Introduction du quantificateur existentiel

$$\frac{\Gamma \vdash \phi_{[t/x]}\ ^{\dagger}}{\Gamma \vdash \exists x\ \phi}\ {\scriptstyle \exists i}$$

†. t : un terme.

Si l'on a montré que ϕ vaut pour un certain terme t (ce que l'on écrit $\phi_{[t/x]}$), alors on a montré qu'il existe un objet qui satisfait $\phi_{[x/x]}$, par conséquent $\exists x\ \phi$.

Elimination du quantificateur existentiel

$$\frac{\Gamma \vdash \exists x\ \phi \qquad \Gamma', \phi_{[y/x]} \vdash \psi\ ^{\ddagger}}{\Gamma, \Gamma' \vdash \psi}\ {\scriptstyle \exists e}$$

‡. y sans occurrence libre dans Γ', ϕ, ψ.

Lorsqu'on a pu prouver $\exists x\ \phi$, on peut utiliser cette conclusion comme hypothèse en donnant un nom à cet x qui satisfait ϕ. Mais donner un nom à cet objet x signifie qu'il n'a aucune raison d'apparaître dans la démonstration par ailleurs. Cet objet x n'a aucune raison d'être l'un des autres objets apparaissant dans la démonstration, raison pour laquelle la condition x n'a pas d'occurrence libre dans Γ', ψ est réclamée.

Intoduction de l'égalité

$$\frac{}{\vdash t = t\ ^{\dagger}}\ {\scriptstyle =i}$$

†. t : un terme.

$t = t$ est une formule démontrable sans hypothèse. Cette règle signifie que la relation d'égalité est réflexive.

Elimination de l'égalité

$$\frac{\Gamma \vdash \phi_{[t/x]} \qquad \Gamma' \vdash t = u}{\Gamma, \Gamma' \vdash \phi_{[u/x]}}\ {\scriptstyle =e}$$

Lorsque, d'une part, on a prouvé $\phi(t)$, et d'autre part $t = u$, alors on a prouvé $\phi(u)$.

Affaiblissement

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle aff}$$

Si je peux prouver ψ avec les hypothèses Γ, alors je peux encore prouver ψ si je prends des hypothèses supplémentaires (parfaitement inutiles par ailleurs).

Contraction

$$\frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle ctr}$$

La contraction est implicite dans la définition même du séquent. En effet, si à la droite du symbole $\vdash$ se trouve une seule formule, à gauche, par contre, nous avons un *ensemble* de formules. Nous savons qu'un ensemble n'est rien d'autre que la collection de ses éléments. Or Γ, ϕ, ϕ désigne l'ensemble qui contient toutes les formules de Γ et ϕ. Le fait d'écrire deux fois ϕ au lieu d'une ne change rien à l'affaire. Cela vient du fait que l'ensemble $\{\phi, \phi\}$ et l'ensemble $\{\phi\}$ ne sont qu'un seul et même ensemble.

Le système de règles que nous obtenons jusqu'ici constitue la *logique minimale*. De manière identique à ce que nous avons vu dans le cadre du Calcul Propositionnel, nous avons également deux règles additionnelles : l'*absurdité intuitionniste* et l'*absurdité classique* qui permettent d'obtenir les systèmes déductifs plus expressifs que sont respectivement la *logique intuitionniste* et la *logique classique*.

Absurdité intuitionniste

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\ {\scriptstyle \bot e}$$

Cette règle peut être vue comme une règle d'*élimination de la contradiction*. Elle dit qu'on peut démontrer n'importe quoi à partir d'hypothèses menant à une contradiction. Ou plutôt, d'une contradiction, on peut déduire absolument n'importe quoi.

Absurdité classique

$$\frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\ {\scriptstyle \bot c}$$

L'absurdité classique correspond à la notion de raisonnement par l'absurde tel qu'il est utilisé, en particulier en mathématiques. Pour démontrer une assertion, je la suppose fausse et montre que je débouche alors sur une contradiction.

Déduction Naturelle

Axiome

$$\frac{}{\phi \vdash \phi}\ ax$$

Règles logiques

$$\frac{\Gamma \vdash \phi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \phi \wedge \psi}\ \wedge i \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \phi}\ \wedge eg \qquad \frac{\Gamma \vdash \phi \wedge \psi}{\Gamma \vdash \psi}\ \wedge ed$$

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash \phi \vee \psi}\ \vee ig \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \phi \vee \psi}\ \vee id \qquad \frac{\Gamma \vdash \psi \vee \phi \qquad \Gamma', \psi \vdash \theta \qquad \Gamma'', \phi \vdash \theta}{\Gamma, \Gamma', \Gamma'' \vdash \theta}\ \vee e$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\ \to i \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\ \to e$$

$$\frac{\Gamma, \phi \vdash \bot}{\Gamma \vdash \neg\phi}\ \neg i \qquad \frac{\Gamma \vdash \neg\phi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \bot}\ \neg e$$

$$\frac{\Gamma \vdash \phi_{[y/x]}\ ^{*}}{\Gamma \vdash \forall x\ \phi}\ \forall i \qquad \frac{\Gamma \vdash \forall x\ \phi}{\Gamma \vdash \phi_{[t/x]}\ ^{\dagger}}\ \forall e$$

$$\frac{\Gamma \vdash \phi_{[t/x]}\ ^{\dagger}}{\Gamma \vdash \exists x\ \phi}\ \exists i \qquad \frac{\Gamma \vdash \exists x\ \phi \qquad \Gamma', \phi_{[y/x]} \vdash \psi\ ^{\ddagger}}{\Gamma, \Gamma' \vdash \psi}\ \exists e$$

$$\frac{}{\vdash t = t\ ^{\dagger}}\ = i \qquad \frac{\Gamma \vdash \phi_{[t/x]} \qquad \Gamma' \vdash t = u}{\Gamma, \Gamma' \vdash \phi_{[u/x]}}\ = e$$

Règles structurelles

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ aff \qquad \frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ ctr$$

Règles de l'absurdité intuitionniste et classique

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \phi}\ \bot e \qquad \frac{\Gamma, \neg\phi \vdash \bot}{\Gamma \vdash \phi}\ \bot c$$

$*$. y sans occurrence libre dans Γ, ϕ.
$\dagger$. t un terme.
$\ddagger$. y sans occurrence libre dans Γ', ϕ, ψ.

Définition 423 *Une déduction – également appelée preuve – dans le système de la Déduction Naturelle, est un arbre fini dont les nœuds sont des séquents $(S_i)_{i\leq k}$, et tel que :*

Pour chaque nœud S_i de la déduction,

- *S_i est une feuille si et seulement si S_i est un axiome,*
- *si S_i n'est pas une feuille, alors l'arbre, dont S_i est la racine et les fils/filles de S_i sont les feuilles, est une instance de l'une des règles présentée dans le tableau de la page 463.*

Nous dirons qu'une déduction s'effectue dans le cadre de :

- *la **logique minimale** si aucune des deux règles de l'absurdité n'est employée ;*
- *la **logique intuitionniste** si la règle de l'absurde intuitionniste est employée, mais non celle de l'absurde classique ;*
- *la **logique classique** lorsque la règle de l'absurde classique est utilisée.*

Une formule ϕ est déductible des hypothèses Γ s'il existe une déduction dont la racine soit le séquent $\Delta \vdash \phi$ pour un ensemble d'hypothèses $\Delta \subseteq \Gamma$.

On notera :

- *$\Gamma \vdash_m \phi$, le fait que cette déduction s'effectue dans le cadre de la logique minimale,*
- *$\Gamma \vdash_i \phi$ lorsque cette déduction s'effectue dans le cadre de la logique intuitionniste,*
- *$\Gamma \vdash_c \phi$ lorsque cette déduction est du ressort de la logique classique.*

Remarque 424 Les conditions du type "y sans occurrence libre dans Γ, ϕ" que ce soit pour la règle de l'élimination du quantificateur existentiel ou pour celle de l'introduction du quantificateur universel est absolument primordiale. Sans le respect de celle-ci, on pourrait très bien construire la démonstration *fausse* suivante de la formule $\exists x\ \phi \rightarrow \forall x\ \phi$:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x\ \phi \vdash \exists x\ \phi}\,ax \qquad \dfrac{}{\phi_{[y/x]} \vdash \phi_{[y/x]}}\,ax}{\exists x\ \phi \vdash \phi_{[y/x]}}\,\exists e \text{ erroné}}{\exists x\ \phi \vdash \forall x\ \phi}\,\forall i}{\vdash \exists x\ \phi \rightarrow \forall x\ \phi}\,\forall i$$

Exemple 425 Une preuve de $\neg\exists x\ \phi \longrightarrow \forall x\ \neg\phi$ en logique minimale :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\exists x\ \phi \vdash \neg\exists x\ \phi}\,ax \qquad \dfrac{\dfrac{}{\phi_{[y/x]} \vdash \phi_{[y/x]}}\,ax}{\phi_{[y/x]} \vdash \exists x\ \phi}\,\exists i}{\neg\exists x\ \phi,\ \phi_{[y/x]} \vdash \bot}\,\neg e}{\neg\exists x\ \phi \vdash \neg\phi_{[y/x]}}\,\neg i}{\neg\exists x\ \phi \vdash \forall x\ \neg\phi}\,\forall i}{\vdash \neg\exists x\ \phi \rightarrow \forall x\ \neg\phi}\,\rightarrow i$$

Exemple 426 Une preuve en logique minimale de la formule de l'exercice précédent dans laquelle l'implication est inversée : $\forall x\ \neg\phi \longrightarrow \neg\exists x\ \phi$

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x\ \phi \vdash \exists x\ \phi}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{\dfrac{}{\forall x\ \neg\phi \vdash \forall x\ \neg\phi}\,{\scriptstyle ax}}{\forall x\ \neg\phi \vdash \neg\phi_{[y/x]}}\,{\scriptstyle \forall e} \qquad \dfrac{}{\phi_{[y/x]} \vdash \phi_{[y/x]}}\,{\scriptstyle ax}}{\forall x\ \neg\phi, \phi_{[y/x]} \vdash \bot}\,{\scriptstyle \neg e}}{\forall x\ \neg\phi, \exists x\ \phi \vdash \bot}\,{\scriptstyle \exists e}}{\forall x\ \neg\phi \vdash \neg\exists x\ \phi}\,{\scriptstyle \to i}}{\vdash \forall x\ \neg\phi \to \neg\exists x\ \phi}\,{\scriptstyle \to i}
$$

Définition 427 *Deux formules ϕ et ψ sont dites équivalentes pour la logique minimale (respectivement la logique intuitionniste ; la logique classique) si on a à la fois $\phi \vdash_m \psi$ et $\psi \vdash_m \phi$ (respectivement $\phi \vdash_i \psi$ et $\psi \vdash_i \phi$; $\phi \vdash_c \psi$ et $\psi \vdash_c \phi$).*

On notera ces relations d'équivalence respectivement $\phi \equiv_m \psi$, $\phi \equiv_i \psi$ et $\phi \equiv_c \psi$.

Remarque 428 Il est très facile de voir qu'il n'y a de démonstration de $\phi \vdash_m \psi$ que si et seulement s'il en existe une du séquent $\vdash_m \phi \longrightarrow \psi$.

Par conséquent, les deux conditions réunies $\phi \vdash_m \psi$ et $\psi \vdash_m \phi$ sont équivalentes à la seule condition $\vdash_m \phi \longleftrightarrow \psi$. Il ressort que deux formules ϕ et ψ sont équivalentes dans une logique donnée, si et seulement si la formule qui témoigne de leur équivalence ($\phi \longleftrightarrow \psi$) peut être démontrée dans cette logique.

Considérons maintenant les règles du système axiomatique que nous avons présentées dans la définition 1, au début de ce chapitre. Ce système axiomatique reposait sur six règles appelées axiomes, auxquels s'ajoutait simplement la règle du *modus ponens*. Il est immédiat que le *modus ponens* fait partie des règles de la Déduction Naturelle, puisqu'il s'agit ni plus ni moins de la règle d'élimination de l'implication.

Quant aux axiomes, les trois premiers ne sont pas différents de ceux du système axiomatique pour le Calcul Propositionnel que nous avions présenté en leurs temps, et pour chacun desquels une démonstration en Déduction Naturelle a été exhibée :

(1) $\theta \longrightarrow (\psi \longrightarrow \theta)$ (voir exemple 121)

(2) $(\theta \longrightarrow (\psi \longrightarrow \theta)) \longrightarrow ((\theta \longrightarrow \psi) \longrightarrow (\theta \longrightarrow \theta))$ (voir exemple 120)

(3) $(\neg\psi \longrightarrow \neg\phi) \longrightarrow ((\neg\psi \longrightarrow \phi) \longrightarrow \psi)$ (si x n'a pas d'occurrence libre dans ϕ) (voir exemple 135).

Or, ces preuves que nous avons effectuées dans le cadre de la Déduction Naturelle du Calcul Propositionnel sont toujours valables ici puisque les règles de la Déduction Naturelle du Calcul Propositionnel font parties intégrantes de celles de la Déduction Naturelle de la logique du 1$^{\text{er}}$ ordre. Il nous reste donc simplement à considérer les quatre derniers axiomes :

(4) $\forall x\ \phi \longrightarrow \phi_{[t/x]}$

(5) $\forall x\ (\theta \longrightarrow \psi) \longrightarrow (\theta \longrightarrow \forall x\ \psi)$ [2]

(6) $x = x$

(7) $x = y \longrightarrow (\phi[x/z] \longrightarrow \phi[y/z])$.

2. Lorsque θ ne contient pas d'occurrence libre de la variable x.

Preuve de l'axiome (4) :

$$\dfrac{\dfrac{\dfrac{}{\forall x\ \phi \vdash \forall x\ \phi}\,{\scriptstyle ax}}{\forall x\ \phi \vdash \phi_{[t/x]}}\,{\scriptstyle \forall e}}{\vdash \forall x\ \phi \to \phi_{[t/x]}}\,{\scriptstyle \to i}$$

Preuve de l'axiome (5) :

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\forall x\ (\phi \to \psi) \vdash \forall x\ (\phi \to \psi)}\,{\scriptstyle ax}}{\forall x\ (\phi \longrightarrow \psi) \vdash \phi_{[y/x]} \to \psi_{[y/x]}}\,{\scriptstyle \forall e} \qquad \dfrac{}{\theta \vdash \theta_{[y/x]}}\,{\scriptstyle ax}}{\forall x\ (\theta \to \psi), \theta \vdash \psi_{[y/x]}}\,{\scriptstyle \to e}}{\forall x\ (\theta \to \psi), \theta \vdash \forall x\ \psi}\,{\scriptstyle \forall i}}{\forall x\ (\theta \to \psi) \vdash \theta \to \forall x\ \psi}\,{\scriptstyle \to i}}{\vdash \forall x\ (\theta \to \psi) \to (\theta \to \forall x\ \psi)}\,{\scriptstyle \to i}$$

(Noter que l'on a $\theta = \theta_{[y/x]}$ puisque θ ne contient pas d'occurrence libre de la variable x.)

Preuve de l'axiome (6) :

$$\dfrac{}{\vdash x = x}\,{\scriptstyle = i}$$

Preuve de l'axiome (7) :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\theta[x/z] \vdash \theta[x/z]}\,{\scriptstyle ax} \qquad \dfrac{}{x = y \vdash x = y}\,{\scriptstyle ax}}{x = y, \theta[x/z] \vdash \theta[y/z]}\,{\scriptstyle = e}}{x = y \vdash \theta[x/z] \longrightarrow \theta[y/z]}\,{\scriptstyle \to i}}{\vdash x = y \longrightarrow (\theta[x/z] \longrightarrow \theta[y/z])}\,{\scriptstyle \to i}$$

Nous venons donc de montrer qu'à chaque démonstration obtenue par le système axiomatique présenté au début de ce chapitre correspond une démonstration en Déduction Naturelle.

2.1 Logique classique et logique intuitionniste

Tout comme dans le cadre du Calcul Propositionnel, si l'on adjoint la règle de l'absurdité intuitionniste à la logique minimale, on obtient les règles de déduction de la Déduction Naturelle en logique intuitionniste. La substitution de la règle de l'absurdité classique à celle de l'absurdité intuitionniste procure finalement l'ensemble des règles de la Déduction Naturelle en logique classique.

Il n'y a donc aucune surprise dans le fait que tous les résultats relatifs à ces trois logiques, que sont la *logique minimale*, la *logique intuitionniste* et la *logique classique*, se retrouvent intégralement dans le cadre de la logique du 1er ordre. Il est en particulier immédiat que nous avons les inclusions strictes suivantes :

$$\textit{logique minimale} \subsetneq \textit{logique intuitionniste} \subsetneq \textit{logique classique}.$$

En effet, toutes les preuves que nous avions dans le cadre du Calcul Propositionnel peuvent être reproduites intégralement pour la logique du 1er ordre.

Nous retrouvons donc, sans surprise, les résultats décrivant ces différentes logiques au moyen de règles dérivées :

Remarque 429 Il y a différentes manières d'obtenir la logique classique, que ce soit à partir de la logique minimale ou de la logique intuitionniste. Ci-dessous quatre présentations équivalentes :

$$\begin{array}{llll}
\textit{log. cl.} = & \textit{log. int.} + & \dfrac{}{\vdash \phi \vee \neg\phi}\,{\scriptstyle ax} & (\textit{principe du tiers exclu}) \\[2ex]
= & \textit{log. int.} + & \dfrac{}{\neg\phi \longrightarrow \phi \vdash \phi}\,{\scriptstyle ax} & (\textit{loi de Peirce}) \\[2ex]
= & \textit{log. min.} + & \dfrac{}{\neg\neg\phi \vdash \phi}\,{\scriptstyle ax} & (\textit{élimination des doubles négations}) \\[2ex]
= & \textit{log. min.} + & \dfrac{}{\neg\psi \longrightarrow \neg\phi \vdash \phi \longrightarrow \psi}\,{\scriptstyle ax} & (\textit{contraposition}).
\end{array}$$

Exemple 430 Une preuve en logique minimale de la formule $\exists x\ \neg\phi \longrightarrow \neg\forall x\ \phi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\exists x\ \neg\phi \vdash \exists x\ \neg\phi}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{\dfrac{}{\forall x\ \phi \vdash \forall x\ \phi}\,{\scriptstyle ax}}{\forall x\ \phi \vdash \phi_{[y/x]}}\,{\scriptstyle \forall e} \qquad \dfrac{}{\neg\phi_{[y/x]} \vdash \neg\phi_{[y/x]}}\,{\scriptstyle ax}}{\forall x\ \phi, \neg\phi_{[y/x]} \vdash \bot}\,{\scriptstyle \neg e}}{\exists x\ \neg\phi, \forall x\ \phi \vdash \bot}\,{\scriptstyle \exists e}}{\exists x\ \neg\phi \vdash \neg\forall x\ \phi}\,{\scriptstyle \neg i}}{\vdash \exists x\ \neg\phi \to \neg\forall x\ \phi}\,{\scriptstyle \to i}$$

Si nous considérons maintenant l'implication inverse de cette formule, nous pouvons en donner une preuve certes, mais pas dans le cadre de la logique minimale ni même dans celui de la logique intuitionniste. Pour montrer $\neg\forall x\ \phi \longrightarrow \exists x\ \neg\phi$, il nous faut avoir recours à la logique classique.

Exemple 431 Une preuve en logique classique de la formule $\neg\forall x\ \phi \longrightarrow \exists x\ \neg\phi$. Nous verrons plus loin qu'il n'existe pas de preuve de cette formule en logique intuitionniste.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\forall x\ \phi \vdash \neg\forall x\ \phi}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\neg\exists x\ \neg\phi \vdash \neg\exists x\ \neg\phi}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{}{\neg\phi_{[y/x]} \vdash \neg\phi_{[y/x]}}\,{\scriptstyle ax}}{\neg\phi_{[y/x]} \vdash \exists x\ \neg\phi}\,{\scriptstyle \exists i}}{\neg\exists x\ \neg\phi, \neg\phi_{[y/x]} \vdash \bot}\,{\scriptstyle \neg e}}{\neg\exists x\ \neg\phi \vdash \phi_{[y/x]}}\,{\scriptstyle \bot c}}{\neg\exists x\ \neg\phi \vdash \forall x\ \phi}\,{\scriptstyle \forall i}}{\neg\exists x\ \neg\phi, \neg\forall x\ \phi \vdash \bot}\,{\scriptstyle \forall i}}{\neg\forall x\ \phi \vdash \exists x\ \neg\phi}\,{\scriptstyle \bot c}}{\vdash \neg\forall x\ \phi \to \exists x\ \neg\phi}\,{\scriptstyle \to i}$$

Pour aller plus avant :

Nous renvoyons aux commentaires sur la Déduction Naturelle que nous avons fait dans le cadre du Calcul Propositionnel à la page 216. Ils sont d'autant plus d'actualité qu'avec la logique du 1er ordre, nous nous trouvons précisément dans le cadre formel qui a vu naître les systèmes de Hilbert, de la Déduction Naturelle et de la logique intuitionniste. Outre les ouvrages mentionnés, page 216, nous recommandons tout particulièrement le manuel de cours de René David, Karim Nour et Christophe Raffalli, intitulé *"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* [DNR04].

Le lecteur séduit par ce domaine d'étude trouvera matière à aiguiser sa curiosité dans les ouvrages *"Natural Deduction : A Proof-Theoretical Study"* de Dag Prawitz [Pra06] et *"Le point aveugle, tome 1 : vers la perfection"* de Jean-Yves Girard [Gir06]. Nous recommandons également tout particulièrement *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00], *"Proof Theory"* de Gaisi Takeuti [Tak13], *"Proofs and types"* de Jean-Yves Girard, Paul Taylor et Yves Lafont [GTL89], ainsi que le *"Handbook of proof theory"* de Samuel R. Buss [Bus98].

Le lecteur intéressé par l'intuitionnisme trouvera une mine d'informations dans *"Elements of intuitionism"* de Michael Dummett [Dum00].

3 Le Calcul des Séquents

Résumé № 62 *La Déduction Naturelle pour la logique du 1^er^ ordre est une simple extension de la Déduction Naturelle pour le Calcul Propositionnel au moyen des règles suivantes :*

$$\frac{\Gamma, \phi_{[t/x]} \vdash \Delta^{\ a}}{\Gamma, \forall x\ \phi \vdash \Delta}\ \forall_g \qquad\qquad \frac{\Gamma \vdash \phi_{[y/x]}, \Delta}{\Gamma \vdash \forall x\ \phi, \Delta^{\ b}}\ \forall_d$$

$$\frac{\Gamma, \phi_{[y/x]} \vdash \Delta}{\Gamma, \exists x\ \phi \vdash \Delta^{\ b}}\ \exists_g \qquad\qquad \frac{\Gamma \vdash \phi_{[t/x]}, \Delta^{\ a}}{\Gamma \vdash \exists x\ \phi, \Delta}\ \exists_d$$

※

a. t un terme.
b. y sans occ. libre dans le séquent conclusion de la règle.

Le Calcul des Séquents de la logique du 1er ordre est également très proche de celui que nous avions défini dans le cadre du Calcul Propositionnel . Tout comme la Déduction Naturelle, les règles de ce système de déduction ne sont pas autre chose que celles développées dans le cadre du Calcul Propositionnel, auxquelles s'ajoutent deux couples de règles, traitant les cas des deux quantificateurs. On trouve ainsi une règle d'introduction à droite et une règle d'introduction à gauche pour le quantificateur universel et pour le quantificateur existentiel.

Nous rappelons qu'un séquent de la forme $\Gamma \vdash \Delta$ où $\Gamma = \{\phi_0, \ldots, \phi_n\}$ et $\Delta = \{\psi_0, \ldots, \psi_k\}$ est interprété intuitivement comme la formule :

$$(\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n) \longrightarrow (\psi_0 \vee \psi_1 \vee \ldots \vee \psi_k).$$

La partie gauche est donc une conjonction d'hypothèses, alors que la partie droite doit être vue comme une disjonction de conclusions. En particulier, la conjonction vide d'hypothèse est interprétée comme le vrai, alors que la disjonction vide de conclusion est interprétée comme le faux.

Les règles du Calcul des Séquents spécifiques à la logique du 1er ordre

- La règle d'introduction gauche du quantificateur universel :

$$\frac{\Gamma, \phi_{[t/x]} \vdash \Delta^{\ *}}{\Gamma, \forall x\ \phi \vdash \Delta}\ \forall_g$$

Cette règle dit que si l'on peut prouver la disjonction symbolisée par Δ, à partir des hypothèses Γ et surtout de $\phi_{[t/x]}$, alors on peut prouver la même chose en prenant $\forall x\ \phi$ à la place de $\phi_{[t/x]}$. Ce qui semble effectivement un affaiblissement, puisque l'hypothèse $\forall x\ \phi$ est beaucoup plus forte que $\phi_{[t/x]}$.

$*$. t un terme.

- La règle d'introduction droite du quantificateur universel :

$$\frac{\Gamma \vdash \phi_{[y/x]}, \Delta}{\Gamma \vdash \forall x\ \phi, \Delta^{\dagger}}\ \forall_d$$

Ici, la restriction sur le caractère libre de y dans $\Gamma, \forall x\ \phi$ et Δ est capital. Avec cette condition, cette règle permet de remplacer la conclusion $\phi_{[y/x]}$, dans laquelle y se comporte en quelque sorte comme un électron libre par $\forall x\ \phi$. L'idée derrière cette règle est que puisque y est absolument quelconque, il représente n'importe quel élément.

- La règle d'introduction gauche du quantificateur existentiel :

Cette règle dit que si l'on peut prouver la disjonction Δ, à l'aide des hypothèses Γ et surtout de $\phi_{[y/x]}$ où y n'est libre ni dans Δ, ni dans Γ, ni dans $\exists x\ \phi$, alors on peut prouver la même chose en prenant $\exists x\ \phi$ en lieu et place de $\phi_{[y/x]}$. L'idée derrière cela est que cet y tient lieu d'une valeur indépendante de Γ ou de Δ. Il fonctionne donc comme le témoin d'un élément satisfaisant $\phi(x)$.

$$\frac{\Gamma, \phi_{[y/x]} \vdash \Delta}{\Gamma, \exists x\ \phi \vdash \Delta^{\dagger}}\ \exists_g$$

- La règle d'introduction droite du quantificateur existentiel :

Cette règle est très naturelle, le témoin t est simplement remplacé par une variable sous la dépendance d'un quantificateur existentiel. On remplace le fait que le terme t vérifie $\phi(x)$, par le fait qu'il existe un élément satisfaisant $\phi(x)$.

$$\frac{\Gamma \vdash \phi_{[t/x]}, \Delta^{*}}{\Gamma \vdash \exists x\ \phi, \Delta}\ \exists_d$$

Exemple 432 Une preuve (en logique minimale) de la formule $\exists x\ \neg\phi \longrightarrow \neg\forall x\ \phi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\phi_{[y/x]} \vdash \phi_{[y/x]}}\ ax}{\neg\phi_{[y/x]}, \phi_{[y/x]} \vdash}\ \neg_g}{\neg\phi_{[y/x]}, \forall x\ \phi \vdash}\ \forall_g}{\exists x\ \neg\phi, \forall x\ \phi \vdash}\ \exists_g}{\exists x\ \neg\phi \vdash \neg\forall x\ \phi}\ \neg_d}{\vdash \exists x\ \neg\phi \to \neg\forall x\ \phi}\ \to_d$$

†. y sans occurrence libre dans le séquent conclusion de la règle (dans $\Gamma, \exists x\ \phi$ ou $\forall x\ \phi$, et Δ).
∗. t un terme.

Calcul des Séquents

Axiomes

$$\frac{}{\phi \vdash \phi}\ ax \qquad\qquad \frac{}{\bot \vdash}\ \bot_g$$

Règles logiques

$$\frac{\Gamma, \phi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta}\ \wedge_{g1} \qquad \frac{\Gamma, \psi \vdash \Delta}{\Gamma, \phi \wedge \psi \vdash \Delta}\ \wedge_{g2} \qquad \frac{\Gamma \vdash \phi, \Delta \qquad \Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \wedge \psi, \Delta}\ \wedge_d$$

$$\frac{\Gamma, \phi \vdash \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \vee \psi \vdash \Delta}\ \vee_g \qquad \frac{\Gamma \vdash \phi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta}\ \vee_{d1} \qquad \frac{\Gamma \vdash \psi, \Delta}{\Gamma \vdash \phi \vee \psi, \Delta}\ \vee_{d2}$$

$$\frac{\Gamma \vdash \phi, \Delta \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \phi \to \psi \vdash \Delta}\ \to_g \qquad \frac{\Gamma, \phi \vdash \psi, \Delta}{\Gamma \vdash \phi \to \psi, \Delta}\ \to_d$$

$$\frac{\Gamma \vdash \phi, \Delta}{\Gamma, \neg\phi \vdash \Delta}\ \neg_g \qquad \frac{\Gamma, \phi \vdash \Delta}{\Gamma \vdash \neg\phi, \Delta}\ \neg_d$$

$$\frac{\Gamma, \phi_{[t/x]} \vdash \Delta\ ^*}{\Gamma, \forall x\ \phi \vdash \Delta}\ \forall_g \qquad \frac{\Gamma \vdash \phi_{[y/x]}, \Delta}{\Gamma \vdash \forall x\ \phi, \Delta\ ^\dagger}\ \forall_d$$

$$\frac{\Gamma, \phi_{[y/x]} \vdash \Delta}{\Gamma, \exists x\ \phi \vdash \Delta\ ^\dagger}\ \exists_g \qquad \frac{\Gamma \vdash \phi_{[t/x]}, \Delta\ ^*}{\Gamma \vdash \exists x\ \phi, \Delta}\ \exists_d$$

Règles structurelles

$$\frac{\Gamma \vdash \Delta}{\Gamma, \phi \vdash \Delta}\ aff_g \qquad \frac{\Gamma \vdash \Delta}{\Gamma \vdash \phi, \Delta}\ aff_d$$

$$\frac{\Gamma, \phi, \phi \vdash \Delta}{\Gamma, \phi \vdash \Delta}\ ctr_g \qquad \frac{\Gamma \vdash \phi, \phi, \Delta}{\Gamma \vdash \phi, \Delta}\ ctr_d$$

Règle de coupure

$$\frac{\Gamma \vdash \phi, \Delta \qquad \Gamma', \phi \vdash \Delta'}{\Gamma, \Gamma' \vdash \Delta, \Delta'}\ cut$$

∗. t un terme

†. y sans occurrence libre dans le séquent conclusion de la règle (dans $\Gamma, \exists x\ \phi$ ou $\forall x\ \phi$, et Δ)

Remarquons que dans la preuve que nous venons de décrire, chacun des séquents ne possède tout au plus qu'une seule formule à droite du symbole $\vdash$, et qu'aucune règle d'affaiblissement n'est utilisée. Nous considérons maintenant l'implication inverse de cette formule, nous en donnons une preuve dans laquelle l'un des séquents possède deux formules à droite du symbole $\vdash$.

Exemple 433 Une preuve en logique classique de la formule $\neg\forall x\ \phi \longrightarrow \exists x\ \neg\phi$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\phi_{[y/x]} \vdash \phi_{[y/x]}}\ {\scriptstyle ax}}{\vdash \phi_{[y/x]}, \neg\phi_{[y/x]}}\ {\scriptstyle \neg_d}}{\vdash \phi_{[y/x]}, \exists x\ \neg\phi}\ {\scriptstyle \exists_d}}{\vdash \forall x\ \phi, \exists x\ \neg\phi}\ {\scriptstyle \forall_d}}{\neg\forall x\ \phi \vdash \exists x\ \neg\phi}\ {\scriptstyle \neg_g}}{\vdash \neg\forall x\ \phi \rightarrow \exists x\ \neg\phi}\ {\scriptstyle \rightarrow_d}$$

Nous retrouvons, dans le cadre de la logique du 1er ordre, les mêmes résultats majeurs que ceux obtenus dans celui du Calcul Propositionnel.

3.1 Logique intuitionniste et logique minimale

Le Calcul des Séquents tel qu'il est présenté ici correspond point pour point à la logique classique. Cela signifie que le séquent $\Gamma \vdash \Delta$ où $\Gamma = \{\phi_0, \ldots, \phi_n\}$ et $\Delta = \{\psi_0, \ldots, \psi_k\}$ est prouvable en Calcul des Séquents si et seulement si le séquent :

$$\vdash (\phi_0 \wedge \phi_1 \wedge \ldots \wedge \phi_n) \longrightarrow (\psi_0 \vee \psi_1 \vee \ldots \vee \psi_k)$$

est prouvable dans le système de la Déduction Naturelle dotée de la règle de l'absurde classique. Pour autant, la logique minimale et la logique intuitionniste trouvent une représentation très simple en Calcul des Séquents :

Théorème 434 *La logique intuitionniste est la version du Calcul des Séquents dont les règles sont restreintes aux séquents avec au plus une formule à droite, la contraction à droite étant considérée comme implicite.*

Théorème 435 *La logique minimale est la version du Calcul des Séquents privée de l'affaiblissement droit et dont les règles sont restreintes aux séquents avec au plus une formule à droite.*

3.2 L'élimination des coupures

Nous avons vu que la règle de coupure en Calcul des Séquents était une règle essentielle pour rendre compte de la manière dont nous raisonnons. Car, souvent, les raisonnements que nous tenons utilisent, comme hypothèses, les conclusions de raisonnements antérieurs. Et ces hypothèses disparaissent en tant que telles puisqu'elles ont été démontrées par ailleurs. Nous retrouvons le fameux théorème d'élimination des coupures.

Théorème 436 (Elimination des coupures) *S'il existe, en Calcul des Séquents classique (resp. intuitionniste), une preuve du séquent $\Gamma \vdash \Delta$, alors il existe une preuve en Calcul des Séquents classique (resp. intuitionniste) de ce séquent sans utilisation de la règle de coupure.*

Par conséquent, nous retrouvons également les corollaires suivants :

Corollaire 437 *Le séquent " $\vdash$ " n'est pas prouvable en logique classique.*

Nous rappelons que le séquent "$\vdash$" se comprend comme "du vrai on prouve le faux", ou "le faux est une conséquence du vrai". Si $\vdash$ était prouvable en Calcul des Séquents, il s'en suivrait que tout séquent $\Gamma \vdash \Delta$ le serait également par la simple utilisation des règles d'affaiblissement. Tout et n'importe quoi pourrait être démontré, rendant dès lors ce système de démonstration caduque.

Preuve du Corollaire 437 : S'il existait une preuve de $\vdash$ en Calcul des Séquents, il en existerait également une qui se ferait sans utilisation de la règle de coupure. Or, toutes les autres règles introduisent une formule soit à droite, soit à gauche. $\dashv$ 437

Corollaire 438 (Propriété de la sous-formule) *Si $\Gamma \vdash \Delta$ est prouvable en logique classique (resp. en logique intuitionniste), alors il en existe une preuve en logique classique (resp. en logique intuitionniste) dans laquelle n'apparaissent que des séquents constitués de sous-formules des formules de Γ et de Δ.*

Preuve du Corollaire 438 : Toute preuve sans coupure de $\Gamma \vdash \Delta$ satisfait les conditions souhaitées.

$\dashv$ 438

Nous avions vu, dans le cadre du Calcul Propositionnel, qu'une conséquence de la propriété de la sous-formule, en logique intuitionniste, était qu'une preuve d'une disjonction passait nécessairement par une preuve d'un des termes de la disjonction :

$$\vdash_i \phi \vee \psi \quad \text{si et seulement si} \quad \Big(\vdash_i \phi \text{ ou } \vdash_i \psi \Big).$$

Ceci reste bien évidemment vrai dans le cadre de la logique du 1$^{\text{er}}$ ordre, mais également le fait qu'une preuve en logique intuitionniste d'une formule existentielle repose sur une preuve de cette formule pour un terme donné :

$$\vdash_i \exists x\ \phi \quad \text{si et seulement si il existe un terme } t \text{ tel que} \quad \vdash_i \phi_{[t/x]}.$$

Le caractère constructif de la logique intuitionniste apparaît ainsi clairement. On ne prouve l'existence d'un élément vérifiant une certaine propriété – décrite par la formule ϕ – que si l'on a prouvé cette propriété pour un élément bien cararctérisé. La preuve est constructive en ce sens qu'elle n'affirme pas l'existence en toute généralité sans avoir au préalable présenté un tel élément, sans l'avoir au préalable construit de toutes pièces.

Pour aller plus avant :

Nous recommandons à nouveau l'ouvrage intitulé *"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* de René David, Karim Nour et Christophe Raffalli [DNR04], ainsi que les plus difficiles *"Le point aveugle, tome 1 : vers la perfection"* de Jean-Yves Girard [Gir06] et *"Proofs and types"* du même auteur associé à Yves Lafont et traduit par Paul Taylor [GTL89]. Parmi les grands classiques sur le sujet, on trouve *"Proof Theory"* de Gaisi Takeuti [Tak13], *"Basic proof theory"* de Anne S. Troelstra et Helmut Schwichtenberg [TS00], ainsi que le *"Handbook of proof theory"* de Samuel R. Buss [Bus98].

---

4 Le théorème de complétude de la logique du 1er ordre

Résumé № 63
Pour tout ensemble de formules closes Γ et toute formule ϕ :

$$\Gamma \vdash_c \phi \iff \Gamma \models \phi.$$

※

Dans le cadre de la logique du 1er ordre, la prouvabilité (c'est-à-dire conséquence syntaxique) et la conséquence sémantique coïncident. C'est d'ailleurs cette correspondance, dont témoigne le théorème de complétude, qui est essentielle pour caractériser la bonne conformité du système de démonstration dans lequel nous travaillons. En effet, tout l'intérêt d'un système déductif est de pouvoir prouver précisément les conséquences sémantiques. Sans adéquation entre ces deux notions de vérité – la vérité syntaxique de la prouvabilité et la vérité sémantique de la satisfaction universelle dans les modèles – la notion même de système démonstratif perd toute sa valeur. Le but du théorème de complétude est de montrer que les règles de la Déduction Naturelle (dans sa version complète, celle de la logique classique), ou celles du Calcul des Séquents n'ont pas été définies au hasard, mais afin de rendre compte de la notion de vérité sémantique.

Il exprime que, d'une part, la classe de toutes les formules démontrables sans utiliser d'hypothèse et, d'autre part, celle de toutes les formules universellement valides ne forment qu'une seule et même classe.

Théorème 439 (Gödel-Kolmogorov) *Soient Γ, un ensemble fini de formules, ϕ une formule de la logique du 1er ordre,*

$$\Gamma \models \phi \quad ssi \quad \Gamma \vdash_c \phi.$$

Corollaire 440 *Soit ϕ une formule de la logique du 1er ordre,*

$$\models \phi \quad ssi \quad \vdash_c \phi.$$

Preuve du Corollaire 440 : C'est une conséquence immédiate du Théorème 439 en prenant comme ensemble d'hypothèses Γ, l'ensemble vide. ⊣ 440

Définition 441 *On dit qu'une théorie de la logique du 1er ordre $\mathcal{T}$ est* non-contradictoire *si*

$$\mathcal{T} \nvdash_c \bot.$$

Cela revient à dire qu'elle ne prouve pas quelque chose et son contraire. Bien évidemment, une théorie qui n'est pas non-contradictoire est dite *contradictoire.*

Corollaire 442 *Soit $\mathcal{T}$ une théorie de la logique du 1er ordre,*

$$\mathcal{T} \not\models \bot \quad ssi \quad \mathcal{T} \nvdash_c \bot.$$

Autrement dit, cette théorie est non-contradictoire (c'est bien ce que $\mathcal{T} \not\models \perp$ signifie : s'il n'est pas vrai que le faux soit vérifié dans tous les modèles qui satisfont la théorie $\mathcal{T}$, cela ne peut être que parce que cette théorie admet au moins un modèle) si et seulement si elle ne permet pas de prouver le faux.

Preuve du Corollaire 442 : C'est encore une fois une conséquence on ne peut plus immédiate du Théorème 439. $\dashv$ 442

Preuve du Théorème 439 : La preuve de ce théorème est nettement plus compliquée que celle équivalente dans le cadre du Calcul Propositionnel .

La direction $\boldsymbol{\Gamma \vdash_c \phi}$ **implique** $\boldsymbol{\Gamma \models \phi}$ est facile : il s'agit tout d'abord de montrer que si l'on a une preuve en logique classique du séquent $\Gamma \vdash \phi$, alors la formule ϕ est vraie dans tous les modèles de Γ (c'est-à-dire dans tous les modèles dans lesquels toutes les formules de Γ sont vérifiées). Cela se démontre par induction sur la longueur de la dite preuve. Cette démarche est tout à fait similaire à ce que nous avons vu dans le cadre du Calcul Propositionnel. La véritable nouveauté provient des règles logiques concernant les quantificateurs.

Par contre, la direction $\boldsymbol{\Gamma \models \phi}$ **implique** $\boldsymbol{\Gamma \vdash_c \phi}$ est d'une toute autre difficulté et nous n'en présentons ici que l'idée de la preuve.

Tout d'abord, nous procédons par l'absurde. C'est-à-dire que nous montrons "$\Gamma \nvdash_c \phi$ implique $\Gamma \not\models \phi$". Remarquons tout de suite que $\Gamma \not\models \phi$ signifie qu'il est faux que ϕ soit vraie dans tout modèle de Γ, par conséquent, qu'il existe un modèle de Γ dans lequel ϕ soit fausse, ou pour le dire encore autrement, il existe un modèle de Γ dans lequel $\neg\phi$ soit vraie. Ce qui se laisse traduire par $\Gamma \cup \{\neg\phi\}$ admet un modèle, c'est-à-dire est satisfaisable.

Par ailleurs, $\Gamma \nvdash_c \phi$ signifie que $\Gamma \cup \{\neg\phi\}$ n'est pas contradictoire. En effet, si $\Gamma \cup \{\neg\phi\}$ était contradictoire, on aurait $\Gamma \cup \{\neg\phi\} \vdash_c \perp$, qui n'est rien d'autre que $\Gamma,\ \neg\phi \vdash_c \perp$ d'où par la règle de l'introduction de la négation $\Gamma \vdash_c \neg\neg\phi$, puis en utilisant l'élimination des doubles négations : $\Gamma \vdash_c \phi$, ce qui contredit $\Gamma \nvdash_c \phi$.

Par conséquent, pour montrer "$\Gamma \nvdash_c \phi$ implique $\Gamma \not\models \phi$", nous montrons :

si $\Gamma \cup \{\neg\phi\}$ n'est pas contradictoire, alors $\Gamma \cup \{\neg\phi\}$ admet un modèle.

Autrement dit, en toute généralité, pour prouver le sens difficile du théorème de complétude de la logique du 1$^{\text{er}}$ ordre, il suffit de prouver que pour toute théorie finie $\mathcal{T}$:

si $\mathcal{T}$ n'est pas contradictoire, alors $\mathcal{T}$ admet un modèle.

Toute la difficulté revient donc à partir d'une théorie non-contradictoire, de lui trouver un modèle. Or, si dans le cas du Calcul Propositionnel, un modèle est un objet simple dans lequel des valeurs de vérités sont attribuées aux variables propositionnelles, ici un modèle est un objet beaucoup plus compliqué. Par exemple, demandons-nous quels vont être les éléments du domaine de base de ce modèle ?

On aimerait voir apparaître un modèle tout ce qu'il y a de plus traditionnel. On s'attendrait à voir des éléments qui ressemblent à ceux des modèles que l'on manipule habituellement. Or, il n'en est rien, contrairement à ce qui se passe dans une écrasante majorité des modèles que l'on visite, où le domaine de base est formé d'objets très éloignés de la logique et des langages à partir desquels sont constituées ces différentes logiques, ici les éléments de base de ce modèle sont eux-mêmes des objets logiques : ce sont des termes du langage. L'astuce de cette preuve est de ne pas dissocier radicalement le domaine logique de celui des modèles, le monde du discours logique et celui de ses réalisations.

Nous avons besoin de deux définitions préalables à l'explicitation de la preuve.

Définition 443 *Une théorie $\mathcal{T}$ est dite complète si elle est non-contradictoire et pour toute formule ϕ du langage, ou bien $\phi \in \mathcal{T}$ ou bien $\neg\phi \in \mathcal{T}$.*

Par conséquent, une théorie complète est une théorie qui intuitivement ne peut être complétée par aucune formule. Aucune formule ne peut y être ajoutée sans rendre la théorie immédiatement inconsistante. Une théorie complète est en quelque sorte une théorie maximale.

Définition 444 *On dit qu'une théorie $\mathcal{T}$ admet des* témoins de Henkin *si cette théorie vérifie que pour toute formule de la forme $\exists x\ \phi$, il existe un symbole de constante* c *tel que la formule $\exists x\ \phi \longrightarrow \phi_{[c/x]}\ \in \mathcal{T}$.*

L'idée de la preuve consiste donc de partir avec une théorie finie non-contradictoire quelconque $\mathcal{T}$, puis :

(1) Montrer que cette théorie $\mathcal{T}$ peut être étendue en une théorie complète $\mathcal{T}'$ admettant des *témoins de Henkin.*

(2) Montrer ensuite que cette théorie $\mathcal{T}'$ admet un modèle, dans la construction duquel, les *témoins de Henkin* jouent un rôle primordial.

Pour cela nous avons besoin de quelques lemmes préparatoires.

Lemme 445 *Soit $(\mathcal{T}_i)_{i\in I}$ une famille de théories non-contradictoires qui est totalement ordonnée par l'inclusion. Alors $\bigcup_{i\in I}\mathcal{T}_i$ est non-contradictoire.*

Preuve du Lemme 445 : Procédons par l'absurde et supposons que $\bigcup_{i\in I}\mathcal{T}_i$ est contradictoire. Puisque $\bigcup_{i\in I}\mathcal{T}_i \vdash_c \bot$ est vérifié, il existe un ensemble fini $\{\phi_0,\dots,\phi_k\} \subseteq \bigcup_{i\in I}\mathcal{T}_i$ tel que $\phi_0,\dots,\phi_k \vdash_c \bot$. Considérons $i_0,\dots,i_k$ des éléments de I vérifiants $\phi_{i_j} \in \mathcal{T}_{i_j}$ (pour chaque $j \leq k$). Puisque $(\mathcal{T}_i)_{i\in I}$ est une famille totalement ordonnée par inclusion, il en est de même de la famille $(\mathcal{T}_{i_j})_{j\leq k}$. Il existe donc un entier $n \leq k$ tel que pour chaque $j \leq k$ on a $\mathcal{T}_{i_j} \subseteq \mathcal{T}_{i_n}$. Par conséquent, puisqu'à la fois $\phi_0,\dots,\phi_k \vdash_c \bot$ et $\{\phi_0,\dots,\phi_k\} \subseteq \bigcup_{j\in\{0,\dots,k\}}\mathcal{T}_{i_j} \subseteq \mathcal{T}_{i_n}$ sont vérifiés, il apparaît que $\mathcal{T}_{i_n} \vdash_c \bot$. Ce qui contredit le caractère non-contradictoire de chacune des théories de la famille $(\mathcal{T}_i)_{i\in I}$. $\dashv$ 445

Lemme 446 *Soit $\mathcal{T}$ une théorie sur un langage $\mathcal{L}$ qui soit non-contradictoire. Alors il existe une théorie $\mathcal{T}_c$ sur le même langage qui soit complète et telle que $\mathcal{T} \subseteq \mathcal{T}_c$.*

Preuve du Lemme 446 : On considère l'ensemble de toutes les théories non-contradictoires sur $\mathcal{L}$ qui étendent $\mathcal{T}$. Muni de l'inclusion, c'est un ordre partiel inductif. En effet, pour toute chaîne $(\mathcal{T}_i)_{i\in I}$, la théorie $\mathcal{T}_I = \bigcup_{i\in I}\mathcal{T}_i$ est non-contradictoire (voir Lemme 445) et c'est un majorant de la chaîne. On peut donc utiliser le lemme de Zorn pour obtenir l'existence d'une théorie $\mathcal{T}_c$ qui est un élément maximal de l'ordre partiel considéré. Il reste à montrer que c'est une théorie complète.
Par l'absurde, supposons qu'il existe une formule ϕ telle que $\phi \notin \mathcal{T}_c$ et $\neg\phi \notin \mathcal{T}_c$. Par maximalité de $\mathcal{T}_c$, on obtient que les théories $\mathcal{T}_c \cup \{\phi\}$ et $\mathcal{T}_c \cup \{\neg\phi\}$ ne sont pas non-contradictoires, ce qui veut dire que $\mathcal{T}_c, \phi \vdash_c \bot$ et $\mathcal{T}_c, \neg\phi \vdash_c \bot$. Par conséquent, on obtient à la fois $\mathcal{T}_c \vdash_c \neg\phi$ et $\mathcal{T}_c \vdash_c \phi$, ce qui implique immédiatement $\mathcal{T}_c \vdash_c \bot$, une contradiction.
$\dashv$ 446

Lemme 447 *Soient Γ une théorie, ϕ une formule et c un symbole de constante n'apparaissant ni dans Γ ni dans ϕ. Alors $\Gamma \vdash_c \phi_{[c/x]}$ implique que $\Gamma \vdash_c \forall x\ \phi$.*

Preuve du Lemme 447 : On montre d'abord que pour toute théorie Δ et toute formule ϕ, si $\Delta_{[c/x]} \vdash_c \phi_{[c/x]}$, alors pour tout terme t du langage, $\Delta_{[t/x]} \vdash_c \psi_{[t/x]}$. La preuve se fait par induction sur la hauteur de la démonstration en remplaçant partout c par t.
Puisque x est liée dans $\forall x\ \phi$, alors sans perte de généralité, on peut supposer que x n'a pas d'occurrence libre dans Γ (sinon, il suffit de considérer la nouvelle formule $\forall y\ \phi_{[y/x]}$ où y est une nouvelle variable). En choisissant pour terme z (une nouvelle variable) dans le résultat précédent, on obtient que, puisque $\Gamma = \Gamma_{[c/x]} \vdash_c \phi_{[c/x]}$, on a $\Gamma = \Gamma_{[z/x]} \vdash_c \phi_{[z/x]}$. Appliquant l'introduction du quantificateur universel, puisque z n'a d'occurrence libre ni dans Γ ni dans ϕ, alors $\Gamma \vdash_c \forall z\ \phi_{[z/x]}$ et donc $\Gamma \vdash_c \forall x\ \phi$.

$\dashv$ 447

Soit $\mathcal{T}$ une théorie sur un langage $\mathcal{L}$. On suppose que $\mathcal{T}$ est non-contradictoire et on cherche un modèle de $\mathcal{T}$. La démonstration se fait en deux étapes.

Première étape. On construit une théorie $\mathcal{T}_h$ sur un langage $\mathcal{L}_h$ telle que :

(1) $\mathcal{T}_h$ est un théorie complète ;

(2) pour toute formule ϕ sur $\mathcal{L}_h$ ayant x pour seule variable libre, il existe un *témoin de Henkin* c_ϕ, c'est-à-dire un symbole de constante de $\mathcal{L}_h$ tel que :

$$\mathcal{T}_h \vdash_c \exists x\ \phi \longrightarrow \phi_{[\mathsf{c}_\phi/x]}.$$

Pour cela, définissons par induction des langages $\mathcal{L}_n$ et des théories $\mathcal{T}_n$, pour tout entier n. On pose $\mathcal{L}_0 = \mathcal{L}$, $\mathcal{T}_0 = \mathcal{T}$ et

$$\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{\mathsf{c}_\phi \mid \phi \text{ est une formule avec une variable libre de } \mathcal{L}_n\},$$

$$\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{\exists x\ \phi \longrightarrow \phi_{[\mathsf{c}_\phi/x]} \mid \phi \text{ est une formule avec une variable libre } x \text{ de } \mathcal{L}_n\}.$$

On considère maintenant $\mathcal{L}_h = \bigcup_{n\in\mathbb{N}} \mathcal{L}_n$ et $\mathcal{T}_\infty = \bigcup_{n\in\mathbb{N}} \mathcal{T}_n$.

Montrons que $\mathcal{T}_\infty$ est non-contradictoire. Par le Lemme 445, il suffit de montrer que $\mathcal{T}_n$ est non-contradictoire pour tout entier n. On fait cela par induction. On a par hypothèse que $\mathcal{T}_0 = \mathcal{T}$ est non-contradictoire. Supposons par l'absurde que $\mathcal{T}_{n+1}$ n'est pas non-contradictoire avec $\mathcal{T}_0, \ldots \mathcal{T}_n$ non-contradictoires. Alors, il existe des formules $\phi_1, \ldots, \phi_k$ de $\mathcal{L}_n$ telles que :

$$\mathcal{T}_n, \bigwedge_{1\leq i\leq k} \left(\exists x\ \phi_i \longrightarrow \phi_{i[\mathsf{c}_{\phi_i}/x]}\right) \vdash_c \bot.$$

On en déduit que :

$$\mathcal{T}_n \vdash_c \bigwedge_{1\leq i\leq k} \left(\exists x\ \phi_i \longrightarrow \phi_{i[\mathsf{c}_{\phi_i}/x]}\right) \longrightarrow \bot$$

et par le Lemme 447 appliqué k fois, on peut conclure que :

$$\mathcal{T}_n \vdash_c \forall y_1 \ldots \forall y_k \left(\bigwedge_{1\leq i\leq k} \left(\exists x\ \phi_i \longrightarrow \phi_{i[y_i/x]}\right) \longrightarrow \bot \right).$$

Or, on sait (voir exercices) que si la formule ψ ne possède pas d'occurrence libre de y, alors les formules $\forall y\ (\theta \longrightarrow \psi)$ et $(\exists y\ \theta \longrightarrow \psi)$ sont syntaxiquement équivalentes :

$$\vdash_c \forall y\ (\theta \longrightarrow \psi) \longleftrightarrow (\exists y\ \theta \longrightarrow \psi).$$

Par conséquent,

$$\mathcal{T}_n \vdash_c \left(\exists y_1 \ldots \exists y_k \bigwedge_{1 \leq i \leq k} \left(\exists x\ \phi_i \longrightarrow \phi_{i[y_i/x]} \right) \right) \longrightarrow \perp.$$

Du fait que si ψ ne possède pas d'occurrence libre de y, on ait :

$$\vdash_c \exists y\ (\phi \wedge \psi) \longleftrightarrow (\exists y\ \phi \wedge \psi)$$

on obtient :

$$\mathcal{T}_n \vdash_c \left(\bigwedge_{1 \leq i \leq k} \exists y_i \left(\exists x\ \phi_i \longrightarrow \phi_{i[y_i/x]} \right) \right) \longrightarrow \perp.$$

On sait de plus que si θ n'a pas d'occurrence libre de y, alors :

$$\vdash_c \exists y\ (\theta \longrightarrow \psi) \longleftrightarrow (\theta \longrightarrow \exists y\ \psi)$$

ce qui permet d'obtenir :

$$\mathcal{T}_n \vdash_c \left(\bigwedge_{1 \leq i \leq k} \left(\exists x\ \phi_i \longrightarrow \exists y_i\ \phi_{i[y_i/x]} \right) \right) \longrightarrow \perp.$$

Or, pour tout $1 \leq i \leq k$, on a :

$$\vdash_c \exists x\ \phi_i \longrightarrow \exists y_i\ \phi_{i[y_i/x]}$$

ce qui implique :

$$\mathcal{T}_n \vdash_c \bigwedge_{1 \leq i \leq k} \left(\exists x\ \phi_i \longrightarrow \exists y_i\ \phi_{i[y_i/x]} \right).$$

Par élimination de l'implication, il vient :

$$\mathcal{T}_n \vdash_c \perp$$

ce qui contredit l'hypothèse d'induction.

On utilise maintenant le Lemme 446 pour étendre $\mathcal{T}_\infty$ en une théorie complète $\mathcal{T}_h$. Soit ϕ une formule de $\mathcal{L}_h$ avec une seule variable libre x. Il reste à vérifier que :

$$\mathcal{T}_h \vdash_c \exists x\ \phi \longrightarrow \phi_{[\mathsf{c}_\phi/x]}.$$

Par définition, ϕ est une suite qui ne contient qu'un nombre fini de symboles de $\mathcal{L}_h$. Par construction, il existe donc un entier n tel que $\phi \in \mathcal{L}_n$ et ainsi :

$$\exists x\ \phi \longrightarrow \phi_{[\mathsf{c}_\phi/x]} \in \mathcal{T}_{n+1} \subseteq \mathcal{T}_h.$$

Seconde étape. On construit maintenant un $\mathcal{L}_h$-modèle $\mathcal{M}$ de $\mathcal{T}_h$, dont la restriction à $\mathcal{L}$ constituera un modèle de $\mathcal{T}$.

On pose :

$$\mathtt{T}_{\mathrm{clos}}(\mathcal{L}_h) = \{t \in \mathcal{T}(\mathcal{L}_h) \mid t \text{ ne contient pas de variable}\}.$$

On définit le modèle $\mathcal{M}$ suivant :

(1)
$$|\mathcal{M}| = \mathtt{T}_{\mathrm{clos}}(\mathcal{L}_h)/\sim,$$
où $t \sim t'$ si et seulement si $\mathcal{T}_h \vdash_c t = t'$;

(2) pour tout symbole de constante c, $\mathsf{c}^{\mathcal{M}} = [\,\mathsf{c}\,]_\sim$;

(3) pour tout symbole de fonction f d'arité n,
$$f^{\mathcal{M}}\Big([t_1]_\sim, \ldots, [t_n]_\sim\Big) = \Big[f(t_1, \ldots, t_n)\Big]_\sim ;$$

(4) pour tout symbole de relation R d'arité n,
$$\Big([t_1]_\sim, \ldots, [t_n]_\sim\Big) \in R^{\mathcal{M}} \text{ si et seulement si } \mathcal{T}_h \vdash_c R(t_1, \ldots, t_n).$$

Vérifions que tout cela est bien défini. Soient $t_1, \ldots, t_n$ et $t'_1, \ldots, t'_n$ des termes tels que $t_i \sim t'_i$ pour tout $1 \leq i \leq n$. Alors on a $\mathcal{T}_h \vdash_c t_i = t'_i$ pour tout $1 \leq i \leq n$. L'élimination de l'égalité appliquée n fois sur le résultat de l'introduction de l'égalité avec $f(t_1, \ldots, t_n)$ nous donne que :

$$\mathcal{T}_h \vdash_c f(t_1, \ldots, t_n) = f(t'_1, \ldots, t'_n).$$

L'élimination de l'égalité appliquée n fois sur l'axiome $R(t_1, \ldots, t_n) \vdash_c R(t_1, \ldots, t_n)$ donne $\mathcal{T}_h, R(t_1, \ldots, t_n) \vdash_c R(t'_1, \ldots, t'_n)$. Par conséquent, nous obtenons :

$$\mathcal{T}_h \vdash_c R(t_1, \ldots, t_n) \longrightarrow R(t'_1, \ldots, t'_n).$$

Puis par symétrie :

$$\mathcal{T}_h \vdash_c R(t_1, \ldots, t_n) \longleftrightarrow R(t'_1, \ldots, t'_n).$$

D'où l'on obtient par *modus ponens* :

$$\mathcal{T}_h \vdash_c R(t_1, \ldots, t_n) \text{ si et seulement si } \mathcal{T}_h \vdash_c R(t'_1, \ldots, t'_n).$$

Par ailleurs $|\mathcal{M}| \neq \emptyset$ car la formule avec une variable libre $\exists x\ (x = x)$ est une formule de $\mathcal{L}_h$ et donc la classe de son témoin de Henkin est un élément de $|\mathcal{M}|$.

Il reste à vérifier que $\mathcal{M} \models_c \mathcal{T}_h$. Pour cela, on prouve que pour toute formule close ϕ, $\mathcal{T}_h \vdash_c \phi$ (c'est à dire que $\phi \in \mathcal{T}_h$) si et seulement si $\mathcal{M} \models_c \phi$. On suppose sans perte de généralité que ϕ ne comporte que le quantificateur $\exists$ et les connecteurs $\wedge, \neg$. Par induction sur la hauteur de ϕ :

(1) Si $ht(\phi) = 0$ et $\phi = \bot$, alors c'est évident puisque $\mathcal{T}_h$ est non-contradictoire.
Si $\phi = R(u_1, \ldots, u_n)$, alors puisque ϕ est une formule close, les termes $u_1, \ldots, u_n$ sont clos. Dans ce cas $\mathcal{M} \models_c \phi$ si et seulement si $({u_1}^{\mathcal{M}}, \ldots, {u_n}^{\mathcal{M}}) \in R^{\mathcal{M}}$, c'est-à-dire (par définition) si et seulement si $([u_1]_\sim, \ldots, [u_n]_\sim) \in R^{\mathcal{M}}$. Par définition, ceci est vrai si et seulement si $\mathcal{T}_h \vdash_c R(u_1, \ldots, u_n)$.

(2) Si $ht(\phi) > 0$:
- Si $\phi = \psi_1 \wedge \psi_2$, alors $\mathcal{M} \models_c \phi$ si et seulement si $\mathcal{M} \models_c \psi_1$ et $\mathcal{M} \models_c \psi_2$. Par hypothèse d'induction, ceci est équivalent à $\mathcal{T}_h \vdash_c \psi_1$ et $\mathcal{T}_h \vdash_c \psi_2$. Par les règles d'introduction et d'élimination de la conjonction, on obtient $\mathcal{M} \models_c \phi$ si et seulement si $\mathcal{T}_h \vdash_c \phi$.
- Si $\phi = \neg\psi$, alors $\mathcal{M} \models_c \phi$ si et seulement si $\mathcal{M} \not\models_c \psi$. Par hypothèse d'induction, ceci est équivalent à $\mathcal{T}_h \nvdash_c \psi$, et par complétude de $\mathcal{T}_h$, cela revient à dire que $\mathcal{T}_h \vdash_c \neg\psi$.
- Si $\phi = \exists x\ \psi$, montrons que $\mathcal{T}_h \vdash_c \phi$ entraîne $\mathcal{M} \models_c \phi$. Considérons pour cela le témoin de Henkin c_ψ. Par construction de $\mathcal{T}_h$, $\mathcal{T}_h \vdash_c \phi$ si et seulement si $\mathcal{T}_h \vdash_c \psi_{[\mathsf{c}_\psi/x]}$ et par l'hypothèse d'induction, ceci équivaut à $\mathcal{M} \models_c \psi_{[\mathsf{c}_\psi/x]}$. Par conséquent, si $\mathcal{T}_h \vdash_c \phi$, alors il existe une stratégie gagnante pour le **V**érificateur dans $\mathbb{E}v\,(\phi, \mathcal{M})$: il lui suffit de choisir ${\mathsf{c}_\psi}^{\mathcal{M}}$ comme valeur pour x. Ainsi, $\mathcal{T}_h \vdash_c \phi$ entraîne $\mathcal{M} \models_c \phi$.

  Pour montrer la réciproque, supposons que $\mathcal{M} \models_c \phi$. Par définition, il existe alors un terme clos t tel que le **V**érificateur a une stratégie gagnante dans
$$\mathbb{E}v\left(\psi_{\left[[t]_\sim/x\right]}, \mathcal{M}\right).$$
  En parallèle, jouons au jeu $\mathbb{E}v\,(\psi_{[t/x]}, \mathcal{M})$ avec cette même stratégie. Si le premier jeu se termine sur une formule atomique
$$R\left(u_1{}_{\left[[t]_\sim/x\right]}, \ldots, u_n{}_{\left[[t]_\sim/x\right]}\right),$$
  alors il s'arrête sur $R\,(u_{1[t/x]}, \ldots, u_{n[t/x]})$ dans le deuxième. Par définition de l'interprétation des termes dans le modèle $\mathcal{M}$, $t^{\mathcal{M}} = [t]_\sim$. Par conséquent, l'interprétation des termes $u_i{}_{\left[[t]_\sim/x\right]}$ et $u_{i[t/x]}$ sont les mêmes dans $\mathcal{M}$. On obtient donc que le **V**érificateur a une stratégie gagnante dans $\mathbb{E}v\,(\psi_{[t/x]}, \mathcal{M})$, c'est-à-dire que $\mathcal{M} \models_c \psi_{[t/x]}$. Par hypothèse d'induction, on obtient que $\mathcal{T}_h \vdash_c \psi_{[t/x]}$. Par la règle d'introduction du quantificateur existentiel, cela implique que $\mathcal{T}_h \vdash_c \phi$.

On a ainsi montré que la $\mathcal{L}_h$-structure $\mathcal{M}$ est un modèle de $\mathcal{T}_h$. Il suffit dès lors de considérer $\mathcal{N}$ la $\mathcal{L}$-structure induite par $\mathcal{M}$, autrement dit la restriction de $\mathcal{M}$ à $\mathcal{L}$, pour obtenir un modèle de $\mathcal{T}$: $\mathcal{N} \models \mathcal{T}$.

$\dashv$ 439

Corollaire 448 (Théorème de compacité) *Soient $\mathcal{L}$ un langage du 1er ordre et $\mathcal{T}$ une théorie de ce langage,*

$$\mathcal{T} \textit{ admet un modèle} \iff \textit{chaque théorie } \text{finie } \mathcal{T}' \subseteq \mathcal{T} \textit{ admet un modèle.}$$

Cet énoncé n'est autre que celui du Théorème de compacité (Théorème 406). Sa preuve directe n'est pas aisée, mais maintenant que nous disposons du théorème de complétude de la logique du 1er ordre, nous allons pouvoir en donner une preuve très facile.

Preuve du Corollaire 448 : Le sens ($\Longrightarrow$) est évident. Pour le sens ($\Longleftarrow$) nous allons procéder par la contraposée et prouver :

$$\mathcal{T} \textit{ n'admet pas de modèle} \Longrightarrow \textit{il existe théorie finie } \mathcal{T}' \subseteq \mathcal{T} \textit{ qui n'admet pas de modèle.}$$

Pour cela, remarquons simplement que si $\mathcal{T}$ n'a pas de modèle, alors $\mathcal{T} \models \bot$ est vérifié (c'est d'ailleurs le seul cas !). Par application du théorème de complétude, cela donne $\mathcal{T} \vdash_c \bot$ et donc il existe un ensemble (nécessairement fini !) d'hypothèses $\Delta \subseteq \mathcal{T}$ tel que $\Delta \vdash_c \bot$. Par application du thèorème de complétude à nouveau (mais cette fois-ci dans l'autre sens) on obtient $\Delta \models \bot$, ce qui montre que la théorie *finie* $\Delta \subseteq \mathcal{T}$ n'a pas de modèle.

$\dashv$ 448

5 Les modèles de Kripke de la logique du 1er ordre

Résumé № 64 *Les modèles de Kripke des logiques intuitionniste et minimale de la logique du 1er ordre sont semblables à ceux de ces logiques dans le cadre du Calcul Propositionnel . La différence est que chaque monde α se comporte comme un modèle de la logique (classique) du 1er ordre – en particulier possède un domaine “ $\mathbb{D}_\alpha$ ” tel que si $\alpha \leq \beta$ alors $\mathbb{D}_\alpha \subseteq \mathbb{D}_\beta$.*
Les modèles de la logique minimale se distinguant de ceux de la logique classique par le simple fait d'autoriser certains mondes à forcer “ $\perp$ ”.
Pour toute théorie $\mathcal{T}$ et toute formule ϕ :

$$\mathcal{T} \vdash_i \phi \iff \mathcal{T} \models_i \phi\,;$$
$$\mathcal{T} \vdash_m \phi \iff \mathcal{T} \models_m \phi.$$

※

Avec le théorème de complétude, nous venons de montrer que la notion de vérité sémantique et la notion de vérité syntaxique coïncident dans le cadre classique. Pour le dire autrement, le théorème de complétude – de la logique classique – montre que la sémantique que nous avons présentée pour la logique du 1er ordre correspond à la notion de preuve telle qu'elle apparaît en Déduction Naturelle ou en Calcul des Séquents. Lorsque nous restreignons le champ des démonstrations possibles en interdisant l'utilisation de la règle de l'absurde classique – ou de manière équivalente le principe du tiers exclu – tout en conservant la même sémantique, ce théorème ne vaut plus. Pour retrouver un théorème de complétude qui fonctionne pour la logique intuitionniste, il faut une sémantique différente, une sémantique qui soit spécifique à la logique intuitionniste : les *modèles de Kripke.*

Les modèles de Kripke pour la logique du 1er ordre diffèrent de ceux du Calcul Propositionnel, dans le même ordre d'idée que les modèles (classiques) de la logique du 1er ordre diffèrent de ceux du Calcul Propositionnel. Afin de faciliter leur présentation, nous allons procéder en deux étapes. Avant de présenter le cas général, nous présenterons tout d'abord le cas particulier des *modèles de Kripke* pour un langage *non égalitaire* $\mathcal{L}$ dépourvu à la fois de constante et de symbole de fonction.

5.1 Logique intuitionniste

Langages non égalitaires et sans symbole de fonction

Définition 449 *Soit $\mathcal{L}$ un langage du 1erordre non égalitaire et sans symbole de fonction (ni de constante). $\mathcal{K} = (|\mathcal{K}|, \leq, \mathbb{D}, \Vdash)$ est un modèle de Kripke de la logique intuitionniste sur le langage $\mathcal{L}$ si :*

(1) $(|\mathcal{K}|, \leq)$ est un ensemble (partiellement) ordonné, les éléments de $|\mathcal{K}|$ étant appelés mondes possibles.

(2) $\mathbb{D}$ est une fonction qui associe à tout élément $\alpha \in |\mathcal{K}|$ un ensemble non vide $\mathbb{D}_\alpha$, qui constitue le domaine du monde α et vérifie pour tous $\alpha, \beta \in |\mathcal{K}|$:

$$\alpha \leq \beta \longrightarrow \mathbb{D}_\alpha \subseteq \mathbb{D}_\beta.$$

(3) $\Vdash$ *est une relation binaire – appelée « forcing » – entre les éléments de* $|\mathcal{K}|$ *et les formules atomiques à paramètres dans* $\bigcup_{\alpha \in |\mathcal{K}|} \mathbb{D}_\alpha$ *vérifiant :*

pour $\alpha, \beta \in |\mathcal{K}|$ *et* $R \in \mathcal{L}$ *un symbole de relation d'arité* n. *La relation* $\Vdash$ *est telle que :*

- $\alpha \nVdash \bot$;
- *si* $\alpha \Vdash R(a_1, \dots, a_n)$ *alors* $a_1, \dots, a_n \in \mathbb{D}_\alpha$;
- *si* $\alpha \Vdash R(a_1, \dots, a_n)$ *et* $\alpha \leq \beta$, *alors* $\beta \Vdash R(a_1, \dots, a_n)$.

La relation de forcing s'étend aux formules. Pour $\alpha \in |\mathcal{K}|$ *et* ϕ, ψ *deux formules de* $\mathcal{L}$ *:*

- $\alpha \Vdash \phi \wedge \psi \iff \alpha \Vdash \phi$ *et* $\alpha \Vdash \psi$;
- $\alpha \Vdash \phi \vee \psi \iff \alpha \Vdash \phi$ *ou* $\alpha \Vdash \psi$;
- $\alpha \Vdash \phi \longrightarrow \psi \iff$ *pour tout* $\beta \in |\mathcal{K}|$ *tel que* $\alpha \leq \beta$, *si* $\beta \Vdash \phi$ *alors* $\beta \Vdash \psi$;
- $\alpha \Vdash \neg\phi \iff \alpha \Vdash \phi \longrightarrow \bot$ [3] ;
- $\alpha \Vdash \forall x\, \phi \iff$ *pour tous* $\beta \in |\mathcal{K}|$, $(\alpha \leq \beta$ *et* $b \in \mathbb{D}_\beta) \Longrightarrow \beta \Vdash \phi_{[b/x]}$;
- $\alpha \Vdash \exists x\, \phi \iff$ *il existe* $a \in \mathbb{D}_\alpha$ *tel que* $\alpha \Vdash \phi_{[a/x]}$.

Remarque 450

(1) Intuitivement, un modèle de Kripke de la logique intuitionniste du 1^er^ ordre est comme un ensemble de modèles (classiques) empilés les uns sur les autres. Si l'on représente le diagramme de Hasse [4] de l'ordre partiel $(|\mathcal{K}|, \leq)$, ces mondes retrouvent les nœuds d'un graphe. Une même formule n'a pas la même valeur de vérité dans tous ces modèles.

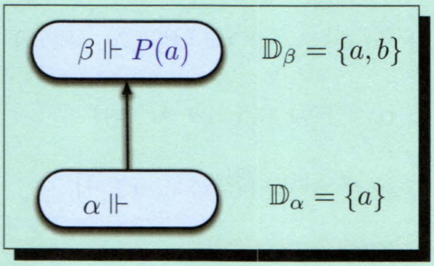
(2) Il est facile de montrer – par induction sur sa hauteur – que toute formule qui est forcée en un monde α, est également forcée au-dessus de α (en tout monde $\beta \geq \alpha$).

Exemple 451 On considère le langage $\mathcal{L}$ dont la signature ne contient que le symbole de relation unaire P.

On construit le modèle de Kripke $\mathcal{K}$ suivant. On se donne deux mondes, α et β avec $\alpha \leq \beta$, dont les domaines sont respectivement :

- $\mathbb{D}_\alpha = \{a\}$,
- $\mathbb{D}_\beta = \{a, b\}$

et la relation de forcing est définie par le seul $\beta \Vdash P(a)$.



3. Cela revient à dire que pour tous $\beta \geq \alpha$, si $\beta \Vdash \phi$ alors $\beta \Vdash \bot$. Or dans le cadre de la logique intuitionniste, aucun monde possible ne peut forcer $\bot$, cette condition est donc équivalente à dire que pour tous $\beta \geq \alpha$, $\beta \nVdash \phi$.

4. Le diagramme de Hasse consiste à représenter chaque monde par un point, avec la convention que si pour deux mondes α et β la relation $\alpha \leq \beta$ est vérifiée, alors β est situé au dessus de α. Le fait que la relation $\alpha \leq \beta$ soit vérifiée est représentée par un segment de droite entre α et β. Pour autant, on ne représente pas toutes les relations, mais uniquement leurs réductions réflexives et transitives (on ne trace pas de relation entre un monde et lui-même, ni entre deux mondes α et β qui pourtant vérifient $\alpha \leq \beta$, pour autant qu'il existe un troisième monde γ vérifiant $\alpha \leq \gamma$ et $\gamma \leq \beta$).

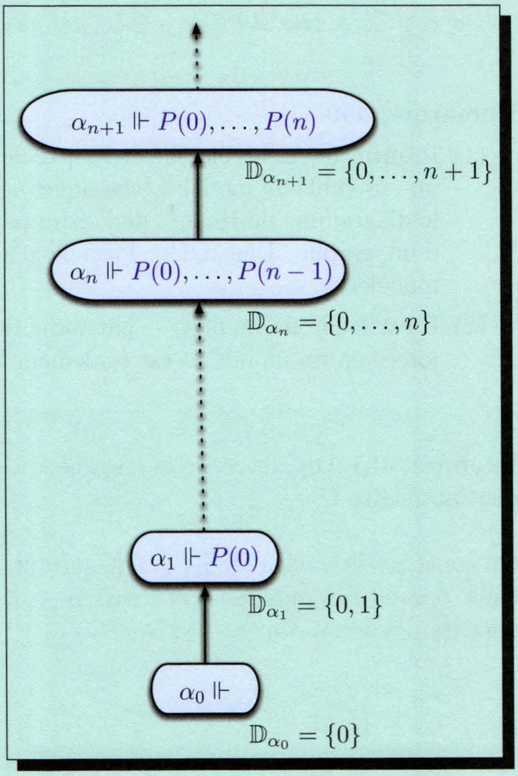
On remarque que les relations suivantes sont vérifiées :

(1) $\beta \Vdash P(a)$
(2) $\alpha \nVdash \neg P(a)$
(3) $\beta \Vdash P(a) \vee \neg P(a)$
(4) $\alpha \nVdash P(a) \vee \neg P(a)$
(5) $\alpha \nVdash \forall x\ (P(x) \vee \neg P(x))$

Exemple 452 On considère le langage $\mathcal{L}$ dont la signature ne contient que le symbole de relation unaire P, puis on construit le modèle de Kripke $\mathcal{K}$ suivant :

On se donne $\{\alpha_n \mid n \in \mathbb{N}\}$ comme ensemble de mondes possibles. Pour chaque entiers k, n on a :

- $\alpha_k \leq \alpha_n$ ssi $k \leq n$
- $\mathbb{D}_{\alpha_n} = \{0, \ldots, n\}$
- $\alpha_n \Vdash P(k)$ ssi $k < n$.



On vérifie aisément :

(1) $\forall n \in \mathbb{N}, \alpha_n \nVdash P(n)$

(2) $\forall n \in \mathbb{N}, \alpha_n \nVdash \neg P(n)$

(3) $\forall n \in \mathbb{N}, \alpha_n \nVdash P(n) \vee \neg P(n)$

(4) $\forall n \in \mathbb{N}, \alpha_n \nVdash \forall x\ \big(P(x) \vee \neg P(x)\big)$

(5) $\alpha_0 \Vdash \neg\forall x\ \big(P(x) \vee \neg P(x)\big)$

(6) $\alpha_0 \nVdash \neg\neg\forall x\ \big(P(x) \vee \neg P(x)\big)$

Nous sommes maintenant en mesure de réintroduire les constantes et symboles de fonction ainsi que l'égalité. Pour faciliter la présentation, nous adopterons la convention selon laquelle les symboles de constante ne sont autres que des symboles de fonction d'arité nulle.

Langages égalitaires avec symbole de fonction

Définition 453 (Modèle de Kripke de la logique intuitionniste) *Soit $\mathcal{L}$ un langage (égalitaire) du 1^er ordre. $\mathcal{K} = (|\mathcal{K}|, \leq, \mathbb{D}, \mathbb{E}, \mathbb{F}, \Vdash)$ est un modèle de Kripke de la logique* *intuitionniste sur le langage $\mathcal{L}$ si :*

(1) $(|\mathcal{K}|, \leq, \mathbb{D}, \Vdash)$ *est un modèle de Kripke*[5] *au sens de la définition qui précède (Définition 449).*

(2) $\mathbb{F}$ *est la donnée, pour chaque symbole de fonction f d'arité n de $\mathcal{L}$ et chaque monde $\alpha \in |\mathcal{K}|$, d'une fonction $f^\alpha : \mathbb{D}_\alpha{}^n \longrightarrow \mathbb{D}_\alpha$.*

(3) $\mathbb{E}$ *est la donnée, pour chaque monde $\alpha \in |\mathcal{K}|$, d'une relation d'équivalence*[6] $\mathbb{E}_\alpha$ *sur* $\mathbb{D}_\alpha$ *qui pour tous $\alpha, \beta \in |\mathcal{K}|$ et pour tous $a, b \in \alpha$ satisfait :*

$$\big(\alpha \leq \beta \text{ et } (a,b) \in \mathbb{E}_\alpha\big) \Longrightarrow (a,b) \in \mathbb{E}_\beta.$$

(4) $\Vdash$ *vérifie de plus, pour tout monde $\alpha \in |\mathcal{K}|$:*

Compatibilité entre $\mathbb{E}$, $\mathbb{F}$ et les symboles de relations de $\mathcal{L}$ *:*
Pour tout symbole de relation R d'arité $n > 0$ et tout symbole de fonction f d'arité $n \geq 0$:
si $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{D}_\alpha$ et $(a_i, b_i) \in \mathbb{E}_\alpha$ $(1 \leq i \leq n)$ alors

(a) $\alpha \Vdash R(a_1, \ldots, a_n) \iff \alpha \Vdash R(b_1, \ldots, b_n)$;

(b) $\big(f^\alpha(a_1, \ldots, a_n), f^\alpha(b_1, \ldots, b_n)\big) \in \mathbb{E}_\alpha$.

On ajoute maintenant quelques règles sur la réalisabilité des formules atomiques lorsqu'elles font intervenir des termes ou l'égalité.

Réalisabilité des formules atomiques
On définit la valeur d'un terme t à paramètres[7] *dans $\mathbb{D}_\alpha$ par :*

(c) si $t = a \in \mathbb{D}_\alpha$, alors $t^\alpha = a$;

(d) si $t = f(t_1, \ldots, t_n)$, alors $t^\alpha = f^\alpha(t_1{}^\alpha, \ldots, t_n{}^\alpha)$.

Puis on ajoute quelques règles sur la réalisabilité des formules atomiques lorsqu'elles font intervenir des termes ou l'égalité :

(e) pour tous termes t et u :

$$\alpha \Vdash u = v \iff (u^\alpha, v^\alpha) \in \mathbb{E}_\alpha \ ;$$

(f) pour tout symbole de relation R d'arité $n > 0$ et tous termes $t_1, \ldots, t_n$:

$$\alpha \Vdash R(t_1, \ldots, t_n) \iff \alpha \Vdash R(t_1{}^\alpha, \ldots, t_n{}^\alpha).$$

La relation de forcing $\Vdash$ s'étend des formules atomiques à toute formule de la même manière que précédemment (dans la Définition 449).

5. Modèle de Kripke d'un langage non égalitaire dépourvu de tout symbole de constante et de tout symbole de fonction.
6. Une relation d'équivalence est une relation binaire qui est à la fois réflexive, symétrique et transitive.
7. Les variables de t sont remplacées par des éléments de $\mathbb{D}_\alpha$.

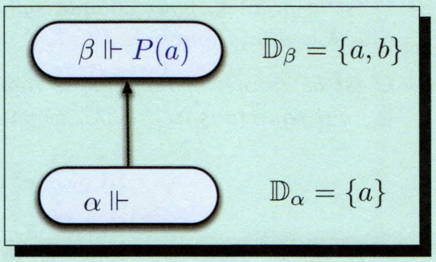
Exemple 454 Dans le modèle de Kripke de l'exemple 451, les relations suivantes sont vérifiées :

(1) $\alpha \nVdash a = b$

(2) $\alpha \nVdash \neg a = b$

(3) $\alpha \nVdash a = b \vee \neg a = b$

(4) $\alpha \nVdash \forall x\, \forall y\, (x = y \vee \neg x = y)$.



On retrouve la définition de l'évaluation d'une formule dans un modèle de Kripke que nous avons vu dans le cadre de la logique modale : cette formule devait être satisfaite en tout monde du modèle de Kripke. Il en va de même ici. Une formule de la logique du 1er ordre est satisfaite dans un modèle de Kripke si elle est satisfaite en tous ses nœuds. Les notions de satisfaction d'une théorie dans un modèle et de conséquence sémantique sont quant à elles rigoureusement les mêmes que dans le cadre du Calcul Propositionnel.

Définition 455 *(Évaluation d'une formule dans un modèle de Kripke) Soient $\mathcal{L}$ un langage de la logique du 1er ordre, $\mathcal{K}$ un modèle de Kripke de la logique intuitionniste sur $\mathcal{L}$ et ϕ une formule de $\mathcal{L}$.*

La formule ϕ est satisfaite dans le modèle $\mathcal{K}$ (noté $\mathcal{K} \models_i \phi$) si $\alpha \Vdash \phi$ est vérifié pour tout monde $\alpha \in |\mathcal{K}|$.

Définition 456 *(Évaluation d'une théorie dans un modèle de Kripke) Soient $\mathcal{L}$ un langage de la logique du 1er ordre, $\mathcal{K}$ un modèle de Kripke de la logique intuitionniste sur $\mathcal{L}$ et $\mathcal{T}$ une théorie de $\mathcal{L}$.*

Le modèle $\mathcal{K}$ satisfait $\mathcal{T}$ (noté $\mathcal{K} \models_i \mathcal{T}$), si $\mathcal{K} \models_i \phi$ est vérifié pour toute formule $\phi \in \mathcal{T}$.

Définition 457 *(Conséquence sémantique intuitionniste) Soient $\mathcal{L}$ un langage de la logique du 1er ordre, ϕ une formule de $\mathcal{L}$ et $\mathcal{T}$ une théorie de $\mathcal{L}$.*

La formule ϕ est conséquence sémantique intuitionniste de $\mathcal{T}$ (noté $\mathcal{T} \models_i \phi$) si pour tout modèle de Kripke de la logique intuitionniste $\mathcal{K}$:

$$\text{si } \mathcal{K} \models_i \mathcal{T} \text{ alors } \mathcal{K} \models_i \phi.$$

La présentation des modèles de Kripke de la logique intuitionniste trouve sa raison d'être dans le résultat qui suit.

Le théorème de complétude de la logique intuitionniste du 1er ordre

Théorème 458 *Soient $\mathcal{L}$ un langage de la logique du 1er ordre, ϕ une formule de $\mathcal{L}$ et Γ une théorie de $\mathcal{L}$.*

$$\Gamma \models_i \phi \quad \text{ssi} \quad \Gamma \vdash_i \phi.$$

Il est à noter que l'énoncé "$\Gamma \models_i \phi$ ssi $\Gamma \vdash_i \phi$" est équivalent à l'énoncé "$\Gamma \not\models_i \phi$ ssi $\Gamma \nvdash_i \phi$". En conséquence, démontrer qu'un énoncé n'est pas prouvable en logique intuitionniste revient à chercher un contre-modèle (généralement dénommé "contre-exemple").

Exemple 459 A partir des exemples 451, 452 et 454 et par application du théorème de complétude de la logique intuitionniste on obtient les relations suivantes :

(1) $\nvdash_i \forall x\ (P(x) \vee \neg P(x))$;

(2) $\nvdash_i \neg\neg\forall x\ \big(P(x) \vee \neg P(x)\big)$;

(3) $\nvdash_i \forall x\ \forall y\ (x = y \vee \neg x = y)$.

5.2 Logique minimale

La logique minimale du 1er ordre n'est qu'une simple variante de la logique intuitionniste. Elle consiste à relâcher l'exigence qu'aucun monde ne puisse forcer $\bot$.

Définition 460 *(Modèle de Kripke de la logique minimale) Les modèles de Kripke $\mathcal{K}$ de la logique minimale sont définis de façon analogue à ceux de la logique intuitionniste à la seule différence que l'on n'exige pas que pour tout monde $\alpha \in |\mathcal{K}|$, on ait $\alpha \nVdash \bot$.*

Les définitions de l'évaluation d'une formule ou l'évaluation d'une théorie ainsi que la conséquence sémantique sont identiques à leur notation près.

Définition 461 *(Évaluation d'une formule dans un modèle de Kripke de la logique minimale) Soient $\mathcal{L}$ un langage de la logique du 1er ordre, $\mathcal{K}$ un modèle de Kripke de la logique minimale sur $\mathcal{L}$ et ϕ une formule de $\mathcal{L}$.*

La formule ϕ est satisfaite dans le modèle $\mathcal{K}$ (noté $\mathcal{K} \models_m \phi$) si $\alpha \Vdash \phi$ est vérifié pour tout monde $\alpha \in |\mathcal{K}|$.

Définition 462 *(Évaluation d'une théorie dans un modèle de Kripke de la logique minimale) Soient $\mathcal{L}$ un langage de la logique du 1er ordre, $\mathcal{K}$ un modèle de Kripke de la logique minimale sur $\mathcal{L}$ et $\mathcal{T}$ une théorie de $\mathcal{L}$.*

Le modèle $\mathcal{K}$ satisfait $\mathcal{T}$ (noté $\mathcal{K} \models_m \mathcal{T}$), si $\mathcal{K} \models_m \phi$ est vérifié pour toute formule $\phi \in \mathcal{T}$.

Définition 463 *(Conséquence sémantique minimale) Soient $\mathcal{L}$ un langage de la logique du 1er ordre, ϕ une formule de $\mathcal{L}$ et $\mathcal{T}$ une théorie de $\mathcal{L}$.*

La formule ϕ est conséquence sémantique minimale de $\mathcal{T}$ (noté $\mathcal{T} \models_m \phi$) si pour tout modèle de Kripke de la logique minimale $\mathcal{K}$:

$$\textit{si } \mathcal{K} \models_m \mathcal{T} \textit{ alors } \mathcal{K} \models_m \phi.$$

Les modèles de Kripke de la logique minimale permettent d'obtenir le résultat qui suit.

Le théorème de complétude de la logique minimale du 1er ordre

Théorème 464 *Soient $\mathcal{L}$ un langage de la logique du 1er ordre, ϕ une formule de $\mathcal{L}$ et Γ une théorie de $\mathcal{L}$.*

$$\Gamma \models_m \phi \quad \textit{ssi} \quad \Gamma \vdash_m \phi.$$

L'énoncé du théorème précédent " $\Gamma \models_m \phi$ ssi $\Gamma \vdash_m \phi$" est bien évidemment équivalent à l'énoncé " $\Gamma \not\models_m \phi$ ssi $\Gamma \nvdash_m \phi$". En conséquence, prouver qu'une formule n'est pas prouvable en logique minimale revient à exhiber un modèle de la logique minimale satisfaisant les hypothèses mais pas la conclusion.

Exemple 465 On considère le langage $\mathcal{L}$ dont la signature ne contient que le symbole de relation unaire P. On construit le modèle de Kripke de la logique minimale $\mathcal{K}$ suivant.

On se donne un unique monde α dont le domaine est $\mathbb{D}_\alpha = \{a\}$ et la relation de forcing est simplement $\alpha \Vdash \bot$.

$$\boxed{\alpha \Vdash \bot \qquad \mathbb{D}_\alpha = \{a\}}$$

Les relations suivantes sont vérifiées :

(1) $\alpha \nvdash \exists x\ P(x)$

(2) $\alpha \vdash \neg\exists x\ P(x)$

(3) $\alpha \vdash \neg\neg\exists x\ P(x)$

(4) $\alpha \nvdash \neg\neg\exists x\ P(x) \longrightarrow \exists x\ P(x)$.

Par ailleurs :

(5) $\alpha \nvdash \neg\exists x\ P(x) \longrightarrow \exists x\ P(x)$

(6) $\alpha \vdash \neg\neg\exists x\ P(x) \vee \exists x\ P(x)$

(7) $\alpha \nvdash \big(\neg\neg\exists x\ P(x) \vee \exists x\ P(x)\big) \longrightarrow \big(\neg\exists x\ P(x) \longrightarrow \exists x\ P(x)\big)$.

Par application du théorème de complétude de la logique minimale, nous obtenons donc :

(8) $\nvdash_m \neg\neg\exists x\ P(x) \longrightarrow \exists x\ P(x)$

(9) $\nvdash_m \big(\neg\neg\exists x\ P(x) \vee \exists x\ P(x)\big) \longrightarrow \big(\neg\exists x\ P(x) \longrightarrow \exists x\ P(x)\big)$.

Par contre, la preuve en Calcul des Séquents ci-dessous montre que nous avons :

$$\vdash_i \big(\neg\neg\exists x\ P(x) \vee \exists x\ P(x)\big) \longrightarrow \big(\neg\exists x\ P(x) \longrightarrow \exists x\ P(x)\big)$$

ce qui démontre que la logique minimale est strictement moins expressive que la logique intuitionniste.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\neg\exists x\ P(x) \vdash \neg\exists x\ P(x)}\,{\scriptstyle ax}}{\neg\neg\exists x\ P(x), \neg\exists x\ P(x) \vdash}\,{\scriptstyle \neg_g}}{\neg\neg\exists x\ P(x), \neg\exists x\ P(x) \vdash \exists x\ P(x)}\,{\scriptstyle aff_d} \qquad \dfrac{}{\exists x\ P(x) \vdash \exists x\ P(x)}\,{\scriptstyle ax}}{\neg\neg\exists x\ P(x) \vee \exists x\ P(x), \neg\exists x\ P(x) \vdash \exists x\ P(x)}\,{\scriptstyle \vee_g}}{\neg\neg\exists x\ P(x) \vee \exists x\ P(x) \vdash \neg\exists x\ P(x) \longrightarrow \exists x\ P(x)}\,{\scriptstyle \rightarrow_d}}{\vdash \big(\neg\neg\exists x\ P(x) \vee \exists x\ P(x)\big) \longrightarrow \big(\neg\exists x\ P(x) \longrightarrow \exists x\ P(x)\big)}\,{\scriptstyle \rightarrow_d}$$

5.3 Traduction de Gödel-Kolmogorov

S'il existe de nombreuses formules de la logique du 1^er ordre qui ne sont pas prouvables (sans hypothèse) en logique intuitionniste, bien qu'elles le soient en logique classique, il n'en demeure pas moins qu'il existe pour toute formule de la sorte, une formule qui lui soit à la fois équivalente (au sens classique du terme) et non seulement prouvable en *logique intuitionniste*, mais également prouvable en *logique minimale*. La traduction de Gödel-Kolmogorov – qui consiste à rajouter des doubles négations un peu partout – réalise ce tour de force. Nous distinguerons, pour sa présentation, les langages égalitaires des autres, plus simples.

Langages non égalitaires

Définition 466 (Traduction de Gödel-Kolmogorov sans égalité) *Soit ϕ une formule de la logique du 1^er ordre ne contenant pas le symbole d'égalité. La traduction de Gödel-Kolmogorov de ϕ (notée ϕ^g) est la formule définie par induction sur la hauteur de ϕ de la façon suivante :*

(1) $\bot^g = \bot$;

(2) $\phi^g = \neg\neg\phi$, *si* ϕ *est atomique ;*

(3) $(\neg\phi)^g = \neg\phi^g$;

(4) $(\phi \wedge \psi)^g = \phi^g \wedge \psi^g$;

(5) $(\phi \vee \psi)^g = \neg\neg(\phi^g \vee \psi^g)$;

(6) $(\phi \longrightarrow \psi)^g = \phi^g \longrightarrow \psi^g$;

(7) $(\forall x\, \phi)^g = \forall x\, \phi^g$;

(8) $(\exists x\, \phi)^g = \neg\neg\exists x\, \phi^g$.

Notation 467 *Pour Γ un ensemble de formules de la logique du 1^er ordre, on écrit Γ^g pour l'ensemble des traductions de Gödel-Kolmogorov des formules de Γ :*

$$\Gamma^g = \{\phi^g \mid \phi \in \Gamma\}.$$

Théorème 468 *Pour tous Γ et ϕ, respectivement un ensemble de formules et une formule, dans lesquelles le symbole d'égalité n'intervient pas :*

$$\Gamma \vdash_c \phi \text{ ssi } \Gamma^g \vdash_m \phi^g.$$

Intuitivement, ce théorème dit que pour prouver une formule en logique classique, il suffit de se restreindre à n'utiliser les raisonnements par l'absurde que pour les formules atomiques, disjonctives et existentielles.

Langages égalitaires

Définition 469 (Traduction de Gödel-Kolmogorov avec égalité) *On rajoute à la définition précédente de la traduction de Gödel-Kolmogorov (sans égalité) une traduction de l'égalité :*

$$(t_1 = t_2)^g = \neg\neg(t_1 = t_2).$$

Dans ce cas, le Théorème 468 devient en toute généralité :

Théorème 470 *Pour tous Γ et ϕ, respectivement un ensemble de formules et une formule :*

$$\Gamma \vdash_c \phi \text{ ssi } \Gamma^g, \forall x\, \forall y\, (\neg\neg x = y \longrightarrow x = y) \vdash_m \phi^g.$$

Pour aller plus avant :

Au lecteur qui voudrait en savoir plus sur les modèles de Kripke des logiques intuitionniste et minimale, nous recommandons à nouveau vivement l'ouvrage de René David, Karim Nour et Christophe Raffalli intitulé *"Introduction à la logique : théorie de la démonstration : cours et exercices corrigés"* [DNR04]. Nous orientons ce même lecteur vers les ouvrages nettement plus difficiles d'accès que sont le *"Proof Theory"* de Gaisi Takeuti [Tak13] et le *"Handbook of proof theory"* de Samuel R. Buss [Bus98].

Quatrième partie

Récursivité, 2^{d} Ordre et Correspondance Preuves-Programmes

Chapitre 14

Différents formats d'infinis

***Résumé* № 65** *Il existe des ensembles infinis de différentes tailles.*
Deux ensembles ont la même taille – ou cardinalité – s'il existe une bijection entre les deux.
Un ensemble A est plus petit qu'un ensemble B s'il existe une injection de A dans B ; et strictement plus petit s'il n'existe pas d'injection de B dans A. S'il existe deux injections $i : A \longrightarrow B$ et $j : B \longrightarrow A$, alors il existe une bijection $g : A \longrightarrow B$.
Il n'y a pas de bijection : $A \longrightarrow \mathcal{P}(A)$. En conséquence, les ensembles $\mathbb{N}, \mathcal{P}(\mathbb{N}), \mathcal{P}(\mathcal{P}(\mathbb{N})), \mathcal{P}\Big(\mathcal{P}(\mathcal{P}(\mathbb{N}))\Big), \ldots$ forment une infinité d'ensembles infinis chacun de taille différente.

Toute théorie construite sur un langage dénombrable et qui possède un modèle infinie, possède également un modèle dénombrable.

※

1 Comparer la taille des ensembles

Comment compare-t-on la taille de deux ensembles ? Il est clair qu'on admet que l'un est plus petit que l'autre s'il contient moins d'éléments. Si ces deux ensembles sont finis, ou si l'un des deux est fini, cet argument est limpide. Mais que se passe-t-il lorsque les deux ensembles sont infinis ? Doit-on dire que les deux ensembles ont le même nombre d'éléments : une infinité ? Afin de répondre à la question, revenons à l'exemple de deux ensembles finis. Imaginons que nous avons un carton de poires et un carton de pommes et nous voulons savoir s'il y a autant de pommes que de poires. Comment allons-nous procéder ? Une première idée consiste à compter d'abord le nombre de pommes (on obtient alors un premier nombre entier m) puis le nombre de poires (on obtient alors un premier nombre entier r) et comparer les deux nombres obtenus. S'ils sont égaux nous dirons que les deux cartons contenaient chacun le même nombre d'éléments – il y a le même nombre de pommes que de poires – s'ils sont différents nous répondrons par la négative. Quoi de plus simple ? Et bien il y a plus simple ! Cette première manière de procéder a le désavantage de nous obliger à compter. Et compter avec des ensembles infinis, cela devient vite compliqué. Ne pourrions-nous pas trouver une seconde manière de procéder qui ne nécessite pas de savoir compter ? En fait, il suffit de prendre une pomme et une poire – de les appareiller en quelque sorte, ou de les marier – puis de les jeter, et recommencer. Tôt ou tard, nous trouverons une poire mais pas de pomme ou une pomme mais pas de poire auxquels cas nous répondrons que les deux cartons ne contenaient pas le même nombre d'éléments ; soit nous ne trouverons ni poire ni pomme et dans ce cas nous sauront que les deux cartons contenaient chacun le même nombre d'éléments.

Cette dernière manière de faire a le très grand avantage de ne pas exiger de savoir compter. Cependant, si nous la transposons au cas d'ensembles infinis, nous n'allons pas nous arrêter au bout d'un certain temps fini pour découvrir que nous avons ôté tous les éléments d'un ensemble mais pas ceux du second, ni même que nous avons bien soustrait les éléments des deux ensembles. Nous pouvons néanmoins réutiliser le processus décrit dans le cadre fini, en stipulant que deux ensembles contiennent le même nombre d'éléments si nous pouvons appareiller ceux-ci deux à deux, les marier en quelque sorte. Si nous ne pouvons pas le faire nous dirons que l'un des ensembles est plus grand que l'autre. Cette notion de mise en couple des éléments, de leur assortiment deux à deux est capturé par le concept de fonction bijective ou *bijection*. On dira que deux ensembles A et B possèdent le même nombre d'éléments s'il existe une bijection $f : A \longrightarrow B$. Si ce n'est pas le cas, on dira qu'il sont de tailles différentes. Cette approche reprend trait pour trait le procédé que nous avons décrit dans le cas des ensembles finis. Mais n'est-il pas vrai qu'entre deux ensembles infinis il existe toujours une bijection et donc que les ensembles infinis ont tous la même taille ? Et bien non ! Ce n'est pas le cas, comme le montre le résultat qui suit.

Théorème 471 (Cantor) *Soit A un ensemble non vide.*

$$\textit{Il n'y a pas de bijection} : A \longrightarrow \mathcal{P}(A).$$

Preuve du Théorème 471 : Par l'absurde, supposons qu'il existe f une telle bijection. On considère l'ensemble suivant :

$$B = \{a \in A \mid a \notin f(a)\}.$$

Comme cet ensemble est un sous-ensemble de A et que f est une bijection – donc en particulier une surjection – il existe $b \in A$ tel que $f(b) = B$. On remarque alors que :

- si $b \in f(b)$, alors $b \in B = \{a \in A \mid a \notin f(a)\}$ d'où $b \notin f(b)$;
- si $b \notin f(b)$, alors $b \notin B = \{a \in A \mid a \notin f(a)\}$ d'où $b \in f(b)$.

D'où il ressort que $b \in f(b)$ si et seulement si $b \notin f(b)$, ce qui est évidemment une contradiction. Ce qui est contredit, c'est l'hypothèse que nous avons faite. A savoir l'existence de la bijection.

$\dashv$ 471

Si l'on songe aux ensembles de tailles finies, ce théorème n'apporte pas grand chose. Il est très facile de montrer [1] que pour un ensemble A qui possède n éléments, l'ensemble de ses parties – $\mathcal{P}(A)$ – en contient lui 2^n. Par ailleurs, pour chaque entier n nous avons $n < 2^n$. Il est donc tout à fait évident qu'il ne peut y avoir de bijection entre deux ensembles finis de tailles différentes.

1. La preuve se fait par induction sur le nombre d'éléments de l'ensemble.

Par contre, dès que les ensembles sont infinis, ce théorème fait pleinement sens. Contrairement au sens commun qui s'imagine qu'il n'existe qu'un seul type d'infini, on voit qu'il en existe plusieurs, et même une infinité. Pour avoir les idées totalement claires sur ce phénomène, nous avons besoin d'un résultat simple dans son énoncé, mais un peu plus ardu dans sa preuve : le Théorème de Cantor-Schröder-Bernstein (Théorème 472) qui dit que lorsqu'on a une injection de A dans B et une injection de B dans A, alors on a une bijection. On déduit aisément de cela que puisqu'il n'y a pas de bijection entre un ensemble A et l'ensemble $\mathcal{P}(A)$ de ses parties, alors il n'y a pas d'injection de $\mathcal{P}(A)$ dans A. En effet, la fonction $f \ : \ A \longrightarrow \mathcal{P}(A)$ qui envoie chaque élément sur le singleton qu'il définit – i.e. $f(a) = \{a\}$ – est une injection. S'il existait une injection de $\mathcal{P}(A)$ dans A, il existerait alors également une bijection de $\mathcal{P}(A)$ vers A.

On voit que si l'on part de l'ensemble infini le plus accessible qui soit : l'ensemble $\mathbb{N}$ de tous les nombres entiers positifs, on obtient qu'il n'y a pas d'injection de $\mathcal{P}(\mathbb{N})$ vers $\mathbb{N}$ et donc l'ensemble $\mathcal{P}(\mathbb{N})$ est "plus gros" que $\mathbb{N}$, bien que ces ensembles soient tous deux infinis. De même, il n'y a pas d'injection de $\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big)$ vers $\mathcal{P}(\mathbb{N})$, ce qui montre que $\mathcal{P}\big(\mathcal{P}(\mathbb{N})\big)$ est plus gros encore. En itérant le fait de prendre les parties d'un ensemble, nous obtenons aisément une suite infinie d'ensembles dont le suivant est strictement plus gros que tous les précédents. Etonnant, non ?! Pire encore, pour chaque ensemble A, il existe autant d'ensembles infinis de tailles différentes deux à deux qu'il existe d'éléments dans A, tous plus effrayants les uns que les autres tels les monstres de *"Where the wild things are"* de Maurice Sendak [Sen63].

Théorème 472 (Cantor-Schröder-Bernstein) *Soient A et B deux ensembles. S'il existe deux* injections *$i : A \longrightarrow B$ et $j : B \longrightarrow A$, alors il existe une* bijection *$g \ : A \longrightarrow B$.*

Preuve du Théorème 472 : On va tout d'abord traiter le cas très particulier où $B \subset A$, puis on considérera le cas général dans un second temps.

Cas particulier : $B \subset A$. On construit par récurrence la suite $(C_n)_{n \in \mathbb{N}}$:

- $C_0 = A \setminus B$,
- C_{n+1} est l'image de C_n par l'injection i,
- C est la réunion de tous les C_n.

La motivation pour la construction de la suite $(C_n)_{n \in \mathbb{N}}$ et la constitution de l'ensemble C est la suivante :

L'ensemble A représente toutes les personnes venues ce soir au spectacle. Pour faire simple, imaginons que chacune de ces personnes portent un numéro, de sorte que A est l'ensemble de tous ces numéros. Chaque personne possède un billet valide pour le spectacle, ce billet lui indique le numéro de son siège grâce à l'injection i : cela signifie par exemple que la personne 137 doit s'asseoir sur le siège $23 = i(137)$. Malheureusement, les gens n'ont pas bien compris le fonctionnement des billets et ils se sont assis sur le siège portant leur numéro à eux au lieu de celui du siège qui leur est indiqué : la personne 137 c'est ainsi assise sur le siège numéro 137. Le problème est qu'en ne respectant pas les indications des billets, tout le monde n'est pas assis. Car l'ensemble des numéros de siège – qui correspond ici à notre ensemble B – n'est qu'un sous-ensemble de l'ensemble A des numéros de personnes. Donc seuls ceux dont le numéro correspond à celui d'un siège existant sont assis. Imaginez par exemple qu'il n'y ait pas de numéro de siège pair, la personne 137 est bien assise, alors que la personne 212 n'est pas assise pour la raison qu'il n'existe pas de siège portant ce numéro. Imaginons encore que le siège qu'attribue le billet à la personne 212 soit le $137 = i(212)$ –

celui-là même occupé par la personne 137. Nous allons donc faire asseoir la personne 212 à sa place (le siège 137), mais pour cela nous devons faire se lever la personne 137 que nous faisons asseoir sur son siège (le $23 = i(137)$) ce qui forcera la personne 23 à se lever, etc.

Ainsi, C_0 représente l'ensemble de toutes les personnes qui sont debout au début de ce processus. L'image de C_0 est l'ensemble des sièges que doivent occuper ces personnes et qui sont pour lors occupés par d'autres personnes assises de manière incorrecte, puisqu'elles occupent les sièges correspondant à leurs numéros au lieu de ceux attribués par leurs billets. Nous faisons donc lever ces dernières que nous allons faire asseoir sur leurs sièges adéquats qui sont pour l'instant occupés par l'ensemble des personnes C_1 que nous faisons lever pour les faire asseoir en C_2, etc.

Le processus continue à l'infini. Nous allons vérifier qu'à la fin de ce processus qui continue à l'infini, tout le monde est assis et le spectacle peut commencer [2]. Pour cela, désignons par h la fonction qui fait correspondre à chaque personne a le siège qu'elle occupe à la fin du processus :

(1) si l'on n'a jamais demandé à cette personne de se lever, le siège qu'elle occupe est celui qu'elle avait choisi de prime abord, donc celui qui porte son numéro : a.

(2) Si au contraire on a demandé à un moment ou à un autre à cette personne de se lever, alors on lui a attribué le siège correctement assigner par son billet : $i(a)$.

Vérifions que tout cela fonctionne : que la fonction h est bien définie et qu'elle attribue un siège à chacun.

Comme nous l'avons dit, la fonction $h:\ A \longrightarrow B$ est définie comme étant l'identité sur $A \setminus C$ et i sur C. Cela signifie que pour $a \in A$:

$$h(a) = \begin{cases} a & \text{si} \quad a \in A \setminus C \\ i(a) & \text{si} \quad a \in A \cap C. \end{cases}$$

On vérifie aisément que :

(1) h est une fonction de A dans B. Pour cela il suffit de vérifier que h est bien à valeurs dans B. Ce qui est le cas puisque pour tout élément $a \in A$:
   - si $a \in A \setminus C$, alors $a \notin C_0$ donc $a = h(a) \in B$;
   - si $a \in A \cap C$, alors $h(a) = i(a) \in B$.

(2) h est *injective* puisque si l'on prend deux éléments différents $a, a' \in A$, alors :
   - si $a, a' \in A \setminus C$, on obtient $h(a) = a \neq a' = h(a')$;
   - si $a, a' \in A \cap C$, on obtient $h(a) = i(a) \neq i(a') = h(a')$;
   - si $a \in A \setminus C$ et $a' \in A \cap C$, on obtient $h(a) = a \neq i(a') = h(a')$ puisque $a \notin C$ alors que $a' \in C$;
   - si $a' \in A \setminus C$ et $a \in A \cap C$, ce cas est symétrique au précédent.

(3) h est *surjective* car pour tout b dans B on a :
   - si $b \notin C$, alors $h(b) = b$;
   - si $b \in C$, alors il existe un entier n tel que $b \in C_n$, de plus n est non nul car $b \in B$ et $C_0 = A \setminus B$. Par conséquent, il existe par construction $a \in C_{n-1}$ tel que $i(a) = b$.

2. Cela ne veut pas dire que tout le monde est assis à l'emplacement désigné par son billet, mais uniquement que nous avons pu attribuer un siège à chaque personne.

Cas général. On considère alors B' l'image de B par l'injection j et par le cas précédent, on obtient une bijection $h : A \longrightarrow B'$. Comme $j : B \longrightarrow B'$ est bijective, il ressort que $j^{-1} \circ i : A \longrightarrow B$ est également bijective. $\dashv$ 472

Les notions d'injection et de bijection vont nous permettre de comparer les tailles des ensembles – qu'ils soient finis ou infinis. On dira de deux ensembles A et B qu'ils sont de même taille s'il existe une bijection qui les relie (on dit alors qu'ils sont équipotents). On dira que A n'est pas plus gros que B s'il existe une injection de A dans B et que A est strictement plus petit que B s'il existe une injection de A dans B mais pas d'injection de B dans A. Pour cela, introduisons une notation des plus simples.

Notation 473 *Soient A et B deux ensembles quelconques. On écrit :*

- $A \lesssim B$ *s'il existe* $i : A \longrightarrow B$ *injective,*
- $A \lnsim B$ *s'il existe* $i : A \longrightarrow B$ *injective, mais il n'existe pas* $j : B \longrightarrow A$,
- $A \approxeq B$ *s'il existe* $f : A \longrightarrow B$ *bijective.*

Avec cette nouvelle notation, le Théorème de Cantor-Schröder-Bernstein (Théorème 472) s'écrit :

$$A \lesssim B \text{ et } B \lesssim A \text{ si et seulement si } A \approxeq B.$$

En conséquence, on peut comparer deux ensembles dès que l'on dispose d'une injection de l'un dans l'autre. Par exemple, si l'on possède une injection d'un ensemble A dans un ensemble B, on peut écrire $A \approxeq B$ s'il existe une injection de B dans A – et dire qu'ils ont la même taille – et $A \lnsim B$ s'il n'en existe pas – auquel cas on dira que A est strictement plus petit que A.

Mais peut-on toujours comparer la taille des ensembles ? N'existerait-il pas deux ensembles tels qu'il n'y ait pas d'injection de l'un dans l'autre ? Et bien, non. En tout cas, si nous acceptons l'*Axiome du Choix*, nous pouvons toujours comparer deux ensembles par leurs tailles respectives. En d'autres termes, s'il n'existe pas d'injection de A dans B, alors il en existe une de B dans A. Autrement dit, on peut toujours comparer deux ensembles : on a soit $A \lesssim B$ soit $B \lesssim A$ et dans le cas où ces deux relations sont vérifiées, on a $A \approxeq B$.

Proposition 474 *Si A est un ensemble infini, alors $\mathbb{N} \lesssim A$.*

Cette proposition dit qu'il n'existe pas d'ensemble infini qui soit plus petit que l'ensemble des entiers naturels. Autrement dit, si un ensemble est plus petit que l'ensemble des entiers, alors il est nécessairement fini.

Preuve de la Proposition 474 : Procédons par l'absurde en supposant que l'on n'a pas $\mathbb{N} \lesssim A$. Puisque deux ensembles sont toujours comparables par la taille, nous avons donc $A \subseteq \mathbb{N}$. Ce qui signifie qu'il existe une injection $i : A \longrightarrow \mathbb{N}$. Regardons l'image B de A par l'injection i : $B = \{n \in \mathbb{N} \mid \text{il existe (un unique puisque } i \text{ est injective) } a \in A\ i(a) = b\}$. Puisque A est infini, il en est de même de son image B. Mais B est alors un ensemble infini d'entiers que l'on peut énumérer : $b_0, b_1, \ldots, b_n, b_{n+1}, \ldots$. Il est alors très facile de voir que la fonction $j : \mathbb{N} \longrightarrow B$ définie par $j(n) = b_n$ est injective et même bijective. En conséquence, la fonction $i : A \longrightarrow B$ étant bijective[3], nous avons $j : \mathbb{N} \longrightarrow B$ et $i^{-1} : B \longrightarrow A$ qui sont toutes deux des bijections et donc leur composée : $i^{-1} \circ j : \mathbb{N} \longrightarrow A$ est elle-même une bijection, contredisant ainsi notre hypothèse initiale selon laquelle il n'existait pas d'injection de $\mathbb{N}$ dans A. $\dashv$ 474

3. Cette fonction est en effet injective par définition de i et surjective par définition de B.

Exemple 475 L'ensemble des entiers relatifs a la même taille que l'ensemble des entiers positifs.

En effet, la fonction $f : \mathbb{N} \longrightarrow \mathbb{Z}$ définie par

$$f(n) = \begin{cases} \frac{n}{2} & \text{si} \quad n \text{ est pair} \\ \frac{n+1}{2} & \text{si} \quad n \text{ est impair} \end{cases}$$

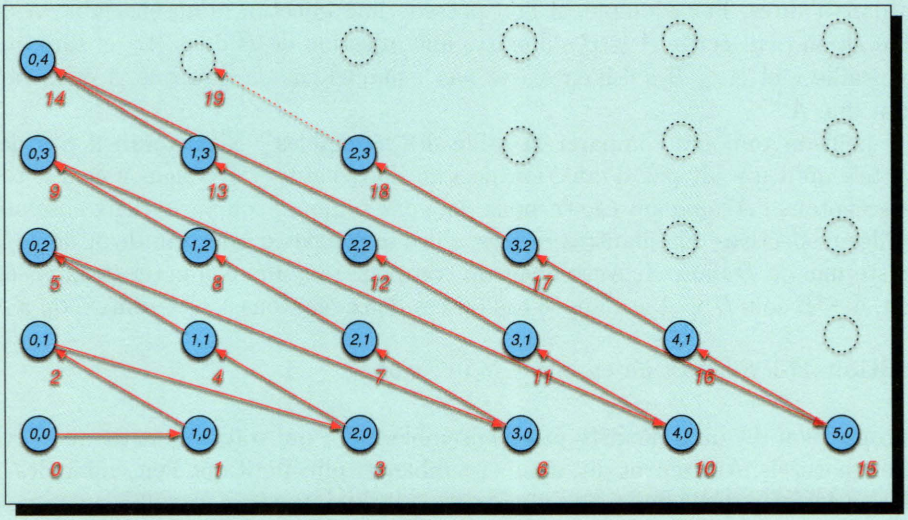
est une bijection.

Exemple 476 L'ensemble $\mathbb{N} \times \mathbb{N}$ des couples d'entiers naturels et l'ensemble $\mathbb{N}$ ont la même taille.

En effet, la fonction $g_2 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ définie par :

$$g_2(n, m) = \frac{(n+m) \cdot (n+m+1)}{2} + m$$

est une bijection. Elle est représentée ci-dessous. On voit qu'elle "mange" petit à petit le plan $\mathbb{N} \times \mathbb{N}$, diagonale après diagonale.



A partir de cette bijection, il est facile de construire une bijection $g_3 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ définie à partir de la précédente par

$$g_3(n, m, p) = g_2\big(g_2(n, m), p\big) = \frac{\left(\frac{(n+m)\cdot(n+m+1)}{2} + m + p\right) \cdot \left(\frac{(n+m)\cdot(n+m+1)}{2} + m + p + 1\right)}{2} + p$$

Plus généralement, on peut aisément définir une bijection $g_{n+1} : \underbrace{\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}}_{n+1} \longrightarrow \mathbb{N}$ par :

$$g_{n+1}(k_0, k_1, \cdots, k_n) = g_2\big(\cdots g_2\big(g_2(k_0, k_1), k_2\big) \cdots k_n\big).$$

Exemple 477 L'ensemble des nombres rationnels $\mathbb{Q}$ a la même taille que l'ensemble des entiers positifs. Nous allons utiliser le Théorème de Cantor-Schröder-Bernstein et pour cela montrer qu'il existe une injection $i : \mathbb{Q} \longrightarrow \mathbb{N}$ et une injection $j : \mathbb{N} \longrightarrow \mathbb{Q}$.

Pour la seconde, c'est très facile puisqu'il suffit de prendre pour j la fonction identité : $id(n) = n$. Pour trouver une injection $i : \mathbb{Q} \longrightarrow \mathbb{N}$, souvenons-nous qu'un élément de $\mathbb{Q}$ est de la forme $\frac{a}{b}$, où b est un entier non nul, a un élément de $\mathbb{Z}$ et il n'existe pas d'entier[4] strictement plus grand que 1 divisant à la fois a et b. Dans l'Exemple 475, nous avons défini une bijection $f : \mathbb{N} \longrightarrow \mathbb{Z}$, nous avons donc également $f^{-1} : \mathbb{Z} \longrightarrow \mathbb{N}$ qui est une bijective, par conséquent la fonction $h : \mathbb{Q} \longrightarrow \mathbb{N} \times \mathbb{N}$ définie par :

$$h\left(\frac{a}{b}\right) = (f^{-1}(a), b)$$

est injective. Comme nous avons par ailleurs dans l'Exemple 476 construit une fonction injective (bijective de surcroit) $g_2 : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

On obtient dans ce cas l'injection souhaitée en considérant la fonction composée $g_2 \circ h : \mathbb{Q} \longrightarrow \mathbb{N}$.

Exemples 478 Les relations suivantes sont vérifiées :

(1) Tout sous-ensemble infini $A \subseteq \mathbb{N}$ vérifie $A \approxeq \mathbb{N}$

(2) si A est fini, alors $A \lnsim \mathbb{N}$

(3) si A est infini, alors $\mathbb{N} \lesssim A$.

En effet, supposons qu'on n'ait pas $\mathbb{N} \lesssim A$. Alors on aurait $A \lesssim \mathbb{N}$, d'où également $A \lnsim \mathbb{N}$.

2 Le théorème de Löwenheim-Skolem

Définition 479 *On dit d'un ensemble A qu'il est* dénombrable *s'il vérifie l'une des deux conditions suivantes :*

(1) A est fini

(2) $A \approxeq \mathbb{N}$.

Dans le second cas, on parle d'un ensemble *infini dénombrable.*

Prouvons tout de suite un petit résultat bien utile.

4. On dit également que a et b sont premiers entre eux. Cette condition est nécessaire si l'on veut avoir une représentation unique de chaque nombre rationnel. On veut par exemple choisir $\frac{-2}{3}$ et non pas $\frac{-6}{9}$ ni $\frac{-4}{6}$.

Lemme 480 *Toute réunion dénombrable d'ensembles dénombrables est dénombrable.*

Preuve du Lemme 480 : Soit $(A_i)_{i\in\mathbb{N}}$ une famille dénombrable d'ensembles dénombrables. On construit une injection f de $\bigcup_{i\in\mathbb{N}} A_i$ dans $\mathbb{N}$ en choisissant pour chaque entier i une injection f_i de A_i dans $\mathbb{N}$, puis en formant $f(a) = g_2\Big(f_i(a), i\Big)$ où g_2 est la fonction définie dans l'Exemple 476 et i désigne le plus petit entier tel que $a \in A_i$.

$\dashv$ 480

Nous allons nous intéresser aux ensembles que nous manipulons en logique du 1er ordre. Bien sûr, du coté de la sémantique, il y a les modèles. Mais comme le domaine d'un modèle peut être un ensemble quelconque, il n'y a rien que nous puissions dire directement à ce sujet. Nous reviendrons à la sémantique plus loin.

Du coté de la syntaxe, par contre, il y a certaines choses très importantes à remarquer :

Proposition 481 *Soit $\mathcal{L}$ est un langage du 1er ordre ne contenant au plus qu'un nombre dénombrable de symboles de fonction, de symboles de constante et de symboles de relations.*

(1) L'ensemble des formules de $\mathcal{L}$ est infini dénombrable.

(2) L'ensemble des formules closes de $\mathcal{L}$ est infini dénombrable.

Preuve de la Proposition 481 : Montrons tout d'abord que le nombre de formules de $\mathcal{L}$ est infini dénombrable.

Remarquons en premier lieu qu'il existe un nombre infini de formules, puisque nous nous sommes donnés une infinité dénombrable de symboles de variables. En conséquence, si notre langage comporte l'égalité, nous avons à disposition la formule $x_n = x_n$ et ce, pour chaque variable x_n. De même si notre langage ne dispose pas de l'égalité, il dispose au moins d'un symbole de relation (sans quoi nous ne pourrions écrire aucune formule atomique et donc aucune formule du tout). Si ce symbole de relation R est k-aire, alors nous avons pour chaque variable x_n la formule $R(x_n, x_n, \dots, x_n)$.

Ensuite, pour montrer que le nombre de formule ne dépasse pas celui des entiers, nous allons chercher une injection i de l'ensemble des formules dans celui des entiers naturels. Cela revient à *coder* chaque formule ϕ par un nombre $i(\phi)$. Plutôt que de nous lancer dans la construction d'un processus de codage fastidieux, utilisons plutôt un codage *"ready made"* :

si nous voulons écrire une telle formule à l'aide de notre ordinateur, que se passe-il ? Nous choisissons un traitement de texte – par exemple LaTeX – qui nous permette d'écrire la formule telle qu'elle apparaisse sous la forme désirée, ce qui nous donne un fichier *"ma_formule.tex"*. Ce fichier est particulier à notre formule ϕ au sens où si nous décidons d'écrire une formule ψ différente de ϕ, alors le fichier obtenu sera également différent. Pour passer du fichier à un entier naturel, il suffit simplement de savoir qu'un tel fichier informatique n'est qu'une suite de zéros et de uns. Cela n'est pas vraiment un nombre, mais on s'en rapproche. Prenons ce fichier qui est une longue suite $a_0a_1a_2 \cdots\cdots a_{k-1}a_k$ (par exemple 001010100101) et plaçons un "1" devant : nous obtenons la suite $1a_0a_1a_2 \cdots\cdots a_{k-1}a_k$ (par exemple 1001010100101) que nous pouvons maintenant lire comme un nombre (c'est même un nombre non nul car il commence par un "1").

Nous avons donc trouvé comment *coder* chaque formule ϕ par un nombre $i(\phi)$. On pourra néanmoins nous objecter que lorsque la formule est trop longue l'ordinateur ne disposera pas de suffisamment de mémoire pour constituer le fichier. A cela, nous répondrons que nous considérons que notre machine dispose d'une réserve inépuisable de mémoire et un temps disponible aussi long que nécessaire.

Bien sûr, si nous changeons de traitement de texte, le codage d'une formule par un entier s'en trouvera modifié, mais pour autant que l'on conserve toujours le même traitement de texte, on obtiendra bien deux codages différents pour deux formules différentes, autrement dit ce codage est bien injectif. Comme nous disposons d'une injection des formules dans les entiers, nous savons que nous n'avons pas plus de formules qu'il n'y a d'entiers. En conséquence, l'ensemble des formules est infini dénombrable.

Pour montrer que l'ensemble des formules closes de $\mathcal{L}$ est infini dénombrable, il suffit de procéder de la même manière.

$\dashv$ 481

Le résultat qui suit est une conséquence – pas du tout évidente – de ce qui précède, mais particulièrement remarquable.

Théorème 482 (Löwenheim-Skolem) *Si $\mathcal{L}$ est un langage du 1^{er}ordre dont la signature est dénombrable, et $\mathcal{T}$ une théorie de ce langage, alors si $\mathcal{T}$ possède un modèle dont le domaine est infini alors :*

(1) il existe un modèle infini dénombrable $\mathcal{M}$,

(2) pour chaque ensemble infini A il existe un modèle $\mathcal{M} \models \mathcal{T}$ dont le domaine $|\mathcal{M}|$ vérifie

$$|\mathcal{M}| \equiv A.$$

Pour nous, ce résultat comporte deux intérêts :

(1) Il dit tout d'abord que si nous travaillons avec une théorie $\mathcal{T}$ construite sur un langage dénombrable, alors pour tout modèle infini non dénombrable de cette théorie, nous pouvons trouver un modèle qui satisfasse exactement les mêmes formules, mais soit cette fois infini dénombrable.

(2) Il dit ensuite que si nous définissons une théorie à l'aide d'un langage dénombrable, afin de décrire au plus près un modèle infini que nous avons en tête, cette théorie ne pourra jamais décrire ce seul modèle car elle aura nécessairement des modèles de toute cardinalité infini non dénombrable.

Preuve du Théorème 482 : Cette preuve est trop avancée pour être distillée dans cet ouvrage. Nous renvoyons le lecteur vers [CLK03b, End72, KK67, Men97, Sho67].

$\dashv$ 482

Avant de conclure ce chapitre, attardons-nous sur les théories que l'on peut construire à partir d'un langage dénombrable.

Proposition 483 *Soit $\mathcal{L}$ est un langage du 1^{er} ordre ne contenant au plus qu'un nombre dénombrable de symboles de fonction, de symboles de constante et de symboles de relations.*

L'ensemble des $\mathcal{L}$-théories n'est pas dénombrable.

Preuve de la Proposition 483 : Nous avons vu dans la Proposition 481 qu'il y a un nombre infini dénombrable de formules closes construites sur le langage $\mathcal{L}$. Or une $\mathcal{L}$-théorie n'est autre qu'un ensemble de formules closes. Donc s'il existe une bijection f entre l'ensemble des formules closes et celui des entiers naturels, cette bijection induit une bijection g entre l'ensemble des $\mathcal{L}$-théories et celui des parties des entiers :

$$g(\mathcal{T}) = \{f(\phi) \mid \phi \in \mathcal{T}\}.$$

$\dashv$ 483

Le fait que même si notre langage ne comporte qu'une signature finie, on peut se demander si l'ensemble des théories qu'il permet de construire est infini non dénombrable. Nous nous exprimons de manière finie. Lorsque nous décrivons quelque chose, nous le faisons irrémédiablement de manière finie et à l'aide de moyens qui sont eux aussi finis – que ce soient les mots, les symboles de toute sorte. En conséquence, dotés de ressources finies, il n'y a qu'un nombre dénombrable de choses que nous pouvons décrire. En effet, la description de quelque chose revient à produire une suite finie de symboles qui sont eux-mêmes en nombre fini. Or, sur un alphabet fini, il n'existe qu'un nombre dénombrable de mots finis (de suites finies d'éléments de cet alphabet). C'est même vrai si l'alphabet est dénombrable. Pour le voir très simplement, imaginons que notre alphabet soit composé des lettres $a_0, a_1, \cdots, a_n, \cdots$. Convenons de noter $\overline{k}^2$ la notation en base 2 d'un entier naturel k. Ainsi, par exemple, $\overline{3}^2 = 11$ et $\overline{12}^2 = 1100$. A chaque mot fini $a_{i_0}a_{i_1}\cdots a_{i_p}$ de cet alphabet, nous allons faire correspondre un nombre entier :

$$f(a_{i_0}a_{i_1}\cdots a_{i_p}) = \overline{i_0}^2\ 3\ \overline{i_1}^2\ 3\ \overline{i_2}^2\ 3\ \cdots\ 3\ \overline{i_p}^2.$$

La fonction f étant évidemment injective et le nombre de mots finis étant clairement infini, il en résulte que l'ensemble des mots finis – ou suites finies – sur un alphabet (non vide) au plus dénombrable est infini dénombrable.

L'ensemble des choses qu'il nous est permis d'énoncer avec nos moyens désespérément finis est irrémédiablement dénombrable. Or, un langage logique fini procure un nombre infini non dénombrable de théories. Comment relier les deux ? Simplement en acceptant que cela nous dit que la plupart de ces théories nous sont radicalement inaccessibles. Pour caractériser celles qui nous sont accessibles, nous allons regarder de plus près comment un ensemble infini d'objet, peut être décrit par un objet lui-même fini. Pour cela, nous allons nous plonger dans l'univers des programmes informatiques, des algorithmes et de la récursivité.

Pour aller plus avant :

Les considérations sur les différentes tailles des ensembles infinis que nous avons présentées dans ce chapitre se retrouvent dans les ouvrages d'introduction à la théorie des ensembles. On conseillera *"Théorie des ensembles"* de Jean-Louis Krivine [Kri07], *"Notes on set theory"* de Yannis N Moschovakis [Mos94], *"Introduction to Set Theory"* de Karel Hrbacek et Thomas Jech [HJ99], *"Elements of set theory"* de Herbert B. Enderton [End77]. On trouvera également ces résultats, ainsi que le théorème de Löwenheim-Skolem, dans les ouvrages de logique mathématique tels que *"Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles"* de René Cori et Daniel Lascar [CLK03b] ; *"A mathematical introduction to logic"* de de Herbert B. Enderton [End72], *"Introduction to mathematical logic"* de Elliot Mendelson [Men97] et *"Mathematical logic"* de Joseph R. Shoenfield [Sho67].

Pour une lecture revigorante, on conseillera *"Satan, Cantor, And Infinity And Other Mind-bogglin"* de Raymond M. Smullyan [Smu12b].

Chapitre 15

Récursivité

***Résumé* № 66** *Une $\mathcal{L}$-théorie $\mathcal{T}$ est "récursivement présentée" s'il existe un programme informatique qui pour toute formule ϕ de $\mathcal{L}$ en entrée, s'arrête au bout d'un temps fini et répond : "oui" si $\phi \in \mathcal{T}$; "non' si $\phi \notin \mathcal{T}$. Elle est "décidable" s'il existe un programme informatique qui pour toute formule ϕ de $\mathcal{L}$ en entrée, s'arrête au bout d'un temps fini et répond : "oui" si $\mathcal{T} \vdash_{c} \phi$; "non" si $\mathcal{T} \nvdash_{c} \phi$.*
La logique du 1^er^ ordre est indécidable.
Une "extension récursive" de $\mathcal{T}$ est une théorie réc. présentée $\mathcal{T}'$ telle que $\mathcal{T} \subseteq \mathcal{T}'$.

Théorèmes d'incomplétude de Gödel :

- **1^er^** *aucune extension récursive consistante de l'arithmétique de Peano n'est décidable ;*
- **2^e^** *aucune extension récursive consistante de l'arithmétique de Peano ne prouve sa propre consistance.*

※

1 Décidabilité

Dans ce chapitre, nous allons porter notre attention vers le fonctionnement d'un programme informatique. Nous n'allons bien sûr pas nous occuper de programmation proprement dite, mais énoncer quelques faits saillants [1].

(1) (a) Tout d'abord, un programme informatique reçoit quelque chose en *entrée* [2] – par exemple une liste de noms propres.

(b) Il effectue ensuite un certain travail [3] et si tout se passe bien, s'arrête et nous rend quelque chose en *sortie* : une réponse – par exemple le programme chargé de

1. Le *lambda*-calcul forme une représentation – extrêmement abstraite s'il en est – de la programmation. Le lecteur intéressé pourra se reporter au chapitre 17 à la section 1 consacrée au λ-calcul pur.
2. Ce quelque chose n'est autre qu'un fichier informatique, donc une suite de zéros et de uns.
3. Qui au fond des choses n'est autre qu'un calcul.

placer des noms par ordre alphabétique nous retournera en sortie la liste de noms que nous lui avions confiés en entrée, mais classés par ordre alphabétique [4].

(c) Si les choses se passent mal, le programme ne s'arrête jamais de travailler et ne nous retourne donc jamais rien [5]

(2) Puisqu'un programme informatique n'est qu'une suite finie de zéros et de uns, il en existe un nombre infini certes, mais seulement dénombrable.

Définition 484 *Soit $\mathcal{L}$ un langage du 1er ordre au plus dénombrable. On dit d'une $\mathcal{L}$-théorie $\mathcal{T}$ qu'elle est :*

(1) "récursivement présentée" s'il existe un programme informatique qui pour toute formule ϕ de $\mathcal{L}$ en entrée, s'arrête au bout d'un temps fini et répond :

- *"oui" si $\phi \in \mathcal{T}$*
- *"non" si $\phi \notin \mathcal{T}$.*

(2) "décidable" s'il existe un programme informatique qui pour toute formule ϕ de $\mathcal{L}$ en entrée, s'arrête au bout d'un temps fini et répond :

- *"oui" si $\mathcal{T} \vdash_c \phi$*
- *"non" si $\mathcal{T} \nvdash_c \phi$.*

La notion de théorie *récursivement présentée* est cruciale. Lorsque nous nous donnons une théorie, nous explicitons quelles sont les formules closes qui la composent. Lorsque cette théorie est axiomatisée, et même lorsqu'elle est infinie – comme c'est le cas de l'arithmétique de Peano (cf. Exemple 399 page 436) par exemple – nous donnons un moyen élémentaire de reconnaître quelles formules en font partie. Il s'avère que ce moyen élémentaire peut toujours être aisément transcris sous forme de programme informatique et même d'un programme informatique dont la simplicité ferait sourire tout informaticien. Cela est très différent lorsque nous nous donnons la théorie d'un modèle. Dans ce cas, nous disons simplement "prenons toutes les formules qui sont vraies dans ce modèle" sans donner le moindre procédé permettant de distinguer celles qui sont vraies de celles qui sont fausses. C'est le cas par exemple lorsque nous considérons l'ensemble des formules vraies dans le modèle standard de l'arithmétique (cf. Remarques 400 page 437). Si nous disposions d'un moyen simple pour faire le tri parmi l'ensemble des formules closes entre celles qui sont vraies dans ce modèle et celles qui sont fausses, chacun des problèmes de l'arithmétique deviendrait alors facilement résoluble. Or il n'en est rien.

La notion de théorie *récursivement présentée* permet de rendre compte de la manière finitiste dont nous accédons à l'infini. Ce dernier n'est jamais donné que comme le déploiement d'un processus intrinsèquement fini.

La notion de théorie *décidable* est également essentielle. Il s'agit réellement de pouvoir décider pour chaque formule donnée si l'on peut prouver cette formule à partir de cette théorie ou non. Il se trouve que même lorsque la théorie est récursivement présentée, il n'est pas toujours possible de décider si une formule est prouvable ou non. Ce que l'on peut faire,

4. Un cas particulier de programme est constitué de ceux qui ne donnent comme réponse que *"oui"* ou *"non"*. On dit que ces programmes *acceptent* ou *rejettent* ce qui leur est soumis en *entrée*. Lorsqu'on regarde ces *entrées* comme des mots – ce ne sont que des suites de symboles après tout ! – l'ensemble des mots qui sont acceptés constitue le langage par rapport auquel le programme détermine l'appartenance ou non de chaque mot par sa réponse *"oui"* ou *"non"*. Un exemple en est donné par la hiérarchie de Chomsky-Schützenberger des langages formels [Cho56].

5. C'est exactement ce qui se passe lorsqu'il y a un *bug*!

c'est construire un programme informatique (encore appelé un *algorithme*) qui, se basant sur le programme reconnaissant les formules qui font partie de la théorie (il en existe un car elle est *récursivement présentée*), peut énumérer toutes les formules qui sont prouvables et donc s'arrêter et répondre *"oui"* dès qu'il tombe sur celle dont nous voulons savoir si elle est prouvable ou non. Mais si cette formule n'est pas prouvable, alors la machine ne détectera jamais sa présence au cours de l'énumération des formules prouvables qu'elle effectue et ne s'arrêtera donc jamais. Certaines théories sont parfaitement décidables, mais d'autres, bien que récursivement présentées ne sont pas décidables. Un cas particulier parmi les théories décidables est celui des théories récursivement présentées qui, si toutefois elles ne prouvent pas une formule, prouvent nécessairement sa négation mais ne prouvent jamais à la fois une formule et sa négation – autrement dit, ses théories sont consistantes. Dans ce cas il est très facile de prendre l'algorithme qui énumère toutes les formules prouvables à partir de cette théorie. Puisque cette dernière prouve toujours une formule ou sa négation, on sait que tôt ou tard vont apparaître soit cette formule, soit sa négation. Dans le premier cas le programme s'arrête et répond *"oui"*, dans le second cas, il s'arrête également et répond *"non"*.

Exemple 485 La théorie $\mathcal{T}_{ord.\ dens.}$ des ordres denses sans premier ni dernier élément présentée dans l'Exemple 379 page 425 ne contient, hormis l'égalité, que le symbole de relation binaire $<$. Ses axiomes sont les suivants :

(1) $\forall x \neg\, x < x$ (irréflexivité)

(2) $\forall x \forall y \neg\, (x < y \;\wedge\; y < x)$ (antisymétrie)

(3) $\forall x \forall y \forall z \;\big((x < y \wedge y < z) \longrightarrow x < z\big)$ (transitivité)

(4) $\forall x \forall y \;(x < y \vee y < x \vee x = y)$ (totalité)

(5) $\forall x \forall z \;\big(x < z \longrightarrow \exists y \;(x < y \wedge y < z)\big)$ (densité)

(6) $\forall y \exists x \; x < y$ (sans premier élément)

(7) $\forall x \exists y \; x < y$ (sans dernier élément).

Cette théorie est bien évidemment récursivement présentée (pour la raison toute simple qu'elle est finie !). Elle est par ailleurs décidable, puisqu'on peut montrer que si elle ne prouve pas une formule, alors elle prouve sa négation et en aucun cas ne prouve une contradiction. Cela provient du fait que tous les modèles dénombrables qui satisfont cette théorie sont isomorphes (cf. [CLK03b, End72, KK67, Men97, Sho67]).

Cela entraîne que tous les modèles (qui sont nécessairement infinis) de cette théorie satisfont exactement les mêmes formules. En effet, par application du théorème de Löwenheim-Skolem (Théorème 482) pour tout modèle infini non dénombrable satisfaisant cette théorie, il existe un modèle infini dénombrable satisfaisant exactement les mêmes formules. Or tous les modèles infinis dénombrables étant isomorphes, il s'en suit que tous les modèles de cardinalité quelconque de $\mathcal{T}_{ord.\ dens.}$ satisfont tous exactement les mêmes formules. Il n'est donc pas possible de trouver une formule ϕ et deux modèles dénombrables $\mathcal{M}$ et $\mathcal{N}$ de cette théorie, tels que $\mathcal{M} \models \phi$ et $\mathcal{N} \models \neg\phi$. D'où, par application du théorème de complétude (Théorème 439, page 474) :

si $\mathcal{T}_{ord.\ dens.} \nvdash_c \phi$ alors $\mathcal{T}_{ord.\ dens.} \not\models \phi$, d'où $\mathcal{T}_{ord.\ dens.} \models \neg\phi$ et donc $\mathcal{T}_{ord.\ dens.} \vdash_c \neg\phi$.

2 Les théorèmes d'incomplétude de Gödel

Lorsqu'on met sur pied une théorie, on a en tête quelque chose. On vise quelque chose que l'on souhaiterait circonscrire, pour ensuite tenter de résoudre toute sorte de problèmes à son sujet. C'était le cas par exemple lorsqu'a été définie l'arithmétique de Peano. Cette axiomatique tente de cerner au plus près ce qu'est l'arithmétique. Ce que l'on souhaite plus que tout, c'est obtenir une théorie décidable qui permette de résoudre ensuite chacun des problèmes que l'on se pose. Si la première théorie qui nous vient à l'esprit n'est pas décidable, nous pouvons toujours nous dire que nous pouvons l'enrichir de nouveaux axiomes afin de la rendre décidable. Cependant, nous voulons toujours préserver le caractère récursivement présenté de notre théorie (nous voulons savoir ce que nous mettons dedans !). Pour cette raison-là, nous introduisons la notion qui suit.

Définition 486 *Soit $\mathcal{L}$ un langage du 1er ordre au plus dénombrable et $\mathcal{T},\mathcal{T}'$ deux $\mathcal{L}$-théories.*

$$\mathcal{T} \text{ est une “extension récursive” de } \mathcal{T}' \text{ si } \begin{cases} \mathcal{T}' \subseteq \mathcal{T} \\ \text{et} \\ \mathcal{T} \text{ est réc. présentée.} \end{cases}$$

Théorème 487 (Premier Théorème d'incomplétude de Gödel)

- *Si l'arithmétique de Peano est consistante, alors elle n'est pas une théorie décidable.*
- *De plus, aucune extension récursive consistante de l'arithmétique de Peano n'est décidable.*

Preuve du Théorème 487 : La preuve est beaucoup trop longue et difficile pour être reproduite ici. Nous renvoyons le lecteur pour des ouvrages en français vers [CLK03b, NNGG89, Kri07], pour des ouvrages en anglais vers [Fra05, Gir87, Lin03, Smi13, Smu92] et pour les curieux qui souhaiteraient accéder à la preuve originale de Kurt Gödel, vers son article de 1931 *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I* [Göd31].

⊣ 487

Ce théorème s'appelle théorème d'incomplétude, car une conséquence immédiate du fait que l'arithmétique de Peano ne soit pas décidable est que cette même théorie n'est pas complète, au sens où la théorie obtenue en prenant toutes les formules qui sont prouvables à partir de l'arithmétique de Peano, soit contient absolument toutes les formules (auquel cas elle est inconsistante) ; soit, pour au moins une formule ϕ, ne contient ni cette formule ni sa négation $(\neg\phi)$ – et donc elle est dite incomplète puisqu'il reste encore de la place pour y introduire soit la formule ϕ soit sa négation, sans pour autant rendre cette nouvelle théorie inconsistante.

La première idée qui vient en tête, lorsqu'on est confronté pour la première fois au théorème d'incomplétude, est de se dire que si l'arithmétique de Peano n'est pas assez forte pour pouvoir décider chacune des questions relatives à l'arithmétique, il nous faut enrichir cette théorie, trouver de nouveaux axiomes pour que cette nouvelle axiomatique devienne enfin décidable et idéalement caractérise au plus près le modèle standard de l'arithmétique. Or le premier théorème d'incomplétude dit que cette direction de recherche est irrémédiablement vouée à l'échec, puisqu'aucune extension récursive consistante de l'arithmétique de Peano n'est décidable. En particulier, il n'existe aucune extension $\mathcal{T}$ de l'arithmétique de Peano telle que pour toute formule de l'arithmétique ϕ, ou bien $\mathcal{T} \vdash_c \phi$ ou bien $\mathcal{T} \vdash_c \neg\phi$ est vérifié, mais pas $\mathcal{T} \vdash_c \phi \wedge \neg\phi$. Autrement dit, aucune extension récursive de l'arithmétique de Peano n'atteint précisément le modèle standard de l'arithmétique.

On pourrait se dire que le problème vient du schéma d'axiomes de récurrence qui dit que pour une propriété quelconque définie au 1$^{\text{er}}$ordre dans le langage de l'arithmétique, une preuve par récurrence suffit pour montrer que tous les entiers satisfont cette propriété. N'y aurait-il pas des propriétés incroyablement compliquées, d'un degré de perversion inimaginable, qui soient la cause de cet apparent "défaut" de l'arithmétique de Peano. En effet, le fait que l'arithmétique de Peano soit infinie permet peut-être à quelque propriété bizarre de se cacher dans cette multitude. En fait il n'en est rien, comme nous allons le voir dans l'exemple suivant.

Exemple 488 L'arithmétique de Robinson [Rob50, CLK03b] est une théorie finie sur le langage $\mathcal{L} = \langle \mathbf{0}, \mathbf{s}, +, \bullet \rangle$ muni de l'*égalité*, où $\mathbf{0}$ est un symbole de constante, $\mathbf{s}$ est un symbole de fonction unaire et $+$ et $\bullet$ sont deux symboles de fonction binaires. Ses axiomes sont les suivants :

(1) $\forall x \;\; \mathbf{s}(x) \neq x$ *(0 n'a pas de prédecesseur)*

(2) $\forall x \forall y \;\; \mathbf{s}(x) = \mathbf{s}(y) \longrightarrow x = y$ *(la fonction successeur est injective)*

(3) $\forall x \;\; (x \neq \mathbf{0} \longrightarrow \exists y \;\; \mathbf{s}(y) = x)$ *(tout nombre non nul admet un prédécesseur)*

(4) $\forall x \;\; x + \mathbf{0} = x$ *(étape de base de la déf. par réc. de l'addition)*

(5) $\forall x \forall y \;\; x + \mathbf{s}(y) = \mathbf{s}(x + y)$ *(étape successeur de la déf. par réc. de l'addition)*

(6) $\forall x \;\; x \bullet \mathbf{0} = \mathbf{0}$ *(étape de base de la déf. par réc. de la multiplication)*

(7) $\forall x \forall y \;\; x \bullet \mathbf{s}(y) = (x \bullet y) + x$ *(étape successeur de la déf. par réc. de la multiplication)*

Comme elle est finie, cette théorie est équivalente à la théorie qui ne contient qu'une unique formule : la conjonction de ces sept axiomes.

Cette arithmétique de Robinson est par ailleurs très pauvre. Elle ne permet pas par exemple de prouver que la multiplication est commutative. Pourtant elle a été mise à jour à la suite de la question suivante : quels sont les axiomes qu'une théorie de l'arithmétique plus faible que celle de Peano doit nécessairement avoir pour pouvoir néanmoins prouver le premier théorème d'incomplétude ? L'arithmétique de Robinson, constitue une réponse minimale. Elle permet, bien qu'étant rudimentaire, de prouver ce résultat. C'est donc une théorie *"récursivement présentée"* (mieux que ça encore : elle est finie !) dont il n'existe pas d'extension récursive qui soit décidable. Etonnant, non ? !

Une conséquence très facile et néanmoins cruciale de ce renforcement du premier théorème d'incomplétude, qui constitue sa preuve dans l'arithmétique de Robinson, est l'indécidabilité de la logique du 1$^{\text{er}}$ ordre.

Théorème 489 (Indécidabilité de la logique du 1$^{\text{er}}$ ordre) *Il n'existe pas d'algorithme permettant de décider pour toute formule ϕ si $\vdash_c \phi$.*

Preuve du Théorème 489 : Procédons par l'absurde et imaginons qu'il existe un tel algorithme. Nous allons montrer que l'arithmétique de Robinson serait décidable, ce qui contredit ce que nous venons de voir. Le gros avantage de l'arithmétique de Robinson par rapport à celle de Peano, c'est qu'elle est finie. Soit donc ϕ_{Rob} la conjonction des sept axiomes de l'arithmétique de Robinson. Pour une formule quelconque du langage de l'arithmétique ψ, nous avons :

$$\phi_{Rob} \vdash_c \psi \text{ si et seulement si } \vdash_c \phi_{Rob} \longrightarrow \psi.$$

Nous pouvons utiliser notre algorithme pour décider si $\vdash_c \phi$ et ce, pour n'importe quelle formule ϕ. Considérons alors $\phi = \phi_{Rob} \longrightarrow \psi$. Décider si $\vdash_c \phi$, c'est décider si $\phi_{Rob} \vdash_c \psi$ qui est la même chose que décider si ψ est prouvable dans l'arithmétique de Robinson ou non.

$\dashv$ 489

Le premier théorème d'incomplétude nous dit qu'aucune extension récursive que ce soit de l'arithmétique de Peano ou de Robinson n'est complète. Cela signifie que pour chaque extension récursive consistante $\mathcal{T}$ d'une de ces deux arithmétiques, il existe une formule ϕ telle qu'on ait à la fois $\mathcal{T} \nvdash_c \phi$ et $\mathcal{T} \nvdash_c \neg\phi$. Par le théorème de complétude cette fois-ci, cela signifie qu'il existe deux modèles $\mathcal{M}$ et $\mathcal{N}$ satisfaisant tous deux la théorie $\mathcal{T}$ et tels que $\mathcal{M} \models \phi$ et $\mathcal{M} \models \neg\phi$. Dès lors, on est en droit de se poser la question suivante : combien de modèles de l'arithmétique de Peano existe-t-il ?

Posée comme cela, la question n'est pas très intéressante, puisque nous savons par le théorème de Löwenheim-Skolem (cf. page 501) que s'il existe un modèle infini dénombrable d'une théorie construite sur un langage fini, alors cette théorie admet des modèles de n'importe quelle cardinalité infinie. Nous pouvons reformuler la question différemment pour éliminer ce problème : combien de modèles dénombrables de l'arithmétique de Peano existe-t-il ?

Mais là encore, il nous faut faire attention. Car si l'on prend le modèle standard $\mathbb{N}$ mais que l'on renomme les entiers différemment – par exemple l'entier k s'appelle maintenant $Raymond_k$ – alors on obtient un second modèle *stricto sensu* différent du premier, mais en tout point pareil au sens où les deux seront isomorphes. Nous devons donc à nouveau reformuler notre question qui devient maintenant : combien de modèles dénombrables de l'arithmétique de Peano non isomorphes existe-t-il ?

Un rapide calcul permet de limiter ce nombre possible : il en existe au plus autant qu'il y a de parties d'entiers naturels, c'est-à-dire autant qu'il y a de nombres réels. Mais la chose la plus étonnante est qu'il y en a exactement autant qu'il y a de nombres entiers réels. Autrement dit, un nombre infini non dénombrable.

Proposition 490 *Si l'arithmétique de Peano est consistante, alors il existe un nombre non dénombrable de modèles de l'arithmétique de Peano.*

Preuve de la Proposition 490 :

(1) Pour chaque partie d'entiers $N \subseteq \mathbb{N}$, nous allons définir une théorie $\mathcal{T}_N$ et montrer que si l'arithmétique de Peano est consistante, alors $\mathcal{T}_N$ admet un modèle $\mathcal{M}_N$;

(2) Puis nous montrerons que pour chaque $N \subseteq \mathbb{N}$, il n'existe qu'un nombre dénombrable de sous-ensembles $N' \subseteq \mathbb{N}$ tels que $\mathcal{M}_N$ et $\mathcal{M}_{N'}$ soient isomorphes.

Tout d'abord, nous allons enrichir le langage de l'arithmétique $\mathcal{L}$ d'un nouveau symbole de constante c. La théorie $\mathcal{T}_N$ est obtenue en ajoutant à l'arithmétique de Peano l'ensemble

$$\{\phi_N \mid n \in N\} \cup \{\neg\phi_N \mid n \notin N\}$$

où ϕ_N est la formule

$$\exists x \Big(x \neq \mathsf{c}_0 \land f_\times\Big(\underbrace{f_s(f_s(\cdots f_s}_{p_n}(\mathsf{c}_0)\ldots), x\Big) = \mathsf{c}\Big)$$

dans laquelle p_n est le $n+1$ème nombre premier [6]. Autrement dit, ϕ_N dit que c est divisible par le $n+1$ème nombre premier.

Pour montrer que la théorie $\mathcal{T}_N$ admet un modèle, il suffit d'utiliser le théorème de compacité (voir page 441). En effet, chaque partie *finie* de la théorie $\mathcal{T}_N$ ne contient qu'un nombre fini de formules parmis $\{\phi_N \mid n \in N\} \cup \{\neg\phi_N \mid n \notin N\}$. Toutes ces formules prises ensemble disent que c est divisible par un certain nombre *fini* de nombres premiers : $p_{i_0}, p_{i_1}, \cdots, p_{i_k}$ et pas par d'autres (également en nombre finis). Il suffit alors de prendre un modèle qui satisfait l'arithmétique de Peano et d'interpréter dans celui-ci c par l'entier obtenu en faisant le produit des nombres $p_{i_0}, p_{i_1}, \cdots, p_{i_k}$ [7].

Par application du théorème de compacité, la théorie $\mathcal{T}_N$ admet un modèle dénombrable $\mathcal{M}_N$.

Maintenant, imaginons qu'il y ait un ensemble d'entiers N ainsi qu'un ensemble P non vide de sous ensembles de $\mathbb{N}$, tels que pour tout $N' \in P$, les modèles $\mathcal{M}_N$ et $\mathcal{M}_{N'}$ soient isomorphes. Fixons pour chaque $N' \in P$ un isomorphisme $\tilde{f}_{N'}$ de $|\mathcal{M}_{N'}|$ dans $|\mathcal{M}_N|$ et dénommons $a_{N'}$ l'élément du domaine de $\mathcal{M}'_N$ par lequel est interprété c dans ${}_{\mathcal{M}N'}$ ($\mathsf{c}^{\mathcal{M}_{N'}} = a_{N'}$) et $b_{N'}$ l'élément du domaine de $\mathcal{M}_N$ sur lequel est envoyé $a_{N'}$ par l'isomorphisme $\tilde{f}_{N'}$. Remarquons tout de suite que puisque $\tilde{f}_{N'}$ est un isomorphisme, on doit avoir pour tout nombre premier p_n : p_n divise $a_{N'}$ si et seulement si p_n divise $b_{N'}$. En effet, par définition de la notion d'isomorphisme, si p_n divise $a_{N'}$, alors il existe un élément $a \in |\mathcal{M}_{N'}|$ tel que :

$$f_\times^{\mathcal{M}_{N'}}\Big(\underbrace{f_s^{\mathcal{M}_{N'}}(f_s^{\mathcal{M}_{N'}}(\cdots f_s^{\mathcal{M}_{N'}}}_{p_n}(\mathsf{c}_0^{\mathcal{M}_{N'}})...), a\Big) = a_{N'} = \mathsf{c}^{\mathcal{M}_{N'}}.$$

D'où dans $\mathcal{M}_N$ nous avons :

$$\tilde{f}_{N'}\bigg(f_\times^{\mathcal{M}_{N'}}\Big(\underbrace{f_s^{\mathcal{M}_{N'}}(f_s^{\mathcal{M}_{N'}}(\cdots f_s^{\mathcal{M}_{N'}}}_{p_n}(\mathsf{c}_0^{\mathcal{M}_{N'}})...), a\Big)\bigg) = \tilde{f}_{N'}(a_{N'}) = b_{N'}.$$

Or $\tilde{f}_{N'}$ étant un isomorphisme, nous avons l'égalité suivante :

$$\tilde{f}_{N'}\bigg(f_\times^{\mathcal{M}_{N'}}\Big(\underbrace{f_s^{\mathcal{M}_{N'}}(f_s^{\mathcal{M}_{N'}}(\cdots f_s^{\mathcal{M}_{N'}}}_{p_n}(\mathsf{c}_0^{\mathcal{M}_{N'}})...), a\Big)\bigg) =$$
$$\bigg(f_\times^{\mathcal{M}_N}\Big(\underbrace{f_s^{\mathcal{M}_N}(f_s^{\mathcal{M}_N}(\cdots f_s^{\mathcal{M}_N}}_{p_n}(\mathsf{c}_0^{\mathcal{M}_N})...), \tilde{f}_{N'}(a)\Big)\bigg).$$

D'où l'on obtient :

$$\bigg(f_\times^{\mathcal{M}_N}\Big(\underbrace{f_s^{\mathcal{M}_N}(f_s^{\mathcal{M}_N}(\cdots f_s^{\mathcal{M}_N}}_{p_n}(\mathsf{c}_0^{\mathcal{M}_N})...), \tilde{f}_{N'}(a)\Big)\bigg) = \tilde{f}_{N'}(a_{N'}) = b_{N'}.$$

Cela signifie ni plus ni moins que $b_{N'}$ est divisible par p_n. Nous avons donc montré que si p_n divise $a_{N'}$, alors p_n divise également l'image de $a_{N'}$: $b_{N'}$.

Puisque la bijection inverse $\tilde{f}_{N'}^{-1}$ constitue un isomorphisme de $\mathcal{M}_N$ dans $\mathcal{M}_{N'}$, de la même manière on montre que si $b_{N'}$ est divisible par p_n, alors il en est de même de $a_{N'}$.

6. Le premier nombre premier est 2, le second 3, le troisième 5, le etc.

7. *Stricto sensu*, on interprète c et par lequel le terme $\underbrace{f_s(f_s(\cdots f_s(\mathsf{c}_0)...)}_{p_{i_0}\cdot p_{i_1}\cdot\cdots\cdot p_{i_k}}$ par le même élément du modèle.

Nous avons donc bien montré que pour tout nombre premier p_n, $a_{N'}$ est divisible par p_n si et seulement si $b_{N'}$ est divisible par p_n.

Revenons maintenant à ce qui nous préoccupe. Si l'on prend N' et N'' deux ensembles d'entiers appartenants à P tels qu'il existe un nombre $n \in N' \setminus N''$. On obtient alors par construction que $a_{N'}$ est divisible par p_n, mais $a_{N''}$ n'est pas divisible par p_n. En conséquence $b_{N'}$ est divisible par p_n, mais $b_{N''}$ n'est pas divisible par p_n, d'où $b_{N'}$ et $b_{N''}$ sont différents.

En conséquence, la fonction dont l'ensemble de départ est P et l'ensemble d'arrivée est l'ensemble $|\mathcal{M}_N|$ et qui envoie N' sur $b_{N'}$ est injective. Ce qui démontre que P est dénombrable.

Formons maintenant la partition $(F_i)_{i\in I}$ de $\mathcal{P}(\mathbb{N})$ suivante : $N, N' \in F_i$ si et seulement si $\mathcal{M}_N$ et $\mathcal{M}_{N'}$ sont isomorphes. D'après le résultat que nous venons d'établir, chaque ensemble F_i est dénombrable et $\bigcup_{i\in I} F_i = \mathcal{P}(\mathbb{N})$ n'est pas dénombrable. D'aprés le Lemme 480, toute réunion dénombrable d'ensembles dénombrables est dénombrable. Il découle donc que l'ensemble I n'est pas dénombrable. Choisissons enfin pour chaque $i \in I$ un ensemble $N_i \in F_i$, il ressort que pour tout couple d'éléments $i \neq j$ de I, $\mathcal{M}_{N_i}$ et $\mathcal{M}_{N_j}$ ne sont pas isomorphes. D'où l'ensemble

$$\{\mathcal{M}_{N_i} \mid i \in I\}$$

est un ensemble *non dénombrable* de modèles *dénombrables* de l'arithmétique de Peano deux à deux non isomorphes.

$\dashv$ 490

Puisque nous avons toujours parlé du premier théorème d'incomplétude de Gödel, il doit en exister un second : le voici.

Théorème 491 (Second Théorème d'incomplétude de Gödel) *Aucune extension récursive consistante de l'arithmétique de Peano ne prouve sa propre consistance.*

Preuve du Théorème 491 : Encore une fois, la preuve est beaucoup trop longue et difficile pour être reproduite ici. Nous renvoyons le lecteur vers [CLK03b, NNGG89, Kri07, Fra05, Gir87, Lin03, Smi13, Smu92].

$\dashv$ 491

Qu'est-ce que cela peut bien vouloir dire qu'une théorie prouve sa propre consistance. C'est en fait assez simple si l'on songe que les théories qui nous intéressent sont des extensions de l'arithmétique de Peano, donc des théories qui parlent de nombres. Maintenant qu'est-ce qu'une théorie consistante ? C'est une théorie qui ne prouve pas à la fois une formule et sa négation. Pour faire encore plus simple, puisque nous nous limitons aux extensions récursives de l'arithmétique de Peano, une telle théorie est consistante si et seulement si elle ne prouve pas la formule *"0=1"*. Nous pouvons dès lors fixer une manière informatique de représenter une preuve – c'est ce qui a été fait pour écrire cet ouvrage ! – en sorte que le bel arbre plus ou moins compliqué que constitue une preuve – pour fixer les choses, disons en Déduction Naturelle – n'est autre qu'un fichier informatique, une suite de zéros et de uns qui devient un entier naturel dès que je lui mets un "1" devant. Donc chaque preuve est représentée par un entier naturel et on peut même caractériser les propriétés (numériques !) que doivent avoir les entiers naturels qui "codent" des preuves de la formules *"0=1"* avec pour hypothèses des formules de l'extension récursive de l'arithmétique de Peano qui nous intéresse. Il ne reste plus qu'à écrire la formule $cons(\mathcal{T})$ qui dit qu'il n'existe pas de nombre satisfaisant ces propriétés.

Le second théorème de Gödel dit que si la théorie $\mathcal{T}$ est consistante, alors $\mathcal{T} \not\vdash_c cons(\mathcal{T})$.

Cela nous dit que si l'arithmétique de Peano est consistante, alors elle ne prouve pas sa propre consistance. Bien sûr, on peut très facilement étendre l'arithmétique de Peano – $\mathcal{T}_\mathcal{P}$ – en lui adjoignant la formule qui dit qu'elle est une théorie consistante – $cons(\mathcal{T}_\mathcal{P})$ – mais cette nouvelle théorie – $\mathcal{T}_\mathcal{P} \cup \{cons(\mathcal{T}_\mathcal{P})\}$ – ne prouvera pas sa propre consistance.

Une autre manière de regarder la chose est de dire que si nous trouvons une théorie qui permette à la fois d'exprimer l'arithmétique de Peano et de prouver que l'arithmétique de Peano est consistante, alors cette théorie ne prouvera pas sa propre consistance et nous n'en serons pas plus avancés, puisqu'il existera toujours la possibilité que notre théorie super-puissante ne soit en fait qu'inconsistante, auquel cas elle prouve absolument tout, y compris la consistance de Peano.

Pour aller plus avant :

La récursivité est traitée dans les ouvrages de logique avancés. On conseillera *"Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles"* de René Cori et Daniel Lascar [CLK03b], *"Computability and logic"* de George S. Boolos, John P. Burgess et Richard C. Jeffrey [BBJ02], *"A first course in logic : an introduction to model theory, proof theory, computability, and complexity"* de Shawn Hedman [Hed04], ainsi que *"Mathematical logic* de Joseph R. Shoenfield [Sho67].

Le lecteur particulièrement intrigué par la récursivité et ses relations à l'informatique pourra se plonger dans les ouvrages suivants : *"Computability Theory : An Introduction to Recursion Theory"* de Herbert B. Enderton [End10], *"Computability theory"* de S Barry Cooper [Coo04], *"Computability : computable functions, logic, and the foundations of mathematics"* de Richard L. Epstein et Walter Alexandre Carnielli [EC89], *"Classical recursion theory : The theory of functions and sets of natural numbers"* de Piergiorgio Odifreddi [Odi92], *"Theory of Computation"* de George Tourlakis [Tou12], *"Proofs and computations"* de Helmut Schwichtenberg et Stanley S. Wainer [SW11], *"Computability : An introduction to recursive function theory"* de Nigel Cutland [Cut80], *"Theory of recursive functions and effective computability"* de Hartley Rogers Jr [RJ87].

Pour le lecteur qui souhaiterait une orientation plus proche de l'informatique, nous conseillons tout particulièrement les excellents *"Introduction to automata theory, languages, and computation"* de John E. Hopcroft, Rajeev Motwani et Jeffrey D. Ullman [HMU01], *"Introduction to the Theory of Computation"* de Michael Sipser [Sip06] et *"Computational complexity"* de Christos H. Papadimitriou [Pap03], *"P, NP, and NP-Completeness : The basics of computational complexity"* de Oded Goldreich [Gol10].

Pour une approche historique, nous dirigeons le lecteur vers *"Engines of Logic : Mathematicians and the Origin of the Computer"* de Martin Davis [Dav01], *"The search for mathematical roots, 1870-1940 : logics, set theories and the foundations of mathematics from Cantor through Russell to Gödel"* de Ivor Grattan-Guinness [GG11] et *"The confluence of ideas in 1936"* de Robin Gandy [Gan95].

Enfin, au sujet des deux théorèmes d'incomplétude de Gödel, nous renvoyons le lecteur d'une part vers les articles originaux : *"Die vollstandigkeit der Axiome des logischen Funktionenkalkuls"* de Kurt Gödel [Göd30] et *"Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I"* de Kurt Gödel [Göd31]. D'autre part vers les ouvrages à destination d'un plus large public suivants : *"Gödel's Theorem : an incomplete guide to its use and abuse"* de Torkel Franzén [Fra05], *"Le théorème de Gödel"* de Ernest Nagel, James R. Newman, Kurt Gödel et Jean-Yves Girard [NNGG89], *"An introduction to Gödel's theorems"* de Peter Smith [Smi13], ainsi que *"Gödel's incompleteness theorems"* de Raymond M. Smullyan [Smu92]. On lire également avec profit le chapitre consacré à ce théorème dans *"Le point aveugle, tome 1 : vers la perfection"* de Jean-Yves Girard [Gir06], ainsi que les ouvrages *"Diagonalization and self-reference"* et *"Forever Undecided"* de Raymond M. Smullyan [Smu94, Smu12a], et également *"Incompleteness in the Land of Sets"* de Melvin Fitting [Fit07].

Chapitre 16

Logique du 2^d ordre et théorie des ensembles

***Résumé* № 67** *La logique du 2^d ordre quantifie non seulement sur les individus, mais aussi sur les relations ainsi que sur les fonctions. Elle est strictement plus expressive que la logique du 1^{er} ordre ; par contre elle ne satisfait :*

(1) ni le théorème de compacité,

(2) ni le théorème de Löwenheim-Skolem,

(3) ni le théorème de complétude (au sens où il existerait un système de preuves contrôlable par informatique qui corresponde à la sémantique usuelle).

La théorie des ensembles de Zermelo-Fraenkel constitue un expédient permettant, tout en restant au premier ordre, de quantifier aussi bien sur les fonctions que les relations. ※

La logique du 1^{er} ordre ne quantifie que sur les individus des domaines des modèles considérés. Elle permet d'exprimer qu'il existe un individu qui satisfait une certaine propriété, ou bien que tous les individus la satisfont. Mais elle ne permet pas de dire qu'il existe une propriété – au sens d'un ensemble d'invidus – que satisfait certaines choses, ni que toutes les propriétés vérifient telles autres choses. La logique du 1^{er} ordre quantifie sur des individus, mais non sur des ensembles d'individus.

Or, tout naturellement, dans le langage courant, nous parlons de propriétés que satisfont des éléments, mais aussi de propriétés que satisfont des ensembles d'éléments. Ainsi, par exemple nous dirons qu'une certaine relation binaire est un ordre totale si cette relation est irréflexive, antisymétrique et transitive et que tout couple d'éléments peut être comparé. Mais nous dirons également qu'un ordre total est un *bon ordre* si tout ensemble non vide possède un plus petit élément. Pour ce faire, nous avons cette fois-ci utilisé une quantification qui ne porte plus seulement sur les éléments que la relation binaire ordonne, mais sur les ensembles de tels éléments. Nous verrons plus loin (Exemple 493) que cette propriété relève du second ordre : elle est exprimable au 2^d ordre mais ne l'est pas au 1^{er} ordre.

Pour comprendre l'idée de base de la logique du 2^{d} ordre, revenons tout d'abord à la logique du 1^{er} ordre et à ce que signifie la quantification pour celle-ci. Lorsque nous avons défini ce qu'était un terme, nous sommes parti de deux notions de base : les *"constantes" et les "variables"*. Ces deux notions ont quelque chose en commun, puisqu'elles ne parlent toutes deux que des individus – les éléments du domaine. Mais pour un modèle donné, la constante est *"constante"* – comme son nom l'indique – alors que la variable *"varie"*. Une constante dénote un individu, une variable représente en quelque sorte toutes les dénotations possibles d'une constante. Autrement dit, une variable est comme une constante qui varie. Si l'on songe maintenant à ce que sont les interprétations des symboles de fonction et des symboles de relation, on voit que celles-ci sont également fixes. Dans un modèle, un symbole de fonction désigne une fonction particulière (parmi toutes celles possibles), un symbole de relation est interprété par une relation particulière (parmi toutes celles possibles).

1 Syntaxe

Dans la logique du 2^{d} ordre, on se propose d'introduire des symboles de variable spécifiques aux fonctions et des symboles de variables spécifiques aux relations, en sorte de pouvoir faire varier leurs interprétation à l'intérieur d'un même modèle.

Pour cela, on ajoute à la logique du 1^{er} ordre deux types de variables – dites variables de second ordre – pour chaque entier k :

(1) $X_0^{f,k}, X_1^{f,k}, X_2^{f,k}, \cdots$ (ce sont les variables qui varient sur les fonctions d'arité k) ;

(2) $X_0^{R,k}, X_1^{R,k}, X_2^{R,k}, \cdots$ (ce sont les variables qui varient sur les relations d'arité k).

Les termes de cette logique sont définis de manière similaire à ceux de la logique du 1^{er} ordre, excepté qu'il nous faut prendre en compte également les variables du second ordre se rapportant à des fonctions.

L'ensemble $\mathtt{T}_{\mathcal{L}}$ des *termes du langage* $\mathcal{L}$ est le plus petit ensemble qui :

- contient les variables du 1^{er} ordre $(x_0, x_1, \cdots)$ et les symboles de constantes,
- pour chaque symbole de fonction d'arité n du langage *f*, chaque fois qu'il contient les termes $t_1, \ldots, t_n$, contient également le terme $f(t_1, \ldots, t_n)$,
- pour chaque variable du second ordre $X^{f,n}$ portant sur les fonctions d'arité n du langage *f*, chaque fois qu'il contient les termes $t_1, \ldots, t_n$, contient également le terme $X^{f,n}(t_1, \ldots, t_n)$.

Les *formules atomiques* sont cette fois de deux formes possibles :

(1) $R(t_1, \ldots, t_n)$ (2) $X^{R,n}(t_1, \ldots, t_n)$

où :

- R est un symbole de relation d'arité n,
- $t_1, \ldots, t_n$ sont des termes du langage $\mathcal{L}$,
- $X^{R,n}$ est une variable du 2^{d} ordre portant sur les relations d'arité n.

L'ensemble des *formules de la Logique du 2^{d} ordre* est alors défini comme le plus petit ensemble qui :

- contient chaque arbre réduit à sa racine (qui est alors une *formule atomique*) et
- chaque fois qu'il contient des formules ϕ et ψ, contient également les formules suivantes :

$$\begin{array}{c}\neg\\ |\\ \phi\end{array}, \quad \begin{array}{ccc} & \vee & \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \wedge & \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longrightarrow & \\ \phi & & \psi\end{array}, \quad \begin{array}{ccc} & \longleftrightarrow & \\ \phi & & \psi\end{array}.$$

- Pour chaque variable du 1er ordre x, chaque entier non nul n et chaque variable du 2d ordre $X^{f,n}$ ou $X^{R,n}$, chaque fois qu'il contient la formule ϕ, contient également les formules suivantes :

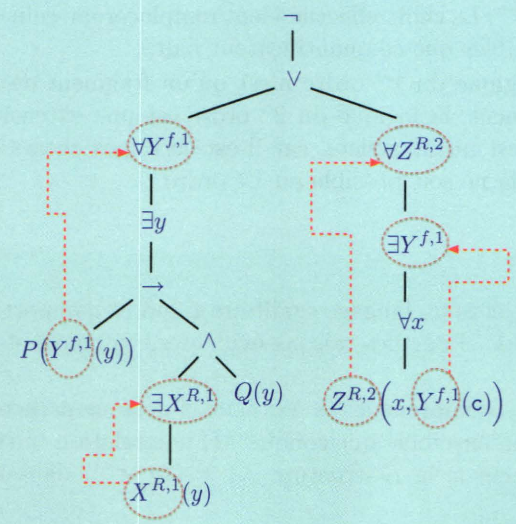
$$\begin{array}{c}\exists x\\ |\\ \phi\end{array}, \quad \begin{array}{c}\forall x\\ |\\ \phi\end{array}, \quad \begin{array}{c}\exists X^{f,n}\\ |\\ \phi\end{array}, \quad \begin{array}{c}\forall X^{f,n}\\ |\\ \phi\end{array}, \quad \begin{array}{c}\exists X^{R,n}\\ |\\ \phi\end{array}, \quad \begin{array}{c}\forall X^{R,n}\\ |\\ \phi\end{array}.$$

Ces formules se linéarisent tout naturellement pour ce qui est des cas identiques à la logique du 1er ordre. Les quatre derniers cas donnent respectivement :

(1) $\exists X^{f,n}\overline{\phi}$ (2) $\forall X^{f,n}\overline{\phi}$ (3) $\exists X^{R,n}\overline{\phi}$ (4) $\forall X^{R,n}\overline{\phi}$.

Enfin la notion d'occurrence de variable libre ou liée est semblable à ce que nous avons vu dans le cadre du 1er ordre, excepté que nous avons maintenant aussi des variables du 2d ordre. On dira donc qu'une occurrence d'une variable x (respectivement $X^{f,n}$, $X^{R,n}$) dans une formule – cette occurrence apparaît nécessairement dans une formule atomique, donc dans une des feuilles de l'arbre que constitue cette formule – est libre s'il n'existe le long de la branche remontant de cette feuille à la racine, aucun nœud de la forme $\forall x$ (respectivement $\forall X^{f,n}$, $\forall X^{R,n}$) ni $\exists x$ (respectivement ni $\exists X^{f,n}$, ni $\exists X^{R,n}$). Dans le cas contraire, le premier quantificateur, portant sur la variable considérée rencontré en remontant le long de la branche, est celui qui lie cette variable. Voila pour la syntaxe.

Exemple 492 Un exemple de formule du 2d ordre dans laquelle P et Q sont des symboles de relation unaire et c un symbole de constante, x et y des variables du 1er ordre, et $X^{R,1}$, $Y^{f,1}$ et $Z^{R,2}$ des variables du 2d ordre :



Cette formule se linéarise en :

$$\neg\Big(\forall Y^{f,1}\exists y\ \big(P(Y^{f,1}(y)) \longrightarrow (\exists X^{R,1}\ X^{R,1}(y) \wedge Q(y))\big) \vee \forall Z^{R,2}\exists Y^{f,1}\forall x\ Z^{R,2}(x, Y^{f,1}(\mathsf{c}))\Big).$$

On appelle logique *monadique du 2ᵈ ordre* la restriction de cette logique aux seules variables du 2ᵈ ordre de la forme $X^{R,1}$. Ce sont donc des variables qui varient sur les relations d'arité 1, autrement dit sur les propriétés que satisfont ou non des individus. On écrit en général simplement ces variables en lettres capitales comme X par exemple au lieu de $X^{R,1}$. Ce fragment de la logique du 2ᵈ ordre a déjà un pouvoir expressif supérieur à la logique du 1ᵉʳ ordre, comme nous le verrons dans l'Exemple 493.

2 Sémantique

La *sémantique standard* de la logique du 2ᵈ ordre est on ne peut plus claire. Tout ce qui concerne la partie de cette logique qui est identique à la logique du 1ᵉʳ ordre est inchangé. Les variables du 2ᵈ ordre, quant à elles, varient sur les fonctions ou les relations dont l'arité n'est autre que celle qu'elles désignent. Pour le dire simplement, le jeu d'évaluation associé à une formule ϕ du 2ᵈ ordre dans un modèle $\mathcal{M}$ du 1ᵉʳ ordre, est identique à celui présenté dans le cadre du 1ᵉʳ ordre, excepté pour les nœuds de la forme :

(1) $\exists X^{f,n}$ (2) $\forall X^{f,n}$ (3) $\exists X^{R,n}$ (4) $\forall X^{R,n}$.

Lorsque le jeu se retrouve dans l'une de ces positions, le ***Vérificateur*** – s'il s'agit du quantificateur existentiel – ou le ***Falsificateur*** – s'il s'agit du quantificateur universel – choisit une fonction d'arité n – c'est-à-dire une fonction de $|\mathcal{M}|^n$ dans $|\mathcal{M}|^n$ – dans la cas où il s'agit d'une variable $X^{f,n}$, ou une relation d'arité n – c'est-à-dire un sous-ensemble de $|\mathcal{M}|^n$ – dans le cas d'une variable $X^{R,n}$. Le choix effectué vient remplacer, au sein des formules atomiques, les occurrences des variables que ce quantificateur liait.

Il est clair que la logique du 1ᵉʳ ordre n'est qu'un fragment de la logique du 2ᵈ ordre. Ou, pour le dire autrement, la logique du 2ᵈ ordre est une extension de la logique du 1ᵉʳ ordre. Cette extension est même stricte, car il est certaines choses que l'on peut exprimer au 2ᵈ ordre sans que cela ne soit possible au 1ᵉʳ ordre.

Exemple 493 On considère un langage égalitaire $\mathcal{L}$ qui ne comporte qu'un unique symbole de relation binaire noté $<$. Pour des raisons évidentes, on convient de noter $x < y$ au lieu de $<(x, y)$.

La théorie $\mathcal{T}_{ord.\ tot.}$ comprenant les axiomes ci-dessous caractérise les ordres totaux. Cela signifie que pour un ensemble quelconque M, une relation binaire $< \subseteq M \times M$ est un ordre total si et seulement si la $\mathcal{L}$-structure $\mathcal{M} = \langle M, <^{\mathcal{M}}\rangle$ dans laquelle $<^{\mathcal{M}} = <$ vérifie $\mathcal{M} \models \mathcal{T}_{ord.\ tot.}$.

$\mathcal{T}_{ord.\ tot.}$ est la théorie qui comprend les quatre axiomes suivants :

(1) $\forall x \neg\, x < x$ (irréflexivité)

(2) $\forall x \forall y \neg\, (x < y \;\wedge\; y < x)$ (antisymétrie)

(3) $\forall x \forall y \forall z\, \big((x < y \wedge y < z) \longrightarrow x < z\big)$ (transitivité)

(4) $\forall x \forall y\, (x < y \vee y < x \vee x = y)$ (totalité)

Par contre, il n'est pas possible d'enrichir la théorie $\mathcal{T}_{ord.\ tot.}$ en une théorie qui décrivent exactement les bons ordres, c'est-à-dire ceux parmi les ordres totaux qui vérifient que tout ensemble non vide d'éléments possède un plus petit élément [1], et ce quand bien même nous y ajouterions une infinité de formules. Plus exactement, nous allons montrer que toute $\mathcal{L}$-théorie $\mathcal{T}$ qui a pour modèle l'ensemble des bons ordres, admet également un modèle qui n'est pas un bon ordre.

Pour cela, nous allons tout d'abord enrichir le langage $\mathcal{L}$ en un langage $\mathcal{L}'$ en ajoutant une infinité de symboles de constantes : $\mathsf{c}_0, \mathsf{c}_1, \mathsf{c}_2, \cdots$. Puis nous formons la $\mathcal{L}'$-théorie $\mathcal{T}'$:

$$\mathcal{T}' = \mathcal{T} \cup \{\mathsf{c}_{i+1} < \mathsf{c}_i \mid i \in \mathbb{N}\}.$$

Il est très facile de voir que chaque sous-théorie finie de la théorie $\mathcal{T}'$ possède un modèle puisque par hypothèse, chaque bon ordre est un modèle de $\mathcal{T}$, donc en particulier celui engendré par l'ordre usuel sur les entiers, et un sous-ensemble fini de $\{\mathsf{c}_{i+1} < \mathsf{c}_i \mid i \in \mathbb{N}\}$ ne fait intervenir qu'un nombre fini de symboles de constantes : $\mathsf{c}_{i_0}, \cdots, \mathsf{c}_{i_k}$. Il suffit dès lors d'interpréter ces constantes par autant d'entiers, tout en respectant l'ordre indiqué pour obtenir un modèle de la sous-théorie finie.

Par le théorème de compacité (cf. page 441), la $\mathcal{L}'$-théorie $\mathcal{T}'$ possède un modèle $\mathcal{M}$. Or, dans ce modèle l'ensemble $\{\mathsf{c}_i^{\mathcal{M}} \mid i \in \mathbb{N}\}$ n'admet pas de plus petit élément. En oubliant les symboles de constantes, le modèle $\mathcal{M}$ devient une $\mathcal{L}$-structure satisfaisant $\mathcal{T}$, mais possédant une *suite infinie descendante d'éléments* qui témoigne qu'elle ne constitue pas un bon ordre.

Par contre la notion de bon ordre est exprimable au 2^{d} ordre. Il suffit pour cela d'ajouter aux axiomes (1)-(4) la formule suivante (dans laquelle nous nous sommes permis d'écrire X au lieu de $X^{R,1}$ pour des raisons de concision) :

$$\forall X \Big(\exists x\; X(x) \longrightarrow \exists y\; \Big(X(y) \wedge \forall z\; \big(X(z) \longrightarrow (y = z \vee y < z)\big)\Big)\Big).$$

Cette formule dit précisément que tout sous-ensemble (X) non vide possède un plus petit élément (y) :

"tout ensemble (X) qui possède un élément (x) possède également un élément (y) qui est plus petit que tous ceux (z) qu'il possède, à l'exception de lui-même".

1. C'est le cas de l'ordre naturel sur les entiers, puisque tout ensemble non vide d'entiers possède un plus petit élément. Ce n'est pas le cas de $\mathbb{Z}$ muni de l'ordre usuel, puisque l'ensemble $\mathbb{Z}$ tout entier ne possède pas de plus petit élément ; ni des nombres réels positifs car l'ensemble $\{\frac{1}{n+1} \mid n \in \mathbb{N}\}$ n'admet pas non plus de plus petit élément. Par contre, tout ordre total qui ne comporte qu'un nombre fini d'éléments est *ipso facto* un bon ordre.

Exemple 494 La *finitude* n'est pas exprimable au 1^er ordre. Par contre elle l'est au 2^d ordre.

Au 1^er ordre nous allons tout d'abord montrer qu'il n'existe pas de théorie $\mathcal{T}$ sur un langage égalitaire $\mathcal{L}$, telle que les modèles qui la satisfont sont exactement tous des ensembles finis.

Procédons par l'absurde et imaginons qu'il existe une telle théorie $\mathcal{T}$. On enrichie alors le langage en ajoutant les nouveaux symboles de constante $\mathsf{c}_0, \mathsf{c}_1, \mathsf{c}_2, \cdots$ pour construire la théorie $\mathcal{T}'$ suivante :

$$\mathcal{T}' = \mathcal{T} \cup \{\mathsf{c}_i \neq \mathsf{c}_j \mid i, j \in \mathbb{N} \text{ and } i \neq j\}.$$

Il est clair que si la théorie $\mathcal{T}'$ admet un modèle, celui-ci ne peut qu'être de domaine infini, puisque chaque nouveau symbole de constante doit être interprété par un élément différent de tous ceux par lesquels sont interprétés tous les autres. Par ailleurs, un tel modèle est également un modèle de $\mathcal{T}$ une fois que l'on a "oublié" les nouveaux symboles de constantes et leurs interprétations. Il nous suffit donc de montrer que $\mathcal{T}'$ admet un modèle pour contredire le fait que $\mathcal{T}$ caractérise les modèles à domaines finis.

Cela découle encore une fois immédiatement du théorème de compacité (voir page 441). Chaque sous-théorie *finie* de $\mathcal{T}'$ admet un modèle, puisque cette sous-théorie ne fait intervenir qu'un nombre fini – disons k – de nouveaux symboles de constante. Dès lors, chaque modèle comportant au moins k éléments la satisfait. En conséquence $\mathcal{T}'$ admet un modèle et donc $\mathcal{T}$ admet un modèle infini, ce qui contredit notre hypothèse première.

Au 2^d ordre la formule suivante caractérise les modèles finis :

$$\forall X^{f,1}\Big(\forall y \exists x\ X^{f,1}(x) = y \longrightarrow \forall z \forall z'\ \big(X^{f,1}(z) = X^{f,1}(z') \longrightarrow z = z'\big)\Big).$$

Cette formule dit de toute fonction dont le domaine d'arrivée est le même que le domaine de départ que si elle est surjective, alors elle est également injective. Cette propriété ne se réalise que si le domaine en question est fini. En effet, pour tout ensemble E infini, il est possible de choisir une infinité dénombrable d'éléments $a_0, a_1, \cdots$ de E pour ensuite définir la fonction suivante :

$$f(a) = \begin{cases} a & \text{si} \quad a \neq a_i \text{ (pour tout } i \in \mathbb{N}) \\ a_0 & \text{si} \quad a = a_0 \\ a_i & \text{si} \quad a = a_{i+1} \text{ (pour } i \in \mathbb{N}). \end{cases}$$

Cette fonction est surjective mais pas injective.

Ainsi la logique du 2^d ordre est plus expressive que la logique du 1^er ordre. Elle en est d'ailleurs une extension toute naturelle. Elle semble donc primer sur celle-ci en tous points. Or il n'en est rien. D'une part ni le Théorème de compacité (voir page 441) ni le Théorème de Löwenheim-Skolem (voir page 501) ne sont vrais dans cette logique. Mais chose plus grave encore, il n'existe pas de théorie de la démonstration satisfaisante pour cette logique. Plus précisément, il n'existe aucun système de preuve qui à la fois permette d'obtenir le théorème de complétude – c'est-à-dire fasse correspondre la notion de conséquence syntaxique à la notion de conséquence sémantique – et soit contrôlable par un programme informatique.

Cela signifie que tout système de preuve, pour lequel il existe un algorithme permettant de décider si une suite de symboles quelconques constitue une preuve, échoue à valider pour chacune des formules ϕ l'équivalence :

$$\vdash \phi \text{ si est seulement si } \models \phi.$$

Dit autrement, tout système de preuve permettant de démontrer pour chaque formule ϕ :

$$\vdash \phi \text{ si est seulement si } \models \phi,$$

est indécidable, au sens où l'ensemble des preuves n'est pas décidable. Ce qui est tout de même très ennuyeux puisque dans ce cas, nous n'avons pas de contrôle effectif sur ce qu'est une preuve et sur ce qui n'en est pas. En résumé, *il n'existe pas de bonne notion de preuve pour la logique du 2^{d} ordre.* Ce qui fait dire à certains que la logique du 2^{d} ordre n'est pas une logique à proprement parler [Qui86].

Il est néanmoins possible de circonvenir à ce problème en modifiant la sémantique de la logique du 2^{d} ordre. Nous avons présenté la sémantique dite *"standard"*, mais il existe une autre sémantique – la *"sémantique de Henkin"* qui permet de retrouver les bonnes propriétés souhaitées pour cette logique. On récupère ainsi le Théorème de complétude, le Théorème de compacité et le Théorème de Löwenheim-Skolem . Cette sémantique permet de controller l'ensemble des fonctions ou l'ensemble des relations sur lesquels les variables du second ordre varient. Tout semble donc aller pour le mieux dans le meilleur des mondes avec cette sémantique plus contraignante. Malheureusement, la logique du 2^{d} ordre munie de cette sémantique n'a pas un pouvoir expressif supérieur à la logique du 1^{er} ordre [Man96, Sha91, Vää01].

3 Une petite idée de la théorie des ensembles

Une solution – retenue entre autres pour fonder les mathématiques – consiste à ne travailler qu'au 1^{er} ordre tout en se restreignant à une théorie au sein de laquelle on puisse parler non seulement des individus, mais aussi des ensembles d'individus, des relations, des fonctions, etc. Cela permet de quantifier non seulement sur les individus, mais aussi sur les ensembles d'individus, sur les fonctions, les relations, et pourquoi pas les ensembles de relations... Pour cela, il est nécessaire que parmi les éléments du domaine d'un modèle, on retrouve non seulement les individus que l'on vise, mais aussi ces outils que sont les fonctions ou les relations. Cette solution s'appelle la *"théorie des ensembles"*.

Les objets dont parle la *théorie des ensembles* sont des ensembles. Les éléments d'un modèle de la théorie des ensembles sont des ensembles et les ensembles de tels éléments, les relations sur de tels éléments, les fonctions entre ces ensembles, tout cela ne sont que des ensembles.

Nous sommes habitués depuis le plus jeune âge à faire la distinction entre un ensemble et ses éléments. L'ensemble étant d'une *"nature"* autre que celle de ses éléments : un ensemble de petits pois n'est pas un petit pois. Ici tout n'est qu'ensemble. Les éléments sont eux-mêmes des ensembles. Mais qu'est-ce qu'un ensemble alors ? C'est précisément ce que tente de décrire la théorie des ensembles. On pourrait penser qu'un ensemble est une collection d'objets. Mais il n'en est rien, comme l'a montré Bertrand Russell au début du XX^{e} siècle [Rus03]. Connu sous le nom de *"paradoxe de Russell"*, celui-ci statue sur le fait que toute collection d'objets n'est pas forcément un ensemble. S'il en était ainsi, nous pourrions considérer la collection de tous les ensembles et ce serait un ensemble. De plus, lorsqu'on dispose d'un ensemble

A d'un coté et d'une propriété P de l'autre, on peut former l'ensemble B des éléments de A qui satisfont la propriété P. Si nous prenons pour A le soit-disant *"ensemble de tous les ensembles"* et pour P la propriété de ne pas s'appartenir, alors nous formons l'ensemble suivant :

$$B = \{x \mid x \notin x\}.$$

Ensuite, si nous posons la question : "cet ensemble vérifie-t-il la propriété en question ou non ?" On voit immédiatement que l'on a : si $B \in B$ alors $B \notin B$ et inversement, si $B \notin B$ alors $B \in B$. D'où $B \in B$ si et seulement si $B \notin B$. Ce qui est évidemment une contradiction.

On ne peut donc pas considérer qu'une collection d'objets est un ensemble. Mais alors que sont les ensembles ? Ce sont précisément les objets qui vérifient ce que dit la théorie des ensembles, autrement dénommée théorie de *Zermelo-Fraenkel* (ou encore *ZF*). Nous allons rapidement passer en revue les axiomes qui forment cette théorie. Deux choses sont à noter :

(1) Le langage est rudimentaire : il s'agit du langage égalitaire ne contenant qu'un unique symbole de relation binaire noté "$\in$".

(2) Les axiomes sont en nombre infini. Exactement comme dans le cas de l'arithmétique de Peano, il y a deux schémas d'axiomes.

Les axiomes de Zermelo-Fraenkel

(1) *Extensionnalité :*

$$\forall x\, \forall y\, \big(\forall z\, (z \in x \longleftrightarrow z \in y) \longrightarrow x = y\big).$$

Cet axiome raconte que deux ensembles sont égaux lorsqu'ils ont exactement les mêmes éléments. Un ensemble n'est défini que par ce qu'il contient et par rien d'autre.

(2) *Paire :*

$$\forall x\, \forall y\, \exists z\, (x \in z \wedge y \in z).$$

Si x et y sont deux ensembles, alors je peux former un ensemble (la paire $\{x, y\}$) qui contient ces deux-là.

(3) *Union :*

$$\forall a\, \exists b\, \forall x\, \forall y\, \big((x \in y \wedge y) \in a \longrightarrow x \in b\big).$$

L'union d'un ensemble est l'ensemble des éléments de ses éléments. On retrouve ainsi la notion usuelle d'union de deux ensembles en remarquant que ce que nous écrivons $A \cup B$ n'est autre que l'union de la paire $\{A, B\}$.

(4) *Infini :*

$$\exists x\, \big(\exists y\, (y \in x) \wedge \forall y\, (y \in x \longrightarrow y \cup \{y\} \in x)\big).$$

Cet axiome semble étrange pour deux raisons :

(a) Il utilise des symboles qui ne font pas partie du langage initial – "$\cup$", "$\{$" et "$\}$" – mais qui ne sont là que comme une manière d'écrire en condensé la formule qui devrait se substituer à $y \cup \{y\} \in x$. Cette formule dit qu'*"il existe un z qui est l'union de la paire formée de y et de $\{y\}$"*[2].

2. Ce dernier ensemble n'étant autre que la paire $\{y, y\}$ puisque si l'on compare les deux ensembles $\{y\}$ et $\{y, y\}$, on voit qu'ils sont égaux – axiome d'extensionnalité – puisqu'ils contiennent exactement les mêmes éléments (à savoir y).

(b) L'infini y est présenté de manière bizarre. Pour comprendre ce qui s'y passe, convenons d'appeler *"successeur"* de y l'ensemble $y \cup \{y\}$. Ce que dit cet axiome, c'est qu'il existe un ensemble x qui contient un ensemble – au sens ou x n'est pas l'ensemble vide, et qui chaque fois qu'il contient un élément, contient également son successeur. On voit donc que dans x il y a y, mais aussi le successeur de y,donc le successeur du successeur de y, puis également le successeur du successeur du successeur de y, etc. Il contient donc une infinité d'éléments. Cet ensemble est donc infini.

(5) *Parties :*

$$\forall x\, \exists y\, \forall z\, \big(\forall u\, (u \in z \longrightarrow u \in x) \longrightarrow z \in y\big).$$

L'axiome des parties dit que si x est un ensemble, alors il en est de même de $\mathcal{P}(x)$.

(6) *Compréhension (schéma d'axiomes) :*

$$\forall z\, \forall w_1 \ldots \forall w_n\, \exists y\, \forall x\, \big(x \in y \longleftrightarrow (x \in z \wedge \varphi)\big),$$

où φ est une formule dont toutes les variables libres figurent parmi $x, z, w_1, \cdots, w_n$. Ce schéma d'axiomes constitue autant d'axiomes qu'il y a de formules φ telles qu'indiquées ci-dessus. C'est à dire un nombre infini dénombrable. Pour chaque formule φ, il est dit que pour chaque ensemble z on peut constituer y qui est l'ensemble des éléments de z qui satisfont la propriété décrite par φ. Une autre manière de voir la chose est de dire que pour chaque formule φ, chaque ensemble z se découpe en deux ensembles, le sous-ensemble de ses éléments qui satisfont φ et celui formé de ceux qui ne la satisfont pas [3].

(7) *Remplacement (schéma d'axiomes) :*

$$\forall D\, \forall w_1 \ldots \forall w_n \Big(\forall x\, (x \in D \longrightarrow \exists ! y\, \varphi) \longrightarrow \exists A\, \forall x\, \big(x \in D \longrightarrow \exists y\, (y \in A \wedge \varphi)\big)\Big),$$

où

- *φ est une formule dont toutes les variables libres figurent parmis $x, y, D, w_1, \cdots, w_n$.*
- *la formulation "$\exists ! y \varphi$" est une abréviation pour "il existe un unique y tel que φ", ce qu'exprime la formule suivante :*

$$\exists y\, \Big(\varphi(x, y, D, w_1, \cdots, w_n) \wedge \forall z\, \big(\varphi(x, z, D, w_1, \cdots, w_n) \longrightarrow z = y\big)\Big).$$

Ce schéma de remplacement est aussi très étrange. En réalité, non seulement il n'est utile que pour fonder des mathématiques très avancées, mais au fond, il ne dit que des choses assez banales. Il constitue un axiome pour chaque formule φ, donc à nouveau une infinité dénombrable d'axiomes. Mais ces formules sont un peu particulières : ces formules se comportent comme des fonctions puisque pour chaque x, il existe un unique y qui satisfasse φ. Autrement dit, à chaque élément, φ en associe un unique – que l'on peut voir comme son image. Ce que dit ce schéma d'axiome est que si l'on dispose d'une telle formule, alors pour tout ensemble D – qu'on appellera ensemble de départ – il existe un ensemble A – qu'on appellera ensemble d'arrivée – qui contient toutes les images des éléments de D telles que définies par φ.

3. Ce sont précisément ceux qui satisfont la formule $\neg\varphi$.

(8) <u>*Choix*</u> :

$$\forall x\, \exists c \forall z\, \exists y\, \forall u \Big(z \in x \longrightarrow \Big(y \in z \wedge y \in c \wedge \big((u \in z \wedge u \in c) \longrightarrow u = y \big) \Big) \Big).$$

L'axiome du choix dit de manière plus absconse, mais en substance, que si l'on dispose d'une famille $(E_i)_{i \in I}$ d'ensembles tous non vides, alors on dispose également d'un ensemble constitué en prélevant un seul et unique élément dans chacun de ces ensembles. C'est cet ensemble qui réalise le *"choix"* à proprement parlé.

(9) <u>*Fondation*</u> :

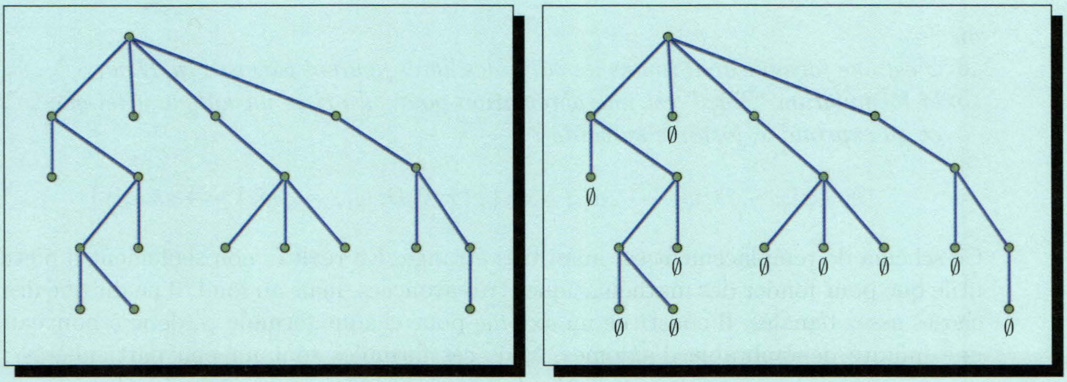
$$\forall x \Big(\exists y\, (y \in x) \longrightarrow \exists y\, \big(y \in x \wedge \neg \exists z\, (z \in x \wedge z \in y) \big) \Big).$$

Cet axiome paraît lui aussi très étrange. Il dit que la relation d'appartenance est bien-fondée. Pour mieux comprendre ce que cela signifie, nous allons faire figurer les ensembles sous forme d'arbres non vides [4] pour lesquels la notion de bonne fondation devient très clair.

Tout d'abord on dit qu'un arbre est *"bien-fondé"* s'il ne possède pas de branche infinie. Cela signifie que tout chemin qui part de la racine, atteint tôt ou tard une feuille. Un arbre T bien-fondé permet de définir un ensemble E de la manière suivante :

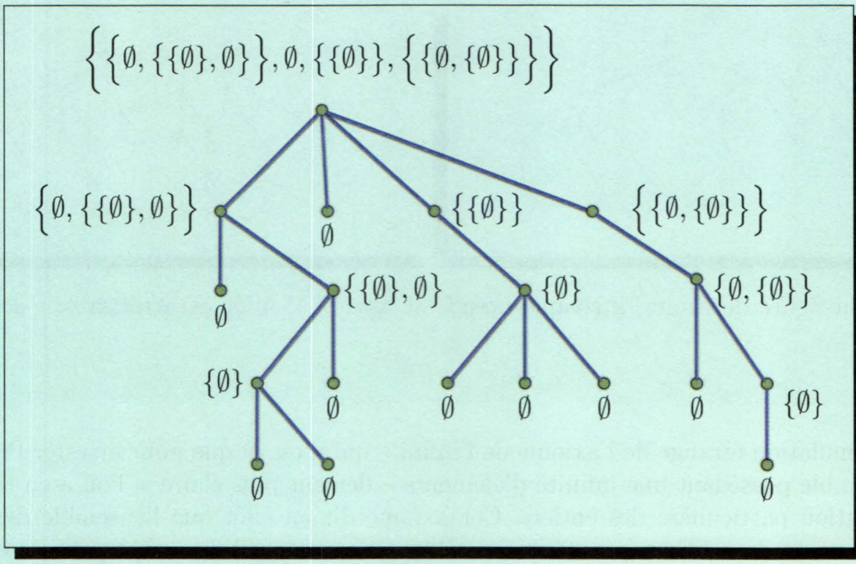
- à chaque nœud n on associe un ensemble E_n formé par l'ensemble des ensembles que dénotent les fils de ce nœud. Précisément, si le nœud n a trois fils n_1, n_2, n_3, alors $E_n = \{E_{n_1}, E_{n_2}, E_{n_3}\}$. Chacun des ensembles $E_{n_1}, E_{n_2}, E_{n_3}$ étant également défini de la sorte en un processus qui se termine aux feuilles puisque l'arbre est bien-fondé.
- L'ensemble que représente l'arbre T est alors E_r où r désigne la racine de l'arbre.

Exemple 495



Nous nous souvenons de l'axiome d'extensionnalité qui stipule que deux ensembles sont égaux s'ils possèdent les mêmes éléments. En conséquence les ensembles $\{\emptyset, \emptyset, \emptyset\}$ et $\{\emptyset, \emptyset\}$ sont tous égaux à $\{\emptyset\}$, raison pour laquelle nous utilisons cette expression raccourcie.

4. Les arbres non vides sont ceux qui possèdent une racine.



On obtient alors que cet arbre représente l'ensemble

$$\Big\{\big\{\emptyset,\{\{\emptyset\},\emptyset\}\big\},\emptyset,\{\{\emptyset\}\},\big\{\{\emptyset,\{\emptyset\}\}\big\}\Big\}\ [5].$$

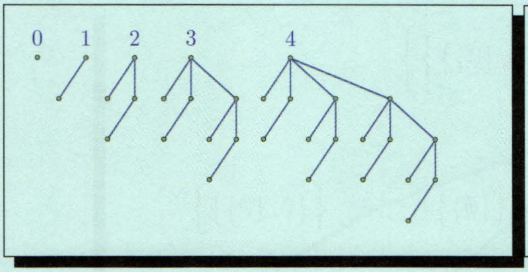
Chaque nombre entier est conçu comme étant l'ensemble de ses prédécesseurs [6]. On voit qu'avec une telle représentation, l'entier naturel $n+1$ est un ensemble qui contient exactement $n+1$ éléments : $\{0, 1, 2, \cdots, n\}$.

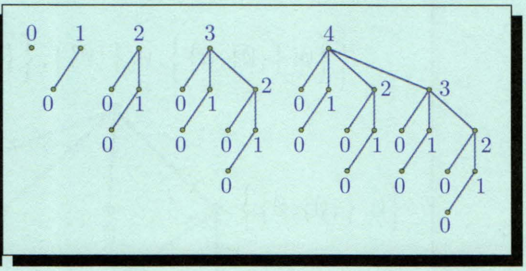
Exemple 496 La figure ci-dessous représente les cinq premiers entiers sous forme d'arbre. Il est à noté qu'on part de 0, représenté par l'ensemble vide et donc par un arbre réduit à sa seule racine – celle-ci n'ayant pas de descendant, l'ensemble qu'elle constitue ainsi est vide. Ensuite, on passe d'un entier n à son successeur $n+1$ en prenant l'arbre de n à la racine duquel on rajoute un fils dont le sous-arbre engendré n'est autre que l'arbre définissant n lui-même. Ce qui d'un point de vue purement ensembliste revient à dire que $n+1$ n'est autre que l'ensemble $n \cup \{n\}$. On vérifie aisément que si n n'est autre que l'ensemble de ses prédécesseurs [7], il en est alors de même de $n+1$.

5. Ou si l'on écrit $\{\}$ au lieu de $\emptyset$: $\Big\{\big\{\{\},\{\{\{\}\},\{\}\}\big\},\{\},\{\{\{\}\}\},\big\{\{\{\},\{\{\}\}\}\big\}\Big\}$.

6. Cela signifie que 0 est représenté par l'ensemble vide, puisque 0 n'a pas de prédécesseur ; que 1 est représenté par l'ensemble $\{0\}$ – c'est-à-dire $\{\emptyset\}$ – que 2 est représenté par l'ensemble $\{0,1\}$ – c'est-à-dire $\big\{\{\emptyset\},\emptyset\big\}$, etc.

7. En effet, si $n = \{0, 1, \cdots, n-1\}$ alors $n+1 = n \cup \{n\} = \{0, 1, \cdots, n-1\} \cup \{n\} = \{0, 1, \cdots, n\}$.

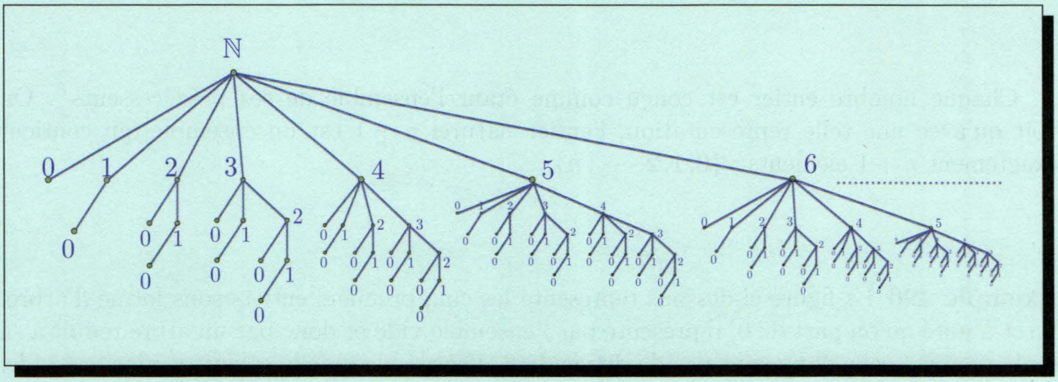




Dans la figure de droite, à chaque nœud est associé l'entier caractérisant le sous-arbre engendré.

La formulation étrange de l'axiome de l'infini – qui n'est là que pour attester l'existence d'un ensemble possédant une infinité d'éléments – devient plus claire si l'on a en tête cette représentation particulière des entiers. Cet axiome dit en effet que l'ensemble des entiers tel que présenté dans l'Exemple 497 existe. Plus exactement, il dit qu'il existe un ensemble dans lequel le suivant est inclus, ce qui revient à dire que l'ensemble des entiers existe si l'on applique correctement l'une des instances du schéma de compréhension.

Exemple 497 L'ensemble des entiers représenté sous forme d'arbre bien-fondé :



Cet arbre est bien-fondé car il n'a pas de branche infinie. Par contre, il n'est pas à *branchement fini* puisque la racine possède une infinité de descendants (tous les entiers).

On voit donc qu'en théorie des ensembles, tout n'est qu'ensemble. Les nombres entiers ne sont tous que des ensembles parmi d'autres. Mais où sont alors passées les fonctions et les relations ? Ce sont aussi des ensembles parmi d'autres mais lesquels ? Pour les trouver, il suffit de se rappeler qu'une relation n-aire R sur un ensemble E n'est qu'un sous-ensemble de l'ensemble

$$\underbrace{E \times E \times \cdots \times E}_{n}.$$

Les axiomes permettent de montrer très facilement que si E existe, alors

$$\underbrace{E \times E \times \cdots \times E}_{n}$$

existe également, ainsi que tous les sous-ensemble, de cet ensemble. Par conséquent, toutes les relations sur E sur là. De même, une fonction n-aire f de D dans A est représentée par son graphe $\mathcal{G}_f$ qui n'est autre qu'un sous-ensemble particulier de

$$\underbrace{D \times D \times \cdots \times D}_{n} \times A$$

vérifiant la condition spécifiant qu'il n'existe qu'une seule image pour chaque n-uplet en entrée et exprimée par la formule $\forall x_1 \, \forall x_1 \, \cdots \, \forall x_n \, \exists! y \; (x_1, x_2, \cdots, x_n) \in \mathcal{G}_f$. La théorie des ensembles permet donc de travailler au 1^{er} ordre tout en manipulant les objets d'ordre second comme les relations ou les fonctions. Par ailleurs, son pouvoir expressif lui permet de fonder les mathématiques et au-delà de formuler l'intégralité de toutes les sciences.

Tout n'est pas rose cependant. Au cœur de la théorie des ensembles de Zermelo-Fraenkel (notée ZF) se cache à nouveau le second théorème d'incomplétude de Gödel, cette fois-ci appliqué à cette théorie même et non à l'arithmétique. En effet, si ZF est une théorie consistante [8], alors $ZF \nvdash_c cons(ZF)$.

Pour aller plus avant :

Le lecteur qui souhaiterait en savoir plus sur la logique du second ordre est invité à consulter *"A mathematical introduction to logic"* de Herbert B. Enderton [End72], *"Computability and logic"* de George S. Boolos , John P. Burgess et Richard C. Jeffrey [BBJ02] ou encore le chapitre consacré à cette logique dans *"Logic and structure"* de Dirk van Dalen [vD97]. Enfin, sera d'un intérêt certain pour le lecteur philosophe : *"To be is to be a value of a variable (or to be some values of some variables)"* de George S. Boolos [Boo84].

Pour une lecture approfondie, nous renvoyons aux ouvrages *"Extensions of first order logic"* de María Manzano [Man96], *"Foundations without Foundationalism : A Case for Second-Order Logic"* de Stewart Shapiro [Sha91], ainsi que l'excellent article de Jouko Väänänen : *"Second-order logic and foundations of mathematics"* [Vää01].

Le lecteur avide de paradoxes – tels que le paradoxe de Russell – est invité à consulter : *"Saving truth from paradox"* de Hartry H. Field [Fie08] ou bien *"La logique un aiguillon pour la pensée"* de Jean-Paul Delahaye [Del12].

Le lecteur qui souhaiterait dépasser la très maigre introduction à la théorie des ensembles de Zermelo-Fraenkel présentée dans ce chapitre est invité à consulter : en français le livre *"Théorie des ensembles"* de Jean-Louis Krivine [Kri07] plutôt que *"Théorie des ensembles"* de Nicolas Bourbaki [Bou70]. En anglais, on conseillera *"Elements of set theory"* de Herbert B. Enderton [End77], *"Basic set theory"* de Azriel Levy [Lev12], *"Notes on set theory"* de Yannis N Moschovakis [Mos94], *"Basic set theory"* de Alexander Shen et Nikolai K Vereshchagin [SV02], *"Introduction to Set Theory"* de Karel Hrbacek et Thomas Jech [HJ99], *"Foundations of set theory"* de Abraham A. Fraenkel, Yehoshua Bar-Hillel et Azriel Levy [FBHL73] ou encore les très accessibles *"Philosophical Devices : Proofs, Probabilities, Possibilities, and Sets"* de David Papineau [Pap12], *"Set Theory and its Philosophy : A Critical Introduction : A Critical Introduction"* de Michael Potter [Pot04] et *"Set theory and the continuum problem"* de Raymond M. Smullyan et Melvin Fitting [SF96]

Les ouvrages qui suivent sont plus conséquents ; néanmoins, les lecteurs avisés y glanerons quelques idées fortes, ne serait-ce qu'à la lecture de préfaces ou préambules : *"Set theory : the third millennium edition"* de Thomas Jech [Jec03], *"Set theory"* de Kenneth Kunen [Kun11], *"A Course on Set Theory"* de Ernest Schimmerling [Sch11], *"Classic Set Theory : For Guided Independent Study"* de Derek C. Goldrei [Gol96], *"Discovering Modern Set Theory : Set-theoretic tools for every mathematician. 2"* de Winfried Just et Martin Weese [JW97], *"Set theory with a universal set : exploring an untyped universe"* de Thomas E. Forster [For95] et *"Sets for mathematics"* de F. William Lawvere et Robert Rosebrugh [LR03].

8. Si elle ne l'est pas, alors il ne reste plus qu'à rentrer chez soi.

Les lecteurs troublés par l'axiome du Choix pourront lire avec profit le livre *"Axiom of choice"* de Horst Herrlich [Her06] ou bien celui de Thomas Jech, *"The axiom of choice"* [Jec08]. Ceux désorientés par les différents infinis se plongeront avec délices dans l'introduction de *"The higher infinite : large cardinals in set theory from their beginnings"* de Akihiro Kanamori [Kan08].

Pour une approche historique de la théorie des ensembles, nous suggérons *"The mathematical development of set theory from Cantor to Cohen"* de Akihiro Kanamori [Kan96] et *"Labyrinth of thought : A history of set theory and its role in modern mathematics"* de Josâe Ferreirâos Domâinguez [Dom07].

Pour les quelques lecteurs intrigués par le problème des fondements, mentionnons qu'il existe une alternative à l'approche ensembliste et à la logique du 1er ordre : la théorie des catégories. A ces lecteurs, nous conseillons de picorer diverses informations dans les ouvrages suivants : *"Topoi : the categorial analysis of logic"* de Robert Goldblatt [Gol06], *"An introduction to category theory"* de Harold Simmons [Sim11], *"Elementary categories, elementary toposes"* de Colin McLarty [McL92], *"Category theory"* de Steve Awodey [Awo06], *"Conceptual mathematics : a first introduction to categories"* de F. William Lawvere et Stephen H. Schanuel [LS09] et l'excellent *"Categories for the working mathematician"* de Saunders Mac Lane [ML98].

Chapitre 17

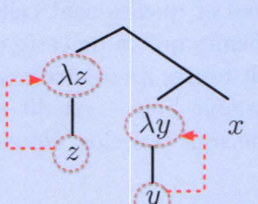
Correspondance preuves-programmes

1 Le λ-calcul

***Résumé* № 68** *Le λ-calcul est un formalisme représentant les fonctions calculables. Les objets s'appellent des λ-*termes *et sont définis par :*

- *chaque variable x est un λ-terme ;*
- *si t est un λ-terme et x une variable, alors λxt est un λ-terme ;*
- *si t, u sont des λ-termes, alors $(t)u$ est un λ-terme.*

Chaque terme possède une représentation arborescente :



$$= \quad (\lambda zz)(\lambda yy)x$$

Le caractère calculatoire est généré par la réduction :

$$(\lambda xt)u \rightsquigarrow t[u/x].$$

※

Tout au long de cet ouvrage nous avons considéré différents systèmes de preuves : les systèmes axiomatiques *à la Hilbert*, la Déduction Naturelle, le Calcul des Séquents. L'idée de la correspondance preuves-programmes est que derrière chaque système de preuve se cache un modèle de calcul. De sorte qu'à chaque preuve, on puisse associer un programme, mais également qu'à chaque programme de ce modèle de calcul particulier, on puisse aussi associer une preuve. Ainsi, plutôt que de la *"correspondance" preuves-programmes*, on parle volontiers de l'*"isomorphisme" preuves-programmes* ou de l'*isomorphisme de Curry-Howard* en référence aux deux découvreurs de cette correspondance dans le cadre intuitionniste.

Il n'y a donc pas une unique correspondance preuves-programmes qui associerait à chaque programme informatique une preuve et *vis-versa*, mais à différents systèmes de preuves correspondent différentes classes de programmes. Ces classes de programmes sont généralement définies par des *systèmes de typage* du lambda calcul.

Le *lambda calcul* – noté λ-calcul – réside au cœur de la sphère calculatoire. C'est un formalisme développé par Alonzo Church au début des années 1930 pour caractériser les fonctions récursives, autrement dit les fonctions calculables. Si en théorie des ensembles tout n'est qu'ensemble – les éléments des ensembles étant eux-mêmes des ensembles – en λ-calcul tout n'est que fonction : les *termes* du λ-calcul sont des fonctions dont les arguments sont eux-mêmes des fonctions et les valeurs qu'elles calculent sont elles-mêmes des fonctions également. En ce sens, le λ-calcul constitue un langage de programmation de très bas niveau (proche de la machine), difficilement maniable pour des utilisations mais très pratique comme langage de programmation théorique, surtout si l'on souhaite réfléchir à ce qu'est la programmation informatique.

Les objets du λ-calcul s'appellent des λ-*termes*. Ils sont définis par récurrence à partir des objets de base que sont les variables, à l'aide de deux opérations dont la première crée une fonction à partir d'une expression et la seconde "applique" cette fonction à une première.

Définition 498 *Les termes du λ-calcul (les λ-termes) sont définis par :*

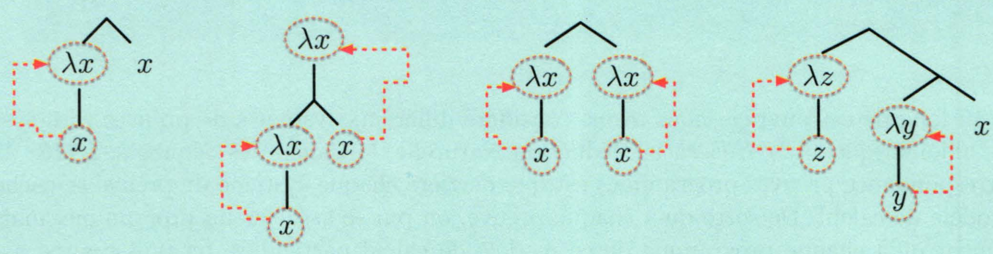
(variable) *chaque variable $x, y, z, \ldots$ est un λ-terme ;*

(λ-abstraction) *si t est un λ-terme et x une variable, alors λxt est un λ-terme ;*

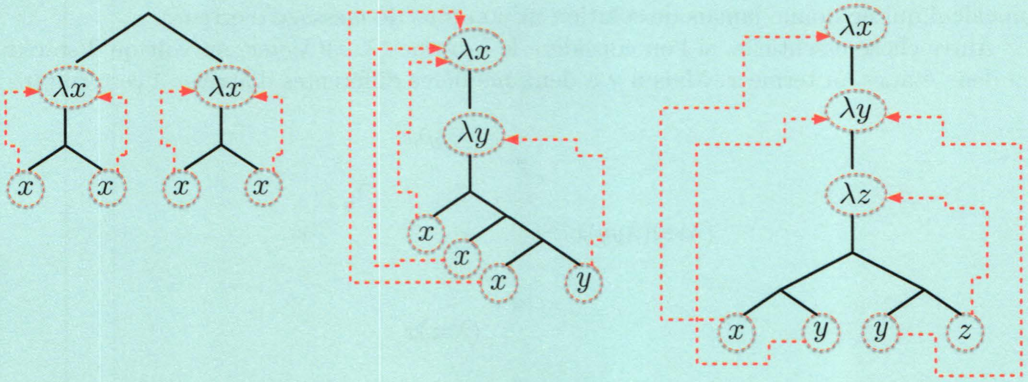
(application) *si t, u sont des λ-termes, alors $(t)u$ est un λ-terme.*

A cette construction sous forme linéaire des termes du λ-calcul correspond une représentation sous forme d'arbre. Les feuilles de ces arbres sont les *variables*, la λ-*abstraction* et l'*application* correspondent respectivement à un quantificateur portant sur une variable et un connecteur binaire. Cette représentation en arbre permet aussi aisément de définir quelles sont les occurrences des variables qui sont liées et quelles sont celles qui sont libres : une occurrence de la variable x est liée si sur le chemin qui va de cette occurrence à la racine se trouve λx, sinon elle est libre. Un λ-terme dont toutes les occurrences de toutes ses variables sont liées – autrement dit qui n'a aucune variable libre – est dit *clos*. Dans l'exemple qui suit, seuls le premier et le quatrième terme ne sont pas clos. Nous nous restreindrons plus tard aux seuls termes clos.

Exemple 499 : Ci-dessous des λ-termes sous forme arborescente et linéaire. Les occurrences liées des variables ainsi que la nature de leurs liaisons sont indiquées en rouge.



$(\lambda xx)x$ $\quad\quad$ $\lambda x(\lambda xx)x$ $\quad\quad$ $(\lambda xx)\lambda xx$ $\quad\quad$ $(\lambda zz)(\lambda yy)x$



$\big(\lambda x(x)x\big)\lambda x(x)x$ $\qquad$ $\lambda x\lambda y(x)(x)(x)y$ $\qquad$ $\lambda x\lambda y\lambda z\big((x)y\big)(y)z$

Lorsqu'on construit le λ-terme λxt, c'est un peu comme si l'on disait que t était une fonction qui dépend de x – donc de la forme $t(x)$ – que l'on pourra ensuite appliquer à un argument a pour obtenir la valeur $t(a)$. Mais contrairement à l'usage habituel des fonctions en mathématiques, où lorsqu'on applique une fonction à un argument on obtient une valeur et on s'arrête là, ici les fonctions ont un caractère opératoire et la valeur que l'on obtient étant elle-même une fonction, il se peut qu'il faille à son tour l'appliquer également, ce qui entraîne bien souvent une chaîne de modifications appelées *réductions*.

Une réduction d'un λ-terme en une étape revient à appliquer une fonction à un argument. Elle consiste à remplacer à l'intérieur de celui-ci toute partie de la forme $(\lambda xt)u$ par $t[u/x]$ [1]. On notera $v \rightsquigarrow w$ la réduction d'un terme v au terme w.

Exemple 500 Quelques exemples de réduction :

(1) $(\lambda yy)x \rightsquigarrow x$

(2) $(\lambda xx)x \rightsquigarrow x$

(3) $(\lambda xx)\lambda xx \rightsquigarrow \lambda xx$

(4) $(\lambda zz)(\lambda yy)x \rightsquigarrow (\lambda yy)x \rightsquigarrow x$

(5) $(\lambda zz)(\lambda yy)x \rightsquigarrow (\lambda zz)x \rightsquigarrow x$

(6) $\big(\lambda x(x)x\big)\lambda x(x)x \rightsquigarrow \big(\lambda x(x)x\big)\lambda x(x)x$

Si l'on excepte le cas (6), tous les autres λ-termes de l'Exemple 500 se réduisent ultimement en un λ-terme que l'on ne peut plus réduire. On dit que la réduction termine, cela correspond au calcul effectué par un programme qui effectivement s'arrête après un certain temps de calcul. Par contre, il n'est pas possible de trouver un λ-terme v tel que $\big(\lambda x(x)x\big)\lambda x(x)x \rightsquigarrow \cdots\cdots \rightsquigarrow v$ et tel que v ne puisse à nouveau plus se réduire. Le λ-terme

1. $t[u/x]$ désigne le terme obtenu en remplaçant dans le terme t chaque occurrence d'une variable libre x par le terme u. Le caractère libre ou non de l'occurrence d'une variable est défini de manière similaire à ce qui se passe dans la logique du 1[er] ordre. Ainsi, pour un terme v, les occurrences des variables libres de v sont : v si v est une variable, sinon, si v est de la forme λxt, ce sont toutes les occurrences des variables libres de t à l'exception de toutes celles de x, et si v est de la forme $(t)u$, ce sont toutes les occurences des variables libres de t plus celles de u.

$\big(\lambda x(x)x\big)\lambda x(x)x$ ne se réduit toujours qu'à lui-même. Cela correspond à un calcul sans fin : un calcul qui ne donne jamais de solution ni non plus de message d'erreur.

Autre chose essentielle, si l'on considère le λ-terme $(\lambda zz)(\lambda yy)x$, on voit qu'il se réduit en deux étapes au terme x. Mais il y a deux manières différentes d'arriver à ce résultat :

$$\begin{tikzcd}
 & (\lambda yy)x \arrow[dr, rightsquigarrow] & \\
(\lambda zz)(\lambda yy)x \arrow[ur, rightsquigarrow] \arrow[dr, rightsquigarrow] & & x \\
 & (\lambda zz)x \arrow[ur, rightsquigarrow] &
\end{tikzcd}$$

De plus, quelle que soit la manière dont on s'y prenne, les différentes suites de réductions aboutissent toujours au même résultat. Ce phénomène n'est pas un cas particulier. Bien au contraire, si l'on peut par une succession de réduction passer d'un premier λ-terme à un λ-terme ultime que l'on ne peut à son tour plus réduire, alors quelle que soit la manière dont on s'y prenne pour réduire ce premier terme, on arrivera toujours au même résultat. Autrement dit, si un chemin mène à un terme irréductible, alors tous les chemins mènent à ce même terme.

Bien sûr, tous les chemins ne mènent pas nécessairement à un terme irréductible : comme nous l'avons vu, le terme $\big(\lambda x(x)x\big)\lambda x(x)x$ ne se réduit jamais qu'à lui-même, ce qui fait que le seul chemin de réduction que l'on obtienne est celui répétant le même terme à l'infini.

$$\big(\lambda x(x)x\big)\lambda x(x)x \rightsquigarrow \big(\lambda x(x)x\big)\lambda x(x)x \rightsquigarrow \cdots\cdots\cdots \rightsquigarrow \big(\lambda x(x)x\big)\lambda x(x)x \rightsquigarrow \cdots\cdots\cdots$$

La relation entre termes du λ-calcul et programme informatique est la suivante : un programme peut être vu comme une fonction qui prend une valeur en *entrée*, puis procède à un calcul pour soit terminer et rendre une valeur en *sortie*, soit ne jamais terminer du tout. Un programme est donc une sorte de fonction partielle [2]. Insistons à nouveau sur le fait qu'à l'intérieur du λ-calcul, il n'y a que des λ-termes : un programme est un λ-terme "p", la valeur en *entrée* est également un λ-terme "e" et l'*exécution* du programme doté de cette valeur n'est autre que le processus de *réduction* du terme "$(p)e$" : si ce processus se termine $(p)e \rightsquigarrow \cdots\cdots \rightsquigarrow s$, un unique terme irréductible "s" est alors atteint et constitue la valeur de *sortie*. Si au contraire le processus de réduction ne s'arrête jamais, alors cela correspond à l'exécution d'un programme qui ne termine pas.

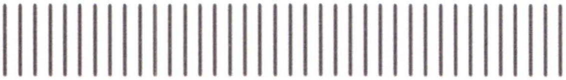
Il est étonnant d'imaginer qu'aux vues de l'extrême indigence de ses moyens, le λ-calcul réussisse à formaliser le fonctionnement de l'informatique toute entière. C'est pourtant bien le cas. Un programme quel qu'il soit peut toujours être représenté sous forme d'un λ-terme : le programme du pilote automatique d'un avion de ligne qui comporte 5 millions de lignes de code peut être intégralement décrit sous la forme d'un λ-terme – un peu long et compliqué mais toujours uniquement basé sur les deux seules opérations que sont l'application et la λ-abstraction.

Bien sûr, il faut faire l'effort de *représenter* au sein de ce formalisme les objets naturels du monde informatique. A commencer par les entiers et les opérations de base que sont l'addition et la multiplication. Si l'on y songe, nous ne nous donnons jamais des entiers sans les représenter sous une certaine forme. Le plus généralement, nous utilisons la représentation

2. Une fonction est partielle si elle n'est pas partout définie. La fonction : $x \longrightarrow \frac{1}{x}$ est partielle, puisqu'elle n'est pas définie en 0.

en base 10 : nous écrivons par exemple “38”. Mais nous pouvons également utiliser une représentation en base 2 et écrire “100110”, ou une notation ensembliste comme indiquée dans l’Exemple 496, ou encore celle indiquée ci-dessous :

Ou également une notation unaire correspondant à se donner trente-huit cure-dents :



En λ-calcul, classiquement les entiers sont représentés par les *“entiers de Church”*. L’idée est que puisque les termes représentent des fonctions, quoi de plus naturel si l’entier “1” est représenté par une fonction f que de représenter l’entier 38 par la fonction $\underbrace{f \circ f \circ f \circ \cdots \circ f}_{38}$?

Ce n’est pas spécialement joli mais c’est très simple.

En guise d’amuse-bouche, l’exemple qui suit montre comment les nombres entiers naturels ainsi que l’addition peuvent être représentés en λ-calcul.

Exemple 501 : Représentation des entiers et de l’addition en λ-calcul.

(1) Chaque entier est représenté par un terme dénommé *entier de Church*. Ainsi l’entier n est représenté par le terme :

$$\mathbf{n} = \lambda x \lambda y \underbrace{(x)(x)\cdots(x)}_{n}\, y.$$

(2) La fonction successeur est représentée par le terme :

$$\mathbf{succ} = \lambda x \lambda y \lambda z\big((x)y\big)(y)z.$$

(3) Si l’on applique ce terme à l’entier de Church $\mathbf{2}$, on obtient le terme $(\mathbf{succ})\mathbf{2}$ suivant[3] :

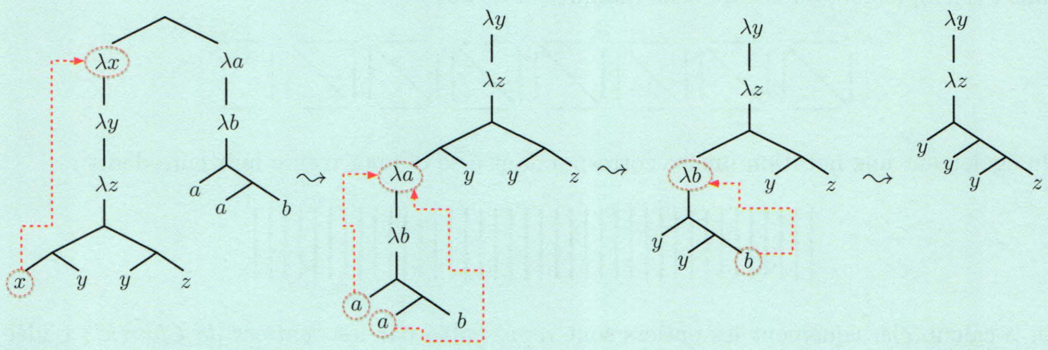
$$(\mathbf{succ})\mathbf{2} = \Big(\lambda x \lambda y \lambda z\big((x)y\big)(y)z\Big)\lambda a \lambda b(a)(a)b.$$

Ce terme se réduit à l’entier de Church $\mathbf{3}$:

$$\begin{aligned}(\mathbf{succ})\mathbf{2} = \Big(\lambda x \lambda y \lambda z\big((x)y\big)(y)z\Big)\lambda a \lambda b(a)(a)b \;&\rightsquigarrow\; \lambda y \lambda z\Big(\big(\lambda a \lambda b(a)(a)b\big)y\Big)(y)z \\ &\rightsquigarrow\; \lambda y \lambda z\Big(\lambda b(y)(y)b\Big)(y)z \\ &\rightsquigarrow\; \lambda y \lambda z(y)(y)(y)z \qquad = \mathbf{3}.\end{aligned}$$

3. Pour cela, nous avons renommé les variables de l’entier de Church 2 qui de $\lambda x \lambda y(x)(x)y$ est devenu : $\lambda a \lambda b(a)(a)b$.

Cette même suite de réductions de (**succ**)**2** à **3** sous forme arborescente :



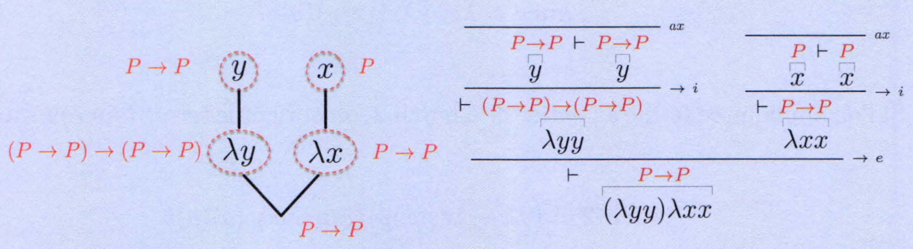
2 Le λ-calcul simplement typé

Résumé № 69 *Les termes du λ-calcul représentent toutes les fonctions calculables. Pour se limiter à celles dont les calculs terminent, on introduit le* typage *des termes. Les types simples sont des formules du Calcul Propositionnel avec "$\longrightarrow$" pour seul connecteur.*

Les termes typables sont définis par :

- *une variable x est un λ-terme de typle ϕ ;*
- *si t est un λ-terme de type ψ et x est un terme de type ϕ, alors λxt est un λ-terme de type $\phi \to \psi$;*
- *si t, u sont des λ-termes de types respectifs $\phi \to \psi$ et ϕ, alors $(t)u$ est un λ-terme de type ψ.*

Il y a une correspondance étroite entre un λ-terme typé et la preuve de son type.



Cette correspondance preuves-programmes s'étend bien au-delà, en particulier à la logique classique du 1er ordre, et incorpore toute la théorie des ensembles.

※

Si l'on veut se doter d'une correspondance entre preuves et programmes, il nous faut nous restreindre aux programmes dont l'exécution termine. Cela est rendu nécessaire par le fait qu'une preuve n'est jamais qu'un objet fini. Dès lors, puisqu'un calcul associé à un λ-terme n'est autre que la série des réductions qu'il génère, il est nécessaire de trouver un moyen de nous restreindre aux seuls λ-termes dont la réduction s'achève. Le moyen employé pour arriver à cette fin s'appelle le "*typage*" du λ-calcul. Pour reprendre les mots de Jean-Yves Girard : le *typage* "est une forme de *surmoi* interdisant certaines formes d'*inceste* logique..." [Gir06]. C'est comme un chapeau dont on affuble certains termes afin de mieux contrôler leurs faits et gestes. Le but est de ne typer que des termes correspondant à des programmes dont l'exécution termine. Cela limite donc la formation des termes aux seuls termes capables d'être dotés d'un type. Ainsi, les règles de formation des λ-termes sont maintenant contraintes par le système de typage considéré : on parle alors de *λ-calcul typé*.

La forme la plus rudimentaire du typage du λ-calcul est construite sur la seule implication à partir de variables propositionnelles – tiens tiens... un peu comme en Calcul Propositionnel, un système preuve à la Hilbert. Cette forme rudimentaire de typage produit le "*λ-calcul simplement typé*". Un type est donc une formule du Calcul Propositionnel réduit au seul connecteur "$\longrightarrow$". La manière dont on associe un type à un λ-terme s'effectue lors de la construction de celui-ci. Plus exactement, la construction des termes du λ-calcul est soumise à la coercition du type : à chaque étape de l'édification, un type doit être associé, sinon rien. Un type est donc une espèce de décoration nécessaire sans laquelle un terme ne peut voir le jour. L'idée et qu'un terme t du λ-calcul ne désigne par seulement une simple fonction, mais une fonction... *d'un certain type précisément*. Et lorsqu'on applique cette fonction, par exemple lorsque nous construisons un type de la forme $(t)u$, nous voulons que le type de u respecte celui des arguments de la fonction t. Ainsi, si le type de t désigne une fonction des entiers dans les entiers, alors le type de u doit être celui d'un entier ; par contre si le type de t désigne cette fois une fonction qui prend comme argument des fonctions des entiers dans les entiers et rend des entiers, alors le type de u ne doit pas être un entier, mais bien une fonction des entiers dans les entiers. Les règles de construction des termes simplement typés sont les suivantes[4] :

Définition 502 *On admet que ϕ et ψ dénotent des formules quelconques du Calcul Propositionnel ne contenant pas d'autres connecteur que "$\longrightarrow$" correspondant respectivement aux type ϕ et ψ.*

Les termes du λ-calcul simplement typé sont alors définis par :

variable *une variable $\overbrace{x}^{\phi}$ est un λ-terme de type ϕ ;*

λ-abstraction *si $\overbrace{t}^{\psi}$ est un λ-terme de type ψ et $\overbrace{x}^{\phi}$ est un terme de type ϕ, alors $\overbrace{\lambda xt}^{\phi\to\psi}$ est un λ-terme de type $\phi \to \psi$;*

application *si $\overbrace{t}^{\phi\to\psi}$, $\overbrace{u}^{\phi}$ sont des λ-termes de types respectifs $\phi \to \psi$ et ϕ, alors $\overbrace{(t)u}^{\psi}$ est un λ-terme de type ψ.*

Il est à noter qu'un terme ne possède pas un unique typage. Il peut être typable de mille et une manières comme on le verra dans l'Exemple qui suit. Mais ce qui importe est que nous ne conservons maintenant que les seuls termes qui admettent un typage et nous rejetons les autres : *"pas de survie sans typage !"*

4. ϕ et ψ désignent des formules du Calcul Propositionnel ne contenant aucun autre connecteur que la simple implication.

Exemple 503

(1) le λ-terme $(\lambda yy)x$ admet un typage : si P est une variable propositionnelle, considérons :

$\circ\ \overbrace{x}^{P}$ $\qquad\circ\ \overbrace{y}^{P}$ $\qquad\circ\ \overbrace{\lambda yy}^{P\to P}$

d'où l'on obtient :

$$\overbrace{(\lambda yy)x}^{P}.$$

(2) le même λ-terme que précédemment admet un typage différent : si P, Q sont des variables propositionnelles, considérons :

$\circ\ \overbrace{x}^{P\to Q}$ $\qquad\circ\ \overbrace{y}^{P\to Q}$ $\qquad\circ\ \overbrace{\lambda yy}^{(P\to Q)\to(P\to Q)}$

d'où l'on obtient :

$$\overbrace{(\lambda yy)x}^{P\to Q}.$$

(3) le λ-terme $(\lambda yy)\lambda xx$ admet un typage : si P est une variable propositionnelle, considérons :

$\circ\ \overbrace{x}^{P}$ $\qquad\circ\ \overbrace{y}^{P\to P}$ $\qquad\circ\ \overbrace{\lambda xx}^{P\to P}$ $\qquad\circ\ \overbrace{\lambda yy}^{(P\to P)\to(P\to P)}$

d'où l'on obtient :

$$\overbrace{(\lambda yy)\lambda xx}^{P\to P}.$$

(4) le λ-terme $(\lambda zz)(\lambda yy)x$ admet un typage : si P est une variable propositionnelle, considérons :

$\circ\ \overbrace{x}^{P}$ $\qquad\circ\ \overbrace{y}^{P}$ $\qquad\circ\ \overbrace{z}^{P}$ $\qquad\circ\ \overbrace{\lambda yy}^{P\to P}$ $\qquad\circ\ \overbrace{\lambda zz}^{P\to P}$ $\qquad\circ\ \overbrace{(\lambda yy)x}^{P}$

d'où l'on obtient :

$$\overbrace{(\lambda zz)(\lambda yy)x}^{P}.$$

(5) L'*entier de Church* $\mathbf{2} = \lambda x\lambda y(x)(x)y$ admet un typage :

$\circ\ \overbrace{x}^{P\to P}$ $\qquad\circ\ \overbrace{y}^{P}$ $\qquad\circ\ \overbrace{(x)y}^{P}$ $\qquad\circ\ \overbrace{(x)(x)y}^{P}$ $\qquad\circ\ \overbrace{\lambda y(x)(x)y}^{P\to P}$

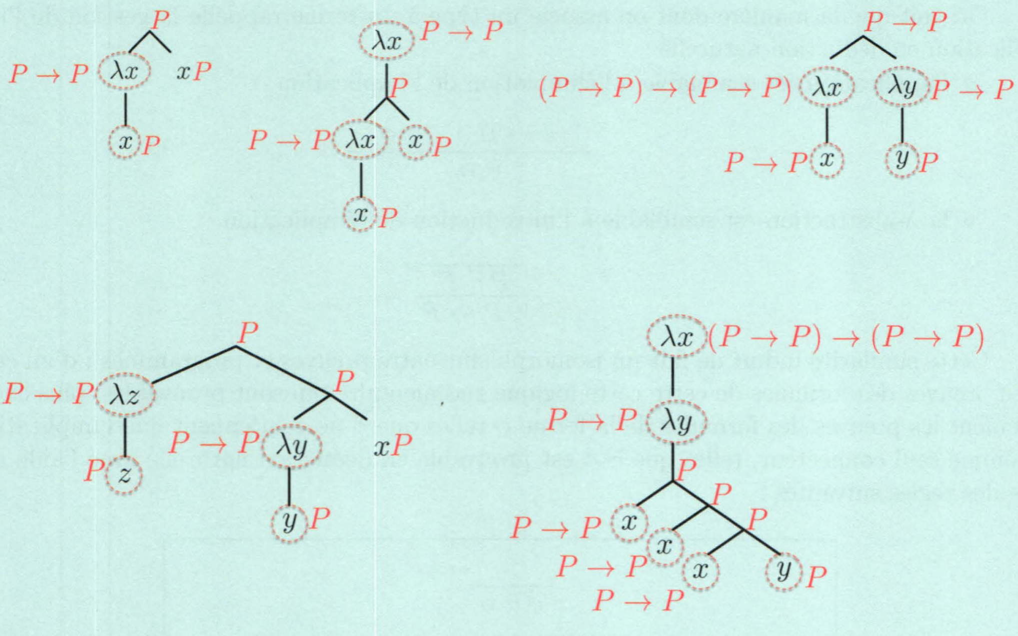
d'où l'on obtient :

$$\overbrace{\lambda x\lambda y(x)(x)y}^{(P\to P)\to(P\to P)}.$$

(6) le λ-terme $(\lambda x(x)x)\lambda x(x)x$ par contre n'admet pas de typage.

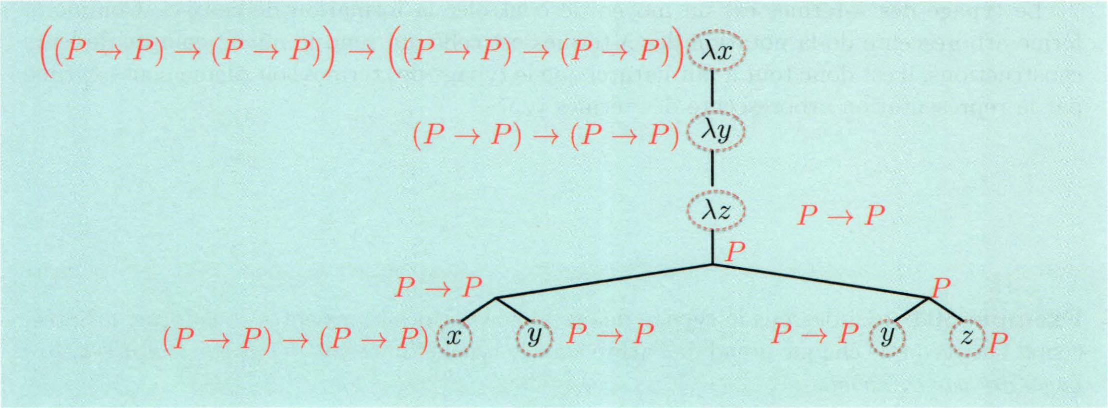
Le typage des λ-termes est un moyen de contrôler la formation de ceux-ci. Comme la forme arborescente de la notation des λ-termes est celle qui rend le mieux compte de leurs constructions, il est donc tout à fait naturel que le typage des termes soit pleinement exprimé par la représentation arborescente des termes typés.

Exemple 504 : Ci-dessous le typage de certains λ-termes représentés sous forme arborescente. On accouple chaque nœud de l'arbre avec le typage du *terme défini par le* ***sous-arbre*** *engendré par ce nœud.*



Il est à noter que le typage d'un terme est entièrement déterminé par le typage de ces variables. En effet, une fois que chacune des feuilles de l'arbre est pourvue d'un type fixé, celui de l'arbre tout entier se résout en partant des feuilles et remontant à la racine. Exactement comme lorsque disposant du squelette d'une preuve d'une part et des axiomes d'autre part, on pouvait aisément remplir tout le cadre de cette preuve.

On remarquera qu'un entier de Church quelconque – ci-dessus l'entier **3**– peut être typé par $P \to P$. Si l'on pose maintenant $\mathbb{N} = (P \to P) \to (P \to P)$, $\mathbb{N}$ devient le type (l'un des types parmi d'autres possible en fait) des entiers de Church . On voit alors qu'avec cette convention, la fonction **succ** (ci-dessous) admet précisément $\mathbb{N} \to \mathbb{N}$ comme typage c'est-à-dire $\big((P \to P) \to (P \to P)\big) \to \big((P \to P) \to (P \to P)\big)$. Autrement dit, le type de **succ** étant $\mathbb{N} \to \mathbb{N}$, ce terme ne peut qu'être appliqué à un terme de type $\mathbb{N}$ ce qui donnera au final un terme lui aussi de type $\mathbb{N}$. Le type de **succ** est donc celui d'une fonction qui ne prend comme argument que des entiers et ne retourne que des entiers : c'est donc précisément le type d'une fonction des entiers dans les entiers.



On voit que la manière dont on associe un type à un terme rappelle la gestion de l'implication en déduction naturelle :

- l'application est semblable à l'élimination de l'implication :

$$\frac{\vdash \phi \to \psi \qquad \vdash \phi}{\vdash \psi}\ {\scriptstyle \to e}$$

- la λ-abstraction est semblable à l'introduction de l'implication :

$$\frac{\dfrac{}{P \vdash P}\ {\scriptstyle ax}}{\vdash P \to P}\ {\scriptstyle \to i}$$

Cette similarité induit de fait un isomorphisme entre preuves et programmes : d'un coté les preuves des formules de cette cette logique rudimentaire qui sont prouvables, plus exactement les preuves des formules de la forme ϕ telles que ϕ ne contiennent que l'implication comme seul connecteur, telles que $\vdash \phi$ est prouvable en déduction naturelle avec l'aide des seules règles suivantes :

$$\frac{}{\phi \vdash \phi}\ {\scriptstyle ax}$$

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\ {\scriptstyle \to i} \qquad \frac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\ {\scriptstyle \to e}$$

$$\frac{\Gamma \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle aff} \qquad \frac{\Gamma, \phi, \phi \vdash \psi}{\Gamma, \phi \vdash \psi}\ {\scriptstyle ctr}$$

Et de l'autre coté, ceux parmi les λ-termes simplement typés qui sont *clos*. Ainsi les formules prouvables de cette logique – en logique minimale [5] – correspondent très précisément aux types des *termes clos* *"typables"* du λ-calcul. Regardons plus précisément comment ça marche.

5. On appelle cette logique la *logique implicative minimale*.

Preuve ⇒ λ-terme clos typé Modulo les règles d'*affaiblissement* et de *contraction*, on fait correspondre à chaque preuve $\vdash_m \phi$, un λ-terme clos dont le type est ϕ[6].

- Les *axiomes* correspondent aux feuilles du λ-terme, autrement dit à ses variables :

$$\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax} \qquad \longmapsto \qquad \dfrac{}{\overset{P}{x} \vdash \overset{P}{x}}\,{\scriptstyle ax}$$

- L'*élimination* de l'implication correspond à l'*application* :

$$\dfrac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \phi}\,{\scriptstyle \to e} \qquad \longmapsto \qquad \dfrac{\overset{\gamma_0}{x_0}, \cdots, \overset{\gamma_k}{x_k} \vdash \overset{\phi\to\psi}{t} \qquad \overset{\gamma'_0}{y_0}, \cdots, \overset{\gamma'_n}{y_n} \vdash \overset{\phi}{u}}{\overset{\gamma_0}{x_0}, \cdots, \overset{\gamma_k}{x_k}, \overset{\gamma'_0}{y_0}, \cdots, \overset{\gamma'_k}{y_n} \vdash \overset{\psi}{(t)u}}\,{\scriptstyle \to e}$$

où Γ, Γ' représentent respectivement les ensembles de formules $\{\gamma_0, \cdots, \gamma_k\}$ et $\{\gamma'_0, \cdots, \gamma'_n\}$.

- L'*introduction* de l'implication correspond à la *λ-abstraction* :

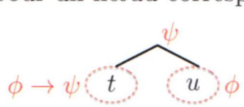
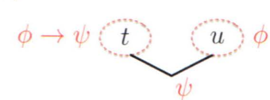
$$\dfrac{\Gamma, \phi \vdash \psi}{\Gamma \vdash \phi \to \psi}\,{\scriptstyle ax} \qquad \longmapsto \qquad \dfrac{\overset{\gamma_0}{x_0}, \cdots, \overset{\gamma_k}{x_k}, \overset{\phi}{x} \vdash \overset{\psi}{t}}{\overset{\gamma_0}{x_0}, \cdots, \overset{\gamma_k}{x_k} \vdash \overset{\phi\to\psi}{\lambda x t}}\,{\scriptstyle ax}$$

où Γ représente l'ensemble de formules $\{\gamma_0, \cdots, \gamma_k\}$.

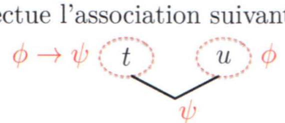
Cette méthode permet de faire correspondre à chaque preuve $\vdash_m \phi$ un λ-terme qui est d'une part clos par construction et d'autre part typable par ϕ. La démonstration rigoureuse de cela se fait par induction sur la hauteur de la preuve en question[7].

λ-terme clos typé ⇒ Preuve L'arbre que constitue le λ-terme donne lieu à l'arbre d'une preuve qui prouve précisément le type de ce terme. A chaque nœud de l'arbre du terme on substitue :

- à une *feuille* qui est une variable typée de la forme $\overset{\phi}{x}$, on associe $\dfrac{}{\phi \vdash \phi}\,{\scriptstyle ax}$
- pour un nœud correspondant à l'*application*, de la forme :


que l'on regarde la tête en bas :


on effectue l'association suivante :



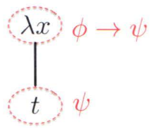
$$\longmapsto \qquad \dfrac{\Gamma \vdash \phi \to \psi \qquad \Gamma' \vdash \phi}{\Gamma, \Gamma' \vdash \psi}\,{\scriptstyle \to e}$$

dans lequel les ensembles finis de formules Γ et Γ' représentent respectivement l'ensemble des types des variables libres de t et l'ensemble des types des variables libres de u.

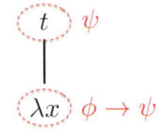
6. Et plus généralement à une preuve avec hypothèses de la forme $\Gamma \vdash_m \phi$, un λ-terme t dont le type est ϕ et dont toutes les variables libres sont typées par des formules de Γ.

7. On montre qu'une preuve de $\Gamma \vdash \phi$ correspond à un λ-terme dont les variables libres sont toutes typées par des formules de Γ.

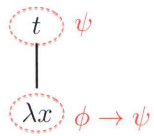
- pour un nœud correspondant à la λ-*abstraction*, de la forme :



que l'on regarde la tête en bas :



on effectue l'association suivante :



$$\longmapsto \quad \dfrac{\Gamma, \phi \ \vdash \ \psi}{\Gamma \ \vdash \ \phi \to \psi} \to_i$$

où ϕ est le type de la variable x et Γ est l'ensemble des types des variables libres du terme λxt.

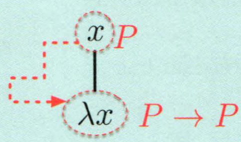
Modulo les règles d'*affaiblissement* et de *contraction*, ce processus permet de passer du terme à la preuve. Le fait que le terme dont on part soit clos, assure que la preuve de la formule que désigne le type de ce terme soit sans hypothèse.

Exemple 505

La preuve la plus simple du séquent $\vdash P \to P$ est :

$$\dfrac{\dfrac{}{P \vdash P}\, ax}{\vdash P \to P} \to_i$$

Le λ-terme clos typé associé à cette preuve, ainsi que les raisons de sa construction, sont indiqués ci-dessous. A noter que le λ-terme est représenté à l'envers (la tête en bas) pour mieux faire ressortir l'étroite relation entre le terme et la preuve.

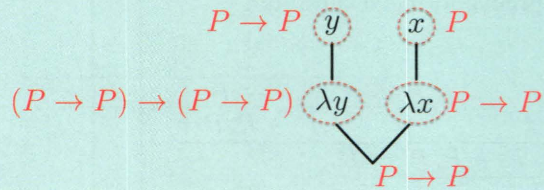


$$\dfrac{\dfrac{}{\underbrace{P}_{x} \vdash \underbrace{P}_{x}}\, ax}{\underbrace{\vdash P \to P}_{\lambda xx}} \to_i$$

Considérons maintenant une autre preuve de $\vdash P \to P$, clairement inutilement plus compliquée :

$$\dfrac{\dfrac{\dfrac{}{P \to P \vdash P \to P}\, ax}{\vdash (P \to P) \to (P \to P)} \to_i \quad \dfrac{\dfrac{}{P \vdash P}\, ax}{\vdash P \to P} \to_i}{P \to P} \to_e$$

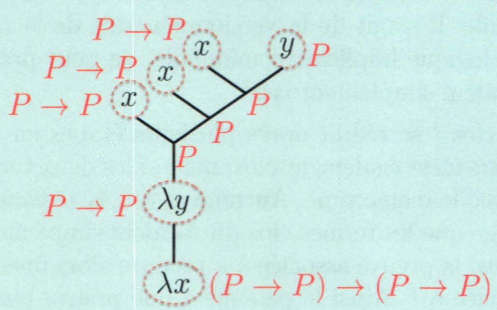
Le λ-terme clos typé associé – présenté à l'envers (la tête en bas) – ainsi que les raisons de sa construction se trouve ci-dessous :



$$\dfrac{\dfrac{\dfrac{}{\overset{P\to P}{y} \vdash \overset{P\to P}{y}}\,ax}{\vdash \overset{(P\to P)\to(P\to P)}{\lambda yy}}\to_i \qquad \dfrac{\dfrac{}{\overset{P}{x} \vdash \overset{P}{x}}\,ax}{\vdash \overset{P\to P}{\lambda xx}}\to_i}{\vdash \overset{P\to P}{(\lambda yy)\lambda xx}}\to_e$$

On peut remarquer dans l'exemple précédent que $\overset{P\to P}{(\lambda yy)\lambda xx}$ et $\overset{P\to P}{\lambda xx}$ sont deux λ-termes clos typés par la même formule $(P \to P)$ tels que le premier terme se réduit au second : $(\lambda yy)\lambda xx \rightsquigarrow \lambda xx$. Est-ce là quelque chose d'étonnant ? Et bien non, pas réellement, car si t est un terme clos typé par ϕ et $t \rightsquigarrow u$, alors u est également un terme clos typable par ϕ. En d'autres termes, la réduction préserve le typage[8].

Exemple 506 On associe cette fois au type d'un λ-terme clos une preuve de la formule que désigne ce type. Pour cela, commençons par écrire le terme la tête en bas. Ainsi $\mathbf{3} = \lambda x\lambda y(x)(x)(x)y$ est représenté sous forme d'arbre inversé avec le typage suivant :



La preuve induite par le typage de ce λ-terme clos est révélée ci-dessous :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\overset{P\to P}{x} \vdash \overset{P\to P}{x}}\,ax \qquad \dfrac{\dfrac{}{\overset{P\to P}{x} \vdash \overset{P\to P}{x}}\,ax \qquad \dfrac{\dfrac{}{\overset{P\to P}{x} \vdash \overset{P\to P}{x}}\,ax \quad \dfrac{}{\overset{P}{y} \vdash \overset{P}{y}}\,ax}{P\to P, P \vdash \overset{P}{(x)y}}\to_e}{P\to P, P \vdash \overset{P}{(x)(x)y}}\to_e}{P\to P, P \vdash \overset{P}{(x)(x)(x)y}}\to_e}{P\to P \vdash \overset{P\to P}{\lambda y(x)(x)(x)y}}\to_i}{\vdash \overset{(P\to P)\to(P\to P)}{\lambda x\lambda y(x)(x)(x)y}}\to_i$$

8. Si $\overset{\phi}{t}$ est clos et $t \rightsquigarrow u$ alors u est clos et $\overset{\phi}{u}$.

En éliminant les λ-termes, on obtient la preuve formelle suivante :

$$
\dfrac{\dfrac{\dfrac{}{P \to P \vdash P \to P}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{}{P \to P \vdash P \to P}\,{\scriptstyle ax} \qquad \dfrac{\dfrac{}{P \to P \vdash P \to P}\,{\scriptstyle ax} \quad \dfrac{}{P \vdash P}\,{\scriptstyle ax}}{P \to P, P \vdash P}\,{\scriptstyle \to e}}{P \to P, P \vdash P}\,{\scriptstyle \to e}}{\dfrac{P \to P, P \vdash P}{\dfrac{P \to P \vdash P \to P}{\vdash (P \to P) \to (P \to P)}\,{\scriptstyle \to i}}\,{\scriptstyle \to i}}\,{\scriptstyle \to e}
$$

Avant d'abandonner la version rudimentaire de la correspondance preuves-programmes que nous venons de présenter, relevons encore quelques conséquences de cette correspondance :

(1) Si pour toute variable propositionnelle P il existe un terme du λ-calcul qui soit typé par P[9], il n'existe par contre pas de terme *clos* dont le type soit P. En effet, si cela était le cas, nous en déduirions une preuve de $\vdash P$, ce qui contredirait le fait que ce séquent n'est pas prouvable.

(2) Il n'existe pas de terme clos du λ-calcul simplement typé dont le type soit de la forme $((\phi \to \psi) \to \phi) \to \phi$, car le séquent $\vdash ((\phi \to \psi) \to \phi) \to \phi$ n'est pas prouvable en logique minimale. Il s'agit de la version générale de la *loi de Peirce*, qui n'étant pas prouvable en logique implicative minimale, ne peut prétendre être le type d'un terme clos du λ-calcul simplement typé.

(3) Lorsqu'un terme clos t se réduit après plusieurs étapes en un terme u irréductible, alors non seulement u est également clos, mais si les deux termes t et u sont typables, alors ils le sont avec le même type. Autrement dit, la *réduction* conserve le type d'un terme. Si l'on songe que les termes clos du λ-calcul simplement typé correspondent à des démonstrations, la preuve associée à u procure alors une espèce de forme normale de la preuve associée à t. Ainsi le passage d'une preuve par la machine du λ-calcul typé est un moyen de lisser celle-ci, de la normaliser en quelque sorte.

Cette correspondance preuves-programmes s'étend bien au delà de la logique implicative minimale et du λ-calcul simplement typé. D'autres systèmes de typage permettent de passer de la logique implicative minimale à des logiques au pouvoir expressif beaucoup plus grand, comme le fragment intuitionniste du Calcul Propositionnel, et surtout au-delà du fragment intuitionniste de la logique du 1er ordre et de ceux d'autres logiques encore.

Notons que la logique intuitionniste étant constructive par nature, il est tout à fait naturel de penser qu'elle constitue le cadre indépassable à l'intérieur duquel progresse la correspondance preuves-programmes. Cela est tellement naturel que cette croyance fonctionna comme un dogme pendant de nombreuses années, jusqu'à ce qu'en 1990, Timothy Griffin montre qu'il n'en est rien et que la logique classique tombe bien également sous le coup de cette correspondance [Gri90].

Mieux que cela, chacun des axiomes de la théorie des ensembles – y compris l'axiome du choix ! – font maintenant partie de la correspondance preuves-programmes. Un peut ainsi associer un programme à toute preuve en mathématiques [Kri00]. Cela permet entre autre

9. Par exemple $\overset{P}{x}$.

de vérifier la validité d'une preuve avec la même facilité que l'on exécute un programme. Les outils qui rendent possible de regarder les preuves comme des programmes s'appellent des *assistants de preuves*. Avec leur aide, les démonstrations que rédigent les mathématiciens sont transcrites dans un langage formel pour être ensuite vérifiées de manière automatique. Dans l'autre sens, puisqu'on peut associer une preuve à de très nombreux programmes informatiques, cela permet également de pouvoir certifier certaines de leurs propriétés avant leur mise en application. Le but ultime étant tout simplement de disposer à la fois d'un programme et d'une *preuve* que ce programme effectue bien ce qu'on lui demande de faire.

Il est en effet tout à fait naïf de croire que pour écrire un programme correspondant à des spécifications précises, il suffit d'être rigoureux. Lorsqu'un programme est à la tête du fonctionnement d'un métro automatique, par exemple, et comporte des millions de lignes de code, il est nécessaire de *démontrer* qu'il ne commettra pas d'impairs à partir du moment où il sera mis en relation avec son environnement. Pour cela, des efforts d'attention et de concentration extrêmes ne suffisent tout simplement pas à embrasser la complexité de la totalité de la tâche : des moyens automatiques sont alors requis.

Plus récemment encore, la correspondance preuves-programmes est intégrée à un nouveau programme de fondation des mathématiques axé sur la correspondance entre un domaine des mathématiques ou plus exactement de la topologie algébrique : l'homotopie et la théorie des types telle qu'elle s'est développée autour du λ-calcul [Awo12]. Chose encore plus étonnante, cet intérêt n'est pas seulement de nature spéculative. Mais il est rendu nécessaire par le besoin croissant de devoir vérifier, par des moyens informatiques, les théorèmes toujours plus compliquées que découvrent les mathématiciens.

Pour aller plus avant :

Pour le lecteur qui souhaiterait dépasser la frêle initiation à l'isomorphisme de Curry-Howard que constitue ce chapitre, nous recommandons principalement les ouvrages suivants : *"Le point aveugle, tome 1 : vers la perfection"* de Jean-Yves Girard [Gir06] et *"Proofs and types"* du même auteur associé à Yves Lafont et traduit par Paul Taylor [GTL89]. Nous conseillons également le livre de Jean-Louis Krivine : *"Lambda-calcul, types et modèles"* [Kri90] ou son équivalent anglais *"Lambda-calculus, types and models"* [Kri93], *"Lectures on the Curry-Howard isomorphism"* de Morten Heine Sørensen et Pawel Urzyczyn [SU06], ainsi que le plus avancé *"Le point aveugle, tome 2 : vers l'imperfection"* de Jean-Yves Girard [Gir07].

Sont également d'intérêt : *"An introduction to substructural logics"* de Greg Restall [Res13], ainsi que les derniers chapitres de *"Structural proof theory"* de Sara Negri et Jan von Plato [NvP08].

Par ailleurs, le lecteur curieux des nouvelles tendances liant homologie et théorie des types lira avec intérêt *"Type theory and homotopy"* de Steve Awodey [Awo12].

Cinquième partie

Annexes

Chapitre 18

Une preuve du théorème de compacité par ultraproduit

Définition 507 (Filtre) *Soit E un ensemble non vide. Un sous-ensemble $\mathcal{F} \subset \mathcal{P}(E)$ est appelé filtre sur E s'il vérifie les points suivants :*
- $\emptyset \notin \mathcal{F}$;
- *si* $A, B \in \mathcal{F}$, *alors* $A \cap B \in \mathcal{F}$;
- *si* $A \in \mathcal{F}$ *et* $A \subset B$, *alors* $B \in \mathcal{F}$.

Intuitivement, un sous-ensemble de E est dans le filtre s'il est assez gros.
Soit E un ensemble et $A \subset E$. Alors, A est dit *cofini* si $E \setminus A$ est fini.

Exemple 508
- Soit $\emptyset \neq A \subset E$. Alors $\mathcal{F} = \{B \subset E : A \subset B\}$ est un filtre.
- Prenons $E = \mathbb{N}$ et $\mathcal{F} = \{A \subset \mathbb{N} : A \text{ est cofini}\}$. Alors F est un filtre. Il est appelé *filtre de Fréchet.*

Définition 509 (Base de filtre) *Soit E un ensemble non vide et $\mathcal{B} \subset \mathcal{P}(E)$. On dit que la collection $\mathcal{B}$ est une base de filtre si elle satisfait les deux conditions suivantes :*
- $\emptyset \notin \mathcal{B}$;
- *si* $A, B \in \mathcal{B}$, *alors* $A \cap B \in \mathcal{B}$.

Le filtre engendré par $\mathcal{B}$ est :

$$\mathcal{F} = \{B \subset E : \exists A \in \mathcal{B} \text{ tel que } A \subset B\}.$$

Il s'agit d'un filtre car :
- $\emptyset \notin \mathcal{F}$.
- *Si* $B, B' \in \mathcal{F}$, *alors il existe* $A, A' \in \mathcal{B}$ *tels que* $A \subset B$ *et* $A' \subset B'$. *Puisque* $A \cap A' \subset B \cap B'$ *et que* $A \cap A' \in \mathcal{B}$, *on a* $B \cap B' \in \mathcal{F}$.
- *Si* $B \in \mathcal{F}$ *et* $B \subset B'$, *alors il existe* $A \in \mathcal{B}$ *tel que* $A \subset B \subset B'$, *ce qui implique* $B' \in \mathcal{F}$.

Exemple 510 Soit I un ensemble non vide et E l'ensemble des parties finies de I. Pour $a \in E$, on définit :

$$E_a = \{b \in E : a \subset b\}.$$

Alors $\mathcal{B} = \{E_a : a \in E\}$ est une base de filtre sur E. Pour cela, vérifions les deux conditions :

- $\emptyset \notin \mathcal{B}$.
- Soient $E_a, E_b \in \mathcal{B}$, alors :

$$\begin{aligned} E_a \cap E_b &= \{c \in E : a \subset c\} \cap \{c \in E : b \subset c\} \\ &= \{c \in E : (a \cup b) \subset c\} \\ &= E_{a \cup b} \in \mathcal{B}. \end{aligned}$$

Définition 511 (Ultrafiltre) *Soit E un ensemble non vide. Un sous-ensemble $\mathcal{U} \subset \mathcal{P}(E)$ est appelé ultrafiltre sur E si :*

- *$\mathcal{U}$ est un filtre sur E ;*
- *pour tout $F \subset E$, on a $F \in \mathcal{U}$ ou $E \setminus F \in \mathcal{U}$ (c'est-à-dire, $\mathcal{U}$ est maximal, voir la preuve de la Remarque 515).*

Pour pouvoir étendre un filtre en un ultrafiltre, nous allons avoir besoin de nous munir de l'Axiome du Choix.

Axiome 1 (Axiome du Choix) *Soit $(A_i)_{i \in I}$, une collection d'ensembles telle que $A_i \neq \emptyset$ pour tout $i \in I$. Alors, il existe une fonction $f : I \longrightarrow \bigcup_{i \in I} A_i$ telle que $f(i) \in A_i$ pour tout $i \in I$.*

L'Axiome du Choix est lui-même équivalent au lemme de Zorn, que l'on énonce maintenant.

Définition 512 (Ensemble inductif) *Un ensemble partiellement ordonné $(X, \leq)$ est dit inductif si toute partie totalement ordonnée (que l'on nomme chaîne) de X admet au moins un majorant.*

Théorème 513 (Lemme de Zorn) *Tout ensemble ordonné inductif admet (au moins) un élément maximal.*

Lemme 514 *L'Axiome du Choix est équivalent au Lemme de Zorn.*

Axiome 2 (Axiome de l'ultrafiltre) *Tout filtre peut être étendu en un ultrafiltre.*

Remarque 515 L'Axiome du Choix implique l'axiome de l'ultrafiltre (mais la réciproque est fausse).

Preuve de la Remarque 515 : Soit $\mathcal{F}$ un filtre sur E. Considérons l'ensemble des filtres sur E qui étendent $\mathcal{F}$. Munis de l'inclusion, c'est un ordre partiel inductif. En effet, soit $(\mathcal{F}_i)_{i \in I}$ une chaîne de ce poset. Montrons que $\bigcup_{i \in I} \mathcal{F}_i$ est un filtre.

- Puisque $\emptyset \notin \mathcal{F}_i$ pour tout $i \in I$, alors $\emptyset \notin \bigcup_{i \in I} \mathcal{F}_i$.
- Soient $A, B \in \bigcup_{i \in I} \mathcal{F}_i$. Alors il existe $j_A, j_B \in I$ tels que $A \in \mathcal{F}_{j_A}, \mathcal{B} \in \mathcal{F}_{j_B}$. Or, $(\mathcal{F}_i)_{i \in I}$ est une chaîne et donc on peut supposer sans perte de généralité que l'on a $\mathcal{F}_{j_A} \subseteq \mathcal{F}_{j_B}$. Par conséquent, $A \cap B \in \mathcal{F}_{j_B} \subseteq \bigcup_{i \in I} \mathcal{F}_i$.
- Soient $A \in \bigcup_{i \in I} \mathcal{F}_i$ et $A \subset B$. Alors il existe $j \in I$ tel que $A \in \mathcal{F}_j$. Ceci implique que $\mathcal{B} \in F_j \subseteq \bigcup_{i \in I} \mathcal{F}_i$.

Par le lemme de Zorn (qui est équivalent à l'Axiome du Choix), nous obtenons l'existence d'un élément maximal de l'ordre partiel, notons le $\mathcal{U}$ et montrons que c'est un ultrafiltre. Soit S un sous-ensemble de E tel que $S \notin \mathcal{U}$, montrons que $E \setminus S \in \mathcal{U}$. Par maximalité de $\mathcal{U}$, l'ensemble $\mathcal{B} = \{S \cap A \mid A \in \mathcal{U}\} \cup \mathcal{U}$ n'est pas une base de filtre. En effet, une base de filtre est incluse dans le filtre qu'elle engendre, et en particulier, $S \in \mathcal{B}$ et $\mathcal{U} \subseteq \mathcal{B}$. Si $\mathcal{B}$ était une base de filtre, alors son filtre engendré serait une extension stricte de $\mathcal{U}$, une contradiction. Or, $\mathcal{B}$ vérifie par construction le deuxième axiome des bases de filtre, par conséquent il ne peut vérifier le premier. Il existe donc $\tilde{S} \in \mathcal{U}$ tel que $S \cap \tilde{S} = \emptyset$, c'est-à-dire $\tilde{S} \subseteq E \setminus S$. Autrement dit, $E \setminus S \in \mathcal{U}$.

$\dashv$ 515

1 Ultraproduit

Définition 516 (Ultraproduit) *Soient $\mathcal{L}$ un langage du 1er ordre, I un ensemble non vide, $(\mathcal{M}_i)_{i \in I}$ une famille de $\mathcal{L}$-structures et un ultrafiltre $\mathcal{U}$ sur I.*
L'ultraproduit $\mathcal{M}$ de la famille $(\mathcal{M}_i)_{i \in I}$ par l'ultrafiltre $\mathcal{U}$ est la $\mathcal{L}$-structure notée :

$$\mathcal{M} = \prod_{i \in I} \mathcal{M}_i \;/_{\mathcal{U}}.$$

On définit d'abord une relation d'équivalence $\sim$ sur $\prod_{i \in I} |\mathcal{M}_i|$ de la façon suivante :

$$(a_i)_{i \in I} \sim (b_i)_{i \in I} \iff \{i \in I \mid a_i = b_i\} \in \mathcal{U}.$$

On vérifie que c'est bien une relation d'équivalence :

Réflexivité *Pour tout $(a_i)_{i \in I} \in \prod_{i \in I} |\mathcal{M}_i|$, on a que $\{i \in I : a_i = a_i\} = I$. Or, $\emptyset \notin \mathcal{U}$ car $\mathcal{U}$ est un filtre. Par conséquent, puisque $\mathcal{U}$ est un ultrafiltre, $I \in \mathcal{U}$ et donc $(a_i)_{i \in I} \sim (a_i)_{i \in I}$.*

Symétrie *Immédiat.*

Transitivité *Si $(a_i)_{i \in I} \sim (b_i)_{i \in I}$ et $(b_i)_{i \in I} \sim (c_i)_{i \in I}$, alors*

$$\{i \in I : a_i = c_i\} \supseteq \{i \in I : a_i = b_i\} \cap \{i \in I : b_i = c_i\}.$$

Or, par hypothèse, $\{i \in I : a_i = b_i\} \in \mathcal{U}$ et $\{i \in I : b_i = c_i\} \in \mathcal{U}$. Puisque $\mathcal{U}$ est un filtre, $\{i \in I : a_i = b_i\} \cap \{i \in I : b_i = c_i\} \in \mathcal{U}$ et donc $\{i \in I : a_i = c_i\} \in \mathcal{U}$. C'est équivalent à dire $(a_i)_{i \in I} \sim (c_i)_{i \in I}$.

Maintenant, on pose :

- $|\mathcal{M}| = \prod_{i \in I} |\mathcal{M}_i| \;/\!\sim$;
- *pour tout symbole de constante c de $\mathcal{L}$,*

$$c^{\mathcal{M}} = [(c^{\mathcal{M}_i})_{i \in I}]_{\sim};$$

◦ *pour tout symbole de fonction f de $\mathcal{L}$,*

$$f^{\mathcal{M}}\left([(a_i^1)_{i\in I}]_\sim,\ldots,[(a_i^N)_{i\in I}]_\sim\right)=[(f^{\mathcal{M}_i}(a_i^1,\ldots,a_i^N))_{i\in I}]_\sim;$$

◦ *pour tout symbole de relation R de $\mathcal{L}$,*

$$\left([(a_i^1)_{i\in I}]_\sim,\ldots,[(a_i^N)_{i\in I}]_\sim\right)\in R^{\mathcal{M}}\iff\left\{i\in I\mid(a_i^1,\ldots a_i^N)\in R^{\mathcal{M}_i}\right\}\in\mathcal{U}.$$

On vérifie que tout ceci est bien défini. C'est-à-dire que si :

$$(a_i^1)_{i\in I}\sim(b_i^1)_{i\in I},\ldots,(a_i^N)_{i\in I}\sim(b_i^N)_{i\in I}$$

alors :

$$(f^{\mathcal{M}_i}(a_i^1,\ldots,a_i^N))_{i\in I}\sim(f^{\mathcal{M}_i}(b_i^1,\ldots,b_i^N))_{i\in I}$$

et :

$$\left\{i\in I\mid(a_i^1,\ldots,a_i^N)\in R^{\mathcal{M}_i}\right\}\in\mathcal{U}\iff\left\{i\in I\mid(b_i^1,\ldots,b_i^N)\in R^{\mathcal{M}_i}\right\}\in\mathcal{U}.$$

- *On vérifie d'abord la première partie :*

$$\left\{i\in I\mid f^{\mathcal{M}_i}(a_i^1,\ldots,a_i^N)=f^{\mathcal{M}_i}(b_i^1,\ldots,b_i^N)\right\}\supseteq\bigcap_{j=1}^N\left\{i\in I:a_i^j=b_i^j\right\}.$$

  Or, le deuxième membre est par hypothèse une intersection finie d'éléments de $\mathcal{U}$ et donc, par définition d'un filtre, c'est un élément de $\mathcal{U}$. Ainsi, le premier membre étend un élément de $\mathcal{U}$ et c'est par conséquent aussi un élément de $\mathcal{U}$. On a ainsi vérifié que :

$$(f^{\mathcal{M}_i}(a_i^1,\ldots,a_i^N))_{i\in I}\sim(f^{\mathcal{M}_i}(b_i^1,\ldots,b_i^N))_{i\in I}.$$

- *On s'occupe maintenant de la deuxième partie.*
  Posons $A=\left\{i\in I\mid(a_i^1,\ldots a_i^N)\in R^{\mathcal{M}_i}\right\}$ et $B=\bigcap_{j=1}^N\left\{i\in I:a_i^j=b_i^j\right\}$ et supposons que

$$\left\{i\in I\mid(a_i^1,\ldots,a_i^N)\in R^{\mathcal{M}_i}\right\}\in\mathcal{U}.$$

  Alors :

$$\left\{i\in I\mid(b_i^1,\ldots b_i^N)\in R^{\mathcal{M}_i}\right\}\supseteq A\cap B.$$

  Or par hypothèse, A et B sont dans $\mathcal{U}$ et de ce fait $A\cap B\in U$. Ainsi, le premier membre étend un élément de $\mathcal{U}$ et c'est donc aussi un élément de $\mathcal{U}$, par définition d'un filtre. Il suffit maintenant de constater que la situation est symétrique pour trouver l'implication inverse.

2 Le théorème de Łoś

Ce résultat est relativement récent puisqu'il date des années 1950 [Łoś55].

Théorème 517 (Théorème de Łoś) *Soit $\mathcal{L}$ un langage du 1^er^ ordre et I un ensemble non vide. Soient encore $(\mathcal{M}_i)_{i\in I}$ une famille de $\mathcal{L}$-structures, un ultrafiltre $\mathcal{U}$ sur I et Φ une formule dont les variables libres sont parmi $x_1,\ldots,x_n$ et $\alpha^1,\ldots,\alpha^n\in|\mathcal{M}|$.*
Alors, si α_i^j est la i-ème projection de α^j,

$$\mathcal{M}=\prod_{i\in I}\mathcal{M}_i\;/\mathcal{U}\models\Phi_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]}\iff\left\{i\in I\mid\mathcal{M}_i\models\Phi_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\}\in\mathcal{U}.$$

Preuve du Théorème 517 : Sans perte de généralité, on peut supposer que seuls $\neg$, $\wedge$ et $\exists$ apparaissent dans Φ. La démonstration se fait par induction sur la hauteur de Φ.

∘ Si $ht(\Phi) = 0$, alors il existe un entier naturel n et des termes $t_1, \ldots, t_n$ tels que $\Phi = R(t_1, \ldots, t_n)$. On obtient

$$\begin{aligned}
&\mathcal{M} \models \Phi_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]} \\
&\iff \left(t_1^{\mathcal{M}}{}_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]}, \ldots, t_n^{\mathcal{M}}{}_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]}\right) \in R^{\mathcal{M}} \\
&\iff \left\{i \in I \mid \left(t_1^{\mathcal{M}_i}{}_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}, \ldots, t_n^{\mathcal{M}_i}{}_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right) \in R^{\mathcal{M}_i}\right\} \in \mathcal{U} \\
&\iff \left\{i \in I \mid \mathcal{M}_i \models \Phi_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \in \mathcal{U}.
\end{aligned}$$

où l'on a utilisé la définition d'évaluation d'une formule dans la première et la troisième équivalence et celle de l'ultraproduit dans la deuxième équivalence.

∘ Si $ht(\Phi) > 0$:

- Si $\Phi = \neg\Psi$, alors :

$$\begin{aligned}
\mathcal{M} \models \Phi_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]} &\iff \mathcal{M} \not\models \Psi_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]} \\
&\iff \left\{i \in I \mid \mathcal{M}_i \models \Psi_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \notin \mathcal{U} \\
&\iff \left\{i \in I \mid \mathcal{M}_i \not\models \Psi_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \in \mathcal{U} \\
&\iff \left\{i \in I \mid \mathcal{M}_i \models \neg\Psi_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \in \mathcal{U}.
\end{aligned}$$

  On utilise le fait que $\mathcal{U}$ est un ultrafiltre (un filtre ne suffirait pas) à la troisième équivalence.

- Si $\Phi = (\Phi_0 \wedge \Phi_1)$, alors :

$$\begin{aligned}
&\mathcal{M} \models \Phi_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]} \\
&\iff \mathcal{M} \models \Phi_{0[\alpha^1/x_1,\ldots,\alpha^n/x_n]} \text{ et } \mathcal{M} \models \Phi_{1[\alpha^1/x_1,\ldots,\alpha^n/x_n]} \\
&\iff \left\{i \in I \mid \mathcal{M}_i \models \Phi_{0[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \in \mathcal{U} \\
&\qquad \text{et } \left\{i \in I \mid \mathcal{M}_i \models \Phi_{1[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \in \mathcal{U} \\
&\Longrightarrow \bigcap_{k=0,1} \left\{i \in I \mid \mathcal{M}_i \models \Phi_{k[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]}\right\} \in \mathcal{U} \\
&\iff \left\{i \in I \mid \mathcal{M}_i \models (\Phi_0 \wedge \Phi_1)_{[\alpha/x_{n_i}]}\right\} \in \mathcal{U}.
\end{aligned}$$

  où l'implication s'obtient par clôture par intersection de l'ultrafiltre $\mathcal{U}$. Complétons maintenant l'implication en équivalence. Il suffit de constater que chacun des ensembles dont on prend l'intersection est une extension de l'intersection elle-même.

- Si $\Phi = \exists x\ \Psi$, alors :

$$\begin{aligned}
&\mathcal{M} \models \Phi_{[\alpha^1/x_1,\ldots,\alpha^n/x_n]} \\
&\qquad\qquad \iff \textit{il existe } [(a_i)_{i\in I}]_\sim \text{ t.q. } \mathcal{M} \models \Psi_{[[(a_i)_{i\in I}]_\sim /x,\alpha^1 /x_1,\ldots, /\alpha^n /x_n]}
\end{aligned}$$

Pour établir l'équivalence à la dernière ligne, il suffit de constater que l'on peut construire $(a_i)_{i\in I}$ grace à l'Axiome du Choix de la façon suivante : pour tout $i \in I$, si :

$$j \in \left\{ i \in I \mid \mathcal{M}_i \models \Phi_{[\alpha_i^1/x_1,\ldots,\alpha_i^n/x_n]} \right\},$$

alors :

$$\textit{il existe } a_j \in |\mathcal{M}_j| \text{ t.q. } \mathcal{M}_j \models \Psi_{[a_j\ /x,\ /\alpha_j^1\ /x_1,\ldots,\alpha_j^n\ /x_n]}$$

auquel cas on choisit un tel élément. Sinon on choisit $a_j \in |\mathcal{M}_j|$ quelconque. On obtient ainsi $[(a_i)_{i\in I}]_\sim$ vérifiant les propriétés recherchées.

$\dashv$ 517

Théorème 518 (Théorème de compacité) *Une théorie est satisfaisable si et seulement si chaque sous-théorie finie est satisfaisable.*

Preuve du Théorème 518 :

- $\Rightarrow$ **:** Évident.
- $\Leftarrow$ **:** Soit I l'ensemble des parties finies de la théorie T. L'Axiome du Choix nous permet de choisir, pour tout $i \in I$, un modèle $\mathcal{M}_i$ de i, puisque chaque sous-théorie *finie* de T est satisfaisable. On cherche maintenant un ultrafiltre $\mathcal{U}$ sur I adéquat pour que l'ultraproduit de ces modèles soit un modèle de T. Si l'on veut que cela fonctionne, il faut que pour toute formule $\Phi \in T$, $\mathcal{M} = \prod_{i\in I} \mathcal{M}_i\ /\mathcal{U} \models \Phi$, c'est-à-dire par le théorème de Łoś que $\{i \in I \mid \mathcal{M}_i \models \Phi\} \in \mathcal{U}$. Or, par construction,

$$\{i \in I \mid \mathcal{M}_i \models \Phi\} \supseteq \{i \in I \mid \{\Phi\} \subseteq i\}.$$

Par conséquent, puisque le filtre engendré par une base est l'ensemble des extensions des éléments de la base, il nous suffit de trouver une base de filtre qui contiennent le second membre. On va donc poser pour base de filtre :

$$\mathcal{B} = \{N_i :\ i \in I\}.$$

où chaque N_i est l'ensemble de toutes les parties finies de T qui étendent la partie finie i :

$$N_i = \{j \in I \mid i \subseteq j\}.$$

Vérifions maintenant que c'est une base de filtre.

- On a que $\emptyset \notin \mathcal{B}$ (par construction).
- Si $N_i, N_j \in \mathcal{B}$, alors $N_i \cap N_j = N_{i\cup j} \in \mathcal{B}$.

Il suffit maintenant de choisir, par l'axiome de l'ultrafiltre, un ultrafiltre $\mathcal{U}$ qui étende le filtre engendré par $\mathcal{B}$.

Pour toute formule $\Phi \in T$, puisque :

$$\underbrace{\{i \in I \mid \{\Phi\} \subseteq i\}}_{\in\mathcal{U}}$$

et :

$$\{i \in I \mid \mathcal{M}_i \models \Phi\} \supseteq \underbrace{\{i \in I \mid \{\Phi\} \subseteq i\}}_{\in\mathcal{U}}$$

il apparaît que :

$$\underbrace{\{i \in I \mid \mathcal{M}_i \models \Phi\}}_{\in \mathcal{U}}$$

et donc :

$$\prod_{i \in I} \mathcal{M}_i \, /\mathcal{U} \models \Phi.$$

$\dashv$ 518

Pour aller plus avant :

Le lecteur qui souhaiterait en savoir plus sur les ultraproduits et ce type de construction est invité à consulter les ouvrages de théorie des modèles mentionnés à la page 443 – entre autres *"Model theory"* de Chen C. Chang et H. Jerome Keisler [CK90], ainsi que *"Models and ultraproducts : An introduction"* de John L. Bell et Alan B Slomson [BS06].

Bibliographie

[AB05] Sergei N. Artemov and Lev D. Beklemishev, “Provability logic”, in *Handbook of Philosophical Logic*, 2nd Edition, volume 13, pages 189–360, Springer, 2005.

[AN92] Antoine Arnauld and Pierre Nicole, *La logique ou l'art de penser*, Tel. Gallimard, 1992.

[Ari70] Aristote, *Organon : Volumes 1 et 2, Catégories. De l'interprétation ; texte, traduction, notes par Jules Tricot*, Librairie Philosophique J. Vrin, 1970.

[Ari92] Aristote, *Organon : Volume 3, Les Premiers Analytiques ; texte, traduction, notes par Jules Tricot*, Librairie Philosophique J. Vrin, 1992.

[Ari95] Aristote, *Organon : Volume 6, Les Réfutations sophistiques ; texte, traduction par Jules Tricot*, Librairie Philosophique J. Vrin, 1995.

[Ari97] Aristote, *Organon : Volume 5, Les Topiques ; texte, traduction par Jules Tricot*, Librairie Philosophique J. Vrin, 1997.

[Ari00] Aristote, *Organon : Volume 4, Les Seconds Analytiques ; texte, traduction nouvelle et notes par Jules Tricot*, Librairie Philosophique J. Vrin, 2000.

[Avi07] Avicenne, *Le Livre de Science. Dânesh-Nâmeh (1021-1037)*, traduit du persan par Muhammad Achena et Henri Massé, Sciences et Humanisme, Les Belles Lettres, 2007.

[Awo06] Steve Awodey, *Category theory*, volume 49, Oxford University Press, 2006.

[Awo12] Steve Awodey, “Type theory and homotopy”, in *Epistemology versus Ontology*, pages 183–201, Springer, 2012.

[Bar81] Jon Barwise, Scenes and other situations, *The journal of Philosophy*, pages 369–397, 1981.

[BBJ02] George S. Boolos, John P. Burgess, and Richard C. Jeffrey, *Computability and logic*, Cambridge University Press, 2002.

[BdRV02] Patrick Blackburn, Maarten de Rijke, and Yde Venema, *Modal logic*, volume 53, Cambridge University Press, 2002.

[BF11] Julian Baggini and Peter S. Fosl, *The Philosopher's Toolkit : A compendium of philosophical concepts and methods*, Blackwell Publishing, 2011.

[BG94] Josiane Boutet and Jean-Blaise Grize, *Construire le sens*, volume 42, P. Lang, 1994.

[Bin07] Ken Binmore, *Game theory : a very short introduction*, Oxford University Press, 2007.

[Bin12] Ken Binmore, *Playing for Real : A Text on Game Theory*, Oxford university press, 2012.

[BK10] Tracey Bowell and Gary Kemp, *Critical thinking : A concise guide*, Routledge, 2010.

[Bla87] Robert Blanché, *Introduction à la logique contemporaine*, Librairie Armand Colin, 1987.

[Bla02] Pierre Blackburn, *Logique de l'argumentation*, Pearson ERPI, 2002.

[Boo47] George Boole, *The mathematical analysis of logic*, Philosophical Library, 1847.

[Boo54] George Boole, *An investigation of the laws of thought : on which are founded the mathematical theories of logic and probabilities*, volume 2, Walton and Maberly, 1854.

[Boo84] George S. Boolos, “To be is to be a value of a variable (or to be some values of some variables)”, *The Journal of Philosophy*, 81(8) :430–449, 1984.

[Boo95] George S. Boolos, *The logic of provability*, Cambridge university press, 1995.

[Bos97] David Bostock, *Intermediate logic*, Oxford University Press, 1997.

[Bou70] Nicolas Bourbaki, *Théorie des ensembles*, volume 1, Hermann Paris, 1970.

[BPV99] Lev D. Beklemishev, Mati R. Pentus, and Nikolai K. Vereshchagin, *Provability, Complexity, Grammars*, volume 192, AMS Bookstore, 1999.

[Bro23] Luitzen Egbertus Jan Brouwer, "On the significance of the principle of excluded middle in mathematics, especially in function theory", *van Heijenoort vH67*, pages 334–345, 1923.

[BS06] John L. Bell and Alan B. Slomson, *Models and ultraproducts : An introduction*, DoverPublications.com, 2006.

[Bus98] Samuel R. Buss, *Handbook of proof theory*, Elsevier Science, 1998.

[BvBW06] Patrick Blackburn, Johan van Benthem, and Frank Wolter, *Handbook of modal logic*, volume 3, Elsevier, 2006.

[BvF03] Jc Beall and Bas C. van Fraassen, *Possibilities and paradox : An introduction to modal and many-valued logic*, Oxford University Press Oxford, 2003.

[Can32] Georg Cantor, *Gesammelte Abhandlungen Mathematischen und philosophischen Inhalts, edited by Zermelo E.* Springer, Berlin, 1932.

[Car03] Lewis Carroll, *Alice's Adventures in Wonderland and Through the Looking Glass and What Alice Found There ; edited with an introduction and notes by Hugh Haughton*, Penguin Classics, 2003.

[Cav47] Jean Cavaillès, *Sur la logique et la théorie de la science*, PUF, 1947.

[CF08] Nino B. Cocchiarella and Max A. Freund, *Modal logic : an introduction to its syntax and semantics*, Oxford University Press Oxford, 2008.

[CH03] Max J. Cresswell and George E. Hughes, *A new introduction to modal logic*, London ; New York : Routledge, 2003, X, 421 p. ; 23 cm.

[CH07] Ian Chiswell and Wilfrid Hodges, *Mathematical logic*, Oxford University Press, 2007.

[Che80] Brian F. Chellas, *Modal logic : an introduction*, Cambridge university press, 1980.

[Cho56] Noam Chomsky, "Three models for the description of language", *IRE Transactions on Information Theory*, 2(3) :113–124, 1956.

[Chr04] Chrysippe, *Oeuvres philosophiques, tomes I et II (édition bilingue grec ancien/ français) ; traduction par Richard Dufour*, Collection Fragments, Les Belles Lettres, 2004.

[Chu96] Alonzo Church, *Introduction to Mathematical Logic*, Princeton Landmark in Mathematics, Princeton University Press, 1996.

[CK90] Chen C. Chang and H. Jerome Keisler, *Model theory*, North Holland, 1990.

[CLK03a] René Cori, Daniel Lascar, and Jean-Louis Préf Krivine, *Logique mathématique, tome 1 : Calcul propositionnel ; algèbre de Boole ; calcul des prédicats*, volume 1, Dunod, Paris, 2003.

[CLK03b] René Cori, Daniel Lascar, and Jean-Louis Préf Krivine, *Logique mathématique, tome 2 : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles*, volume 2, Dunod, Paris, 2003.

[Coo04] S Barry Cooper, *Computability theory*, CRC Press, 2004.

[Cou13] Louis Couturat, *La logique de Leibniz d'après des documents inédits (Éd. 1901)*, Collection Philosophie, Hachette Livre BNF, 2013.

[Cut80] Nigel Cutland, *Computability : An introduction to recursive function theory*, Cambridge university press, 1980.

[CZ97] Alexander Chagrov and Michael Zakharyaschev, *Modal logic*, volume 199, Clarendon Press Oxford, 1997.

[Dav01] Martin Davis, *Engines of Logic : Mathematicians and the Origin of the Computer*, WW Norton & Company, 2001.

[Del88] André Delessert, *Introduction à la logique*, Presses polytechniques et universitaires romandes, 1988.

[Del12] Jean-Paul Delahaye, *La logique un aiguillon pour la pensée*, Belin, 2012.

[DNR04] René David, Karim Nour, and Christophe Raffalli, *Introduction à la logique : théorie de la démonstration : cours et exercices corrigés, (2nd édition)*, Dunod, 2004.

[Dom07] Josâe Ferreirâos Domâinguez, *Labyrinth of thought : A history of set theory and its role in modern mathematics*, Springer, 2007.

[DP75] Arthur Conan Doyle and Sidney Paget, *The Complete Adventures and Memoirs of Sherlock Holmes : A Facsimile of the Original Strand Magazine Stories, 1891-1893*, Bramhall House, 1975.

[DRL00] Yannis Delmas-Rigoutsos and René Lalement, *La logique ou l'art de raisonner*, Le Pommier-Fayard, 2000.

[dSE99] Antoine de Saint-Exupéry, *Le petit prince*, Folio, Gallimard, 1999.

[Dum00] Michael Dummett, *Elements of intuitionism*, volume 39, Oxford University Press, 2000.

[EC89] Richard L. Epstein and Walter Alexandre Carnielli. *Computability : computable functions, logic, and the foundations of mathematics*, CRC press, 1989.

[EF05] Heinz-Dieter Ebbinghaus and Jörg Flum, *Finite model theory*, Springer, 2005.

[EFT78] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas, *Einführung in die mathematische Logik*, Wissenschaftliche Buchgesellschaft Darmstadt, 1978.

[Ehr61] Andrzej Ehrenfeucht, "An application of games to the completeness problem for formalized theories", *Fund. Math*, 49(129-141) :13, 1961.

[End72] Herbert B. Enderton, *A mathematical introduction to logic*, Academic Press, 1972.

[End77] Herbert B. Enderton, *Elements of set theory*, Academic Press, 1977.

[End10] Herbert B. Enderton, *Computability Theory : An Introduction to Recursion Theory*, Academic Press, 2010.

[Euc90] Euclide, *Les Éléments ; traduction et commentaires par Bernard Vitrac*, volume 1, Presses Universitaires de France, 1990.

[Eul03] Leonhard Euler, *Lettres a une princesse d'allemagne : sur divers sujets de physique et de philosophie*, Presses polytechniques et universitaires romandes, 2003.

[FBHL73] Abraham A. Fraenkel, Yehoshua Bar-Hillel, and Azriel Levy, *Foundations of set theory*, Elsevier, 1973.

[FHMV95] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Vardi, *Reasoning About Knowledge*, MIT Press, 1995.

[Fie08] Hartry H. Field, *Saving truth from paradox*, Oxford University Press Oxford, 2008.

[Fit52] Frederic Brenton Fitch, *Symbolic Logic : an introduction*, Ronald Press Co., 1952.

[Fit07] Melvin Fitting, *Incompleteness in the Land of Sets*, College Publications, 2007.

[FM98] Melvin Fitting and Richard L. Mendelsohn, *First-order modal logic*, volume 277, Springer, 1998.

[For95] Thomas E. Forster, *Set theory with a universal set : exploring an untyped universe*, Clarendon Press, 1995.

[Fra50] Roland Fraïssé, "Sur une nouvelle classification des systèmes de relations", *Comptes Rendus Hebdomadaires des Séances de l'Académie des Sciences*, 230(11) :1022–1024, 1950.

[Fra05] Torkel Franzén, *Gödel's Theorem : an incomplete guide to its use and abuse*, AK Peters, 2005.

[Fre71] Gottlob Frege, *Écrits logiques et philosophiques ; traduction par Claude Imbert*, Éditions du Seuil, 1971.

[FT91] Drew Fudenberg and Jean Tirole, *Game theory. 1991*, MIT Press, 1991.

[Gan95] Robin Gandy, "The confluence of ideas in 1936", in *The Universal Turing Machine A Half-Century Survey*, pages 51–102, Springer, 1995.

[Gar06] James W. Garson, *Modal logic for philosophers*, Cambridge University Press Cambridge, 2006.

[GG00] Paul Gochet and Pascal Gribomont, "Logique, méthodes pour l'informatique fondamentale", *Paris : Hermès*, 2000.

[GG11] Ivor Grattan-Guinness, *The search for mathematical roots, 1870-1940 : logics, set theories and the foundations of mathematics from Cantor through Russell to Godel*, Princeton University Press, 2011.

[Gib92] Robert Gibbons, *A primer in game theory*, Harvester Wheatsheaf Hertfordshire, 1992.

[Gir87] Jean-Yves Girard, "Proof theory and logical complexity", vol. i, *Studies in Proof Theory. Bibliopolis (Napoli) and Elsevier Science Publishers (Amsterdam)*, 1987.

[Gir00] Rod Girle, *Modal logics and Philosophy*, McGill-Queen's Press-MQUP, 2000.

[Gir03] Rod Girle, *Possible worlds*, McGill-Queen's Press-MQUP, 2003.

[Gir06] Jean-Yves Girard, *Le point aveugle, tome 1 : vers la perfection*, Hermann, 2006.

[Gir07] Jean-Yves Girard, *Le point aveugle, tome 2 : vers l'imperfection*, Hermann, 2007.

[Göd30] Kurt Gödel, "Die vollstandigkeit der axiome des logischen funktionenkalkuls", *Monatshefte fur Mathematik und Physik*, 37 :349–360, 1930.

[Göd31] Kurt Gödel, "Über formal unentscheidbare sätze der principia mathematica und verwandter systeme i", *Monatshefte für Mathematik*, 38(1) :173–198, 1931.

[Göd86] Kurt Gödel, "On the intuitionistic propositional calculus", *Collected Works*, 1 :223–225, 1986.

[Gol96] Derek C. Goldrei, *Classic Set Theory : For Guided Independent Study*, Chapman & Hall, 1996.

[Gol06] Robert Goldblatt, *Topoi : the categorial analysis of logic*, volume 98, Courier Dover Publications, 2006.

[Gol10] Oded Goldreich, *P, NP, and NP-Completeness : The basics of computational complexity*, Cambridge University Press Cambridge, 2010.

[Gri67] Jean-Blaise Grize, "Logique des classes et des propositions", in Jean Piaget, editor, *Logique et Connaissance Scientifique*, Encyclopédie de la Pléiade, Gallimard, 1967.

[Gri73] Jean-Blaise Grize, *Logique moderne*, volume 3, Gauthier-Villars, 1973, 3 vol. ; 22 cm.

[Gri82a] Jean-Blaise Grize, *De la logique à l'argumentation*, volume 134, Librairie Droz, 1982.

[Gri82b] Jean-Blaise Grize, "Introduction à la logique naturelle et approche logique du langage", in *Approches formelles de la sémantique naturelle*, 1982.

[Gri90] Timothy Griffin, "A formulae-as-types notion of control", in Frances E. Allen, editor, *POPL*, pages 47–58, ACM Press, 1990.

[GTL89] Jean-Yves Girard, Paul Taylor, and Yves Lafont, *Proofs and types*, volume 7, Cambridge University Press Cambridge, 1989.

[HA28] David Hilbert and Wilhelm Ackermann, "Grundzüge der theoretischen logik", *Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen*, 27, 1928.

[HAL50] David Hilbert, Wilhelm Ackermann, and Robert E. Luce, *Principles of mathematical logic*, Chelsea Publishing Company New York, 1950.

[Hal03] Joseph Y. Halpern, *Reasoning about uncertainty*, MIT Press, 2003.

[Hed04] Shawn Hedman, *A first course in logic : an introduction to model theory, proof theory, computability, and complexity*, Oxford University Press Oxford, 2004.

[Her06] Horst Herrlich, *Axiom of choice*, Springer, 2006.

[HJ99] Karel Hrbacek and Thomas Jech, *Introduction to Set Theory, Revised and Expanded*, Crc Press, 1999.

[HMU01] John E. Hopcroft, Rajeev Motwani, and Jeffrey D. Ullman, *Introduction to automata theory, languages, and computation*, Addison-Wesley Publishing Co., Reading, Mass., 2001, Addison-Wesley Series in Computer Science.

[Hob39] Thomas Hobbes, *The English Works of Thomas Hobbes of Malmesbury*, volume 1, Bohn, 1839.

[Hod97] Wilfrid Hodges, *A Shorter Model Theory*, Cambridge University Press, 1997.

[Hod01] Wilfrid Hodges, *An introduction to elementary logic*, Penguin Books, 2001.

[HS79] Jaakko Hintikka and Esa Saarinen, *Game-theoretical semantics : Essays on semantics*, volume 5, Springer, 1979.

[HW79] Godfrey Harold Hardy and Edward Maitland Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1979.

[Jec03] Thomas Jech, *Set theory : the third millennium edition*, Springer, 2003.

[Jec08] Thomas Jech, *The axiom of choice*, DoverPublications.com, 2008.

[JW97] Winfried Just and Martin Weese, *Discovering Modern Set Theory : Set-theoretic tools for every mathematician. 2*, volume 1, American mathematical society, 1997.

[Kan96] Akihiro Kanamori, "The mathematical development of set theory from cantor to cohen", *The Bulletin of Symbolic Logic*, 2(1) :1–71, 1996.

[Kan08] Akihiro Kanamori, *The higher infinite : large cardinals in set theory from their beginnings*, Springer, 2008.

[Kay91] Richard Kaye, *Models of Peano arithmetic*, Clarendon Press Oxford, 1991.

[KK67] Georg Kreisel and Jean-Louis Krivine, *Éléments de logique mathématique : théorie des modèles*, volume 3, Dunod, 1967, VIII, 212 p. : ill. ; 25 cm.

[Kle52] Stephen C. Kleene, *Introduction to Metamathematics*, D. Van Nostrand Company, Inc., Princeton, New Jersey, 1952.

[Kle67] Stephen C. Kleene, *Mathematical Logic*, John Wiley & Sons, 1967.

[Kol25] Andrei Nikolaevich Kolmogorov, "On the principle of excluded middle", *Mat. Sb*, 32(4) :646–667, 1925.

[Kri90] Jean-Louis Krivine, *Lambda-calcul, types et modèles*, études et recherche en informatique, Masson, 1990.

[Kri93] Jean-Louis Krivine, *Lambda-calculus, types and models*, Ellis Horwood series in computers and their applications, Masson, 1993.

[Kri00] Jean-Louis Krivine, "The curry-howard correspondence in set theory", in *LICS*, pages 307–308, IEEE Computer Society, 2000.

[Kri07] Jean-Louis Krivine, *Théorie des ensembles*, Cassini, 2007.

[Kun11] Kenneth Kunen, *Set theory*, College Publications, 2011.

[Lea99] Christopher C. Leary, *A friendly introduction to mathematical logic*, Prentice Hall PTR, 1999.

[Lei84] Gottfried W. Leibniz, "Nova methodus pro maximis et minimis, itemque tangentibus, quae nec fractas nec irrationales quantitates moratur, et singulare pro illis calculi genus", *Acta Eruditorum*, Leipzig, 1684.

[Lei11] Gottfried W. Leibniz, *Gothofredi Guillelmi Leibnitii Opera Philosophica Quae Extant Latina Gallica Germanica Omnia... (French Edition) ; ed. Joannes Eduardus Erdmann*, Nabu Press, 2011.

[Lei12] Gottfried W. Leibniz, *Dissertatio de arte combinatoria, in qua, ex arithmeticae fundamentis, (Éd. 1666)*, Collection Sciences, Hachette Livre BNF, 2012.

[Lep01] François Lepage, *Éléments de logique contemporaine*, Cambridge Univ Press, 2001.

[Ler98] Jean Leroux, *Introduction à la logique*, Diderot, 1998, VI, 344 p. : fig. ; 24 cm.

[Lev12] Azriel Levy, *Basic set theory*, Courier Dover Publications, 2012.

[Lib04] Leonid Libkin, *Elements of finite model theory*, Springer, 2004.

[Lin03] Per Lindström, *Aspects of incompleteness*, volume 10, AK Peters Matick, 2003.

[Lit53] John E. Littlewood, *A mathematician's miscellany*, London : Methuen and Co., 1953.

[LL78] Paul Lorenzen and Kuno Lorenz, *Dialogische logik*, Wissenschaftliche Buchgesellschaft Darmstadt, 1978.

[Łoś55] Jerzy Łoś, "Quelques remarques, théorèmes et problèmes sur les classes définissables d'algèbres", *Mathematical interpretation of formal systems*, pages 98–113, 1955.

[LR03] F. William Lawvere and Robert Rosebrugh, *Sets for mathematics*, Cambridge University Press, 2003.

[LS09] F. William Lawvere and Stephen H. Schanuel, *Conceptual mathematics : a first introduction to categories*, Cambridge University Press, 2009.

[Man96] María Manzano, *Extensions of first order logic*, volume 19, Cambridge University Press, 1996.

[Mar02] David Marker, *Model theory : an introduction*, Springer, 2002.

[McK06] Thomas J. McKay, *Plural predication*, Clarendon Press Oxford, 2006.

[McL92] Colin McLarty, *Elementary categories, elementary toposes*, Oxford University Press, 1992.

[Men97] Elliot Mendelson, *Introduction to mathematical logic*, CRC press, 1997.

[ML98] Saunders Mac Lane, *Categories for the working mathematician*, volume 5, Springer verlag, 1998.

[Mon09] Martin Montminy, *Raisonnement et pensée critique : introduction à la logique informelle*, Presses de l'Université de Montréal, 2009.

[Mos94] Yannis N. Moschovakis, *Notes on set theory*, Springer-Verlag New York, Inc., 1994.

[NNGG89] Ernest Nagel, James R. Newman, Kurt Gödel, and Jean-Yves Girard, *Le théorème de Gödel*, Éditions du Seuil, 1989.

[NvP08] Sara Negri and Jan von Plato, *Structural proof theory*, Cambridge University Press, 2008.

[Odi92] Piergiorgio Odifreddi, *Classical recursion theory : The theory of functions and sets of natural numbers*, North Holland, 1992.

[OR94] Martin J. Osborne and Ariel Rubinstein, *A course in game theory*, MIT press, 1994.

[Osb04] Martin J. Osborne, *An introduction to game theory*, volume 3, Oxford University Press New York, 2004.

[Pap03] Christos H. Papadimitriou, *Computational complexity*, John Wiley and Sons Ltd., 2003.

[Pap12] David Papineau, *Philosophical Devices : Proofs, Probabilities, Possibilities, and Sets*, Oxford University Press, 2012.

[Pas79] Blaise Pascal, *L'esprit de la géométrie et de l'art de persuader*, Ed. Pédagogie Moderne, 1979.

[Pla82] Platon, *La République VIII-X ; texte établi et traduit par Émile Chambry*, Les belles lettres, 1982.

[Pog10] Francesca Poggiolesi, *Gentzen calculi for modal propositional logic*, volume 32, Springer, 2010.

[Poi85] Bruno Poizat, *Cours de théorie des modèles : une introduction à la Logique mathématique contemporaine*, Bruno Poizat, 1985.

[Poi00] Bruno Poizat, *A course in model theory : an introduction to contemporary mathematical logic*, Springer, 2000.

[Pop94] Sally Popkorn, *First steps in modal logic*, Cambridge University Press, 1994.

[Pot04] Michael Potter, *Set Theory and its Philosophy : A Critical Introduction : A Critical Introduction*, Oxford University Press, 2004.

[Pra06] Dag Prawitz, *Natural Deduction : A Proof-Theoretical Study*, Dover, 2006.

[Pri01] Graham Priest, *An introduction to non-classical logic*, Cambridge University Press, 2001.

[Qui86] Willard Van Orman Quine, *Philosophy of logic*, Harvard University Press, 1986.

[Res13] Greg Restall, *An introduction to substructural logics*, Routledge, 2013.

[Riv03] François Rivenc, *Introduction à la logique*, Payot & Rivages, 2003.

[Riv05] François Rivenc, *Introduction à la logique pertinente*, Presses universitaires de France, 2005.

[RJ87] Hartley Rogers Jr., *Theory of recursive functions and effective computability*, MIT press, 1987.

[Rob50] Raphael M. Robinson, "An essentially undecidable axiom system", in *Proceedings of the international Congress of Mathematics*, volume 1, pages 729–730, 1950.

[Rob69] Joel W. Robbin, *Mathematical logic : a first course*, WA Benjamin New York and Amsterdam, 1969.

[Ros44] Alf Ross, "Imperatives and logic", *Philosophy of Science*, 11(1) :30–46, 1944.

[Rot00] Philipp Rothmaler, *Introduction to model theory*, volume 15, CRC Press, 2000.

[Rus03] Bertrand Russell, *The principles of mathematics*, volume 1, Cambridge University Press, 1903.

[RW12] Bertrand Russell and Alfred N. Whitehead, *Principia mathematica*, volume 2, University Press, 1912.

[Sal94] Jean Salem, *Introduction à la logique formelle et symbolique : avec des exercices et leurs corrigés*, Nathan, 1994.

[Sch11] Ernest Schimmerling, *A Course on Set Theory*, Cambridge University Press, 2011.

[Sen63] Maurice Sendak, *Where the wild things are*, Harper & Row, 1963.

[SF96] Raymond M. Smullyan and Melvin Fitting, *Set theory and the continuum problem*, Oxford University Press, Inc., 1996.

[Sha91] Stewart Shapiro, *Foundations without Foundationalism : A Case for Second-Order Logic*, Oxford University Press, 1991.

[Sho67] Joseph R. Shoenfield, *Mathematical logic*, volume 21, Addison-Wesley Publishing Co., Reading, Mass., 1967.

[Sim11] Harold Simmons, *An introduction to category theory*, Cambridge University Press, 2011.

[Sip06] Michael Sipser, *Introduction to the Theory of Computation*, volume 2, Thomson Course Technology Boston, 2006.

[Smi03] Peter Smith, *An introduction to formal logic*, Cambridge University Press, 2003.

[Smi13] Peter Smith, *An introduction to Gödel's theorems*, Cambridge University Press, 2013.

[Smu86] Raymond M. Smullyan, *This book needs no title : a budget of living paradoxes*, Simon and Schuster, 1986.

[Smu92] Raymond M. Smullyan, *Gödel's incompleteness theorems*, Oxford University Press New York, 1992.

[Smu94] Raymond M. Smullyan, *Diagonalization and self-reference*, Clarendon press Oxford, 1994.

[Smu95] Raymond M. Smullyan, *First-order logic*, Courier Dover Publications, 1995.

[Smu00] Raymond M. Smullyan, *To Mock a Mockingbird : and other logic puzzles including an amazing adventure in combinatory logic*, Oxford University Press, 2000.

[Smu09a] Raymond M. Smullyan, *The Lady or the Tiger ? : and Other Logic Puzzles*, Courier Dover Publications, 2009.

[Smu09b] Raymond M. Smullyan, *Logical labyrinths*, A K Peters Ltd., 2009.

[Smu11a] Raymond M. Smullyan, *Alice in puzzle-land : A Carrollian tale for children under eighty*, Courier Dover Publications, 2011.

[Smu11b] Raymond M. Smullyan, *What is The Name of This Book ?(The Riddle of Dracula and Other Logic Puzzles)*, Courier Dover Publications, 2011.

[Smu12a] Raymond M. Smullyan, *Forever Undecided*, Knopf, 2012.

[Smu12b] Raymond M. Smullyan, *Satan, Cantor, And Infinity And Other Mind-bogglin*, Random House LLC, 2012.

[Sti03] John Stillwell, *Elements of number theory*, Springer, 2003.

[SU06] Morten Heine Sørensen and Pawel Urzyczyn, *Lectures on the Curry-Howard isomorphism*, volume 149, Elsevier, 2006.

[SV02] Alexander Shen and Nikolai K. Vereshchagin, *Basic set theory*, American Mathematical Society, 2002.

[SW11] Helmut Schwichtenberg and Stanley S. Wainer, *Proofs and computations*, Cambridge University Press, 2011.

[Sza69] Manfred Egon Szabo, *The collected papers of Gerhard Gentzen*, volume 160, North-Holland Amsterdam, 1969.

[Tak13] Gaisi Takeuti, *Proof Theory*, Courier Dover Publications, 2013.

[Tar69] Alfred Tarski, *Introduction à la logique*, Gauthier-Villars, 1969.

[TK03] Paul Tidman and Howard Kahane, *Logic and philosophy : A modern introduction*, Belmont CA : Wadsworth Thomson Learning, cop., 2003, X, 532 p. : ill. ; 25 cm.

[Tou11a] George Tourlakis, *Lectures in Logic and Set Theory : Volume 2, Set Theory*, volume 83 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, 2011.

[Tou11b] George Tourlakis, *Mathematical logic*, John Wiley & Sons, 2011.

[Tou12] George Tourlakis, *Theory of Computation*, John Wiley & Sons, 2012.

[TS00] Anne S. Troelstra and Helmut Schwichtenberg, *Basic proof theory*, Cambridge University Press, 2000.

[TvD88] Anne Sjerp Troelstra and Dirk van Dalen, *Constructivism in mathematics*, volume 1, Elsevier Science, 1988.

[Vää01] Jouko Väänänen, "Second-order logic and foundations of mathematics", *Bulletin of Symbolic Logic*, 7(4) :504–520, 2001.

[Vää11] Jouko Väänänen, *Models and games*, volume 132, Cambridge University Press, 2011.

[vB01] Johan van Benthem, "Logic in games", *Lecture Notes, ILLC Amsterdam*, 2001.

[vB03] Johan van Benthem, "Logic and game theory : Close encounters of the third kind", in Gregory Mints and Reinhard Anton Muskens, editors, *Games, logic, and constructive sets*, CSLI Publications, 2003.

[vB06] Johan van Benthem, "Introduction : Alternative logics and classical concerns", in Johan van Benthem, Gerhard Heinzmann, Manuel Rebuschi, and Henk Visser, editors, *The Age of Alternative Logics*, pages 1–7, Springer, 2006.

[vB10] Johan van Benthem, *Modal Logic for Open Minds*, Center for the Study of Language and Information, 2010.

[vD97] Dirk van Dalen, *Logic and structure*, Berlin : Springer, 1997, 332 p. : ill. ; 24 cm.

[Vel06] Daniel J. Velleman, *How to prove it : a structured approach*, Cambridge University Press, 2006.

[Ven94] John Venn, *Symbolic Logic*, volume 251, American Mathematical Soc, 1894.

[Ver99] Xavier Verley, *Logique symbolique*, Ellipses, 1999.

[Ver01] Denis Vernant, *Introduction à la logique standard : calcul des propositions des prédicats et des relations*, Flammarion, 2001.

[vH77] Jean van Heijenoort, *From Freege to Gödel : A Source Book in Mathematical Logic, 1879-1931*, Harvard University Press, 1977.

[vNM07] John von Neumann and Oskar Morgenstern, *Theory of games and economic behavior (commemorative edition)*, Princeton university press, 2007.

[Wag11] Pierre Wagner, *La logique*, Paris, PUF «Que sais-je ?», 2011.

[War07] Nigel Warburton, *Thinking from A to Z*, Routledge, 2007.

[Zah98] Jacques Zahnd, *Logique élémentaire : cours de base pour informaticiens*, Presses polytechniques et universitaires romandes, 1998, XII, 430 p. : fig. ; 24 cm + 1 cahier.

[Zeg10] Mark Zegarelli, *Logic For Dummies*, John Wiley & Sons, 2010.

Index des symboles

Index des noms propres

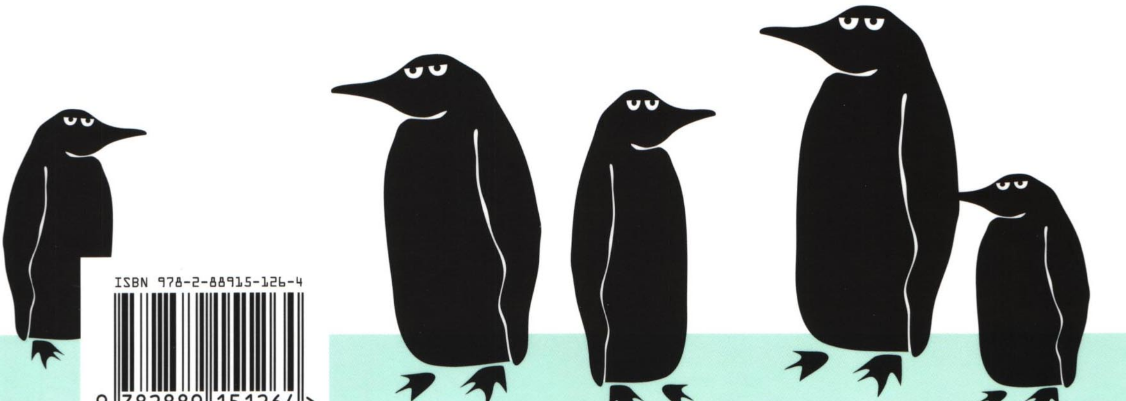
Index général

LA LOGIQUE pas à pas

Jacques Duparc

Mettre les bases de la logique à la portée de tous, et plus particulièrement des non-mathématiciens, tel est l'objectif de ce manuel. Tout spécifiquement conçu pour les étudiants entretenant une relation conflictuelle avec les sciences, ou définitivement rétifs aux maths et au formalisme, il ne requiert aucune formation ou bagage préalable. Pas question cependant de maintenir le lecteur à distance, et de ne lui proposer que quelques aperçus lointains : c'est au contraire au cœur même de la matière que Jacques Duparc emmène celui-ci, en le guidant pas à pas sur une trace moderne et novatrice, privilégiant le jeu et l'intuitivité. Claire et didactique, une référence incontournable pour l'apprentissage de la logique.

Jacques Duparc est docteur de l'Université Diderot Paris 7. Il est actuellement professeur de logique à l'Université de Lausanne (UNIL) et chargé de cours à l'Ecole polytechnique fédérale de Lausanne (EPFL).



ISBN 978-2-88915-126-4

9 782889 151264 >

Presses polytechniques et universitaires romandes