

Jean-Paul Delahaye

La logique, un aiguillon pour la pensée



Belin: POUR LA SCIENCE

Dans la même collection aux Éditions Belin-Pour la Science

- Claude ALLÈGRE et René DARS, *La géologie. Passé, présent et avenir de la Terre*, 2^e édition, 2012.
- Bernard VALEUR, *La couleur dans tous ses éclats*, 2011.
- Étienne GUYON, Jean-Pierre HULIN & Luc PETIT, *Ce que disent les fluides*, 2^e édition augmentée, 2011.
- Pierre CAUSERET, Jean-Luc FOUQUET et Liliane SARRAZIN-VILAS, *La Lune à portée de main*, 2010.
- Sébastien DIEGUEZ, *Maux d'artistes*, 2009.
- Jean-Michel COURTY et Édouard KIERLIK, *La physique buissonnière*, 2010.
- Étienne GUYON (sous la dir. de), *Matière et matériaux – De quoi est fait le monde ?*, 2010.
- Jean-Paul DELAHAYE, *Mathématiques pour le plaisir*, 2010.
- Lucas SALOMON, *Cerveau, drogues et dépendances*, 2010.
- Robert PASCAL, Hervé MARTIN, Muriel GARGAUD, Purificación LÓPEZ-GARCÍA, Thierry MONTMERLE, *Le Soleil, la Terre... la vie*, 2009.
- Yaël NAZÉ, *L'astronomie des Anciens*, 2009.
- Nicolas GAUVRIT, *Vous avez dit hasard ? Entre mathématiques et psychologie*, 2009.
- Sébastien STEYER et Alain BÉNÉTEAU, *La Terre avant les dinosaures*, 2009.
- Hans-Peter NOLLERT, Hanns RUDER, *Carnets de voyages relativistes*, 2008.
- Audouin DOLLFUS, *Les autres mondes*, 2008.
- Patrick CORDIER et Hugues LEROUX, *Ce que disent les minéraux*, 2008.
- Bernard VALEUR, *Sons et lumière*, 2008.
- Yves CORBOZ, *Météorologie*, 2008.
- Alessandra BENUZZI-MOUNAIS, *La fusion nucléaire*, 2008.
- Alain DORESSOUNDIRAM et Emmanuel LELLOUCH, *Aux confins du système solaire*, 2008.
- Rémi CADET, *L'invention de la physiologie*, 2008.
- Gilbert PIETRYK (sous la dir. de), *Panorama de la physique*, 2007.
- Bernard FRANCOU et Christian VINCENT, *Les glaciers à l'épreuve du climat*, 2007.
- Cédric RAY et Jean-Claude POIZAT, *La physique par les objets quotidiens*, 2007.
- Hervé THIS, *De la science aux fourneaux*, 2007.
- Adolphe NICOLAS, *Futur empoisonné – Quels défis ? Quels remèdes ?*, 2007.
- Jean-Paul DELAHAYE, *Complexités*, 2006.
- Denis SAVOIE, *Cosmographie – Comprendre les mouvements du Soleil, de la Lune et des planètes*, 2006.
- Louis BOYER, *Feu et flammes*, 2006.
- Marcel BOURNÉRIAS & Christian BOCK, *Le génie des végétaux*, 2006.
- François FORGET, François COSTARD & Philippe LOGNONNÉ, *La planète Mars*, 2^e édition, 2006.
- Alain NICOLAS, *Parcelles d'infini – Promenades au jardin d'Escher*, 2005.
- Bernard VALEUR, *Lumière et luminescence*, 2005.
- Pierre CHAUVE, *Des grottes et des sources*, 2005.
- Yaël NAZÉ, *Les couleurs de l'Univers*, 2005.
- Thérèse ENCRENAZ et Fabienne CASOLI, *Planètes extrasolaires*, 2005.
- François MICHEL, *Roches et paysages*, 2005.
- Michel BLAY, *Les figures de l'arc-en-ciel*, 2005.
- Pierre CAUSERET, Jean-Luc FOUQUET & Liliane SARRAZIN-VILAS, *Le ciel à portée de main*, 2005.
- John KING, *Le monde fabuleux des plantes*, 2004.
- Jean-Paul DELAHAYE, *Les inattendus mathématiques*, 2004.

Consultez ces ouvrages et nos autres titres sur nos sites Internet :

www.pourlascience.fr

www.editions-belin.com

Illustration couverture : © Images.com/Corbis Christopher Zacharow

Le code de la propriété intellectuelle n'autorise que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » [article L. 122-5] ; il autorise également les courtes citations effectuées dans un but d'exemple ou d'illustration. En revanche « toute représentation ou reproduction intégrale ou partielle, sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite » [article L. 122-4].

La loi 95-4 du 3 janvier 1994 a confié au C.F.C. (Centre français de l'exploitation du droit de copie, 20, rue des Grands-Augustins, 75006 Paris), l'exclusivité de la gestion du droit de reprographie. Toute photocopie d'œuvres protégées, exécutée sans son accord préalable, constitue une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal.

© Pour la Science 2012

ISBN 978-2-84245-115-8

BIBLIOTHÈQUE SCIENTIFIQUE

La logique,

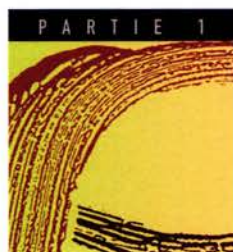
un aiguillon pour la pensée

Jean-Paul Delahaye

Belin: POUR LA SCIENCE

8, rue Férou - 75278 Paris cedex 06
www.editions-belin.fr – www.pourlascience.fr

Préface	6
Introduction	8
Bibliographie	195
Index	198



La logique de l'infini

..... 10

- L'infini est-il paradoxal en mathématiques ? 12
- Imaginer l'infini ou le découvrir ? 25
- L'ensemble de tous les ensembles 34



L'incomplétude et les limites logiques

..... 44

- L'incomplétude, le hasard et la physique 46
- Presque tout est indécidable 54



La logique du désordre et des probabilités

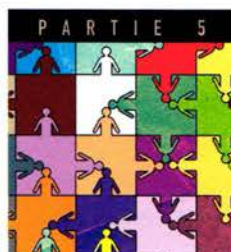
..... 62

- L'étonnante loi de Benford 64
- Le désordre total n'existe pas 73
- Pierre, feuille, ciseaux 81
- La Belle au bois dormant, la fin du monde et les extraterrestres 90



Logiques de graphes et de nombres

..... 100



Logique sociale, économique et humaine

..... 130

- Une propriété cachée des graphes 102
- Graphes et algorithmes pour ballons 111
- Un terrain de course numérique 120

- La répartition idéale des biens existe-t-elle ? 132
- Escroquerie ou jeu risqué ? 141
- Tao : l'éducation réussie d'un surdoué 150



La logique rencontre la physique

..... 158

- Concevoir l'univers comme un ordinateur 160
- Libre arbitre et mécanique quantique 170
- Suicide et immortalité quantiques 178
- Quand la physique démontre
des théorèmes mathématiques 187



Dans la vie, il y a des gens avec qui vous ne partagez aucun centre d'intérêt : lorsque vous les croisez, vous n'avez rien à leur dire. Et puis, il y a des gens avec qui vous avez 10 ou 20 pour cent de centres d'intérêt communs, rarement ce pourcentage atteint 50 pour cent. Avec Jean-Paul Delahaye, il se trouve que nos sujets communs sont sans doute plus proches de 80 pour cent même si cela ne signifie pas pour autant que nous soyons d'accord sur tout, loin s'en faut. Le résultat en est que lorsque nous commençons à discuter, nous ne nous arrêtons plus, quitte à ce que celui qui est dans la ville de l'autre (il habite Lille et moi Paris) manque rater son train pour rentrer chez lui. On l'aura compris, je trouve les domaines sur lesquels travaille Jean-Paul tout à fait passionnants qu'il s'agisse de logique, de théorie des ensembles, de théorie des nombres, d'informatique ou de physique. Et c'est justement le sujet de ce présent livre.

Vus de loin, ces domaines peuvent paraître déconnectés, mais il y a en fait une véritable unité logique dans l'ensemble de ces thèmes dès lors qu'on prend la peine de creuser la signification profonde cachée en eux, et ce livre aidera le lecteur qui le souhaite à la trouver.

Le travail de synthèse et de popularisation scientifique accompli par Jean-Paul Delahaye depuis plusieurs années est remarquable. Il met à la disposition de tous, des connaissances dans des champs scientifiques aussi variés que les mathématiques, la logique, la physique, en écrivant des textes qui ne nécessitent pour leur compréhension que des connaissances du niveau du premier cycle universitaire. Ce nouveau livre ne trahit pas l'esprit des précédents : faire prendre conscience au lecteur qu'au-delà des idées reçues, l'intuition est bien souvent trompeuse et montrer comment l'analyse des paradoxes les plus troublants peut faire progresser notre compréhension des domaines les plus difficiles de la science moderne.

Les exemples exposés dans ce livre ont une importance qui dépasse leur simple statut de résultats d'une discipline scientifique donnée. Considérés dans leur ensemble, ils imposent une nouvelle vision de la science elle-même, en ayant des conséquences philosophiques profondes sur la manière de considérer les connaissances qu'elle peut fournir.

Une des grandes découvertes philosophiques de la science contemporaine récente est la mise en avant de limites que les savants des périodes antérieures ne pouvaient pas soupçonner. Il n'est pas exagéré de dire que les plus grandes avancées théoriques du XX^e siècle en mathématiques et en physique ont conduit à une remise en cause drastique des fondations sur lesquelles on pensait pouvoir s'appuyer.

C'est tout d'abord vrai en physique où, après la théorie de la relativité qui avait déjà malmené nos concepts rassurants d'espace et de temps absolus et indépendants, la mécanique quantique a apporté la vision d'un monde qui ne ressemble plus du tout à celui auquel nous sommes habitués. Ce monde n'est plus déterministe, il n'est pas possible d'y connaître simultanément la position et la vitesse d'un objet et, pire, il est non local, c'est-

à-dire que ce qui est fait à un endroit semble avoir instantanément une influence (subtile certes) à un autre endroit.

Mais c'est vrai aussi en mathématiques et en logique alors que ces deux disciplines sont pour beaucoup le symbole même de la solidité et de la certitude. Les exemples que donne Jean-Paul Delahaye dans ce livre suscitent pour la plupart l'étonnement ou au moins conduisent le lecteur à une profonde remise en cause de beaucoup d'idées reçues. Les théorèmes d'incomplétude découverts par Kurt Gödel ont porté un coup fatal au programme, proposé par David Hilbert, de montrer qu'en mathématiques tout ce qui est vrai peut être démontré. Il existe des propositions qui bien que vraies ne peuvent pas être prouvées. On les appelle des indécidables. Et cette incomplétude s'est finalement révélée omniprésente. Pour reprendre le titre d'un chapitre de ce livre «presque tout est indécidable!»

Jean-Paul Delahaye nous fait également découvrir le domaine fascinant des ensembles et de l'infini. Georg Cantor en créant la théorie des ensembles a ouvert la porte à des réflexions sur l'infini qui vont bien au-delà de tout ce qu'on peut penser même en laissant libre cours à une imagination débridée. Cantor nous avait déjà montré qu'il existe, après l'infini des nombres entiers, des infinis successifs de plus en plus grands. Mais la théorie des ensembles moderne conceptualise des infinis qui sont encore incommensurablement plus grands que tous ceux que vous pouvez imaginer en prolongeant à l'infini la suite des infinis en question. Et même cela n'est qu'un début...

Jean-Paul Delahaye nous fait également découvrir que des questions mathématiques très simples à formuler peuvent être redoutablement complexes à démontrer. Il ne s'agit plus ici d'indécidables, mais de conjectures dont on se dit à première vue qu'en quelques minutes de réflexion on doit pouvoir les résoudre, et qui finalement résistent tant que certaines ont demandé des siècles de travail aux meilleurs mathématiciens pour être résolues et que d'autres sont toujours ouvertes. Ce qui semble simple est parfois infiniment subtil.

Et ces considérations mènent parfois, quand on en examine les conséquences les plus extrêmes, à des réflexions qui flirtent avec la science-fiction. Jean-Paul Delahaye ne s'en prive pas lorsqu'il évoque des sujets comme la fin du monde, l'immortalité quantique, les extraterrestres ou l'univers compris comme un ordinateur. Ces sujets peuvent paraître trop risqués tellement ils sont prospectifs, mais il n'y a aucune raison de s'interdire de réfléchir sur ces thèmes du moment qu'on leur applique la même rigueur de raisonnement que pour des sujets plus classiques. Et le plaisir ludique qu'on y trouve compense amplement l'incertitude des conclusions auxquelles on aboutit !

En fin de compte, ce livre prouve une chose essentielle : on peut faire de la science et apprendre en s'amusant. Alors profitez-en !

Hervé Zwirn

Professeur associé à l'Université Paris-Diderot

Organiser ses pensées rigoureusement et solidement. Les lier les unes aux autres de manière ferme en réseaux complexes que les mathématiques aident à analyser. Savoir se fixer des hypothèses, en tirer mécaniquement des affirmations nouvelles et identifier ce qu'une telle méthode – axiomatique – réussit ou ne réussit pas à atteindre. S'interroger sur l'infini de Cantor qui n'est ni absurde ni totalement élucidé comme l'illustre l'hypothèse du continu. Attribuer une force plus ou moins grande à une possibilité, la mesurer, savoir la maîtriser, cesser de s'étonner de ce qu'on tire de ces probabilités correctement évaluées. Identifier les règles inattendues que les nombres et les graphes satisfont et qui sont parfois très éloignées de ce que nous imaginions. Remettre en cause ce que nous croyons évident du monde physique sans pour autant tomber dans la contradiction. Voilà quelques objectifs de la logique conçue largement et que ce livre tente de présenter.

Nous avons voulu que la variété des sujets abordés soit accessible, de sorte que tout en restant aussi précis que possible nous évitions les développements techniques que les experts font entre eux, mais qui demandent des efforts coûteux en temps et en énergie, et qu'on ne peut envisager présenter quand on s'intéresse à une vaste série de sujets.

La logique, dans le sens ouvert que nous adoptons, a connu d'incroyables progrès depuis deux siècles. On y a découvert l'infini des cardinaux et de l'ensemble de tous les ensembles (première partie); l'incomplétude de Gödel et l'incalculabilité de Turing (deuxième partie); la troublante loi de Benford et de déconcertants paradoxes probabilistes (troisième partie); la théorie de l'ordre inévitable de Ramsey et des régularités inespérées en arithmétique (quatrième partie); de troublants raisonnements économiques et sociaux (cinquième partie); et l'incroyable mécanique quantique qui perturbe notre vision de la totalité du monde (sixième partie). Parler de tout cela à la fois est certainement une gageure!

Obtenu en sélectionnant, en reclassant et en mettant à jour des articles de la rubrique mensuelle *Logique et calcul* de la revue *Pour la Science*, cet ouvrage présente les avantages et les défauts de cette méthode d'exploration d'un domaine aussi large. Parmi les avantages, il y a l'indépendance des chapitres les uns relativement aux autres: certes ils se complètent et de nombreux liens apparaîtront entre ce qui est donné ici ou là, mais on peut ouvrir le livre à n'importe quel endroit, et lire sans craindre de devoir revenir en arrière à la recherche d'une information manquante. Parmi les défauts de la méthode, et même si nous avons tenté d'en atténuer les effets, il y a la présence de certaines redondances: le texte semble parfois pour les points les plus délicats revenir plusieurs fois sur une même idée ou un même raisonnement. Peut-être y verra-t-on un intérêt: examinée sous diverses facettes, une idée délicate finit par apparaître plus simple, plus naturelle et... plus logique.

Précisons enfin, que tout en recherchant l'exactitude et le sérieux qu'exige bien évidemment la science du raisonnement, nous avons aussi accepté l'esprit d'amusement et la curiosité spéculative qui sont dans l'essence même du travail du logicien. Peut-être même que certains chapitres vous étonneront par leur témérité, voire leur imprudence, quand ils évoquent la fin du monde, le suicide collectif, l'impuissance des mathématiques ou l'univers-ordinateur. La logique est l'instrument par excellence de jeu abstrait, nous l'avons parfois utilisé comme tel ; nous espérons que le lecteur saura lui aussi y trouver de l'agrément.



La logique de l'infini

L'infini est un sujet d'étude qui ne cesse de surprendre. Contrairement aux autres domaines des mathématiques, le travail n'y est pas seulement déductif. Il faut, comme l'a compris Gödel, en trouver les règles par essai d'axiomes et de théories nouvelles. Le vertige que l'exploration des totalités infinies nous fait éprouver, et l'étonnement dont on est saisi par les limitations logiques rencontrées constituent des plaisirs intellectuels souvent dérangeants.

L'infini est-il paradoxal en mathématiques ?

Pour résoudre le paradoxe du tout et des parties et affronter l'hypothèse du continu, notre idée de l'infini actuel doit évoluer ; aujourd'hui encore, nous découvrons de nouveaux infinis.

L'éternité, c'est long, surtout vers la fin.
Woody Allen

1. Le paradoxe de l'hôtel Hilbert

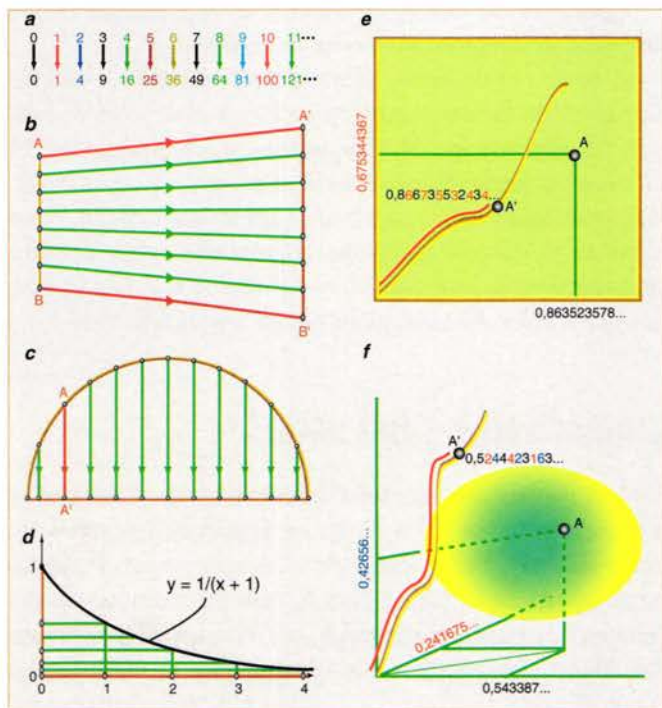
L'histoire suivante illustre pourquoi des ensembles infinis actuels ont longtemps paru absurdes. Un hôtel infini dont les chambres sont numérotées par les entiers $0, 1, 2, 3, \dots$ est complet pour la nuit (un client occupe chaque chambre). Arrive un client : « Pas de problème, lui répond le responsable de l'accueil. Installez-vous dans la chambre 0. Je demande au client de la chambre 0 de passer dans la chambre 1, à celui de la chambre 1 de passer dans la chambre 2, etc. » L'accueil dispose bien sûr d'un téléphone spécial qui permet de téléphoner simultanément à toutes les chambres en demandant au client de la chambre n de passer en $n + 1$. Le nouveau client a pu être reçu. Dix minutes plus tard arrive un car (infini, bien sûr) de nouveaux clients qui demandent à passer la nuit dans l'hôtel. « Pas de problème », répond le responsable de l'accueil au chauffeur du car, et il utilise son téléphone pour demander au client de la chambre n de passer dans la chambre $2n$. Il indique alors au chauffeur du car que le voyageur numéro i de son autocar peut disposer de la chambre $2i + 1$ (qui est effectivement libre, puisque toutes les chambres de numéro impair ont été libérées). Une demi-heure plus tard arrive un groupe plus important constitué d'une infinité de cars, chacun ayant à leur bord une infinité de passagers. « Pas de problème, je vous arrange ça », répond le responsable de l'accueil. Il téléphone au client de la chambre i de passer dans la chambre $2i + 1$ (ce qui libère toutes les chambres ayant un numéro pair) et donne la consigne suivante au responsable du groupe d'autocars : le passager numéro i du bus j doit occuper la chambre $2^{j+1}(2i + 1)$. Tout se passe bien, et jamais deux voyageurs différents ne se sont vus attribuer la même chambre.

L'infini mathématique peut-il être maîtrisé ? Autrement dit, peut-on faire une théorie de l'infini qui évite tout paradoxe et toute incohérence ? Pour répondre à ces questions, nous distinguerons paradoxes et situations logiquement peu satisfaisantes.

Un paradoxe au sein d'une théorie est la possibilité de démontrer une chose et son contraire. Dans cette situation, tout en n'utilisant que des raisonnements fondés sur les axiomes de la théorie, nous pouvons en tirer une affirmation A et l'affirmation contraire $\text{Non } A$. En mathématiques, les paradoxes (on les dénomme aussi contradictions, inconsistances, antinomies) sont inacceptables, et les logiciens font tout pour les éviter.

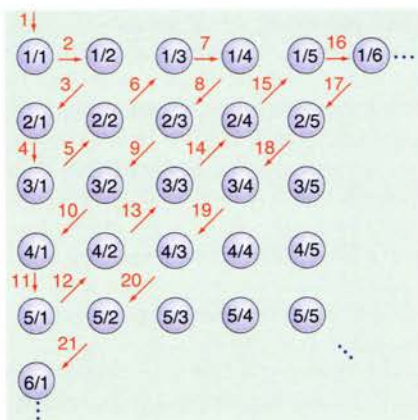
Aujourd'hui, les mathématiciens connaissent toutes sortes de moyens pour contourner les paradoxes au sein des théories mathématiques de l'infini. La question subsiste : ces moyens atteignent-ils leurs fins ?

Une situation logiquement insatisfaisante apparaît lorsqu'une théorie nous permet d'énoncer des propriétés étonnantes, parfois opposées à notre attente, sans toutefois qu'une véritable contradiction apparaisse. Nous pouvons alors continuer à développer la théorie en espérant que la difficulté sera résolue plus tard. Parfois nous finissons par accepter la situation jugée gênante, et ce qui était perçu comme douteux devient alors banal, comme si une métamorphose de nos conceptions profondes s'était produite.



2 Les paradoxes de la réflexivité: si les ensembles infinis existent en acte et non pas potentiellement, comme les ensembles que l'on complète petit à petit, alors l'ensemble des carrés est aussi grand que l'ensemble des nombres entiers : on peut associer chaque élément de l'un à un élément de l'autre [a]. Similairement [b], le segment AB est aussi « grand » que le segment A'B', et la demi-circonférence d'un cercle est « égale » à son diamètre [c]. On peut aussi mettre en correspondance [d] les points réels d'un segment et les points d'une demi-droite infinie par la relation $y = 1/(x+1)$. Similairement, Cantor (il fut très surpris de cette possibilité) a mis en relation l'ensemble des points d'une surface plane avec les points d'une courbe quelconque. Pour cela, on associe aux deux coordonnées d'un point une valeur obtenue en intercalant les décimales des deux nombres représentant les coordonnées, et l'on associe à cette valeur un point de la courbe dont la distance à l'origine (prise le long de la courbe) est égale à la valeur obtenue [e]. De la même façon, on associe les points d'un volume aux points d'une courbe [f].





3 L'ensemble infini des nombres rationnels [c'est-à-dire l'ensemble des nombres qui sont le quotient de deux nombres entiers] semble supérieur à l'ensemble des nombres entiers. Cantor démontra que l'on peut appairer les nombres rationnels dans un réseau carré et associer un nombre entier à chaque nombre rationnel en traçant le chemin coloré représenté sur la figure. L'ensemble des nombres rationnels est dénombrable !

4 Cantor a prouvé qu'il existe des infinis plus grands que l'infini dénombrable [ensemble dont on peut numéroter tous les éléments]. Examinons d'abord [page ci-contre] un ensemble fini comportant trois éléments : nous dénombrons huit sous-ensembles (2^3) distincts (a). Pour un ensemble de N éléments, il existe 2^N sous-ensembles différents [chaque élément peut être, ou non, pris dans le sous-ensemble]. Construisons les sous-ensembles d'un ensemble infini dénombrable d'éléments (b). Nous démontrons par l'absurde qu'il est impossible de numéroter chaque élément de cet ensemble, donc que l'ensemble infini des sous-ensembles d'un ensemble dénombrable n'est pas dénombrable. Supposons que cela soit possible. Chaque sous-ensemble est représenté par un ensemble de cartes, chaque sous-ensemble s'étendant à l'infini vers la droite. Nous numérotions chaque sous-ensemble de haut en bas. Les numérotions-nous ainsi tous ? Non. Examinons le sous-ensemble constitué par les cartes de la diagonale et supposons que nous avons retourné toutes les

Quelle est aujourd'hui la situation entre paradoxes infinis, situations insatisfaisantes tolérées et digérées ?

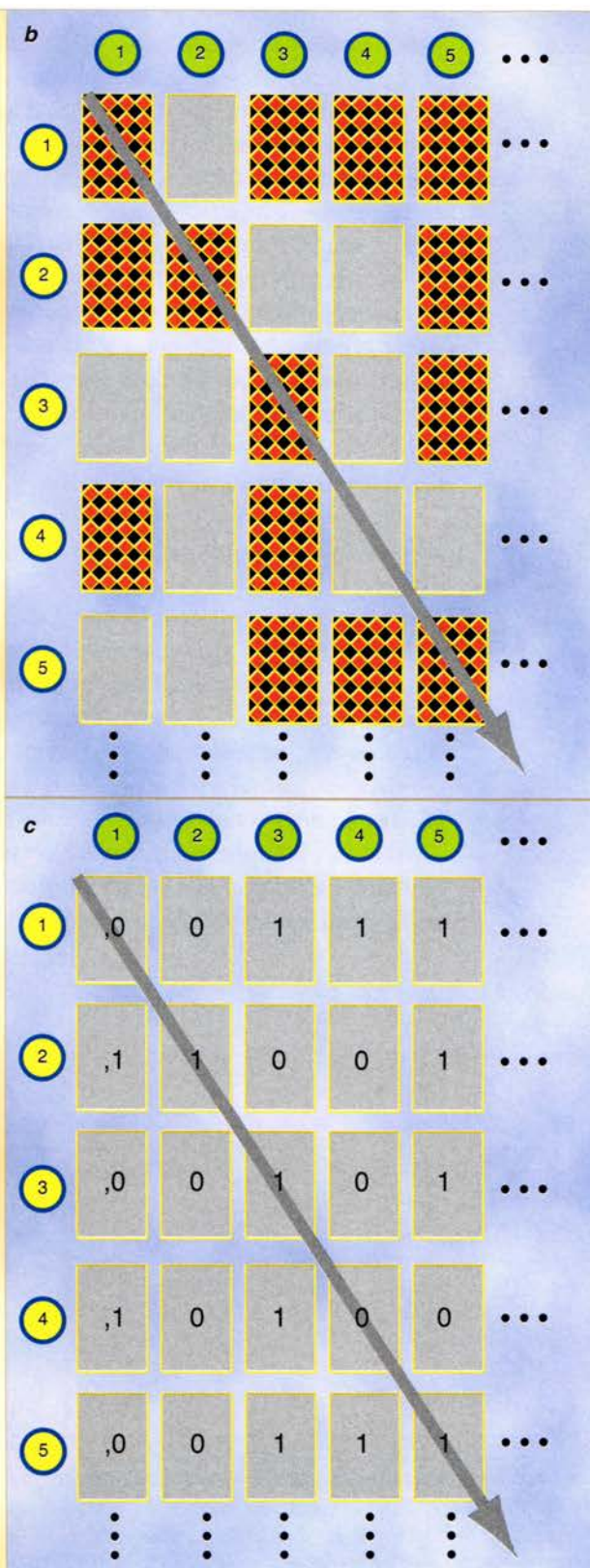
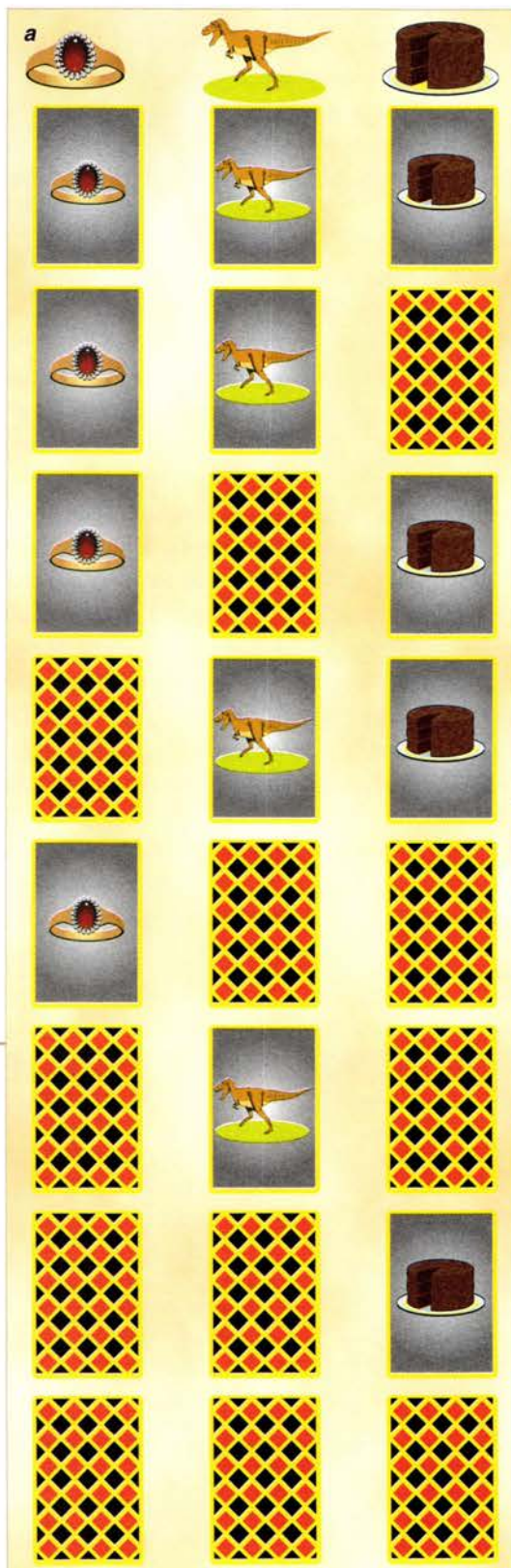
Pour le savoir, nous allons passer en revue quelques paradoxes de l'infini mathématique, paradoxes qui décideront de son histoire. À chaque fois, nous évoquerons les solutions mathématiques avancées et nous nous interrogerons pour savoir si ces solutions sont satisfaisantes en tout point ou si, au contraire, elles laissent des zones d'ombre qui marquent la limite de cette prétendue maîtrise de l'infini par le formalisme des mathématiques modernes.

L'impensable infini actuel

L'infini n'a pas été accepté facilement, et on a longtemps espéré pouvoir s'en passer. Aristote refusait l'infini actuel (ou infini en acte), c'est-à-dire pris d'un seul tenant. Il déniait toute existence physique à l'infini, mais lui reconnaissait une certaine existence mathématique, car il lui semblait nécessaire d'envisager des grandeurs de plus en plus élevées : chaque entier est suivi d'un autre ; aucun point n'est le dernier point d'une droite. Les mathématiciens ont tenté de se contenter de cet infini potentiel ou en tout cas de s'y ramener, en évitant autant que possible l'infini actuel.

Euclide, par exemple, n'énonce pas qu'il existe une infinité de nombres premiers, mais que « les nombres premiers sont en plus grande quantité que toute quantité de nombres premiers proposée », ce qu'il démontre en établissant que, si

cartes : il n'est pas identique au premier sous-ensemble, car la première carte est différente ; il n'est pas identique au deuxième, car la deuxième carte, retournée, est différente, et ainsi de suite. Le n -ième sous-ensemble diffère du nouveau sous-ensemble, car la carte numéro n est retournée. Nous avons ainsi confectionné un sous-ensemble qui ne fait pas partie de la liste. Donc l'ensemble des sous-ensembles n'est pas numérotable... Cette preuve diagonale de Cantor sert à prouver que l'ensemble des nombres réels (les nombres rationnels et les nombres irrationnels) n'est pas dénombrable. Examinons (c) les nombres réels du segment de longueur unité : la distance de chaque point à l'origine est écrite sous forme binaire 0,011010010111... Le point dont la distance à l'origine est mesurée par les chiffres inversés de la diagonale ne figure pas dans l'énumération, et il est donc impossible de numéroter tous les nombres réels du segment unité... L'ensemble des nombres réels a la puissance $2^{\aleph_0}$. C'est un infini plus grand que l'infini dénombrable.



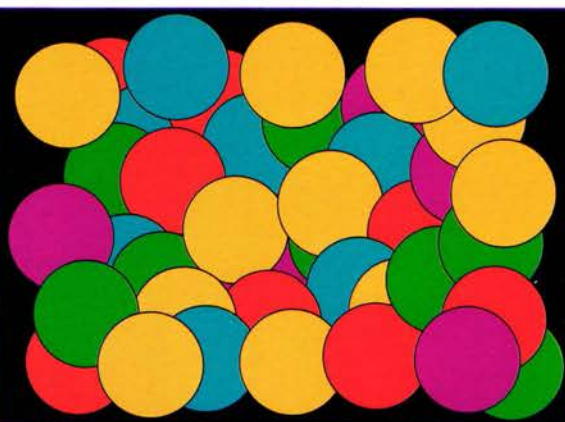
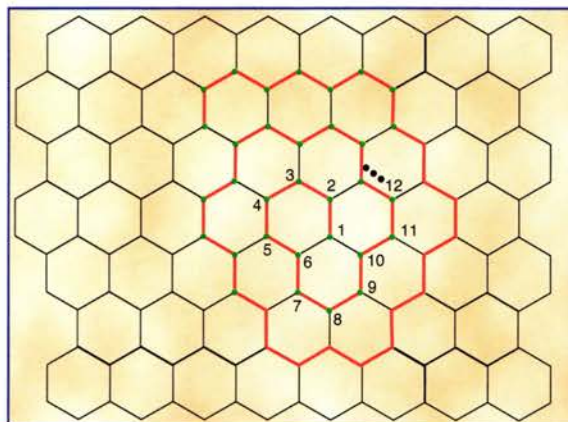
des nombres premiers sont donnés par avance $p_1, p_2, \dots, p_k$, on peut en construire un (le plus petit diviseur premier de $p_1 p_2 \dots p_k + 1$) qui sera différent de tous ceux qui étaient donnés.

La raison profonde de cette méfiance vis-à-vis de l'infini actuel est le paradoxe de la réflexivité : si un ensemble est infini, il est possible de le mettre en correspondance un à un – on dit aussi bijective, ou biunivoque – avec une de ses parties propres (c'est-à-dire différente de lui-même). La relation qui associe n^2 au nombre n , par exemple, établit une correspondance bijective entre les nombres entiers $0, 1, 2, 3, \dots$ et les nombres pairs $0, 1, 4, 9, \dots$ lesquels sont pourtant moins nombreux.

Le même problème surgit à propos du segment des nombres réels compris entre 0 et 1 (noté aujourd'hui $[0,1]$) et celui des nombres réels compris entre 0 et 2 (la correspondance bijective est celle qui, à x , associe $2x$) ; généralisant, on met sans aucune peine en correspondance bijective deux segments de droite AB et $A'B'$ quelconques. Plus gênante encore la correspondance qui à x associe $1/(x+1)$, car elle met en correspondance bijective l'intervalle des nombres réels compris entre 0 et 1, noté $]0, +1[$, et l'ensemble des nombres réels positifs, noté $]0, +\infty[$.

En quoi le paradoxe de la réflexivité est-il un paradoxe, nous demandons-nous aujourd'hui ? C'est un paradoxe, car le principe du tout et de la partie qui indique que « le tout est plus gros que la partie » y est mis en défaut. On n'imagine pas de renoncer à une vérité aussi claire. On craint que notre raison ne puisse résister à la remise en cause d'un tel principe immédiat. Reconsidérer ce principe du tout et de la partie apparaîtrait d'une audace insensée, et c'est pourquoi on a bien souvent préféré conclure que seul un être infini lui-même, Dieu par exemple, peut penser l'infini. L'Église s'opposait d'ailleurs à toute tentative des hommes de penser l'infini actuel. Saint Thomas d'Aquin considérait que quiconque pensait concevoir l'infini actuel entraînait en concurrence avec la nature unique et absolument infinie de Dieu.

Il faudra 2000 ans pour franchir cet obstacle. Le principe du tout et de la partie qui, à vrai dire, n'est guère utile en mathématiques, devait être reconsidéré : ce principe éminemment paradoxal empêchait tout progrès dans la compréhension de l'infini actuel.



5 La différence entre $\aleph_0$ et $2^{\aleph_0}$ est importante en géométrie, quand apparaissent des ensembles infinis. Ainsi le nombre de sommets d'un pavage hexagonal du plan est $\aleph_0$, car on peut tracer une spirale (en rouge), où

l'on numérote tous les sommets. En revanche, le nombre de cercles que l'on peut disposer sur une feuille finie est un infini $2^{\aleph_0}$, car le centre de chaque cercle est un point du plan.

Cette audace sera le fait du philosophe mathématicien tchèque Bernhard Bolzano (1781-1848), dont l'ouvrage *Les paradoxes de l'infini*, publié après sa mort en 1851, envisage des correspondances bijectives entre une totalité et l'une de ses parties propres, sans s'en émouvoir. Au contraire Bolzano propose de voir dans ces correspondances la caractéristique des totalités infinies, ce qui revient à abandonner, pour les totalités infinies, le principe du tout et de la partie. Plus tard, le mathématicien allemand Richard Dedekind (1831-1916) définira qu'un ensemble est infini s'il peut être mis en bijection avec une de ses parties propres: aujourd'hui, on adopte souvent cette définition en théorie des ensembles pour définir un ensemble infini.

Avant Bolzano, Gottfried Leibniz avait défendu l'idée de l'infini actuel: «Je suis tellement pour l'infini actuel qu'au lieu d'admettre que la nature l'abhorre, comme l'on dit vulgairement, je tiens qu'elle l'affecte partout, pour mieux marquer la perfection de son Auteur.» (Leibniz, *Opera omnia studio*

6. L'hypothèse du continu et la notation des aleph

Cantor proposa de noter les infinis de la façon suivante :

– L'infini des entiers est noté $\aleph_0$ (ce qui se lit aleph zéro)

– L'infini suivant est noté $\aleph_1$, etc.

Par ailleurs, l'infini des nombres réels (le continu) est noté $2^{\aleph_0}$.

La justification de cette notation est que, d'une part, on démontre que l'ensemble des nombres réels a la même taille que l'ensemble des parties de $\aleph_0$, et que, d'autre part, dans le cas fini, on montre que le nombre de parties d'un ensemble à n éléments est 2^n (par analogie, on note donc 2^a la taille de l'ensemble des parties d'un ensemble de taille a).

L'échelle des infinis donnée par le théorème fondamental de Cantor est notée: $\aleph_0$, $2^{\aleph_0}$, $2^{2^{\aleph_0}}$, etc.

La question de savoir s'il n'y a rien entre $\aleph_0$ et $2^{\aleph_0}$ s'écrit : $\aleph_1$ est-il égal à $2^{\aleph_0}$?

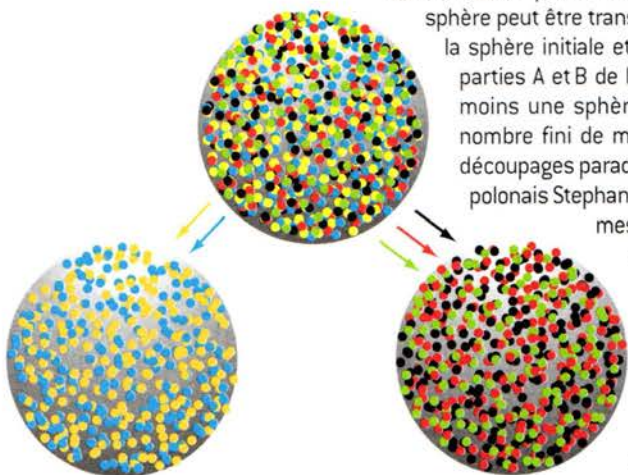
L'affirmation $\aleph_1 = 2^{\aleph_0}$ est appelée hypothèse du continu.

L'affirmation que, pour tout i : $\aleph_{i+1} = 2^{\aleph_i}$ est appelée hypothèse généralisée du continu.

Ces affirmations ont été démontrées indépendantes des axiomes classiquement acceptés pour la théorie des ensembles : jamais il ne sera possible à partir d'eux de savoir ce qu'il en est de la vérité de ces affirmations. Cela ne signifie cependant pas que tout espoir soit perdu de savoir si ces affirmations sont vraies ou fausses : il est possible que certains axiomes concernant les ensembles aient été oubliés et que, lorsque nous les découvrirons et les ajouterons aux axiomes connus, l'hypothèse du continu devienne démontrable.

7 Le paradoxe de Banach-Tarski : on établit qu'une sphère peut être décomposée en un nombre fini de morceaux, qui, une fois déplacés [sans déformation], se recomposent en deux sphères identiques à la sphère de départ. Plus généralement, une sphère peut être transformée en un cube sans aucune condition de volume sur la sphère initiale et sur le cube final. Et plus généralement encore, si deux parties A et B de l'espace sont de taille bornée et contiennent chacune au moins une sphère de rayon positif, alors on peut décomposer A en un nombre fini de morceaux qui, après déplacement, reconstitueront B. Ces découpages paradoxaux ont été découverts en 1924 par les mathématiciens polonais Stephan Banach et Alfred Tarski, qui travaillaient sur la théorie de la mesure [théorie abstraite des aires et des volumes]. Bien que

ces découpages choquent profondément le sens commun, qui s'attend à ce qu'en déplaçant des morceaux d'un objet on n'en modifie pas le volume, il n'y a pas « paradoxe » au sens strict : aucune contradiction n'est introduite dans la théorie des ensembles. Ces découpages montrent seulement que le monde du continu mathématique et les conséquences de l'axiome du choix ne correspondent pas à nos attentes intuitives.





Gottfried Leibniz
[1646-1716]



Carl Friedrich Gauss
[1777-1855]



Bernard Bolzano
[1781-1848]

Ludov. Dutens, tome II, partie X.) Bolzano place cette citation en exergue de son ouvrage révolutionnaire.

Cependant l'infini actuel que défend Leibniz est différent de celui des totalités infinies considérées actuelles dans le problème du paradoxe de la réflexivité. Leibniz défend plutôt un infini philosophique, celui du monde physique pris comme un tout. L'infiniment petit (qui est confronté à d'autres paradoxes qu'on utilise parfois pour attaquer les nouvelles méthodes de calcul que Leibniz défend) ne saura vraiment trouver une place confortable et assurée en mathématiques qu'en se débarrassant de son objectualité, c'est-à-dire quand on ne parlera plus des infiniment petits comme d'objets mathématiques, mais comme de limites.

Les mathématiciens du XX^e siècle sauront redonner aux infiniment petits un statut d'objet authentique. La méthode utilisée au XIX^e siècle pour rendre rigoureux le calcul infinitésimal est un renoncement à l'infini actuel, auquel on substitue un infini potentiel, celui de quantités qui s'approchent de plus en plus de leur limite.

Le prince des mathématiciens, Gauss (1777-1855), exprimant le sentiment partagé par la communauté mathématique de son époque, écrivait par exemple : « Je conteste qu'on utilise un objet infini comme un tout complet ; en mathématiques, cette opération est interdite ; l'infini n'est qu'une façon de parler. »

On peut donc affirmer que, malgré quelques tentatives diverses pour fonder une science mathématique de l'infini, c'est Bolzano et nul autre qui, en affrontant le paradoxe de la réflexivité, a le premier ouvert la voie à ce qui aujourd'hui est notre conception de l'infini mathématique pris comme un tout.

La solution actuelle du paradoxe de la réflexivité

La solution du paradoxe de la réflexivité proposée par Bolzano et rendue parfaitement claire par le développement ultérieur de la théorie des ensembles en termes modernes s'énonce ainsi : la relation « est contenu dans » entre ensembles ne doit pas être confondue avec la relation « avoir une taille plus petite que » : les nombres carrés sont contenus dans les nombres entiers, mais comme totalité ils ont même taille. Il est bien vrai que, si l'ensemble A est contenu dans l'ensemble B, alors la taille de A est inférieure ou égale à celle de B, mais elle peut être égale.

Au lieu de « taille », on emploie souvent le terme technique de « cardinal », mais c'est sans importance, l'idée unique de la solution du paradoxe est d'admettre qu'un ensemble A



Leopold Kronecker
[1823-1891]



Richard Dedekind
[1831-1916]



Georg Cantor
[1845-1918]



Kurt Gödel
[1906-1978]

strictement contenu dans un ensemble B a parfois la même taille. Il faut accepter ce qui paraissait paradoxal et décréter que ça ne l'est plus par une opération de dédoublement de concept: «être contenu dans» n'est pas «avoir une taille plus petite que».

Ce pas franchi, n'allons-nous pas tomber sur des contradictions qui conduiraient à une mathématique inconsistante, et donc intenable? Le jeu en vaut certainement la chandelle, mais il n'est pas facile à mener et ce sont d'autres que Bolzano qui le joueront, car, il faut bien le dire, Bolzano, comme essoufflé par l'audace de sa proposition initiale, ne mène pas le développement mathématique qu'elle appelle pourtant. L'exploration mathématique de l'algèbre des bijections sera longue et tortueuse, et Bolzano inaugure une période d'instabilité grave et de controverses parfois acerbes. Le travail principal sera fait par le mathématicien allemand Georg Cantor (1845-1918), qui découvrira de nombreuses propriétés des tailles d'ensembles infinis qui lui sembleront souvent à la limite du paradoxe. Cantor distinguera les tailles des ensembles. Si le contraire avait été vrai – c'est-à-dire si chaque ensemble infini avait pu être mis en bijection avec chaque autre –, la théorie de la taille des ensembles infinis aurait singulièrement manqué d'intérêt! Cantor s'aperçoit, en 1874, que l'ensemble des nombres réels ne peut pas être mis en bijection avec l'ensemble des nombres entiers: il est de taille strictement plus grande. Le raisonnement diagonal que Cantor découvre en simplifiant son raisonnement de 1874 sera le prototype même du raisonnement permettant de démontrer des résultats d'impossibilité en mathématiques. Dans ce théorème, on suppose que ce qu'on veut établir est faux (ici, qu'il existe une bijection entre l'ensemble $\mathbb{N}$ des entiers et l'ensemble $\mathbb{R}$ des réels), puis on joue sur la diagonale du tableau qu'elle définit (le i -ème chiffre du nombre réel $f(i)$), et l'on déduit une contradiction.

Mieux (ou pire!), Cantor montre, toujours par un raisonnement diagonal, qu'il existe une infinité de tailles possibles différentes pour les ensembles infinis. Plus précisément, un ensemble E ne peut jamais être mis en bijection avec l'ensemble de ses parties, noté $\mathcal{P}(E)$. L'ensemble $\mathcal{P}(\mathbb{N})$ des parties de $\mathbb{N}$ (qui est composé de l'ensemble des nombres pairs, de l'ensemble des nombres premiers, etc.) ne peut pas être mis en bijection avec $\mathbb{N}$. De même, l'ensemble $\mathcal{P}(\mathcal{P}(\mathbb{N}))$ (ensemble des parties de l'ensemble $\mathcal{P}(\mathbb{N})$) ne peut pas être mis en bijection avec $\mathcal{P}(\mathbb{N})$; etc.

Ces résultats constituent une première avancée dans la compréhension de l'infini actuel et la preuve que ce qu'on découvre est digne d'intérêt: les résultats construisent une hiérarchie des totalités infinies où l'esprit trouve ses repères. Ces premiers résultats ne sont pas sans soulever réprobations et critiques. Le célèbre mathématicien Kronecker est

8. Paradoxe de Russell

Soit l'ensemble des x qui ne sont pas éléments d'eux-mêmes : $E = \{x; x \notin x\}$.

Si $E \in E$, alors, par définition, $E \notin E$. Si $E \notin E$, alors, par définition, $E \in E$: c'est contradictoire !

Le paradoxe de l'ensemble des ensembles qui ne se contiennent pas eux-mêmes (paradoxe de Russell) est aujourd'hui correctement résolu en théorie des ensembles de la façon suivante.

On définit les méthodes qui permettent de créer de nouveaux ensembles à partir d'ensembles existant déjà (réunion, ensemble des parties, etc.), et il ne suffit pas de considérer une propriété (par exemple, $x \notin x$) pour pouvoir affirmer qu'il existe un ensemble regroupant tous les objets qui satisfont cette propriété. La notation $E = \{x; x \notin x\}$ ne désigne pas nécessairement un objet légitime de la théorie des ensembles sur lequel on peut raisonner comme le fait le paradoxe ; si on veut l'utiliser, il faut établir que c'est un

ensemble par utilisation des règles que fixe la théorie. Pour $E = \{x; x \notin x\}$, on n'y arrive pas. Dans la théorie Zermelo-Fraenkel (désignée par ZF), la présentation correcte du raisonnement ci-dessus est donc :

Supposons qu'il existe un ensemble défini par :

$E = \{x; x \notin x\}$.

Si $E \in E$, alors, par définition, $E \notin E$. Si $E \notin E$, alors, par définition, $E \in E$, c'est contradictoire, donc il n'existe pas d'ensemble défini par l'égalité : $E = \{x; x \notin x\}$.

Pour des raisons analogues, il n'existe pas d'ensemble de tous les ensembles, ni d'ensemble de tous les cardinaux, ou d'ensemble de tous les ordinaux. Cette solution classique aux paradoxes de la théorie des ensembles, découverts au début du XX^e siècle, réussit bien. Aucun nouveau paradoxe n'a été découvert dans la théorie ZF jusqu'à présent (voir plus de détails sur ces questions au chapitre 3 *L'ensemble de tous les ensembles*).

particulièrement sévère et il bloquera un manuscrit de Cantor en en retardant la parution dans le *Journal de Crelle*, l'un des plus prestigieux journaux de mathématiques, auquel Cantor refusera par la suite de proposer ses travaux.

Cantor découvre un résultat étonnant

L'article dont Kronecker a retardé la publication contient un résultat de Cantor tout à fait étonnant qui, bien que ne constituant pas un paradoxe, fut à n'en pas douter considéré sur le moment comme créant une situation logiquement peu satisfaisante. Cantor, toujours occupé à classer les infinis, a en effet découvert avec stupeur que l'ensemble des points d'une surface (un carré, par exemple) possède la même taille que l'ensemble des points d'un segment de droite. Du point de vue de leur taille d'ensemble infini, une droite et un plan (ou même un espace de dimension n) sont identiques. Il écrira à Dedekind à ce propos : « Je le vois, mais je ne le crois pas. »

Cantor adopte l'attitude téméraire qui consiste à accepter cette nouvelle vérité sans la décréter paradoxale, malgré la gêne qu'elle engendre. Comme aucune contradiction vérifiable ne découle des raisonnements et des calculs que Cantor élabore avec soin, il faut avoir l'audace d'accepter ce que nos facultés de raisonnement produisent et, aussi déconcertante que soit cette nouvelle réalité de l'infini actuel, il faut en poursuivre l'exploration.

À vrai dire, au tournant du XX^e siècle, certaines contradictions (ce qu'on appellera les antinomies) sembleront rendre la construction cantorienne intenable. Toutefois, en quelques années, ces difficultés seront circonscrites (plusieurs méthodes seront même proposées) et ce qui apparut à certains comme la faillite de la théorie mathématique de l'infini actuel sera en définitive l'occasion pour cette théorie de se forger une armure qu'aujourd'hui rien n'est venu sérieusement érafler.

Revenons à Cantor qui, en théoricien consciencieux, développe une arithmétique de l'infini, c'est-à-dire une extension, aux nombres qui lui servent à mesurer l'infini, des

règles de calcul qu'on applique aux nombres entiers, servant à mesurer le fini. À cette occasion, il est contraint de distinguer deux types de nombres infinis, les cardinaux et les ordinaux. Les cardinaux sont les tailles des ensembles quand on les considère de manière brute, sans tenir compte d'un possible ordre entre leurs éléments. Cantor introduit en 1893 la notation $\aleph_0$ pour le cardinal de l'ensemble des nombres entiers, $2^{\aleph_0}$ pour le cardinal du continu (l'ensemble des nombres réels), qui est le même que celui de $\mathcal{P}(\mathbb{N})$, l'ensemble des parties de $\mathbb{N}$. Il utilise $2^{2^{\aleph_0}}$ pour le cardinal de $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, etc.

L'hypothèse du continu

L'autre type de nombres infinis de Cantor, les ordinaux, sert à mesurer la taille des ensembles lorsque leurs éléments sont ordonnés selon un bon ordre (un ordre tel que toute partie de l'ensemble possède un plus petit élément). Au-delà des ordinaux finis, qu'on assimile aux nombres entiers, il y a ω , le premier ordinal transfini, puis $\omega+1$, $\omega+2$, etc., qu'on obtient en ajoutant des unités une à une à ω . Plus loin encore, on trouve 2ω , $2\omega+1$,... puis ω^2 , ω^ω , etc.

Cantor découvre alors un problème qui finalement se révélera d'une difficulté qu'aujourd'hui encore nous n'avons pas totalement maîtrisée : l'hypothèse du continu.

Le cardinal de l'ensemble des nombres réels $\mathbb{R}$, ce qu'on appelle le continu et qui est mesuré par $2^{\aleph_0}$, est strictement plus grand que le cardinal des entiers (appelé infini dénombrable et mesuré, nous l'avons dit, par $\aleph_0$). Mais y a-t-il un autre cardinal entre les deux ? L'hypothèse du continu est l'affirmation qu'entre ces deux tailles d'ensembles infinis, $\aleph_0$ et $2^{\aleph_0}$, il n'y en a pas d'autres. Comme Cantor désigne par $\aleph_1$ le plus petit des cardinaux plus grands que $\aleph_0$, l'hypothèse du continu est simplement l'affirmation $2^{\aleph_0} = \aleph_1$. (L'hypothèse généralisée du continu est l'affirmation que $2^{\aleph_s} = \aleph_{s+1}$ pour tout s .)

Deux situations sont envisageables : soit (a) il n'y a pas d'autres tailles infinies entre $\mathbb{N}$ et $\mathbb{R}$, ce qui est équivalent à dire que « tout sous-ensemble infini de $\mathbb{R}$ peut être mis

9. Paradoxe de l'autoréférence et de l'infini

Chacun connaît le paradoxe du menteur. Un personnage dit « je mens ». S'il dit vrai, alors il ment, donc il ne dit pas vrai : c'est absurde. S'il ment, alors ce qu'il dit est vrai, et donc il ne ment pas : c'est absurde. On résout ce paradoxe en disant qu'il faut s'interdire les phrases autoréférentes. Les choses ne sont peut-être pas si simples, car on s'est aperçu récemment que l'introduction de l'infini permet d'éviter l'autoréférence tout en maintenant une situation paradoxale.

Soit une infinité de personnes placées en rang :

$s(0), s(1), \dots, s(n), \dots$

Chacune dit : « Au moins une personne derrière moi ment. »

Qui dit vrai ? Qui ment ?

D'après le sens des phrases prononcées :

- derrière toute personne qui dit vrai, il y a au moins une personne qui ment ;

- si une personne ment, alors toutes les personnes derrière elle disent vrai.

Si on désigne par M les personnes qui mentent et par H celles qui sont honnêtes et ne mentent pas, les deux règles précédentes se traduisent :

- derrière tout H, il y a au moins un M ;
- derrière un M, il n'y a que des H.

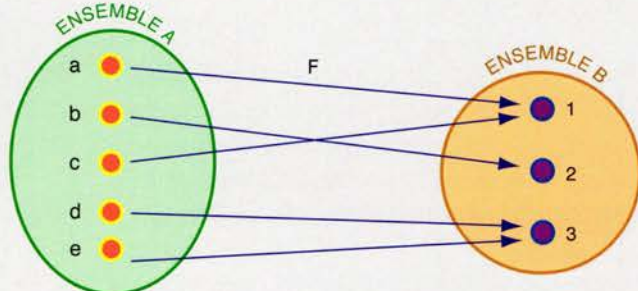
Il est impossible de concevoir une suite de M et de H qui vérifie ces deux règles (car tout M doit être suivi uniquement de H, ce qui ne se peut pas, puisque tout H doit être suivi d'au moins un M). Comme dans le cas du menteur, mais cette fois à cause de l'infini des personnes, la situation est paradoxale. Ces paradoxes, dits sémantiques, sont encore examinés par les logiciens, et aucune solution totalement satisfaisante ne semble en avoir été trouvée.

en bijection avec $\mathbb{N}$ ou avec $\mathbb{R}$ » (c'est là un énoncé simple et, en apparence, très concret) ; soit (b) il y en a d'autres et alors il faudrait savoir combien et comment on les obtient. Nul ne peut prétendre disposer d'une idée claire des nombres réels s'il n'a une réponse précise au problème de l'hypothèse du continu. Cantor s'épuisera à le résoudre

et n'y réussira pas, bien qu'il ait parfois pensé, à tort, avoir résolu la question.

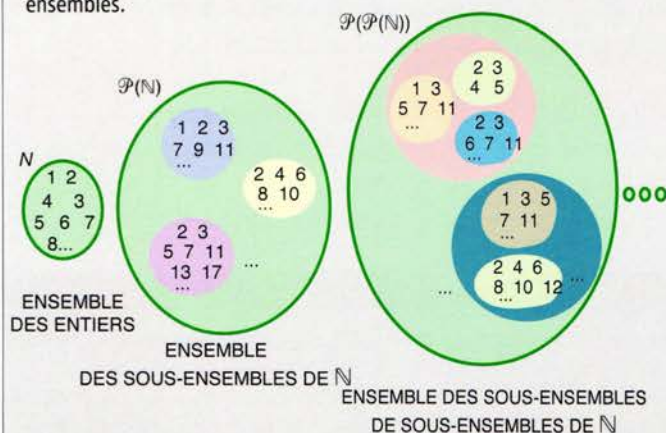
10. Un axiome définissant un grand cardinal

Une surjection de A vers B est une application F qui atteint tout point de B : pour tout élément β dans l'ensemble B, il existe un élément α de l'ensemble A tel que $F(\alpha) = \beta$.



S'il existe une surjection de l'ensemble A vers l'ensemble B, on dit que A est plus gros que B. Si, de plus, il n'existe pas de surjection de B vers A, on dit que A est strictement plus gros que B.

Cantor a montré que l'ensemble $\mathcal{P}(A)$ des parties d'un ensemble A est toujours strictement plus gros que l'ensemble A. Il en résulte qu'il existe une infinité d'ensembles de plus en plus gros, $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, et, accessoirement, qu'il n'existe pas d'ensemble de tous les ensembles.



Voici un exemple d'axiome de grands cardinaux : il existe un ensemble non dénombrable A tel que, si A est strictement plus gros que B, alors A est aussi strictement plus gros que l'ensemble $\mathcal{P}(B)$ des parties de B, plus gros que l'ensemble $\mathcal{P}(\mathcal{P}(B))$ des parties de $\mathcal{P}(B)$, etc., et plus généralement, plus gros que tout ensemble définissable à partir de l'ensemble B. Le cardinal de A est un grand cardinal. Cependant ces axiomes sont, dans la grande majorité des cas, des indécidables de Gödel : avec les axiomes habituels de la théorie des ensembles, on ne peut prouver ni qu'ils sont vrais ni qu'ils sont faux. Il faut donc les accepter tels quels, sans que l'on puisse espérer les démontrer à partir des axiomes de la théorie des ensembles. Ils sont pourtant utiles.

L'indécidabilité ne résout rien

Plus tard, la théorie des ensembles formalisée, deux résultats importants furent démontrés concernant l'hypothèse du continu. En 1938, le mathématicien autrichien Kurt Gödel prouva que, si la théorie habituelle des ensembles est consistante (ne conduit pas à une contradiction), alors la même théorie complétée par l'axiome qui affirme que l'hypothèse du continu est vraie ne conduit pas plus à une contradiction. Admettre l'hypothèse du continu n'est donc pas susceptible de faire s'effondrer la théorie usuelle des ensembles. En 1963, Paul Cohen ira plus loin : si la théorie des ensembles est consistante, alors la même théorie complétée en ajoutant l'affirmation que l'hypothèse du continu est fausse est, elle aussi, sans contradiction.

Ces deux résultats regroupés permettent de dire que celui qui admet la théorie usuelle des ensembles peut, sans risque supplémentaire de contradiction, prendre l'hypothèse du continu ou prendre sa négation. La théorie des ensembles laisse le choix aux mathématiciens de considérer l'hypothèse du continu comme vraie ou comme fausse.

Cette indécidabilité de l'hypothèse du continu n'est pas un paradoxe : la théorie ne se contredit pas,

au contraire elle ne dit rien. Toutefois cette *sous-détermination* est logiquement très insatisfaisante et profondément troublante.

En effet, considérons le monde des nombres entiers : il n'est pas arbitraire, ce n'est pas nous qui décidons si un nombre est pair ou impair, premier ou composé, etc. Pourquoi donc le monde des nombres réels serait-il arbitraire, et nous permettrait de décider en fonction de nos goûts qu'il existe des parties infinies de $\mathbb{R}$ impossibles à mettre en bijection avec $\mathbb{N}$ ou $\mathbb{R}$, ou qu'au contraire il n'en existe pas ?

Comme le pensait Cantor lui-même, ainsi que Gödel, l'hypothèse du continu doit être vraie ou fausse, et la théorie des ensembles doit nous permettre de le savoir, à moins qu'elle ne soit qu'une illusion, ce qui signifierait que la compréhension qu'elle nous donne de l'infini actuel est factice. La situation créée par les résultats de Gödel et de Cohen sur l'hypothèse du continu est logiquement insatisfaisante, mais c'est toute la signification de la théorie de l'infini actuel proposée par Cantor qui est en cause, et, finalement, c'est l'idée même d'une théorie de l'infini actuel qui se joue.

Voies pour aller plus loin

L'indécidabilité de l'hypothèse du continu ne règle donc pas la question de l'infini, mais au contraire l'exacerbe : si vraiment la théorie des ensembles fournit une compréhension de l'infini actuel et n'est pas qu'un jeu gratuit entre symboles mathématiques, sans contrepartie dans le monde réel, il doit être possible d'avancer encore.

Une première voie consiste à remettre en cause la théorie usuelle des ensembles. Cette théorie, notée ZF (en l'honneur des deux mathématiciens E. Zermelo et A. Fraenkel qui la définirent au début du XX^e siècle), peut être jugée insatisfaisante pour diverses raisons. En particulier, parce qu'elle engendre des situations contraires à l'intuition concernant l'existence d'objets mathématiques qu'on ne peut pas construire (*voir la figure 7*). Diverses éventualités, théorie des types, théorie constructiviste des ensembles, théorie des ensembles avec ensemble universel, etc., ont été proposées sans toutefois retenir vraiment l'attention des mathématiciens, qui restent attachés à la simplicité de Zermelo-Fraenkel et ne semblent pas trouver très grave la situation créée par l'hypothèse du continu. Il est vrai que ces théories alternatives obligent à réévaluer tout le travail mathématique déjà fait, alors qu'aucune véritable contradiction n'est apparue. Seule une insatisfaction philosophique pousse certains à vouloir abandonner Zermelo-Fraenkel.

La seconde voie consiste à admettre que Zermelo-Fraenkel est satisfaisante, c'est-à-dire qu'elle n'énonce que des choses acceptables pour les ensembles, mais qu'elle est incomplète. Certains axiomes manqueraient, et le travail du logicien et du mathématicien serait de les rechercher pour les ajouter. Ces axiomes découverts (ou au moins certains d'entre eux), l'hypothèse du continu ou sa négation deviendrait prouvable.

Cette seconde voie n'est pas du tout absurde et, en insistant sur l'incomplétude actuelle de la théorie des ensembles, on ne fait que prendre au sérieux les théorèmes généraux d'incomplétude démontrés par Kurt Gödel en 1931, dont l'indécidabilité de l'hypothèse du continu ne serait qu'une manifestation en théorie des ensembles. Cette seconde voie conduit au programme de recherche de trouver de nouveaux axiomes à ajouter à la théorie des ensembles, programme que Kurt Gödel lui-même a défendu (*voir le chapitre 2*).

Les travaux faits en logique mathématique sur ce que l'on dénomme les grands cardinaux constituent le domaine de recherche d'où pourrait provenir la solution de l'énigme de

l'hypothèse du continu (une partie infinie de $\mathbb{R}$ est-elle toujours en bijection avec $\mathbb{N}$ ou $\mathbb{R}$?), tout en étant le domaine où les mathématiciens rencontrent de nouveaux infinis actuels dont la taille vertigineuse aurait fait tourner la tête à Cantor lui-même.

Les grands cardinaux

Les axiomes de grands cardinaux sont des affirmations portant sur des ensembles monstrueusement grands. Délicats à définir, ils procèdent de principes analogues à celui qui consiste à affirmer que non seulement $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, ... sont des infinis actuels légitimes, mais qu'il y en a de plus grands encore, dont certains qui contiennent à la fois $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$,

Les axiomes de grands cardinaux sont vis-à-vis de la théorie Zermelo-Fraenkel comme l'est l'hypothèse du continu : on peut choisir, sans risquer d'introduire de contradiction, de les ajouter ou d'ajouter leur négation (en fait, les ajouter pourrait, en théorie, introduire une contradiction, mais personne en pratique n'en trouve jamais). Toutefois, contrairement à ce qui se passe pour l'hypothèse du continu, il est naturel de les tenir pour vrais. En effet, adopter leur négation serait limiter la taille des ensembles possibles, ce qui n'est pas naturel. De plus, cette même négation contredit un principe d'ouverture et de tolérance qui suggère d'accepter tous les objets qui n'introduisent pas d'incohérence. On dit que les axiomes des grands cardinaux sont vrais *a priori*. Une autre raison conduit à accepter les axiomes des grands cardinaux. D'une façon qui a étonné les mathématiciens, ces axiomes de grands cardinaux se classent linéairement les uns par rapport aux autres comme s'ils désignaient véritablement une hiérarchie d'infinis (au-delà de celle mise en lumière par Cantor et la complétant). S'ils n'étaient qu'un jeu formel et gratuit de logiciens, rien n'expliquerait qu'ils s'ordonnent ainsi les uns relativement aux autres. Pour les logiciens K. Kanamori et M. Magidor, «cet aspect hiérarchique de la théorie des grands cardinaux est quelque peu mystérieux, mais c'est aussi un argument fort en faveur de l'adoption des axiomes de grands cardinaux et du fait qu'ils fournissent les extensions naturelles de Zermelo-Fraenkel».

La possibilité de trouver des liens entre les axiomes de grands cardinaux et l'hypothèse du continu est réelle, et des résultats partiels ont déjà été obtenus : certaines parties infinies de $\mathbb{R}$ dont on ne sait pas montrer dans Zermelo-Fraenkel qu'elles peuvent être mises en bijection avec $\mathbb{N}$ ou $\mathbb{R}$, peuvent être mises en bijection avec $\mathbb{N}$ ou $\mathbb{R}$ grâce aux axiomes de grands cardinaux.

La théorie que Cantor a créée semblerait donc tenir debout et, mieux que cela, progresser par ajouts de nouveaux axiomes naturels. L'infini actuel n'est ni paradoxal ni logiquement insatisfaisant (comme l'indécidabilité de l'hypothèse du continu nous a conduit à le craindre un moment), mais au contraire cohérent et vraisemblable. Comme en physique, où notre conception du temps et de l'espace a dû être revue à la lumière de la théorie de la relativité (laquelle, en dépit des premières apparences, n'est nullement paradoxale), en mathématiques la conception de l'infini actuel force à reconstruire notre idée des objets et à revoir notre conception de la réalité mathématique. À celui qui accepte cette réforme profonde des conceptions, on ne peut opposer aucun paradoxe. On peut même penser que les situations logiquement insatisfaisantes qu'on croit encore percevoir se dissiperont à mesure que notre esprit acceptera pleinement le nouvel univers conceptuel proposé par ces mathématiques de l'infini actuel, qu'aujourd'hui encore les mathématiciens affinent et perfectionnent.

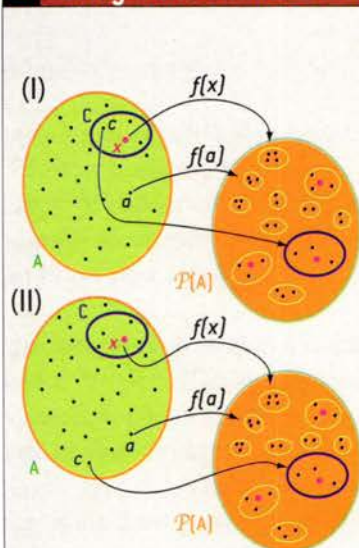
Imaginer l'infini, ou le découvrir ?

La science de l'infini progresse. De nouveaux axiomes conduisent à la résolution de l'énigme du continu : existe-t-il un infini intermédiaire entre celui des entiers et celui des réels ?

L'infini est-il réel ou n'est-ce qu'une fiction de mathématiciens ? Pour répondre à cette question, le logicien examine les propriétés de l'infini. Si tout est possible et qu'aucun outil ne nous fait avancer dans la connaissance de l'infini, c'est qu'il est imaginaire et que nous l'inventons. Si, au contraire, des vues cohérentes et contraignantes s'imposent et que des idées naturelles et variées déterminent d'une manière concordante ses propriétés, c'est qu'au-delà des axiomes, des démonstrations et des formalismes mathématiques, il y a bien un infini véritable hors de nous.

L'hypothèse du continu (il n'y a pas d'ensembles infinis de taille intermédiaire entre l'ensemble des entiers et l'ensemble des réels) concerne une propriété élémentaire de l'infini qu'on ne réussissait pas à trancher. Les progrès obtenus ces dernières années pour sa résolution (l'hypothèse doit-elle être acceptée ou rejetée ?) suggèrent qu'elle est fausse et que l'infini n'est pas une invention libre de théoriciens, mais bien une réalité que le génie des chercheurs,

1. Il y a une infinité d'infinis



L'une des plus importantes découvertes de Cantor est qu'il existe une infinité de types différents d'infinis. Cela résulte de ce que l'ensemble $\mathcal{P}(A)$ des parties de A ne peut pas être mis en bijection avec A .

En voici la démonstration : supposons qu'il existe une bijection f de A sur $\mathcal{P}(A)$ reliant chaque élément a de A à chaque élément $f(a)$ de $\mathcal{P}(A)$. Nous allons en déduire une contradiction. Définissons un sous-ensemble C de l'ensemble A , l'ensemble $C = \{x; x \text{ est dans } A \text{ et } x \text{ n'est pas élément de l'élément } f(x) \text{ de } \mathcal{P}(A)\}$. Puisque C est une partie de A (éventuellement vide), c'est un élément de $\mathcal{P}(A)$; comme f est bijective (par hypothèse), il existe un certain c (unique) de A tel que $C = f(c)$. Si c est dans C (schéma I), alors il possède la propriété que possèdent par définition les éléments de C , et donc c n'est pas élément de $f(c) = C$. C'est absurde. Si c n'est pas dans C (schéma II), alors c n'est pas élément de $f(c)$, donc par définition de C , c est dans C . C'est absurde.

Cette contradiction montre que f n'existe pas. Cette démonstration est à rapprocher du paradoxe du barbier qui rasait tous les barbiers qui ne se rasent pas eux-mêmes : on ne peut pas dire que le barbier se rase, ni qu'il ne se rase pas.

$\mathcal{P}(A)$ qui est au moins aussi gros que A est donc strictement plus gros que A .

Partant de $\mathbb{N}$ l'ensemble infini des nombres entiers, grâce au résultat précédent, on obtient une première échelle d'ensembles infinis : $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$, ...

en particulier Hugh Woodin, nous fait mieux connaître. L'intelligibilité et la cohérence des vues sur l'infini élaborées par les logiciens confortent l'idée que l'infini préexiste à la découverte que nous en faisons et qu'en le comprenant nous en observons la réalité.

Selon Patrick Dehornoy, de l'Université de Caen : « Les résultats de H. Woodin montrent que le problème du continu et, plus généralement, la notion d'infini non dénombrable ne sont pas intrinsèquement vagues et inaccessibles à l'analyse, mais peuvent faire l'objet d'une véritable théorie conceptuelle allant bien au-delà de l'exploration formelle des conséquences d'axiomes plus ou moins arbitraires. »

Galilée remarqua qu'il y avait autant de nombres entiers que de nombres carrés : l'ensemble des entiers peut être mis en bijection avec l'ensemble des carrés $0 \rightarrow 0$; $1 \rightarrow 1$; $2 \rightarrow 4$; $3 \rightarrow 9$; etc. À chaque élément du premier ensemble correspond un élément unique du second, sans oubli et sans répétition. On concluait de ce « paradoxe de Galilée » que la compréhension de l'infini était réservée à Dieu... ou bien que l'infini n'existait pas.

Le génie de Cantor

Si le mot génie a un sens, alors il s'applique à Georg Cantor (1845-1918). Cantor fait progresser fondamentalement la question en démontrant, vers 1874, que l'ensemble des nombres réels est plus gros (ne peut pas être mis en bijection) avec celui des entiers et ce résultat pose la base mathématique d'une théorie rigoureuse de l'infini. Aujourd'hui les chercheurs explorent cet infini cantorien construisant une science pleine de surprises qui, décennie après décennie, devient plus précise, plus riche... et plus difficile.

Un résultat fondamental de Cantor est qu'aucun ensemble E ne peut être mis en bijection avec l'ensemble de ses parties $\mathcal{P}(E)$. Pour les ensembles finis, c'est évident, car par exemple $E = \{a, b, c\}$ possède trois éléments alors que l'ensemble de ses parties $\mathcal{P}(E) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ en possède huit (plus généralement un ensemble à n éléments possède 2^n parties). Dans le cas des ensembles infinis, c'est moins évident, mais vrai aussi : $\mathcal{P}(E)$ est toujours plus grand que E (voir l'encadré 1). Cela donne une infinité de types d'infinis différents, de plus en plus gros.

– Il y a l'infini de $\mathbb{N}$, l'ensemble des nombres entiers : $\{0, 1, 2, \dots\}$. Cet infini, noté $\aleph_0$, est dénommé *infini dénombrable*.

– Il y a l'infini de $\mathcal{P}(\mathbb{N})$, l'ensemble des parties de $\mathbb{N}$. Cet ensemble $\mathcal{P}(\mathbb{N})$ se met facilement en bijection avec l'ensemble des nombres réels, $\mathbb{R}$, et constitue *le continu*, noté $2^{\aleph_0}$.

– Il y a plus gros encore, l'infini de $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, l'ensemble des parties de $\mathcal{P}(\mathbb{N})$, noté $2^{2^{\aleph_0}}$, etc.

Par ailleurs, à côté de cette première série infinie d'infinis, la théorie de Cantor indique qu'il existe aussi un plus petit type d'infini juste au-dessus de $\aleph_0$, noté $\aleph_1$, et un autre juste au-dessus de $\aleph_1$, noté $\aleph_2$, etc.

Disposant ainsi de deux hiérarchies d'infinis, la question naturelle qu'il se pose est : ces deux hiérarchies coïncident-elles ? Autrement dit, $\aleph_1$ est-il égal à $2^{\aleph_0}$? $\aleph_2$ est-il égal à $2^{\aleph_1}$, ..., $\aleph_k$ est-il égal à $2^{\aleph_{k-1}}$, ... ? La première égalité de cette liste est équivalente à l'affirmation que tout sous-ensemble infini de l'ensemble $\mathbb{R}$ des nombres réels se met en bijection avec $\mathbb{N}$ ou avec $\mathbb{R}$. C'est l'*Hypothèse du continu*, notée HC, qui s'écrit donc : $\aleph_1 = 2^{\aleph_0}$. Cette question occupera une partie de la fin de la vie de Cantor qui croyait à l'exactitude de l'hypothèse du continu. Il ne réussira malheureusement pas à la prouver et il est possible que cet échec ait contribué à la détérioration de sa santé mentale.

La question est importante : si la théorie des ensembles infinis est bien la théorie d'une réalité que nous ne fixons pas nous-mêmes, nous devons régler la question de l'hypothèse du continu de manière positive ou négative : il y a ou il n'y a pas d'ensembles infinis de taille intermédiaire entre celle de $\mathbb{N}$ et celle de $\mathbb{R}$!

Notons qu'un des adversaires de Cantor, le mathématicien Kronecker, pensait que les infinis hiérarchisés de Cantor sont une illusion (une «vue de l'esprit»), ce qu'il exprima par cette phrase restée célèbre : «Dieu a créé les nombres entiers; le reste est l'œuvre de l'homme.»

La question de l'hypothèse du continu fut reconnue comme centrale et David Hilbert la plaça à la tête de sa liste des 23 questions mathématiques à résoudre pour le XX^e siècle, liste dont il fit l'énumération à Paris en 1900 lors du Deuxième congrès international de mathématiques. Malgré cette position centrale, les progrès seront lents. Dans un premier temps, ils conduiront à des résultats qu'on interprétera le plus souvent comme des indications que l'infini de Cantor est une fiction théorique.

L'axiomatisation habituelle de la théorie des ensembles est notée ZFC à partir des initiales des mathématiciens Ernst Zermelo (1871-1953) et Abraham Fraenkel (1891-1965), le C indiquant qu'on accepte l'axiome du choix.

Kurt Gödel (1906-1978) prouve en 1938 que si ZFC est non contradictoire alors ZFC + HC (ce qu'on obtient en ajoutant l'axiome affirmant l'hypothèse du continu) est aussi une théorie non contradictoire. En clair : accepter HC n'introduit pas de contradictions, s'il n'y en a pas déjà.

La méthode de Gödel consiste à se donner une structure qui vérifie les axiomes de ZFC, puis à en extraire une sous-structure (comme on extrait le sous-corps $\mathbb{R}$ des nombres réels, du corps des nombres complexes $\mathbb{C}$). La sous-structure vérifie toujours les axiomes de ZFC, mais vérifie en plus HC. Si ZFC est non contradictoire, cette construction montre que ZFC + HC l'est aussi : la non-contradiction de ZFC implique celle de ZFC + HC.

2. Le dieu d'Anselme et le maximalisme ontologique

Anselme de Cantorbéry (1034-1109) prétendait prouver l'existence de Dieu par un maximalisme ontologique étrangement semblable à celui des logiciens modernes : «Dieu s'il existe est parfait argumente Anselme. Mais la perfection implique l'existence. L'existence est une qualité supérieure à l'inexistence, donc fait partie de la perfection. Comme Dieu a toutes les qualités, il doit exister, il existe donc.»

Dans le *Proslogion*, Anselme explique que l'existence réelle est encore plus parfaite que l'existence en pensée : «Nous croyons que tu es quelque chose de tel que rien de plus grand ne puisse être pensé. Est-ce qu'une telle nature n'existe pas, parce que l'insensé a dit en son cœur : Dieu n'existe pas ? Mais du moins cet insensé, en entendant ce que je dis : quelque chose de tel que

rien de plus grand ne puisse être pensé, comprend ce qu'il entend ; et ce qu'il comprend est dans son intelligence, même s'il ne comprend pas que cette chose existe. Autre chose est d'être dans l'intelligence, autre chose d'exister. [...] Et certes l'Être qui est tel que rien de plus grand ne puisse être pensé, ne peut être dans la seule intelligence ; même, en effet, s'il est dans la seule intelligence, on peut imaginer un être comme lui qui existe aussi dans la réalité et qui est donc plus grand que lui. Si donc il était dans la seule intelligence, l'être qui est tel que rien de plus grand ne puisse être pensé serait tel que quelque chose de plus grand pût être pensé.»

Anselme utilise les paradoxes de l'infini (Dieu) à des fins positives contrairement aux Grecs qui y voyaient des apories.



Cette méthode de construction de *modèles internes* est importante, mais elle n'est pas suffisante pour démontrer que l'on peut aussi ajouter non-HC (la négation de HC) à ZFC.

Une méthode « externe », le « forcing », introduite par Paul Cohen (1934-2007), est comparable à ce qu'on fait classiquement en mathématiques quand, partant de $\mathbb{N}$, l'ensemble des entiers positifs ou nuls, on introduit de nouveaux nombres pour obtenir $\mathbb{Z}$ (l'ensemble des entiers relatifs), ou lorsque l'on construit le corps des nombres réels $\mathbb{R}$ à partir du corps des nombres rationnels $\mathbb{Q}$. Cohen montra en 1963 que l'on peut tout aussi bien ajouter non-HC à ZFC sans introduire de contradiction. Dans un tel forcing, on part d'une structure qui vérifie ZFC, puis on introduit de nouveaux éléments dans cette structure, ce qui l'agrandit. Bien menée, cette extension produit une nouvelle structure vérifiant cette fois ZFC et la négation de HC, car, par exemple, on a $2^{\aleph_0} = \aleph_2$.

Choisissez vous-même !

Le résultat de Cohen associé à celui de Gödel signifie que les axiomes de ZFC sont extensibles soit par HC, soit par non-HC sans que cela introduise de contradiction (à condition qu'il n'y en ait pas déjà). L'axiome HC est indépendant des autres, on dit aussi « HC est indécidable dans ZFC » : on a le libre choix entre HC et non-HC ! Cette liberté de choix a souvent été interprétée dans un sens antiréaliste : l'infini n'existe pas réellement, il est ce que nous voulons qu'il soit !

Gödel n'était pas de cet avis et pensait d'ailleurs que l'hypothèse du continu est fausse. L'idée qu'il défendait constitue ce qu'on nomme parfois la doctrine des axiomes manquants. Il écrivait :

« Si le sens des termes de base de la théorie des ensembles est admis, il en résulte que les concepts ensemblistes et les théorèmes de la théorie des ensembles décrivent une réalité bien déterminée à propos de laquelle la conjecture de Cantor [l'hypothèse du continu] est vraie ou fausse. Son indécidabilité à partir des axiomes connus aujourd'hui signifie nécessairement que ces axiomes ne donnent pas une description complète de cette réalité. »

Le travail du mathématicien et du logicien doit donc, selon cette doctrine, être la recherche de nouveaux axiomes qui, associés à ceux de ZFC, permettront de démontrer soit que HC est vraie, soit que HC est fausse. Cette recherche de nouveaux axiomes doit se fonder sur des critères séparant les « bons axiomes » (conformes aux propriétés des *vrais ensembles*) des « mauvais axiomes ». Quels peuvent être ces critères ?

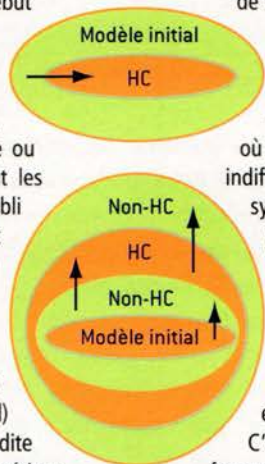
Le premier d'entre eux est bien sûr la non-contradiction : un axiome nouveau ne doit pas contredire les axiomes usuels de ZFC qui ont été posés parce qu'évidents en eux-mêmes. L'axiome du choix a, lui aussi, été montré indépendant des autres axiomes de ZFC par Gödel et Cohen et on le considère comme vrai.

Le second critère permettant de considérer qu'un axiome est acceptable est le *maximalisme ontologique*. L'idée en est assez simple : tout axiome qui affirme que l'univers des ensembles est grand doit être adopté, car l'univers des ensembles, s'il existe, n'est limité par aucun principe et est donc aussi grand que tout ce qui est possible. Tout principe mathématique affirmant l'existence d'ensembles de grande taille est vrai *a priori* selon ce maximalisme ontologique qui sert donc de guide concret à la recherche de nouveaux axiomes naturels pour enrichir ZFC.

Le premier axiome conforme au maximalisme ontologique n'est pas nouveau et appartient déjà à ZFC, car c'est celui qui affirme que l'univers des ensembles en contient qui sont

3. ZF, modèles internes et modèles externes

La théorie des ensembles a été axiomatisée au début du xx^e siècle. Le système d'axiomes de Zermelo-Fraenkel avec axiome du choix (ZFC) est considéré comme une base convenable pour cette théorie (on n'y a jamais trouvé de contradiction). Pour savoir si l'hypothèse du continu est vraie ou fausse, on cherche à la démontrer en utilisant les axiomes de ZFC. Malheureusement, il a été établi qu'on ne parviendrait jamais à établir non-HC (Gödel, 1938) ou HC (Cohen, 1963) à partir de ZFC, sauf si ZFC est contradictoire. La méthode consiste à partir d'une structure satisfaisant les axiomes de ZFC (on dit « modèle de ZFC »), puis à construire à partir de ce modèle une autre structure qui satisfait en plus HC (Gödel) ou non-HC (Cohen). La méthode de Gödel est dite interne, car le nouveau modèle est extrait de l'intérieur



de celui donné au départ. La méthode de Cohen, nommée forcing, est externe, car elle procède par extension du modèle initial qu'on fait grossir. Le forcing peut être opéré plusieurs fois conduisant successivement à des modèles où HC est fausse, puis vraie, puis fausse, etc. Cette indifférence du forcing au sujet de HC marque une symétrie entre HC et non-HC et ne fournit donc pas d'indices pour préférer HC à non-HC ou l'inverse. Une idée importante, étudiée ces dernières années, a été la recherche de nouveaux axiomes qui provoquent une rupture de symétrie entre HC et non-HC. Il semble que lorsque la rupture de symétrie est possible, elle favorise toujours non-HC. C'est la base de l'argument de Hugh Woodin en faveur de non-HC.

infinis. La théorie ZFC dont on retire l'axiome affirmant qu'il existe des ensembles infinis pour le remplacer par sa négation « Tout ensemble est fini » est une théorie équivalente à l'arithmétique, une théorie intéressante, mais limitée. L'adoption de l'axiome de l'infini fait entrer dans le véritable univers mathématique qui accepte les objets infinis, comme les nombres réels utilisés dans les sciences de la nature.

Maximalisme ontologique

Aller au-delà de ce maximalisme ontologique de base – l'affirmation qu'il y a des ensembles infinis – a été une occupation centrale de la théorie des ensembles depuis 50 ans et a donné naissance à une multitude d'axiomes nouveaux baptisés « axiomes de grands cardinaux ». Voici un exemple simple : le maximalisme ontologique nous force à admettre qu'il existe un ensemble plus gros que tous ceux de la série : $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$... Ces ensembles infinis de plus en plus gros font frémir tant leur taille s'accroît rapidement en allant vers la droite (l'essentiel des mathématiques habituelles se satisfait des 4 premiers niveaux). Pourtant il en existe de plus gros encore !

Dans cette quête fructueuse d'axiomes de grands cardinaux, les logiciens espéraient que l'un des axiomes découverts et étudiés aurait une incidence sur l'hypothèse du continu, soit parce qu'avec l'adoption de cet axiome supplémentaire on démontrerait qu'elle est vraie, soit parce qu'on démontrerait qu'elle est fausse. Si cela s'était produit, le problème de HC aurait été considéré comme définitivement réglé. En effet, un axiome naturel (car conforme au principe du maximalisme ontologique) aurait fixé le statut de HC, et donc, sans avoir à ajouter HC (ou non-HC) aux axiomes de ZFC, mais en ajoutant seulement cet axiome naturel, nous aurions disposé d'une théorie de l'infini tranchant d'une manière non arbitraire la question qui hantait Cantor.

Malheureusement cette attente d'un règlement de l'hypothèse du continu par les axiomes de grands cardinaux a été déçue et, à l'inverse, on a pu établir que de larges classes

d'axiomes de grands cardinaux étaient sans effet sur HC. Le maximalisme ontologique laisse donc, en apparence, toujours le libre choix d'adopter ou de rejeter HC.

Stabiliser les entiers et au-delà

Cet échec temporaire de la doctrine des axiomes supplémentaires, et donc de l'idée que l'infini est une réalité déterminée, nous contraint à rechercher d'autres critères pour la formulation d'axiomes acceptables. Le plus important d'entre eux est assez subtil, mais c'est de lui que viennent les progrès récents et l'espoir d'une solution proche de HC.

La méthode du forcing de Cohen est très puissante et dans certains cas presque trop. On peut ainsi agrandir par forcing un modèle de ZFC et s'arranger pour que HC devienne fausse (c'est ce qu'a proposé Cohen), mais on peut ensuite agrandir à nouveau le modèle obtenu et s'arranger pour que HC devienne vraie ! Le forcing, en quelque sorte, n'a pas d'avis sur HC : il permet successivement de la rendre vraie, puis fausse (ou l'inverse!).

En revanche, pour un énoncé d'arithmétique E (énoncé ne mentionnant que des entiers, par exemple : « Il existe une infinité de nombres premiers jumeaux ») si un modèle se prononce, en démontrant que E y est vrai par exemple, alors toute extension par forcing de ce modèle se prononcera de la même manière : E y restera vrai.

Pour les énoncés d'arithmétique, le forcing ne peut pas faire basculer les modèles (alors qu'il peut faire basculer HC) de vrai à faux ou l'inverse : le domaine des entiers est stable par forcing dans ZFC. C'est là une propriété très satisfaisante de ZFC : cela signifie que ZFC est un système convenable pour les entiers.

4. Petit lexique de logique

Axiome du choix : l'axiome du choix indique que si un ensemble d'ensembles est donné, on peut prélever un élément dans chaque ensemble pour en constituer un nouveau. De $\{\{a, b, c\}, \{1, 2\}, \{A, E, I, O, U\}\}$, on peut tirer $\{b, 1, U\}$.

démonstrables sont nommées les indécidables du système.

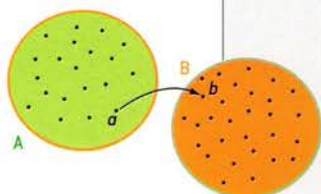
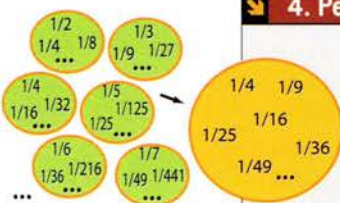
Grands cardinaux : ensembles de tailles gigantesques, plus grands que tous ceux de la série $\mathbb{N}$, $\mathcal{P}(\mathbb{N})$, $\mathcal{P}(\mathcal{P}(\mathbb{N}))$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$... Ces grands cardinaux sont construits sur la base d'axiomes ajoutés à ceux de ZFC.

Bijection ou correspondance bijective : opération qui fait correspondre à chaque élément a de l'ensemble A un élément unique b de l'ensemble B et réciproquement. Les ensembles infinis des nombres entiers et des nombres pairs sont en bijection et ont donc la même taille.

Hypothèse du continu : il n'existe pas d'ensemble infini de taille intermédiaire entre celle de l'ensemble $\mathbb{N}$ des nombres entiers et celle de l'ensemble $\mathbb{R}$ des nombres réels.

Complétude : un système est complet si pour toute formule A on peut démontrer A ou non-A. Gödel a établi que tout système assez puissant pour y faire de l'arithmétique et non contradictoire est incomplet. Les formules A telles que ni A ni non-A ne sont

Modèle : un modèle d'un ensemble d'axiomes est une structure qui vérifie chaque axiome. Un modèle des axiomes des groupes est simplement un groupe (comme le groupe des rotations dans l'espace).



INDÉCIDABLE



À part certains énoncés assez artificiels directement tirés de la logique, on n'a jamais proposé d'énoncés arithmétiques pour lesquels on puisse prouver que ZFC est insuffisant. La stabilisation des entiers par ZFC n'est pas la complétude logique qui serait « Pour toute formule E , E est démontrable ou non- E est démontrable ». Les résultats d'incomplétude de Gödel interdisent définitivement une telle complétude parfaite. On peut cependant voir la stabilisation des entiers comme une « complétude faible ». Il faut se réjouir de cette propriété de ZFC et essayer de la prolonger.

Un axiome qui, ajouté à ZFC, stabiliserait de la même façon non plus seulement les entiers, mais une partie plus grande de l'univers des ensembles, serait un axiome satisfaisant, car il approcherait un peu plus de la complétude qui, même si elle est inaccessible dans sa totalité, est bien évidemment attendue (même sous ses formes faibles) de tout bon système axiomatique.

Dispose-t-on de candidats ?

Grâce à cette idée, on dispose d'une méthode nouvelle et fondée de manière intelligible, pour séparer les axiomes qu'il est raisonnable d'ajouter de ceux qu'il faut écarter : on leur demandera de prolonger la stabilisation que ZFC opère sur les entiers, c'est-à-dire de stabiliser une partie plus grande de l'univers ensembliste.

Pour résumer, ajouter de nouveaux axiomes à ZFC (en particulier, afin de savoir si HC est vraie ou pas) ne doit pas se faire arbitrairement, ce serait admettre que l'infini est une fiction, mais doit se faire sur la base de critères naturels dont les trois principaux sont les suivants :

- Les axiomes ne doivent pas introduire de contradiction.
- Les axiomes doivent être conformes au maximalisme ontologique et doivent donc être compatibles avec les axiomes de grands cardinaux connus.
- Les axiomes doivent, si possible, stabiliser de nouvelles parties de l'univers des ensembles, c'est-à-dire constituer un progrès vers l'inaccessible, mais approchable, complétude.

A-t-on découvert de tels axiomes naturels ? La réponse est oui, deux axiomes semblent satisfaire à tous ces critères et sont donc candidats comme nouveaux axiomes de la théorie des ensembles.

Le premier est l'axiome de détermination projective, DP. Cet axiome, qui est l'aboutissement des recherches menées dans les décennies 1970 et 1980, exprime que tous les jeux d'une certaine catégorie de jeux infinis possèdent des stratégies gagnantes permettant à l'un des deux joueurs de gagner à tout coup. Une série de résultats dus en particulier à Jan

Un modèle de ZFC est une structure qui vérifie les axiomes de ZFC.

Parties d'un ensemble : ensemble $\mathcal{P}(A)$ constitué des ensembles dont les éléments sont les combinaisons des éléments de A . L'ensemble $\mathcal{P}(A)$ est toujours plus grand que l'ensemble A de départ. L'ensemble $\mathcal{P}(\mathbb{N})$ des parties de $\mathbb{N}$ est de même taille que l'ensemble $\mathbb{R}$ des réels.

ZFC : axiomes de Zermelo-Fraenkel, permettant toutes les opérations habituelles de la théorie des ensembles, auxquels on a ajouté l'axiome du choix.



Zermelo Fraenkel

Théorie non contradictoire : théorie dont les axiomes sont tels que l'on ne peut démontrer une chose et son contraire. Une théorie est non contradictoire si et seulement si, il existe un modèle qui rend vrai chacun de ses axiomes.

Mycielski, Yiannis Moschovakis et Alexander Kechris montre que DP stabilise la partie de l'univers des ensembles correspondant à $\aleph_1$, ce qui va donc un peu plus loin que la stabilisation par ZFC des entiers (qui constituent la partie de l'univers des ensembles correspondant à $\aleph_0$). De surcroît, l'axiome DP est compatible avec les axiomes des grands cardinaux, car – et ce fut l'un des aboutissements de la recherche de cette période – Donald Martin et John Steel ont établi en 1985 que DP était lui-même, en un sens précis, un axiome de grand cardinal.

Malheureusement, DP ne dit rien concernant HC et laisse donc toujours le choix entre l'ajouter ou ajouter sa négation ! Il faut aller encore plus loin et chercher des axiomes qui stabilisent l'univers des ensembles au-delà de $\aleph_1$.

C'est là que les derniers progrès de la théorie se sont présentés. Un nouvel axiome MMW (*Martin Maximum de Woodin*) a été proposé par H. Woodin qui nous conduit tout près de la solution attendue pour HC. Bien que la situation ne soit pas définitivement réglée, les résultats concernant cet axiome semblent converger de manière résolue vers la conclusion que HC est fausse. Voici pourquoi.

D'une part, cet axiome stabilise la partie de l'univers des ensembles correspondant cette fois à $\aleph_2$ (on a gagné un degré par rapport à DP). Cet axiome est donc un bon axiome au sens des critères adoptés aujourd'hui pour trier les axiomes.

D'autre part, il apparaît très probable que le nouvel axiome est conforme au maximalisme ontologique, car un axiome assez semblable a été démontré compatible avec les axiomes de grands cardinaux.

Troisième point : moyennant une hypothèse jugée raisonnable et dont on espère obtenir la preuve rapidement (cette hypothèse est nommée Ω -conjecture), on sait que HC est fausse quand on adopte MMW.

Dernier point, peut-être le plus important : toujours sous la réserve de l' Ω -conjecture, on sait que tout axiome qui stabiliserait la partie de l'univers correspondant à $\aleph_2$ aurait aussi

5. La Ω -logique



Un des arguments forts en faveur de non-HC est fondé sur une nouvelle logique proposée par Hugh Woodin (*photographie ci-contre*) : la Ω -logique. Cette logique est une généralisation de la logique mathématique usuelle. Elle présente un aspect syntaxique (on définit ce qu'est une démonstration correcte) ainsi qu'un aspect sémantique (on définit ce qu'est un modèle). Le théorème de complétude pour cette logique, c'est-à-dire la démonstration qu'un système est non contradictoire

(point de vue syntaxique) si et seulement si, il possède des modèles (point de vue sémantique), n'a été que partiellement démontré. Pour y arriver, il faudrait établir ce qu'on a appelé la Ω -conjecture. La Ω -logique est la logique des grands cardinaux dans le sens suivant : une formule est démontrable à l'aide d'axiomes de grands cardinaux (d'un certain type très général), si et seulement si, elle est démontrable en Ω -logique.

La Ω -logique permet donc un point de vue global et puissant intégrant directement l'idée que les axiomes de grands cardi-

naux sont valides. Son introduction constitue un progrès équivalent à celui du passage de l'arithmétique à la théorie des ensembles (transition d'une théorie des objets finis à une théorie qui accepte l'infini). Avec la Ω -logique, on passe de l'infini usuel à l'infini des grands cardinaux.

Hugh Woodin a formulé un nouvel axiome naturel MMW, et, sous réserve que la Ω -conjecture soit vraie, il a établi que $ZFC + DP + MMW$ a pour conséquence la fausseté de HC, ainsi que l'affirmation que tout axiome naturel de la même catégorie entraîne aussi la fausseté de HC.

Il apparaît donc que dans un univers où les grands cardinaux sont acceptés pleinement, le choix n'est plus possible entre HC ou non-HC.

La rupture de symétrie constatée en Ω -logique en faveur de non-HC est sans doute la solution à l'énigme de Cantor qui, après 120 ans d'hésitation et de progrès dans la compréhension de l'infini, se résout grâce à la Ω -logique : Cantor et Gödel avaient raison de croire que l'hypothèse du continu n'est pas laissée à notre libre choix, sa fausseté s'impose à nous.

pour conséquence la fausseté de HC. Autrement dit, si tout cela est confirmé, toute méthode de stabilisation des ensembles jusqu'à $\aleph_2$ a pour conséquence que HC est fausse. Patrick Dehornoy propose de dire que HC est « essentiellement fausse ».

Moyennant quelques points en attente, mais dont la résolution ne semble pas inaccessible, le programme de Gödel de recherche de nouveaux axiomes naturels permettant la résolution de HC toucherait donc à son terme en produisant une réponse négative à la question que Cantor découvrait il y a 120 ans : le continu est-il le premier infini juste au-delà de l'infini dénombrable ?

Notons d'ailleurs que des résultats partiels suggèrent fortement qu'entre le dénombrable et le continu, il n'y aurait qu'un seul infini intermédiaire ; autrement dit, on semble s'acheminer vers la formule inattendue : $2^{\aleph_0} = \aleph_2$. Savoir ce qui se passe au-delà apparaît hors de portée, du moins pour le moment : l'infini conserve bien des mystères. Même si la question n'est pas totalement réglée aujourd'hui et si quelques spécialistes disent même qu'une solution opposée à celle de H. Woodin n'est pas exclue, par exemple par la découverte d'un axiome de grand cardinal qui aurait pour conséquence HC, les progrès faits sont considérables. Ils concernent la formulation et la classification des grands cardinaux dont la compréhension constitue une théorie de l'infini dont il est impossible de prétendre qu'elle a été fixée arbitrairement par les mathématiciens.

L'infini de mieux en mieux compris

Les progrès portent sur l'axiome DP qu'un accord quasi général considère comme devant être ajouté à ZFC et dont il a été prouvé qu'il nous approchait d'une forme de complétude. L'accord sur DP, dont H. Woodin dit qu'il le considère aussi vrai que les axiomes de l'arithmétique élémentaire, montre que le programme d'ajouter des axiomes naturels aux axiomes de base de la théorie des ensembles n'est pas une utopie : l'infini est approchable, il se dévoile progressivement lorsque nous prenons la peine de l'examiner, nous en découvrons la réalité.

Ceux qui craignent de formuler une conclusion philosophique trop abrupte s'exprimeront plus prudemment et comme P. Dehornoy diront seulement : « Il semble difficile de nier que la compréhension développée par H. Woodin et les théories qu'il élabore portent sur quelque chose, quand bien même cette chose ne serait pas l'infini non dénombrable en termes duquel les résultats sont aujourd'hui énoncés. »

Les derniers progrès concernent des constructions conceptuelles dont la somme dessine un paysage de plus en plus net et cohérent des ensembles jusqu'au niveau de $\aleph_2$, laissant entrevoir que l'axiome MMW sera bientôt ajouté à ZFC + DP et qu'il permettra de dire que HC est fausse. H. Woodin à qui l'on doit une partie importante des dernières avancées ne veut pas conclure trop vite, mais il est clair : « Il y a 10 ans, je pensais qu'il y avait une chance que l'hypothèse du continu possède une solution. Maintenant, je pense vraiment qu'elle possède une solution. »

Ces progrès de la logique mathématique ont une portée philosophique évidente, car si l'infini n'est pas ce que nous décidons, et que ses formes s'imposent à notre esprit, cela signifie sans nul doute quelque chose d'incroyablement profond sur le monde et la façon dont nous en prenons connaissance.

L'ensemble de tous les ensembles

L'ensemble de tous les ensembles est généralement considéré comme un concept contradictoire. Il s'agit là d'une erreur.

En histoire des sciences, on a souvent du mal à comprendre comment les solutions aujourd'hui adoptées ont été si difficiles à trouver et à mettre au point, tant les consensus élaborés par nos illustres prédécesseurs nous semblent parfois faciles. C'est le cas pour la théorie des ensembles, dont on n'imagine plus se passer et dont la naissance fut pourtant un douloureux moment de l'histoire des mathématiques. Au début du XX^e siècle, on pensa à y renoncer à cause des paradoxes qu'on y avait décelés. Lorsqu'une solution fut trouvée, celle qu'on nomme aujourd'hui ZFC, l'axiomatique de Zermelo-Fraenkel avec axiome du choix, la communauté mathématique fut rassurée ; depuis bientôt un siècle, la théorie ZFC, qui sert de support à pratiquement tout ce qui se fait en mathématiques, est universellement perçue comme simple et naturelle.

Pour éviter les paradoxes, ZFC impose quelques contraintes qui sont devenues des vérités mathématiques absolues : il n'y a pas d'ensemble de tous les ensembles, un ensemble ne peut pas être élément de lui-même, il n'y a pas d'ensemble de tous les ordinaux, ni d'ensemble de tous les cardinaux, etc. Or ces affirmations catégoriques sont inutiles et trompeuses ! En effet, des théories alternatives des ensembles nous autorisent à traiter, sans rencontrer de paradoxe, de l'ensemble de tous les ensembles, d'ensembles qui sont éléments d'eux-mêmes, etc. Méfions-nous des vérités définitives que l'habitude et la paresse nous font adopter et qui ne sont que des conventions liées au choix d'une solution particulière favorisée par l'histoire.

Les paradoxes ensemblistes...

Alors que la théorie des ensembles entrevue par le mathématicien Bernard Bolzano au début du XIX^e siècle et développée par Georg Cantor à partir de 1873 commençait à s'imposer comme la théorie de base des mathématiques, le logicien et philosophe anglais Bertrand Russell publia en 1903 ce que l'on dénomme aujourd'hui l'antinomie de Russell (*voir l'encadré 1*) et qui est une contradiction en plein cœur de la théorie de Cantor. Le raisonnement est le même que celui fait à propos du barbier qui ne rase que tous les habitants de sa ville qui ne se rasent pas eux-mêmes. S'il se rase lui-même, alors c'est qu'il ne se rase pas ; s'il ne se rase pas lui-même, alors il possède la propriété qui fait qu'il doit se raser, et donc il se rase lui-même.

Le choc produit par l'antinomie de Russell fut très grave. Il ébranla par exemple l'Allemand Richard Dedekind qui cessa un moment de publier ses travaux sur la théorie des nombres. Le philosophe allemand Gottlob Frege prit connaissance de l'antinomie de Russell en mettant la dernière main à son ouvrage sur les fondements de l'arithmétique. Il y ajouta une note exprimant son désarroi : « Un scientifique peut difficilement être confronté à une situation plus désagréable que celle de voir les bases de son travail disparaître au moment précis où il s'achève. J'ai été mis dans cette situation par une lettre de Bertrand Russell alors que le livre était pratiquement sous presse. »

Plusieurs mathématiciens considérèrent qu'il fallait abandonner la théorie des ensembles. En fait, la raison de l'inquiétude ne venait pas seulement du paradoxe de Russell, mais d'une série d'autres. Le premier paradoxe découvert en théorie des ensembles est en réalité celui de Cesare Burali-Forti paru en 1897. Il envisage l'ensemble de tous les ordinaux (un ordinal est un ensemble ordonné tel que toute partie possède un plus petit élément). Cet ensemble, s'il existe, définit un nouvel ordinal dont on montre qu'il est strictement plus grand que tous les ordinaux utilisés pour le définir, ce qui est absurde. L'ensemble de tous les cardinaux (nombres qui servent à mesurer la taille, finie ou infinie, des ensembles) est sujet à la même difficulté.

... Et leur résolution

Ces paradoxes techniques gênent le mathématicien, mais le paradoxe le plus grave est sans doute le paradoxe de l'ensemble de tous les ensembles que Cantor connaissait sans doute dès 1899. Il se déduit d'un théorème général démontré par Cantor qui indique que l'ensemble $\mathcal{P}(E)$ des parties d'un ensemble E est toujours plus gros que l'ensemble E lui-même. Il existe ainsi un ensemble de « puissance » supérieure à celle de tout ensemble E donné : c'est l'ensemble des sous-ensembles de E . Appliqué à l'ensemble de tous les ensembles, le théorème de Cantor conduit à l'idée que celui-ci, puisqu'il contient toutes ses parties, est strictement plus gros que lui-même, ce qui est aussi absurde que $1 > 1$.

Retomber sur ses pieds, c'est-à-dire éliminer les paradoxes, nécessite de les analyser et de modifier la façon dont nous raisonnons, de façon à ce qu'ils ne puissent plus survenir.

La résolution des paradoxes ensemblistes donna lieu à de nombreux travaux, dont ceux de Russell lui-même, qui constituent ce qu'on nomme la théorie des types et sur laquelle nous reviendrons.

La solution qui est adoptée aujourd'hui par les mathématiciens, ZFC, provient d'une axiomatisation de la théorie des ensembles proposée par Ernst Zermelo en 1908 et complétée dans les années 1920 par Abraham Fraenkel et John von Neumann. L'idée de cette solution est que seuls certains regroupements d'objets doivent être acceptés comme ensembles, mais pas tous. Il ne suffit pas de disposer d'une



Georg Cantor

propriété, par exemple « l'ensemble x n'est pas élément de lui-même » pour avoir le droit de parler de l'ensemble des objets vérifiant la propriété, il faut être plus restrictif.

La théorie classique des ensembles : ZFC

La théorie ZFC soutient donc que certains regroupements définis par une propriété sont trop gros, et que seuls les regroupements soigneusement et progressivement construits, comme nous l'expliquons plus loin, sont des ensembles. La méthode se dénomme théorie de la limitation de taille.

Examinons les axiomes de ZFC pour voir comment s'effectue l'élimination des paradoxes. Le premier axiome indique, conformément au bon sens, que deux ensembles sont identiques si et seulement s'ils ont les mêmes éléments : un ensemble est caractérisé par ses éléments, les connaître c'est le connaître. Les axiomes qui suivent donnent des moyens de construire de nouveaux ensembles à partir d'ensembles déjà connus. Ces axiomes sont les règles « légales » de définition et de manipulation de ces êtres mathématiques que sont les ensembles.

L'axiome de la réunion indique que si E est un ensemble, le regroupement des éléments d'ensembles appartenant à E , c'est-à-dire des x appartenant à des y appartenant à E , constitue encore un ensemble. De $E = \{\{a, b\}, \{\pi, 1/e\}, \{1, 2, 3\}\}$, on déduit l'existence de l'ensemble $\{a, b, \pi, 1/e, 1, 2, 3\}$. Ainsi, l'ensemble des nombres de Fibonacci (1, 1, 2, 3, 5, 8, 13, 21,...) et l'ensemble des nombres triangulaires (1, 3, 6, 10, 15,...) forment un nouvel ensemble. Vous pouvez « parler » de l'ensemble des éléments présents dans l'un au moins des deux ensembles.

L'axiome de l'ensemble des parties affirme que le regroupement des sous-ensembles d'un ensemble E constitue lui aussi un ensemble. De $E = \{0, 1, 2\}$, on déduit l'existence de $\mathcal{P}(E) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$. Notons « pour le plaisir » que si l'ensemble E a k éléments, il y a C_k^1 éléments individuels, C_k^2 paires d'éléments, etc., et la formule du binôme donne $(1 + 1)^k = 1 + C_k^1 + C_k^2 + \dots + 1 = 2^k$. L'ensemble des parties de E a ainsi 2^k éléments.

L'axiome de séparation ou axiome de compréhension restreint indique que si $P(x)$ est une propriété (telle $x > 3$) et que E est un ensemble, alors les x qui sont dans E et qui vérifient cette propriété restrictive $P(x)$ constituent aussi un ensemble. Il est essentiel de noter que cet axiome permet de définir un ensemble à partir d'une propriété, ce qui est bien sûr souhaitable, mais qu'il impose la restriction de ne prendre que des x présents dans un ensemble déjà connu E .

- Cette définition permet d'envisager l'ensemble des nombres premiers. Pour cela, on part de l'ensemble des entiers (construit préalablement) et de la propriété $P(x)$: « x n'a pas de diviseurs autres que 1 et lui-même. »

- La propriété $x = x$, seule, ne définit pas un ensemble. Si c'était le cas, la formule définirait l'ensemble de tous les ensembles, ce qui contredirait le théorème de Cantor de ZFC.

- « Posséder deux éléments exactement » ne définit pas un ensemble dans ZFC.

L'axiome de compréhension dans sa forme restreinte (mentionnant un ensemble E) est la clef de la résolution des paradoxes : elle empêche la définition d'ensembles trop gros. On ne peut pas parler de l'ensemble de tous les ensembles ni de l'ensemble des x

1. Les ensembles qui ne sont pas éléments d'eux-mêmes

L'antinomie de Bertrand Russell (*photographie ci-contre*) fut un tel choc qu'elle conduisit certains logiciens et mathématiciens, tel Dedekind, à abandonner temporairement la théorie des ensembles. Russell distingue deux types d'ensembles, les ensembles qui sont un élément d'eux-mêmes (comme l'ensemble des idées, qui est une idée) et les ensembles qui ne sont pas éléments d'eux-mêmes (comme l'ensemble des éléphants, qui n'est pas un éléphant).

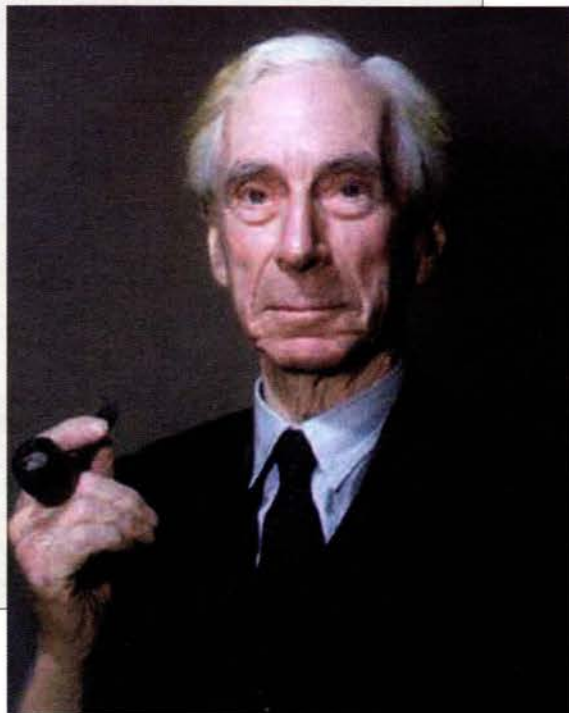
Le paradoxe consiste à raisonner de la manière suivante. Considérons l'ensemble E des ensembles qui ne sont pas élément d'eux-mêmes. Deux cas sont à envisager : E est élément de lui-même ou ne l'est pas.

– Si E n'est pas élément de lui-même, alors il possède la propriété caractéristique des éléments de E et il est donc dans E . Mais alors, E est élément de lui-même. C'est une contradiction !

– Si E est élément de lui-même, alors il n'a pas la propriété caractéristique des éléments de E (ne pas être élément d'eux-mêmes), ce qui implique que E ne peut pas être élément de lui-même. C'est, à nouveau, une contradiction.

Le catalogue de tous les catalogues qui ne se mentionnent pas eux-mêmes conduit pareille-

ment à une contradiction. S'il se mentionne lui-même, il n'est pas dans ce catalogue, mais s'il n'est pas dans le catalogue, alors c'est un catalogue qui ne se mentionne pas lui-même et il devrait y être.



qui possèdent la propriété de ne pas être éléments d'eux-mêmes. Les paradoxes de Russell et Cantor sont donc évités, de même d'ailleurs que le paradoxe de l'ensemble des ordinaux et celui de l'ensemble des cardinaux.

L'axiome de remplacement indique que si, étant donnée une fonction R telle que pour tout élément x d'un ensemble E , la fonction R détermine un élément y , alors les éléments y constituent un nouvel ensemble, F . En clair, l'image d'un ensemble E par une fonction R est un ensemble. Contrairement à l'axiome de séparation, l'axiome de remplacement peut engendrer (d'une manière contrôlée) des ensembles F qui ne sont pas inclus dans E .

L'axiome de l'infini indique qu'il existe au moins un ensemble infini E . Il existe plusieurs façons de définir un ensemble infini. L'une d'elles, due à Dedekind, consiste à dire que E est infini si E possède un sous-ensemble F différent de E , et que l'on peut mettre en bijection avec E . Selon cette définition, l'ensemble des entiers est infini, car l'ensemble des entiers peut être mis en bijection avec l'ensemble des entiers pairs en doublant chaque entier (fonction $n \rightarrow 2n$).

L'axiome de fondation (AF), proposé par von Neumann en 1925, est explicité sur la figure 3 : il n'existe pas de chaînes infinies de boîtes-ensembles les unes dans les autres et pas de boîtes-ensembles qui se contiennent elles-mêmes !

L'axiome du choix (le « C » de ZFC) indique que si E est un ensemble d'ensembles non vides, alors il existe un ensemble F qui a un élément commun exactement avec chaque ensemble de E . De $\{\{0, 1, 2\}, \{\pi, 1/e\}, \{A, B\}\}$, on déduit l'existence d'un ensemble F comme $\{2, 1/e, B\}$. L'axiome du choix crée certaines difficultés et c'est pour cela qu'on le fait apparaître dans le nom ZFC de la théorie.

Il est remarquable que ces simples axiomes, tous assez naturels, permettent l'expression de pratiquement toutes les idées et démonstrations mathématiques et que depuis plus d'un siècle qu'on explore les conséquences de ZFC, jamais aucune contradiction n'y a été découverte. Cependant, la méthode adoptée par ZFC opère une distinction entre ensembles et regroupements (définis seulement par une propriété). Cette distinction interdit de considérer que certains regroupements simples et naturels sont d'authen-

2. Les axiomes de fondation et d'antifondation

L'axiome de fondation de ZFC indique que partant d'un ensemble (une boîte), si l'on prend l'un de ses éléments (une boîte-ensemble dans la boîte) et qu'on prend un élément dedans, et qu'on prend encore un élément dedans, etc., alors nécessairement on est obligé de s'arrêter : il n'existe pas de chaînes infinies descendantes $x_0, x_1, x_2, x_3, x_4, \dots$ avec $x_1 \in x_0, x_2 \in x_1, x_3 \in x_2, x_4 \in x_3, \dots$

Cet axiome correspond à l'idée que lorsqu'on passe des êtres vivants aux cellules, des cellules aux molécules, des molécules aux atomes, des atomes aux quarks etc., on finit nécessaire-

ment par arriver à un ultime niveau qui n'est plus décomposable. L'axiome interdit aussi qu'un ensemble puisse se retrouver à l'intérieur de lui-même : $x \in x$ et interdit donc l'ensemble de tous les ensembles qui aurait cette propriété.

Le monde de la théorie classique des ensembles ZFC de Zermelo-Fraenkel correspond donc à une vue hiérarchisée du monde qui est facile à appréhender. C'est ce côté hiérarchisé et rassurant que la théorie des hyperensembles propose d'abandonner.

L'axiome d'antifondation qui définit la théorie des hyperensembles exprime que tout système d'équations, fini ou infini, de la forme : $x = \{1, \{7, 8\}, y, z\}; y = \{2, x, z\}; z = \{5\}$ (à gauche des variables représentant des ensembles, à droite des expressions utilisant les mêmes variables-ensembles) possède une solution unique : un hyperensemble.

L'équation $x = \{x\}$ définit l'hyperensemble le plus simple. Il est noté Ω et contient un élément : lui-même. C'est une sorte de bouteille de Klein. L'hyperensemble infiniment profond $\{1, \{2, \{3, \{...\}\}\}\}$ est le x_1 de la solution du système d'équations : $x_1 = \{1, x_2\}, x_2 = \{2, x_3\}, x_3 = \{3, x_4\}$, etc.

Cette possibilité de construire des ensembles infiniment profonds est un outil puissant de modélisation des structures autoréférentes souvent rencontrées en informatique où des objets dépendent mutuellement et cycliquement les uns des autres (jeux de pointeurs, flux de données, machines reliées en réseaux, etc.). Jon Barwise et John Etchemendy, dans leur livre intitulé *The Liar* («Le menteur»), traitent les phrases autoréférentes et, par exemple, la phrase «je mens» est associée à l'hyperensemble $m = \{\text{faux}, \{m\}\}$ (une valeur de vérité, suivie d'un contexte simple composée dans ce cas de la phrase elle-même).



tiques ensembles... ce qui est étrange. En un mot, la solution exprimée dans ZFC apparaît comme une rustine : elle répare la théorie initiale de Cantor, mais elle lui enlève sa beauté et sa généralité. Elle en limite la puissance en interdisant en particulier de mentionner un ensemble universel contenant la totalité des ensembles ou de définir le nombre n comme le regroupement de tous les ensembles possédant n éléments, selon l'élégante idée de Cantor et de Frege.

Les révisions possibles

Une extension de ZFC donne un statut théorique aux regroupements problématiques (ensemble de tous les ensembles, ensembles des ordinaux, etc). Elle consiste à introduire, à côté de la notion d'ensemble, la notion de *classes* en définissant certaines opérations entre classes, dont en particulier la définition d'une classe à partir d'une propriété. La classe de tous les x qui vérifient $x = x$ correspond à l'ensemble de tous les ensembles. Cette théorie de von Neumann, Bernays et Gödel, notée NBG, est une première méthode pour disposer du droit de mentionner les gros ensembles problématiques interdits dans ZFC. Cependant, cette façon d'étendre ZFC n'est pas jugée satisfaisante, car elle se fonde sur une distinction artificielle et injustifiée entre deux catégories de regroupements, les ensembles et les classes, un peu comme dans une société qui considérerait deux types de citoyens : ceux qui jouissent pleinement de tous les droits (les ensembles), et ceux qui n'en ont qu'une partie sans qu'on sache trop bien pourquoi.

Une méthode plus élégante pour augmenter le pouvoir de ZFC consiste à revoir l'axiome de fondation qui est le dernier historiquement ajouté à ZFC et que d'ailleurs Cantor n'avait pas envisagé du tout.

En interdisant directement l'ensemble de tous les ensembles, l'axiome de fondation est rassurant. Cependant, on s'était déjà débarrassé des paradoxes avant de l'introduire. L'utilisation de l'axiome de fondation ressemble un peu à la méthode consistant à pendre un noyé pour être certain qu'il est bien mort ! Notons aussi que même si AF à lui seul évite le paradoxe de l'ensemble de tous les ensembles, il est inopérant contre d'autres paradoxes et ne constitue donc pas une alternative complète à la doctrine de la limitation de la taille que met en œuvre ZFC.

Le Britannique Peter Aczel, et indépendamment les Italiens Marco Forti et Furio Honsell, ont proposé dans les années 1980 de renoncer à AF et de le remplacer. Acceptons l'idée qu'il y a des ensembles qui appartiennent à eux-mêmes, comme on accepte l'idée qu'il y a des nombres dont le carré est -1 , et imposons par un axiome particulier qu'il y en existe de toutes les sortes imaginables.

L'axiome d'antifondation, noté AFA (voir l'encadré 2), indique non seulement qu'il y a toutes sortes d'ensembles appartenant à eux-mêmes, mais que précisés par une loi adéquate, ils sont uniques. Cette double affirmation d'existence et d'unicité confère à l'axiome AFA toute sa force et en fait l'intérêt. L'axiome AFA crée une révolution comparable à l'introduction des nombres complexes. En plus de tous les « ensembles habituels » qui bien sûr restent des ensembles dans cette théorie, il y a maintenant une multitude d'autres ensembles « antifondés » qu'on dénomme *hyperensembles*.

Les hyperensembles

En particulier, dans la théorie des hyperensembles $ZFC - AF + AFA$ (tous les axiomes de ZFC , moins l'axiome de fondation, plus l'axiome AFA), il y a un hyperensemble unique noté Ω qui vérifie $x = \{x\}$. L'hyperensemble Ω est un être étrange possédant un seul élément, lui-même. D'après AFA , il est le seul à posséder cette propriété. Il représente une sorte de monde autiste, refermé en boucle sur lui-même !

Il y a aussi un hyperensemble unique qui vérifie $x = \{x, \emptyset\}$. C'est un objet étrange qui possède deux éléments : l'ensemble vide et lui-même. Il y a aussi l'hyperensemble infiniment profond $\{0, \{1, \{2, \{3, \{\dots\}\}\}\}$ (voir l'encadré 2).

Ajouter un nouvel axiome comme AFA fait prendre des risques : si ZFC ne conduit jamais à une contradiction, en est-il de même de $ZFC - AF + AFA$? La réponse est oui : on ne prend aucun risque avec AFA . En effet, P. Aczel a prouvé un résultat de « consistance relative » analogue à un autre obtenu par von Neumann pour AF : si la théorie usuelle des ensembles, ZFC , ne conduit jamais à une contradiction, alors il en est de même de $ZFC - AF + AFA$. Les hyperensembles n'introduisent aucun danger particulier de contradiction.

L'intérêt d'une théorie se prouve en l'appliquant. C'est aujourd'hui chose faite pour la théorie des hyperensembles. Les domaines dans lesquels elle a été utilisée sont principalement liés à l'informatique et à l'analyse des paradoxes. Plusieurs livres (voir la bibliographie) en donnent le détail. Notons que P. Aczel avait été amené à introduire les hyperensembles alors qu'il étudiait le problème informatique de la représentation formelle des flux de données et la synchronisation entre systèmes communicants fonctionnant de manière ininterrompue comme le sont les ordinateurs connectés en réseaux. Un autre domaine d'application des hyperensembles est celui des bases de données et de la formalisation du langage naturel.

L'ensemble de tous les ensembles ?

La théorie des hyperensembles propose certes une extension de la notion d'ensemble. Mais elle ne donne pas encore la possibilité de parler de l'ensemble de tous les ensembles, car le théorème de Cantor y est toujours valide. C'est sur le problème de traiter de tels « gros regroupements » que des avancées remarquables ont été faites, dont plusieurs ces dernières années.

Au départ, il y a la tentative au début du XX^e siècle par Russell d'éviter les paradoxes par sa fameuse « théorie des types » qui a été abandonnée du fait de sa complication. Dans ce système, on considère les ensembles niveau par niveau, le niveau $n + 1$ étant celui des ensembles dont les éléments sont de niveau n . Chaque ensemble appartient à un niveau donné et il y a une infinité de catégories d'objets différents, ce qui crée de sérieuses contraintes de manipulation. Le système ZFC , qui n'envisage qu'un seul type d'objets, a donc été préféré.

Les paradoxes sont évités par Russell, car les seules formules autorisées dans sa théorie pour définir par compréhension de nouveaux ensembles doivent respecter le système de niveaux. Une formule comme « x appartient à x » n'a pas de sens dans la théorie, car dans une formule correcte de la théorie des types, la relation d'appartenance ne peut relier que deux niveaux différents.

3. Les progrès en théorie des ensembles

	ENSEMBLE DE TOUS LES ENSEMBLES	ANTINOMIE DE RUSSELL
THÉORIE CLASSIQUE DES ENSEMBLES ZFC AVEC L'AXIOME DE FONDATION	Le paradoxe est éliminé par l'axiome de compréhension. On ne prend des éléments d'ensembles que dans des ensembles connus. <i>Inconvénient : ce regroupement naturel est éliminé.</i>	Le paradoxe est éliminé par l'axiome de fondation (pas d'emboîtement à l'infini) et il n'y a pas d'ensembles qui se contiennent eux-mêmes. <i>Inconvénient : les ensembles autoréférents seraient utiles.</i>
THÉORIE CLASSIQUE DES ENSEMBLES ZFC AVEC L'AXIOME D'ANTIFONDATION	Le paradoxe est éliminé par l'axiome de compréhension. On ne prend des éléments d'ensembles que dans des ensembles connus. <i>Inconvénient : il n'y a toujours pas de gros regroupements.</i>	L'axiome d'antifondation autorise les emboîtements à l'infini : les ensembles qui se contiennent eux-mêmes existent et sont caractérisés par des équations.
THÉORIE DES TYPES DE RUSSELL	Les deux paradoxes sont éliminés. On considère les ensembles niveau par niveau, le niveau $n+1$ étant celui des ensembles dont les éléments sont de niveau n . Il existe un ensemble de tous les ensembles par niveau, mais pas d'ensemble vraiment universel, car les niveaux ne se mélangent pas. <i>Inconvénient : il y a une infinité de niveaux et la pratique est difficile.</i>	
THÉORIE NFU (NEW FOUNDATION ET URÉLÉMENTS)	Les deux paradoxes sont éliminés. À chaque fois qu'apparaît le symbole d'appartenance $\in$ dans une formule définissant un ensemble, le niveau de la variable à droite doit être $n+1$ si celui de la variable de gauche est n . Dérivée de la théorie de Russell, cette théorie est d'utilisation plus simple, car les niveaux portent sur les variables et non sur les ensembles.	

Reprise par le logicien et philosophe américain Willard Quine en 1937, la théorie des types de Russell est devenue un nouveau système d'axiomes bien plus simple dénommé *New Foundation* (NF). Malheureusement, Ernst Specker démontra en 1953 que NF contredit l'axiome du choix, ce qui rend NF malcommode pour les mathématiciens attachés à l'axiome du choix et qui, même s'ils s'en méfient, veulent pouvoir l'utiliser librement. Cela conduisit alors Ronald Jensen à proposer une nouvelle version de la théorie de Quine, nommée cette fois NFU (car on y introduit des objets dénommés «uréléments»), compatible avec l'axiome du choix. Depuis, cette théorie dont on peut dire qu'elle possède autant de bonnes propriétés que ZFC, tout en permettant de parler et de manipuler l'ensemble de tous les ensembles et d'autres «gros ensembles», est défendue comme un substitut possible à ZFC.

Un livre de Randall Holmes présente NFU d'une manière élémentaire et prouve ainsi que tout ce qui est fait avec ZFC peut l'être aussi commodément avec NFU. Si NFU n'est aujourd'hui pas utilisée, et même est souvent totalement ignorée, c'est sans doute principalement parce qu'elle est apparue tardivement. Voyons comment NFU évite les paradoxes.

Alors que ZFC (avec l'axiome AF ou dans sa version AFA) attaque les paradoxes en limitant la définition des ensembles à partir des formules par la contrainte de l'axiome

de séparation, NF et NFU évitent les paradoxes sans cet artifice en exigeant en revanche que les formules qu'on utilise pour définir les ensembles soient « stratifiées ».

« Stratifié » signifie qu'il faut qu'on puisse attribuer des niveaux à chaque variable des formules utilisées pour définir les ensembles, d'une manière telle qu'à chaque fois qu'apparaît le symbole d'appartenance, $\in$, le niveau de la variable à droite soit $n + 1$ si celui de la variable de gauche est n . Contrairement à la théorie des types qui obligeait à attribuer des niveaux aux ensembles eux-mêmes (multipliant ainsi des différentes sortes d'objets), ici l'attribution d'un niveau doit seulement se faire sur les variables des formules qu'on veut utiliser pour définir des ensembles. On est passé d'une contrainte globale d'attribution des niveaux à chaque élément de l'Univers, à une contrainte temporaire et syntaxique s'appliquant juste aux formules utilisées pour définir des ensembles et qu'on peut oublier une fois l'ensemble défini. En pratique, la vérification que les formules qu'on utilise sont stratifiées est assez facile et moins contraignante que l'axiome de séparation de ZFC.

Donnons des exemples. La formule $x = x$ ne pose pas de problème. Comme elle n'utilise pas le symbole d'appartenance, elle est considérée stratifiée et, en conséquence, il existe un ensemble U des ensembles vérifiant $x = x$. Cet ensemble U est bien sûr l'ensemble de tous les ensembles qui a donc une existence pleine au sein de la théorie de Quine ou de la théorie de Jensen.

Comment éviter certains paradoxes

La formule $x \in x$ n'est bien sûr pas stratifiée, de même que la formule $x \notin x$ qui conduirait au paradoxe de Russell. Ces deux formules ne définissent pas d'ensembles et on évite donc le paradoxe de Russell. Si E est un ensemble, la formule $x \notin E$ est stratifiée, ce qui signifie que dans NF ou NFU, le complémentaire d'un ensemble (vis-à-vis de tout) existe, alors que dans ZFC le complémentaire d'un ensemble n'existe que relativement à un autre ensemble.

Le paradoxe de Cantor créé par le théorème de Cantor est évité, car dans NF et NFU le théorème de Cantor n'est plus vrai (sa démonstration s'appuie sur une formule non stratifiée). C'est peut-être dommage, mais c'est le coût qu'il faut accepter de payer pour que l'on puisse parler de l'ensemble de tous les ensembles.

Dans NF et NFU, on peut introduire et manipuler sans problème l'ensemble de tous les ordinaux, et l'ensemble de tous les cardinaux. Ces théories sont donc bien une autre façon de slalomer entre les paradoxes sans jamais s'y cogner. Elles montrent que l'ensemble de tous les ensembles et bien d'autres gros ensembles interdits dans les théories des ensembles de type ZFC (avec AF ou avec AFA) peuvent recevoir un statut simple, au sein d'une théorie mathématique homogène, et que c'est donc une erreur de croire que l'ensemble de tous les ensembles et les autres gros ensembles de ZFC sont des concepts paradoxaux.

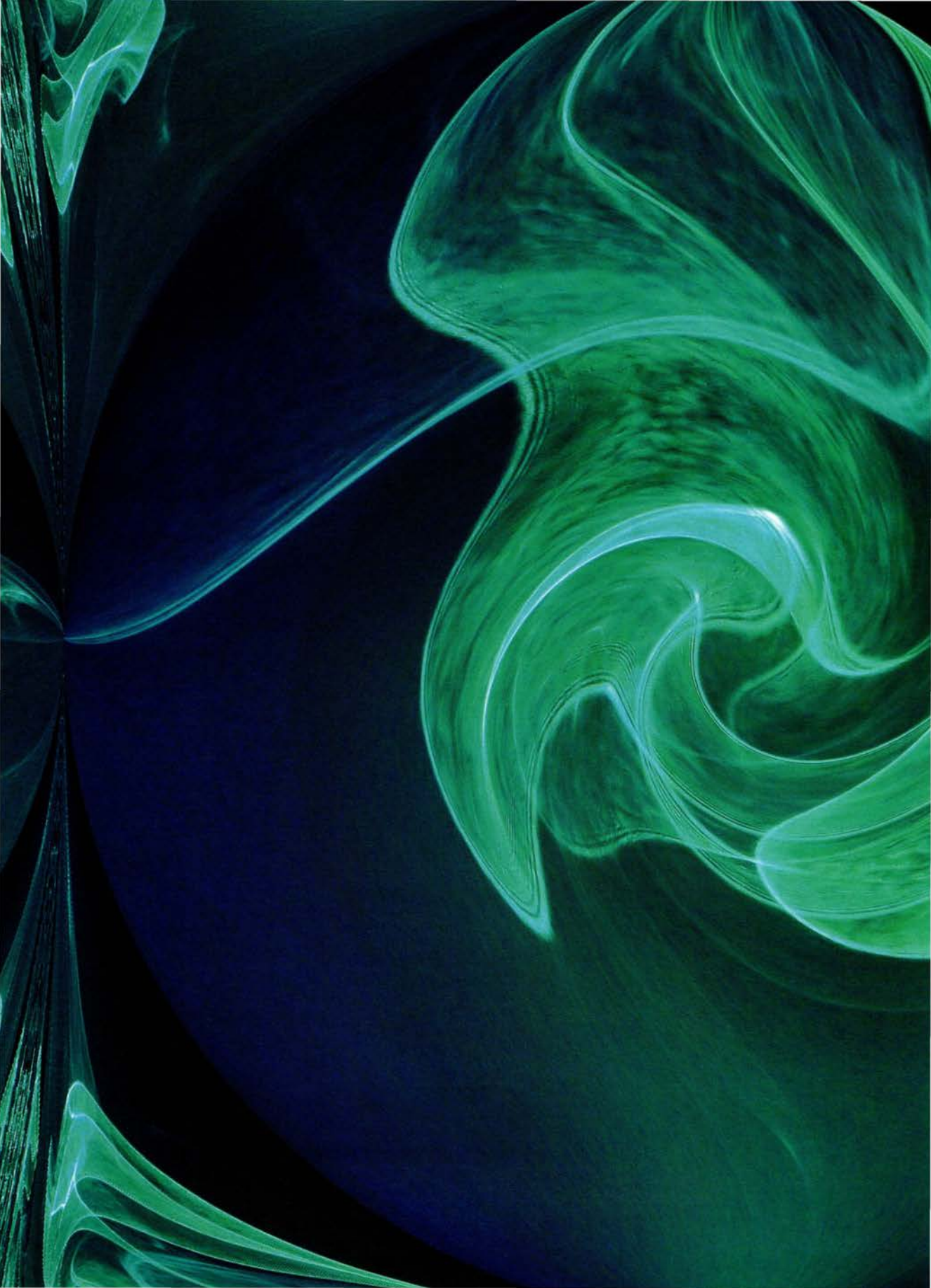
Citons R. Holmes, défenseur de NFU y compris pour l'initiation et l'enseignement : « La raison pour laquelle nous croyons que NFU est un bon moyen pour l'apprentissage de la théorie des ensembles est qu'elle autorise presque toutes les constructions naturelles de la théorie naïve des ensembles, qui est celle de Frege et cela sans limitations artificielles. [...] Les nombres cardinaux finis ou infinis peuvent être définis en suivant les idées de Cantor et Frege. De même, pour les ordinaux. [...] Les grosses classes inté-

ressantes sont vraiment des ensembles : c'est le cas de l'ensemble de tous les groupes, de l'ensemble de tous les espaces topologiques [...].»

L'ordre d'arrivée sur le terrain

Venues trop tard sans doute pour s'imposer maintenant devant ZFC, les théories alternatives des ensembles, que ce soient NBG, $ZFC - AF + AFA$ ou NFU, présentent toutes des avantages sur ZFC dont elles étendent le pouvoir de représentation. Ces théories, et d'autres encore que nous n'avons pas mentionnées ici, mettent à la disposition des mathématiciens des univers plus riches et plus étendus (à chaque fois en un sens précis). Elles constituent peut-être de meilleures bases pour fonder les mathématiques et penser l'Univers, y compris celui de la physique. La relative indifférence dont elles sont victimes illustre les aléas de l'histoire des sciences où, comme dans les compétitions militaires et commerciales, l'ordre d'arrivée sur le terrain joue un rôle déterminant, condamnant parfois les meilleurs à jouer les seconds rôles, voire à la mort.

Il serait cependant souhaitable que le plus grand nombre possible de mathématiciens, de scientifiques et de philosophes ait conscience de cette sorte d'injustice et ne pense pas faussement que l'autoréférence ensembliste (x appartient à x) est contradictoire, ni que parler de l'ensemble de tous les ensembles et des autres « grosses classes » (ce qu'on a toujours eu envie de faire) conduit inévitablement au désastre de l'inconsistance. Ce n'est pas vrai.



L'incomplétude et les limites logiques

Tout système logique rigoureux est insatisfaisant parce que contradictoire ou incapable de dire tout ce qu'on voudrait qu'il dise. Voilà la découverte principale de Kurt Gödel. Cette *incomplétude* n'est pas bénigne comme certains ont voulu le croire : elle est gravissime et concerne une multitude de domaines. Elle change notre vision des mathématiques et de la science dans sa totalité. La logique en passant par les mathématiques obtient là ses plus extraordinaires succès... philosophiques.

L'incomplétude, le hasard et la physique

Le logicien Leonid Levin vient de démontrer un résultat qui renforce le théorème d'incomplétude de Gödel ; il en tire la conclusion qu'aucun procédé physique ne peut contourner la fameuse incomplétude.

Plus de 75 ans après sa découverte en 1930, le théorème d'incomplétude de Kurt Gödel (toute théorie formelle non contradictoire des mathématiques contient des propositions indécidables, c'est-à-dire dont on ne pourra démontrer ni qu'elles sont justes ni qu'elles sont fausses) suscite encore des interrogations et fait l'objet de compléments. De remarquables résultats viennent d'être obtenus par Leonid Levin, chercheur d'origine ukrainienne maintenant professeur à l'Université de Boston (ce logicien est célèbre pour avoir formulé en 1971, en même temps que Stephen Cook, la plus célèbre conjecture de l'informatique théorique, $P \neq NP$). Les théorèmes de L. Levin renforcent la portée du résultat de Gödel et suggèrent que certaines informations propres au monde mathématique ne peuvent être extraites du monde physique.

La généralisation qui a été démontrée s'appuie sur la théorie algorithmique de l'information d'Andreï Kolmogorov (dont L. Levin fut un élève) ; elle confirme que les pistes envisagées pour s'affranchir du théorème d'incomplétude à l'aide de mécanismes physiques produisant un véritable « hasard » (la mécanique quantique suggère qu'il en existe) n'aboutiront jamais.

Cette nouvelle version conduit L. Levin à une conjecture étonnante sur les rapports entre le monde physique et le monde mathématique : une loi de conservation de l'information s'ajouterait aux lois de conservation déjà postulées en physique. Grâce à L. Levin, plus personne ne peut nier que l'incomplétude logique nous apprend quelque chose d'important sur la nature des mathématiques et qu'elle fait partie des lois fondamentales de l'univers. Sa portée concernerait non seulement le monde abstrait du calcul et des mathématiques, mais aussi celui de la physique dans sa totalité.

Pour examiner l'apport récent et inattendu de L. Levin, revenons au fameux théorème que Gödel proposa à la communauté mathématique éberluée.

Souvenons-nous que les mathématiques reposent sur des systèmes d'axiomes dont les combinaisons, associées à des règles de déduction, donnent tous les théorèmes. Pour faciliter notre exposé, nous nous référons principalement au système formel (*voir une définition page 48*) de l'arithmétique de Peano, noté $\mathcal{PA}$, mais tout ce que nous envisagerons s'applique aussi au système formel de la théorie des ensembles et à tout système formel qui permet de démontrer des résultats mathématiques intéressants.

Le système d'axiomes $\mathcal{PA}$ de Peano est un ensemble de conventions permettant d'écrire des formules et des démonstrations mathématiques concernant les nombres entiers. En utilisant ce système, nous pouvons écrire et démontrer une formule qui signi-

fié que « $30 = 2 \times 3 \times 5$ » ou que «40 est la somme de deux carrés» (36 et 4). Nous pouvons aussi écrire et démontrer des formules signifiant «Le carré d'un multiple de 3 est toujours un multiple de 9» ou «Il existe une infinité de nombres premiers». Nous pouvons aussi écrire des énoncés au sujet d'un programme (par exemple écrit en langage C ou JAVA) et affirmer que ce programme calcule successivement toutes les décimales de π . Mieux, nous pouvons écrire et démontrer des énoncés qui traitent de $\mathcal{PA}$ lui-même, par exemple: « $\mathcal{PA}$ démontre que $30 = 2 \times 3 \times 5$.»

Parmi les axiomes de $\mathcal{PA}$, certains concernent les opérations arithmétiques (du type $x + 0 = x$) et autorisent le raisonnement par récurrence: si «0 vérifie la propriété A »

1. Carnap, Gödel et Levin



« Le 26 août 1930, de nombreux membres du cercle de Vienne se rencontrent au Café Reichsrat (b) pour discuter des derniers détails du voyage qu'ils ont prévu à Königsberg. Dans la ville d'Emmanuel Kant doit se tenir le Deuxième congrès sur la théorie de la connaissance des sciences exactes. [...] Lors d'une pause pendant les préparatifs, Gödel(c) s'entretient avec Carnap (a) sur sa découverte de l'incomplétude; trois jours plus tard, ils poursuivent leur conversation dans le même café.

Toutefois, Carnap ne saisit pas tout de suite la portée du résultat de Gödel et présente encore, dans sa conférence du 5 septembre, la démonstration de la non-contradiction comme un critère nécessaire de validité des théories axiomatiques. Le jour même, Gödel expose sa démonstration du théorème d'incomplétude, mais passe inaperçu après les conférences longues et ardues de Hans Reichenbach, Werner Heisenberg et Otto Neugebauer.

Le 7 septembre, lors d'une session de discussion sur les conférences passées, Gödel énonce à nouveau son théorème, en réponse à une intervention de von Neumann: " On peut même (sous réserve de la non-contradiction des mathématiques classiques) donner des exemples de théorèmes qui, bien que sémantiquement exacts, sont indémontrables dans le système formel des mathématiques classiques. " Peine perdue, l'annonce du théorème d'incomplétude est

noyée dans l'activité générale. Dans le compte rendu, le nom de Gödel n'apparaît même pas. » (Extrait de *Gödel*, de G. Guerriero, *Les Génies de la Science*, n° 20.) Le théorème d'incomplétude de Gödel passa dans un premier temps inaperçu: sans doute dérangeait-il trop. Cependant, petit à petit, il fut reconnu comme un résultat central en logique et même en mathématiques. L'étude et le développement de ses conséquences en philosophie des mathématiques, en logique et, bien au-delà, en science, ne semblent pas terminés.

Leonid Levin (d) vient d'en formuler une généralisation qui concerne la physique elle-même: l'impossibilité de disposer d'un système complet d'axiomes pour l'arithmétique, ou les mathématiques classiques, persiste même lorsque l'on accepte, pour construire de nouveaux axiomes, d'utiliser des algorithmes probabilistes ou des processus qui ne créent pas d'information sur le problème de l'arrêt, ce qui est vraisemblablement le cas de la totalité des processus naturels.

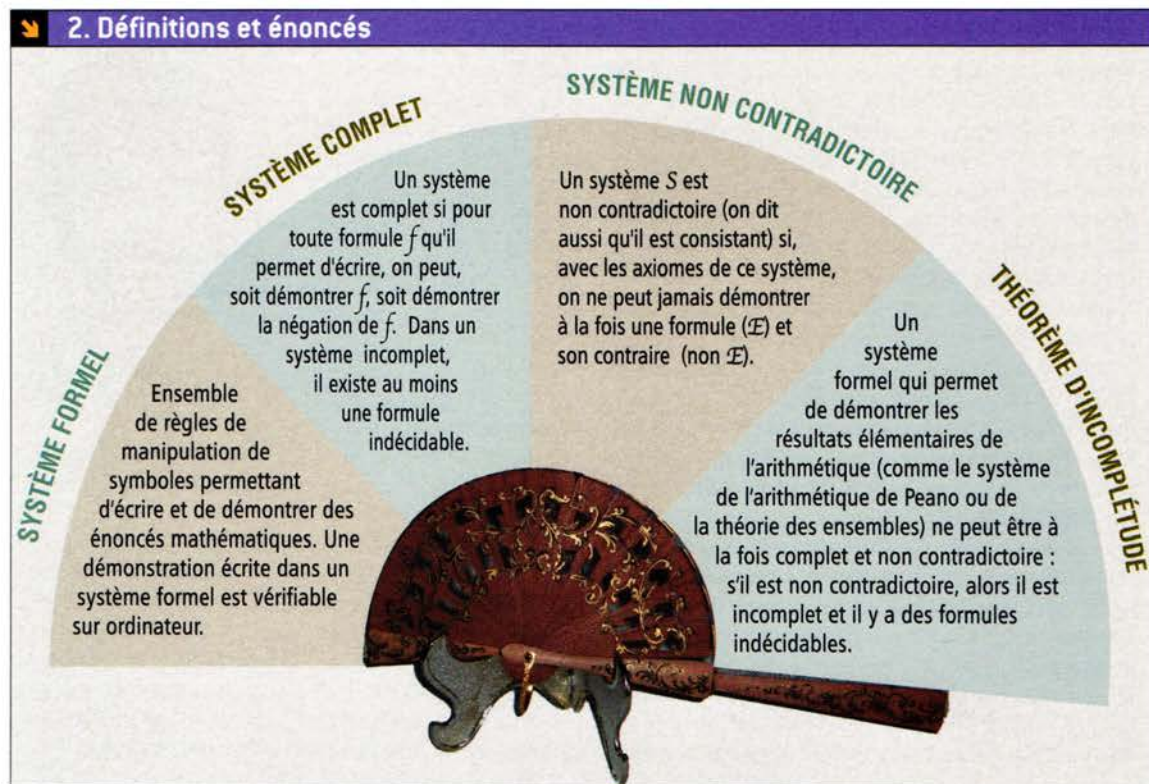


et si « n vérifie A implique que $n + 1$ aussi », alors « tout entier vérifie A ». Les raisonnements utilisés par les mathématiciens pour démontrer des propriétés concernant les nombres entiers s'y expriment sans trop de mal et, à vrai dire, de nombreux mathématiciens pensaient (avant Gödel) que tout énoncé vrai concernant les nombres entiers pouvait être démontré en suivant les règles de $\mathcal{PA}$.

On dit que $\mathcal{PA}$ est un système formel pour l'arithmétique car, quand on l'utilise, les raisonnements sur les entiers se ramènent à des manipulations formelles, c'est-à-dire à des manipulations de symboles obéissant à des règles intangibles. Vérifier qu'une démonstration écrite dans $\mathcal{PA}$ est correcte ne demande aucune intelligence et peut être fait mécaniquement. Ainsi, le contrôle des démonstrations est, pour tout système formel digne de ce nom, une opération mécanisable que l'on peut donc confier à un programme, et lorsque les mathématiciens prennent la peine d'écrire leurs démonstrations dans les notations de $\mathcal{PA}$, aucune contestation n'est possible.

On admet que $\mathcal{PA}$ est non contradictoire, c'est-à-dire qu'on ne peut pas, en l'utilisant, établir que deux propriétés se contredisent comme « 137 est un nombre premier » et « 137 est un nombre composé ». On a de bonnes raisons de croire que $\mathcal{PA}$ n'est pas contradictoire, la principale étant qu'on n'a jamais rencontré de contradiction en l'utilisant. Nous verrons qu'il est illusoire de vouloir le démontrer.

Le premier théorème d'incomplétude de Gödel appliqué à $\mathcal{PA}$ indique qu'il existe une formule F , concernant les entiers et exprimable dans le symbolisme de $\mathcal{PA}$, qu'on ne pourra pas démontrer avec $\mathcal{PA}$, et qui sera telle qu'on ne pourra pas non plus établir



«non F » (l'affirmation que F est fausse). Un tel énoncé échappe à $\mathcal{PA}$ avec lequel on ne peut démontrer que F est vraie, ni démontrer que F est fausse : il y a, en quelque sorte, un trou dans $\mathcal{PA}$. Une telle formule F est dénommée indécidable de $\mathcal{PA}$ et c'est à cause d'elle que $\mathcal{PA}$ est incomplet.

La démonstration de Gödel qui prouve l'existence d'indécidables repose sur la mise au point d'une formule G analogue au paradoxe d'Épiménides le Crétois (lequel affirme «Je mens»). Cette formule G énonce : « G n'est pas démontrable dans $\mathcal{PA}$ » (si G était démontrable, alors G serait vraie, car $\mathcal{PA}$ ne démontre que des choses vraies, et donc G ne serait pas démontrable!). Le raisonnement de Gödel ne s'applique pas seulement à $\mathcal{PA}$, mais à tout système formel assez puissant, et il s'y applique de manière constructive : si vous disposez d'un système formel S , la démonstration de Gödel vous donne de manière explicite et mécanique une formule F , indécidable dans S .

L'énoncé affirmant que « $\mathcal{PA}$ n'est pas contradictoire» est un énoncé désigné par $\mathcal{NC}(\mathcal{PA})$ que l'on peut exprimer dans $\mathcal{PA}$. Le second théorème d'incomplétude de Gödel nous dit que si $\mathcal{PA}$ n'est pas contradictoire alors $\mathcal{NC}(\mathcal{PA})$ est justement l'un des indécidables de $\mathcal{PA}$. C'est pourquoi démontrer la non-contradiction de $\mathcal{PA}$ est illusoire : $\mathcal{PA}$ ne pouvant le faire, des systèmes plus élémentaires que $\mathcal{PA}$ ne peuvent pas le faire non plus, et donc seuls des systèmes plus puissants peuvent y parvenir, ce qui semble inutile : la preuve de non-contradiction obtenue n'aura de sens que si le système plus puissant utilisé est lui-même non contradictoire, ce qui sera encore plus difficile à prouver et nécessitera un système encore plus puissant !

Suffirait-il d'ériger les indécidables en axiomes ?

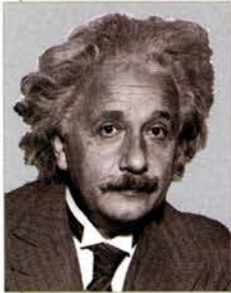
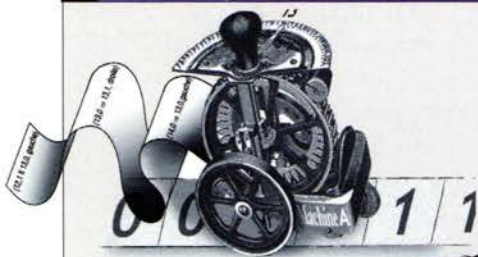
Une idée vient naturellement à l'esprit : pour contourner l'incomplétude de $\mathcal{PA}$, et faire que $\mathcal{PA}$ soit complet, pourquoi ne pas ajouter la formule indécidable F (ou sa négation) aux axiomes de $\mathcal{PA}$? Une fois F ajoutée, elle devient décidable car, en tant qu'axiome, elle est instantanément démontrée : le trou serait-il bouché ?

Ce serait trop simple ! Si l'on ajoute F aux axiomes de $\mathcal{PA}$, on obtient un nouveau système formel $\mathcal{PA}'$ (qui n'est plus $\mathcal{PA}$ puisque l'ensemble des axiomes a changé). La démonstration de Gödel s'applique à $\mathcal{PA}'$ qui est donc incomplet lui aussi, et elle fournit un énoncé indécidable F' dans $\mathcal{PA}'$. Ajouter F' aux axiomes de $\mathcal{PA}'$ ne ferait que repousser le problème et conduire à un système $\mathcal{PA}''$ qui posséderait encore un indécidable F'' , etc.

Cette impossibilité de compléter $\mathcal{PA}$ en lui ajoutant des axiomes n'est cependant pas absolue. Croire en un tel absolu, remarque L. Levin, conduit à des interprétations fausses des théorèmes d'incomplétude, par exemple celle affirmant que la vérité mathématique est incomplète, alors que ce sont nos moyens formels d'y accéder qui sont inadaptés.

Comme L. Levin le rappelle, dans l'abstrait, si on considère toutes les façons possibles d'ajouter des axiomes – en quantité finie ou infinie –, il y en a qui donnent des «systèmes» non contradictoires et complets. Ainsi, pour toute formule $\mathcal{L}$, on pourra démontrer $\mathcal{L}$, ou démontrer *non* $\mathcal{L}$, avec les axiomes. Le mot «systèmes» dans la phrase précédente est mis entre guillemets, car ces systèmes d'axiomes complets ne sont pas de vrais systèmes formels : il est certes possible d'ajouter dans l'abstrait des axiomes jusqu'à en gaver le système pour qu'on ne trouve plus aucun indécidable, mais dans ce cas on perd la vérifiabilité mécanique des preuves du système obtenu (si ce n'était pas le cas, on aurait un système qui contredirait le théorème de Gödel).

3. Incomplétudes



D'après le théorème de Gödel, un système formel, par exemple l'arithmétique de Peano, comporte des propositions indécidables. Peut-on le compléter en lui ajoutant des axiomes – éventuellement une infinité – de façon à obtenir un système complet (dépourvu d'indécidables) et non contradictoire ? Si on détermine les nouveaux axiomes par un procédé mécanique – par la complétion algorithmique –, le théorème de Gödel lui-même donne la réponse : non, ce que l'on obtiendra, si c'est un système non contradictoire, sera encore incomplet.

En revanche, il semblait envisageable d'ajouter des axiomes par un procédé aléatoire (combinaison de calculs et de tirages au sort), le procédé conduisant à l'infini à un système non contradictoire et complet. Étendant le résultat de Gödel, Leonid Levin a démontré que cette piste n'aboutit pas. L'incomplétude – on devrait peut-être dire « l'incomplétabilité » – est encore plus grave que ce que le théorème de Gödel de 1930 énonçait.

Les résultats de L. Levin généralisent encore cela et on peut les interpréter en affirmant qu'aucun procédé physique utilisé pour ajouter des axiomes ne peut compléter $\mathcal{PA}$ (ou tout système intéressant). L'idée, poussée à son extrême, suggère qu'aucune méthode, y compris celles incluant des humains, même aussi intelligents qu'Albert Einstein, n'avancera dans la direction d'une complétion progressive (telle que le suggérait Gödel, qui défendait qu'une partie essentielle du travail des mathématiciens serait de trouver de nouveaux axiomes).

Illustrons cette idée, essentielle pour comprendre le travail de L. Levin. Une méthode de complétion envisageable dans l'abstrait consiste à numérototer toutes les formules que l'on obtient en utilisant $\mathcal{PA}$: $F_0, F_1, \dots, F_n, \dots$. Puis on procède de la manière suivante :

– si F_0 est un indécidable de $\mathcal{PA}$, on ajoute F_0 aux axiomes, cela donne $\mathcal{PA}_1$; sinon

$\mathcal{PA}_1 = \mathcal{PA}$ (on ne change pas $\mathcal{PA}$);

– si F_1 est un indécidable de $\mathcal{PA}_1$, on ajoute F_1 aux axiomes de $\mathcal{PA}_1$; cela donne $\mathcal{PA}_2$; sinon, on ne change rien $\mathcal{PA}_2 = \mathcal{PA}_1$, etc.

Cette opération infinie de complétion donne un système non contradictoire complet $\mathcal{PA}_{\text{infini}}$. Le problème est qu'avec cette méthode, le « système » obtenu n'est plus vraiment un système formel. En effet, pour contrôler qu'une démonstration est correcte, il faut pouvoir tester si une formule donnée F est un axiome de $\mathcal{PA}_{\text{infini}}$. Or la méthode utilisée pour construire $\mathcal{PA}_{\text{infini}}$ ne fournit pas de procédé mécanique de test déterminant cela (savoir si une formule est indécidable n'est pas algorithmiquement testable).

L. Levin à la suite d'autres logiciens remarque que parmi les procédés abstraits, certains ne sont pas physiquement absurdes et permettent parfois de construire des objets intéressants non calculables par algorithme. On peut, par exemple en lançant une pièce de monnaie ou en observant le résultat d'une désintégration radioactive, entreprendre la construction d'une suite infinie de 0 et de 1 qui ne sera pas calculable par algorithme. Le hasard véritable, fondement de la mécanique quantique, est donc, dans certains cas, en mesure de construire des objets non calculables. La question se pose alors : ne pourrait-on pas, à l'aide d'un procédé mêlant des calculs et des tirages au hasard (comme décider si un indécidable est choisi comme axiome, dans son acception vraie ou fausse, par tirage au sort), construire un système non contradictoire complétant l'arithmétique de Peano $\mathcal{PA}$?

David Hilbert qui, semble-t-il, n'a jamais accepté l'incomplétude de $\mathcal{PA}$ pensait-il à cela ? Nous l'ignorons, mais la question méritait d'être posée... et résolue.

Le système obtenu à l'infini ne serait pas un véritable système formel (il ne permettrait pas une vérification mécanique des démonstrations, sinon il contredirait le théorème de Gödel), mais serait un système complet ayant une infinité d'axiomes résultant d'une méthode physiquement acceptable. On aurait surmonté l'incomplétude par un procédé raisonnable fondé sur le hasard. Si cette complétion par « algorithme probabiliste » était possible, nous pourrions nous approcher autant que nous le souhaitons d'un système dépourvu de trou, contournant ainsi l'incomplétude de Gödel, qui ne serait donc plus une fatalité.

Généralisant des résultats plus anciens concernant les algorithmes probabilistes, les théorèmes nouveaux de L. Levin prouvent en particulier que ce rêve est lui aussi inaccessible.

L'information sur le problème de l'arrêt

Quelle a été la méthode de L. Levin pour obtenir cette généralisation puissante et inespérée du théorème d'incomplétude ? La méthode a consisté à démontrer deux types de résultats par ailleurs intéressants en eux-mêmes.

Tout d'abord, L. Levin a étendu la théorie de l'information pour qu'elle sache envisager des suites infinies et il a défini un « contenu commun d'information » entre deux suites infinies. Il a aussi démontré des résultats de conservation de l'information qui s'appliquent en particulier aux algorithmes probabilistes.

Ensuite, L. Levin a établi que si un système d'axiomes complète celui de l'arithmétique – en ne laissant aucun trou – alors ce système porte nécessairement une information infinie sur la solution du problème de l'arrêt d'un programme. Ce problème de l'arrêt est la pierre de touche de la théorie de la calculabilité dont Alan Turing a démontré en 1936 qu'il était impossible à résoudre par algorithme (voir la figure 5).

4. Hasards

Les méthodes de calcul par algorithme ne permettant pas de compléter le système $\mathcal{PA}$, on peut envisager d'utiliser le hasard pour choisir les axiomes qui « complèteraient » le système de Peano. La question est : quel hasard ?

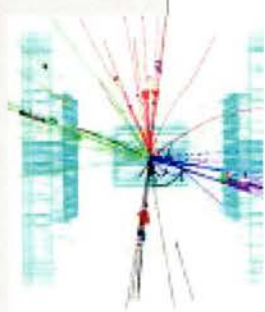
Non pas ce que nous appelons ordinairement hasard, lequel ne traduit, en physique classique, que notre incapacité à tenir compte des plus fines influences dans l'analyse du comportement des systèmes. Quand nous lançons une pièce en l'air, il n'y a pas de hasard vrai : les équations du mouvement sont connues et, si l'on sait mesurer avec suffisamment de précision les conditions initiales, le côté où tombe la pièce est déterminé sans ambiguïté.

En mécanique quantique, le hasard est intrinsèque : c'est le cas dans une désintégration radioactive par exemple. La radioactivité, terme inventé vers 1898 par Marie Curie, est un phénomène physique naturel au cours duquel des noyaux atomiques instables se désintègrent en dégageant de l'énergie sous forme de rayonnements divers, pour se transformer en des noyaux atomiques plus stables. Selon la mécanique

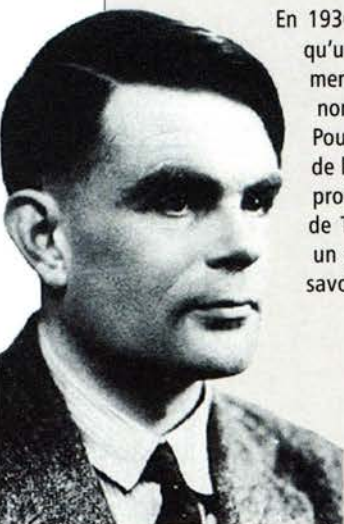
quantique, il est théoriquement impossible de prévoir le moment où un atome va se désintégrer.

Le hasard quantique est radicalement différent du hasard ordinaire : il s'agit d'un « vrai » hasard, un hasard intrinsèque, qui persiste quelle que soit la précision des mesures. Erwin Schrödinger le dira poétiquement : « La durée de vie d'un atome radioactif est encore moins prévisible que celle d'un moineau en bonne santé. » Notons que cette notion de hasard n'a jamais été acceptée par Einstein : le hasard en science, pensait-il, est l'entrée du diable dans un couvent !

Pour compléter un système, une méthode serait de choisir au hasard d'ajouter soit $\mathcal{G}$, soit la négation de $\mathcal{G}$ ($\mathcal{G}$ est l'indécidable de Gödel de $\mathcal{S}$, le système auquel on s'intéresse). Puis on recommencerait avec le nouveau système, etc. Les résultats de L. Levin montrent qu'une telle méthode ne marche pas.



5. Certaines informations sont spécifiques au monde mathématique



En 1936, Alan Turing montre le premier qu'une suite peut être mathématiquement parfaitement définie et pourtant non calculable par algorithme.

Pour cela, il considère le problème de l'arrêt d'un programme (en fait, le problème de l'arrêt d'une machine de Turing, ce qui revient au même) : un programme étant donné, peut-on savoir si, une fois démarré, il finira par s'arrêter ou s'il tournera indéfiniment ?

La réponse est non : aucun programme ne peut, par analyse des programmes qu'on lui fournirait en données, indiquer sans jamais se tromper ceux qui s'arrêteront et ceux qui poursuivront sans fin leurs calculs.

Prenons l'ensemble (dénombrable) de tous les programmes. Soit la suite S de '0' et de '1', $S = (a_0, a_1, a_2, \dots)$, définie par : $a_i = 1$ si le programme numéro i s'arrête, $a_i = 0$ sinon. Cette suite S est non calculable par programme. C'est le premier objet mathématique démontré non calculable. Depuis, beaucoup d'autres l'ont été.

La suite S est au cœur du résultat principal de Leonid Levin. Il établit en effet que tout système d'axiomes qui serait une extension complète et non contradictoire du système de l'arithmétique de Peano $\mathcal{PA}$ posséderait une infinité d'informations en commun avec S . La suite S est une sorte de sésame devant la porte de la complétude : pour compléter un système, il faut bien connaître S .

Or, nous ne le pouvons pas : L. Levin montre qu'un algorithme probabiliste (utilisant des calculs et des tirages au sort) ne peut pas accéder à une information substantielle sur la suite S démontrée non calculable par Turing.

L. Levin postule ensuite un principe plus général : aucun procédé physique utilisant des calculs, des tirages au sort et aucun processus physique raisonnable ne peuvent accéder à une information substantielle concernant S .

Ce postulat d'indépendance entre processus physiques et informations mathématiques est une loi de conservation de l'information : certaines informations ne sont pas dans le monde physique et ne peuvent pas y être produites. Ce postulat, comparable aux lois de conservation de l'énergie, du moment cinétique, etc., énoncés classiquement en physique, fixerait des limites définitives aux informations qu'on pourra extraire du monde physique. Il serait en quelque sorte la raison profonde du phénomène d'incomplétude qui concernerait non seulement les mathématiques, mais aussi la physique.

La conjonction de ces résultats implique qu'un procédé probabiliste ou un processus physique ne créant pas d'information sur le problème de l'arrêt (ce qui est vraisemblablement le cas de tous ceux qu'on peut raisonnablement envisager) ne peut, sur la base de $\mathcal{PA}$, construire un système d'axiomes complet et consistant. Précisons cela.

Des mondes à part

La notion d'information utilisée dans le raisonnement de L. Levin est celle mesurée par la théorie de la complexité de Kolmogorov, aussi dénommée théorie algorithmique de l'information : le contenu en information d'un objet (ou complexité de Kolmogorov de l'objet) est, par définition, la taille mesurée en bits du plus petit programme capable d'engendrer l'objet. Ce plus petit programme doit être vu comme une version comprimée au maximum de l'objet, et c'est pourquoi on parle parfois de contenu incompressible d'information. La théorie de l'information généralisée par L. Levin permet aussi de parler de la quantité d'information que possèdent en commun deux objets, et c'est en mesurant cette information mutuelle que L. Levin parvient à son résultat.

La suite S (voir l'encadré 5) des résultats concernant l'arrêt de programmes joue un rôle central en informatique théorique et dans la démonstration de L. Levin. C'est un sésame indispensable et inaccessible pour atteindre la complétude. Cette suite S est un mot de passe qu'aucun calcul, ni tirage au sort, ne peut approcher, et dont l'igno-

rance interdit l'accès à tout système complet non contradictoire construit à partir de $\mathcal{PA}$. Un procédé physique ne créant pas d'information sur S , il n'y a pas d'espoir de compléter $\mathcal{PA}$.

Au-delà de cette compréhension profonde de l'impossibilité de compléter $\mathcal{PA}$ par algorithmes probabilistes, L. Levin propose d'aller plus loin, au moins à titre de jeu spéculatif. Il défend l'idée que tout ce qui se passe dans le monde physique, même si cela ne se réduit pas à du calcul et des tirages au sort, est sujet aux lois de conservation de l'information : il est inconcevable d'après lui que le monde physique produise de l'information en quantité substantielle sur une suite comme S ou sur d'autres suites non calculables du même type.

Si l'on adopte ce postulat d'indépendance $\mathcal{PI}$ entre monde physique et monde mathématique, qui est une loi de conservation de l'information (analogue à la loi de conservation de l'énergie), on arrive à une forme renforcée et de nature physique du théorème d'incomplétude de Gödel : ce n'est plus seulement l'impossibilité de la complétion de $\mathcal{PA}$ par un algorithme qui doit être affirmée, mais l'impossibilité de la complétion de $\mathcal{PA}$ par un processus physique quelconque.

Cette forme étonnante du théorème de Gödel, contrairement aux deux autres (la forme initiale de Gödel et celle concernant les algorithmes aléatoires), n'est pas démontrable, car il s'agit d'un énoncé physique reposant sur un principe de conservation, pas plus démontrable que les autres principes de conservation que l'on postule en physique. Avec, d'une part, le résultat mathématique prouvé sur les liens forts entre tout système complétant $\mathcal{PA}$ et S et, d'autre part, la formulation du postulat d'indépendance comparable à une loi physique de conservation, une conception nouvelle des rapports entre mathématiques et physique est née.

Cette traduction de l'incomplétude logique proposée par L. Levin en un énoncé de physique aurait certainement réjoui Gödel : à Princeton, il aimait se promener longuement avec Einstein et il passa plusieurs années de sa vie à travailler sur les équations de la relativité générale. Même quand il ne le sait pas, le mathématicien ne travaille jamais uniquement pour lui : il fait aussi avancer la physique !

Presque tout est indécidable !

Grâce aux notions probabilistes, les logiciens démontrent que l'incomplétude de Gödel est beaucoup plus grave et incontournable que tout ce que l'on pouvait craindre.

L'incomplétude est l'incapacité, découverte et démontrée par Kurt Gödel, de concevoir un système mathématique qui capte toutes les vérités mathématiques. Le hasard est l'incapacité, que chacun a expérimentée, de prévoir ce qui va arriver. Quels sont les liens entre ces deux concepts centraux de la philosophie et de la science moderne ?

À cette question, les logiciens proposent aujourd'hui trois faisceaux de réponses. Chacun d'eux suggère des idées en opposition avec la conception traditionnelle des mathématiques comme science dont les connaissances s'acquièrent par la démonstration.

Raisnable, donc troué !

Découvert en 1930, le théorème d'incomplétude de Gödel affirme qu'en définissant de façon raisonnable ce que sont les preuves mathématiques, alors certaines vérités mathématiques échappent nécessairement à ces preuves.

Le mot « raisonnable » correspond à trois exigences. D'abord, on ne souhaite pas que les preuves conduisent à démontrer des affirmations contradictoires. Ensuite, on veut que les preuves permettent de démontrer les énoncés élémentaires vrais de l'arithmétique, par exemple que 25 est un carré, ou qu'il existe une infinité de nombres premiers. Enfin, si quelqu'un utilise cette définition des preuves pour démontrer un théorème, on exige que la preuve soit vérifiable sans risque d'erreur et d'une manière automatique. Ainsi, « raisonnable » pour un système de preuves signifie consistant, permettant de mener les raisonnements d'arithmétique élémentaire et vérifiable mécaniquement.

L'incomplétude démontrée par Gödel est avant tout une déception : elle affirme qu'avec une notion raisonnable de preuve mathématique, certaines vérités mathématiques ne pourront pas être prouvées : tout système raisonnable de preuves possède des trous. À y regarder de près, l'incomplétude de Gödel affirme un peu plus que la présence d'un trou dans tout système de preuves imaginables : elle affirme une « incomplétabilité ».

Le premier lien entre l'incomplétude et les probabilités que nous mentionnons précise justement cette « incomplétabilité ». Une conséquence directe du théorème de Gödel est qu'en ajoutant des vérités comme axiomes à l'aide d'un algorithme – qui éventuellement en ajoute progressivement une infinité – jamais on ne complète vraiment. Même après l'ajout, par un algorithme, d'une infinité d'axiomes à un système de preuves

1. Petite histoire de l'indécidabilité



David Hilbert rêvait de trouver un système complet d'axiomes dont on pourrait établir de manière simple qu'il était non contradictoire et qui permettrait de développer toutes les mathématiques.



Kurt Gödel démontre en 1931 que tout système assez puissant pour faire des mathématiques intéressantes et non contradictoires est incomplet : certaines affirmations mathématiques vraies n'y sont pas démontrables.



Alan Turing, grâce à son travail sur la notion d'algorithmes, permet de mieux comprendre le théorème d'incomplétude et de réaliser qu'il concerne un grand nombre de problèmes de programmation (et donc d'informatique).



Paul Cohen démontre l'indépendance de l'axiome du choix et de l'hypothèse du continu au sein de la puissante théorie des ensembles : l'indécidabilité concerne donc cette théorie centrale des mathématiques.



Andreï Kolmogorov propose une définition mathématique de la notion de complexité qui s'applique en physique et qui est donc touchée par l'indécidabilité : celle-ci est importante, y compris dans les sciences de la nature.



Per Martin-Löf, en formulant une définition rigoureuse de la notion de suite aléatoire infinie, permet une compréhension approfondie des liens entre probabilités et indécidabilité.



Yuri Matiyasevich, en montrant l'indécidabilité du dixième problème de Hilbert concernant les équations polynomiales diophantiennes, permet la formulation d'équations arithmétiques – complexes – indécidables.



Jeff Paris et Leo Harrington ont formulé un énoncé d'arithmétique ne provenant pas de la logique et indécidable dans l'arithmétique élémentaire : ainsi, l'indécidabilité touche les parties les plus basiques des mathématiques.



Gregory Chaitin, en définissant le nombre Ω – dont une théorie mathématique ne peut connaître qu'un nombre fini de chiffres –, produit un concentré d'indécidabilité déconcertant.



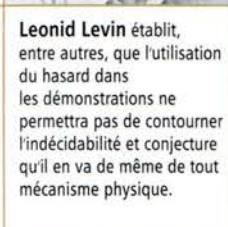
Robert Solovay aggrave encore le résultat de G. Chaitin en produisant une variante du nombre Ω dont *aucun* chiffre n'est connaissable par l'utilisation de la théorie usuelle des ensembles.



Cristian Calude établit diverses formes fortes du théorème de Gödel qui en éclairent la nature et qui signifient que presque tout énoncé est indécidable.



Raymond Smullyan tire des principes de la démonstration de Gödel un ensemble de problèmes paradoxaux qui en aident la compréhension et contribuent à populariser le résultat et sa démonstration.



Leonid Levin établit, entre autres, que l'utilisation du hasard dans les démonstrations ne permettra pas de contourner l'indécidabilité et conjecture qu'il en va de même de tout mécanisme physique.

incomplet, le nouveau système de preuves obtenu, bien que plus complet, ne le sera pas totalement : il existera encore des énoncés mathématiques vrais qui ne seront pas démontrables avec la notion élargie de preuves.

Que se passe-t-il si l'on ajoute des axiomes au système que l'on veut compléter en utilisant le hasard ? Le hasard permettrait-il de compléter totalement ? Concrètement, l'idée est d'utiliser des algorithmes probabilistes, c'est-à-dire des procédés de calcul qui, de temps en temps, décident de l'opération à effectuer en tirant au hasard un bit 0 ou 1, en lançant une pièce de monnaie par exemple.

La réponse à cette question subtile a été brillamment élucidée par Leonid Levin. L. Levin a montré que même en utilisant un algorithme probabiliste, on ne réussit jamais à compléter un système raisonnable de preuves. C'est notre première leçon sur les rapports du hasard et de l'incomplétude : le hasard ne permet pas de boucher le trou de l'incomplétude.

Le hasard n'aidera pas à compléter

Dans l'esprit de L. Levin, ce résultat d'incomplétabilité possède une forme étendue. Pour lui, aucun système physique (même s'il fonctionne durant un temps infini) ne pourra compléter un système raisonnable de preuves : soit il donnera des contradictions, soit il laissera des trous. L. Levin conjecture un principe d'indépendance entre la physique et le

La probabilité pour qu'une formule vraie de longueur n tirée au hasard soit indécidable tend vers 1 quand n tend vers l'infini : à l'infini, toutes les formules sont indécidables.

monde mathématique s'appuyant sur une loi de conservation de l'information : aucun procédé physique ne crée de l'information avec suffisamment d'efficacité pour compléter un système incomplet. Pour lui, cette loi est aussi fondamentale que d'autres lois de

conservation de la physique. Les arguments de L. Levin sont irréfutables dans le cas des algorithmes probabilistes, car ce sont des démonstrations mathématiques ; dans le cas plus général des procédés physiques quelconques, ces conjectures intéressantes n'ont sans doute pas été assez étudiées jusqu'à présent et aucun philosophe, à ma connaissance, ne les a analysées ou commentées. Ces arguments montrent que la limitation énoncée par le théorème de Gödel est plus grave qu'une simple limitation des systèmes de preuves : elle résulte d'un gouffre définitivement infranchissable entre le monde abstrait des mathématiques et celui de la physique (*voir des détails au chapitre précédent*).

La première réponse à notre interrogation est nette et négative : le hasard ne permet pas de combler le trou de l'incomplétude. La suite va confirmer la gravité, souvent insoupçonnée ou niée, de l'incomplétude logique découverte par Gödel.

La deuxième façon d'envisager la question des rapports entre incomplétude et probabilités est de se demander si l'incomplétude, finalement, ne serait pas un phénomène logique de peu d'importance du fait qu'elle ne concernerait que des énoncés « rares » ou qui surviennent avec une probabilité négligeable quand on les choisit « au hasard ».

Un système raisonnable de preuves étant fixé (par exemple l'arithmétique élémentaire de Peano ou la théorie des ensembles de Zermelo-Fraenkel), tombe-t-on fréquemment sur des indécidables ? Doit-on au contraire dire qu'ils sont rares ? Ces questions peuvent-elles recevoir une signification mathématique précise, par exemple à l'aide de formulations probabilistes ?

Cristian Calude, de l'Université d'Auckland en Nouvelle-Zélande, qui s'intéresse depuis longtemps à ce problème avec quelques collègues, a su y apporter plusieurs réponses. Celles-ci vont toutes dans le sens contraire de ce que nous désirions : un système S raisonnable de preuves étant fixé, alors une formule vraie y sera bien plus souvent indécidable que démontrable dans S . Il y a pire : l'indécidabilité, avec le système S , est quasi certaine dans l'ensemble infini des formules vraies !

La première série de résultats que C. Calude a obtenue avec Helmut Jürgen, de l'Université d'Ontario au Canada, et M. Zimand, de l'Université de Townson aux États-Unis, a été mise au point et publiée en 1994. Elle signifie que pour tout système raisonnable de preuves et pour toute notion topologique « d'ensemble rare » adaptée aux considérations et aux objets de la logique, l'ensemble des formules vraies prouvables est un ensemble « rare » dans l'ensemble des formules vraies. L'indécidabilité est la règle majoritaire dans l'ensemble infini des formules vraies ; avec tout système raisonnable de preuves, les formules vraies démontrables sont une proportion négligeable des formules vraies. L'essentiel de ce qui est vrai est inaccessible. Non seulement tout système raisonnable de preuves est troué, mais topologiquement, un tel système n'est qu'un immense trou !

L'interprétation de cette découverte est incompatible avec l'idée que les mathématiciens se font de leur science. Le raisonnement mathématique permet certes de lier les vérités mathématiques – des axiomes (admis), on tire d'autres vérités (démontrées) grâce au travail de déduction –, mais les liens entre « hypothèses posées » et « vérités prouvées » sont ténus et partiels. Les mathématiciens sont fiers de leurs démonstrations, car ils croient qu'elles sont puissantes et générales et qu'elles constituent la méthode d'accès privilégiée aux vérités du monde abstrait. Le résultat sur la rareté des formules vraies démontrables indique que cette puissance est illusoire : à l'infini, les liens créés par le raisonnement mathématique sont d'une extrême inefficacité. Parmi les formules vraies qu'on aimerait capter dans un système de preuves, toutes, sauf une partie infinitésimale d'entre elles, sont indécidables. Le raisonnement mathématique n'établit pratiquement aucune déduction, sa puissance est une impression trompeuse résultant peut-être de ce que notre intérêt se limite au tout début de la liste infinie des formules vraies.

Le raisonnement n'est qu'une méthode limitée ne résolvant qu'une partie dérisoire du problème ! Les résultats de 1994 expriment une impuissance définitive du raisonnement mathématique. Notons que cette impuissance est démontrée par un raisonnement mathématique..., ce qui est un petit paradoxe !

Bien sûr, on peut répliquer que ce qui intéresse le mathématicien, ce ne sont pas tous les énoncés vrais, mais uniquement certains d'entre eux bien particuliers, et qu'en conséquence, la rareté topologique des énoncés démontrables n'est peut-être pas vraiment ennuyeuse.

2. L'indécidabilité

Pour Leonid Levin, l'incapacité d'un système raisonnable de preuves à démontrer tout ce qui est vrai (théorème d'incomplétude de Gödel) ne peut être réparée ni par l'utilisation du hasard (méthode des algorithmes probabilistes) ni par l'utilisation d'un mécanisme physique et cela même si on le faisait fonctionner indéfiniment.

Aucune machine, aussi étrange et complexe qu'elle soit, ne peut engendrer des formules qu'on ajouterait comme axiomes et qui à l'infini fournirait un système complet pour les mathématiques. L. Levin pense qu'à cause d'un principe de conservation de l'information, de telles machines ne peuvent pas exister, comme il ne peut pas exister de mouvement perpétuel à cause du principe de conservation de l'énergie.



Une autre façon d'analyser le résultat sur la rareté des énoncés démontrables est de le voir comme la confirmation de la philosophie défendue par Gödel lui-même : faire des mathématiques, ce n'est pas seulement faire fonctionner le raisonnement à partir d'axiomes fixés une fois pour toutes, mais c'est aussi rechercher de nouveaux axiomes. Cette conception gödélienne des mathématiques comme quête de nouveaux énoncés à accepter sans preuve a été récemment illustrée par les travaux sur l'hypothèse du continu. À propos de ce problème, le travail du mathématicien aboutit à proposer l'adjonction de nouveaux axiomes à ceux traditionnellement considérés pour la théorie des ensembles. Le développement de la méthode expérimentale en mathématiques illustre aussi cette idée qu'il est utile d'envisager d'autres voies d'accès à la vérité que celle de la démonstration.

Une seconde série de résultats de C. Calude et H. Jürgensen (publiée en 2005) apporte un éclairage nouveau sur l'indécidabilité topologique de 1994 et vient la renforcer. Cette fois, la forte probabilité de l'incomplétude devient formulable en quelques mots simples, en même temps qu'une explication profonde du phénomène est proposée. C. Calude et H. Jürgensen ont donné un sens et une démonstration à l'idée avancée par Gregory Chaitin dès 1974 que l'incomplétude, dans certains cas, est la conséquence de la complexité.

La complexité, cause de l'indécidabilité

La longueur d'un énoncé mathématique E est le nombre de signes qu'il faut pour l'écrire : ainsi l'énoncé mathématique $1 + 6 = 7$ est de longueur 5. La complexité de Kolmogorov $K(E)$ d'un énoncé mathématique E est le nombre de signes du plus petit programme qui réalise l'impression de E : ainsi la complexité de Kolmogorov de la suite 010101... 01 (01 répété 100 fois, donc de longueur 200) est le nombre de signes, dans le langage de programmation donné, de l'instruction « Imprimer 100 fois 01 ». C. Calude et H. Jürgensen mesurent la complexité d'un énoncé mathématique E par la différence $d(E) = K(E) - \text{longueur}(E)$. Les énoncés dont la d -complexité est négative sont relativement simples, seuls ceux ayant une d -complexité positive sont complexes. Cette nouvelle mesure de complexité d'une formule ne remet pas en cause l'intérêt de $K(E)$ qui, à bien des égards, reste plus naturelle, mais elle est la bonne façon de dire d'une formule qu'elle est vraiment complexe. Précisons que la complexité $d(E)$ est souvent petite comparée à $K(E)$, mais que cela n'empêche pas $d(E)$ d'être parfois très grande et de dépasser n'importe quel nombre fixé à l'avance. Cette complexité conduit à la démonstration du remarquable résultat suivant : un système raisonnable de preuves ne peut démontrer que des énoncés E dont la complexité $d(E)$ est inférieure à une constante k (dépendant du système en question).

Dit autrement, toutes les formules trop complexes au sens de d sont indécidables. L'indécidabilité est donc conséquence de la complexité quand elle est mesurée par d . L'origine de l'indécidabilité, sa cause profonde, serait une trop grande complexité, affirmation qui n'est peut-être pas surprenante, mais qu'il est remarquable d'avoir formulé et démontré avec précision. Dès qu'un système raisonnable de preuves est fixé, la limite de son pouvoir de démonstration est aussitôt fixée par une constante k qui mesure le maximum de la complexité des formules que le système démontrera. Cela ne signifie pas que le système ne démontrera qu'un nombre fini de formules (c'est faux en général) ni d'ailleurs que toutes les formules vraies de complexité inférieure à k seront démontrables (certains indécidables sont assez simples), mais cela signifie que $d(E)$ ne sera jamais grand si E est démontrable.

Il résulte alors assez simplement de ce résultat mentionnant d que si l'on note $P(n)$ la proportion de formules de longueur n , vraies et démontrables dans un système raisonnable de preuves fixé S , alors $P(n)$ tend vers 0 quand n tend vers l'infini. En d'autres termes : une formule vraie prise au hasard parmi les formules de longueur n a une probabilité $P(n)$ d'être démontrable qui devient nulle quand n tend vers l'infini. À l'infini, toutes les formules vraies sont indécidables !

Cette seconde série de rapports entre probabilités et incomplétude aggrave ce que Gödel et L. Levin indiquaient sur la difficulté d'accès à la vérité mathématique. Les résultats et conceptions de L. Levin impliquent que le monde des vérités mathématiques est inaccessible depuis notre monde réel, soumis aux lois de la physique qui ne nous permettront jamais autre chose que l'utilisation de systèmes gravement incomplets et impossibles à compléter. Les résultats découverts par C. Calude et ses collègues signifient, de plus, que ces systèmes incomplets dont nous sommes obligés de nous satisfaire ne donnent accès, dans chaque cas particulier, qu'à une partie infinitésimale du monde mathématique !



3. Freeman Dyson, collègue physicien de Gödel...

Le physicien Freeman Dyson, de l'*Institute for Advanced Studies* de Princeton, a côtoyé Kurt Gödel pendant des années. Il est persuadé que l'indécidabilité est un phénomène courant en mathématiques et que bien des énoncés simples et compréhensibles par tous sont indécidables. Il en propose un.

« Nous savons grâce à Kurt Gödel qu'il existe des énoncés mathématiques vrais qui ne peuvent pas être démontrés. J'aimerais obtenir un peu mieux. Je voudrais un énoncé vrai, non démontrable et suffisamment simple pour être compris par les non-mathématiciens. Je vais en proposer un. Les nombres qui sont des puissances de deux sont 2, 4, 8, 16, 32, 64, 128, etc. Les nombres qui sont des puissances de cinq sont : 5, 25, 125, 625, etc. Un nombre étant donné, par exemple 131 072 (qui est une puissance de deux), son nombre inversé 270 131 s'obtient en prenant ses chiffres dans l'ordre inverse. J'affirme que jamais le nombre inversé d'une puissance de deux n'est une puissance de cinq. Les chiffres d'une puissance de deux assez grande semblent se présenter aléatoirement sans qu'aucun ordre n'y soit détectable. S'il se trouvait que le nombre renversé d'une puissance de deux soit une puissance de cinq, cela serait purement accidentel. Les chances pour que cela se produise avec une puissance de deux supérieure à un milliard sont infé-

2	2
4	4
8	8
16	61
32	23
64	46
128	821
256	652
512	215
1024	4201
2048	8402
4096	6904
8192	2918
16384	48361
32768	86723
65536	63556
131072	270131
262144	441262
524288	882425
1048576	6758401
2097152	2517902
4194304	4034914
8388608	8068838
16777216	61277761
33554432	23445533
67108864	46880176
134217728	827712431
268435456	654534862
536870912	219078635
1073741824	4281473701

rieures à une chance sur un milliard. La probabilité pour que cela survienne est donc au total inférieure à un milliardième. C'est pour cela que je crois que mon affirmation est vraie.

Mais l'hypothèse que les chiffres dans une puissance de deux surviennent au hasard implique que l'affirmation est indémontrable. Toute preuve devrait se fonder sur une propriété déterminée des chiffres. L'affirmation est vraie uniquement par chance et elle ne peut pas être démontrée parce qu'il n'y a pas de raisons mathématiques à cela. » L'énoncé de Dyson est peut-être vrai et indécidable – par exemple dans le système de la théorie des ensembles –, mais les séduisants arguments heuristiques qu'il propose n'établissent ni que l'énoncé est vrai ni qu'il s'agit d'un indécidable : il s'agit juste d'une intuition argumentée. D'autres affirmations mathématiques (nommées conjectures) sont jugées probables sans qu'on puisse les démontrer, ni démontrer qu'elles sont indécidables dans un système précis, et des milliers d'affirmations sont dans cette situation. Plusieurs livres de mathématiques en font des listes (par exemple Richard Guy : *Unsolved Problems in Number Theory*, Springer, 2004 ; V. Klee et S. Wagon, *Old and new Unsolved Problems in Plane Geometry and Number Theory*, Math. Assoc. of America, 1996).

Les suites tirées au hasard sont indécidables

Le troisième lien entre l'incomplétude et les probabilités est que tout ce qui est aléatoire est « essentiellement indécidable ».

Quelques précisions sont nécessaires pour donner un sens à cette affirmation. La notion de suite infinie aléatoire a été définie de manière précise grâce à la théorie de la calculabilité par Per Martin-Löf en 1966. Une suite binaire infinie $(x_0, x_1, \dots, x_n, \dots)$ est aléatoire si, à chaque fois que l'on considère la complexité de Kolmogorov des n premiers éléments de la suite, celle-ci vaut environ n , autrement dit si aucun début de la suite n'est compressible.

Voici maintenant le rapport entre ces suites aléatoires au sens de Martin-Löf et l'incomplétude. On suppose donné un système raisonnable de preuves S (par exemple celui

4. Un concentré d'indécidabilité

L'incomplétude se manifeste parfois avec une force inouïe. C'est le cas avec le nombre Oméga (Ω) de Gregory Chaitin. Ce nombre est défini comme la probabilité qu'un programme tiré au hasard s'arrête. Pour tirer un programme au hasard, on procède de la manière suivante : on convient d'écrire les programmes en base 2 (par exemple en utilisant un codage binaire des caractères). Le tirage au hasard d'un programme consiste à choisir à pile ou face avec une pièce non truquée des « 0 » et des « 1 » jusqu'à avoir un programme complet, et ensuite à le faire fonctionner. Cela fixe une procédure précise permettant l'évaluation de Ω et cette procédure ne comporte aucune ambiguïté.

Lorsque le langage de programmation et la convention de notation évoquée sont choisis, Ω est un être mathématique comme $\log(2)$ ou π . Puisque Ω est une probabilité, il est compris entre 0 et 1 et possède donc un développement binaire infini $\Omega = 0, a_1 a_2 \dots a_n \dots$.

La suite des chiffres de Ω est normale au sens de Borel : la fréquence avec laquelle on rencontre 0 ou 1 est $1/2$, la fréquence avec laquelle on rencontre la séquence 00 (ou 01, ou 10 ou 11) est $1/4$, et plus généralement la fréquence avec laquelle on rencontre une séquence déterminée de 0 et de 1 de longueur k est $1/2^k$.

Le nombre Ω est transcendant (il n'est solution d'aucune équation polynomiale à coefficients entiers).

Le nombre Ω est non calculable : aucun algorithme ne peut en égrainer les chiffres un à un.

Le nombre Ω est aléatoire au sens de Per Martin-Löf (voir le texte).

Le nombre Ω possède des chiffres qui, sauf pour un nombre fini d'entre eux, sont indécidables dans le sens suivant. Un



système raisonnable de preuves peut déterminer certains chiffres de Ω , c'est-à-dire démontrer des énoncés du type « $a_i = 1$ » ou « $a_i = 0$ », mais un système raisonnable de preuves ne démontrera qu'un nombre fini d'énoncés de ce type. Pour presque tous les chiffres a_i de Ω , l'énoncé vrai qui indique sa valeur (par exemple $a_{1273} = 1$) échappe à la théorie : elle ne le démontre pas, ni ne démontre sa négation ; pourtant Ω est défini de manière parfaitement précise et donc il est vrai que : soit $a_i = 0$, soit $a_i = 1$. Un système raisonnable de preuves ne peut quasiment rien savoir des chiffres de Ω , qui, de

manière définitive, sont pour lui inconnaissables (sauf pour une quantité finie d'entre eux).

Le nombre Ω de Chaitin est un cauchemar pour un esprit rationnel : il est « gravement indécidable », mais il existe des nombres Oméga qui sont pires. Associé à chaque système de preuves, le mathématicien Robert Solovay en a défini un qui est « le plus indécidable possible », on l'appelle le nombre Ω de Solovay. Son « inconnaissabilité » est absolue, car le système S auquel il est associé ne permet de connaître aucun chiffre de ce nombre. Dit autrement, tous les énoncés sans exception du type « $a_i = k$ » concernant les chiffres binaires de ce nombre sont des indécidables du système concerné.

Pour les 60 ans de G. Chaitin, la médaille en haut à gauche a été gravée par ses amis. La première citation est *Omne uno implicetur quod non attingitur ipsum*, le « o » de « uno » est remplacé par « Ω » : « Tout est dans Ω , mais Ω n'est pas atteignable. » La seconde citation est *Fortuita eveniunt vera mathematicae*, soit « Les vérités mathématiques sont en réalité tortueuses ».

de la théorie des ensembles ou celui de l'arithmétique élémentaire). Lorsqu'une suite (x_n) est aléatoire au sens de Martin-Löf, alors deux cas sont possibles :

– ou bien la suite (x_n) ne peut pas être définie dans S , et alors bien sûr on ne peut rien prouver dans S concernant (x_n) puisqu'on ne peut même pas en parler ! (ce cas n'est pas très intéressant, mais il ne faut pas l'oublier!),

– ou bien la suite (x_n) peut y être définie, ce qui est le cas par exemple des chiffres du nombre Oméga de G. Chaitin et alors, comme G. Chaitin l'a montré pour Oméga et C. Calude dans un cas plus général, le nombre de chiffres de la suite (x_n) que S permet de connaître est fini, autrement dit : (x_n) est essentiellement indécidable (*voir l'encadré 4*).

Si un procédé physique engendre une suite aléatoire (et en mécanique quantique on pense que de tels procédés existent) alors il engendre de l'indécidable. Par ailleurs, toutes les suites aléatoires qu'on peut définir en mathématiques avec précision (le nombre Oméga de G. Chaitin est une de ces suites) constituent des monstres d'indécidabilité.

Robert Solovay a d'ailleurs découvert une sorte de résultat ultime au sujet de l'indécidabilité des suites aléatoires. Son extraordinaire théorème indique qu'à tout système raisonnable de preuves S donné, est associé un nombre aléatoire Oméga(S), définissable dans S , mais tel que tous les énoncés de la forme «le n -ième chiffre de Oméga(S) est 0» sont indécidables dans S . Ce nombre bien présent dans S et que S peut désigner est néanmoins totalement inaccessible dans le détail, par les moyens de preuves de S puisqu'aucun de ses chiffres n'est connu de S : dans ce nombre Oméga de Solovay, l'incomplétude et le hasard se rejoignent sous une forme extrême et absolue.

Le hasard et l'incomplétude sont deux formes différentes de l'ignorance forcée que la science moderne a dû admettre et qu'elle essaie de comprendre. Leurs liens sont puissants, nombreux et subtils. À chaque fois qu'on arrive à élucider un de ces liens – et les trois liens que nous avons mentionnés ne sont peut-être pas les seuls possibles –, on découvre des formes renforcées du résultat de Gödel de 1930.

Le vieux théorème d'incomplétude, loin de décrire un innocent phénomène ne concernant les mathématiques que de loin comme cela a parfois été dit, se révèle, année après année, plus profond, plus grave et plus fondamental, en même temps qu'il nous force à revoir nos idées sur la nature réelle des mathématiques et de leurs rapports avec la physique.



La logique du désordre et des probabilités

Nos idées sont parfois « naturellement fausses ». En probabilité, le phénomène paraît fréquent. La loi de Benford affirme, contre toute logique, que les nombres dont le premier chiffre est un 1 sont plus utilisés que les nombres dont le premier chiffre est un 2. La comprendre est un défi, de même que l'identification de ce que les grandes structures finies rendent inévitable et que la théorie de Ramsey étudie. Les simulations d'un simple jeu de cour de récréation et les raisonnements sur un hypothétique sujet amnésique conduisent à leur tour à des résultats absurdes... ou peut-être seulement vrais, mais nous obligeant à corriger nos préjugés logiques.



L'étonnante loi de Benford

Le « 1 » apparaît en premier bien plus souvent que les autres chiffres !

Ce phénomène est imparfaitement expliqué, mais il permet de dépister les tricheurs.

Je vous propose le pari suivant : ouvrons le journal, choisissons une page au hasard et notons le premier nombre que nous rencontrons ; si le premier chiffre significatif de ce nombre est supérieur à 3, je vous donnerai 100 euros, sinon c'est vous qui me donnerez 100 euros.

La proposition vous est, semble-t-il, nettement favorable : il n'y a en effet que trois chiffres qui me font gagner (1, 2, 3), alors qu'il y en a six pour vous (4, 5, 6, 7, 8, 9) ; le 0 ne compte pas, car il ne peut pas être un premier chiffre significatif. Vous pensez donc gagner environ deux fois sur trois. Serais-je idiot de vous proposer un tel pari ?

Eh bien non : si vous acceptez, je gagnerai dans plus de 60 pour cent des cas. Aussi étonnant que cela paraisse, le premier chiffre significatif d'un nombre rencontré dans un article de journal n'a pas autant de chances d'être un 1, un 2, un 3, ..., ou un 9 (la probabilité serait alors 1/9, ou 11,11 pour cent). La loi de Benford indique que, dans

a



b



1 Les données recueillies par Benford et publiées en 1938 (c) sont d'une grande variété : toutes indiquent que le premier chiffre significatif de données statistiques (longueur des rivières, des routes, altitudes des montagnes, population des villes, aires des circonscriptions religieuses avant la Révolution française) est 1 avec une fréquence de 30 pour cent au lieu de 11 pour cent si les chiffres de 1 à 9 apparaissaient avec la même fréquence. De même le 2 est

surreprésenté, mais moins, et plus souvent premier chiffre significatif que « 3 ». Enfin, le 9 est le plus rare. On retrouve cette répartition bizarre détaillée sur l'histogramme (e) en géographie, en mathématiques pour le premier chiffre de certaines suites, dans les résultats sportifs, etc. (tableau d, traduit de Benford). Les proportions coïncident bien avec la série découverte par Benford (dernière ligne du tableau d sous l'intitulé « prédite ») : la probabilité pour qu'un nombre

c

THE LAW OF ANOMALOUS NUMBERS

FRANK BENFORD

Physicist, Research Laboratory, General Electric Company,
Schenectady, New York

(Introduced by Irving Langmuir)

(Read April 22, 1937)

ABSTRACT

It has been observed that the first pages of a table of common logarithms show more wear than do the last pages, indicating that more used numbers begin with the digit 1 than with the digit 9. A compilation of some 30,000 first digits taken from widely divergent sources shows that there is a logarithmic distribution of first digits when the numbers are composed of four or more digits. An analysis of the numbers from different sources shows that the numbers taken from unrelated subjects, such as a group of newspaper items, show a much better agreement with a logarithmic distribution than do numbers from mathematical tabulations or other formal data. There is here the peculiar fact that numbers that individually are without relationship are, when considered in large groups, in good agreement with a distribution law—hence the name "Anomalous Numbers."

A further analysis of the data shows a strong tendency for bodies of numerical data to fall into geometric series. If the series is made up of numbers containing three or more digits the first digit forms a logarithmic series. If the numbers contain only single digits the geometric relation still holds but the simple logarithmic relation no longer applies.

An equation is given showing the frequency of first digits in the different orders of numbers 1 to 10, 10 to 100, etc.

The equation also gives the frequency of digits in the second, third, ... place of a multi-digit number, and it is shown that the same law applies to reciprocals. There are many instances showing that the geometric series, or the logarithmic law, has long been recognized as a common phenomenon in factored functions and in the ordinary affairs of life. The wire gauge and drill gauge of the mechanic, the magnitude scale of the seismometer and the sensory response curves of the psychologist are all particular examples of a relationship that seems to extend to all human affairs. The Law of Anomalous Numbers is thus a general probability law of widespread application.

PART I: STATISTICAL DERIVATION OF THE LAW

It has been observed that the pages of a much used table of common logarithms show evidences of a selective use of the natural numbers. The pages containing the logarithms of the low numbers 1 and 2 are apt to be more stained and frayed by use than those of the higher numbers 8 and 9. Of

PROCEEDINGS OF THE AMERICAN PHILOSOPHICAL SOCIETY,
Vol. 74, no. 4, MARCH, 1938

BENFORD

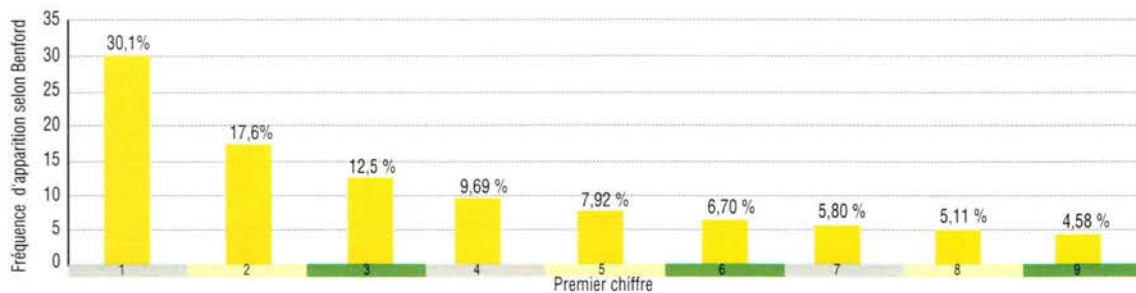
Printed in U. S. A.

551

d

Premier chiffre	1	2	3	4	5	6	7	8	9	Échantillon
Rivières	31,0	16,4	10,7	11,3	7,2	8,6	5,5	4,2	5,1	335
Populations	33,9	20,4	14,2	8,1	7,2	6,2	4,1	3,7	2,2	3 259
Constantes	41,3	14,4	4,8	8,6	10,6	5,8	1,0	2,9	10,6	104
Journaux	30,0	16,4	12,0	10,0	8,0	6,0	6,0	5,0	5,0	100
Chaleurs spéc.	31,0	18,4	16,2	14,6	10,6	4,1	3,2	4,8	4,1	1 389
Pression	31,0	18,3	12,8	9,8	8,3	6,4	5,7	4,4	4,7	703
Puissance perdue	30,0	18,4	11,9	10,8	8,1	7,0	5,1	5,1	3,8	690
Poids moléculaires	26,7	25,2	15,4	10,8	6,7	5,1	4,1	2,8	3,2	1 800
Drainage	27,1	23,9	13,8	12,6	8,2	5,0	5,0	2,5	1,8	159
Poids atomiques	47,2	18,7	5,5	4,4	6,6	4,4	3,3	4,4	5,5	91
$n-1, \sqrt{n}$	25,7	20,3	9,7	6,8	6,6	6,8	7,2	8,0	8,9	5 000
Architecture	36,8	14,8	14,3	7,5	8,3	8,4	7,0	7,3	5,6	560
Reader's Digest	33,4	18,5	12,4	7,5	7,1	6,5	5,5	4,9	4,2	308
Coûts	32,4	18,8	10,1	10,1	9,8	5,5	4,7	5,5	3,1	741
Voltage X	27,9	17,5	14,4	9,0	8,1	7,4	5,1	5,8	4,8	707
Base-ball	32,7	17,6	12,6	9,8	7,4	6,4	4,9	5,6	3,0	1 458
Rayonnement	31,0	17,3	14,1	8,7	6,6	7,0	5,2	4,7	5,4	1 165
Adresses	28,9	19,2	12,6	8,8	8,5	6,4	5,6	5,0	5,0	342
$n^1, n^2, \dots, n^6$	25,3	16,0	12,0	10,0	8,5	8,8	6,8	7,1	5,5	900
Mortalité	27,0	18,6	15,7	9,4	6,7	6,5	7,2	4,8	4,1	418
Moyenne	30,6	18,5	12,4	9,4	8,0	6,4	5,1	4,9	4,7	1 011
Valeurs prédites	30,1	17,6	12,5	9,69	7,92	6,70	5,80	5,11	4,58	

e



pris dans une grande série de données commence par le chiffre c [$c = 1, 2, \dots, 9$] est $\log_{10}[1 + 1/c]$. Ci-contre, Frank Benford [a] à l'époque de la publication de son article, en mars 1938, et les célèbres cartes de Vidal-Lablache [b] où le phénomène est patent quand on mesure les différentes caractéristiques géographiques. Dans son article [c], Frank Benford a dénommé cette observation la loi des nombres anormaux: «Il a été observé que les premières

pages des tables de logarithmes [utilisées avant les ordinateurs pour les calculs précis] sont plus usées que les dernières pages, ce qui indique que les nombres les plus utilisés commencent plus fréquemment par 1 que par 9. Une compilation de plus de 20 000 premiers chiffres des nombres provenant de sources très différentes montre une distribution logarithmique de ces chiffres quand les nombres ont plus de quatre chiffres.»

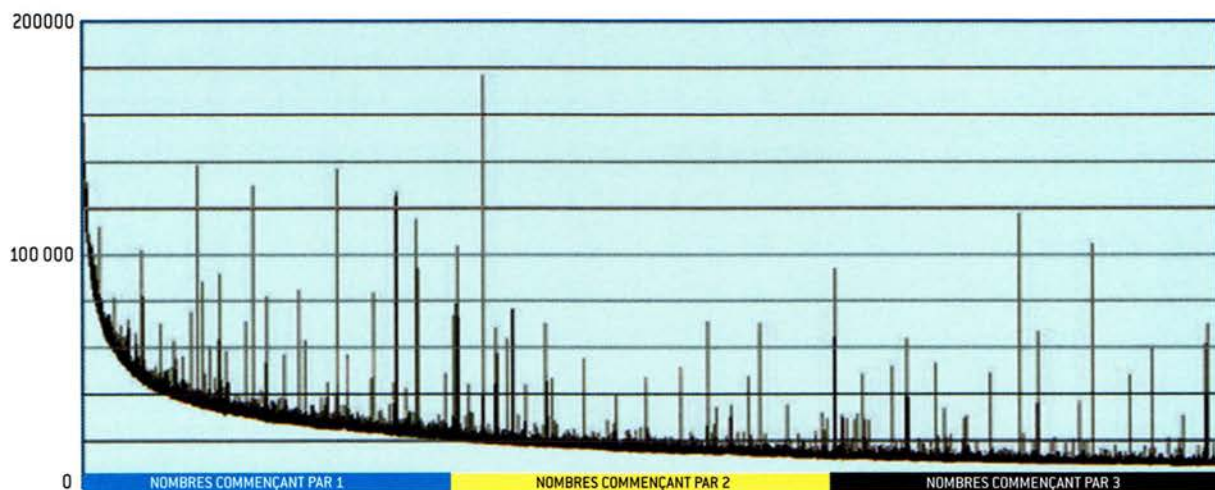
un contexte général comme celui d'un article de journal, les probabilités p de rencontrer les différents chiffres comme premier chiffre significatif sont, exprimées en pourcentage : $p(1) = 30,1$; $p(2) = 17,6$; $p(3) = 12,5$; $p(4) = 9,7$; $p(5) = 7,9$; $p(6) = 6,7$; $p(7) = 5,8$; $p(8) = 5,1$; $p(9) = 4,6$. Puisque $30,1 + 17,6 + 2,5 = 60,2$, je gagnerai mon pari dans 60,2 pour cent des cas.

Quelle est donc cette loi bizarre du premier chiffre significatif, si contraire à l'intuition ?

Découverte deux fois

Universellement connue aujourd'hui sous le nom de loi de Benford, cette loi a été découverte en 1881 par l'astronome Simon Newcomb, qui avait observé une détérioration des tables de logarithmes bien plus importante pour les pages des nombres commençant par 1 que pour les pages des nombres commençant par 9. L'article qu'il publia sur le sujet dans le *Journal of Mathematics* passa inaperçu ; aussi, lorsque 57 ans plus tard, le physicien Frank Benford remarqua à son tour l'usure inégale des pages des tables de logarithmes, il crut être le premier à formuler cette loi qui, aujourd'hui porte indûment son nom.

Les articles de Newcomb et de Benford ne se contentent pas de constater, ils proposent chacun la même formule mathématique donnant la probabilité des chiffres. La probabilité que le chiffre c soit le premier chiffre significatif d'un nombre est, d'après eux, $\log_{10}(1 + 1/c)$, où $\log_{10}$ désigne le logarithme décimal : $\log_{10}(10)=1$; $\log_{10}(1)=0$; $\log_{10}(ab) = \log_{10}(a) + \log_{10}(b)$; $\log_{10}(a/b) = \log_{10}(a) - \log_{10}(b)$. Remarquons que leur



2 La table des constantes numériques de Simon Plouffe contient un milliard de constantes (occupant 45 gigaoctets de mémoire !) dont bien sûr π , e , $\sqrt{2}$, $\sqrt{3}$, $\sin(1)$, $\log \pi$, $\exp[\sqrt{2}]$, etc., mais aussi des sommes de séries et des valeurs de fonctions classiques évaluées en divers points, etc. Les statistiques sur le premier chiffre des constantes présentes dans la table le 6 novembre 2006 sont : 38,046 % des entrées commencent par 1 ; 15,433 % commencent par 2 ; 10,871 %

commencent par 3 ; 8,195 % commencent par 4 ; 6,913 % commencent par 5 ; 6,066 % commencent par 6 ; 5,225 % commencent par 7 ; 4,777 % commencent par 8 et 4,475 % des entrées commencent par 9. C'est à peu près les statistiques de la loi de Benford, mais avec un écart à la loi non négligeable compte tenu du très grand nombre de constantes considérées. La courbe tracée montre des pics qui sont dus à ce que S. Plouffe a étudié certains nombres avec une attention particulière.

proposition convient parfaitement pour une probabilité puisque la somme des probabilités est égale à 1 (un des chiffres doit apparaître au premier rang):

$$\begin{aligned} &\log_{10}(1 + 1/1) + \log_{10}(1 + 1/2) + \dots + \log_{10}(1 + 1/9) = \\ &\log_{10}(2) + \log_{10}(3/2) + \log_{10}(4/3) + \dots + \log_{10}(10/9) = \\ &\log_{10}[2 \times (3/2) \times (4/3) \times \dots \times (10/9)] = \log_{10}(10) = 1 \end{aligned}$$

Avant d'examiner en quel sens cette loi est une loi scientifique, et comment nous pouvons l'expliquer, voyons sa généralisation.

La mantisse est en rapport avec l'écriture d'un nombre en notation scientifique. La mantisse d'un nombre R est le nombre a , compris entre 1 et 10, tel que $R = a \times 10^n$ (ainsi la mantisse de 5 000 000 est 5, la mantisse de 1 024 est 1,024, la mantisse de 0,25 est 2,5). Alors la probabilité, selon la loi de Benford, que la mantisse d'un nombre réel soit dans l'intervalle $[a, b]$ est $(\log_{10}(b) - \log_{10}(a))$.

Cette généralisation redonne la version initiale de la loi de Benford pour $a = c$ et $b = c + 1$, car: $\log_{10}(c + 1) - \log_{10}(c) = \log_{10}[(c+1)/c] = \log_{10}(1+1/c)$, la probabilité que le premier chiffre soit c . Il résulte aussi de cette généralisation que lorsqu'une série de nombres satisfait la loi de Benford, la probabilité de trouver un deuxième chiffre significatif égal à y (par exemple 5) dépend du premier chiffre x . Ainsi, la probabilité que le deuxième chiffre significatif soit 5 quand le premier vaut 1 est: $(\log(1,6) - \log(1,5)) / (\log(2) - \log(1)) = 9,31$ pour cent. La probabilité que le deuxième chiffre significatif soit 5 quand le premier est 8 est $(\log(8,6) - \log(8,5)) / (\log(9) - \log(8)) = 9,93$ pour cent.

La généralisation permet d'étudier les autres chiffres et le résultat se conforme cette fois à l'intuition: si une série de nombres satisfait la loi de Benford, alors plus un chiffre est loin après le premier chiffre, plus la probabilité qu'il soit un 1, un 2, ... ou un 9 est proche de 1/10 (cette fois le 0 est possible). Pour le deuxième chiffre significatif, les probabilités p sont respectivement: $p(0)=11,96$; $p(1)=11,39$; $p(2)=10,88$; $p(3)=10,43$; $p(4)=10,03$; $p(5)=9,67$; $p(6)=9,34$; $p(7)=9,03$; $p(8)=8,76$; $p(9)=8,50$. Pour le quatrième chiffre, toutes les probabilités sont comprises entre 9,98 pour cent et 10,02 pour cent.

La loi est-elle toujours valable ?

Immanquablement, face à cette prétendue «loi», nous nous posons de nombreuses questions: est-elle vraiment toujours vérifiée? En quel sens s'agit-il d'une loi? D'où provient-elle et que signifie-t-elle?

Bien sûr, la réponse à la première question est: non, la loi n'est pas systématiquement vérifiée. Ainsi, les numéros de téléphone que l'on trouve dans un annuaire ne la vérifient pas, car les opérateurs distribuent les numéros en fonction de critères particuliers et systématiques (les numéros commencent d'ailleurs souvent par 0). Les tailles des êtres humains adultes mesurées en mètres commencent dans plus de 95 pour cent des cas par un 1 et donc la «loi de Benford» n'est pas satisfaite pour des données statistiques sur les tailles. Les prix de vente d'un modèle particulier de voiture neuve varient peu d'un concessionnaire à l'autre et donc ne vérifient pas la loi: à chaque fois qu'une donnée statistique est contrainte de rester dans un intervalle étroit, la loi de Benford n'est pas satisfaite.

Benford, pour tester son idée, avait collecté 20 229 observations diverses incluant des données géographiques, des résultats sportifs, des valeurs de constantes physiques, des prix, des séries mathématiques, etc. Il avait constaté, d'une part, que quand on regroupe toutes les données, la loi était satisfaite avec une bonne précision, comme on le voit sur

le tableau de la figure 1. D'autre part, de nombreuses séries la satisfaisaient « à peu près » : elles montraient au moins une nette décroissance de la fréquence des chiffres en fonction de leur rang. Depuis, ces constatations ont été souvent contrôlées et vérifiées.

Cependant, des études récentes fondées sur des collectes de nombres bien plus volumineuses et un examen statistique plus fin tempèrent l'enthousiasme. P. Scott et M. Fasli, de l'Université de l'Essex, ont examiné 230 séries statistiques incluant au total près de 500 000 données. Ils remarquent que le phénomène de décroissance des probabilités d'un chiffre au suivant est quasi général, mais qu'il ne suit de près la loi de Benford que dans 29 séries. La loi des logarithmes est une approximation, souvent grossière, de ce qui est observé.

Les lois déterminant réellement la probabilité d'apparition du premier chiffre significatif sont, dans le monde réel, des variantes de la loi pure fixée par les logarithmes que Newcomb et Benford ont formulée. Le cas des chiffres provenant de données financières est caractéristique : les chiffres de ce domaine s'écartent assez nettement de la loi de Benford. Reste que même si l'ajustement n'est pas parfait et ne le devient pas nécessairement quand on augmente le nombre des données examinées, la loi de Benford pour de nombreuses séries numériques réelles est pertinente en première approximation et bien meilleure que l'attribution d'une probabilité de $1/9$ à chaque chiffre que nous souffle l'intuition. Pourquoi cela ?

Suites mathématiques et Benford

Considérons d'abord les suites purement mathématiques pour lesquelles un ensemble de résultats, certains récents, éclaire la règle et ses exceptions.

En 1968, le mathématicien russe Vladimir Arnold, associé à André Avez, démontra que la suite numérique (2^n) satisfait la loi de Benford à l'infini, dans le sens suivant : la proportion des éléments de la suite considérée jusqu'à n , dont le premier chiffre est 1, tend vers $\log_{10}(2)$ quand n tend vers l'infini, conformément à la loi de Benford et il en va de même pour les autres chiffres c pour lesquels la limite est bien le $\log_{10}(1 + 1/c)$ attendu.

Ce résultat a depuis été généralisé. On a d'abord montré que la suite (r^n) , r étant un nombre réel positif, satisfait la loi de Benford à l'infini pourvu que $\log_{10}(r)$ ne soit pas un nombre rationnel (c'est-à-dire un rapport de deux entiers). Les suites (3^n) , (4^n) , (5^n) satisfont donc la loi de Benford, alors que (10^n) et $(\sqrt{10})^n$ ne la satisfont pas, ce qu'il est facile de constater.

En 2005, Paul Jolissaint, de l'Institut de mathématiques de Neuchâtel, a démontré un résultat général concernant les suites définies par une relation de récurrence du type $x(n) = a_1x(n-1) + a_2x(n-2) + \dots + a_px(n-p)$. Ce résultat indique que la suite de Fibonacci 1, 1, 2, 3, 5, 8, ... (définie par $x(0) = x(1) = 1$ et $x(n) = x(n-1) + x(n-2)$) satisfait la loi de Benford à l'infini. Le résultat s'applique aussi à la suite obtenue en ne retenant qu'un élément sur deux de ces suites ou en ne retenant que les éléments dont le numéro est un carré parfait, et plus généralement à toutes les suites extraites en ne retenant que les termes dont le numéro est donné par un polynôme (fixé) à coefficients entiers ne prenant que des valeurs positives différentes. Il est remarquable que la démonstration de ce beau théorème s'appuie sur un résultat de 1916 dû au mathématicien Hermann Weyl (1885-1955).

D'autres démonstrations récentes établissent que les suites $n!$ et n^n satisfont aussi parfaitement la loi de Benford à l'infini. Les coefficients du binôme de Newton (qu'on trouve dans le triangle de Pascal) satisfont eux aussi la loi de Benford. Nous savons encore que si (x_n)

satisfait la loi de Benford, il en va de même de (cx_n) , c constante positive quelconque, ou même de (x_n^p) , p étant un entier quelconque non nul.

En revanche, il a été démontré que, pour b positif et p_n le n -ième nombre premier, aucune des suites : $(b, 2b, 3b, \dots, nb, \dots)$, $(1, 2^b, 3^b, \dots, n^b, \dots)$, $(\log_b 1, \log_b 2, \log_b 3, \dots, \log_b n, \dots)$, $(1, 2, 3, 5, \dots, p_n, \dots)$, $(\log_b 2, \log_b 3, \log_b 5, \dots, \log_b p_n, \dots)$ ne vérifie la loi de Benford parce que les fréquences associées aux chiffres ne convergent pas.

La table de constantes mathématiques que Simon Plouffe collecte depuis de nombreuses années et qui contient aujourd'hui plus d'un milliard de nombres est intéressante, car elle satisfait en gros la loi de Benford. S. Plouffe utilise d'ailleurs cette loi pour détecter des erreurs qui pourraient s'y glisser. Les exceptions en certains points à la loi s'expliquent par la façon dont il a engendré sa collection en s'intéressant à des nombres particuliers.

Cesàro à la rescousse

Reste que les résultats qu'on obtient dans le monde parfait des mathématiques ne justifient pas ce que Newcomb et Benford ont vu pour les séries de nombres provenant du monde réel. Aussi de nombreuses études tentent d'expliquer rationnellement l'étrange phénomène. Quatre types d'explications sont proposés.

Pour les numéros des maisons qu'on trouve dans des adresses collectées dans un annuaire, et qui vérifient assez bien la loi de Benford, une idée simple vient à l'esprit. Si une rue possède 50 numéros, alors plus d'un cinquième des numéros commencent par un 1 (à cause de 10, 11, 12, ..., 19) ; si elle en possède 20 ou 200, plus de la moitié des numéros commencent par un 1. Il est donc parfaitement normal que dans une rue dont la longueur est inconnue, on trouve en moyenne plus souvent des numéros commençant par 1 que par 9 (et plus généralement par le chiffre c que par $c + 1$).

Si on note $f_1(n)$ la fréquence des entiers commençant par 1 parmi les entiers compris entre 1 et n (de même on notera $f_2(n)$ la fréquence pour le 2, $f_3(n)$ la fréquence pour le 3, etc.), on s'aperçoit que la suite $f_1(n)$ n'est pas convergente et qu'elle oscille indéfiniment entre $1/9$ et $5/9$. L'oscillation est de plus en plus lente, mais son amplitude reste de $4/9$. La suite $f_9(n)$ oscille, elle, entre $1/81$ et $1/9$. Comment s'en sortir ?

Pour adoucir ces oscillations, l'idée est de faire la moyenne des $f_1(k)$ pour k variant de 1 jusqu'à n : $[f_1(1) + f_1(2) + \dots + f_1(n)]/n$, c'est ce que l'on nomme la moyenne de Cesàro $s_1(n)$ de la suite $f_1(n)$. On obtient alors une nouvelle suite qui ne converge toujours pas, mais qui varie

3. Cesàro explique Benford !

Les numéros des maisons dans les rues obéissent à la loi de Benford à la condition de faire des moyennes successives selon le principe inventé par le mathématicien Ernesto Cesàro (1859-1906). On désigne par $f_1(n)$ la fréquence du chiffre 1 comme premier chiffre dans la suite des n premiers nombres :

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, ...

De même, $f_2(n)$ est la fréquence du chiffre 2 comme premier chiffre dans la suite des n premiers nombres :

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, ...

et ainsi de suite pour $f_3(n)$, $f_4(n)$, $f_5(n)$, ..., $f_9(n)$.

On effectue alors la moyenne à la Cesàro des $f_1(n)$:

$$s_1(n) = [f_1(1) + f_1(2) + f_1(3) + f_1(4) + f_1(5) + f_1(6) + f_1(7) + \dots + f_1(n)]/n.$$

Et de même :

$$s_2(n) = [f_2(1) + f_2(2) + f_2(3) + f_2(4) + f_2(5) + f_2(6) + f_2(7) + \dots + f_2(n)]/n.$$

Puis on réitère pour les moyennes de Cesàro $t_1(n)$, $t_2(n)$:

$$t_1(n) = [s_1(1) + s_1(2) + s_1(3) + s_1(4) + s_1(5) + s_1(6) + s_1(7) + \dots + s_1(n)]/n,$$

et :

$$t_2(n) = [s_2(1) + s_2(2) + s_2(3) + s_2(4) + s_2(5) + s_2(6) + s_2(7) + \dots + s_2(n)]/n.$$

La valeur de $f_1(n)$ varie entre $1/9$ et $5/9$ et la valeur de la suite $f_9(n)$ entre $1/81$ et $1/9$. En continuant ainsi, on obtient des valeurs qui oscillent de moins en moins, et B. Flehinger a démontré qu'en poursuivant ces calculs de moyennes, l'intervalle de variation de ces sommes se réduit, à l'infini, à la valeur attendue, soit $\log_{10}(2)$ pour celle associée au 1.

Cette convergence d'une suite à la Cesàro est une idée intéressante dans la mesure où elle fait converger des suites qui étaient divergentes. L'exemple souvent cité est la suite 01010101... qui converge vers $1/2$ au sens de Cesàro.

17

cette fois dans un intervalle plus étroit. En recommençant ce procédé de moyenne, on obtient des suites qui varient dans des intervalles de plus en plus étroits et B. Flehinger a démontré en 1966 que l'intervalle qu'on obtient en poursuivant ces calculs de moyennes de moyennes s'approche, à l'infini, de la valeur attendue, soit $\log_{10}(1 + 1/1) = \log_{10}(2)$.

Pour les autres chiffres, le constat est analogue et donc, dans le sens très particulier des moyennes itérées de Cesàro, on peut dire que la fréquence des nombres commençant par c dans l'ensemble de tous les entiers est $\log_{10}(1 + 1/c)$.

D'autres méthodes de ce type permettent d'attribuer une « mesure » (une fréquence) à l'ensemble des nombres entiers commençant par 1 (ou 2, ..., ou 9). Toutes celles connues et possédant des propriétés raisonnables (par exemple que l'ensemble des nombres pairs ait pour mesure 1/2) conduisent au même résultat et accordent à l'ensemble des nombres entiers commençant par c la mesure $\log_{10}(1 + 1/c)$ conforme à ce que dicte la loi de Benford. On peut interpréter ces résultats comme la démonstration que la suite des entiers 1, 2, 3, ..., n , ... vérifie une forme « faible » (à la Cesàro) de la loi de Benford.

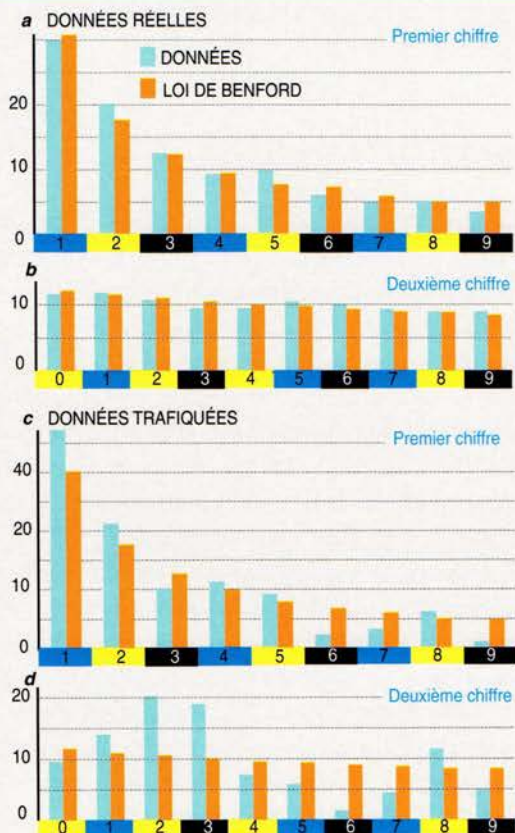
Lorsqu'on utilise ces mesures, on constate que le quotient de la densité des nombres premiers commençant par c sur la densité de tous les nombres premiers est exactement $\log_{10}(1 + 1/c)$. Les nombres premiers qui au sens de la fréquence ne suivent pas la loi de Benford (car il n'y a pas convergence de la fréquence) la vérifient donc au sens de ces mesures.

4. La détection des fraudes

L'analyse des chiffres (*digital analysis*), discipline récente, s'assure de la cohérence interne et de la vraisemblance de grandes quantités de données numériques. Elle explore systématiquement les chiffres des séries étudiées pour y repérer des anomalies de fréquence signifiant souvent que les données ont été manipulées, falsifiées ou inventées. La loi de Benford est un outil de cette discipline.

Ce type d'analyse a été utilisé avec succès par les services fiscaux américains pour repérer des fraudeurs. Récemment une étude statistique minutieuse a été menée par A. Saville sur les données fournies par 34 entreprises dont 17 étaient connues pour avoir manipulé leurs comptes. Une pure analyse des chiffres, en se limitant aux séries dont il était présumé qu'elles devaient vérifier la loi de Benford (ce n'est pas le cas de toutes les séries), a conduit à identifier les 17 entreprises classées suspectes. Le test n'est cependant pas parfait, puisque quatre autres entreprises *a priori* non suspectes ont aussi été désignées par les tests. Voir Adrian Saville, *Using Benford's Law to Detect Data Error and Fraud*, *South African Journal of Economic and Management Sciences*, 2006, pp. 341-354.

Les chercheurs ont également examiné (voir ci-contre), le premier chiffre (a et c) et le deuxième chiffre (b et d) du coefficient de corrélation de données réelles publiées dans un journal américain de sociologie (<http://ideas.repec.org/e/pdi71.html>), et de données trafiquées. La tricherie est bien visible sur le second chiffre.



Aussi merveilleux que soient ces résultats, ils ne suffisent pas à expliquer tous les cas concrets où les données statistiques sont conformes à la loi de Benford. Il faut trouver d'autres explications.

Invariances et mélanges

Les statisticiens se sont longtemps étonnés : la loi de Benford est satisfaite pour les longueurs des fleuves quand on mesure celles-ci en kilomètres, mais aussi quand on les mesure en miles ou avec n'importe quelle unité de longueur. Cette invariance par multiplication des données par une constante a été étudiée et Roger Pinkham a démontré en 1961 que la seule loi sur les mantisses invariante par multiplication (la probabilité que la mantisse de x soit comprise entre a et b est égale à la probabilité que c fois la mantisse de x soit comprise entre a et b : $\text{pr}(a < \text{mantisse}(x) < b) = \text{pr}(a < c \times \text{mantisse}(x) < b)$) est la loi de Benford.

En clair, s'il existe une loi pour les mantisses et que, comme on s'y attend, cette loi ne dépend pas des unités de mesure utilisées pour collecter les données, alors cette loi ne peut être que celle de Benford. Un résultat analogue concernant le changement de base de numération a été démontré par T. Hill en 1995. Ces deux résultats, associés à ceux sur les mesures cités plus haut, établissent de manière concordante que la seule loi envisageable pour le premier chiffre significatif est la loi de Benford et non pas la loi équitable du 1/9 que nous soufflait notre trompeuse intuition.

Même si la loi de Benford est la seule possible pour les mantisses et le premier chiffre significatif, cela ne démontre pas que pour des données réelles, c'est elle que l'on rencontrera. Une troisième catégorie de résultats nous approche de ce but.

Un théorème de T. Hill de 1996 montre qu'un bon mélange de lois quelconques – ne vérifiant pas individuellement la loi de Benford – donne des nombres vérifiant globalement la loi de Benford. Sous une forme un peu plus précise, le résultat est le suivant.

Si nous choisissons au hasard une distribution de probabilités (dans un ensemble varié de distributions ne vérifiant pas individuellement la loi de Benford), et si nous prenons un nombre selon cette distribution et que nous recommençons un grand nombre de fois cette double opération de choix, alors si le processus général de ces choix est indépendant de la base (ou des unités de mesure), la série produite vérifiera la loi de Benford.

Ce théorème expliquerait pourquoi quand on prend tous les nombres trouvés dans un journal – ils proviennent de lois variées et sans liens précis qui toutes ne vérifient pas la loi de Benford – alors on obtient un ensemble de nombres se conformant assez bien à la loi de Benford.

Pourtant, même si ce dernier résultat explique que des données mélangées satisfont la loi de Benford, il semble nécessaire aussi que des processus probabilistes simples engendrent des données numériques vérifiant la loi de Benford. On imagine alors des algorithmes élémentaires donnant des séries aléatoires conformes à la loi de Benford et on argumente que le monde réel agit comme ces algorithmes. Par exemple, si l'on choisit au hasard uniformément des nombres x entre deux entiers a et b et qu'on calcule c^x (c positif), alors la série de nombres ainsi engendrés vérifie la loi de Benford.

D'autres résultats du même genre (multiplications de nombres aléatoires entre eux, exponentielle de loi normale, etc.) décrivent des mécanismes probabilistes qui produisent des séries numériques satisfaisant la loi de Benford, au moins approximativement.

Reste cependant une insatisfaction : les processus proposés ne recouvrent pas la généralité des cas dont les données numériques vérifient la loi de Benford. On ne voit pas ainsi d'explication à ce que la table des constantes mathématiques de S. Plouffe se conforme à la loi de Benford.

Fraudes et interrogations

Même imparfaitement analysée, la loi logarithmique sur les chiffres est utilisée. Des statisticiens convaincus que, sauf cas exceptionnels, des données doivent la vérifier l'utilisent pour repérer des comptabilités truquées ou le manque de sérieux de séries statistiques économiques suspectées d'être bidonnées. Le test de la loi de Benford serait même un outil courant dans la chasse aux fraudes fiscales.

Une étude de psychologie expérimentale menée par Andrea Dickmann, de l'Institut fédéral suisse de technologie à Zurich, a validé cette méthode. Des sujets à qui on demande de créer des données fantaisistes les produisent sans respecter la loi de Benford (ou très imparfaitement) et produisent donc des données faciles à distinguer des séries réelles. Quelqu'un d'informé peut simuler des données et tromper un test fondé sur le premier chiffre significatif; en revanche, A. Dickmann montre que si l'on prend en compte le second chiffre significatif, la fraude devient si manifeste qu'aucun sujet humain ne semble en mesure d'échapper à ce repérage statistique.

La loi de Benford apparaît si importante à certains, qu'ils ont suggéré d'en tenir compte pour la conception des ordinateurs afin que ceux-ci exploitent le fait qu'ils rencontreront plus souvent des nombres commençant par 1 que par 9 (et plus généralement c que $c + 1$). Un tel ajustement de la structure des ordinateurs permettrait de mieux gérer leurs mémoires et leurs calculs qu'on ne le fait aujourd'hui, puisque nos machines sont conçues en supposant implicitement que chaque chiffre possède la probabilité $1/9$ d'apparaître comme premier chiffre significatif.

La grande question qui reste posée par la loi de Benford est finalement: est-ce nous humains ou le monde physique dans lequel nous vivons, ou une raison plus générale encore qui explique les nombreuses séries numériques s'ajustant à la loi logarithmique de Benford?

Le fait que la loi ne soit pas spécifique de la base 10, les constantes mathématiques de S. Plouffe, les théorèmes généraux d'invariance, les algorithmes probabilistes de génération et les démonstrations que des catégories importantes de suites mathématiques se conforment à la loi de Benford, tout cela nous a fait progresser. Il semble à peu près certain aujourd'hui que l'explication ultime n'est pas liée à notre façon d'examiner le monde et de le mettre en chiffres, ni à une propriété singulière de notre univers physique (et que d'autres univers physiques possibles pourraient ne pas posséder), mais résulte de principes généraux encore incomplètement identifiés et que seules les mathématiques conduiront à formuler entièrement... peut-être.

Le désordre total n'existe pas

En 1933, Esther Klein soumit un puzzle géométrique à un groupe de mathématiciens.

Il en résulta un article de Paul Erdős et George Szekeres, le mariage d'Esther Klein et de George Szekeres et... un théorème de Sárközy.

Si vous dessinez un grand nombre de points sur une feuille sans que trois d'entre eux soient alignés, alors six points délimiteront un hexagone convexe ne contenant aucun autre point (voir la figure 2). Ce « théorème de l'hexagone vide inévitable » est plus difficile à démontrer qu'on ne l'imagine à la lecture de son énoncé. C'est seulement en 2007 que, simultanément et indépendamment, Tobias Gerken, de l'Université technique de Munich, et Carlos Nicolas, de l'Université du Kentucky, en ont proposé une démonstration. Une preuve plus courte a aussitôt été découverte par Pavel Valtr de l'Université Charles à Prague.

Cet hexagone convexe vide est inévitable s'il y a un nombre assez grand de points. Mais combien exactement ? On sait que 29 points ne suffisent pas à garantir l'hexagone vide (résultat dû à Mark Overmars de l'Université d'Utrecht) et que 463 suffisent (démontré en 2007 par Vitaliy Koshlev de l'Université indépendante de Moscou). Il est difficile d'être plus précis et le défi est ouvert à tous, y compris aux amateurs de programmation qui feront progresser nos connaissances s'ils trouvent des ensembles de plus de 29 points non alignés sans hexagone convexe vide.

Les démonstrations du théorème de l'hexagone vide s'appuient sur les solutions d'un problème géométrique de la même catégorie, nommé par Paul Erdős *Problème à l'heureuse issue* de par son histoire. À Budapest en 1933, Erdős et quelques étudiants(es) se réunissaient régulièrement pour parler de mathématiques et d'autres sujets. Esther Klein proposa un jour une énigme :

Montrez que si cinq points sont placés de manière quelconque sur un plan (c'est-à-dire sans que trois d'entre eux soient alignés) alors il y en a quatre qui forment les sommets d'un quadrilatère convexe.



Permission from "The Mathematical Coloring Book" by Alexander Sotir, Springer, 2009. Copyrights reserved.

1 George Szekeres et Esther Klein, mariés en 1937 après la démonstration du « problème à l'heureuse issue ». En médaillon, leur ami et collègue, Paul Erdős, à 17 ans ; quatre ans après, Erdős sera docteur en mathématiques.

Erdős et George Szekeres écoutèrent la solution d'Esther Klein, mais n'en restèrent pas là et, un an plus tard, généralisèrent et publièrent la propriété suivante: quand on dessine suffisamment de points sur un plan sans en aligner trois, on y trouve les sommets d'un quadrilatère convexe, avec plus de points, on est certain de trouver un pentagone convexe, puis, avec un peu plus de points encore, un hexagone convexe, etc.

La formulation mathématique est:

Pour tout entier n donné, il existe un entier N , tel que tout ensemble de N points ou plus placés sur le plan en position quelconque (c'est-à-dire sans que trois points soient alignés) contient un sous-ensemble de n points déterminant les sommets d'un polygone convexe (pouvant contenir d'autres points).

Géométrie et mariage

Le plus petit entier qui garantit la présence des sommets d'un polygone convexe à n côtés est noté $g(n)$. Il est immédiat que $g(3)=3$. Esther Klein avait montré que $g(4)=5$. On sait aussi que $g(5)=9$ (résultat dû à E. Makai) et que $g(6)=17$ (résultat dû à Szekeres et L. Peters). Au-delà, on ne connaît pas les valeurs de $g(n)$. Erdős et Szekeres prouvèrent cependant que: $g(n) \geq 1+2^{n-2}$. On sait aujourd'hui que $g(n) \leq C(2n-5, n-3)$, où la notation $C(n, k)$ désigne le coefficient du binôme $n!/(k!(n-k)!)$.

Les premières valeurs de $g(n)$ suggèrent que, pour tout n à partir de 3, $g(n)$ vaut exactement $1+2^{n-2}$, mais c'est là une conjecture qui semble d'une extrême difficulté: personne n'a su la démontrer. Erdős avait l'habitude de proposer des récompenses pour les conjectures qui l'intéressaient: plus une conjecture lui semblait difficile, plus la somme offerte était importante. Erdős avait promis de payer 500 dollars pour la démonstration de $g(n) = 1+2^{n-2}$.

Erdős, mort en 1996, ne paiera donc jamais ces 500 dollars, mais soyez rassuré: Ronald Graham a pris la relève et il promet 1 000 dollars pour cette preuve (ou la preuve que pour certaines valeurs de n la formule n'est pas exacte).

Le minimum d'ordre

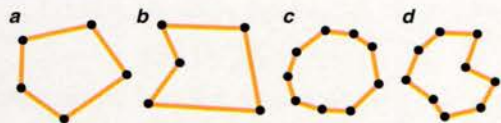
Le théorème de Erdős et Szekeres qui affirme l'existence de $g(n)$ et la conjecture associée aux valeurs de $g(n)$ sont intéressants car, à chaque fois, il s'agit d'affirmations signifiant qu'un minimum d'ordre est inévitable. Il est naturel de considérer que n points disposés pour former les sommets d'un polygone convexe constituent un îlot organisé dans un ensemble de points, car un tel ensemble constitue une sorte de groupement circulaire de n points. Le théorème de Erdős et Szekeres affirme que de tels îlots d'ordre sont inévitables dès que le nombre de points est assez grand et que plus le nombre de points envisagés est grand, plus on trouve de grands regroupements circulaires de points.

Erdős donna le nom de « problème à l'heureuse issue » (*Happy ending problem*) à l'énigme pour $n = 4$ car, en 1937, Esther Klein et Szekeres se marièrent et la légende veut que le problème soumis au groupe de 1933 ait été un élément déterminant de leur histoire. Ils vécurent ensemble jusqu'au 28 août 2005, date à laquelle ils décédèrent tous les deux à une demi-heure d'intervalle. Doit-on considérer qu'il s'agit, là encore, d'une « heureuse issue »?

L'histoire ne sera d'ailleurs pas terminée tant qu'on n'aura pas réussi à obtenir plus de précision concernant $g(n)$, d'autant que des généralisations en dimensions supérieures à 2

2. Les polygones inévitables

1. Polygone convexe. Un ensemble de n points du plan détermine un polygone convexe de n points si, par définition, en rejoignant bien les points, on obtient une forme sans creux.



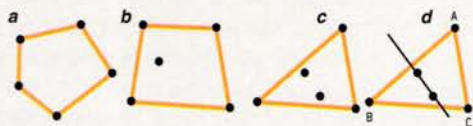
Cinq points déterminent un pentagone convexe (a) ou non convexe (b), neuf points déterminent un enneagone convexe (c) ou non convexe (d).

2. Le problème à l'heureuse issue. Le « problème à l'heureuse issue » est de montrer que si cinq points sont donnés sur le plan en position quelconque (c'est-à-dire sans qu'il y en ait trois d'alignés) alors quatre d'entre eux déterminent un quadrilatère convexe.

La démonstration procède en distinguant trois cas.

1. Les cinq points déterminent un pentagone convexe (a). Dans ce cas, quatre d'entre eux, quels qu'ils soient, déterminent un quadrilatère convexe.

2. Le plus petit polygone convexe qui contient les cinq points (nommé enveloppe convexe des cinq points) est un quadrilatère (b). Alors, les quatre sommets de ce quadrilatère-enveloppe constituent le quadrilatère convexe recherché.



Notons que pour obtenir l'enveloppe convexe de n points, un excellent dispositif analogique consiste à planter des clous sur les n points et à placer un élastique autour de ces points.

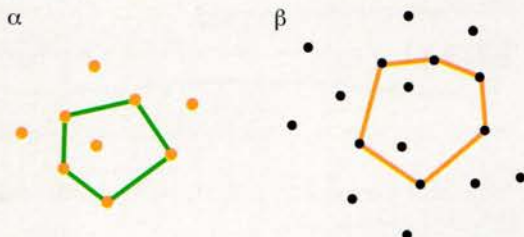


3. Le plus petit polygone qui contient les cinq points est un triangle (c). Alors, la droite déterminée par les deux points qui ne sont pas des sommets de ce triangle ABC coupe deux côtés du triangle, AB et BC (d). Les deux points intérieurs et les deux points A et C sont les sommets du quadrilatère convexe recherché.

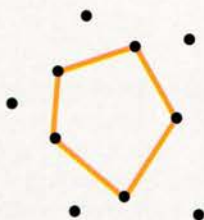
3. Le polygone convexe inévitable. En plaçant N points (ici N est égal à 9) sur le plan en position quelconque (sans que trois d'entre eux soient alignés) alors on

est certain de trouver parmi eux cinq points déterminant un pentagone convexe (α).

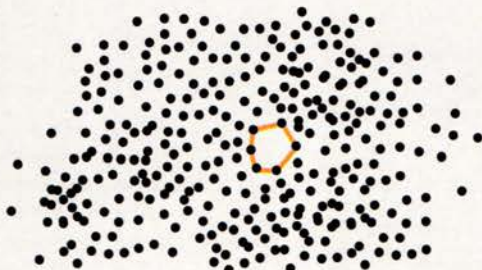
En plaçant 17 points sur le plan en position quelconque (sans que trois d'entre eux soient alignés) alors on est certain de trouver parmi eux six points déterminant un hexagone convexe (β). Plus généralement, le théorème de Erdős-Szekeres de 1935 indique que pour tout entier n , il existe un entier N , tel que N points en position quelconque sur le plan contiennent nécessairement un sous-ensemble de n points déterminant les sommets d'un polygone convexe à n côtés.



4. Le pentagone vide et l'hexagone vide. Si l'on dispose plus de 10 points en position quelconque sur le plan, alors on est certain de trouver parmi eux cinq points déterminant un pentagone convexe qui ne contiendra aucun autre point.



On vient tout juste de démontrer que si on dispose plus de 463 points en position quelconque sur le plan, alors on est certain de trouver parmi eux six points déterminant un hexagone convexe qui ne contiendra aucun autre point. C'est le théorème de l'hexagone convexe vide.



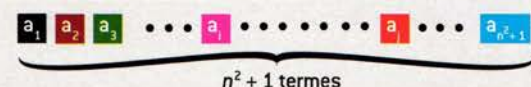
Le nombre 463 peut certainement être réduit, mais pour l'instant personne ne sait comment s'y prendre.

3. Le théorème des sous-suites monotones

Parmi les résultats démontrés par Erdős (photo page ci-contre) et Szekeres dans leur article de 1935, un théorème indique qu'un minimum d'ordre existe dans toute suite numérique (c'est un théorème « à la Ramsey ») : *De toute suite de $n^2 + 1$ nombres différents, on peut extraire une sous-suite croissante de longueur $n + 1$ ou une sous-suite décroissante de longueur $n + 1$.*

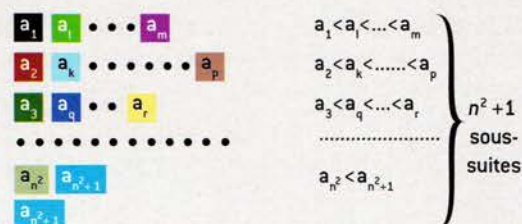
En particulier, dans toute suite de 10 nombres, on trouve obligatoirement une suite de 4 nombres croissants ou décroissants. Cherchez pour (31, 30, 53, 12, 27, 11, 66, 21, 87, 32).

Voici la démonstration du théorème.



Prenons une suite de nombres différents de longueur $n^2 + 1$.

Pour chaque a_i , considérons la plus longue sous-suite croissante qui commence par a_i .



Si l'une de ces sous-suites a plus de n éléments, notre raisonnement est terminé. Nous supposons donc que chacune de ces sous-suites a une longueur inférieure ou égale à n . Puisqu'il y a $n^2 + 1$ nombres, nous disposons de $n^2 + 1$ sous-suites croissantes différentes (chacune commence par un nombre différent).

Classons toutes ces sous-suites par taille: celles de taille 1,

Suites de longueur 1



Suites de longueur 2



Suites de longueur j



Pour la longueur j , plus grand nombre p de suites

$n^2 + 1$ suites et n séries de suites de longueur $1, 2, 3, \dots, j, \dots, n$

celles de taille 2, etc., jusqu'à celles de taille n . Pour au moins un entier j entre 1 et n , le nombre de sous-suites de taille j est plus grand que n (sinon le nombre total de sous-suites serait inférieur ou égal à n^2 , or il y en a $n^2 + 1$). Soit j cette taille et $p > n$ le nombre de sous-suites croissantes de taille j .



Considérons le premier élément de chacune des sous-suites de taille j . Cela nous donne p entiers différents pris dans la suite initiale. Nous les classons comme dans la suite initiale pour obtenir une sous-suite de la suite initiale de longueur p .



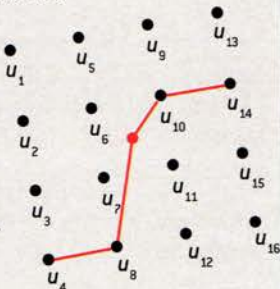
Notons $b_1, b_2, \dots, b_p$ cette sous-suite et montrons qu'elle est décroissante. Comme elle possède p éléments avec $p > n$, cela terminera la démonstration.

Si $b_1 < b_2$ alors la sous-suite croissante, commençant par le nombre b_1 et se poursuivant par les p éléments de la sous-suite croissante qui commence à b_2 et a pour longueur j (elle existe par définition), serait une sous-suite de longueur $j + 1$ commençant à b_1 . Or une telle suite ne peut exister puisque par définition la sous-suite croissante la plus longue qui commence à b_1 a pour longueur j . Donc $b_1 > b_2$. De même $b_2 > b_3 > b_4 > \dots > b_p$, ce que nous voulions établir.

Une question naturelle se pose: peut-on améliorer le $n^2 + 1$ et le remplacer par un nombre plus petit? La réponse est non et un simple dessin permet de comprendre pourquoi. En considérant les ordonnées des 17 points, de celui le plus à gauche, u_1 , vers celui le plus à droite, u_{16} , et en incluant entre u_8 et u_9 le point rouge, on obtient une suite de 17 nombres différents. Comme le théorème l'indique, on extrait sans mal une suite monotone croissante de longueur 5 de cette suite de 17 nombres. Une telle suite est représentée graphiquement ci-dessous par un tracé montant passant par 5 points (il y a d'autres tracés montant ou descendant de 5 points).

Si l'on enlève le point central, on constate qu'aucun tracé montant ou descendant de 5 points n'est plus possible, ce qui signifie que les ordonnées des 16 points pris de gauche à droite constituent une suite de

nombres différents dont on ne peut extraire aucune sous-suite croissante ou décroissante de longueur 5. Ce schéma se généralise évidemment pour tout n : il est donc impossible d'améliorer le $n^2 + 1$ du théorème des sous-suites monotones.



ont été proposées et que ces généralisations sont accompagnées de conjectures sur les valeurs exactes des fonctions $g(n)$ associées.

Notons aussi que dans l'article de 1935 qui établit que $g(n)$ existe toujours, Erdős et Szekeres utilisent et redémontrent le théorème de Ramsey qui venait à peine d'être découvert. Ce théorème de Ramsey, dont Erdős explorera les variantes et les généralisations tout le reste de sa vie, est l'expression dans le cas des graphes de l'affirmation qu'un peu d'ordre est inévitable. Toujours dans l'article publié en 1935 et après la démonstration de l'existence de $g(n)$, Erdős et Szekeres envisageaient un autre problème géométrique du même type. Est-il vrai que :

Pour tout entier n , il existe un entier N , tel que si N points ou plus sont placés en position quelconque sur un plan, alors n d'entre eux délimitent un polygone convexe ne contenant pas de point.

Il est évident que 3 points assurent un triangle vide. La solution du problème d'Es-ther Klein s'adapte à 5 points qui assurent un quadrilatère convexe vide. Heiko Harborth a prouvé que 10 points assurent un pentagone convexe vide.



Erdős (buste de Gabriella Bollobás).

Les structures vides

Là encore, une interprétation en termes d'ordre minimum s'impose. Un quadrilatère convexe vide, un pentagone convexe vide, un hexagone convexe vide, etc., plus encore qu'un quadrilatère convexe, un pentagone convexe, un hexagone convexe, etc., sont des structures organisées. La question posée est alors :

Un nombre assez grand de points assure-t-il la présence de ces structures organisées ?

Le cas des valeurs de n à partir de 7 constitue une salubre mise en garde à ne pas énoncer un principe trop général concernant « l'inévitable présence de l'ordre ». Joseph Horton a en effet établi en 1983 que pour tout N , aussi grand soit-il, il existe des ensembles de N points ne contenant aucun heptagone convexe vide et donc aucun octogone convexe vide, etc. Certaines structures sont inévitables, pas toutes !

Restait à résoudre le cas $n = 6$ de l'hexagone convexe vide : assez de points en position quelconque assurent-ils la présence d'un hexagone convexe vide, oui ou non ? Cela vient d'être démontré, comme nous l'indiquions dans les premières lignes de ce chapitre.

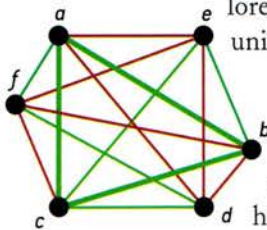
Les démonstrations s'appuient sur le fait que certains polygones convexes sont inévitables et procèdent par une analyse combinatoire délicate où une multitude de cas soigneusement énumérés et examinés amènent à la conclusion. Toutefois, aucune démonstration courte et directe n'a encore été proposée ! Le théorème de l'hexagone vide est l'une de ces petites merveilles mathématiques auxquelles aucune voie rapide ne semble donner accès. La présence de certaines sous-structures organisées dans les objets mathématiques assez gros (ensembles de points, graphes, suites numériques, ensembles de nombres entiers, etc.) est une propriété remarquable dont nous allons donner d'autres exemples.

Précisons que ces résultats « de type Ramsey » n'affirment pas seulement des certitudes probabilistes, mais des certitudes absolues. On sait que si une suite de tirages à pile ou face effectués avec une pièce non truquée est poursuivie assez longtemps, elle finit nécessairement par produire 10 fois pile consécutivement.

Le « nécessairement » de la phrase précédente est un « nécessairement » probabiliste. Il se peut qu'on n'obtienne jamais 10 fois pile consécutivement. Dans le langage des probabilités, on dit que 10 fois de suite pile est « presque sûr ». Les résultats de type

Le résultat le plus célèbre de présence certaine d'un ordre dans un grand objet mathématique et qui donne son nom à cette catégorie de théorèmes est celui démontré en 1928 par Frank Ramsey (1903-1930) sur les graphes bicolores. Un graphe bicolore complet de N points est un graphe ayant N sommets et tel que tout couple de sommets $a-b$ est joint par un arc coloré en brun ou en vert. Un sous-graphe unicolore de taille n est un sous-ensemble de n sommets du graphe tel que tous les arcs reliant ses n sommets sont de la même couleur (tous bruns, ou tous verts).

On sait que $R(3) = 6$: ainsi, dans toute assemblée de six personnes, il y a au moins trois personnes a, b, c qui se connaissent entre elles ou trois personnes qui ne se connaissent pas. Ce fait correspond à l'impossibilité géométrique de colorier avec deux couleurs les arcs d'un graphe reliant deux à deux les sommets d'un hexagone sans former un triangle dont les côtés sont de la même couleur.



On a prouvé que $R(4) = 18$. On sait que $R(5)$ est compris entre 43 et 49 et que $R(6)$ est compris entre 102 et 165. Le calcul des $R(n)$ est si difficile que Erdős racontait l'histoire suivante :

« Imaginons que des extraterrestres bien plus puissants que nous arrivent sur Terre et nous demandent la valeur de $R(5)$ sous la menace d'une destruction totale de la planète. Dans ce cas, nous devrions enrôler tous nos ordinateurs et tous nos mathématiciens pour calculer cette valeur. En revanche, s'ils nous demandaient $R(6)$, il faudrait alors tenter de détruire les extraterrestres. »

La fonction qui à n associe $R(n)$ est une fonction très rapidement croissante et certaines variantes du théorème de Ramsey ont permis la définition de fonctions si rapidement croissantes que les méthodes de l'arithmétique élémentaire ne sont plus assez puissantes pour démontrer ces variantes. L'une de ces variantes, formulée en 1977 par Jeff Paris et Leo Harrington, a été le premier théorème d'arithmétique non tiré de la logique mathématique dont on a pu établir qu'il était indécidable dans l'arithmétique de Peano.

La version infinie du théorème de Ramsey est le beau et très simple résultat suivant. Si G est un graphe dont les sommets sont les entiers, alors on peut trouver un sous-ensemble infini d'entiers tel qu'il y ait un arc entre deux quelconques de ces entiers, ou tel qu'il n'y ait aucun arc entre les nœuds correspondant à ces entiers.

Ramsey, mort très jeune, n'a jamais soupçonné l'importance que prendrait son résultat, à l'origine d'un domaine foisonnant de recherche très loin d'être épuisé aujourd'hui. Ramsey n'avait proposé son théorème que comme résultat intermédiaire pour prouver un théorème de logique mathématique qui n'intéresse plus personne aujourd'hui!

Les ensembles de points et les graphes ne sont pas les seules structures mathématiques à connaître des inévitables îlots d'ordre. Le théorème suivant, lui aussi démontré par Erdős et Szekeres, concerne les suites de nombres, et indique qu'on peut toujours

extraire des sous-suites monotones, c'est-à-dire croissantes ou décroissantes (voir la figure 3). La version infinie de ce résultat, que l'on déduit du théorème de Ramsey infini cité plus haut, affirme que de toute suite infinie de nombres différents, on peut extraire une sous-suite infinie croissante ou une sous-suite infinie décroissante.

Les suites numériques aussi

Certains résultats considérés comme appartenant à la théorie de Ramsey ont été démontrés avant que Ramsey formule son théorème! Celui de Van der Waerden (1903-1996) démontré en 1927 est remarquable: il indique que tout coloriage des entiers avec deux couleurs contient des progressions arithmétiques de nombres d'une même couleur aussi longue qu'on le veut. Sa version finie stipule que pour tout n , il existe un entier $W(n)$ tel que tout coloriage en deux couleurs des entiers de 1 à $W(n)$ contient un sous-ensemble de n entiers de la même couleur en progression arithmétique.

On sait par exemple que $W(3) = 9$. D'une part, le coloriage 1 2 3 4 5 6 7 8 montre que $W(3) > 8$ (jamais trois nombres en progression arithmétique ne sont de la même couleur pour ce coloriage). D'autre part, en essayant tous les coloriages bicolores possibles des entiers de 1 à 9 (il y en a 512), on vérifie que tous ont trois nombres de la même couleur en progression arithmétique.

La fonction $W(n)$, comme précédemment la fonction $g(n)$, est l'objet d'une attention soutenue de la part des mathématiciens. On formule des conjectures à son sujet et des récompenses sont parfois proposées (et remportées!). Ron Graham, le grand spécialiste de la théorie de Ramsey, avait ainsi promis 1 000 dollars à celui qui établirait que :

$$W(n) < 2^{2^{\cdot^{\cdot^{\cdot^2}}}} \text{ } n \text{ fois}$$

4. Un théorème de András Sárközy

Les théorèmes affirmant que la présence d'ordre (au moins en petite quantité) est assurée, et dont le théorème de Ramsey est le prototype, se retrouvent dans de nombreux domaines des mathématiques. Le théorème de András Sárközy illustre l'ordre inévitable en arithmétique.

Voyons d'abord un exemple. Prenons la suite des nombres de 1 à 5: {1, 2, 3, 4, 5}. Formons des sous-ensembles A , en prenant pour chacun trois éléments (on dit qu'on a choisi une densité e un peu supérieure à $1/2$) de cette suite. Alors il y a dans tout sous-ensemble A deux nombres dont la différence est un carré (notez que 1 est un carré, le carré de 1). Vérifions avec les dix sous-ensembles {1, 2, 3}, {1, 2, 4}, {1, 2, 5}, {1, 3, 4}, {1, 3, 5}, {1, 4, 5}, {2, 3, 4}, {2, 3, 5}, {2, 4, 5}, {3, 4, 5}.

Un peu plus généralement, si un sous-ensemble A de {1, 2, ..., N } avec $N > 8$ a une densité supérieure ou égale à $1/2$, alors il contient deux nombres dont la différence est un carré.

En effet, soit A contient deux nombres consécutifs dont la différence (1) est un carré et la propriété est vraie. Soit A ne

contient pas deux entiers consécutifs; puisque sa densité est supérieure ou égale à $1/2$ et que N est strictement supérieur à 8, il contient 3 nombres pairs ou 3 nombres impairs consécutifs, et donc contient deux nombres espacés de 4 qui est un carré.

Plus généralement, le théorème de A. Sárközy stipule que, pour toute densité e positive, aussi petite soit-elle, il existe un entier N_0 tel que tous les sous-ensembles A de densité supérieure à e pris dans {1, ..., N } où $N > N_0$ contiennent deux nombres dont la différence est un carré.

A. Sárközy (photographie) est professeur de mathématiques à l'Université Eötvös-Lorand de Budapest. Il a écrit 62 articles avec Erdős, ce qui est le record.



Il a dû s'acquitter de cette somme à Timothy Gowers qui prouva en 2001 que :

$$W(n) < 2^{2^{2^{2^{n+9}}}}$$

R. Graham, beau joueur, propose maintenant 1 000 dollars à celui qui démontrera :

$$W(n) < 2^{n^2}$$

En arithmétique, la présence inévitable d'ordre peut s'exprimer de nombreuses façons. Le théorème de Sárközy (ou théorème de Sárközy-Furstenberg) a été démontré en 1977 simultanément et indépendamment par le mathématicien hongrois András Sárközy et par le mathématicien israélien Hillel Furstenberg (voir l'encadré 4). En voici l'énoncé qu'il faut apprendre soigneusement pour le réciter correctement à vos amis ébahis :

Pour tout nombre réel $\epsilon > 0$, il existe un entier N_0 , tel que si $N > N_0$ et si A est un sous-ensemble de $\{1, 2, \dots, N\}$ ayant un nombre d'éléments au moins égal à ϵN , alors A contient deux éléments dont la différence est un carré parfait.

Ces résultats affirmant la présence d'îlots organisés inévitables sont parfois interprétés avec excès : contrediraient-ils la théorie de la complexité de Kolmogorov, selon laquelle l'ordre est exceptionnel ? Qu'en est-il ?

Ordre et complexité

La théorie de la complexité de Kolmogorov mesure l'ordre par le taux de compression. La taille du plus petit programme qui permet d'engendrer une suite finie s de 0 et de 1 est la complexité de Kolmogorov de cette suite, notée $K(s)$. Une affirmation de base de la théorie est qu'une suite prise au hasard, sauf cas exceptionnel, n'est pas compressible ou très peu compressible. Un simple argument de décompte montre précisément qu'une suite sur mille au plus parmi toutes les suites de n bits peut être représentée par un fichier de taille inférieure à $n - 10$ (et plus généralement qu'une suite sur 2^k parmi toutes les suites de longueur n , peut être compressée de plus de k bits).

De tels résultats signifient que l'ordre est rare et qu'on ne le trouve pas systématiquement. Cependant, ils ne contredisent pas les multiples théorèmes de la théorie de Ramsey dont nous avons donné quelques exemples. En effet, les théorèmes de type Ramsey affirment que dans toute structure assez grande, certaines sous-structures organisées sont nécessairement présentes. Cependant, dans chaque cas particulier, le rapport entre la taille de la sous-structure organisée inévitable et la taille de l'objet mathématique où on la trouve tend vers zéro.

Les îlots d'ordre sont obligatoires, mais de plus en plus petits, d'où d'ailleurs les fonctions rapidement croissantes que nous mentionnions, et donc leur présence ne contredit en rien le côté exceptionnel des structures globalement organisées affirmé par la théorie de Kolmogorov.

De l'ordre, oui il y en a nécessairement en petite quantité, c'est ce que dit la théorie de Ramsey, mais cet ordre est rare et localisé : les grandes structures possédant une organisation globale (donc une faible complexité de Kolmogorov) sont rarissimes.

Pierre, feuille, ciseaux

Joué comme un jeu de conquête, l'ancien jeu chinois de la pierre, de la feuille et des ciseaux éclaire les phénomènes de synchronisation et la logique du maintien de la diversité animale.

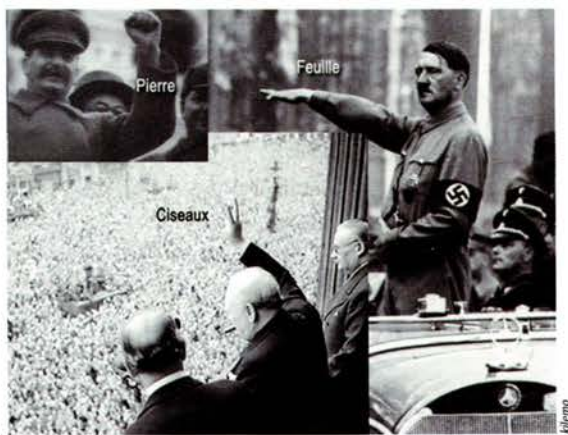
Les mathématiciens sont comme les Français: quoi que vous leur disiez, ils le traduisent dans leur propre langue et le transforment en quelque chose de totalement différent.

Goethe

Et de très intéressant... aurait dû ajouter Goethe: ainsi, les mathématiciens ont transformé un jeu d'enfants, Pierre-feuille-ciseaux, en un riche modèle des interactions animales. Qui n'a joué à ce jeu? La pierre (P) casse les ciseaux, les ciseaux (C) découpent la feuille et la feuille (F) enveloppe la pierre. Deux joueurs placent chacun leur main droite dans le dos et choisissent l'un des trois symboles: le poing fermé pour la pierre, la main allongée pour la feuille, deux doigts en forme de ciseaux. Les deux joueurs dévoilent leur choix en avançant la main, parfois en proférant un cri. Si les deux choix sont identiques, ils recommencent, sinon le joueur qui détient le symbole le plus fort des deux a gagné le coup.

Le jeu est ancien et l'on en trouve des traces en Chine dès l'époque Ming (1368-1644). Il est connu dans le monde entier et ses variantes sont innombrables. On y joue avec un plus grand nombre de symboles, on ajoute le puits, le feu, l'eau, etc., ou alors avec d'autres triplets. Dans une version japonaise, les trois symboles sont le guerrier, le tigre et la mère du guerrier. Il y a aussi le feu, le serpent et l'eau, ou encore le serpent, la grenouille et la limace.

Parmi les stratégies du type «jouer P avec la probabilité x , jouer F avec la probabilité y , jouer C avec la probabilité z », nommées *stratégies mixtes*, la stratégie correspondant aux coefficients $x = y = z = 1/3$ est imbattable: si vous l'adoptez, tout joueur sera, à la longue, *ex aequo* avec vous; il ne pourra ni vous battre... ni même perdre s'il le souhaitait. Cette stratégie ne résoudra pourtant pas toutes les questions que pose le jeu. D'une part, un être humain est incapable d'engendrer dans sa tête des choix vraiment aléatoires avec des probabilités fixées à l'avance: celui qui souhaite jouer la stratégie mixte 1/3-1/3-1/3 ne le peut pas! D'autre part, les joueurs humains utilisent l'information sur les coups déjà joués: ils ne peuvent pas s'en empêcher même s'ils essayent. Le jeu est en partie psychologique et il y a parfois mieux à faire que





1 Pierre-feuille-ciseaux est pratiqué sous divers noms : Janken ou Yakyuken au Japon, Kawi-Bawi-Bo en Corée, Jack-En-Poy ou Bato-Bato-Pick aux Philippines, Ko-papír-ollo en Hongrie, etc. Le vainqueur du championnat du monde en 2007 fut l'Américaine Andrea Farina (à gauche). Le jeu, s'il n'est joué qu'une seule fois, est une forme de tirage au sort. Aussi, en 2005, le président de la *Maspro Denkoh Corporation* Takashi Hashiyama, qui ne réussissait pas à choisir si la collection d'œuvres de sa compagnie (comportant des tableaux de Cézanne, Van Gogh et, de Picasso, *Le boulevard de Clichy*, à droite) devait être vendue par Chris-



tie's ou Sotheby's, organisa une séance de jeu pour fixer sa décision. Les représentants à Tokyo des deux salles des ventes furent conviés à jouer à *Pierre-feuille-ciseaux*. Christie's gagna : il avait choisi les ciseaux alors que Sotheby's avait opté pour la feuille ! (Pour plus de détails voir le *New York Times* du 29 avril 2005 : <http://www.nytimes.com/2005/04/29/arts/design/29scis.html>). De toutes les parties de *Pierre-feuille-ciseaux*, c'est sans doute celle à l'enjeu le plus important : la vente portait sur une somme de plus de dix millions de dollars dont plus de 12 pour cent sont revenus à Christie's.

la stratégie 1/3-1/3-1/3. Si, par exemple, vous remarquez que votre adversaire n'utilise pas P, alors en jouant invariablement C vous gagnerez toujours (s'il joue F, vous gagnez, s'il joue C, le coup est nul). Bien sûr, il risque de s'apercevoir de votre tactique et de se mettre à jouer P, ce qui vous perdra !

Certains logiciels jouent mieux que les êtres humains, car en repérant les régularités qu'ils adoptent (même quand ils font tout pour ne pas être réguliers), leur attitude donne un léger avantage à une machine attentive et bien programmée. Le programme *Sagace* de Christophe Meyer exploite ainsi les faiblesses humaines.

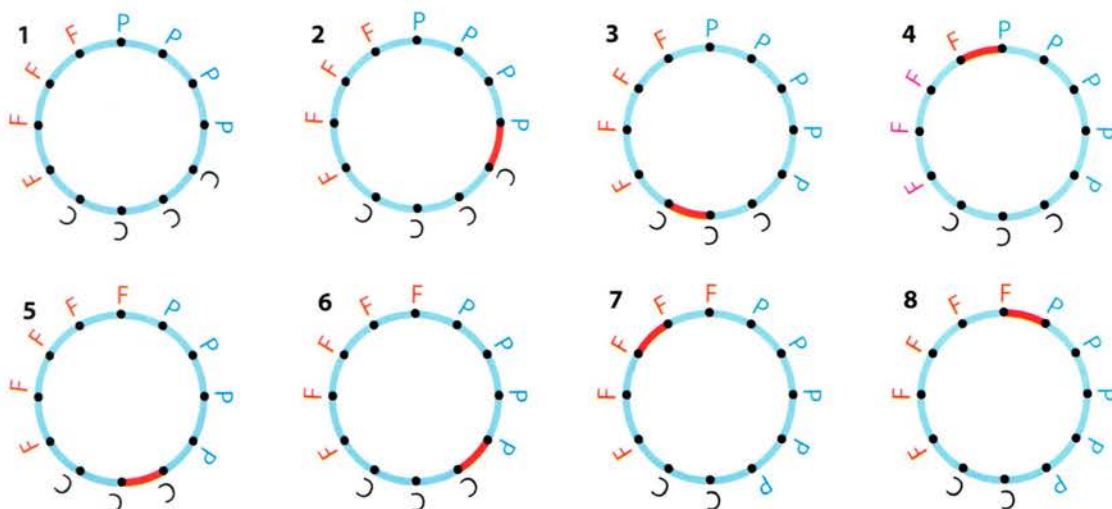
Comme nous allons le voir dans la suite de ce chapitre, joué sur un graphe, le jeu en apparence simple engendre des comportements collectifs inattendus et délicats à élucider. Certains mécanismes découverts lors de récentes études expliquent les phénomènes de synchronisation et d'uniformisation et éclairent le maintien de la diversité dans le monde biologique.

Dans le jeu sur un graphe, un ensemble de points est fixé, les nœuds du graphe. Sur chacun est placé un symbole de type P (pierre), F (feuille) ou C (ciseaux). Certains couples de points sont reliés par les *arcs* du graphe.

Les règles du combat

Cette disposition constitue la configuration initiale dont l'évolution se fait selon un processus aléatoire : un nœud N est choisi au hasard équitablement (chaque nœud a la même probabilité d'être choisi) parmi tous les nœuds et un nœud N' directement relié à N est choisi au hasard équitablement aussi. Si les deux symboles portés par N et N' sont de même force, rien ne se produit, sinon le plus faible des deux symboles est remplacé par le plus fort qui occupe alors les deux nœuds N et N'. On recommence, en choisissant un nouveau nœud au hasard, etc. Les combats successifs permettent au gagnant de chaque rencontre d'occuper le terrain de l'adversaire. Ce processus d'évolution est répété un très grand nombre de fois (*voir un exemple sur la figure 2*).

Dans cet exemple, le combat revient à choisir au hasard deux nœuds voisins de l'anneau, ce qui conduit soit au *statu quo* si les nœuds portent le même symbole, soit à un gain de territoire pour le plus fort. Si tout s'équilibrait, les zones ne feraient que se déplacer, chacune gardant en moyenne quatre éléments et tournant dans le sens des aiguilles d'une montre. Cependant, les tirages au sort des combats ne donnent pas des résultats parfaitement réguliers : les tailles des zones tenues par les C, les P et les F fluctuent et ces fluctuations s'amplifient. Inévitablement, l'une des trois zones disparaît, ce qui



2 Le jeu sur un anneau. Un anneau est composé de 12 nœuds chacun lié à ses deux voisins. Au départ, on place quatre P, quatre C et quatre F. Le jeu consiste à tirer au hasard un arc liant deux nœuds, puis à faire jouer l'un contre l'autre les deux symboles (F l'emporte sur P, P l'emporte sur C et C l'emporte sur F). Le symbole qui gagne occupe alors les deux nœuds. Selon le hasard qui fait jouer

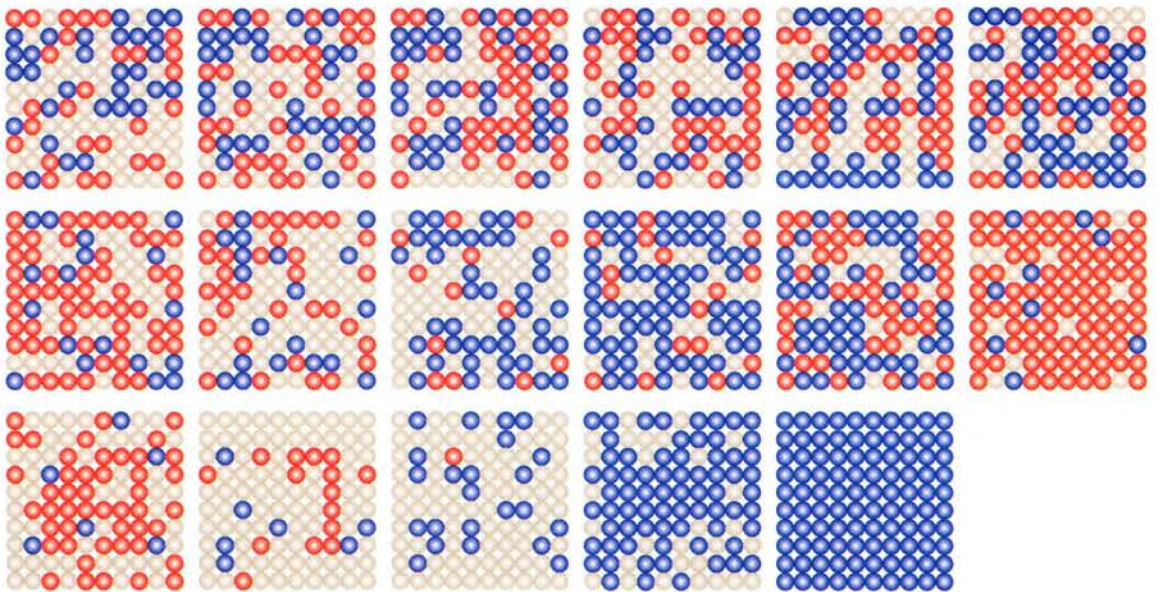
ainsi les nœuds les uns contre les autres, soit le jeu préserve la variété, les trois symboles coexistant toujours, soit l'un des symboles finit par disparaître, ce qui entraîne la disparition d'un second symbole, tout l'anneau étant alors occupé par un symbole unique et inamovible [cette occupation unique devient quasi certaine quand le nombre de tirages d'arcs tend vers l'infini].

entraîne la disparition d'une deuxième zone et il ne reste plus qu'un seul symbole sur tout le terrain. Si la zone qui disparaît en premier est celle des C, les F envahissent tout; si la zone des P disparaît, les C envahissent l'anneau et si les F disparaissent, les P dominent totalement et définitivement.

Dans le cas d'une configuration initiale irrégulière de C, de F et de P sur un anneau (même beaucoup plus grand) qu'on remplit en tirant au hasard les emplacements des C, des F et des P, l'évolution est de même type. Les déplacements de frontières des différentes zones homogènes amènent assez rapidement une configuration uniforme.

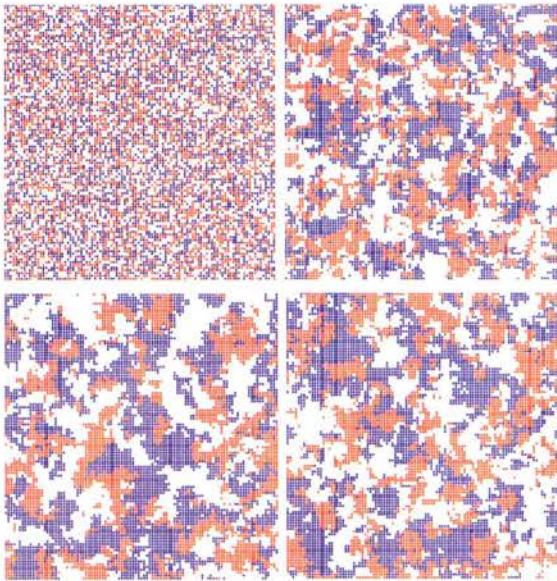
Cette évolution à long terme vers un gagnant définitif (imprévisible) est bien plus générale et se produit pour tout graphe connexe (un graphe connexe est un graphe d'un seul tenant, c'est-à-dire tel que deux nœuds sont toujours reliés par au moins un chemin). Le résultat dont la démonstration est exposée page 86 est: « Pour tout graphe connexe et toute configuration initiale de *pierres*, de *feuilles* et de *ciseaux* sur le graphe, la probabilité pour que le système se retrouve au bout d'un temps fini dans un état uniforme (l'un des symboles occupant tous les nœuds) est de 100 pour cent. »

Notons que cela n'interdit pas qu'il existe des suites de tirages particuliers assurant le maintien indéfini des trois symboles sur le graphe (tout comme si vous lancez un dé, vous pouvez obtenir une série ne comportant que des 6). Si l'on considère le graphe circulaire envisagé plus haut et que les arcs sont tirés les uns après les autres en tournant dans le sens des aiguilles d'une montre, il restera toujours des exemplaires des trois symboles. Le sens du

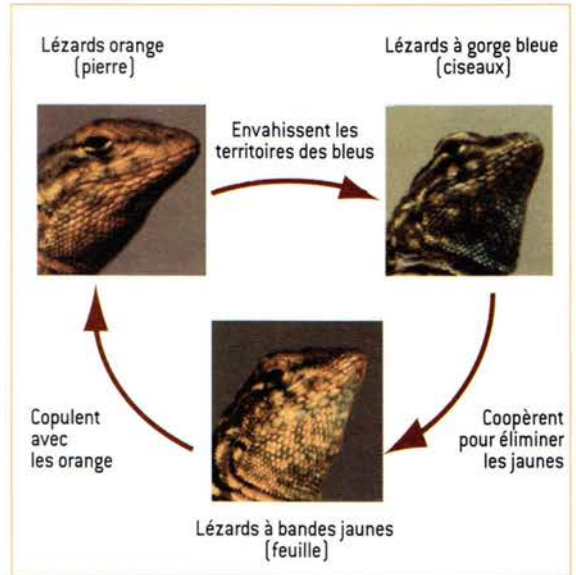


3 Le jeu sur un graphe complet (où chaque nœud est relié à chaque autre). Pour visualiser l'évolution, on représente le graphe comme si les nœuds étaient disposés sur un damier. On part d'une configuration aléatoire des trois symboles *Pierre*, *feuille*, *ciseaux* (on utilise pour chacun une couleur, rouge, blanc ou bleu). On représente l'évolution en dessinant le graphe toutes les 100 étapes (100 combats). Dans un premier temps, le graphe reste à peu près homogène avec 33 pour cent de

chacun des symboles. Au bout de dix étapes (donc 1 000 combats sur un arc), la couleur bleue domine. Deux cents combats plus tard, le rouge domine. Puis c'est le blanc, puis le bleu, cette fois définitivement. Dans le cas de graphes de taille plus grande, la phase d'uniformisation partielle avec domination cyclique d'un symbole dure plus longtemps avant la victoire définitive d'un des symboles. Les simulations de cette figure ont été réalisées par Rémi Dorat.



4 Le jeu sur un graphe-damier où chaque case du damier n'est liée qu'à ses huit voisines. Au départ, le damier est rempli aléatoirement par les trois symboles *Pierre*, *feuille*, *ciseaux*. L'évolution fait apparaître des zones homogènes, qui se déplacent tout en gardant une taille à peu près constante. Aucun symbole ne domine. En théorie, la domination totale et définitive d'un symbole se produit au bout d'un temps fini avec une



probabilité de 100 pour cent. En pratique, ce moment vient si tardivement que l'on considère que les trois symboles coexistent. Les relations de domination cyclique entre souches ou espèces dans le monde vivant sont l'une des causes du maintien de la diversité biologique. Le cas du lézard californien *Uta stansburiana* est frappant, car trois variétés de lézards semblent y jouer à *Pierre-feuille-ciseaux*.

résultat d'évolution à long terme est que ce type de suites de tirages préservant la diversité possède une probabilité nulle de se poursuivre à l'infini.

Nous allons voir que la réalité expérimentale est encore plus intéressante que la théorie mathématique qui indique un peu sèchement qu'au bout d'un certain temps, le système s'uniformise totalement (*voir l'encadré 5*).

Nous allons d'abord observer l'évolution de graphes complets, c'est-à-dire de graphes dont chaque nœud est relié à chaque autre (graphes ayant donc $n(n-1)/2$ arcs pour n nœuds). De façon à visualiser les changements, nous utilisons une grille carrée où deux cases sont liées qu'elles soient côte à côte sur le dessin ou qu'elles ne le soient pas.

Vérification expérimentale

La figure 3 représente l'évolution d'un graphe complet de 100 nœuds. On part d'une configuration aléatoire: rouge pour le symbole *Pierre*, blanc pour *Feuille*, bleu pour *Ciseaux*. Puis on tire successivement 100 arcs du graphe où les combats correspondants sont joués, ce qui donne une nouvelle répartition. Au bout de 17 étapes de 100 combats aléatoires (donc 1 700 combats), le graphe est devenu uniformément bleu: les *Ciseaux* ont gagné. On voit cependant que l'évolution est passée par une phase d'oscillation généralisée: sur le dixième dessin, les cases en bleu dominent largement, puis

sur le dessin 12, c'est au tour des cases rouges d'être majoritaires, avant de laisser la place au dessin 14 aux cases blanches, avant enfin le retour de la domination bleue, cette fois définitive. Pour des graphes complets plus grands, le phénomène de synchronisation est encore plus net et le temps nécessaire avant son interruption par la domination totale d'un symbole devient long, car la phase de domination tournante possède un très grand nombre d'étapes.

Ce mouvement tournant où chacun des trois symboles prend le dessus à tour de rôle s'explique partiellement: les *Feuilles* vivent en exploitant les *Pierres*, et si les *Feuilles* se mettent à dominer, elles éliminent presque totalement les *Pierres*; la situation créée est alors favorable aux *Ciseaux* qui n'ont plus à craindre les *Pierres* et qui rencontrent avec une fréquence croissante les *Feuilles*, qu'ils éliminent; les *Ciseaux* deviennent donc plus nombreux, se multipliant aux dépens des *Feuilles*. Cette domination des *Ciseaux* est favorable aux *Pierres* (plus fortes que les *Ciseaux*) qui deviennent alors majoritaires un peu plus tard, etc.

Reste que cette explication est partielle, car si elle justifie que cela tourne dès que l'un des symboles domine, elle n'indique pas pourquoi l'un des symboles prend rapidement le dessus, engendrant l'oscillation synchronisée de tout le graphe: on pourrait imaginer que tout s'équilibre en gros et que les écarts s'effacent vite dès qu'ils se produisent. Nous allons d'ailleurs voir plus loin des graphes d'un autre type où l'équilibre des effectifs est préservé sur des longues périodes.

Dans la nature, un tel phénomène de domination cyclique a été plusieurs fois observé. Le lézard californien, *Uta stansburiana*, étudié par B. Siverno et C. Lively, présente ce comportement de domination cyclique, car il y a trois sortes de mâles qui semblent pris dans un jeu sans fin de *Pierre-feuille-ciseaux* sur un graphe. L'accouplement est à l'origine du cycle car, dans cette cruciale compétition, les mâles à gorge orange l'emportent sur les mâles à gorge bleue qui eux-mêmes dominent les mâles à bandes jaunes qui à leur tour sont plus efficaces sexuellement que les mâles à gorge orange.

Les lézards

Le détail de leur curieux jeu est le suivant. Les mâles à gorge bleue possèdent des harems composés de trois femelles environ et ne cherchent à défendre que de petits territoires. Quand ils sont les plus nombreux, les mâles à gorge orange, qui eux sont particulièrement agressifs, réussissent à s'imposer et font disparaître la quasi-totalité des mâles à gorge bleue. Les lézards orange ont un tempérament dominant à cause d'une forte concentration en testostérone. Cela les conduit d'ailleurs à constituer des harems ayant jusqu'à sept femelles et à exercer leur domination sur de vastes territoires.

Ils se substituent donc aux mâles à gorge bleue dont le nombre faiblit rapidement sans toutefois s'annuler. Interviennent alors les mâles à bandes jaunes qui s'introduisent dans les camps des mâles à gorge orange en se faisant passer pour des femelles. Ces mâles à bandes jaunes deviennent de plus en plus nombreux et un moment arrive où ils sont majoritaires. Cela laisse réapparaître les mâles à gorge bleue, car ceux-ci savent reconnaître les mâles travestis et les chassent. Cela conduit au retour de la situation initiale avec une majorité de mâles à gorge bleue. Comme dans le cas de nos graphes complets, un cycle répété de confi-

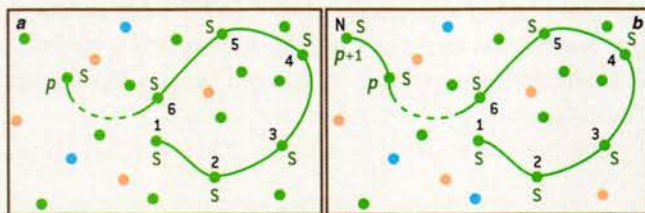


gurations, où dominent successivement chacune des trois catégories de mâles, se poursuit sans interruption sur les territoires étudiés.

À une échelle bien plus petite, dans le domaine de la chimie, les réactions de Belousov-Zhabotinskii peuvent s'interpréter comme la manifestation d'un jeu de *Pierre-feuille-ciseaux* joué à l'échelle microscopique entre composants chimiques. Dans ce cas cependant, aucun

5. L'inévitable uniformisation

La démonstration du résultat que l'on aboutit toujours à l'uniformisation se fait en deux étapes. On établit d'abord que : « Pour tout graphe connexe et pour toute configuration initiale donnée, il existe un tirage d'arcs conduisant l'un des symboles à tout envahir. » Le raisonnement se fait par récurrence. Prenons un graphe connexe de taille n , et une configuration initiale donnée. Nous allons montrer que pour tout entier p inférieur ou égal à n , il existe une suite de tirages d'arcs conduisant (quand on effectue dans l'ordre tous les combats déterminés par les arcs) à un paquet de p nœuds rattachés (formant un sous-graphe connexe) portant le même symbole S .



– Cela est évidemment vrai pour $p = 1$.

– Supposons cela vrai pour $p < n$ et considérons la séquence de choix d'arcs qui conduit à un paquet connexe de p symboles S identiques (a). Montrons qu'on peut en déduire une suite de choix d'arcs qui conduit à un paquet connexe de $p + 1$ symboles identiques (d'après le principe du raisonnement par récurrence, cela nous donnera le résultat). Soit un nœud N , voisin de ce paquet : il y en a au moins un, car le graphe entier est connexe. Si ce nœud N porte le symbole S , nous avons un paquet connexe de $p + 1$ symboles S et le raisonnement est terminé (b). Supposons alors que N porte un symbole S' différent de S .

Si S' est battu par S , on tire l'arc liant le nœud N au paquet de S et l'on a une suite de choix d'arcs (c) qui conduit à un paquet connexe de S de taille $p + 1$: le raisonnement est terminé.

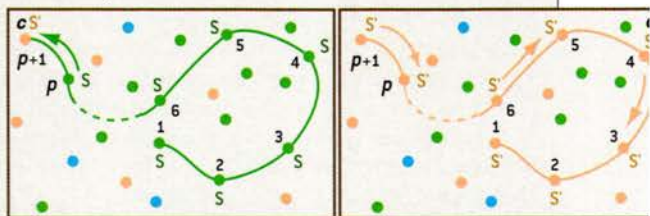
Si S est battu par S' , on choisit la même séquence d'arcs que celle qui conduisait au paquet de p symboles S , suivie d'une suite de tirages progressifs (d) de ces arcs de proche en proche qui font que S' envahit tout le paquet de S , lequel devient donc un paquet connexe de $p + 1$ symboles S' . Cela est possible, car le paquet de p symboles S est connexe. On a alors un paquet de $p + 1$ symboles S' . Dans chaque cas possible, on dispose d'une suite des choix d'arcs conduisant

à un paquet connexe de $p + 1$ symboles identiques. Le raisonnement par récurrence est terminé.

Notons (c'est important pour la seconde partie du raisonnement) que la longueur de la suite d'arcs qui fait passer d'un paquet de p nœuds identiques à un paquet de $p + 1$ nœuds identiques s'obtient en ajoutant au plus p arcs à celle nécessaire pour avoir un paquet de p nœuds identiques. Au total, si le graphe possède n nœuds, on sera certain d'avoir un graphe uniforme en utilisant une suite d'arcs déterminant les combats successifs de longueur au plus $1 + 2 + 3 + 4 + \dots + (n - 1) = n(n - 1)/2$.

Montrons maintenant que l'uniformisation survient avec une probabilité de 100 pour cent. Cette seconde partie du raisonnement utilise l'évidence probabiliste qu'en répétant un tirage au hasard dans l'attente d'un événement ayant une probabilité non nulle de se produire, il finit par se réaliser, ou plus exactement, il se réalise « à l'infini » avec une probabilité de 100 pour cent (en lançant un dé indéfiniment, vous finirez par tomber sur un 6 : s'il est possible,

en théorie, de ne jamais avoir de 6, cet événement a une probabilité nulle : si l'on attend longtemps, on est certain d'avoir un 6).



Partant d'un graphe de n nœuds dans une configuration donnée, nous savons qu'il existe une suite d'arcs qui uniformise le graphe. Cette suite a une longueur inférieure à $n(n - 1)/2$. La probabilité qu'un arc donné soit choisi lors d'une étape du processus d'évolution aléatoire est plus grande que $1/(nk)$ (un nœud est choisi avec une probabilité $1/n$ et un voisin avec une probabilité $1/k$ au plus, où k est le nombre maximum de voisins que possède un nœud du graphe). La probabilité pour qu'une suite d'arcs qui uniformise le graphe soit choisie est donc supérieure à $(1/(nk))^{n(n-1)/2}$, un nombre strictement positif. À l'infini, la probabilité pour qu'au moins une fois une séquence conduisant à l'uniformisation soit choisie est donc de 100 pour cent.

composant ne devient globalement dominant et c'est plutôt à une coexistence des compétiteurs qu'on assiste; ceux-ci se regroupent par zones homogènes mobiles et créent un jeu animé de dessins étonnants, qu'on a associé à l'idée même de phénomène complexe.

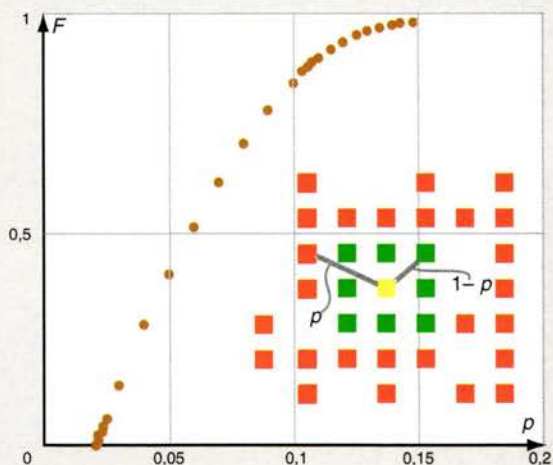
Il est simple d'obtenir l'équivalent de cette dynamique chimique dans le monde abstrait des graphes du jeu *Pierre-feuille-ciseaux*: il suffit de ne pas considérer des graphes complets, mais des graphes réguliers comme ceux correspondant aux cases d'un damier. Chaque case est reliée à ses huit voisines et non plus à toutes les cases comme précédemment.

La figure 4 montre des configurations typiques observées après un long moment d'évolution lorsque l'on considère des graphes-damiers de ce type. Cette fois, la représentation du graphe sur un damier prend tout son sens, puisque les nœuds du graphe ne sont reliés qu'aux huit nœuds correspondant aux huit cases voisines. Au début, le système est placé dans un état totalement mélangé (1/3-1/3-1/3). Rapidement, apparaissent des zones homogènes des trois couleurs et ces zones se déplacent et changent de forme de manière incessante tout en gardant des caractéristiques globales stables: la taille des zones homogènes est à peu près constante, ainsi que leur vitesse de déplacement et le type de motifs dessinés. Ici, aucun symbole ne domine les autres. L'évolution se traduit par des mouvements ininterrompus des frontières interzones. La zone de séparation entre *Pierres* et *Feuilles* se déplace, car les *Pierres* reculent devant les *Feuilles*; de même, les *Feuilles* reculent devant les *Ciseaux* et les *Ciseaux* devant les *Pierres*. L'examen détaillé des effectifs montre une oscillation limitée autour de 1/3 de la proportion de chacun des symboles. Cette fluctuation apparaît comme une variation statistique inévitable qui, ne prenant pas d'ampleur, ne conduira en pratique jamais à la domination d'un symbole.

6. Jeux intermédiaires Pierre-feuille-ciseaux.

On définit une famille continue entre le jeu sur un graphe complet et le jeu sur un graphe-damier. On se fixe un paramètre p entre 0 et 1. À chaque coup, on choisit un premier nœud N au hasard uniformément parmi tous les nœuds. Pour le second nœud N' , on choisit entre deux méthodes A et B, la méthode A choisie avec une probabilité p et la méthode B avec une probabilité $1 - p$. Si la méthode A est choisie, on prend pour N' un nœud quelconque du graphe. Si la méthode B est retenue, on choisit N' parmi les huit voisins de N . Les nœuds N et N' ainsi déterminés livrent alors combat. Pour $p = 0$, tout se passe comme quand on jouait au jeu sur un graphe-damier, pour $p = 1$, comme si on jouait sur un graphe complet. Pour p assez petit (jusqu'à 0,002), l'évolution du graphe se fait en préservant un bon mélange: les trois symboles restent présents en proportion équilibrée 1/3-1/3-1/3. Lorsque p se trouve entre 0,002 et 0,15, la proportion de chaque symbole fluctue dans le système, ce que l'on mesure par un paramètre de fluctuation F ($F = 0$, pas de fluctuation; $F = 1$, variation maximale des effectifs). Au-delà de 0,15, le système devient violemment oscillant comme dans le cas d'un graphe complet: chacun des symboles domine à tour de

rôle, le graphe passant par des états où un symbole occupe la quasi-totalité du graphe, toutes les cases du graphe sont synchronisées (ces simulations ont été menées par A. Szolnoki et G. Szabó).



Les deux cas rencontrés, oscillation synchronisée de tout le graphe ou formation de zones homogènes mobiles, correspondent à deux modes de la dynamique d'évolution des graphes de *Pierre-feuille-ciseaux*. Dans les deux types de graphes, nous savons qu'à long terme l'un des états envahit tout. Cependant, le temps nécessaire pour que se produise cette domination définitive est très différent dans les deux cas. Dans le cas des graphes complets, ce temps augmente lentement en fonction de la taille du graphe. Dans le cas des graphes-damiers, l'instant de la stabilisation est repoussé bien plus loin, si bien qu'en pratique, le système reste dans un état mixte où les trois symboles coexistent.

Temps de convergence différents

La théorie nous indique pourtant que l'un des états finit toujours par dominer; la simulation nous montre qu'avec les graphes complets, cette domination arrive rapidement, alors qu'avec les graphes-damiers, sa venue est tellement éloignée dans le temps que c'est une stabilisation avec coexistence des trois états qu'il faut considérer comme l'évolution normale à moyen terme de la dynamique du graphe. Une étude détaillée des caractéristiques de ces dynamiques a été menée par Rémi Dorat à coup de simulations massives et prolongées. Il montre que le temps d'uniformisation croît exponentiellement dans le cas des graphes-damiers.

La situation de coexistence des trois symboles est sans doute une explication du maintien de la diversité dans certaines situations biologiques. Le terrain où trois espèces se rencontrent (les dominations se conformant à un schéma circulaire du type *Pierre-feuille-ciseaux*) est assimilable à un graphe de type graphe-damier. La dynamique de domination montre alors sur le terrain des motifs plus ou moins semblables à ceux vus lors des simulations.

Benjamin Kerr, Margaret Riley, Marcus Feldman et J. M. Bohannan, dans un article de la revue *Nature*, proposent une telle interprétation de leur expérience réalisée avec trois souches d'*Escherichia coli*, en relation non transitive comme les symboles *Pierre-feuille-ciseaux*. La conclusion de leur étude est conforme à ce qui est montré par les simulations. Lorsque l'espace où est réalisée l'expérience est petit et, plus généralement, lorsque les relations entre souches sont assimilables à celles décrites par un graphe complet, l'une des souches domine rapidement. En revanche, lorsque les interactions se déroulent sur un espace plus grand, cette fois assimilable à un graphe de type damier, les trois souches coexistent avec des mouvements des zones occupées par chacune d'elles, mouvements assez semblables à ceux vus lors des simulations.

Des études sur des graphes intermédiaires entre les graphes complets et les graphes-damiers ont été réalisées par György Szabó, Attila Szolnoki et Rudolf Izsák. Divers phénomènes de transition de phases ont pu être mis en évidence, et ils permettent de mieux comprendre toutes ces dynamiques discrètes nées d'un jeu élémentaire (*voir l'encadré 6*). La science n'a jamais fini d'étudier les jeux: même les plus simples suggèrent des modèles explicatifs utiles, dont la logique ne peut être élucidée que par la simulation, car ici le raisonnement abstrait ne suffit plus.

La Belle au bois dormant, la fin du monde et les extraterrestres

L'analyse de plusieurs énigmes troublantes suggère la notion d'anamorphose probabiliste et fournit la solution du paradoxe de l'Apocalypse.

Dans le Laboratoire de psychologie probabiliste de l'Université de Hasardville, les discussions font rage. Elles portent sur le résultat d'une expérience dont nous allons décrire le protocole. Le dimanche soir, alors que *La Belle au bois dormant* (nous la dénommerons *Belle* dans ce qui suit) est endormie, nous lançons une pièce de monnaie pour un tirage à pile ou face. Une grande confiance règne entre *Belle* et les expérimentateurs ; elle est renforcée par un huissier qui contrôle que tout se déroule selon les règles acceptées par tous.

Si la pièce est tombée sur FACE, le lendemain (le lundi) on réveille *Belle* et on a un entretien avec elle. Si c'est PILE, on la réveille le lundi, on a un entretien avec elle, puis on la rendort après l'avoir soumise à un traitement qui lui fait complètement oublier la journée du lundi. Enfin, toujours dans le cas de PILE, on la réveille à nouveau le mardi (elle ignore qu'on est mardi) et on a un autre entretien avec elle.

Ces expériences doivent mesurer le bon sens probabiliste de *Belle*. À la fin d'un entretien, on lui demande quelles probabilités, $\Pr(\text{FACE})$ et $\Pr(\text{PILE})$, elle attribue au tirage réalisé le dimanche soir, alors qu'elle était endormie ?

Belle réfléchit : « La pièce est normale et l'huissier qui contrôle le déroulement des opérations me garantit que le résultat obtenu par ce tirage à pile ou face détermine la suite des opérations conformément au protocole : un réveil le lundi si FACE, un réveil le lundi et un autre le mardi si PILE. À chaque réveil, je n'aurai aucune information en plus de celles dont je disposais le dimanche soir avant que la pièce ne soit lancée. Avant de m'endormir dimanche, j'attribuais la probabilité $1/2$ à FACE et à PILE ; donc, quand je suis réveillée lors de l'expérience, je dois attribuer la même probabilité $1/2$ à chaque éventualité. Ma réponse est donc : $1/2$ pour FACE, et $1/2$ pour PILE. » La démonstration semble irréfutable. Et pourtant...

Après réflexion, *Belle* se ravise et propose un autre raisonnement : « Imaginons qu'on fasse l'expérience 100 fois en opérant 100 semaines de suite. Dans environ la moitié des semaines (50), je serai réveillée le lundi après un tirage FACE. Les autres semaines (50 environ) PILE aura été tiré et je serai réveillée le lundi et le mardi ; dans ces cas-là, je serai donc réveillée 100 fois. Au total, lors des 100 semaines je serai réveillée environ 150 fois et, sur ces 150 réveils, FACE sera la bonne réponse 50 fois, et PILE la bonne réponse 100 fois. À chaque fois que je suis réveillée, la probabilité que la pièce lancée le dimanche soit tombée sur FACE est donc de $1/3$ et, pour PILE, c'est $2/3$. Ma réponse sera donc : $1/3$ pour FACE, et $2/3$ pour PILE. » Cher lecteur, êtes-vous du côté des partisans du $1/2 - 1/2$ ou des partisans du $1/3 - 2/3$?

Les organisateurs désirent que *Belle* prenne les choses au sérieux, aussi introduisent-ils un enjeu financier. Si *Belle* indique correctement le résultat du lancer du dimanche soir, elle gagne 1000 euros; si elle se trompe, elle n'a rien. *Belle* raisonne de la façon suivante:

«Imaginons comme précédemment que le jeu soit organisé 100 semaines consécutives. Lors des 100 expériences en choisissant toujours FACE, je gagnerai environ 50000 euros, alors qu'en choisissant de répondre toujours PILE, je gagnerai 100000 euros environ. Cela confirme que FACE "est" moins probable que PILE; puisque PILE fait gagner le double de ce que ferait gagner FACE, sa probabilité "est" double de celle de FACE. On a bien $\Pr(\text{FACE}) = 1/3$, $\Pr(\text{PILE}) = 2/3$. C'est sûr, c'est le bon résultat, l'argent ne trompe pas! Non seulement j'indiquerai les évaluations $1/3$ pour FACE et $2/3$ pour PILE, mais je parierai toujours pour PILE. Je suis si certaine de mon évaluation que je suis prête à payer 650 euros pour avoir le droit de jouer, car mon gain moyen sera de $1000 \times 2/3 = 666,6$ euros.»

Musée de la Ville de Paris. Musée Carnavalet, Paris, France, Bridgman Art Library.



1 Le paradoxe de *La belle au bois dormant*. Le dimanche soir *La belle au bois dormant* est endormie et on lance une pièce. Si elle retombe sur FACE alors on réveille *La belle au bois dormant* le lundi, elle évalue les probabilités de PILE et de FACE et se rendort. Si c'est PILE, on la réveille le lundi, elle doit évaluer les probabilités de PILE ou de FACE, et se rendort en oubliant cet épisode, mais on la réveille aussi le mardi et elle réévalue les probabilités avant de se rendormir. Lors des entretiens, on demande à *La belle au bois dormant* quelle est, à son avis, la probabilité que FACE soit

tombé, et quelle est la probabilité que PILE soit tombé ? Elle peut répondre $1/2$ pour FACE et $1/2$ pour PILE en arguant que la pièce a une chance sur deux de tomber sur une des deux faces ou $1/3$ pour FACE et $2/3$ pour PILE, car on lui pose la question deux fois plus souvent (le lundi et le mardi) quand c'est PILE. Êtes-vous partisan de $1/2 - 1/2$ ou partisan de $1/3 - 2/3$? L'illustration est une peinture de la représentation, au théâtre du Vaudeville à Paris vers 1820, de *La belle au bois dormant* d'après le conte de Perrault (1628-1703).

La solution $1/3 - 2/3$ semble ainsi confirmée par l'introduction de l'enjeu des 1 000 euros et tout paraît réglé. Cela est-il certain ? Le directeur du laboratoire trouve que ce protocole de pari lui coûte trop cher et décide qu'il ne veut pas risquer plus de 1 000 euros par expérience. Aussi le système de pari est-il redéfini et nous dénommerons le nouveau protocole, le pari du directeur : lorsque PILE tombe, le laboratoire ne propose le pari que le lundi et, toujours dans le cas de PILE, lorsque *Belle* est réveillée le mardi, on a avec elle l'entretien prévu, mais on ne lui propose aucun pari. Lorsque FACE tombe, on opère comme précédemment avec un réveil lundi et un pari.

Belle reprend son raisonnement et ses calculs. « Durant 100 semaines de jeu, si je choisis toujours FACE, je gagnerai 50 000 euros environ, les 50 semaines où FACE sera tombé. Si je choisis toujours PILE, je gagnerai 50 000 euros environ : les semaines où PILE sera tombé, car le lundi on m'aura offert le pari. Donc les deux choix se valent : j'ai le même intérêt à parier sur PILE que sur FACE. »

Ce pari confirme donc l'évaluation $1/2 - 1/2$, ce qui est gênant puisque le premier pari avait donné l'assurance que $1/3 - 2/3$ était la bonne évaluation. Le plus paradoxal semble ici que *Belle*, lorsqu'elle est réveillée, évalue les probabilités qu'elle accorde à FACE ou à PILE sans savoir si on va lui offrir la possibilité de parier. Donc son évaluation de la probabilité de FACE ou PILE avec les règles du protocole de pari initial ou celles du protocole de pari du directeur devrait être la même : tout y est exactement identique au moment où on l'interroge sur son évaluation des probabilités. Comment se peut-il que « monétairement » les deux choses soient différentes et donc que, finalement, les probabilités qu'elle doit attribuer à FACE ou à PILE soient différentes : si c'est le protocole de pari initial, $1/3 - 2/3$, si c'est le protocole de pari du directeur, $1/2 - 1/2$?

La confusion semble à son comble. Deux raisonnements en apparence rationnels conduisent à deux conclusions différentes. L'introduction d'enjeux ne résout pas le problème, car la façon dont on fait les paris renforce, soit la proportion $1/3 - 2/3$, soit la proportion $1/2 - 1/2$.

Le protocole sans mardi

Je vais présenter un raisonnement qui remet tout en ordre, mais je dois préciser que cette solution ne fait pas l'unanimité des spécialistes. Considérons une autre expérience, l'expérience sans mardi, qui éclaircira le dilemme.

– Le dimanche soir, après avoir endormi *Belle* comme précédemment, on lance la pièce de monnaie non truquée.

– *Belle* est toujours réveillée le lundi quand la pièce tombe sur FACE. Si elle tombe sur PILE, on relance la pièce et si elle tombe encore sur PILE, *Belle* est alors réveillée. Sinon elle n'est pas réveillée. Lors de l'entretien, les organisateurs lui demandent alors de parier sur FACE ou PILE en lui disant que si elle devine correctement le résultat du tirage du dimanche, elle gagnera 1 000 euros. Le mardi, rien ne se passe.

– *Belle* est ensuite endormie et elle oublie ce qu'elle a fait le lundi, sauf que, lorsqu'elle a gagné, elle garde dans sa poche les 1 000 euros qu'elle trouve à son réveil.

– Dans le cas des lancers PILE-FACE où les expérimentateurs ne la réveillent pas, *Belle* dort le lundi toute la journée et, à son réveil un des jours suivants, elle trouve bien sûr sa poche vide sans savoir si c'est parce qu'elle a été réveillée et a perdu son pari, ou parce qu'elle a dormi continûment.

Les lundis où *Belle* est réveillée, elle peut raisonner ainsi, car elle connaît le protocole : « La pièce n'est pas truquée, donc la probabilité de PILE est la même que la probabilité de FACE. Mon pari est indifférent, je vote donc toujours pour PILE. » Pourtant, sur 100 expériences, elle gagnera environ 25 000 euros, alors qu'elle en aurait gagné 50 000 si elle avait parié sur FACE : pour *Belle*, il n'est pas vrai que la pièce tombe une fois sur deux sur PILE. On comprend ici l'erreur : le fait qu'on ne la réveille pas systématiquement le lundi lorsque PILE est tombé fausse sa vision du tirage du dimanche soir : *Belle* voit plus souvent FACE, car la moitié des tirages PILE lui sont cachés ! Sa vision est soumise à un « filtre probabiliste » qui change le $1/2 - 1/2$ réel de la pièce en $2/3 - 1/3$ en faveur de FACE.

Le raisonnement consistant à dire que « La pièce n'est pas truquée, donc la probabilité de PILE est la même que la probabilité de FACE » est faux. *Belle* doit prendre en compte l'effet de filtre auquel elle est soumise quand elle est engagée dans le protocole expérimental. L'histoire du pêcheur décrit figure 2 est un autre exemple d'effet de filtre. Les effets de sélection observationnelle sont fréquents et toujours dangereux. Les éviter est l'objectif principal des techniques de sondages.

Dangereux effets de filtre

Une célèbre erreur commise à cause de l'effet de filtre s'est produite à propos de l'élection de Franklin Roosevelt en 1936. Le *Literary Digest* avait interrogé certains électeurs en se fondant principalement sur les listes des propriétaires de téléphones et de véhicules automobiles, et en avait déduit que Alf Landon serait élu président des États-Unis contre Roosevelt. Or ce dernier fut élu. L'erreur, due au fait que les électeurs pauvres

LA FÉE ÉLECTRICITÉ AU SECOURS DES CONTES
(AUJOURD'HUI : LA BELLE AU BOIS DORMANT)



2. Effet de filtre et effet de loupe

Lorsqu'un pêcheur sait qu'un poisson sur deux du lac où il pêche mesure moins de 5 centimètres, la moitié des poissons qu'il pêchera ne dépasseront pas 5 centimètres. Cependant, si les mailles de son filet sont trop larges et qu'elles laissent passer la moitié des poissons de moins de 5 centimètres, alors le pêcheur trouvera dans son filet $2/3$ de poissons de plus de 5 centimètres et $1/3$ de poissons de moins de 5 centimètres. Son filet filtre les poissons et cette sélection fausse sa vision du contenu du lac. Les effets de sélection observationnelle sont fréquents et un des principaux objectifs des techniques de sondages est de les éviter.

Dans le cas de l'expérience de *La belle au bois dormant*, il se produit un effet opposé à l'effet de filtre, l'effet de loupe. Lorsque, dans la première expérience, la pièce, lancée le dimanche soir, tombe sur PILE, cela double l'observation du résultat PILE.

Ainsi, de même que l'effet de filtre, l'effet de loupe modifie les probabilités observées. En astrophysique, le phéno-

mène comparable de loupe gravitationnelle conduit à voir deux fois certains objets célestes qui pourtant sont uniques. Ces effets de filtre et de loupe (regroupés sous le nom d'effets d'anamorphose probabiliste) sont la clef de plusieurs paradoxes et ont donné lieu à de nombreux échanges ces dernières années.

n'avaient ni téléphone ni voiture, et qu'ils soutenaient plutôt Roosevelt, permit à George Gallup de prouver le bien-fondé des méthodes de son Institut de sondages : il avait, quant à lui, émis un pronostic exact en n'interrogeant qu'un petit nombre de gens, mais en évitant les effets de sélection (de filtre). Une erreur similaire relevée par Hervé le Bras dans les études démographiques concerne le nombre moyen de frères et de sœurs par famille. Vous savez que le nombre moyen d'enfants par famille est de 2. En revanche, si vous demandez aux enfants combien ils ont de frères et sœurs y compris eux-mêmes, et que vous faites la moyenne des réponses obtenues, le résultat sera bien supérieur à 2... Logique, car vous n'avez pas interrogé les enfants des familles où il n'y en a pas et qui auraient fait baisser la moyenne ! De plus, les enfants de familles à deux enfants sont deux fois plus souvent interrogés que ceux de familles à un enfant, etc.

L'expérience sans mardi est claire : le protocole est tel qu'un effet de filtre opère sur ce que *Belle* « voit » du lancer de pièce du dimanche soir. Pour elle, malgré le fait incontestable que la pièce n'est pas truquée, on la réveille toujours pour FACE, alors que pour PILE on ne la réveille qu'une fois sur deux seulement. Donc un réveil correspond à FACE deux fois sur trois et PILE une fois sur trois : il n'y a pas de paradoxe, juste un effet de filtre. Dans le paradoxe initial, la distorsion du protocole est un phénomène analogue qui, au lieu de provoquer un effet de filtre sur les données (en masquant certains tirages), opère un effet de loupe : lorsque PILE tombe, *Belle* voit deux fois PILE, une fois le lundi et une autre fois le mardi. Le protocole fausse la vision que *Belle* a du tirage de la pièce. Du fait de cette déformation, elle voit un monde où la pièce tombe deux fois plus souvent sur PILE que sur FACE. Au total, il n'y a rien de mystérieux : un effet de



3. La formule de Bayes

La formule de Bayes indique comment, en fonction d'une information nouvelle, il faut réévaluer des probabilités précédemment attribuées.

On dispose de la probabilité $\Pr(A)$ pour l'événement A . La formule de Bayes est une formule compliquée qui exprime un fait simple : quand un événement apparaît,

les théories où cet événement est le plus probable sont renforcées. Comme nous allons le voir en chiffres, si les tricheurs gagnent toujours et que vous perdez contre un adversaire, il devient plus probable que c'est un tricheur, que vous ne le pensiez *a priori*.

En termes abstraits, un événement E se produit et on veut connaître la probabilité, notée $\Pr(A|E)$, d'avoir A sachant que E s'est produit. Il existe une formule qui exprime cette probabilité $\Pr(A|E)$ que l'on cherche à connaître en fonction de $\Pr(A)$, $\Pr(E|A)$, $\Pr(\text{non } A)$, $\Pr(E|\text{non } A)$ qui sont connues. Cette formule indique que :

$$\Pr(A|E) = \frac{\Pr(A) \cdot \Pr(E|A)}{\Pr(A) \cdot \Pr(E|A) + \Pr(\text{non } A) \cdot \Pr(E|\text{non } A)}$$

Exemple. Le tricheur

Je joue avec un partenaire qui pourrait tricher. J'évalue *a priori* que la probabilité que mon partenaire triche est 1/10 :

$$\Pr(A) = \Pr(\text{tricheur}) = 1/10.$$

Lorsque je joue avec un tricheur, il gagne dans 2/3 des cas :

$$\Pr(\text{je perds} | \text{tricheur}) = 2/3.$$

Comme je suis expert, je sais que, face à un joueur honnête, je gagne 99 fois sur 100 :

$$\Pr(\text{je perds} | \text{non tricheur}) = 1/100.$$

Je viens de jouer et j'ai perdu.

Quelle est la probabilité *a posteriori* pour que, en face de moi, il y ait un tricheur ? On applique la formule de Bayes avec $A = \text{tricheur}$, $E = \text{je perds}$:

$$\Pr(\text{tricheur} | \text{je perds}) = \Pr(A).$$

$$\Pr(E|A) / [\Pr(A) \cdot \Pr(E|A) + \Pr(\text{non } A) \cdot \Pr(E|\text{non } A)] = 1/10 \cdot 2/3 / [1/10 \cdot 2/3 + 9/10 \cdot 1/100] = 88,1 \%$$

La probabilité, après avoir perdu, que j'ai joué avec un tricheur est bien plus forte maintenant : elle est passée de 10 % à 88,1 %. Avant que je ne perde, il était peu probable que le joueur en face de moi soit un tricheur, maintenant c'est presque certain. C'est le glissement bayésien.

loupe grossit la probabilité de PILE, comme un effet de filtre diminue celle de PILE dans l'expérience sans mardi. Ces phénomènes qu'on peut regrouper sous le nom d'anamorphoses probabilistes sont la clef du paradoxe de *La Belle au bois dormant*.

Oui, c'est bien $1/3 - 2/3$

Tout semble être rentré dans l'ordre à l'exception du protocole de pari du directeur, qui reste à élucider. Cette dernière difficulté va être résolue en évoquant ce que l'on dénomme le glissement Bayésien, connu depuis longtemps.

La clef de la solution est que dans le protocole du directeur, il faut distinguer l'évaluation que doit faire *Belle* quand on l'interroge, et le pari qu'elle doit faire quand on lui propose de parier, car le fait qu'on lui propose un pari est, avec ces règles, une information nouvelle. Lorsqu'elle donne son évaluation pour FACE et pour PILE, elle doit proposer $1/3 - 2/3$, car au moment même où elle fournit cette évaluation tout est exactement identique au protocole initial pour lequel elle prend en compte l'effet de loupe probabiliste identifié plus haut. En revanche, lorsqu'on lui propose de parier, les choses changent, car elle sait alors que l'on n'est pas mardi (dans le protocole du directeur, aucun pari n'est proposé le mardi). Elle doit prendre en compte cette information nouvelle, ce qui a pour effet d'annuler l'effet de loupe et la conduit à l'évaluation $1/2 - 1/2$.

Les calculs des gains moyens avec le protocole de pari du directeur confirment ce $1/2 - 1/2$. Un calcul numérique basé sur ce qu'on appelle la formule de Bayes (voir l'encadré 3) montre que l'évaluation de $1/3 - 2/3$ passe à $1/2 - 1/2$ entre le moment où on a l'entretien avec *Belle* sans lui offrir de pari et le moment où on lui offre le pari. La confusion est levée : le pari du directeur, en introduisant une information, faussait le $1/3 - 2/3$ qui est la bonne évaluation que doit faire *Belle* à cause de l'effet de loupe probabiliste. Notons les leçons de cette histoire :

- Le fait qu'une pièce de monnaie ne soit pas truquée ne signifie pas que nous devons observer autant de FACE que de PILE. Lorsque nous sommes pris dans un protocole expérimental qui biaise par anamorphose probabiliste nos observations – soit par effet de filtre, soit par effet de loupe – une autre vision des tirages peut nous être offerte.
- Le seul fait de proposer un pari constitue parfois une information qui change les évaluations de probabilité.

La conséquence remarquable de l'étude du paradoxe de *La belle au bois dormant* (qui n'en est plus un si vous acceptez le point de vue des filtres et des loupes probabilistes) est qu'il résout le paradoxe de l'Apocalypse. Ce paradoxe introduit en 1983 par l'astrophysicien Brandon Carter, et sur lequel le philosophe canadien John Leslie a attiré l'attention au début des années 1990, a donné lieu à un grand nombre d'articles.

En 1993, je l'ai mentionné dans un article et des dizaines de lettres m'ont été envoyées, proposant des idées pour sa résolution. Parmi les solutions proposées, beaucoup sont normatives : elles consistent à décréter qu'on n'a pas le droit de raisonner avec les probabilités quand le temps est impliqué, ou parce qu'on se réfère à une notion trop vague d'être humain. Les solutions normatives sont insatisfaisantes, car elles limitent le champ d'application des concepts probabilistes et ne correspondent pas à ce qui est en général admis. Se rassurer à bon compte en s'interdisant de raisonner est trop facile.

Rappelons le paradoxe. Imaginons que deux théories, *A* et *B*, sur le destin ultime de l'humanité, sont en compétition :

Théorie A. La fin de l'humanité se produira avant 2050 et, au total, il y aura eu environ cent milliards (10^{11}) d'êtres humains.

Théorie B. La fin de l'humanité se produira bien plus tard et, au total, il y aura eu cent mille milliards (10^{14}) d'êtres humains.

Imaginons que l'on détermine *a priori*, par des analyses provenant de diverses sciences fondamentales (mathématiques, physique, chimie, biologie, etc.), que : $\Pr(A) = 1/2$ et $\Pr(B) = 1/2$. Le paradoxe de Brandon Carter défendu avec acharnement par John Leslie consiste à proposer l'argumentation suivante. Les évaluations $\Pr(A) = 1/2$ et $\Pr(B) = 1/2$ sont faites dans le cadre général des sciences, mais je dispose d'une information particulière qui me permet de réévaluer ces probabilités : « Je suis un humain dont le rang de naissance est inférieur à cent milliards » (événement *E*). Dans la théorie *A*, l'événement *E* est banal (inévitables même), en revanche, dans la théorie *B*, cet événement est étonnant, car cela me place dans le premier millième des êtres humains, chose statistiquement peu probable (la probabilité de *E* sachant *B* est $1/1\,000$). Si une information est plus probable dans le cadre d'une théorie *A* que dans le cadre d'une théorie *B*, et que j'apprends alors que cette information est vraie, cela renforce ma confiance en la théorie *A* et diminue celle que j'ai concernant la théorie *B*. La formule de Bayes permet de rendre cela précis. Le calcul détaillé dans l'encadré 4 conduit à :

– Probabilité de *A* sachant que *E* est vrai = $0,9990 = 99,90\%$.

– Probabilité de *B* sachant que *E* est vrai = $0,001 = 0,10\%$.

Le paradoxe de l'Apocalypse

Il y a un « glissement bayésien » en faveur de l'hypothèse d'une fin proche de l'humanité. Un tel glissement a lieu même si plus de deux théories sont en compétition et se produit quelles que soient les hypothèses numériques formulées. La fin de l'humanité serait donc plus proche que ce que l'on peut croire en se fiant uniquement aux risques évalués scientifiquement. Raisonnement troublant !

Il se trouve qu'en regardant bien et aux valeurs près des paramètres numériques, la situation décrite dans le paradoxe de l'Apocalypse est exactement la même que celle du paradoxe de *La belle au bois dormant* lorsque, dans le protocole de pari du directeur, elle apprend qu'on est lundi parce qu'on lui propose un pari.

Lorsque *Belle* raisonne, elle oppose deux théories : celle qui affirme que FACE est tombé et dans laquelle son existence au sein de l'expérience sera unique (puisque'elle ne sera pas réveillée le mardi), et celle qui affirme que PILE est tombé et dans laquelle son existence au sein de l'expérience sera double. Reasonner comme Leslie et Carter le proposent consiste à dire que les probabilités de FACE et PILE sont $1/2 - 1/2$ et, lorsque *Belle* apprend que c'est lundi (l'équivalent d'apprendre que je suis dans le premier millième des humains), je dois réévaluer les probabilités de FACE et PILE, ce qui renforce FACE (un calcul avec la formule de Bayes donne $2/3$ pour FACE et $1/3$ pour PILE). En résumé : on part de $1/2 - 1/2$ pour FACE et PILE, et en utilisant l'information qu'on est lundi, on arrive à $2/3 - 1/3$ en faveur de FACE. Mais raisonner ainsi c'est commettre un grave oubli : l'effet de loupe. Le raisonnement correct, lui, se déroule en trois phases.

4. Le paradoxe de l'Apocalypse

Dans l'expérience de pensée qui va suivre, deux théories, que nous désignerons par A et B , sont en compétition.

Théorie A. La fin de l'humanité se produira avant 2050 et au total il y aura eu environ cent milliards (10^{11}) d'êtres humains.

Théorie B. La fin de l'humanité se produira bien plus tard et au total il y aura eu cent mille milliards (10^{14}) d'êtres humains.

Supposons que l'on sache par des analyses provenant des diverses sciences fondamentales que: $\Pr(A) = 1/2$ et $\Pr(B) = 1/2$. L'information « Je suis un humain dont le rang de naissance est inférieur à cent milliards » (événement E) permet grâce à la formule de Bayes de réévaluer les probabilités de A et de B .

(I) Sans prise en compte de l'effet de loupe.

Les calculs, analogues à ceux du cas du tricheur, donnent:
 $\Pr(A|E) = \Pr(E|A) \Pr(A) / [\Pr(E|A) \Pr(A) + \Pr(E|B) \Pr(B)] = 1 \times 1/2 / [1 \times 1/2 + 1/1000 \times 1/2] = 0,999 = 99,9 \%$

$\Pr(B|E) = 0,1 \%$.

La probabilité d'une fin proche de l'humanité est donc 99,9 %. C'est le troublant paradoxe de l'Apocalypse défendu par B. Carter et J. Leslie.

(II) Avec prise en compte préalable de l'effet de loupe.

En fait, les évaluations $\Pr(A) = \Pr(B) = 1/2$ sont faites dans un contexte atemporel alors que nous, humains, sommes situés dans l'Univers. C'est la même différence qu'entre la situation de *Belle* avant l'expérience et sa situation quand on l'interroge durant l'expérience. Prendre en compte que nous sommes situés dans l'Univers consiste à évaluer l'effet de loupe probabiliste. Puisqu'il y a mille fois plus d'humains lorsque la théorie B est satisfaite, la réévaluation donne :

$\Pr'(A|E) = 1/1001$; $\Pr'(B|E) = 1000/1001$

L'utilisation de la formule de Bayes à partir de $\Pr'(A)$ et $\Pr'(B)$ fournit une seconde réévaluation qui donne :

$\Pr(A|E) = \Pr(B|E) = 1/2$

Le paradoxe de l'Apocalypse a disparu.



Shutterstock / sdecoret

- (a) Le dimanche soir *Belle* attribue les probabilités $1/2$ pour FACE et $1/2$ pour PILE.
- (b) Le lundi matin, avant qu'on lui offre de parier (c'est-à-dire avant qu'elle apprenne qu'on est lundi), elle prend en compte l'effet de loupe engendré par le protocole dans lequel elle est située, et elle attribue donc les probabilités $1/3$ pour FACE et $2/3$ pour PILE.
- (c) Le lundi matin un peu plus tard, quand on lui offre le pari et qu'elle sait donc qu'on est lundi (information nouvelle), elle réexamine ses évaluations et, utilisant la formule de Bayes, retombe sur l'évaluation $1/2$ pour FACE et $1/2$ pour PILE qu'elle avait obtenue le dimanche soir.

Dans le cas du paradoxe de l'Apocalypse, le raisonnement correct calqué sur le précédent se formule ainsi.

(a) Utilisant diverses analyses scientifiques, on attribue les probabilités $1/2$ pour la théorie *A* et $1/2$ pour la théorie *B*. Cette phase se place avant que je ne prenne en compte mon existence dans l'Univers. C'est l'équivalent de l'examen de la pièce de monnaie que *Belle* effectue le dimanche soir qui lui indique que la pièce n'est pas truquée et que les probabilités sont donc $1/2$, pour FACE comme pour PILE.

(b) Je prends en compte ma situation dans l'Univers, ce qui est équivalent à prendre en compte que je participe à une expérience du type de celle organisée pour *Belle*. Je sais que, dans de telles expériences, je subis un effet de loupe probabiliste. Ici, l'effet est très sensible puisque les êtres humains sont mille fois plus nombreux dans la théorie *B* que dans la théorie *A*. Je réévalue mes attributions de probabilités, ce qui donne ici : $1/1001 = 0,1\%$ pour *A* et $1000/1001 = 99,9\%$ pour *B*.

(c) Je prends maintenant en compte mon rang de naissance et par utilisation de la formule de Bayes je trouve (voir les calculs encadré 4) : Probabilité de *A* sachant que *E* est vrai = $1/2$, probabilité de *B* sachant que *E* est vrai = $1/2$.

Je suis retombé sur mes évaluations de départ. Il n'y a plus de paradoxe. Cette compensation exacte entre l'effet de loupe qui grossit la probabilité à attribuer à l'hypothèse que l'humanité va survivre longtemps et l'effet de la formule de Bayes qui grossit la probabilité que l'humanité va bientôt disparaître se produit avec tous les jeux de données imaginables.

Cela règle définitivement le problème du prétendu paradoxe de Leslie-Carter. Il est amusant de noter que lorsqu'il s'agit du paradoxe de *La belle au bois dormant*, les gens ayant participé aux débats se sont répartis à peu près équitablement entre partisans du $1/2 - 1/2$ et partisans du $1/3 - 2/3$, alors que dans le cas du paradoxe de l'Apocalypse, pourtant formellement équivalent, la presque totalité des avis refusait le mode de raisonnement de Leslie-Carter. Selon les enjeux, la rationalité varie... Encore un effet de sélection.

La vie dans l'Univers

L'idée que finalement il faut prendre en compte l'effet de loupe probabiliste dans des cas comme celui du paradoxe de l'Apocalypse a malgré tout une conséquence ennuyeuse (qui est l'un des arguments utilisés par ceux qui s'opposent à la solution $1/3 - 2/3$ du paradoxe de *La belle au bois dormant*). En effet, quand on s'interroge sur la possibilité de la vie extraterrestre, on aboutit à une conclusion qu'on peut juger contre-intuitive. Supposons pour simplifier que deux théories s'opposent.

Théorie A. Les lois de la physique rendent peu vraisemblable que la vie apparaisse sur une planète et il n'y a en moyenne qu'une planète donnant naissance à la vie par galaxie.

Théorie B. Les lois de la physique rendent assez vraisemblable que la vie apparaisse sur une planète et il y a en moyenne un milliard de planètes portant la vie par galaxie.

Imaginons qu'en raisonnant sur la base de données scientifiques générales (mathématiques, physique, chimie, biologie théorique, etc.), on évalue $\Pr(A) = 1/2$, $\Pr(B) = 1/2$. Alors si nous voulons être cohérents avec la solution adoptée pour le paradoxe de l'Apocalypse, nous devons prendre en compte l'effet de loupe probabiliste et conclure que $\Pr(A)$ et $\Pr(B)$ doivent être réévaluées par nous humains situés dans l'Univers à un instant donné et non pas à l'extérieur. Les calculs aboutissent alors à la conclusion qu'en recherchant la vie autour de nous dans notre Galaxie, la Voie lactée, nous avons un milliard de fois plus de chances de trouver d'autres planètes habitées que de ne pas en trouver. De $1/2$ pour A , $1/2$ pour B , nous passons par prise en compte de l'effet de loupe à $1/1\,000\,000\,001$ pour A et $1\,000\,000\,000/1\,000\,000\,001$ pour B .

L'hypothèse A est devenue totalement improbable (moins d'une chance sur un milliard) et il y a donc sans doute des extraterrestres proches de la Terre. Cette réévaluation n'est-elle pas troublante ? Êtes-vous toujours aussi sûr que l'effet de loupe doit être pris en compte et qu'il est la solution définitive du paradoxe de l'Apocalypse et du problème de *La belle au bois dormant* ?



Logiques de graphes et de nombres

Les progrès dans l'étude des graphes ou des nombres entiers conduisent à des résultats profonds dont la difficulté logique étonne : pourquoi faut-il tant de temps et parfois des démonstrations de plusieurs milliers de pages pour que ces structures nous livrent leurs secrets ? Les raisons mystérieuses des mondes combinatoires et finis sont un sujet de perplexité que des générations de chercheurs acharnés ne réussissent qu'à effleurer tant ce qui s'y trame est subtil et délicat.

Une propriété cachée des graphes

Le travail d'un mathématicien est autant de formuler de nouvelles vérités du monde abstrait que de les démontrer. Le théorème des mineurs énonce une caractéristique importante des graphes. La longueur extravagante de sa démonstration est une insondable énigme logique.

Le mathématicien Phil Davis a défendu que seuls les théorèmes superficiels avaient une démonstration simple et courte, et que les vérités profondes étaient «naturellement» difficiles à débusquer. Le théorème des mineurs est l'un de ces résultats profonds et extrêmement difficiles à démontrer. Énoncé il y a plus de 30 ans par un groupe de mathématiciens autour de Klaus Wagner, sa démonstration ne fut terminée qu'en 2004. Elle occupe environ 500 pages et est principalement due à Neil Robertson et Paul Seymour. Ce nouveau théorème est considéré comme un des plus importants de la théorie des graphes.

Un graphe est un ensemble de points nommés nœuds reliés par des arcs (ou arêtes) et le théorème des quatre couleurs est le plus célèbre de la théorie des graphes. Bien que la démonstration du théorème des mineurs soit non constructive (elle établit l'existence d'objets, sans expliquer comment les construire), ses conséquences algorithmiques sont très générales. Grâce à ce théorème, les mathématiciens ont prouvé qu'une vaste famille de problèmes appartient à la classe P des problèmes traitables en temps polynomial (c'est-à-dire efficacement), ce qui, dans bien des cas, n'est pas évident du tout.

Il a pour origine un joli théorème graphique et concret que beaucoup d'amateurs de jeux connaissent: le théorème de Kazimierz Kuratowski (1896-1980). Ce dernier stipule que les graphes planaires, c'est-à-dire pouvant être dessinés sur un plan sans croisement des arcs, sont exactement les graphes qui ne «contiennent» aucune des deux formes K_5 et $K_{3,3}$ (voir ces graphes sur la figure 1). En Russie, le théorème de Kuratowski est nommé «théorème de Pontryagin-Kuratowski», car le mathématicien Lev Pontryagin (1908-1988) l'aurait découvert avant Kuratowski, mais aurait négligé de le publier.

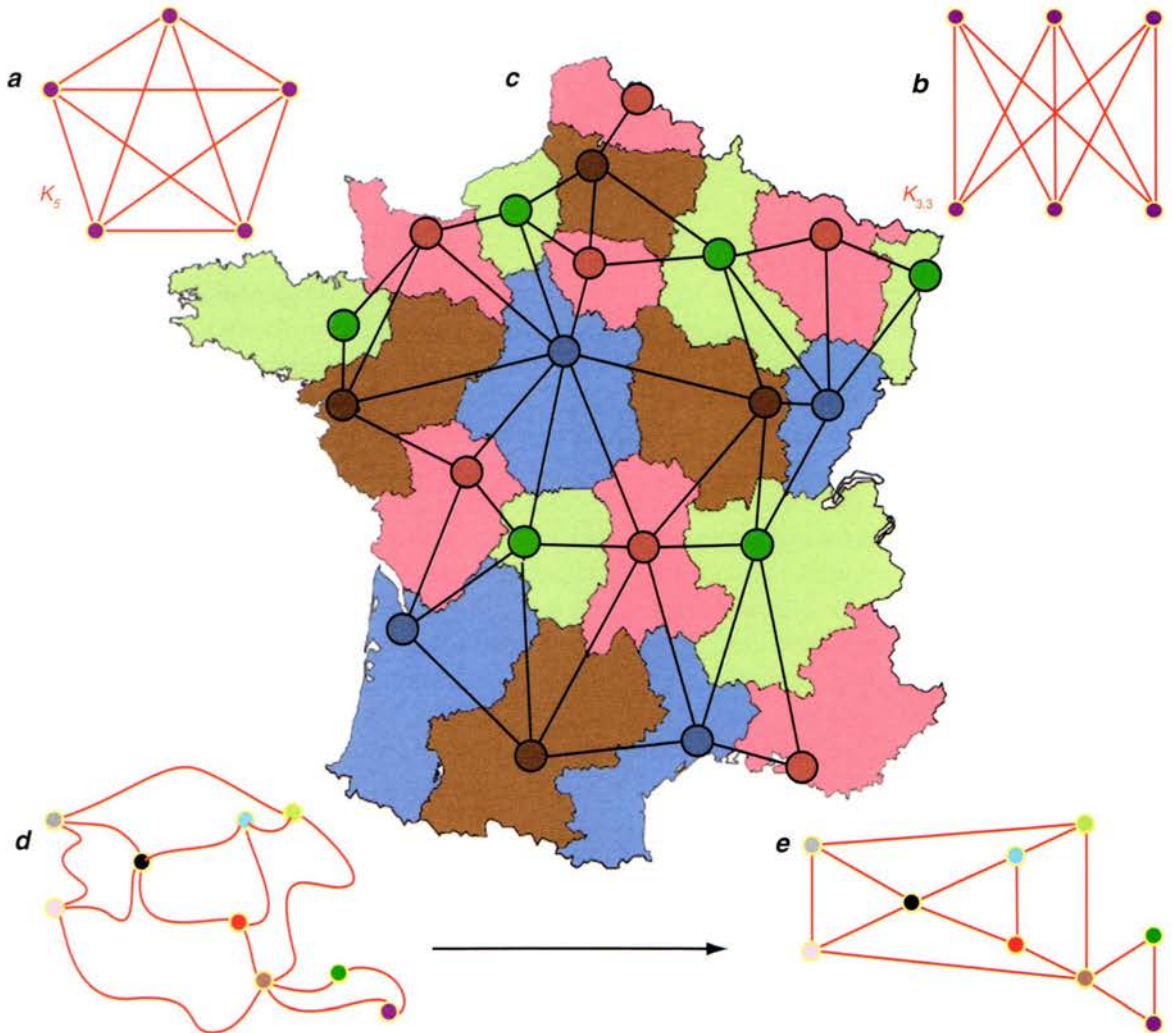
Le théorème des mineurs

Avant d'énoncer le théorème des mineurs, nous allons nous familiariser avec les graphes pour en goûter l'intérêt. Les graphes que nous considérons ici sont non orientés, l'arête ab entre les nœuds a et b ne se distinguant pas de l'arête ba ; les arcs ne forment pas de boucle (il n'y a pas d'arc de type aa) et entre deux nœuds a et b , on ne s'autorise à placer l'arc ab qu'une seule fois.

Pour énoncer le théorème de Robertson et Seymour, il faut préciser ce qu'on entend par *graphe contenu dans un autre*. Le graphe G est un mineur du graphe G' , si en partant de G' et en le réduisant par les opérations de (a) suppression d'une arête, (b) contraction

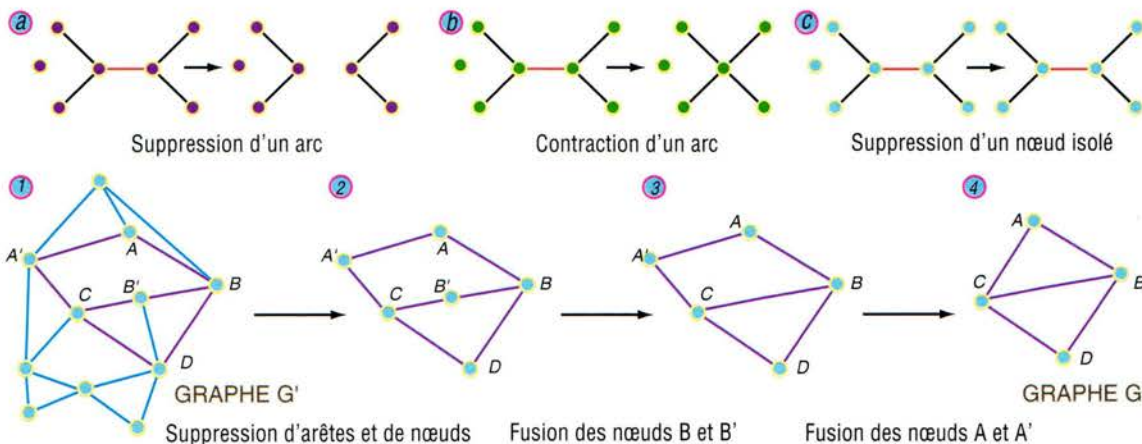
d'une arête (les deux nœuds aux extrémités de l'arête choisie sont fusionnés) ou suppression d'un nœud isolé (c), on obtient G (voir la figure 2). Ces opérations réduisent toujours la taille d'un graphe, mais ne permettent évidemment pas de réduire un graphe à n'importe quel graphe ayant moins de nœuds et moins d'arêtes.

Muni de cette notion, le théorème de Robertson et Seymour s'exprime en 14 mots : Dans toute suite infinie de graphes, l'un est le mineur d'un autre. Ou en s'autorisant plus de mots : À chaque fois qu'une suite infinie de graphes $G_0, G_1, \dots, G_n, \dots$ est donnée, il est possible de trouver deux graphes G_i et G_k (avec i différent de k) tels que G_i est un mineur de G_k .



1 Les graphes planaires sont tracés sur la surface d'un plan sans que jamais deux arêtes se croisent. Les graphes K_5 (a) et $K_{3,3}$ (b) ne sont pas planaires et le théorème de Kuratowski affirme qu'un graphe est planaire si et seulement si on n'y trouve ni K_5 ni $K_{3,3}$. Le plus célèbre théorème de la théorie des graphes indique qu'on peut toujours colorier une carte sans que deux pays voisins aient la même couleur en

n'utilisant que quatre couleurs, tout comme on peut colorier (avec quatre couleurs) les nœuds d'un graphe planaire de façon qu'il n'y ait pas deux nœuds reliés de la même couleur (c) (le théorème des quatre couleurs se généralise aux graphes sans mineur K_5). Le théorème de Fary-Wagner indique que tout graphe planaire peut être dessiné avec des segments de droite non sécants (d donne e).



2 Le graphe G est un mineur du graphe G' si, en réduisant le graphe G' par des opérations (a), (b) ou (c), on obtient G. Il n'est pas toujours facile d'observer qu'un graphe est le mineur d'un autre. Le graphe G illustré ici est un mineur de G' (sa structure est « à l'intérieur » de G').

Le sens du théorème est que dans toute famille infinie de graphes, il y en a au moins deux dont les structures sont intimement liées puisque l'un se déduit de l'autre par utilisation des opérations (a), (b) et (c). C'est vraiment là un résultat profond concernant la variété des structures qu'on peut rencontrer dans le monde mathématique des graphes.

Il faut d'ailleurs noter que l'affirmation qu'il y a deux graphes (G_i, G_k) , avec i différent de k , dont l'un est un mineur de l'autre, entraîne immédiatement qu'il existe une infinité de couples différents (G_i, G_k) , avec i différent de k , tels que G_i est un mineur de G_k . En effet, quand on a trouvé un couple de tels graphes, on les enlève de la suite infinie (qui reste infinie!), on applique à nouveau le théorème, on trouve donc un second couple de graphes dont l'un est le mineur de l'autre, puis on l'enlève, on en trouve un troisième, etc.

Cette propriété des graphes est surprenante, car il n'existe pas de théorème équivalent pour les sous-ensembles finis de nombres entiers : il est en effet possible de définir une suite infinie de sous-ensembles de nombres $E_1, E_2, \dots, E_n, \dots$ tels qu'aucun n'est une partie d'un autre (au sens habituel de l'inclusion d'ensembles). Il suffit par exemple de considérer $E_1 = \{0, 1\}$, $E_2 = \{1, 2\}$, $E_3 = \{2, 3\}$, etc.

Minoration et obstruction

On trouve aussi facilement une infinité de fonctions de $\mathbb{R}$ (l'ensemble des nombres réels) dans $\mathbb{R}$, sans qu'aucune ne soit plus petite qu'une autre (f est plus petite que g si $f(x)$ est inférieur à $g(x)$ pour tout x). On prend par exemple les fonctions $f_0, f_1, f_2, f_3, \dots$ définies par : $f_n(x) = (x - n)^2$.

Ainsi, il existe une infinité d'ensembles d'entiers deux à deux « non comparables », il existe une infinité de fonctions deux à deux « non comparables », mais il n'existe pas d'infinité de graphes deux à deux « non comparables » !

Sous sa première forme, le théorème de Robertson et Seymour est magnifiquement simple, mais sans doute un peu abstrait, et à vrai dire, pas très commode d'utilisation... La

seconde forme du théorème – qui permettra de comprendre le lien avec le vieux résultat de Kuratowski – est plus concrète et c'est elle qui a des conséquences dans le domaine de l'algorithmique des graphes. Pour l'énoncer, abordons les notions d'ensemble « stable par minoration » et d'« ensemble d'obstructions ».

Un ensemble E de graphes est dit stable par minoration (ou clos par mineur) si tout mineur d'un graphe de E est lui-même dans E .

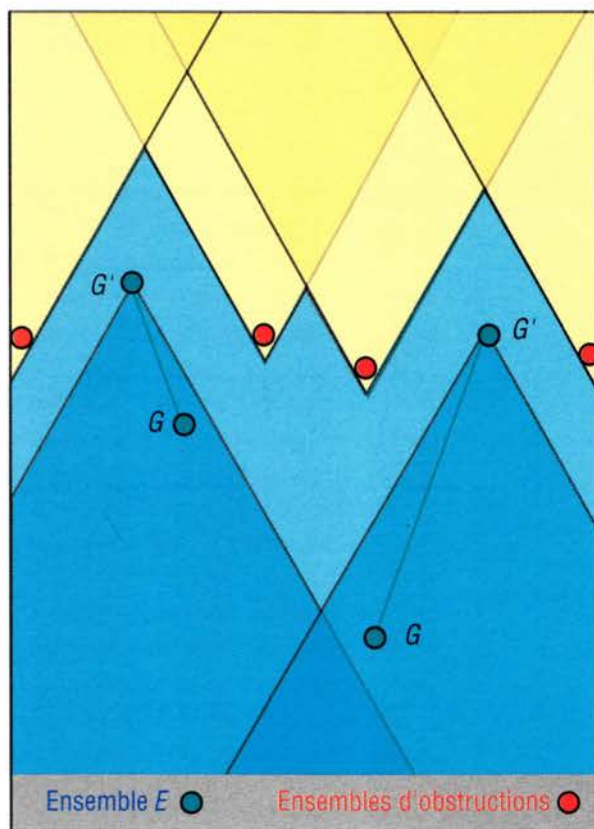
L'ensemble des graphes planaires est stable par minoration. En effet, si on prend un graphe dessinable sans croisement d'arêtes sur un plan et qu'on lui applique une des opérations (a), (b) ou (c), il est clair que le graphe obtenu est encore dessinable sur un plan sans croisement d'arêtes : ni la suppression d'arêtes ou de nœuds isolés ni la contraction d'arêtes n'obligent des arêtes qui ne se croisaient pas à se croiser, et donc tout graphe obtenu à partir d'un graphe planaire en effectuant une ou plusieurs fois les opérations (a), (b) ou (c) est encore un graphe planaire.

Similairement, si l'on considère l'ensemble des graphes dessinables sans croisement d'arêtes sur un tore (ou sur une bande de Möbius ou sur n'importe quelle surface aussi compliquée soit-elle), il est évident, par le même raisonnement, qu'il s'agit encore d'un ensemble de graphes stables par minoration. La stabilité par minoration est courante : de nombreuses catégories de graphes sont stables par minoration (voir l'encadré 5).

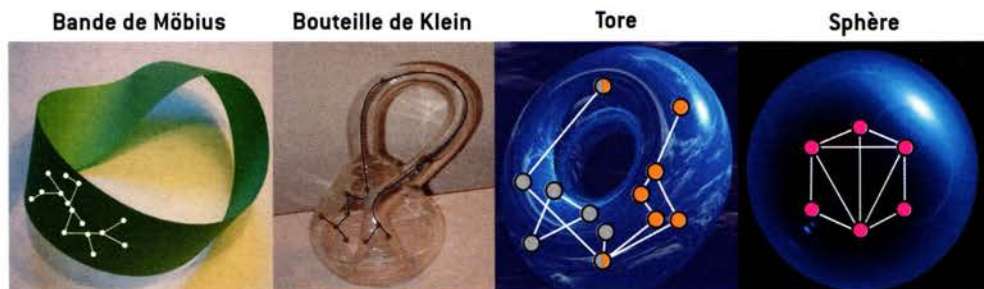
Seconde forme du théorème de Robertson et Seymour

Un ensemble de graphes E peut être défini par la donnée de graphes interdits : on ne veut pas que tel ou tel graphe soit un mineur des graphes de E . L'ensemble des graphes planaires, d'après le théorème de Kuratowski, est définissable de cette façon : les graphes planaires sont les graphes n'ayant aucun des graphes K_5 ou $K_{3,3}$ comme mineurs.

La seconde forme du théorème de Robertson et Seymour est justement l'affirmation que ce qui se produit pour les graphes planaires, stables par minoration et définissables par interdiction, est général. Voyons cette seconde forme : *Tout ensemble E de graphes stables par minoration est définissable comme l'ensemble des*



3 Dans toute suite infinie de graphes, l'un est mineur d'un autre, énonce le théorème de Robertson et Seymour. Pour visualiser le théorème, représentons un ensemble E de graphes par un rectangle. Chaque point représente un graphe et la relation « G est un mineur de G' » est symbolisée par « G est dans le cône en dessous de G' » : un ensemble stable par minoration est une partie du plan qui, dès qu'il contient un point, contient aussi tout le cône sous ce point. L'ensemble bleu est stable par minoration. La première forme du théorème des mineurs signifie qu'on ne peut pas trouver une infinité de points sans que l'un au moins soit situé dans le cône d'un autre. Si un ensemble est stable par minoration, alors on peut aussi trouver un nombre fini de points rouges [les graphes constituant l'ensemble d'obstructions] de façon que E est l'ensemble des points-graphes dont le cône ne contient jamais de point-graphe rouge.



4 Un ensemble E de graphes est stable par minoration si, lorsque G est un graphe de E , tous les mineurs de G sont aussi dans E . Si S est une surface fixée (un plan, un tore, une sphère, une bande de Möbius, etc.), l'ensemble des graphes qu'on peut y dessiner sans croisement d'arêtes est stable par minoration.

graphes n'ayant pour mineur aucun des graphes d'une liste finie, caractéristique de E , et appelée ensemble d'obstructions de E .

L'ensemble d'obstructions des graphes planaires est K_5 , $K_{3,3}$ et pour chaque ensemble E de graphes stable par minoration, il existe un ensemble d'obstructions fini analogue qui est propre à E .

La famille des graphes appelés forêts (chaque graphe de cette famille est une juxtaposition d'arbres) est stable par minoration, elle est donc définissable par obstructions; on montre que l'ensemble d'obstruction des forêts est constitué du seul graphe K_3 (le graphe à trois nœuds a, b, c et trois arêtes ab, bc, ca).

La démonstration que les deux formes du théorème de Robertson et Seymour sont équivalentes n'est pas évidente, mais elle tient en une page. La vraie difficulté qui a nécessité 500 pages de raisonnements et de calcul reste mystérieuse. Précisons quand même que la démonstration donnée introduit des outils et concepts dont l'utilité va au-delà de la simple preuve du théorème des mineurs et que, comme on le souhaite toujours dans une démonstration, ce qu'on apprend sur le chemin est aussi important que le point d'arrivée.

La force et l'intérêt de la seconde forme du théorème résultent en particulier qu'on en tire immédiatement des conséquences algorithmiques.

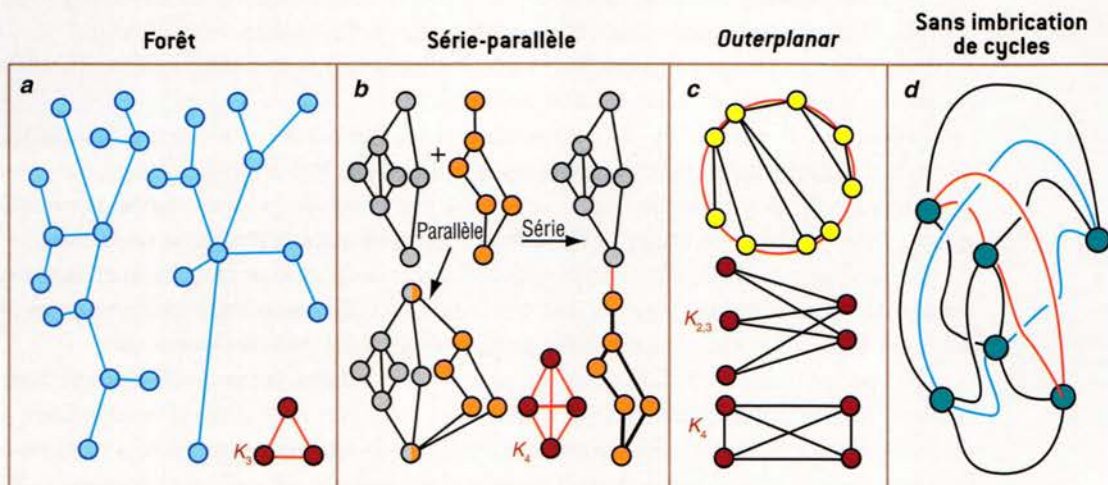
Il existe un algorithme rapide...

On sait en effet tester rapidement si un graphe contient un graphe fixé G comme mineur. Des méthodes réalisant ce test ne prennent qu'un temps t proportionnel environ à n^3 , n étant la taille du graphe testé. Il en va de même si, au lieu d'un mineur, on doit tester un nombre fini et fixé de mineurs, car un nombre fini d'algorithmes fonctionnant en un temps proportionnel à n^3 , exécutés consécutivement, donne un algorithme fonctionnant aussi en un temps proportionnel à n^3 .

Pour tester si un graphe G appartient à un ensemble E stable par minoration, on sait donc grâce à la deuxième version du théorème de Robertson et Seymour qu'il existera toujours un algorithme efficace en n^3 . On déterminera les graphes de l'ensemble d'obstructions de E , puis on vérifiera qu'aucun de ces graphes n'est un mineur du graphe G . On peut ainsi savoir si un graphe est planaire en temps proportionnel à n^3 .

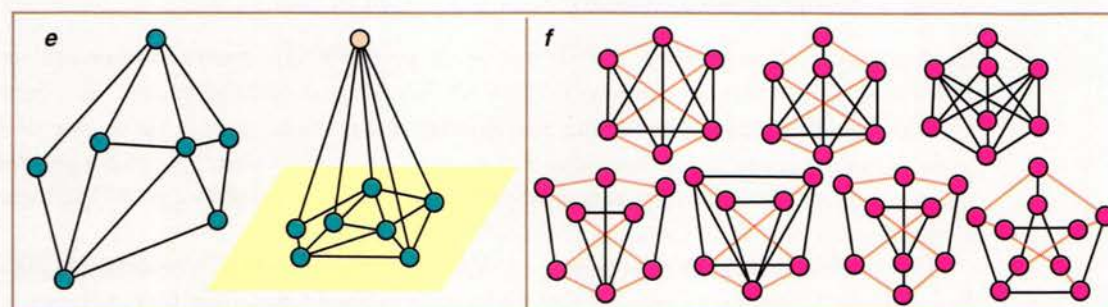
5. Petite zoologie des graphes stables par minoration

En plus des exemples d'ensembles de graphes stables par minoration présentés figure 4, en voici cinq autres qui prouvent l'intérêt de la notion.



Les forêts : un arbre est un graphe d'un seul tenant sans cycle (a), une forêt est un graphe composé d'un ou plusieurs arbres. Un graphe est une forêt si et seulement s'il ne possède pas K_3 comme mineur. Un graphe est « série-parallèle » (b) si on l'obtient en partant de graphes élémentaires ayant un seul nœud ou une arête liant deux nœuds et en opérant une ou plusieurs fois les opérations de mise en parallèle, de mise en série ou de simples juxtapositions (comme les forêts à partir des arbres). Un graphe est série-parallèle si et seulement s'il ne contient pas K_4 comme mineur. Un graphe est *outerplanar* (c) s'il

est possible de le dessiner sur le plan sans croisement, en plaçant tous les nœuds sur un cercle et cela de façon que les arêtes soient toutes à l'intérieur du cercle (tout arbre est *outerplanar*). Un graphe G est *outerplanar* si et seulement si ni $K_{2,3}$ ni K_4 ne sont des mineurs de G . Dans le graphe (d), les cycles bleu et rouge sont imbriqués. Un graphe est *sans imbrication de cycles* si on peut arranger ses nœuds et ses arêtes dans l'espace de façon que jamais deux cycles du graphe soient imbriqués : la famille des graphes sans imbrication de cycles est stable par minoration.



Les graphes planaires sont sans imbrication de cycles et si on prend un graphe planaire (e) et qu'on relie chaque nœud du graphe à un nœud en dehors du plan, on obtient un graphe sans imbrication de cycles. On montre qu'un graphe G est sans imbrication de cycles si et seulement si aucun des sept graphes dessinés en f (constituant l'ensemble de Petersen) n'est un mineur de G . Les graphes *sans cycle noué* sont ceux que l'on peut placer dans l'es-

pace sans que jamais les arêtes d'un cycle fassent un nœud autre que la simple boucle. Ils constituent un ensemble de graphes stable par minoration. On ne connaît pas de caractérisation de ces graphes en termes de mineurs interdits, comme c'est le cas pour les familles précédentes. Pourtant, on sait qu'une telle caractérisation par mineurs interdits existe, d'après le théorème de Robertson et Seymour.

Ce n'est pas une nouveauté et on sait même faire mieux puisqu'on connaît des algorithmes linéaires (fonctionnant en temps proportionnel à n) testant si un graphe est planaire. Comme nombre d'algorithmes de théorie des graphes, ils sont utiles pour la conception et le dessin des circuits VLSI (*Very Large Scale Integration*: circuit intégré à très grande densité). Mais le théorème de Robertson et Seymour est intéressant, car d'application très générale: pour toute surface S , quelle qu'elle soit, il indique qu'on peut savoir en un temps proportionnel à n^3 au plus, si un graphe pourra être dessiné sur S sans croisement d'arêtes. Et ça, c'est nouveau!

Cependant, il y a un hic, et l'enthousiasme suscité auprès des programmeurs à la recherche d'algorithmes efficaces pour les graphes doit être tempéré. Pour trouver un algorithme polynomial testant l'appartenance à une classe de graphes stables par minoration, il faut d'abord identifier l'ensemble d'obstructions caractéristique de la classe.

Or justement, c'est là qu'il y a un problème. La démonstration de Robertson et Seymour est une démonstration non constructive: elle conduit à l'affirmation qu'il existe toujours un ensemble d'obstructions, mais elle ne fournit pas de procédé pour le déterminer.

Cela pourrait être secondaire, car on espérerait se débrouiller pour chaque cas particulier et finalement découvrir par des méthodes *ad hoc* les ensembles d'obstructions. Il se trouve que ce n'est pas simple et que la difficulté de trouver les ensembles d'obstructions est réelle. Nous sommes dans la situation de celui qui sait qu'il y a un trésor caché quelque part (c'est ce que dit le théorème de Robertson et Seymour pour chaque ensemble stable par minoration), mais qui ne sait pas où précisément se trouve le trésor, ni même comment s'en approcher.

M. Fellows, M. Langston, R. Downey et B. Courcelle ont démontré qu'on n'automatiserait jamais l'utilisation du théorème des mineurs: il n'existe pas d'algorithme permettant de calculer l'ensemble des mineurs à partir de la définition d'une classe de graphes stable par minoration, et ce, que la définition soit donnée par un programme de test ou qu'elle soit donnée par une formule logique.

Insaisissables ensembles

Cette situation étrange nous fait douter de la possibilité de trouver facilement des ensembles d'obstructions. Cependant, les mathématiciens aiment relever des défis. Considérons l'exemple en apparence parfaitement élémentaire du tore (la surface d'un pneu). On est aujourd'hui incapable de déterminer l'ensemble d'obstructions des graphes qu'on peut y dessiner sans croisement d'arêtes (ensemble de graphes qui est stable par minoration comme nous l'avons mentionné).

Des études menées sur ce problème par Wendy Myrvold et John Chambers en 2002 ont conduit à l'étonnant résultat que l'ensemble d'obstructions du tore contient au moins 16 629 graphes! Pour le plan, l'ensemble d'obstructions possède deux éléments, K_5 et $K_{3,3}$, pour le tore, il en faut des milliers!

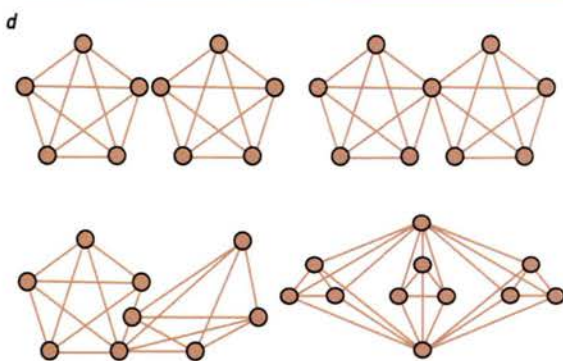
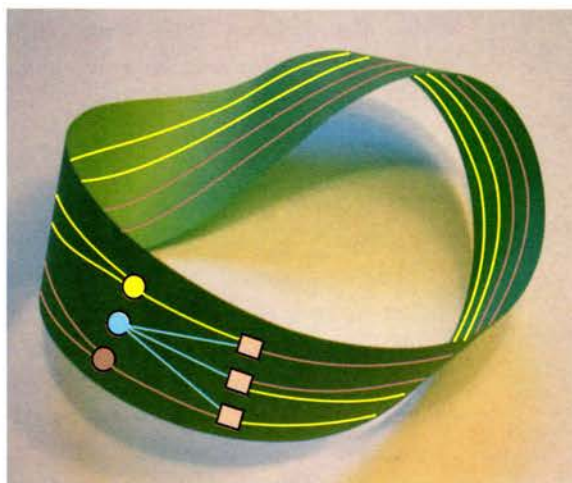
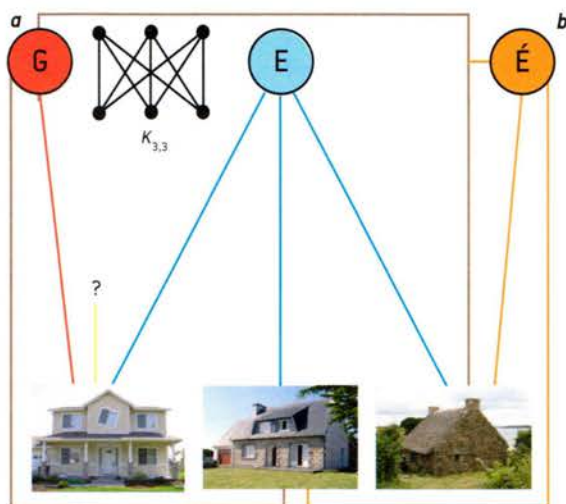
Une thèse de Jennifer Woodcock, de l'Université de Victoria, consacrée au problème des algorithmes testant si un graphe peut être dessiné sur un tore, ne propose finalement qu'un algorithme exponentiel en temps. Un algorithme linéaire a bien été trouvé, mais il semble si difficile à programmer qu'il est inutilisable.

Nous sommes dans un domaine où finalement il faut distinguer trois types de résultats algorithmiques: 1) ceux indiquant qu'un algorithme existe pour une tâche donnée;

2) ceux formulant précisément l'algorithme pour la tâche; 3) ceux conduisant à l'écriture d'un programme réalisant la tâche.

Pour le dire autrement, l'effectivité peut être existentielle, théorique ou réelle et seule bien sûr la troisième est susceptible d'utilisations concrètes!

La situation est désagréable et le contraste entre le plan (obstruction avec deux graphes seulement, algorithme linéaire utilisable en pratique) et le tore (ensemble d'obstructions inconnu, et programmes exponentiels) est ahurissant. La surface d'un tore est l'une des plus simples qu'on puisse imaginer!



E Le graphe $K_{3,3}$ (a) ne peut être dessiné dans le plan sans croisement d'arêtes: le problème est analogue à l'impossible approvisionnement en eau, gaz et électricité de trois maisons sans intersection des canalisations. Toutefois, ce graphe $K_{3,3}$ peut être dessiné sans intersection sur la bande de Möbius (b). D'après le théorème de Robertson et Seymour, chacun des ensembles de graphes définis par une surface élémentaire est caractérisé par un ensemble d'obstructions (les graphes ayant pour mineur un des graphes de l'ensemble d'obstructions ne font pas partie de l'ensemble). Pour le carré ou l'anneau, l'ensemble d'obstructions est K_5 et $K_{3,3}$. Pour le ruban de Möbius et le plan projectif (une

demi-sphère dont le cercle du pourtour est cousu sur un côté limitant une bande de Möbius), Dean Archdeacon a réussi (non sans mal) à établir que l'ensemble d'obstructions est constitué de 35 graphes. Pour le tore et pour la bouteille de Klein, personne n'a encore réussi à trouver l'ensemble d'obstructions. On sait juste que pour le tore (c), il contient plusieurs milliers de graphes. Un résultat partiel a été découvert récemment par Andrei Gagarin, Wendy Myrvold, John Chambers: l'ensemble des graphes qu'on peut dessiner sans croisement sur le tore et n'ayant pas pour mineur $K_{3,3}$ a pour ensemble d'obstructions les quatre graphes montrés en d.

Heureusement le cas de ce qu'on nomme le plan projectif et celui, équivalent, de l'anneau de Möbius sont moins décevants. L'anneau de Möbius s'obtient en prenant une bande de papier dont on colle les deux bouts après avoir fait faire un demi-tour à l'un des bouts. Le plan projectif est une des surfaces les plus simples dans la classification topologique des surfaces; on l'obtient en «cousant» le pourtour d'un ruban de Möbius sur le cercle-frontière d'une demi-sphère. La difficulté est que la visualisation dans l'espace habituel de cette surface comporte des intersections: la surface se traverse elle-même (*voir la figure 1*). Ces deux surfaces possèdent le même ensemble d'obstructions, composé de 35 graphes bien identifiés, découvert en 1980 par Dan Archdeacon. On connaît donc un algorithme (qu'on peut programmer) qui détermine en temps n^3 si un graphe peut être dessiné sans croisement d'arêtes sur l'anneau de Möbius ou le plan projectif.

Pour la bouteille de Klein, qui est une surface presque aussi élémentaire que le tore, à nouveau c'est l'inconnu: il y a un ensemble fini d'obstructions, mais il résiste à toute identification.

Malices

Tout se passe comme si le monde mathématique nous faisait des farces. Moyennant un très long et difficile raisonnement, il accepte de nous dire que, pour le tore comme pour le plan, il existe un algorithme en n^3 et facile à programmer indiquant quels sont les graphes qu'on peut y dessiner sans croisement d'arêtes, mais il ne nous le donne pas, et tout porte à croire que le trouver est à nouveau un difficile travail. Parfois même, on croit trouver un algorithme efficace, mais il se révèle impossible à mettre en œuvre du fait de sa complexité. L'existence d'algorithmes polynomiaux dont on croyait qu'elle déterminait la frontière entre le faisable et l'infaisable n'est finalement pas le critère ultime pour qu'un résultat mathématique soit pratiquement utilisable: à y regarder de près, cette frontière semble se diviser en zones dont la connaissance et la compréhension demanderont beaucoup de travail et de temps. La structure logique du réel mathématique résiste à nos tentatives de réduction.

Graphes et algorithmes pour ballons

Les sculptures réalisées avec des ballons sont à l'origine d'un nouveau domaine de recherche mathématique : l'algorithmique des ballons. Étonnamment, certains concepts de logique mathématique y sont importants.

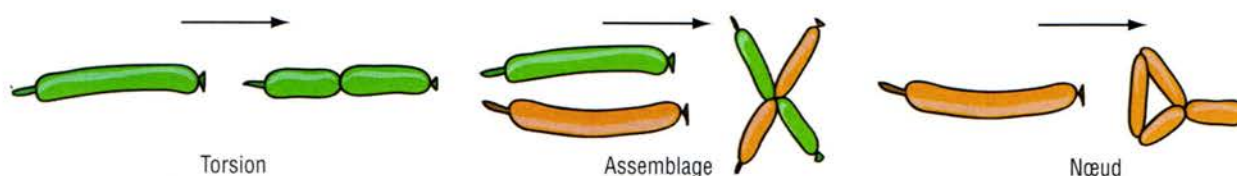
Les mathématiques sont partout : la théorie des graphes et la théorie du calcul s'immiscent dans des domaines où personne n'imaginait qu'elles avaient quelque chose à apporter. Il y a quelques années, Erik Demaine, Martin Demaine et Vi Hart ont proposé une analyse des questions mathématiques que soulève l'assemblage des ballons. Cette discipline, mineure, mais qui plaît aux enfants, est pratiquée dans les numéros de music-hall. Les artistes obtiennent des formes animales, des fleurs, des personnages, ou des polyèdres. Son analyse marque peut-être la naissance d'une nouvelle spécialité mathématique avec sa propre logique.

Histoire de ballons

Longtemps les ballons étaient faits avec des morceaux d'intestins ou de vessie prélevés chez les mammifères ou les poissons. Galilée gonflait des vessies de porc pour mesurer le poids de l'air. Les premiers ballons de football étaient faits eux aussi d'une vessie (de porc, de mouton ou de bœuf) gonflée et enserrée dans une surface de cuir composée de morceaux lacés afin d'en assurer la robustesse.

Grand progrès : en 1824, Michael Faraday fabrique des ballons en collant deux feuilles de caoutchouc l'une à l'autre et il les utilise pour mener des expériences sur l'hydrogène. Les ballons qui vont nous occuper sont ceux fabriqués d'un seul tenant toujours en caoutchouc, obtenu d'abord à partir de l'hévéa, puis synthétisé artificiellement ; ces ballons devinrent de fabrication courante à partir de 1930.

L'art de la sculpture avec des ballons, nommé *balloonerie*, est apparu aux États-Unis dans la première moitié du XX^e siècle, sans qu'il soit possible d'en déterminer avec précision la date de naissance. Le premier livre traitant du sujet est celui de Don Alan



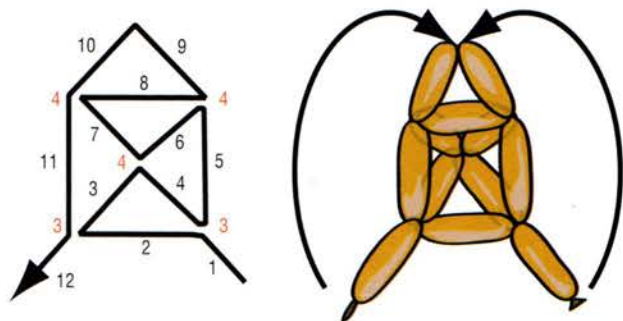
intitulé *Rubber Circus* imprimé en 1958 après un premier tirage limité ronéoté en 1952. Sur le Web, on peut toujours acheter cet ouvrage qui décrit bien sûr les modèles de base de tout artiste balloonneur : le petit chien et la girafe !

En France, des sculptures de ballons sont présentées au public à la fin des années 1950 par l'illusionniste Freddy Fah, suivi un peu plus tard par Jean Merlin qui en fait un numéro complet de cabaret. Les problèmes mathématiques que posent ces sculptures résultent des quelques opérations qu'on doit réaliser avec précision et sans faire éclater les ballons pour créer les structures désirées. Ces belles constructions ne sont possibles qu'avec des ballons robustes et colorés : les experts recommandent ceux de la firme *Qualatex* ou ceux de *Sempertex*, nouvel arrivant apprécié pour la résistance et la large gamme de couleurs de ses produits.

Réaliser une sculpture de ballons consiste à gonfler – partiellement le plus souvent –, puis tordre et nouer un ou plusieurs longs ballons de façon à obtenir des « segments » de ballons dont les extrémités sont liées et dont l'ensemble évoque une forme, animale ou autre. Certaines sculptures ne demandent qu'un seul ballon, d'autres en nécessitent plusieurs, parfois des centaines. Les ballons les plus fréquemment utilisés sont le ballon « 260 » (deux pouces de diamètre, 60 pouces de long) et le ballon « 160 » (un pouce de diamètre et 60 pouces de long).

Rappelons qu'un pouce vaut 2,6 centimètres. Les dessins de la page précédente montrent quelques manipulations simples avec un ou deux ballons.

Une manipulation délicate qui permet, en théorie, de tout faire avec un seul ballon consiste, après avoir opéré un certain nombre de torsions et nœuds délimitant des poches indépendantes, à provoquer l'éclatement de certaines poches qui disparaissent donc de la sculpture.



Graphes eulériens

À chaque sculpture en ballons est naturellement associé le graphe dont les arcs sont les « segments » de ballons, et dont les nœuds sont les points de rétrécissement obtenus par torsion et nouage des ballons. Un graphe étant donné, représentant par exemple un motif décoratif, plusieurs questions naturelles se posent : chacune donne lieu à un théorème de la « théorie mathématique des ballons ».

Considérons d'abord le problème des sculptures sans éclatement et avec un seul ballon que nous nommerons sculptures simples à un seul ballon. Quels sont les graphes qu'on peut réaliser de cette façon ?

La réponse est connue depuis longtemps, car le problème revient à trouver un parcours du graphe de la sculpture qui passe une et une seule fois par chaque arc du graphe. On retombe donc sur le célèbre problème où il s'agit de tracer une figure sans lever le crayon. Un tel parcours trouvé, la réalisation de la sculpture n'est plus qu'une question d'adresse et de patience pour qui dispose d'un ballon assez long (ce que nous supposons toujours). De tels parcours se nomment parcours eulériens, et l'on connaît la caractérisation des graphes où existe un tel parcours depuis 1736, date à laquelle le mathématicien suisse

Leonhard Euler (1707-1783) a résolu la question :

Théorème d'Euler. Un graphe connexe, c'est-à-dire d'un seul tenant, possède un parcours eulérien (et peut donc donner lieu à une sculpture simple avec un seul ballon) si tous les nœuds du graphe sont de degré pair (c'est-à-dire sont les extrémités d'un nombre pair d'arcs) sauf éventuellement deux d'entre eux qui sont alors nécessairement les extrémités du parcours (et donc du ballon dans la sculpture).

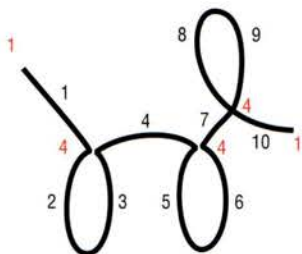
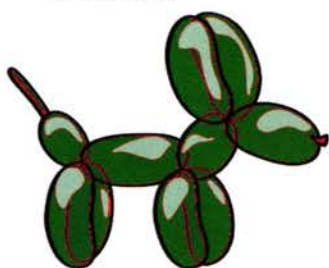
Si le graphe possède plus de deux nœuds de degré impair, il n'admet pas de parcours eulérien, car chaque nœud de degré impair consomme une extrémité du parcours. Un graphe qu'on peut parcourir sans répétition possède donc deux nœuds de degré impair si les extrémités du parcours sont distinctes, et zéro sinon (dans ce cas, on parle de «circuit» eulérien). Il est moins évident que si le nombre de nœuds de degré impair est 0 ou 2, alors le graphe admet un parcours eulérien (la démonstration utilise un raisonnement par récurrence sur le nombre d'arcs du graphe).

Le cube, qui possède six nœuds, chacun d'eux étant l'extrémité de trois arcs, ne peut pas être parcouru par un chemin sans répétition et n'est donc pas réalisable en sculpture sans éclatement avec un seul ballon.

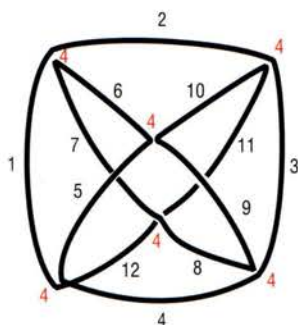
Le graphe du «petit chien», qui ne possède que des nœuds de degré pair (sauf l'extrémité de la tête et celle de la queue), est réalisable en sculpture sans éclatement à un seul ballon. L'octaèdre, qui possède six nœuds de degré 4, est réalisable en sculpture simple à un seul ballon.



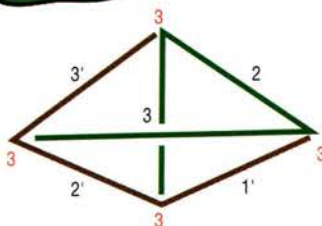
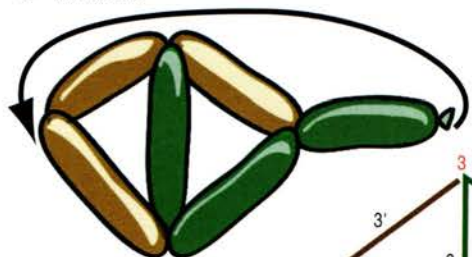
a Petit chien



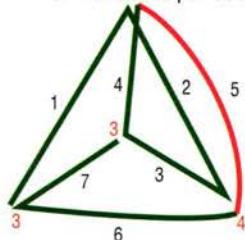
b Octaèdre



c Tétrahèdre



d Tétrahèdre par éclatement



1 Constructions avec un et deux ballons. Le célèbre « petit chien » [a] possède deux nœuds de degré impair (l'extrémité de la tête et l'extrémité de la queue). Il peut donc être construit avec un seul ballon. L'octaèdre [b] ne possède aucun sommet de degré impair, il peut être construit avec un seul ballon dont les extrémités seront nouées. En revanche, le tétraèdre a quatre sommets où trois segments se rencontrent [c] et ne peut être construit avec un seul ballon, il en faut deux. À moins que l'on triche en ajoutant un segment et en l'éclatant ensuite [d]...

Combien de ballons ?

Certains graphes intéressants – celui du cube par exemple – méritent quand même d'être réalisés en ballons. Quand un ballon ne suffit pas, combien au minimum en faut-il (toujours en s'interdisant la méthode des éclatements partiels) ?

La réponse, que nous allons détailler, est assez simple. Désignons par $2n$ le nombre de nœuds de degré impair du graphe. Ce nombre est écrit sous la forme $2n$, car il est nécessairement pair : un graphe possède un nombre pair d'extrémités d'arcs (le double du nombre d'arcs) et donc un nombre pair de nœuds de degré impair. La sculpture est réalisable sans éclatement avec n ballons et impossible à réaliser avec moins de n ballons.

Pour le cube, qui possède $8 = 2 \times 4$ nœuds de degré 3, il faut donc quatre ballons, ce que l'on vérifie sans peine. En s'y prenant bien, quatre ballons de même longueur donnent le graphe du cube.

La démonstration que, pour $2n$ nœuds de degré impair, n ballons au moins sont indispensables est évidente. En effet, à chaque nœud de degré impair, le balloonneur est obligé de placer une extrémité de ballon, ce qui lui demande donc au moins n ballons pour un graphe ayant $2n$ nœuds de degré impair.

Que n ballons suffisent toujours pour un graphe à $2n$ nœuds impairs demande un

petit raisonnement que voici. Soit un graphe avec $2n$ nœuds impairs, complétons-le en ajoutant des arcs reliant les nœuds impairs deux à deux sauf pour deux d'entre eux; cela demande $n - 1$ arcs exactement. Le graphe obtenu satisfait les conditions du théorème d'Euler et peut donc être parcouru sans répétition par un chemin unique. Considérons ce chemin. En enlevant (par la pensée ou par éclatement) les $n - 1$ arcs ajoutés à l'instant, on obtient n chemins (ou moins) et donc n ballons suffisent pour construire le graphe initial.

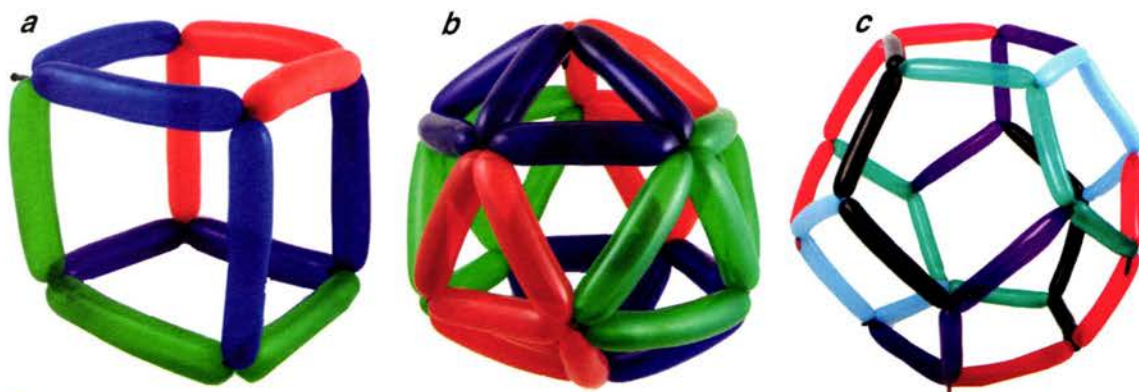
Ces premiers résultats envisagent uniquement des structures obtenues par un sculpteur qui ne veut pas pratiquer l'éclatement partiel des ballons qu'il manipule. Celui qui a appris à opérer ces éclatements contrôlés saura réaliser tout graphe connexe à l'aide d'un seul ballon: il ajoutera des arcs au graphe qu'il veut réaliser de façon à supprimer les nœuds de degré impair, puis, une fois construit le nouveau graphe avec un seul ballon (ce qui est possible puisqu'il n'y a plus de nœuds impairs), il fait éclater les segments de ballons correspondant aux arcs ajoutés et ce qui reste de sa sculpture est le graphe voulu.

Le facteur chinois

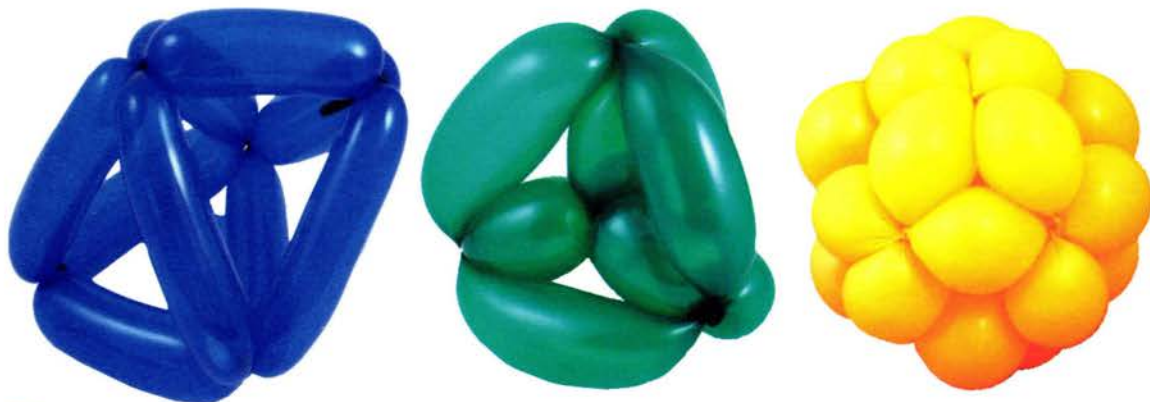
Ce balloonneur peut tout faire avec un seul ballon, mais on imagine qu'il voudra certainement minimiser la longueur totale des segments qu'il doit faire éclater lors de la phase finale de sa construction. Un graphe étant donné – ayant éventuellement un grand nombre de nœuds de degré impair – comment s'y prendre pour le construire avec un seul ballon, en faisant éclater une longueur aussi petite que possible de segments de ballon dans la phase finale de la manipulation?

La question est équivalente à celle-ci: comment parcourir en un seul chemin (comportant éventuellement des passages répétés sur un même arc) le graphe de la sculpture visée, complété éventuellement d'autres arcs que ceux de ce graphe, en passant par tous les arcs du graphe visé, et cela en empruntant un chemin dont la longueur totale est la plus petite possible?

En effet, une fois ce chemin minimal trouvé, le sculpteur de ballons réalisera le graphe correspondant avec un seul ballon, et fera éclater tous les segments de ballons



2 Les polyèdres platoniciens. Quand on s'interdit la méthode des éclatements partiels, l'octaèdre est le seul des cinq polyèdres platoniciens réalisable avec un seul ballon. Nous avons vu que le tétraèdre demande deux ballons, le cube quatre [a], l'icosaèdre six [b] et le dodécaèdre dix [c].



3 Quelques belles constructions avec un seul ballon, et une jolie sculpture composée de cinq tétraèdres emboîtés (les photographies de cette page et de la précédente ont été prises par Eric Demaine, Martin Demaine et Vi Hart).

correspondant aux arcs ajoutés. Le fait d'avoir le chemin de longueur minimal assure qu'il fait éclater une longueur minimale de segments de ballon.

Il se trouve que ce problème est connu en théorie des graphes sous le nom de *Problème du facteur chinois*, nom donné en l'honneur du mathématicien chinois Mei-Ku Kwan qui l'étudia en 1962. La méthode pour le résoudre consiste simplement à rechercher les arcs inutiles (qu'on va ajouter dans un premier temps, puis qu'on fera éclater) en les prenant parmi les arcs reliant deux à deux les nœuds de degré impair, jusqu'à ce qu'il ne reste plus que deux nœuds de degré impair. Il existe un grand nombre de façons différentes de mener l'ensemble de ces appariements, et chacune conduit à une perte de longueur de ballons qui lui est propre.

Ballons longs, ballons courts

La question est alors de découvrir le système d'appariements le plus économique. On sait traiter ce problème d'appariement en temps polynomial (c'est-à-dire par un algorithme dont le temps de calcul n'augmente pas trop vite en fonction de la taille des données), car il se ramène à un problème classique de recherche opérationnelle.

Le problème de la construction la plus économique d'une sculpture avec un seul ballon et des éclatements partiels possède donc une solution algorithmique satisfaisante. Celle-ci se généralise d'ailleurs sans peine au cas de la recherche de la construction la plus économique avec k ballons (k fixé) et éclatements.

D'autres questions encore se posent à l'artiste balloonneur et la théorie des graphes va l'aider à les résoudre.

Un résultat simple, mais peu connu, a été démontré par Anton Kotzig en 1957 et se révèle important pour les sculpteurs de ballons : tout graphe connexe ayant un nombre pair d'arcs, $2n$, se décompose en n couples de deux arcs ayant un sommet commun (autrement dit en n chemins de longueur 2). On peut le démontrer par récurrence comme pour le théorème d'Euler. Ce résultat signifie pour un sculpteur de ballons que toute sculpture d'un graphe de $2n$ arcs d'un seul tenant est réalisable en utilisant n ballons

qui donneront chacun deux arcs exactement. Si tous les arcs du graphe ont la même longueur (c'est par exemple le cas pour la réalisation des squelettes des polyèdres réguliers), alors le sculpteur peut mener sa construction avec n ballons ayant chacun la longueur de deux arcs (nous parlerons de *ballons doubles*).

Dans le cas d'un graphe ayant un nombre impair d'arcs, $2n + 1$, il résulte immédiatement du théorème précédent que sa réalisation demande n ballons doubles et un ballon simple (de longueur un arc) : on enlève un arc, on construit le graphe obtenu avec n ballons doubles, on complète le graphe avec le ballon simple.

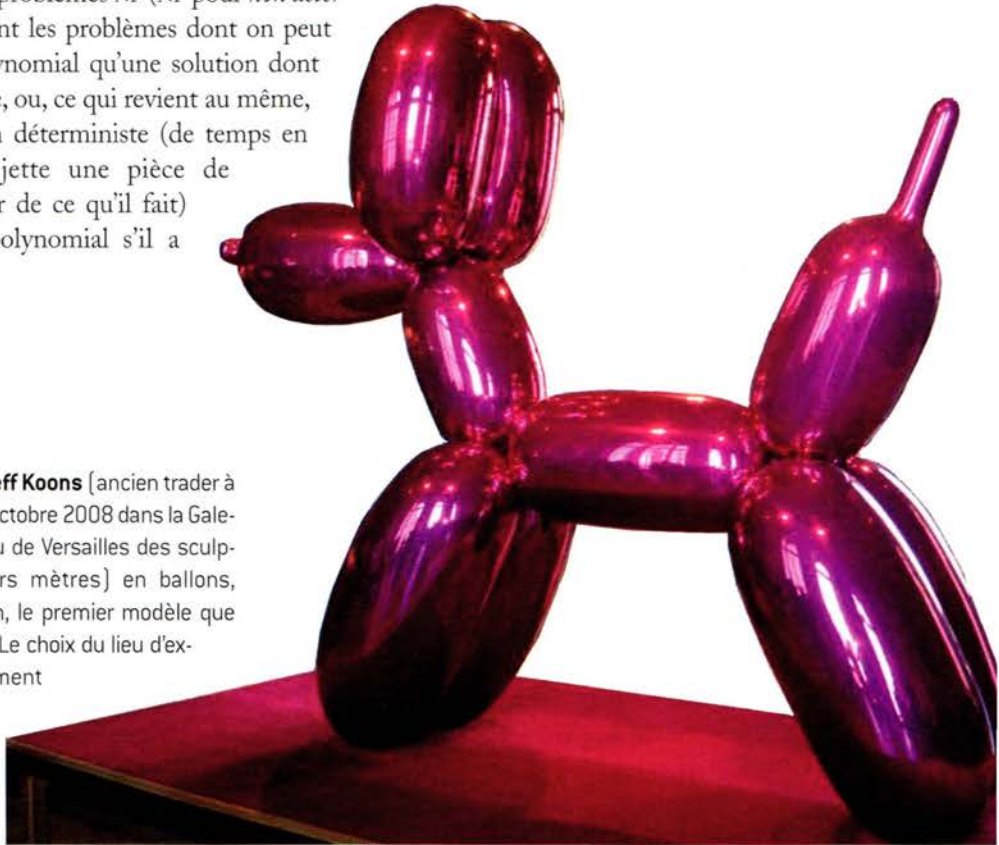
Ces décompositions d'un graphe avec des ballons doubles sont faciles à trouver à la main pour tout graphe ayant un petit nombre d'arcs, et l'on connaît même des algorithmes polynomiaux qui produisent ces décompositions si on souhaite s'attaquer à de grands graphes. Un artiste ballooneur dont le but est de tout réaliser avec des ballons doubles (et éventuellement un ballon de longueur 1, si c'est inévitable) a donc toutes les raisons d'être satisfait.

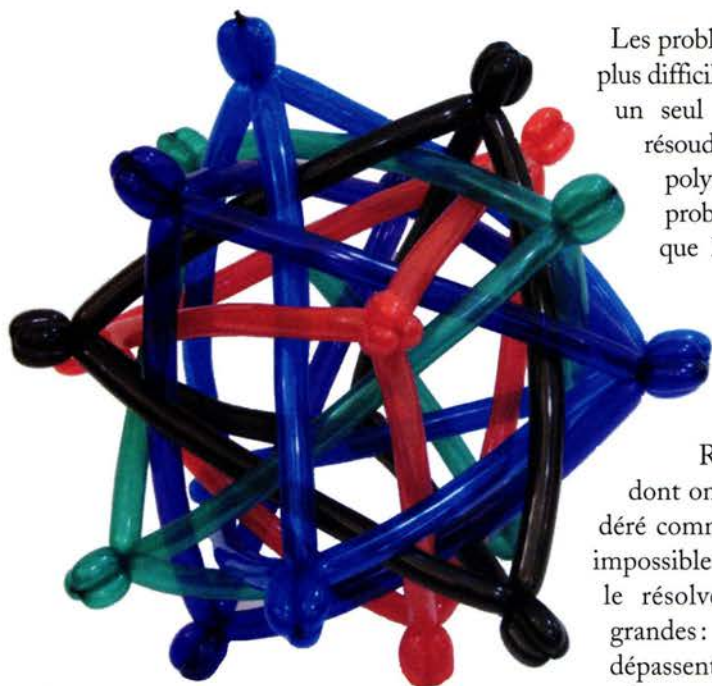
En revanche, la question posée pour les ballons doubles devient plus difficile pour les ballons triples, ou les ballons de longueur k (k fixé, $k > 2$). Un graphe étant donné (dont nous supposons que tous les arcs ont la même longueur), peut-on en faire la sculpture avec des ballons ayant tous la même longueur k ($k > 2$) ?

Pour que la réponse soit positive, il faut bien sûr que le nombre d'arcs du graphe soit un multiple de k , mais ce n'est pas suffisant en général et le problème de savoir si oui ou non il y a une décomposition en ballons de longueur k appartient à la catégorie des problèmes NP-complets (si $k > 2$).

Rappelons que les problèmes NP (NP pour *non déterministe polynomial*) sont les problèmes dont on peut vérifier en temps polynomial qu'une solution dont on dispose est correcte, ou, ce qui revient au même, qu'un algorithme non déterministe (de temps en temps l'algorithme jette une pièce de monnaie pour décider de ce qu'il fait) résoudra en temps polynomial s'il a une chance parfaite.

4 L'artiste américain Jeff Koons (ancien trader à Wall Street) a exposé en octobre 2008 dans la Galerie des glaces du château de Versailles des sculptures géantes (plusieurs mètres) en ballons, notamment le petit chien, le premier modèle que tout débutant assemble. Le choix du lieu d'exposition a été diversement apprécié...





5 Cinq tétraèdres emboîtés : il faut deux ballons par tétraèdre, donc, en tout, 10 ballons.

Les problèmes NP-complets sont les problèmes les plus difficiles de cette catégorie et savoir en résoudre un seul en temps polynomial permettrait de résoudre tous les autres problèmes NP en temps polynomial, ce que l'on considère comme peu probable. Démontrer que $P \neq NP$ (c'est-à-dire que les problèmes NP-complets ne peuvent pas être résolus en temps polynomial) ou l'inverse, démontrer que $P = NP$, rapportera un million de dollars, offert par l'Institut Clay, au premier mathématicien qui réussira.

Retenons seulement qu'un problème dont on a établi qu'il est NP-complet est considéré comme difficile et qu'en pratique, il devient impossible de faire fonctionner les algorithmes qui le résolvent dès que les données sont trop grandes : les temps de calcul des algorithmes dépassent tout ce qui est pratiquement faisable, même avec les ordinateurs les plus puissants disponibles.

La situation est donc la suivante : dans le cas général, un artiste balloonneur ne pourra pas en temps raisonnable déterminer si le graphe auquel il s'intéresse est oui ou non réalisable uniquement avec des ballons de longueur 3 (ou $k > 3$) : la malédiction de la complexité algorithmique le concerne et rend impossibles en pratique certaines tâches que tout le monde imaginait faciles avant d'y réfléchir.

En fait, E. Demaine, M. Demaine et V. Hart ont démontré un résultat plus fin encore. Même si l'on ne s'intéresse qu'aux graphes correspondant aux arêtes d'un polyèdre convexe ayant $2n$ nœuds de degré impair (ce qui implique qu'il faut au moins n ballons différents pour le sculpteur se refusant aux éclatements partiels), le problème de savoir s'il est possible ou non de le construire en n ballons de même longueur est NP-complet.

Plusieurs conjectures non résolues concernent ces problèmes de décomposition d'un graphe en chemins de longueur k (k fixé, $k > 2$) et c'est là un sujet de recherche actif en théorie des graphes qu'il faudra faire avancer si l'on veut que l'art de la balloonerie s'appuie sur une théorie mathématique vraiment satisfaisante.

Polyèdres

En regard de ces résultats plutôt négatifs concernant les constructions en ballons de longueurs identiques, les auteurs déjà mentionnés ont trouvé le résultat positif suivant :

- Tout polyèdre régulier platonicien (il y en a 5), ou tout polyèdre archimédien (il y en a 13) peut être réalisé avec des ballons de longueur égale et dont le nombre est ce qu'on peut faire de mieux, c'est-à-dire la moitié du nombre de nœuds de degré impair.

Rappelons que les polyèdres platoniciens ont, par définition, toutes leurs faces identiques à un même polygone régulier et tous leurs sommets identiques. Les polyèdres

archimédiens ont, eux, tous leurs sommets identiques, mais leurs faces qui sont aussi des polygones réguliers peuvent être différentes, comme c'est le cas pour l'icosaèdre tronqué qui est l'assemblage de 12 pentagones réguliers et de 20 hexagones réguliers et qui est la forme officielle du ballon de football telle que la FIFA (Fédération Internationale de Football Association) l'a fixée.

Les auteurs montrent qu'on peut toujours s'arranger, dans ces sculptures en ballons des polyèdres platoniciens et archimédiens, pour que les formes données aux ballons d'une construction soient géométriquement identiques et que les ballons d'une construction soient disposés de manière régulière. Cela donne bien sûr lieu à des travaux pratiques qui produisent de jolies sculptures.

Parmi les autres résultats de la théorie des sculpteurs de ballons, notons encore :

- Les polyèdres semi-réguliers des deux séries infinies les bipyramides (deux pyramides construites sur un polygone régulier, à n côtés, collées l'une à l'autre par leur base) et les antiprismes (deux polygones à n côtés et $2n$ triangles équilatéraux) peuvent toujours être fabriqués avec un seul ballon sans utiliser l'éclatement.

- Tout polyèdre convexe peut être réalisé avec un seul ballon (et sans éclatement) à condition d'ajouter un point central au polyèdre qui sera joint à tous les sommets de degré impair.

- Le cube et le dodécaèdre réguliers sont tous les deux faisables avec des ballons triples.

D'autres questions concernant en particulier les sculptures avec des ballons de longueurs identiques sont à l'étude et leurs réponses viendront bientôt, on l'espère, enrichir ce nouveau domaine des mathématiques ludiques qui peut intéresser aussi bien les jeunes enfants que les spécialistes de la théorie de la complexité, montrant, encore une fois, que des considérations introduites à l'origine en logique (celles portant sur les classes P, NP, NP-complets) concernent tout le monde.

Un terrain de course numérique

Certaines suites de nombres premiers semblent faire la course.
Comprendre qui gagne et pourquoi demande la mise en œuvre
de raisonnements mathématiques et logiques d'une étonnante subtilité.

Certaines questions mathématiques restent fermement bloquées malgré tous les efforts faits pour les résoudre. C'est le cas de l'hypothèse de Riemann qui concerne la densité asymptotique des nombres premiers. Énoncée il y a 150 ans, on attend toujours qu'elle devienne un théorème. D'autres questions sont moins abruptes : on n'en a pas de solutions complètes, mais elles s'éclairent lentement, et, de décennie en décennie, on en découvre les clefs et on en ouvre les portes. C'est le cas des « courses de nombres premiers » dont nous présentons une petite histoire.



Shutterstock/Nomad_Soul

Les nombres premiers impairs se classent en deux catégories : ceux de la forme $4n+1$ (divisés par 4, ils donnent le reste 1), soit, dans l'ordre, 5, 13, 17, 29, 37..., et ceux de la forme $4n+3$ (divisés par 4, ils donnent le reste 3), soit 3, 7, 11, 19, 23, 31...

Quelle équipe gagne ?

On parlera de l'équipe $[1 \bmod 4]$ pour la première catégorie de nombres premiers, et de l'équipe $[3 \bmod 4]$ pour la seconde. Notons qu'il ne peut pas y avoir de nombres premiers qui, divisés par 4, donnent le reste 0, car de tels nombres sont multiples de 4, ni de nombres premiers supérieurs à 2 qui, divisés par 4, donnent 2, car de tels nombres sont nécessairement pairs (en effet $4n+2 = 2(2n+1)$). Laquelle de nos deux équipes $[1 \bmod 4]$ et $[3 \bmod 4]$ gagne ?

Cette première formulation est imprécise. D'ailleurs, les deux équipes de nombres premiers sont toutes deux infinies et donc à égalité concernant la taille. Pour donner un sens à la question, il faut voir les deux équipes comme s'affrontant dans une course infinie et comparer les nombres de l'équipe $[1 \bmod 4]$ inférieurs à n , que nous noterons $[1 \bmod 4; n]$, à ceux de l'équipe $[3 \bmod 4]$ inférieurs à n , notés $[3 \bmod 4; n]$.

À l'instant n , les deux équipes peuvent être à égalité, ou l'une peut devancer l'autre. Pour $n = 20$, on a par exemple :

$$[1 \bmod 4; 20] = \{5, 13, 17\}$$

$$[3 \bmod 4; 20] = \{3, 7, 11, 19\}.$$

La seconde équipe mène par 4 à 3. Pour $n = 50$:

$$[1 \bmod 4; 50] = \{5, 13, 17, 29, 37, 41\}$$

$$[3 \bmod 4; 50] = \{3, 7, 11, 19, 23, 31, 43, 47\}.$$

La seconde équipe mène par 8 à 6. Quand on va jusqu'à $n = 100$, la seconde équipe l'emporte encore par 13 à 11. On note $\|1 \bmod 4; 100\| = 11$; $\|3 \bmod 4; 100\| = 13$. De manière générale, $\|r \bmod a; n\|$ désignera le nombre de nombres premiers inférieurs ou égaux à n , qui donnent le reste r quand on les divise par a .

Pour $n = 200$, la même équipe reste en tête par 24 à 21 : $\|1 \bmod 4; 200\| = 21$; $\|3 \bmod 4; 200\| = 24$.

La course se poursuit à l'infini (voir le tableau de la figure 1). La seconde équipe semble en tête de manière continue. C'est le mathématicien russe Pafnouti Tchebychev (1821-1894), dans une lettre datée du 23 mars 1853, qui en fit la remarque la première fois. Depuis, une multitude d'articles mathématiques ont été consacrés à ce problème et plus généralement aux courses entre nombres premiers.

L'observation du tableau montre que l'avance de l'équipe $[3 \bmod 4]$ n'est pas très grande et il n'est pas

1. La course

Résultats aux passages intermédiaires de la course entre le nombre de nombres premiers inférieurs à n de la série $4n+1$ et de la série $4n+3$. La série $4n+3$ fait la course en tête. Cela durera-t-il jusqu'à l'infini ?

n	$\ 1 \bmod 4; n\ $	$\ 3 \bmod 4; n\ $	écart
100	11	13	2
200	21	24	3
300	29	32	3
400	37	40	3
500	44	50	6
600	51	57	6
700	59	65	6
800	67	71	4
900	74	79	5
1000	80	87	7
2000	147	155	8
3000	211	218	7
4000	269	280	11
5000	329	339	10
6000	383	399	16
7000	442	457	15
8000	499	507	8
9000	554	562	8
10 000	609	619	10
20 000	1125	1136	11
50 000	2549	2583	34
100 000	4783	4808	25

2. Hypothèse de Riemann et marche aléatoire

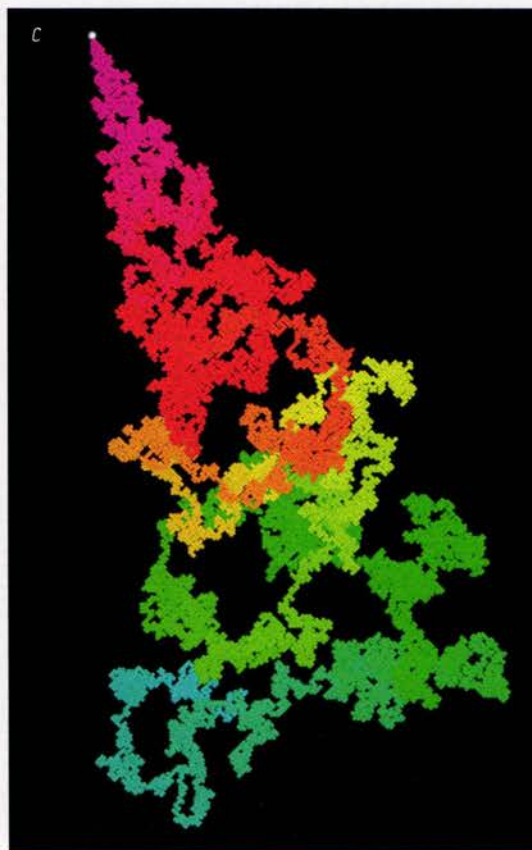
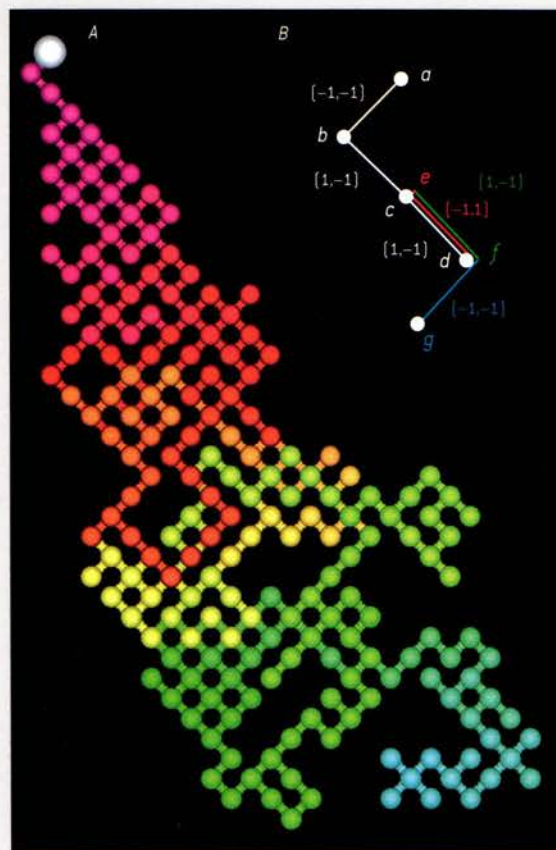
Dans son mémoire de 1859 sur les nombres premiers, Bernhard Riemann (1826-1866) rencontre une difficulté pour établir rigoureusement une propriété qui lui apparaît avoir des conséquences intéressantes. Il ne dispose que d'un argument incomplet et écrit: «Il est certain que nous aimerions avoir ici une démonstration plus rigoureuse. J'ai cependant provisoirement mis de côté cette recherche après avoir mené quelques tentatives inabouties, car cette démonstration ne semble pas indispensable à la poursuite de mon travail.»

Cent cinquante années plus tard, la communauté des mathématiciens est toujours à la recherche de cette démonstration laissée de côté par le grand mathématicien allemand. Voici un énoncé de l'hypothèse qui joue un rôle important dans l'histoire des courses de nombres premiers. Considérons la suite de Liouville $l(n)$ qui vaut $+1$ si l'entier n possède un nombre pair de facteurs premiers, et -1 si n possède un nombre impair de facteurs premiers. Exemples: le nombre 2 a 1 facteur premier, 1 est impair, donc $l(2) = -1$, le nombre 3 a 1 facteur premier, 1 est impair donc $l(3) = -1$, le nombre 4 a 2 facteurs premiers, 2 est pair, donc $l(4) = 1$; similairement, $l(5) = -1$, $l(6) = l(2.3) = 1$, $l(7) = -1$, $l(8) = l(2.2.2) = -1$,....

L'hypothèse de Riemann est simplement l'affirmation suivante: pour tout nombre strictement positif ϵ , la suite $[(1) + l(2) + \dots + l(n)]/n^{1/2+\epsilon}$ converge vers 0 quand n tend vers l'infini. Cet énoncé exprime que la parité du nombre de facteurs premiers d'un entier se comporte de manière semblable à une suite obtenue par des tirages à pile ou face au hasard. C'est une affirmation de l'aspect aléatoire du comportement des nombres premiers.

Jean-François Colonna a réalisé une représentation de la suite de Liouville pour les nombres de 2 à 1 000 à gauche (A) et de 3 000 à 100 000 à droite (C). Pour réaliser cette représentation, on prend la suite de Liouville et on regroupe deux par deux les termes, ce qui donne les vecteurs de déplacement d'un point au suivant. Ainsi pour aller de a à b , $l(2) = -1$ et $l(3) = -1$, on se déplace selon le vecteur $(-1;-1)$. Le début de la suite est représenté en (B): $(-1;-1)$, $(1;-1)$, $(1;-1)$, $(-1;1)$, $(-1;1)$, $(-1;-1)$, $(1;-1)$, $(1;-1)$... Notons que le trajet revient parfois en arrière.

La progression dans le mouvement est indiquée par la variation des couleurs. Les courbes ressemblent à une marche aléatoire et c'est ce qu'exprime l'hypothèse de Riemann.



certain qu'elle se creuse quand n augmente. Peut-on savoir que l'avance persiste et démontrer des résultats précis qui donnent un sens à cette observation empirique de Tchebychev?

Que l'avance de la seconde équipe ne devienne jamais très nette s'explique par le théorème des nombres premiers pour les progressions arithmétiques, qui fut conjecturé par le mathématicien français Legendre (1752-1833), puis démontré en 1837 par le mathématicien allemand Dirichlet (1805-1859) et enfin établi sous la forme qui nous intéresse en 1896 par le mathématicien belge De la Vallée Poussin (1866-1962).

En un combat douteux

Ce théorème stipule que si l'on considère une progression arithmétique $an+r$, (a et r deux entiers fixés, n entier prenant les valeurs $0, 1, 2, \dots$) et que si a et r n'ont pas de facteurs premiers en commun (c'est le cas pour les concurrents de la course envisagée au-dessus : $a = 4, r = 1$ et $a = 4, r = 3$), alors il existe une infinité de nombres premiers de la forme $an + r$. De plus, si a est fixé, la densité asymptotique des nombres premiers est la même dans les différentes progressions arithmétiques $an + r$ quand r varie (r sans facteur premier commun avec a).

Dans notre course entre $[1 \bmod 4]$ et $[3 \bmod 4]$, cela signifie que le rapport R de leurs effectifs jusqu'à n :

$$\|1 \bmod 4; n\| / \|3 \bmod 4; n\|$$

tend vers 1 quand n tend vers l'infini. Si ce rapport R tendait vers une limite L supérieure à 1, cela signifierait que l'équipe $[1 \bmod 4]$ devancerait toujours l'autre équipe à partir d'un certain moment. Si le rapport tendait vers une limite inférieure à 1, cela signifierait que l'équipe $[3 \bmod 4]$ devancerait toujours l'autre à partir d'un certain moment. Le fait que la limite soit 1 ne donne donc pas la solution de notre problème. Notons que cette valeur n'interdit pas qu'une équipe domine l'autre à partir d'un certain moment : en effet, si l'écart reste par exemple toujours entre 10 et 50 (comme le tableau de la figure 1 le suggère) alors la limite L est 1 (car $(k+50)/k$ tend vers 1 quand k tend vers l'infini) et pourtant l'une des équipes est toujours en tête.

Le résultat cité, loin de simplifier le travail, indique donc au contraire que si un sens précis peut être donné à la domination de l'équipe $[3 \bmod 4]$ sur l'équipe $[1 \bmod 4]$, cela sera nécessairement subtil. L'examen attentif des deux séries de nombres premiers montre que l'espoir d'une domination continue à partir d'un certain instant est très probablement injustifié.

D'ailleurs en y regardant de près, quand n augmente, arrivé au nombre premier 26 861, l'équipe $[1 \bmod 4]$ qui a toujours été dominée passe en tête. Cela ne dure qu'un instant. L'équipe $[3 \bmod 4]$ repasse aussitôt devant et le reste jusqu'au nombre premier 616 841 qui voit à nouveau l'équipe $[1 \bmod 4]$ reprendre l'avantage. Plusieurs croisements ont alors lieu jusqu'en 633 798, et là, l'équipe $[3 \bmod 4]$ retrouve la tête pour un très long moment. Il faut attendre 12 306 137 pour voir à nouveau l'équipe $[1 \bmod 4]$ retrouver la première position. Se ressaisissant un peu plus loin, l'équipe $[3 \bmod 4]$ double son adversaire en 12 382 326 et maintient alors une avance jusqu'en 951 784 481 où, à nouveau, $[1 \bmod 3]$ la rattrape et la dépasse.

Malheureusement, la poursuite de l'examen de la course semble ne jamais conduire à une conclusion définitive. Régulièrement, pour de courtes périodes, l'équipe $[1 \bmod 4]$

dépasse l'équipe $[3 \bmod 4]$ qui, même si elle mène le plus souvent, ne réussit apparemment jamais à s'imposer d'une façon durable.

Les théoriciens des nombres savent depuis 1914 que l'espoir d'une domination continue d'une des deux équipes est illusoire. En effet cette année-là, le mathématicien anglais John Littlewood (1885-1977) démontre que les deux équipes se croisent une infinité de fois.

Notre volonté de donner un sens à la domination apparente de l'équipe $[3 \bmod 4]$ aurait-elle rencontré un obstacle insurmontable? Ce n'est pas certain, car le suivi détaillé des croisements des deux équipes suggère que même si $[1 \bmod 4]$ repasse en tête de temps en temps, elle y reste peu de temps. La domination de l'équipe $[3 \bmod 4]$ pourrait donc signifier que les instants n où cette équipe gagne sont plus nombreux que ceux où l'équipe $[1 \bmod 4]$ gagne. Cette idée correspond à la conjecture de Knapowski et Turan proposée en 1962:

Le pourcentage $p(n)$ d'entiers $x \leq n$, pour lesquels l'équipe $[3 \bmod 4]$ devance l'équipe $[1 \bmod 4]$ tend vers 100 quand n tend vers l'infini.

Le calcul donne: $p(26\,860) = 100\%$ (jusqu'à 26 860, l'équipe $[3 \bmod 4]$ domine toujours); $p(5 \cdot 10^5) = 99,9\%$; $p(10^7) = 97,4\%$; $p(10^9) = 99,9\%$; $p(10^{11}) = 97,2\%$. Certes, on ne s'éloigne guère de 100%, mais ces données numériques ne sont pas assez claires ni régulières pour appuyer la conjecture! On connaît de nombreuses situations en mathématiques où un phénomène numérique est vrai pour les entiers pas trop grands et devient faux plus loin. Serait-on dans une telle situation?

L'histoire mathématique de ce problème semble alors s'engager définitivement vers une issue décevante. En 1996, Jerzy Kaczorowski et Peter Sarnak établissent indépendamment que la conjecture de 1962 est fausse: le pourcentage $p(n)$ des cas où l'équipe $[3 \bmod 4]$ l'emporte sur l'équipe $[1 \bmod 4]$ ne tend pas vers 100, mais varie sans jamais converger.

Mission accomplie

La diminution de densité des nombres premiers de taille n quand n augmente est mesurée par le logarithme népérien de n , $\log(n)$, et elle est donnée par le théorème des nombres premiers qui affirme que la densité des nombres premiers autour de n est approximativement $1/\log(n)$: en prenant au hasard un nombre proche de n , il sera premier avec une probabilité $1/\log(n)$. C'est un des plus beaux résultats de la théorie des nombres.

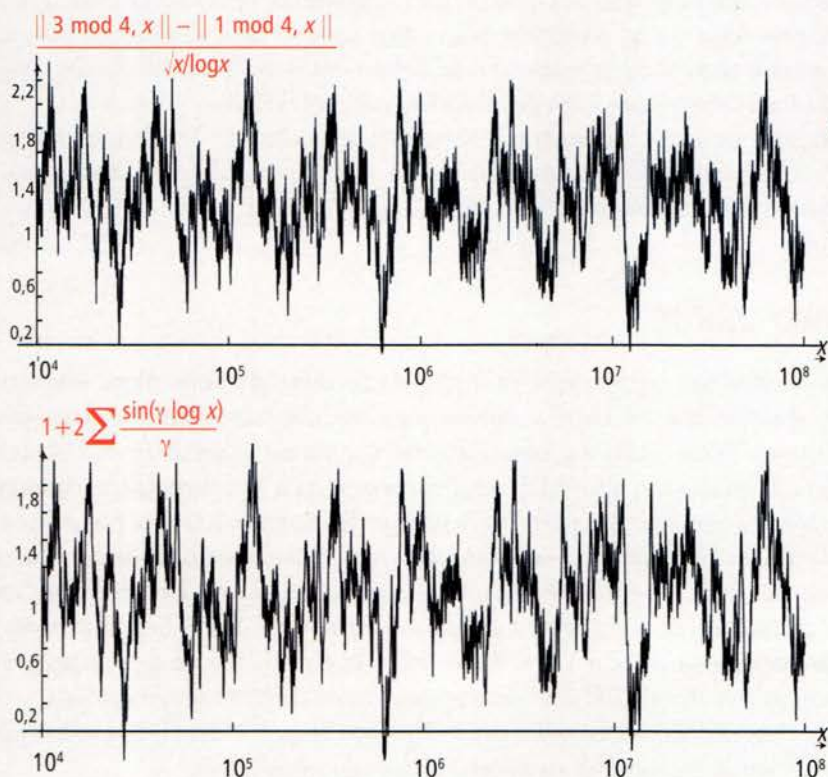
Une des conséquences de ce résultat est l'évaluation de la valeur des nombres premiers en fonction de leur position dans la suite infinie des nombres premiers: la valeur du n -ième nombre premier est environ $n \log(n)$.

On peut tenir compte de la décroissance de densité en mesurant l'importance d'un ensemble E de nombres par la somme de leurs inverses. Cela revient au calcul d'une moyenne pondérée car alors, plus un nombre est grand, moins sa présence compte dans le poids attribué à E . On est conduit à définir la mesure dite logarithmique:

$$m(E) = \lim_{n \rightarrow \infty} \frac{1}{\log(n)} \sum_{\substack{x \in E \\ x \leq n}} \frac{1}{x}$$

La formule semble compliquée, elle est pourtant naturelle. Pour mesurer le poids d'un ensemble E , on fait la somme des inverses de ses éléments, jusqu'à n ; on divise le résultat par $\log(n)$ (car la somme de tous les inverses des entiers jusqu'à n est environ $\log(n)$, $\log(n)$ étant juste un facteur de normalisation) et on fait tendre n vers l'infini pour prendre en compte tous les éléments de E .

3. Nombres devinés, car impossibles à calculer



$$\frac{||3 \bmod 4, x|| - ||1 \bmod 4, x||}{\sqrt{x/\log x}} \approx 1 + 2 \sum_{\gamma > 0 \text{ tels que } 1/2 + i\gamma \text{ annule } L(s)} \frac{\sin(\gamma \log x)}{\gamma}$$

où la fonction L est définie pour $s > 1$ par $L(s) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \dots$

Le calcul exact du nombre de nombres premiers de la forme $4n + 3$ inférieurs à x (noté $||3 \bmod 4; x||$) et du nombre de nombres premiers de la forme $4n + 1$ inférieurs à x (noté $||1 \bmod 4; x||$) devient pratiquement impossible (ou trop cher en temps de calcul!) lorsque x atteint 10^{13} environ, car pour le mener, il faut énumérer tous les nombres premiers jusqu'à la valeur de x souhaitée. Cependant, grâce à la formule indiquée sur la figure et au calcul des valeurs qui annulent la fonction L , une variante de la fonction de Riemann, on peut évaluer l'écart entre $||3 \bmod 4; x||$ et $||1 \bmod 4; x||$ pour des valeurs de x bien plus grandes.

Ces évaluations sont remarquablement précises, comme on le constate en observant les graphes reproduits où la courbe des valeurs réelles et la courbe obtenue par l'ap-

proximation, quoique toutes deux d'apparence aléatoire, sont presque identiques.

En 1999, Carter Bays et Richard Hudson, en utilisant une telle formule, ont évalué qu'au-delà des changements de signes déjà connus, il devait se produire un nouveau changement de signe vers $1,4898 \times 10^{12}$ et un autre encore vers $9,3190 \times 10^{12}$. Le premier changement prédit a depuis été trouvé en :

1 488 478 427 089

Il est remarquable que les techniques indirectes d'évaluation permettent ainsi de savoir où se trouvent des nombres qui sont au-delà de nos moyens de calcul explicite. Ainsi le calcul des valeurs complexes où la fonction de Riemann s'annule, de la forme $1/2 + i\gamma$, fait plus que vérifier la conjecture de Riemann, il améliore la précision de certaines formules de calcul où interviennent les nombres premiers.

Lorsqu'elle existe, cette mesure $m(E)$ attribuée à E , du fait de la normalisation opérée par la division par $\log(n)$, est un nombre entre 0 et 1. Plus un ensemble d'entiers est gros, plus sa mesure logarithmique sera proche de 1 ; plus un ensemble est dispersé et éparpillé, plus sa mesure logarithmique sera proche de 0 : l'ensemble de tous les entiers a pour mesure logarithmique 1 ; un ensemble fini a pour mesure logarithmique 0. Avec cette mesure se produit alors le miracle attendu : la mesure $m(G)$ de l'ensemble G des entiers n où l'équipe $[3 \bmod 4]$ devance l'équipe $[1 \bmod 4]$ vaut 0,9959280...

Cette égalité exprime clairement la domination notée par Tchebychev : l'équipe $[3 \bmod 4]$ est en tête 99,59 pour cent du temps. Ce remarquable résultat est dû aux mathématiciens Michael Rubinstein et Peter Sarnak et il fut publié en 1994.

Le dernier chiffre

Précisons toutefois que ce théorème et la plupart de ceux que nous allons mentionner concernant d'autres courses entre nombres premiers n'ont été obtenus qu'en faisant deux hypothèses. D'une part, il a fallu admettre une forme généralisée de l'hypothèse de Riemann. D'autre part, il a fallu aussi supposer vraie une hypothèse dénommée *Grand Simplicity Hypothesis* qui porte sur les zéros des fonctions L (des fonctions classiquement utilisées en théorie des nombres). Ces hypothèses sont considérées toutes les deux comme très difficiles à démontrer, mais probablement vraies. Le fait d'avoir réussi à résoudre la question de Tchebychev même sous la réserve de ces hypothèses est une belle victoire de l'esprit d'opiniâtreté. Bien sûr, ici la satisfaction ne sera complète que lorsque les deux hypothèses utilisées sans preuve seront définitivement établies.

Reste une question (au moins) : pourquoi le 3 gagne-t-il sur le 1 dans la course modulo 4 ? Pour tenter d'y répondre, considérons d'autres courses du même genre.

4. Le dernier chiffre

Tous les nombres premiers (sauf 2 et 5) se terminent par un des quatre chiffres 1, 3, 7 ou 9. Ces quatre catégories de nombres sont-elles de même taille ? Pour le savoir, on fait des décomptes.

Sur la ligne d'une valeur de x , on a indiqué le nombre de nombres premiers inférieurs ou égaux à x se terminant par 1, ou par 3, par 7 ou par 9 (en rouge le nombre le plus élevé de chaque ligne).

On remarque que les colonnes des chiffres 3 et 7 dominent celles de 1 et 9, qui ne sont jamais en tête. Cette constatation reste-t-elle vraie indéfiniment ?

Si oui, peut-on trouver une règle qui explique pourquoi le dernier chiffre d'un nombre premier est un peu plus souvent 3 ou 7 que 1 ou 9 ? La réponse est oui : c'est parce que 1 et 9 sont des carrés qu'ils sont dominés par 3 et 7.

x	Chiffre 1	Chiffre 3	Chiffre 7	Chiffre 9
100	5	7	6	5
200	10	12	12	10
500	22	24	24	23
1000	40	42	46	38
2000	73	78	77	73
5000	163	172	169	163
10 000	306	310	308	303
20 000	563	569	569	559
50 000	1274	1290	1288	1279
100 000	2387	2402	2411	2390
200 000	4478	4517	4503	4484
500 000	10 386	10 382	10 403	10 365
1000 000	19 617	19 665	19 621	19 593

5. La course mystérieuse

Toutes les courses entre nombres premiers ne sont pas élucidées. Ainsi, l'écart entre deux nombres premiers différents de 2 est toujours un nombre pair 2, 4, 6, 8, ... Le décompte des paires de nombres premiers dont l'écart est 2 (les premiers « jumeaux », par exemple 11-13, 17-19) semble montrer qu'ils sont approximativement en même quantité que les nombres premiers dont l'écart est 4 ou dont l'écart est 8.

Aucun gagnant ne semble se détacher clairement et les colonnes restent remarquablement proches les unes des autres, se croisant sans relâche. Aujourd'hui ce type de courses entre nombres premiers reste incompris et aucun résultat comparable à ceux obtenus pour les courses du type $[1 \bmod 4] - [3 \bmod 4]$ n'est disponible.

x	Écart de 2	Écart de 4	Écart de 8
10^3	35	41	38
10^4	205	203	208
10^5	1224	1216	1260
10^6	8169	8144	8242
10^7	58 980	58 622	58 595
10^8	440 312	440 258	439 908
10^9	3 424 506	3 424 680	3 426 124
10^{10}	27 412 679	27 409 999	27 411 508
10^{11}	224 376 048	224 373 161	224 365 334
10^{12}	1 870 585 220	1 870 585 459	1 870 580 394

Examinons une deuxième course, cette fois avec quatre concurrents.

Le chiffre des unités d'un nombre premier au-delà de 5 est nécessairement 1, 3, 7 ou 9 (car les nombres se terminant autrement sont nécessairement pairs ou multiples de 5). Cela correspond aux formes $10n + 1$, $10n + 3$, $10n + 7$, $10n + 9$ et, avec nos notations, à une course entre quatre équipes: $[1 \bmod 10]$, $[3 \bmod 10]$, $[7 \bmod 10]$ et $[9 \bmod 10]$. Qui gagne ?

Un tableau de résultats est proposé à la figure 4. Sait-on donner un sens à ce qu'on observe, c'est-à-dire que les deux équipes $[3 \bmod 10]$ et $[7 \bmod 10]$ dominent les deux autres ? La réponse a été trouvée et démontrée (toujours par M. Rubinstein et P. Sarnak). Dans une course de ce type, l'important pour une équipe $[r \bmod a]$ est la propriété pour r d'être un carré modulo a . Expliquons cela.

Lorsque l'on s'intéresse aux nombres modulo 10 (c'est-à-dire écrits sous la forme $10n + r$), certains nombres sont des carrés, d'autres non.

$0 \times 0 = 0 \bmod 10$	$1 \times 1 = 1 \bmod 10$
$2 \times 2 = 4 \bmod 10$	$3 \times 3 = 9 \bmod 10$
$4 \times 4 = 16 = 6 \bmod 10$	$5 \times 5 = 25 = 5 \bmod 10$
$6 \times 6 = 36 = 6 \bmod 10$	$7 \times 7 = 49 = 9 \bmod 10$
$8 \times 8 = 64 = 4 \bmod 10$	$9 \times 9 = 81 = 1 \bmod 10$

Les carrés modulo 10 (c'est-à-dire en ne prenant en compte que le chiffre des unités) sont 0, 1, 4, 5, 6 et 9. Les nombres 3 et 7 ne sont pas des carrés modulo 10.

La règle générale, démontrée sous réserve des deux hypothèses mentionnées plus haut, pour savoir qui gagne dans une course de nombres premiers modulo a , est la suivante :

- Entre deux équipes dont l'une correspond à un carré et l'autre non, celle qui est un carré perd. Précisément : la mesure logarithmique des entiers où celle qui n'est pas un carré gagne est strictement supérieure à $1/2$.

- Entre deux équipes, correspondant à des carrés, ou entre deux équipes ne correspondant pas à des carrés, il y a égalité, ce qui signifie que l'ensemble des n où l'une l'emporte sur l'autre a pour mesure logarithmique $1/2$.

Dans le cas du chiffre des unités des nombres premiers (la « course modulo 10 »), on a donc les résultats généraux suivants :

- Il y a autant (au sens de la mesure logarithmique) de nombres premiers se terminant par 1 ou 9 ;
- Il y a autant (au sens de la mesure logarithmique) de nombres premiers se terminant par 3 ou 7 ;
- Il y en a plus (au sens de la mesure logarithmique) se terminant par 3 ou 7 qu'il n'y en a se terminant par 1 ou 9.

6. La course entre $\text{Li}(x)$ et $\pi(x)$

Soit $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x . La fonction logarithme intégral $\text{Li}(x)$ en donne une approximation :

$$\text{Li}(x) = \int_2^x \frac{dt}{\log t}$$

L'hypothèse de Riemann est l'affirmation que les deux quantités ne sont jamais très éloignées et qu'il existe une constante R telle que :

$$|\pi(x) - \text{Li}(x)| < R\sqrt{x} \log x$$

Cependant, lorsque l'on réalise les calculs, on découvre que $\text{Li}(x)$ est toujours plus grand que le nombre de nombres premiers inférieurs à x .

En 1914, J. Littlewood a pourtant démontré que des croisements se produisaient une infinité de fois : la domination de l'équipe Li est expérimentalement vérifiée, alors qu'un résultat théorique indique que cette domination n'a plus lieu pour certains nombres x infiniment nombreux. Les mêmes techniques que celles utilisées pour les courses entre nombres premiers montrent que les entiers où $\text{Li}(x)$ est en tête constituent un ensemble dont la mesure logarithmique est 0,99999973... autrement dit, $\text{Li}(x)$ est en tête 99,999973% du temps.

Le premier changement de signe de la différence $\text{Li}(x) - \pi(x)$, annoncé par Littlewood, mais jamais observé, doit avoir lieu environ vers $1,3982 \times 10^{316}$. Cette prédiction est faite par une méthode analogue à celle décrite en figure 3.

La règle générale explique non seulement ce qui se passe pour le chiffre des unités des nombres premiers, mais aussi ce que nous avons constaté, la domination de l'équipe $[3 \bmod 4]$ sur l'équipe $[1 \bmod 4]$ (1 est un carré modulo 4, mais 3 ne l'est pas).

L'explication intuitive de la règle générale est que tout se passe comme si la répartition des nombres premiers entre deux suites arithmétiques $an + r$ et $an + r'$ (pouvant contenir des nombres premiers) se faisait parfaitement au hasard. Cependant, si r est un carré modulo a et que r' n'en est pas un, alors le léger désavantage créé par les carrés (qui sont des nombres composés et vont dans $an + r$ et pas dans $an + r'$) pénalise légèrement l'équipe $[a \bmod r]$ qui à l'infini est dominée par l'autre équipe au sens de la mesure logarithmique.

Poursuite

Tout n'est pas réglé pour autant. Découvertes à l'aide de calculs informatiques parfois massifs, de nouvelles observations engendrent de nouvelles questions théoriques. Récemment par exemple, un phénomène étrange a été observé, puis démontré à propos de la course modulo 8.

L'équipe $[1 \bmod 8]$ perd contre les trois autres $[3 \bmod 8]$, $[5 \bmod 8]$, $[7 \bmod 8]$. C'est conforme au résultat général sur les carrés, car en calculant

modulo 8, aucun des nombres 3, 5, 7 n'est un carré alors que 1 est un carré. Les trois équipes $[3 \bmod 8]$ et $[5 \bmod 8]$ et $[7 \bmod 8]$ qui sont en tête à tour de rôle peuvent se classer de six façons différentes (car il y a six façons d'ordonner trois éléments).

On aurait pu penser que chaque classement se produirait dans $1/6$ des cas au sens de la mesure logarithmique. Ce n'est pas le cas. En effet, Andrew Feuerverger et Greg Martin ont démontré que (en utilisant des notations évidentes) :

$$m(3 > 5 > 7) = m(7 > 5 > 3) = 0,1928013\dots,$$

$$m(3 > 7 > 5) = m(5 > 7 > 3) = 0,1664263\dots,$$

$$m(5 > 3 > 7) = m(7 > 3 > 5) = 0,1407724\dots$$

Pourquoi donc ? Quel est le secret de cet étrange désordre qui a pour conséquence que lorsque 3 est en tête alors 5 a plus de chance de dominer 7 que l'inverse ?

Malgré les fantastiques progrès obtenus dans la compréhension de la logique des nombres premiers relatés ici, celle-ci nous réserve sans doute encore de belles surprises.



Logique sociale, économique et humaine

La logique consiste parfois à comprendre que là où il semble y avoir un seul problème, il y en a en réalité plusieurs aux solutions incompatibles, et qui rendent donc impossible la résolution générale. C'est ce que nous découvrons pour le problème de la répartition équitable des biens. Quant à savoir où est passé l'argent dans l'inégalable escroquerie de Bernard Madoff, la logique des taux d'intérêt et des capitaux fictifs nous entraîne dans un délicat travail d'analyse aux résultats inattendus. L'humain exceptionnel, et Terence Tao en est un autre, suit une logique que sans doute nous ne pouvons que percevoir imparfaitement.

La répartition idéale des biens existe-t-elle ?

Différents objectifs et différentes méthodes sont utilisables pour répartir des biens ou des ressources : ils conduisent à des résultats incompatibles dont il est utile de comprendre la logique intriquée.

En collaboration avec Philippe Mathieu

L'histoire de la modélisation dans les sciences humaines et en particulier en économie conduit presque invariablement à une double conclusion. 1) Il est très difficile de faire des modèles précis et exacts ; quand vous essayez, une bonne âme vous explique que vous êtes naïf en pensant représenter le réel avec la méthode retenue. 2) Concevoir des modèles et les étudier est important : on dégage des idées, on rend possibles des théorèmes et des programmes qui renforcent la compréhension et aident à prendre de meilleures décisions.

Le partage des richesses

Le partage de ressources entre les membres d'une communauté est un éternel problème humain, souvent très mal résolu. L'humanité ne cerne pas bien le but qu'elle poursuit et veut concilier des objectifs contradictoires.

Ce problème se pose quand il faut répartir les richesses disponibles entre les agents économiques, entre individus, entre groupes sociaux, entre entreprises ou institutions concurrentes, etc., mais aussi quand on doit décider comment attribuer le temps de parole, partager l'eau, l'électricité, les recettes fiscales, ou des moyens techniques entre diverses entités qui attendent chacune leur part. Améliorer l'efficacité d'un algorithme ou d'un réseau d'ordinateurs se ramène aussi bien souvent à un problème d'allocation ; c'est ce qui explique que, venant en renfort aux économistes et aux mathématiciens, les informaticiens étudient aujourd'hui ces questions.

Examinons le problème sur un exemple simple et considérons deux entités (deux « agents ») qui doivent se partager divers biens (supposés insécables) auxquels elles accordent plus ou moins de valeur. Les agents seront notés A et B . Les biens seront notés a , b , c et d . Nous supposerons qu'il n'y a qu'un exemplaire de chaque bien.

L'agent A attribue autant d'importance au bien a et au bien b (utilité 10), et moins aux deux autres (utilité $c = 3$, utilité $d = 1$). L'utilité d'un bien, l'intérêt qu'on éprouve pour le bien, est ici toujours mesurée par un entier positif. Les utilités pour l'agent B des biens a , b , c et d sont respectivement de 2, 3, 2, et 2.

1. Le jugement de Salomon



Salomon, nouveau roi des Hébreux, reçoit en songe un message de l'Éternel : « Demande ce que tu veux que je te donne. » Salomon répond : « Accorde donc à ton serviteur un cœur intelligent pour juger ton peuple, pour discerner le bien du mal ! »

Peu de temps après, se présentent devant lui deux prostituées. La première raconte les faits suivants : elles vivent ensemble, seules dans une maison et ont accouché à peu d'intervalle chacune d'un fils. Or, toujours d'après son récit, l'enfant de l'autre femme est mort car « elle s'était couchée sur lui ». Puis, elle aurait interverti les deux enfants afin de conserver pour elle l'enfant vivant.

Et les voilà demandant justice à Salomon, chacune accusant l'autre d'être la mère de l'enfant mort et réclamant pour elle l'enfant vivant. On connaît le verdict de Salomon : « Coupez en deux l'enfant qui vit, et donnez-en la moitié à l'une et la moitié à l'autre. » La vraie mère sera celle qui accepte de ne plus l'être pour qu'au moins son enfant

vive : « Ah mon seigneur, donnez-lui l'enfant qui vit et ne le faites point mourir. »

Que disent les mathématiques du problème de Salomon ? Imaginons les données suivantes. Une des deux mères, *A*, alloue 20 points à l'enfant vivant avec elle, 3 points pour l'attribution de l'enfant à la mère *B*, et 5 points pour la moitié de l'enfant coupé en deux. L'autre mère, *B*, attribue 13 à l'enfant vivant avec elle, 0 point pour l'attribution de l'enfant à la mère *A* et 4 points à la moitié de l'enfant coupé en deux.

Le jugement utilitariste favorisant la somme des allocations des deux agents donne l'enfant à la mère *A*, la somme des allocations étant égale à 20. Le jugement égalitariste, qui recherche l'allocation donnant la plus grande valeur possible à la mère la moins bien servie, c'est-à-dire 4, amènerait Salomon à ordonner que l'enfant soit coupé en deux... La loi de distribution de biens est affaire de choix : ici l'égalitarisme n'indique pas la solution satisfaisante.

Utilités	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>
Agent <i>A</i>	10	10	3	1
Agent <i>B</i>	2	3	2	2

Bien sûr, on pourra envisager d'autres exemples avec plus de deux agents et plus de quatre biens à répartir, chacun pouvant aussi exister en plusieurs exemplaires.

Pour simplifier, imaginons dans un premier temps qu'un monarque absolu décide de l'attribution des biens. Comment doit-il les distribuer au mieux ? Posez-vous la question quelques secondes, avant de lire la suite.

Votre réponse est sans doute : la meilleure allocation des biens aux agents dépend du but que le monarque poursuit. S'il veut que, globalement, la « société » de ses deux sujets soit la plus satisfaite (recherche du bien-être social maximum), il doit trouver l'allocation des ressources qui conduit à une somme maximale d'utilités. Pour chaque allocation possible, la satisfaction d'un agent est la somme des utilités (comptées avec ses valeurs) pour les biens qui lui sont attribués. La meilleure allocation maximise la somme des satisfactions des deux agents : *max-som*.

Rien ne dit que le but du monarque soit cette maximisation globale du total des satisfactions (point de vue *utilitariste*). Le monarque, soucieux de ne pas trop défavoriser un agent, peut rechercher l'allocation qui donne la plus grande valeur possible à la satisfaction de l'agent le moins bien servi : il cherche à maximiser le minimum des satisfactions de *A* et de *B* : *max-min*. Ce point de vue *égalitariste* évite qu'un agent soit trop mécontent. Notons cependant que cela peut être catastrophique et se faire aux dépens de l'utilité globale. Il faut choisir !

Quatre allocations optimales différentes

Ce choix est un problème moral et politique, pas mathématique. Hélas, l'intérêt général (utilitarisme) ne coïncide que rarement avec l'intérêt du plus pauvre (égalitarisme) comme nous le verrons plus loin.

Présentons aussi une troisième conception nommée *élitiste*. Pour l'élitiste, ce qui compte, c'est que le plus satisfait ait la satisfaction la plus grande possible : *max-max*. L'idée se défend si, par exemple, diverses entités composées de plusieurs agents doivent s'affronter et que chaque entité est représentée par le « champion » du groupe. L'intérêt du monarque sera de concentrer les richesses sur un seul agent, celui qui est le plus à même de représenter le groupe.

Un autre point de vue encore est celui qui opère un compromis entre les trois points de vue précédents. On l'appelle le point de vue *nashien*, du nom du mathématicien économiste John Nash.

Le point de vue nashien est que la meilleure allocation maximise le produit des satisfactions des agents : *max-pro*. Pour que ce produit soit grand, il ne faut pas que certains agents ne reçoivent rien (car, si un facteur est nul, le produit l'est aussi), mais aussi qu'une certaine équité soit assurée (par exemple, quand la somme *s* de deux nombres *a* et *b* est fixée, le maximum du produit *ab* est atteint pour $a = b = s/2$). Le point de vue nashien conduit à une allocation équilibrant à peu près les satisfactions des divers agents et assure que le total des satisfactions reste élevé.

Pour voir que les quatre objectifs possibles d'un monarque ne conduisent pas à la même allocation optimale, examinons notre exemple... que nous avons choisi pour prouver que les quatre objectifs possibles sont tous différents.

2. Échanges rationnels et suite d'échanges



Un marché du troc au Pérou

Un échange de biens entre l'agent A et l'agent B est rationnel (l'agent A donne un de ses biens à B , et l'agent B donne en échange un de ses biens à A) si A y gagne (sa satisfaction est plus élevée après l'échange) et si B y gagne aussi.

Considérons les biens a, b, c, d, e, f et les agents A, B, C qui y attribuent les valeurs (utilités) suivantes :

Utilités	a	b	c	d	e	f
Agent A	1	2	3	9	1	1
Agent B	2	1	1	2	3	5
Agent C	3	1	1	10	5	3

On suppose que l'allocation initiale est :

$\{A (10) : a d ; B (4) : b e ; C (4) : c f\}$ som = 18.

Voici la liste complète des échanges rationnels :

- A donne a à B et B donne b à A . La satisfaction de A passe de 10 à 11, celle de B passe de 4 à 5.
- A donne a à C et C donne c à A . La satisfaction de A passe de 10 à 12, celle de C passe de 4 à 6.
- B donne e à C et C donne f à B . La satisfaction de B passe de 4 à 6, celle de C passe de 4 à 6.

Parmi les suites d'échanges rationnels, il y a les deux suivantes :

Suite d'échanges rationnels 1 :

$[A$ donne a à B et B donne b à $A]$

$[B$ donne e à C et C donne f à $B]$.

Cette suite conduit à l'allocation :

$\{A (11) : b, d ; B (7) : a f ; C (6) : c e\}$ som = 24.

Suite d'échanges rationnels 2 :

$[B$ donne e à C et C donne f à $B]$

$[A$ donne a à C et C donne c à $A]$.

Cette suite conduit à l'allocation :

$\{A (12) : c, d ; B (6) : b f ; C (8) : a e\}$ som = 26.

Chacune de ses deux allocations finales est telle que plus aucun échange rationnel ne peut se produire (marché bloqué).

On tire de cet exemple deux conclusions.

– Une séquence d'échanges rationnels peut conduire à une allocation bloquée qui n'est pas la meilleure de celles accessibles par des suites d'échanges rationnels (c'est ce qui se passe dans le cas de la suite d'échanges 1) : laisser faire le marché ne donne pas nécessairement l'allocation optimale que le marché puisse atteindre et l'issue des échanges dépend du hasard. Dans notre exemple, le problème est lié à l'ordre des rencontres de A avec B et C : si A rencontre B et échange avec lui, il ne pourra plus échanger avec C , alors que cela aurait été plus profitable.

– La suite d'échanges rationnels qui donne le meilleur résultat possible est la suite d'échanges 2 qui conduit à une allocation dont la somme des utilités est 26. Ce n'est pas l'allocation utilitariste optimale qui ici serait :

$\{A (5) : b, c ; B (5) : f ; C (18) : a, d, e\}$ som = 28.

L'allocation optimale utilitariste est inaccessible si on s'impose de n'opérer que des échanges rationnels. Se restreindre à des échanges rationnels interdit donc dans certains cas d'arriver à la meilleure allocation, et remet au hasard l'accès à la meilleure allocation accessible. Cette dernière peut se trouver exclue elle aussi à cause d'un ordre malheureux des échanges, bloquant le marché prématurément lequel manque alors doublement son optimum.

Utilités	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>
Agent <i>A</i>	10	10	3	1
Agent <i>B</i>	2	3	2	2

Pour obtenir la meilleure allocation correspondant au point de vue utilitariste, on donne chaque bien à celui qui y accorde le plus d'importance et donc *A* se voit attribuer les biens *a*, *b* et *c* et *B* récupère *d*. La satisfaction de *A* est 10+10+3, celle de *B* est 2 et donc le total, le bien-être social, vaut 25. On ne peut pas faire mieux et cette allocation optimale se note :

$$\{A(23): a, b, c; B(2): d\} \text{ max-som} = 25.$$

Bien sûr, *B* se sentira mal aimé. Un monarque égalitariste et donc soucieux de faire que le moins bien loti de ses sujets reçoive le plus possible donnera le bien *a* à *A* (qui aura donc 10) et les biens *b*, *c*, *d* à *B* (qui aura donc 7). Il est impossible de faire mieux que 7 pour le minimum des agents, car pour que *B* ait plus que 7, il faudrait tout lui donner et *A* se retrouverait avec 0. L'allocation égalitariste optimale est :

$$\{A(10): a; B(7): b, c, d\} \text{ max-min} = 7.$$

Le coût du point de vue égalitariste est de 8 utilités. En effet, au lieu d'avoir un total de 25 utilités, la communauté des deux agents *A* et *B* dispose d'un total de seulement 17 utilités. Le point de vue utilitariste ne coïncide pas avec le point de vue égalitariste ; c'est décevant, et mieux vaut en avoir conscience. Malheureusement, ce n'est pas tout : le point de vue élitiste, lui encore, produit une allocation optimale différente. Il faut tout donner à *A* et rien à *B*. Il est évident que c'est la meilleure allocation pour l'élitiste, car pour maximiser ce que le meilleur possède, il faut tout lui donner. Comme ici, il est plus rentable de tout donner à *A* qui en tire une utilité totale de 24 que de tout donner à *B* qui n'en aurait tiré qu'une utilité totale de 9, le mieux

3. Échanges multiples

L'exemple suivant (où l'on adopte le point de vue utilitariste) montre que si le réseau des relations entre agents est incomplet, il peut devenir impossible d'atteindre l'allocation optimale uniquement en faisant des dons sociaux (lorsque le réseau est complet, les dons sociaux conduisent toujours à l'allocation optimale). L'exemple montre aussi qu'en autorisant des échanges rationnels quelconques (plusieurs biens contre plusieurs, pourvu que chacun y gagne), alors une suite d'échanges conduit parfois à l'allocation optimale.

On suppose trois agents *A*, *B* et *C* disposés selon le schéma : $A \longleftrightarrow B \longleftrightarrow C$

Les biens sont *a*, *b*, *c*, *d* et les agents y attribuent les valeurs suivantes :

Utilités	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>
Agent <i>A</i>	2	6	9	1
Agent <i>B</i>	7	4	5	8
Agent <i>C</i>	3	10	4	2

On suppose que l'allocation initiale est :

$$\{A(8): a, b; B(5): c; C(2): d\} \text{ som} = 15$$

L'allocation optimale est :

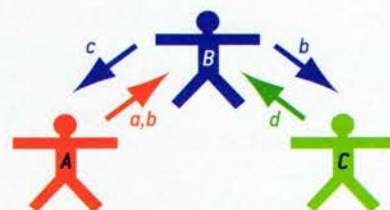
$$\{A(9): c; B(15): a, d; C(10): b\} \text{ som} = 34$$

À partir de la situation de départ, même si les agents acceptent de faire des dons sociaux, on n'arrivera pas à l'allocation optimale, car *A* ne peut pas donner *b* (qui vaut 6 pour lui) à *B* (pour qui *b* ne vaut que 4).

En revanche, si les agents opèrent des échanges multiples (plusieurs biens contre un seul) et même en n'acceptant que des échanges rationnels (chaque contractant y gagne), cette fois l'allocation optimale est atteinte en deux échanges. D'abord, *A* échange avec son voisin *B* les biens *a* et *b* contre *c* (*A* y gagne 1, *B* y gagne 6), ce qui donne :

$$\{A(9): c; B(11): a, b; C(2): d\} \text{ som} = 22.$$

Ensuite *B* échange, avec son voisin *C*, *b* contre *d* (*B* y gagne 4, *C* y gagne 8), ce qui les conduit à l'optimum.



est que A prenne tout. Le monarque élitiste opte donc pour :

$$\{A(24) : a, b, c, d; B(0) : \text{rien}\} \text{ max-max} = 24.$$

Remarquons que, là encore, le choix élitiste engendre un coût pour la communauté formée par A et B : globalement, elle n'obtient que 24 utilités alors que 25 est possible.

Pour le point de vue nashien, la meilleure allocation est de donner les biens a et b à A et c et d à B , ce qui engendre une satisfaction de 20 pour A et de 4 pour B , et donc un produit des satisfactions de 80. On ne peut pas faire mieux pour le produit. L'allocation optimale pour le nashien est donc encore différente des trois précédentes :

$$\{A(20) : a, b; B(4) : c, d\} \text{ max-pro} = 80.$$

Selon l'objectif que le monarque se fixe, quatre répartitions différentes sont les meilleures allocations ! Pour résoudre un problème d'allocation, il est nécessaire d'avoir analysé ce qu'on croit le meilleur objectif pour la communauté concernée. Cette leçon morale et politique mériterait d'être connue de tout citoyen, car elle montre qu'il n'y a pas qu'une seule conception possible de l'intérêt général, mais plusieurs, et qu'un compromis est inévitable. La question de savoir si le point de vue nashien est le bon compromis admet probablement une réponse négative, car d'autres compromis sont envisageables, et mathématisables, conduisant à d'autres solutions optimales...

Complications

S'il y a n agents et m biens à répartir, le nombre d'allocations possibles est n^m , ce qui est vite énorme. Pour 100 biens et 10 agents, cela fait 10^{100} , ce qu'on ne peut pas traiter en envisageant chaque cas : les plus gros calculs informatiques faisables aujourd'hui comportent de l'ordre de 10^{24} opérations. On utilise donc des méthodes mathématiques plus subtiles. Pour le point de vue utilitariste et le point de vue élitiste, on connaît d'excellents algorithmes rapides ; pour le point de vue égalitariste, cela devient plus difficile, et pour le point de vue nashien, on est très rapidement dans l'impossibilité de calculer en temps raisonnable la solution optimale et on doit donc se contenter de solutions approchées.

D'autres difficultés sont plus profondes et plus graves : elles naissent de l'hypothèse qu'un monarque puisse être parfaitement informé et puisse décider des attributions de chacun.

Pour rendre le modèle plus réaliste, il faut le reformuler en prenant en compte deux éléments. D'une part (a), le fait que les biens au début sont déjà dans les mains de certains agents, peut-être mal répartis, mais d'une façon qu'on ne peut négliger. D'autre part (b), que tous les échanges ne sont pas intéressants pour les agents qui, sauf cas particuliers, ne souhaiteront pas y perdre quand évoluera l'allocation initiale.

Quels échanges peuvent souhaiter faire des agents détenteurs de biens ? Avec ces échanges acceptables, les agents réussiront-ils à construire une allocation intéressante selon un des points de vue utilitariste, égalitariste, élitiste ou nashien ?

Lors d'un échange de biens, personne ne souhaite perdre. Si tous les agents attribuaient les mêmes valeurs aux biens, aucun échange ne serait possible, car ce que l'un gagnerait serait perdu par l'autre. Quand les agents n'accordent pas les mêmes valeurs aux différents biens, certains échanges sont gagnants pour les deux agents.

Si j'ai des pommes et que je les aime moins que les poires, et si vous avez des poires et que vous les aimez moins que les pommes, alors nous serons gagnants en échangeant. Tout le monde peut être gagnant dans un échange, et c'est bien pour cela qu'il y en a depuis la nuit des temps.

Un échange entre un agent A et un agent B est qualifié de *rationnel* si, comme dans l'exemple des pommes et des poires, chacun y trouve son compte. Aucune autorité régulatrice n'est nécessaire, car chacun en tire un bénéfice. Notons aussi que pour pratiquer un tel échange, chaque agent n'a besoin que de connaître ses propres utilités, aucune information globale centralisée n'est nécessaire.

Le problème économique de l'allocation, grâce à cette notion d'échange rationnel, peut mieux coller à la réalité. Partant d'une attribution de biens entre agents (fixée par des événements passés dont on ne remet pas en cause le résultat), est-il possible en opérant une suite d'échanges rationnels d'arriver à une allocation des ressources qui soit conforme au point de vue utilitariste (ou égalitariste, etc.)? Si ce n'est pas possible, quelle est la suite d'échanges rationnels qui permet d'en approcher le plus? Comment calculer ces suites optimales d'échanges?

Le même problème peut être posé en imaginant des agents qui n'opèrent pas les échanges à deux, mais en se regroupant à trois ou plus. On peut aussi imaginer et étudier des agents altruistes qui acceptent, conscients que c'est l'intérêt général, d'opérer des échanges qui leur soient temporairement défavorables ou partiellement défavorables. Il

est intéressant par exemple d'envisager des agents qui acceptent des échanges où ils sont perdants à la condition que globalement le bien-être social augmente. Si un agent A possédant un bien qui pour lui vaut 5 le donne à un agent B pour qui le bien vaut 6, cela augmentera la valeur cumulée des utilités de 1 (et donc le bien-être social tel que le conçoit un utilitariste). Les échanges, où même si l'un des contractants est perdant, qui augmentent le bien-être social sont dénommés *échanges sociaux*. Lorsque l'échange se réduit au passage d'un seul bien d'un agent à un autre, on parle de *don social*.

Indispensables dons sociaux

Les problèmes plus réalistes qui n'envisagent que des échanges rationnels, ou que des échanges sociaux, conduisent à des leçons intéressantes. Voici quelques-uns des résultats obtenus.

– Comme on s'y attendait, en partant d'une répartition quelconque et en n'envisageant que des échanges rationnels (à deux ou même à plus de deux), il sera rare d'arriver à la meilleure allocation utilitariste ou même conforme à un des autres points de vue. La raison en est très simple: si l'un des agents détient au départ beaucoup de biens, il n'acceptera pas de s'en séparer pour aller vers une allocation qui satisfasse un point de vue collectif (quel qu'il soit). Avec les données de notre exemple, si, au départ, tous les biens sont dans les mains de B , aucun échange rationnel ne sera possible, et on restera dans la situation initiale qui n'est une bonne allocation selon aucun des quatre points de vue considérés. Une société d'agents qui n'acceptent de procéder qu'à des échanges rationnels, une forme d'égoïsme, se condamne à ne pas atteindre une bonne satisfaction générale, et cela quel que soit le point de vue utilitariste, égalitariste, élitiste ou nashien.



– En revanche, quelle que soit l'allocation initiale, il existe une suite de dons sociaux qui conduit à l'allocation optimale pour le point de vue utilitariste. L'idée de la démonstration est que chaque agent qui détient un bien dont l'utilité pour lui est inférieure à l'utilité pour un autre agent le lui donne. Chaque don de ce type améliore le total des satisfactions, et cette suite de dons sociaux ne s'arrête que lorsque chaque bien est dans les mains de celui pour lequel l'utilité du bien est la plus grande. Toute suite de tels dons sociaux sera finie et aboutira à l'allocation optimale utilitariste.

La variété et la richesse des agents informatiques envisageables n'ont guère de bornes et permettent l'expérimentation systématique d'une multitude d'hypothèses complexes.

On a là une situation intéressante, où les agents, pourvu qu'ils acceptent d'opérer des dons sociaux, vont vers la solution optimale utilitariste et cela sans contrôle centralisé des échanges. La conclusion est ici très morale : sans dons sociaux, si chacun n'accepte que de faire des échanges rationnels, alors l'allocation optimale utilitariste est le plus souvent inaccessible, alors que si chacun pratique le don social, on arrive à cette allocation optimale. En redéfinissant la notion de don social pour l'adapter aux autres points de vue, on a des résultats analogues.

Des agents plus ou moins bien informés

Sur un plan algorithmique, le calcul des séquences d'échanges rationnels conduisant à l'allocation la meilleure selon tel ou tel point de vue est plus compliqué que le simple calcul de l'allocation optimale : il faut considérer une grande variété de suites d'échanges rationnels, certaines d'entre elles conduisant à des impasses (c'est-à-dire à des allocations non optimales qu'on ne peut plus faire évoluer, voir l'encadré 2). Un problème délicat aussi est celui de la décision d'arrêt : quand et comment les agents sont-ils informés qu'ils ont fait assez de transactions et qu'ils peuvent s'arrêter ? Diverses variantes du problème ont été examinées et des algorithmes ont été élaborés pour calculer efficacement les bonnes séquences d'échanges rationnels ou autres.

Ces modèles de la recherche des séries optimales d'échanges rationnels, comme toute modélisation mathématique en sciences humaines, ne sont pas jugés assez réalistes. Dans le cas des échanges rationnels, ils présentent au moins deux défauts majeurs.

S'il existe une suite d'échanges (conduisant par exemple à la meilleure allocation utilitariste accessible), comment les agents peuvent-ils le savoir à moins de disposer chacun d'une source parfaite d'information et d'une bonne capacité de calcul ? Dans la réalité, les agents sont partiellement informés et ils font les échanges (rationnels ou non) en ne prenant en compte que ce qu'ils savent et bien souvent en préférant mener les échanges les meilleurs pour eux dans l'immédiat, même si cela les conduit dans l'impasse. Ces politiques égoïstes engendrent des échanges qui conduisent à une assez bonne allocation, mais pas la meilleure de celles accessibles. La coordination des échanges par une autorité est, dans certains cas, envisageable : elle reste toujours difficile, car les agents croient qu'ils sont mieux placés que quiconque pour défendre leur intérêt. Le marché s'autorégule mal !

Dans la réalité, les agents sont situés dans un espace qui n'est pas homogène. Des contraintes géographiques (ou d'autre nature) limitent les échanges possibles. En clair,

le graphe des échanges possibles n'est pas un graphe complet (chaque agent n'est pas relié à chaque autre). Ce graphe « d'acointance » incomplet doit être pris en considération.

La modélisation multi-agents

Des travaux récents montrent qu'une série de transactions fondées sur une information locale et un graphe d'acointance permettent de s'approcher petit à petit d'une allocation optimale. On tente aussi de mettre au point des méthodes telles que plus on laissera les transactions s'opérer, meilleur sera le résultat atteint.

Plus les modèles tentent de devenir réalistes, plus il devient nécessaire de mettre en œuvre des techniques informatiques où chaque agent (économique, social, ou autre) est représenté par un programme indépendant. Les sources d'informations du programme et les interactions qu'il peut avoir avec les autres programmes du système sont définies et délimitées.

Ce type de représentation informatique, qui dans sa méthode approche du réel en mimant les composants objet par objet, est nommé simulation multi-agents. C'est une technique souvent plus satisfaisante que les modèles mathématiques, car la complexité de ces derniers est limitée par nos facultés de résolution des équations. Au contraire, la variété et la richesse des agents informatiques envisageables n'ont guère de bornes et permettent l'expérimentation systématique d'une multitude d'hypothèses complexes ainsi que la formulation d'explications naturelles.

Les systèmes multi-agents permettent de ne pas trop caricaturer le monde et accroissent l'intérêt des résultats obtenus. L'informatique aujourd'hui est une source de progrès dans la finesse et la précision des modèles, et tout cela permet aux chercheurs de découvrir sans cesse de nouvelles règles, de nouveaux principes, de nouvelles morales qui s'organisent selon des logiques qu'il faut reconnaître et comprendre.

Escroquerie ou jeu risqué ?

Les pyramides de Ponzi sont considérées comme des escroqueries bancaires, contre lesquelles il faut lutter sans merci. Elles ressemblent cependant à d'autres jeux d'argent parfaitement légaux.

L'affaire Bernard Madoff serait la plus importante escroquerie de l'histoire humaine. L'argent volatilisé est évalué entre 10 et 65 milliards de dollars et dépend beaucoup des méthodes de calcul adoptées (nous y reviendrons). C'est la somme nécessaire pour acheter de 20 000 à 100 000 beaux appartements à Paris ! L'escroquerie de Madoff se fonde sur un mécanisme nommé *pyramide de Ponzi* dont la nature mathématique et économique est plus subtile qu'il n'y paraît. Nous verrons que certaines études techniques concluent que, même si l'on sait avoir affaire à une pyramide de Ponzi, il est parfois rationnel d'y déposer son argent.

Charles Ponzi

L'idée de base est simple. L'escroc propose un rendement supérieur aux rendements promis par les autres banques ou organismes de dépôts – par exemple 30 % par an alors que les autres proposent 10 %. Ensuite, au lieu de placer l'argent confié, l'escroc le garde et l'utilise pour rembourser le capital et les intérêts promis à ceux qui souhaitent quitter le système : les nouveaux arrivants paient ceux qui se retirent. Bien sûr, l'escroc se sert aussi dans la caisse de la pyramide pour ses propres besoins !

L'Italien Charles Ponzi mit en place une telle arnaque en 1920 aux États-Unis. Il promettait un profit de 50 % pour un dépôt de 45 jours et de 100 % pour 90 jours (ce qui n'est déjà pas très cohérent, puisqu'une somme déposée 45 jours, puis 45 jours à nouveau avec les intérêts des premiers 45 jours, rapporte 125 % en 90 jours !).

Ponzi prétendait opérer sur des coupons postaux internationaux qui, à cause des variations du cours des monnaies, pouvaient s'acheter dans un pays et se revendre plus cher dans un autre. Comme il payait les rendements promis à ceux qui retiraient leurs mises, le bruit se répandit que son affaire était sérieuse. Le lendemain d'un jour où un article favorable fut publié dans le *Boston Post*, des milliers d'habitants de Boston accoururent à son bureau pour y déposer leur argent.



Cependant, un analyste remarqua que le volume des affaires de Ponzi nécessitait que 160 millions de coupons postaux soient en circulation, or leur nombre total n'atteignait pas 30 000. La pyramide s'écroula alors et Ponzi se retrouva en prison. Après en être sorti, il tenta de nouvelles escroqueries qui le conduisirent à nouveau en prison et il n'en sortit qu'en 1934, date à laquelle il fut expulsé vers l'Italie. L'analyse de ses comptes ne permit pas de retracer en détail ce qu'était devenu l'argent qui lui avait été confié, et les investisseurs ne récupérèrent qu'un tiers de leur dépôt.

Bien que son nom soit attaché à ce type d'escroquerie, la pyramide de Ponzi avait été pratiquée avant lui. Charles Dickens en avait décrit le principe dans une nouvelle, *Little Dorrit*, publiée en 1857. Des dizaines d'affaires de ce type se sont produites partout dans le monde avant celle record de Bernard Madoff qui, le 29 juin 2009, a été condamné à 150 ans de prison. Les détails de cette histoire aident à comprendre la nature des pyramides de Ponzi qui réserve quelques surprises.

Une pyramide de Ponzi peut tenir indéfiniment si les clients ne réclament pas leurs avoirs et les laissent en place, trop contents de voir les sommes promises augmenter régulièrement et rapidement. Dans un tel cas, l'argent dû suit une croissance exponentielle : si, par exemple, le taux promis est 30 % par an, l'argent dû au bout de n années est égal à l'argent déposé multiplié par $(1,30)^n$.

Exponentielle contrainte

Cette croissance exponentielle de l'argent dû n'a rien d'extraordinaire : elle existe pour tous les dépôts rémunérés à taux fixe dans toutes les banques du monde : $X\%$ par an correspond à une multiplication du capital par $1 + X/100$ chaque année ! Le problème d'une pyramide de Ponzi n'est pas là, il est dans le fait que l'argent confié n'est pas placé (ou placé à un taux inférieur au taux promis) et que l'organisateur de la pyramide ne possède donc pas l'argent qu'il doit. Une banque fonctionnant normalement fait fructifier de $Y\%$ par an l'argent qu'on lui a confié, avec un Y plus grand que le X promis aux clients.

Si chaque client de la pyramide de Ponzi retire ses avoirs au bout d'un temps moyen donné (par exemple trois ans) alors ce n'est pas seulement l'argent dû qui croît exponentiellement (ce qui comme nous l'avons dit est normal), mais, bien plus inquiétant, c'est aussi l'argent que de nouveaux clients doivent déposer pour payer ceux qui se retirent. Cela nécessite en effet un recrutement exponentiellement croissant de nouveaux clients qui cessera d'être possible à un moment ou un autre, provoquant alors l'écroulement de la pyramide. Le plus souvent, les autorités interviennent avant l'écroulement et elles arrêtent l'organisateur de la pyramide. Aussi les épargnants victimes accusent-ils souvent les autorités d'être la véritable cause de la volatilisation de leurs dépôts !

Nous nommerons *pyramide de Ponzi standard* une pyramide où l'argent n'est pas du tout placé par l'escroc (ou l'est à un taux inférieur au taux de rémunération promis), et où les clients retirent leur avoir au bout d'un temps moyen déterminé (par exemple trois ans), situation qui exige une augmentation exponentielle des nouveaux dépôts.

L'escroc qui gère une pyramide de Ponzi standard souhaite cacher la nature de son système : il laisse donc entendre qu'il dispose de méthodes particulières, plus ou moins secrètes, qui lui permettent de servir les intérêts annoncés en opérant de manière régulière sur les marchés. Souvent, au départ, c'est vrai et ce n'est que progressivement, après l'échec de ce qu'il pensait une méthode infaillible, qu'il met en place sa pyramide.

1. Suivi d'une pyramide de Ponzi fictive



Sommes versées aux clients qui se retirent



Sommes dues aux clients restants



Sommes dans le compte (après retraits)

Dans cet exemple, le taux annuel promis est de 30 %, alors que le taux « normal » offert par les banques est de 10 %. Nous supposons que le gestionnaire de la pyramide place l'argent dont il dispose à ce taux de 10 %. Les clients retirent ce qu'ils ont déposé au bout de trois années. On imagine que la pyramide recrute chaque année un nouveau client qui y dépose 100 000 euros le 1^{er} janvier. Puisque cette pyramide ne recrute qu'un seul nouveau client, on devine qu'elle ne peut pas tenir bien longtemps. On a noté l'évolution de cette pyramide. Les trois

premières années, la pyramide s'enrichit, car de nouveaux clients viennent y déposer de l'argent et personne n'en retire. Dès la troisième année, quand les clients commencent à retirer de l'argent, avec les intérêts excessifs promis, l'argent détenu par la pyramide se met à décroître. Pour qu'une telle pyramide puisse tenir, il faudrait que l'accroissement des clients soit exponentiel, ce qui bien sûr n'est pas réaliste. Dès la sixième année, la pyramide ne peut pas verser l'argent qu'elle doit au client qui se retire. La pyramide s'écroule.

Après avoir creusé un trou, modéré au début, dans son fond, la pyramide de Ponzi grossit presque contre la volonté de son gestionnaire. Celui-ci espère boucher le trou qui est apparu dû à l'échec de ses méthodes honnêtes, et il se trouve alors entraîné dans une spirale – logarithmique ! – d'actes délictueux (affirmations fausses sur ses méthodes, maquillages des comptes et des transactions, etc.) qui, tôt ou tard, précipitent sa chute.

Où est l'argent ?

Si la pyramide n'est pas standard parce que les épargnants laissent indéfiniment leur argent dans la pyramide, alors le gestionnaire n'a pas nécessairement besoin d'en trouver de nouveaux pour que la pyramide tienne indéfiniment. Les escrocs qui gèrent les pyramides de Ponzi savent que leur seule chance de faire durer la pyramide est que les déposants y laissent leur argent : aussi tentent-ils de les convaincre de ne pas le réclamer. Ils imposent par exemple une durée minimale de placement de plusieurs années et proposent des avantages (augmentation des intérêts) à ceux qui laissent l'argent longtemps.

Intéressons-nous à une pyramide standard à l'instant où elle s'arrête parce que les autorités la font cesser ou parce que son initiateur disparaît ou se dénonce à la police.

Quand la pyramide s'effondre, la question naturelle et inévitable est : où est l'argent ? Il n'a pas pu disparaître, mais alors dans quelles poches cet argent se trouve-t-il ? Bernard Madoff, même avec un mode de vie impérial, n'a pas dépensé une somme équivalente à 100 000 appartements parisiens. Qui détient aujourd'hui l'argent perdu par son système ?

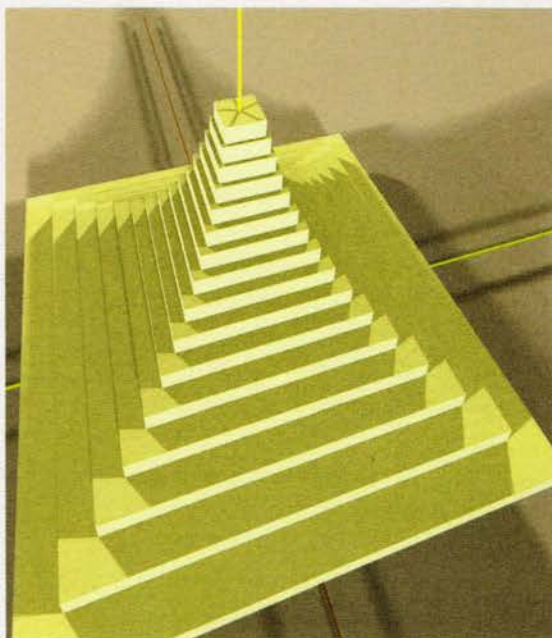
Il ne faut pas croire que tout l'argent dû (et réclamé à cor et à cri par les épargnants) est perdu. Une partie de cet argent est fictive et n'a jamais été dans la poche de personne. Les juges américains chargés de l'affaire Madoff parlent de *fictitious profits*. Si un escroc promet 100% par an et que Monsieur Dupont place 1 000 euros, doit-on dire, quand la pyramide s'effondre au bout de deux ans, qu'il a perdu : (a) 1 000 euros (ce qu'il a versé à la pyramide), (b) 4 000 euros (ce qui lui était promis au bout de deux ans) ou (c) 1 000 euros, plus ce que lui aurait donné un « placement normal » à $X\%$ pendant deux ans, soit $1\,000 \times (1+X/100)^2$ euros ?

La réponse la plus raisonnable est (c) même si cela déplaît à ceux qui ont rêvé de (b). En effet, il n'est pas envisageable de se fonder sur l'argent promis : si un escroc vous fait croire qu'en achetant tel tableau ancien pour 4 000 euros, vous pourrez le revendre le double le lendemain et que cela se révèle faux, tout le monde considérera que vous avez perdu 4 000 euros et non pas 8 000. Il en va de même pour une pyramide de Ponzi : ce que Monsieur Dupont a rêvé et qui n'a jamais existé n'a pas vraiment été perdu. Raisonnablement, l'argent dû aux victimes est (c) (même si les remboursements et indemnisations partielles se font plutôt sur la base de (a)), et c'est à son sujet que la question se pose : où est-il passé ?

Dans le cas de Madoff, quand on parle de 65 milliards de dollars, il s'agit de l'argent rêvé. L'argent vraiment perdu (c) ou (a) est bien inférieur. D'après certaines évaluations mentionnées lors de son procès, il serait de l'ordre de 10 milliards de dollars. Cette dernière évaluation résulte cependant d'un calcul prudent et sans doute incomplet de (a) et il est vraisemblable que, comme dans l'affaire Ponzi, les calculs précis de (a), (b) et (c) resteront impossibles (l'histoire s'étend sur une trentaine d'années!).

Cet argent disparu (c) est composé de quatre parts.

2. La forme d'une pyramide de Ponzi



L'idée est qu'il y a une base croissante de nouveaux déposants pour permettre, à ceux qui le souhaitent, de retirer leur argent. Comme le taux offert par la pyramide est supérieur à celui qu'on peut normalement obtenir et que les investisseurs retirent régulièrement leur argent (par exemple au bout de trois ans), la dette contractée par la pyramide s'accroît exponentiellement. Cela rend nécessaire la souscription d'un nombre toujours plus important de nouveaux clients... jusqu'à ce que la pyramide s'écroule, ne pouvant plus satisfaire les demandes de retrait des clients qui prennent leurs bénéfices.

Les pyramides usuelles sont de mauvaises représentations des pyramides de Ponzi, car leur base ne s'accroît que linéairement si on considère la largeur des tranches (et quadratiquement si on considère l'aire des tranches). Dans le cas d'une pyramide de Ponzi usuelle, l'accroissement de la dette sera exponentiel : chaque nouvelle couche ajoutée en bas de la pyramide pour qu'elle tienne possède une taille obtenue en multipliant par une constante C ($C > 1$) la taille de la couche précédente (illustration de Francesco De Comitè).

Part 1. L'argent que l'escroc et ses complices se sont attribué sous forme de salaires, de commissions, de prétendus profits des fonds, en piochant dans la caisse. Cet argent est dû aux épargnants et l'escroc et ses complices doivent le rendre.

Ces sommes volées aux épargnants sont parfois faibles en regard des sommes manquantes.

Part 2. Des sommes importantes d'argent ont servi à payer des frais liés au fonctionnement de la pyramide : salaires des employés du fonds, loyer des bureaux, commissions diverses, dépenses en publicité, déplacements, impôts, etc.

Cet argent est perdu et ne pourra pas être récupéré. Les employés non complices n'ont pas à rendre leurs salaires ou commissions : ils ont été employés pour faire un travail qu'ils ont réalisé. L'ignorance que leur employeur volait l'argent utilisé pour payer leur salaire ne peut leur être reprochée ! De même, les autres dépenses (loyer, électricité, etc.) sont perdues.

Dans cette part, l'argent payé en impôts par les sociétés faisant fonctionner la pyramide peut être d'une nature un peu différente et, sur le plan des principes, on devrait s'interroger sur son éventuelle restitution aux épargnants floués. Cependant, il est improbable que les victimes le récupèrent : pour l'État, l'argent n'a pas d'odeur et il refuse de rembourser les impôts perçus issus du fonctionnement de la pyramide, même quand sa nature frauduleuse a été établie.

La frontière entre la part 1 et la part 2 est incertaine. Les commissions attribuées aux rabatteurs des fonds Madoff sont ainsi difficiles à classer. Si ces rabatteurs sont des complices, ces commissions sont à mettre dans la part 1, c'est de l'argent volé. Si ces rabatteurs sont seulement d'honnêtes et habiles vendeurs, cet argent est à mettre dans la part 2 et peut être gardé. La réalité que les juges doivent éclaircir est, dans le cas Madoff, très délicate : il y a toute une gamme de nuances entre les indubitables complices informés de la nature des méthodes de Madoff et les naïfs travaillant au service de l'escroc profitant innocemment du système et, souvent, plaçant l'argent gagné dans la pyramide !

Part 3. Si on accepte l'idée que (c) est la bonne évaluation de l'argent qu'on devrait retrouver pour rembourser les victimes et que l'escroc n'a pas placé l'argent à sa disposition pour en tirer un rendement normal, une partie de l'argent disparu (la différence entre (c) et (a)) est passée indirectement dans les caisses de l'État qui, comme quand vous ne placez pas votre argent, en tire du profit du fait de l'inflation. Bien sûr, là encore, l'État n'accepte pas de rembourser ces sommes. L'argent perdu des parts 2 et 3 est comparable à de l'argent perdu par un investisseur qui aurait prêté de l'argent à une entreprise obligée de déposer le bilan.

Part 4. Une part des sommes confiées à la pyramide de Ponzi a été utilisée pour payer ceux qui ont retiré à temps ce qui leur était promis et à qui la pyramide a versé les rendements élevés annoncés. Plus la pyramide fonctionne longtemps, plus cette part de l'argent disparu est proportionnellement importante. Dans le cas Madoff, certains fonds de placement français ont déposé de l'argent dans la pyramide et l'ont retiré avec les intérêts



promis, car un analyste de la banque se méfiait des rendements promis. Votre banque, et vous aussi peut-être, détenez une part de l'argent disparu...

Cet argent peut, en toute logique, être réclamé et l'a été partiellement par exemple dans l'affaire Madoff. Pourtant, à moins que ces clients n'aient été informés de l'escroquerie (ce sont alors des complices), on ne peut guère reprocher aux chanceux ou aux malins qui se sont retirés à temps de l'avoir fait. D'autant plus qu'en prêtant cet argent à un taux élevé, ils ont pris des risques... qu'il est logique de rétribuer.

En connaissance de cause

L'argent disparu par le paiement des intérêts excessifs promis par la pyramide a un statut comparable à celui que gagne un receleur ignorant. Qu'en dit le droit ? En France, l'article 321 du code pénal stipule :

Le recel est le fait de dissimuler, de détenir ou de transmettre une chose, ou de faire office d'intermédiaire afin de la transmettre, en sachant que cette chose provient d'un crime ou d'un délit. Constitue également un recel le fait, en connaissance de cause, de bénéficier, par tout moyen, du produit d'un crime ou d'un délit. Le recel est puni de cinq ans d'emprisonnement et de 375 000 euros d'amende.

La loi est formelle : un individu coupable de recel doit avoir bénéficié « en connaissance de cause [...] du produit du crime ou du délit ». L'argent versé à ceux qui ont su s'échapper à temps de la pyramide n'a pas à être rendu car, s'ils ont bénéficié d'un vol, ils ne le savaient pas.

L'avocat de ceux qui veulent récupérer l'argent auprès de ceux qui se sont sauvés à temps argumentera que le taux proposé par l'escroc, très au-dessus des taux pratiqués ailleurs, montrait qu'il s'agissait d'une pyramide de Ponzi et donc que ceux qui avaient retiré leur argent à temps se doutaient nécessairement qu'ils bénéficiaient d'un argent escroqué et devaient le rendre.

Bien sûr l'avocat des bénéficiaires répondra que, s'il y avait eu des doutes sérieux, les autorités seraient intervenues ; qu'elles aient laissé faire constituait une assurance que le placement était honnête. La défaillance de l'État joue un rôle clé dans l'évaporation de cette part 4.

Son absence de réaction fait que l'État est responsable de cette partie de l'argent soustrait aux victimes et devrait les rembourser... Bien sûr, comme pour les impôts, il ne faut pas y compter et, de surcroît, l'État s'est servi dans cette part 4 par l'impôt (de type impôt sur les plus-values) : non seulement il est responsable des pertes de ceux qui ont perdu, mais il a pris une part à ceux qui ont gagné !

Il existe quelques exceptions à ce refus de l'État : dans l'affaire Madoff, certaines victimes ont obtenu le droit de défalquer de leurs revenus une partie des sommes perdues et la possibilité de récupérer une part des sommes payées au titre d'impôts sur les plus-values.

Notons un paradoxe concernant l'argent gagné par ceux qui se sont retirés à temps. D'un côté, plus ils soupçonnent que l'affaire était une escroquerie, plus ils sont conscients de prendre un risque et plus, sur un plan économique, leur rémunération est justifiée par le risque pris. En revanche, du point de vue du droit, plus les investisseurs soupçonnent l'escroquerie, plus leur situation s'apparente à celles de receleurs informés et plus il est légitime de leur faire rendre l'argent.

3. La vente pyramidale



Assez semblable dans son principe général, l'illusion d'une possible croissance exponentielle indéfinie, la vente pyramidale est une forme d'escroquerie dans laquelle le profit ne provient pas d'une activité de vente, mais principalement du recrutement de nouveaux associés (ou pigeons). Leur nombre doit s'accroître de manière irréaliste, chaque nouvel arrivant retrouvant son investissement initial (versé au niveau au-dessus) par exemple s'il réussit à recruter cinq nouveaux associés. Les chaînes de lettres fonctionnent sur la même illusion.

Seuls les initiateurs du système profitent de la pyramide. Ce type de pratique se cache parfois derrière les termes de marketing multiniveaux ou commercialisation à paliers multiples (MLM *Multi-Level Marketing*). On a tenté d'interdire ces pratiques. La loi n° 95-96 du 1 février 1995 art. 13 (*Journal Officiel* du 2 février 1995) vise ce qu'elle nomme les « Ventes ou prestations » à la boule de neige » et prévoit une amende pouvant aller jusqu'à 4500 euros et une peine de prison maximale d'un an.

Finalement seule la part 1 peut être récupérée et rendue aux victimes. Non seulement les victimes doivent faire le deuil de l'écart entre l'argent rêvé et l'argent qu'un placement normal leur aurait procuré (et cet écart peut être énorme), mais de plus elles doivent faire le deuil des parts 2, 3 et 4. Autant dire que l'affaire est douloureuse et que l'argent perdu l'est bel et bien.

Poussons l'analyse et imaginons le cas extrême d'une pyramide de Ponzi où l'escroc ne se sert pas dans la caisse de la pyramide et n'a pas de frais, car il gère tout lui-même sans payer d'impôts, et en plaçant l'argent de la pyramide à chaque instant au taux normal offert pour les placements de ce type.

Des pyramides de Ponzi équitables ?

Le seul argent perdu quand la pyramide s'écroule est celui qui a été donné à ceux qui se sont retirés à temps par ceux qui sont restés jusqu'à l'instant de l'écroulement. La pyramide n'a alors été qu'un système de transfert d'argent. Tous ceux qui ont participé sont comparables, certains ont gagné ce que d'autres ont perdu dans un jeu équitable, équivalent à une loterie où la totalité de l'argent misé est redistribuée – à la différence près que les investisseurs ne savaient pas qu'il s'agissait d'une loterie.

Le tout n'est donc qu'une sorte de jeu d'argent auquel les participants ont choisi de jouer, aveuglés par l'appât du gain et croyant bénéficier d'un privilège à eux seuls réservés (Madoff persuadait ses clients qu'en prenant leur argent en compte, il leur faisait un cadeau).

Se pose alors la question : n'y a-t-il pas des circonstances particulières où entrer sciemment dans une pyramide de Ponzi est rationnel ?

La question a été analysée plusieurs fois, à propos des systèmes d'assurance sociale et des caisses de retraites qu'on a comparés à des pyramides de Ponzi.

4. Détails sur l'affaire Madoff

L'effondrement d'une pyramide de Ponzi engendre une série de difficultés pour les juges et experts chargés d'indemniser ceux qui doivent l'être. Toutes sortes de situations sont à envisager dans le cas de Madoff.



— Les gens trop près de Bernard Madoff sont suspectés d'être des complices et doivent rendre tout ou partie des biens qu'ils détiennent. C'est le cas des personnes de sa famille et de ses amis dont on pense qu'ils ont été informés de la nature de son fonds, ou à qui on reproche de ne pas avoir voulu comprendre le miracle des rendements proposés par Madoff et des commissions astronomiques qu'il versait aux recruteurs de nouveaux clients.

— Il y a ceux qui ont retiré beaucoup d'argent peu de temps avant la découverte de la fraude et auxquels il est naturel de demander d'en rembourser une partie. Sans les accuser de complicité, le juge chargé de liquider la pyramide n'est pas disposé à admettre que ce qu'ils ont tiré du fonds, au moins dans un passé récent, leur est définitivement acquis.

— Il y a ceux qui ont bénéficié des rendements exceptionnels au travers de fonds qui eux-mêmes plaçaient l'argent chez Madoff sans nécessairement en avertir leurs clients. Ces clients ne peuvent guère être tenus pour responsables, d'autant que parfois on leur avait dit que leur argent était investi en bons du Trésor américain.

La multitude des comptes et transactions opérés dans tous les sens par les fonds Madoff rendent impossible d'y voir clair et aucun règlement équitable de l'affaire ne pourra sans doute jamais avoir lieu. Des questions simples sont

impossibles à trancher : est-ce que les organisations caritatives qui ont reçu des dons de Madoff doivent les rendre (au moins pour les dons récents) ? Les intermédiaires qui touchaient d'importantes commissions, mais qui croyaient à l'honnêteté de Madoff (et plaçaient chez lui une part de leur argent), et ont au final gagné des fortunes grâce à lui, doivent-ils rendre ce qui leur reste aujourd'hui et vendre les appartements achetés grâce aux bons rendements de leur argent placé chez Madoff ?

La part de ceux qui ont retiré de l'argent avec les intérêts importants de Madoff joue un rôle très important dans le bilan qu'on doit faire de la pyramide : citons un exemple rapporté dans le livre *Et surtout n'en parlez à personne* de Romain Gubert et Emmanuel Saint-Simon. L'organisation caritative *Hadassah* (une organisation de femmes qui soutient des projets) annonçait avoir perdu 90 millions de dollars chez Madoff. Cependant, les responsables, en examinant l'histoire de leurs comptes ouverts dès 1987, ont abouti à une conclusion assez étonnante. L'association a déposé 37 millions de dollars au cours des années (principalement en deux fois, à la suite de dons). Les intérêts s'ajoutant aux capitaux déposés, l'association en a pu retirer 130 millions de dollars jusqu'en 2008. Donc, même avec l'annihilation finale du compte consécutive à l'écroulement de la pyramide, l'association a gagné 93 millions de dollars grâce à Madoff. D'autres associations ayant investi plus récemment ont un bilan très négatif et certains investisseurs récents ont même perdu tout ce qu'ils ont déposé sans rien en retirer.

La comparaison est assez juste, mais n'est pas très grave, car la croissance de la population est aussi exponentielle : la pyramide ne s'effondrera pas tant que la croissance de la population se maintiendra, ce qui peut durer des décennies ou même des siècles. De plus, si l'on s'y prend assez à l'avance, des mécanismes sont envisageables pour passer en douceur d'un régime à croissance exponentielle de la population à un régime de population constante ou modérément croissante. Sur d'aussi longues durées, grâce à la lenteur des évolutions, l'assurance sociale et les caisses de retraites sont à certains moments des pyramides de Ponzi. On en modifie progressivement les paramètres pour les transformer à temps en systèmes stabilisés ne risquant pas l'effondrement, et c'est ce qui est en train de se produire dans de nombreux pays aujourd'hui. Entrer dans de telles pyramides de Ponzi, ce qu'on n'a d'ailleurs guère le choix de refuser, n'est en rien irrationnel.

Notons que si vous êtes informé que le fonds de Monsieur X est une pyramide de Ponzi, mais qu'elle ne s'effondrera pas rapidement, il est rationnel d'y déposer votre argent pour quelque temps et de le retirer avec les intérêts supérieurs, si vous savez éviter d'être présent au moment de la chute.

Utpal Bhattacharya, de l'Université d'Indiana à Bloomington aux États-Unis, s'est posé une autre question moins évidente cette fois: est-il toujours irrationnel d'entrer dans une pyramide lors du dernier «round»?

Sa conclusion est qu'il peut être tout à fait rationnel d'entrer dans une pyramide au dernier moment s'il existe un espoir d'indemnisation des victimes après le krach. L'idée générale est que du point de vue de l'analyse du «jeu», cette indemnisation quand elle se produit est assimilable au paiement par ceux qui ne jouent pas d'une somme à ceux qui jouent et qui, du coup, se retrouvent bénéficier d'une espérance positive de gain en acceptant simplement de participer au jeu. Tout se passe pour le déposant comme s'il achetait un billet à une loterie subventionnée qui distribuerait plus d'argent que ce que rapporte la vente les billets.

Comme U. Bhattacharya le note dans son article (publié en 2003), certains schémas financiers et certains fonds d'investissements ressemblent à des pyramides de Ponzi. Utiliser l'argent de l'État pour indemniser les victimes de l'effondrement de tels fonds ne peut qu'encourager des montages de plus en plus risqués et de plus en plus proches des pyramides de Ponzi à effondrement garanti et rapide.

Aujourd'hui, après l'écroulement d'une partie du système bancaire et financier international en 2008, et la décision de nombreux gouvernements d'exiger des contribuables de se porter au secours des établissements défaillants, il est légitime de se demander si on n'a pas assisté et subi (pour ceux qui n'étaient pas «dans la partie») un tel jeu de dupes. Tout ne serait donc qu'une pyramide de Ponzi dont les victimes ne sont pas ceux qui se sont engagés dedans, mais ceux qui, de l'extérieur, renflouent et paient pour que perdure un système profitant à d'autres. En toute logique et en toute équité, on aurait dû refuser de secourir les acteurs des systèmes financiers en détresse à qui aujourd'hui on ne demande pas le remboursement des salaires, primes, commissions et bonus touchés pendant que la pyramide enflait.

Tao : l'éducation réussie d'un surdoué

Qu'il s'occupe de nombres premiers ou de géométrie fractale, Terence Tao invente et produit des résultats mathématiques de première importance. Nombreux sont ceux qui le considèrent comme le meilleur mathématicien vivant.



Terence Tao est un mathématicien sympathique, modeste, aimant travailler avec ses collègues. Il s'intéresse à l'enseignement et à la diffusion des mathématiques vers tous les publics, il est curieux et poursuit des travaux simultanément dans plusieurs domaines de recherche. Avec son épouse Laura, ingénieur à la NASA, ils élèvent leur fils et rien ne semble vraiment extraordinaire dans la vie de cet universitaire aujourd'hui professeur à Los Angeles.

Pourtant, T. Tao est considéré par de nombreux chercheurs comme le plus grand génie vivant des mathématiques. Il est devenu docteur de l'Université de Princeton à l'âge de 20 ans et, une décennie plus tard, ses travaux lui ont valu la plus importante distinction mathématique, la médaille Fields qui lui a été décernée au Congrès international de mathématiques de Madrid en 2006 conjointement avec les Russes Grigori Perelman et Andreï Okounkov, et le Français Wendelin Werner.

Ses parents Billy Tao, pédiatre, et sa mère, Grace Tao, professeur de mathématiques, sont des Chinois cantonnais de Hong-Kong qui émigrèrent en Australie où T. Tao naquit en 1975 à Adélaïde. Alors qu'il avait à peine deux ans, ses parents racontent qu'ils le surprisent en train d'apprendre à compter à un autre enfant... de cinq ans. Quand on lui demanda comment il connaissait les nombres et les lettres, il répondit qu'il les avait appris en regardant l'émission télévisée *Sesame Street*.

Son parcours d'enfant prodige est tout à fait étonnant, mais le plus remarquable dans son cas est l'intelligence qui a été déployée par ses parents et les différents éducateurs et professeurs autour de lui pour l'aider sans le contraindre, le soutenir sans l'enfermer, et lui offrir tout ce qui était nécessaire et utile à l'épanouissement de sa personnalité et de son talent.

Il a suivi un système complexe de scolarité ajustée où, en fonction de sa progression différente selon les disciplines, il assistait à des cours dans plusieurs classes à la fois avec une avance d'un an, deux ans ou plus selon les matières. Ce soin minutieux de son entourage a permis un développement harmonieux de son intérêt pour les mathématiques, en même temps qu'un apprentissage accéléré, progressif et complet de la discipline. Cela lui a forgé une culture profonde et développé chez lui une capacité technique parfaite.

Arrivé à l'âge de mener ses propres travaux, ces qualités ont pleinement produit leurs effets, faisant de lui un être exceptionnellement imaginatif et compétent, d'une efficacité

inégalable, qui adore son métier de mathématicien, semble heureux, ouvert au monde extérieur et doté d'une capacité de travail hors du commun.

Mentionnons quelques étapes de ce parcours ahurissant.

À huit ans, il obtient un total de 760 points sur 800 au test standardisé de mathématiques SAT (*Scholastic Assessment Test*) utilisé aux États-Unis pour mesurer le niveau des élèves à l'entrée au collège, alors que dans toute l'histoire de ce test seul un autre candidat a dépassé 700.

Tableau de chasse

Dès l'âge de neuf ans, il avait atteint le niveau de mathématiques permettant d'entrer à l'Université et commençait d'ailleurs à en étudier les programmes. En 1986, à dix ans, il est le plus jeune compétiteur aux Olympiades internationales de mathématiques et il y reçoit la médaille de bronze. L'année suivante, il obtient la médaille d'argent avant, un an plus tard, d'emporter la médaille d'or qu'il se voit donc remettre avant ses 13 ans, performance qui ne s'était jamais produite.

Il écrit un livre de mathématiques à 15 ans, centré sur les méthodes qu'il utilise pour attaquer et résoudre les difficiles problèmes qu'on soumet aux concurrents des Olympiades mathématiques.

À 20 ans, il soutient une thèse de mathématiques à l'Université de Princeton dans le domaine de l'analyse harmonique sous la direction de Elias Stein... et depuis il a encadré à son tour quatre étudiants en doctorat.

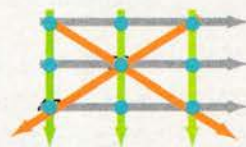
Il reçoit le prix Salem en 2000, le prix Böcher en 2002, le prix de l'Institut Clay en 2003, un prix de l'*American Mathematical Society* et la médaille de la Société australienne de mathématiques en 2005. En 2006, il se voit attribuer le prix Ramanujan et la médaille Fields qui couronne cette série inégalée de récompenses... que nous n'avons énumérée qu'incomplètement.

Le 18 mai 2007, il est élu *Fellow* de la *Royal Society* de Londres, puis, en 2009, il devient membre de l'*American Academy of Art and Science*.

Aujourd'hui, T. Tao a déjà publié plus de 150 articles dans les meilleures revues de mathématiques ainsi que six livres. Il tient aussi un blog extrêmement fourni où il expose et discute les nombreux sujets de recherche auxquels il s'intéresse. John Gardnett, professeur à l'Université de Californie, indique que : « Terry est comme Mozart. Les mathématiques débordent et coulent de lui sans effort. La différence avec Mozart est qu'il n'a aucun problème de personnalité : tout le monde l'aime bien. Il n'y a qu'un mathématicien par génération possédant un tel talent. Le sien est inouï et il est probablement le meilleur mathématicien vivant aujourd'hui. Terry sait débrouiller les problèmes les plus compliqués et les réduit à des choses simples. »

1. Carrés magiques

L'une des conséquences immédiates des résultats de Terence Tao est l'existence de carrés magiques de toutes tailles dont les éléments sont des nombres premiers, comme les carrés magiques d'ordres 3 et 4.



17	89	71
113	59	5
47	29	101

Somme 177

41	89	83
113	71	29
59	53	101

Somme 213

37	83	97	41
53	61	71	73
89	67	59	43
79	47	31	101

Somme 258

41	71	103	61
97	79	47	53
37	67	83	89
101	59	43	73

Somme 276

Il est impossible d'évoquer tous les sujets sur lesquels T. Tao a travaillé et les résultats remarquables qu'il a obtenus, car une large part d'entre eux appartient à des domaines spécialisés des mathématiques dont seuls quelques experts appréhendent le sens. Cependant, plusieurs travaux de T. Tao concernent des parties des mathématiques que tout le monde comprend. C'est bien sûr à ceux-là que nous allons nous intéresser.

Progressions arithmétiques de nombres premiers

Aujourd'hui, l'étude de la suite des nombres premiers avance lentement. Plus d'un siècle avait été nécessaire pour élucider les constatations élémentaires faites par Tchebychev sur les courses de nombres premiers (*voir pages 120-129*). L'un des sujets les plus délicats les concernant est l'étude des écarts qui les séparent. La conjecture des nombres premiers jumeaux énonce par exemple qu'il existe une infinité de couples de nombres premiers séparés de deux unités, comme le sont 11 et 13 ou 857 et 859. Cette conjecture résiste à tous les assauts, malgré les efforts considérables faits pour en venir à bout. Une autre conjecture du même type portait sur les nombres premiers en progression arithmétique; elle est maintenant tombée.

Les nombres premiers 3, 7 et 11 forment une progression arithmétique de longueur 3 et de raison 4:

$$7 = 3 + 4; 11 = 7 + 4.$$

Les nombres premiers 5, 11, 17, 23, 29 forment une progression arithmétique de longueur 5 et de raison 6:

$$11 = 5 + 6; 17 = 11 + 6; 23 = 17 + 6; 29 = 23 + 6.$$

Plus on cherche de longues progressions arithmétiques de nombres premiers, plus il faut aller loin pour le premier terme et accepter que la raison soit grande. Le record de longueur est aujourd'hui de 26 termes; cette progression a été découverte le 12 avril 2010 par Benoît Périchon:

$$43142746595714191 + 23681770.223092870.n, \text{ avec } n = 0, 1, 2, \dots, 25.$$

On ne connaît pas aujourd'hui de progression arithmétique de nombres premiers de longueur 27. Précisons bien qu'il s'agit ici de progressions arithmétiques de nombres premiers non nécessairement consécutifs (par exemple, entre 3 et 7, il y a 5). La recherche de nombres premiers consécutifs en progression arithmétique est aussi intéressante, mais bien sûr plus difficile encore: la plus longue séquence de ce type connue aujourd'hui a pour longueur 10. Elle a pour raison 210 et commence au nombre colossal suivant:

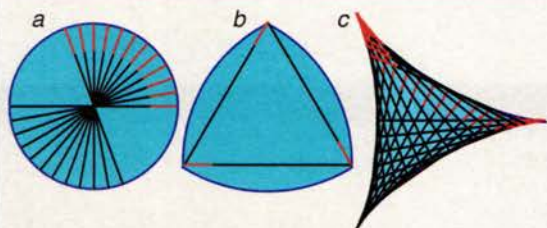
1 009 969 72 469 714 247 637 786 655 587 969 840 329 509 325 689 190 041 803 603
417 758 904 341 703 348 882 159 067 229 719.

Sur ce sujet, toute avancée théorique était considérée comme d'une extrême difficulté. En l'absence de méthodes reconnues, on désespérait même d'obtenir le moindre résultat rapidement. En particulier, les spécialistes considéraient comme hors de portée la démonstration de la conjecture affirmant qu'il existe des progressions arithmétiques de nombres premiers de toute longueur. Pourtant, en 2004, T. Tao et Ben Green, de l'Université de Cambridge, ont réussi l'exploit de démontrer que pour tout entier N donné, il existe une infinité de progressions arithmétiques de nombres premiers de longueur N . Ce résultat est maintenant connu sous le nom de théorème de Green-Tao et il vaut à leurs auteurs l'admiration de tous les chercheurs en mathématiques.

Précisons deux points. (a) Le théorème de Green-Tao ne concerne pas les progressions arithmétiques de nombres premiers successifs ; même si on considère que le résultat est sans doute vrai avec la contrainte « successifs », il faudra encore attendre. (b) Le résultat n'a pas pour conséquence qu'il existe des suites de nombres premiers en progression arithmétique de longueur infinie : il y en a d'aussi longues qu'on le veut, mais pas de longueur infinie. On sait qu'il ne peut pas exister de progression arithmétique de nombres premiers de longueur infinie, car s'il en existait, ils ne se « raréfieraient pas » et cela contredirait le résultat démontré depuis longtemps que la densité des nombres premiers tend vers zéro.

Ce qui a beaucoup étonné la communauté des arithméticiens dans la méthode de preuve utilisée par B. Green et T. Tao est qu'elle est profondément novatrice et provient d'une attaque organisée du problème conçue comme une offensive militaire. T. Tao explique d'ailleurs :

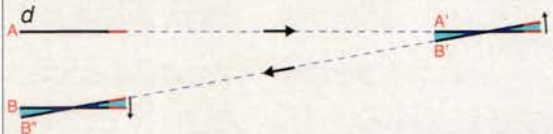
2. L'aiguille de Kakeya



Parmi les sujets sur lesquels Terence Tao travaille, celui né du problème de Kakeya est des plus fascinants. Il s'agit de faire tourner une aiguille de 180 degrés de façon que l'aire balayée soit la plus petite possible. Il est évidemment possible de tourner l'aiguille dans un disque (a), dans un triangle de Reuleaux (b) ou dans la surface qui a été longtemps considérée comme la plus petite possible, la deltaïde (c). En 1928, à la surprise générale, Abram Besicovitch a démontré que l'aire balayée pouvait être réduite autant qu'on le voulait. La méthode se décompose en trois étapes.

I) Pour déplacer une aiguille de longueur 1 d'une position A à une position B parallèle à la position A, on peut réduire l'aire nécessaire autant qu'on veut. Tout tient dans le dessin (d) suivant, où l'aiguille est translatée de A à A', tourne vers B', est translatée vers B'', puis est tournée vers B (lors des deux translations, l'aire balayée est nulle). En utilisant une oblique de plus en plus horizontale, on réduit autant qu'on le veut l'aire (en bleu) balayée par l'aiguille pour passer de A à B.

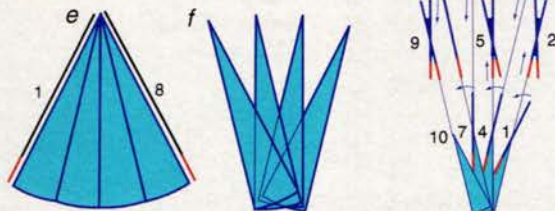
II) Pour faire tourner l'aiguille en diminuant l'aire utilisée, on



découpe le secteur d'angle en secteurs plus petits. Sur le dessin (e), on envisage un secteur de 30 degrés (qu'il faudrait

prendre 6 fois pour obtenir une rotation de l'aiguille de 180 degrés) que l'on découpe en 4 morceaux. On rapproche par translation les 4 morceaux pour qu'ils se superposent le plus possible, ce qui diminue l'aire totale (f). La figure obtenue permet de faire tourner l'aiguille de 30 degrés selon l'opération « en hachoir » (1-2-3-4-5-6-7-8-9-10) indiquée sur la figure g. Au total, on aura une surface d'aire inférieure à celle du secteur initial (e), tout en pouvant toujours faire tourner l'aiguille de 30 degrés.

(III) On opère cette construction de manière répétitive en augmentant par étapes successives le nombre des secteurs, par exemple en le multipliant par 4 à chaque fois. On diminue ainsi autant qu'on le veut l'aire nécessaire à la rotation de l'aiguille. Les arbres obtenus se nomment arbres de Perron, car cette méthode a été



décrite par le mathématicien O. Perron en 1928. Avec 24117248 pièces et 11 étapes de construction, l'aire obtenue est cinq fois plus petite que l'aire du secteur d'angle initial.

T. Tao a démontré que les constructions de ce type en dimension n conduisent à des ensembles qui, même s'ils sont très fins (à la limite, leur aire est nulle), ne le sont pas autant qu'on pourrait le souhaiter : leur dimension fractale est assez grande.

« Beaucoup de gens, face à un problème de mathématiques, tentent de le résoudre frontalement. Même s'ils réussissent, ils ne comprennent pas toujours très bien ce qu'ils ont fait. De mon côté, avant de régler les détails, je travaille la stratégie. Une fois que vous avez la stratégie, même un problème très compliqué se trouve découpé en une série de petits problèmes. Je n'arrive pas à me satisfaire de la simple résolution d'un problème et je cherche toujours à voir ce qui se passe si on change un peu l'énoncé. C'est en expérimentant qu'on accède à la compréhension profonde des situations et qu'on finit par avoir une bonne idée de ce qui est important ou accessoire. »

Même si de telles considérations aident T. Tao à créer des méthodes victorieuses pour affronter les problèmes que les autres mathématiciens ne savent pas résoudre, c'est avant tout parce que T. Tao possède un talent exceptionnel qu'il réussit.

L'un des ingrédients principaux de la méthode de B. Green et T. Tao pour le théorème sur les progressions arithmétiques a été un théorème du mathématicien hongrois Endre Szemerédi qui indique :

« Si un ensemble E de nombres entiers est tel que le rapport

$$[\text{nombre d'éléments de } E \text{ inférieurs à } n] / n$$

 ne tend pas vers zéro, alors E contient des progressions arithmétiques de toute longueur. »

3. Le théorème de Green-Tao

En 2004, Ben Green et Terence Tao démontrent un résultat attendu depuis longtemps : il existe des progressions arithmétiques de nombres premiers aussi longues qu'on le veut. Voici des progressions arithmétiques de toutes les longueurs jusqu'à 26. Pour chaque longueur k , on a indiqué la progression ayant cette longueur et dont le dernier terme est le plus petit possible.

La démonstration de Green et Tao ne se contente pas de prouver qu'il existe pour tout entier k une progression de nombres premiers de longueur k , elle établit qu'on peut trouver une suite arithmétique de nombres premiers de longueur k composée uniquement de nombres inférieurs à :

$$2222222100k$$

En théorie, pour un k donné, cela permet de trouver des progressions arithmétiques de longueur k de manière effective : on essaie toutes les progressions jusqu'à la borne donnée par B. Green et T. Tao ; comme elles sont en nombre fini, on en trouve nécessairement une composée uniquement de nombres premiers. En pratique, il devient très vite impossible de mener le calcul, quels que soient les moyens informatiques utilisés.

Les calculs menés pour les petites valeurs de k montrent que la borne donnée par le théorème de Green-Tao pourrait être remplacée par la borne bien plus petite : $k! + 1$.

k	Progression	Dernier terme
3	$3 + 2n$	7
4	$5 + 6n$	23
5	$5 + 6n$	29
6	$7 + 30n$	157
7	$7 + 150n$	907
8	$199 + 210n$	1669
9	$99 + 210n$	1879
10	$199 + 210n$	2089
11	$110437 + 13860n$	249037
12	$110437 + 13860n$	262897
13	$4943 + 60060n$	725663
14	$31385539 + 420420n$	36850999
15	$115453391 + 4144140n$	173471351
16	$53297929 + 9699690n$	198793279
17	$3430751869 + 87297210n$	4827507229
18	$4808316343 + 717777060n$	17010526363
19	$8297644387 + 4180566390n$	83547839407
20	$214861583621 + 18846497670n$	572945039351
21	$5749146449311 + 26004868890n$	6269243827111
22	$11410337850553 + 47518019n$	08201410428753
23	$403185216600637 + 9523 \cdot 23n$	449924511422857
24	$515486946529943 + 136831 \cdot 23n$	1217585417914253
25	$6171054912832631 + 366384 \cdot 23n$	8132758706802551
26	$43142746595714191 + 23681770 \cdot 223092870 \cdot n$	175223597495211691

Ce résultat ne s'applique pas directement aux nombres premiers, car justement le rapport mentionné tend vers 0 si E est l'ensemble de nombres premiers. Cependant, ce résultat délicat possède plusieurs démonstrations récemment élaborées et c'est en extrayant les éléments importants et en les combinant que B.Green et T.Tao ont pu mener leur attaque stratégique et obtenir la conclusion recherchée pour l'ensemble E des nombres premiers. La démonstration est qualifiée d'élémentaire, car elle ne met pas en œuvre les méthodes de théorie analytique des nombres (faisant usage de fonctions à variables complexes) qu'on pensait pourtant essentielles à la réussite de ce type d'exploits.

Une chose remarquable à propos du théorème de Green-Tao est qu'il a de très nombreuses conséquences intéressantes conduisant en particulier à traiter d'autres conjectures, dont par exemple celle affirmant l'existence de carrés magiques de nombres premiers de toutes les tailles (*voir l'encadré 1*). L'idée est de partir d'un carré magique classique (donc composé avec les nombres entiers $1, 2, \dots, n^2$) et de remplacer partout dans le carré magique le terme i par le i -ème terme d'une progression arithmétique de nombres premiers de longueur n^2 .

Faire tourner une aiguille ?

Parmi les thèmes auxquels T.Tao s'intéresse et qu'il contribue à faire progresser, l'un d'eux est particulièrement fascinant, car, bien que formulé au départ comme un problème géométrique élémentaire, il s'est révélé avoir des liens avec de nombreux autres sujets mathématiques. Il s'agit des diverses variantes et généralisations du problème de Kakeya.

Quel espace faut-il pour faire demi-tour ? En voiture, pour faire un demi-tour, il vous faut disposer d'une certaine aire autour de la voiture. Simplifié par les mathématiciens, le problème devient celui du demi-tour d'une aiguille ou problème de Soichi Kakeya, que

4. Changer un seul chiffre...

Le nombre premier 127 écrit en base 2 est 1111111. En modifiant l'un de ses chiffres, on a :

1111110 = 126; 1111101 = 125;

1111011 = 123; 1110111 = 119;

1101111 = 111; 1011111 = 95; 0111111 = 63.

Ce sont tous des nombres composés. Autrement dit, le nombre 127 est premier, mais dès qu'on change l'un de ses chiffres en base 2, il devient composé. Nous dirons que 127 est un nombre premier instable en base 2 (*weakly prime number in base 2*). C'est le cas aussi de 173, 191, 233.

Existe-t-il une infinité de tels nombres ?

Et en base 10, existe-t-il de tels nombres ?

Dans un article récent de 2008, T.Tao donne une solution complète du problème : dans toute base de numération B , il existe une infinité de nombres premiers instables. Le résultat précise même que dans toute base B , la proportion de ces nombres premiers parmi les n premiers nombres premiers est strictement supérieure à une constante positive (autrement dit, ces nombres ne se rarefont pas à l'infini).

En base 10, les premiers nombres premiers instables sont : 294 001 ; 505 447 ; 584 141 ; 6 04 171 ; 971 767 ; 1 062 599 ; 1 282 529 ; 1 524 181 ; 2 017 963 ; 2 474 431 ; 2 690 201 ; 3 085 533 326 489 ; 4 393 139 ; 5 152 507 ; 5 564 453 ; 5 575 259 ; 6 173 731 ; 6 191 371 ; 6 236 179 ; 6 463 267 ; 6 712 591 ; 7 204 777 ; 7 469 789.

Ce type de résultats a une certaine importance pour les tests de primalité (algorithme pour savoir si un nombre entier est un nombre premier ou non). En effet, si un nombre n est donné à un algorithme sous la forme de la suite de ses chiffres en base 10 par exemple, le résultat de Tao a pour conséquence que l'algorithme ne peut établir que le nombre est premier qu'après avoir pris connaissance de tous ses chiffres.

Pour un nombre donné, un test de primalité devra donc mener un calcul au moins proportionnel à sa longueur L : il ne peut pas exister de test très rapide de primalité comme il en existe pour déterminer si un nombre est divisible par 2 ou 5 (le dernier chiffre suffit), par 4 (les deux derniers chiffres suffisent).

Comme le fait remarquer T. Tao dans son blog, le résultat sur la fréquence de ces nombres, associé au résultat sur les suites arithmétiques de nombres premiers, permet d'affirmer qu'il existe des suites arithmétiques de nombres premiers instables en base B (B quelconque) de toute longueur.

Les nombreuses remarques que contient l'article où il démontre ce résultat illustrent la méthode de T. Tao : après avoir démontré le théorème principal, il en examine soigneusement les hypothèses une à une, envisage les généralisations possibles, recherche des contre-exemples, et commente les conséquences algorithmiques de son travail.

5. Un peu de magie

Ensembles magiques

Les ensembles magiques de nombres premiers sont des ensembles de nombres premiers tels qu'en faisant la moyenne deux à deux des éléments de l'ensemble, on ne trouve que des nombres premiers tous distincts. L'ensemble {3, 7, 19} est magique, car la moyenne entre 3 et 7 vaut 5 (qui est premier), entre 7 et 19 elle vaut 13 (qui est premier), entre 3 et 19 elle vaut 11 (qui est premier).

Voici un tableau des quelques ensembles magiques.

- | | |
|----|--|
| 2 | 3, 7 |
| 3 | 3, 7, 19 |
| 4 | 3, 11, 23, 71 |
| 5 | 3, 11, 23, 71, 191 |
| 6 | 3, 11, 23, 71, 191, 443 |
| 7 | 5, 17, 41, 101, 257, 521, 881 |
| 8 | 257, 269, 509, 857, 1697, 2309, 2477, 2609 |
| 9 | 257, 269, 509, 857, 1697, 2309, 2477, 2609, 5417 |
| 10 | 11, 83, 251, 263, 1511, 2351, 2963, 7583, 8663, 10691 |
| 11 | 757, 1009, 1117, 2437, 2749, 4597, 6529, 10357, 11149, 15349, 21757 |
| 12 | 71, 1163, 1283, 2663, 4523, 5651, 9311, 13883, 13931, 14423, 25943, 27611. |

Une des conséquences du théorème de Green-Tao est qu'il existe des ensembles magiques aussi grands que l'on veut.

Ensembles supermagiques

Pour construire les ensembles supermagiques de nombres premiers, on impose que toutes les moyennes (de deux nombres ou plus) soient des nombres premiers et que tous les nombres premiers ainsi obtenus soient différents.

Comme l'a montré Andrew Granville, le théorème de Green-Tao implique qu'on peut trouver de tels ensembles aussi grands que l'on veut. Pourtant, en pratique, on ne sait pas aller plus loin que ceux-ci :

- | | |
|---|---|
| 2 | 3, 7 |
| 3 | 7, 19, 67 |
| 4 | 5, 17, 89, 1277 |
| 5 | 209173, 322573, 536773, 1217893, 2484733. |

celui-ci posa en 1917: quelle est la plus petite surface permettant à une aiguille de longueur 1 de faire un demi-tour?

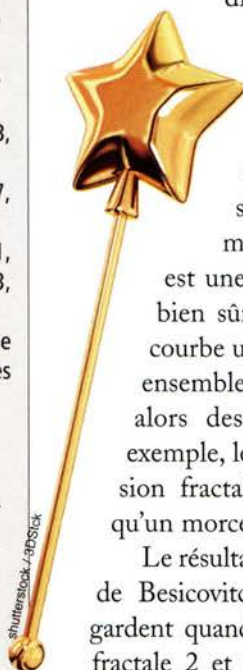
Bien sûr, un cercle de diamètre 1 suffit et donc le nombre cherché est inférieur à $\pi/4 = 0,78539...$ (l'aire du cercle de diamètre 1). Un triangle équilatéral de hauteur 1 suffit encore et possède une aire un peu plus petite qui est $\sqrt{3}/3 = 0,57535...$ Cependant, à la surprise générale, le mathématicien russe Abram Besicovitch démontra en 1919 que, quel que soit le nombre $\epsilon > 0$ qu'on se fixe, il est possible de trouver un morceau du plan d'aire inférieure à ϵ permettant le demi-tour d'une aiguille de longueur 1. L'encadré 2 donne l'idée de la démonstration de cet étonnant résultat.

Depuis, on s'intéresse au problème des sous-ensembles du plan possédant un segment de longueur 1 dans toutes les directions possibles, les «ensembles de Besicovitch». On généralise bien sûr la définition à toutes les dimensions n .

Parmi les résultats démontrés, l'un d'eux, dû à Roy Davis en 1971, indique que même si un ensemble de Besicovitch du plan est d'aire nulle, il contient tellement de points que sa dimension fractale de Minkowski est nécessairement 2. La dimension fractale d'un ensemble est une sorte de mesure de sa densité: un point a bien sûr une dimension fractale égale à 0, et une courbe une dimension égale à 1. Cependant certains ensembles fractals sont de nature intermédiaire et ont alors des dimensions fractales non entières. Par exemple, le fameux flocon de von Koch est de dimension fractale $3/2$: c'est plus qu'une courbe et moins qu'un morceau de plan.

Le résultat de R. Davis signifie donc que les ensembles de Besicovitch du plan, bien qu'ayant une aire nulle, gardent quand même la propriété d'avoir une dimension fractale 2 et sont donc en quelque sorte «extrêmement épais». Ce résultat est important et l'on pense qu'il s'étend à toutes les dimensions. Cette conjecture est toujours non démontrée, mais on progresse et il est étonnant de voir à quel point elle a intéressé de prestigieux mathématiciens dont Jean-Pierre Kahane (membre de l'Académie des sciences), Charles Fefferman (médaillé Fields 1978), Jean Bourgain (médaillé Fields 1994), Timothy Gowers (médaillé Fields 1998) et T. Tao (médaillé Fields 2006).

En 1999, J. Bourgain a établi que la dimension fractale d'un ensemble de Besicovitch était d'au moins $0,52n + 0,48$,



ce qui donne par exemple : 3,08 pour $n = 5$; 5,68 pour $n = 10$; 52,48 pour $n = 100$. Ces résultats ont été améliorés par Nets Katz et T. Tao qui ont obtenu : 3,58 pour $n = 5$; 6,51 pour $n = 10$; 59,23 pour $n = 100$.

Le problème a toutes sortes de variantes intéressantes et c'est l'un des domaines préférés de T. Tao qui, en plus du record qu'on vient de citer concernant la conjecture de Makeya, a publié plusieurs articles importants sur le sujet.

Changement d'un chiffre

T. Tao a une sensibilité de mathématicien moderne. Outre qu'il sait programmer, il connaît bien les problèmes de l'informatique théorique et ne dédaigne pas de s'y intéresser. L'un de ses résultats sur les nombres premiers concerne la densité des nombres premiers qui deviennent composés dès qu'on en modifie un chiffre. Ce résultat a des conséquences pour les algorithmes qui testent si un nombre est premier ou non.

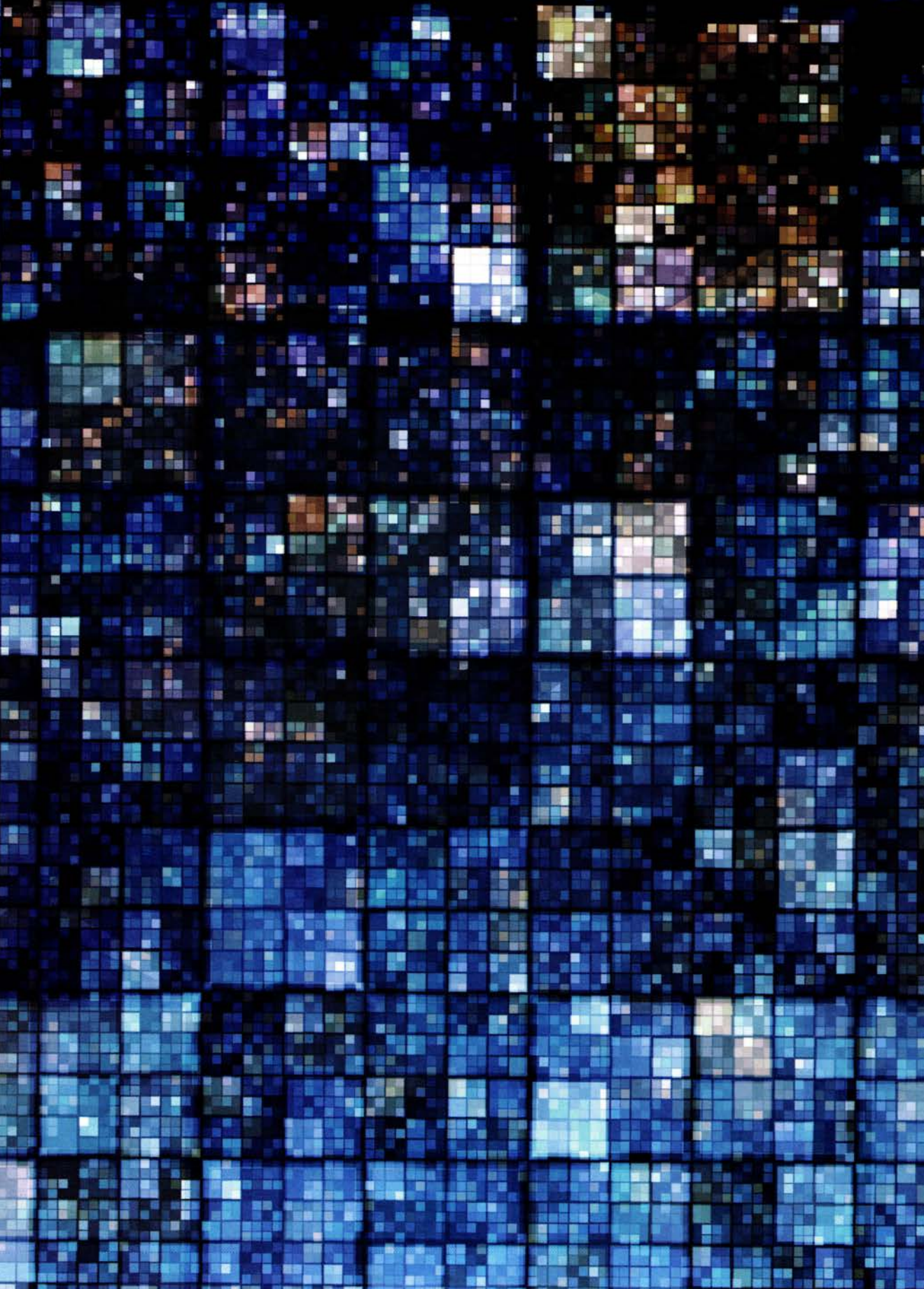
Contrairement à certains mathématiciens qui éprouvent une certaine hésitation, voire de la répugnance, à évoquer toute considération un peu vague à propos des mathématiques, T. Tao (en particulier dans son blog) n'hésite pas à s'adonner à des réflexions méthodologiques, philosophiques ou logiques sur les mathématiques. La recherche des principes généraux de raisonnement ou d'analyse des situations le préoccupe de manière continue et semble jouer un rôle central dans son approche stratégique des questions les plus difficiles.

Récemment, ses réflexions sur divers principes généraux comparables pour l'analyse au principe des tiroirs ont conduit deux logiciens, Jaime Gaspar et Ulrich Kohlenbach, de l'Université de Darmstadt en Allemagne, à une série de résultats très fins sur les axiomatiques de l'analyse. Chose amusante à ce sujet, qui montre que T. Tao, tout aussi génial qu'il soit, est sujet comme tout le monde à l'erreur, la formulation d'un des principes généraux d'analyse par T. Tao s'est révélée fausse, et il a dû en proposer une version corrigée.

Réflexions sur les fondements, modernité, ouverture

Toujours dans le cadre des analyses stratégiques et méthodologiques générales, T. Tao aime bien mentionner le hasard et le pseudohasard qu'on trouve dans les objets mathématiques. Dans le cas de l'ensemble des nombres premiers, l'idée est d'évaluer leur importance relative et d'exploiter les deux composantes (structurée et aléatoire) de cet ensemble infini pour les contrôler simultanément, ce qui est important dans le cas des suites arithmétiques de nombres premiers. Il est clair en effet que, d'une part, les nombres premiers constituent un ensemble très structuré (à partir de 2, il n'y a plus aucun nombre premier pair ; la densité des nombres premiers est bien déterminée, etc.) et que, d'autre part, cet ensemble a aussi des traits qui le rapprochent des objets aléatoires : la conjecture de Riemann s'interprète d'ailleurs comme l'affirmation que la parité du nombre de facteurs premiers des entiers se comporte comme une suite aléatoire (*voir page 122*).

On le voit, loin d'être seulement un technicien parfait à l'efficacité surhumaine, T. Tao construit sa conception des mathématiques sur des bases modernes et recherche autant que possible à prendre du recul pour apercevoir l'univers mathématique dans sa totalité, dont il est sans doute aujourd'hui celui qui en comprend le mieux les mystères et la beauté.



La logique rencontre la physique

Plongés dans les apparences d'un monde classique, les physiciens nous disent que nous ne pouvons que comprendre imparfaitement la logique du monde quantique. C'est sans doute dommage, car la mécanique quantique concerne notre libre arbitre comme John Conway le met en évidence, et car elle nous force à reformuler la logique du tout de l'Univers et de nos modes d'action sur lui, ce que l'idée du suicide quantique prouve. Quant à l'affirmation risquée que le monde est un ordinateur, elle nous plonge dans une série d'énigmes dont il faut à nouveau nous amuser plutôt que nous en inquiéter.

Concevoir l'univers comme un ordinateur

La science-fiction devance parfois la science. Une étrange nouvelle d'Isaac Asimov sur le devenir ultime de l'humanité semblait dessiner un programme de recherche et même en prévoir les résultats...

Isaac Asimov considérait que sa meilleure nouvelle, parmi les centaines qu'il nous a laissées, était *The Last Question* parue en novembre 1956 dans la revue *Science-Fiction Quarterly*. La traduction française, *La dernière question*, a été publiée dans *Le robot qui rêvait* (J'ai lu, 1988).

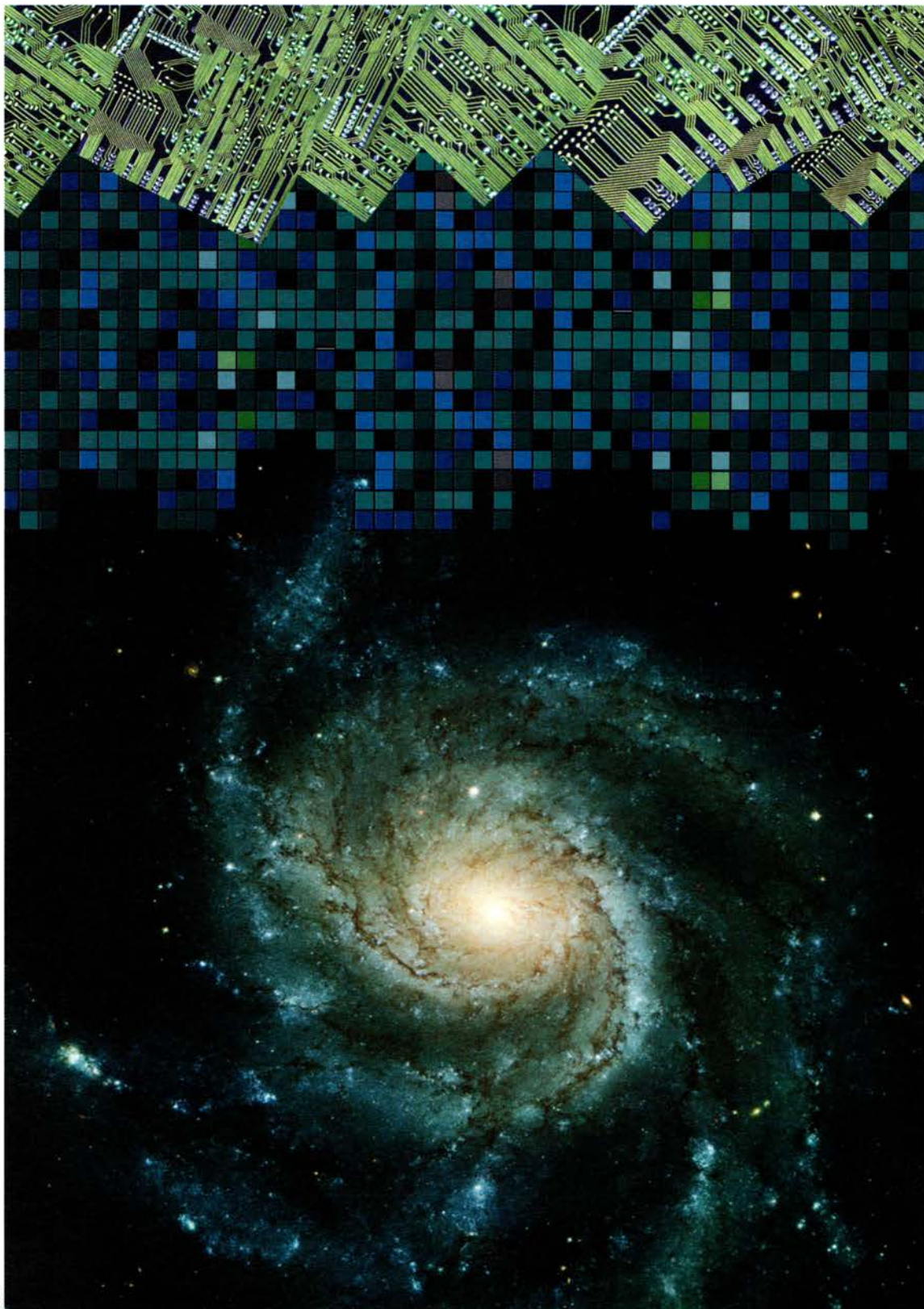
Dans ce texte d'une vingtaine de pages, Asimov raconte l'histoire, à partir de 2061, d'un ordinateur nommé *AC*, qui devient de plus en plus puissant et auquel l'humanité remet progressivement son destin en lui posant toutefois régulièrement la question : « Comment l'entropie peut-elle être inversée ? » Car l'augmentation inévitable de l'entropie résultant du second principe de la thermodynamique semble condamner l'humanité à « la mort thermique », un état du monde où toutes les températures s'étant égalisées, plus aucun travail ne peut être accompli (car pour produire du travail, il faut une source chaude et une source froide) et plus aucune vie n'est possible. Dans le récit d'Isaac Asimov, à chaque fois la machine répond : « Il n'y a pas encore assez de données pour une réponse significative. »

L'histoire qui s'étend sur « dix trillions d'années » se termine dans un univers où l'homme ayant disparu, *AC* découvre enfin la solution à la question : « Et il advint que *AC* comprit comment inverser la direction de l'entropie. Mais il n'y avait plus d'hommes à qui *AC* pouvait donner la réponse. Peu importait. La réponse serait donnée dans les faits. Pendant une nouvelle période hors du temps, *AC* réfléchit au meilleur moyen de s'y prendre. Avec soin *AC* organisa ses programmes. Le conscient de *AC* embrassa tout ce qui avait été un Univers et réfléchit sombrement à ce qui était maintenant le Chaos. Étape par étape, il fallait que cela advienne. Et *AC* dit : « Que la lumière soit ! Et la lumière fut. »

La fin de cette nouvelle ambitieuse contiendrait la première mention de l'idée que l'univers tout entier pourrait n'être qu'un ordinateur. L'idée d'Asimov est bien celle d'un monde qui recommence et qui n'est que l'exécution d'un programme.

Cette idée d'un monde-ordinateur ou d'un univers de calcul a séduit quelques chercheurs visionnaires et spéculateurs qui la déclinent assez différemment. Le récent livre de Seth Lloyd (spécialiste de mécanique quantique et professeur au MIT) intitulé *Programming the Universe* en fait son thème central et tente d'en examiner les différents aspects.

1 Le modèle le plus simple d'univers-ordinateur est celui des automates cellulaires. Une difficulté de leur utilisation est que la présence de cases qui pavent l'espace introduit des directions privilégiées, alors que toutes les expériences montrent que l'univers est globalement isotrope.



Dès 1969 cependant – 13 ans après la parution de la nouvelle d'Asimov et sans doute indépendamment –, Konrad Zuse (1910-1995) proposa de donner de la consistance scientifique à l'idée d'un univers qui ne serait qu'un grand calcul. Konrad Zuse est l'ingénieur allemand qui a conçu et mis au point, en 1941, le premier ordinateur général à programmes enregistrés; bien que son nom soit assez peu connu, il est l'un des personnages les plus importants de l'histoire de l'informatique, à l'égal d'Alan Turing ou de John von Neumann.

Konrad Zuse, inventeur et théoricien

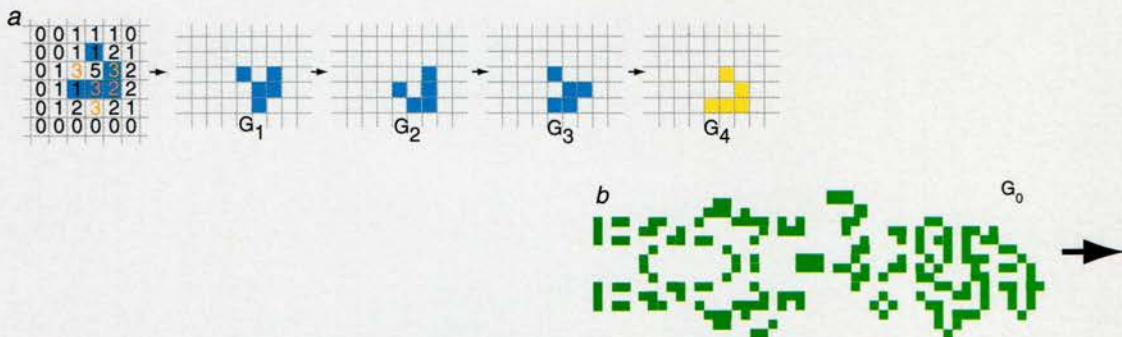
Le livre de ce visionnaire *Rechnender Raum* de 1969 (la version anglaise, *Calculating Space*, est téléchargeable sur internet) explore l'idée que des réseaux d'automates cellulaires servent de modèles pour décrire une physique totale et ultime du monde, où tout ce qui s'y déroule est ramené à un calcul discret, c'est-à-dire évitant l'utilisation du continu. Le continu – l'ensemble des nombres réels – est aujourd'hui un outil employé sans précaution par tous les physiciens pour décrire le temps, l'espace et de très nombreuses variables de la physique. Cependant, certains physiciens sont gênés par ce continu qui crée des situations jugées invraisemblables.

Le prix Nobel de physique 1965, Richard Feynman – et il n'est pas le seul – a exprimé clairement son malaise: «J'ai toujours été intrigué par le fait qu'en suivant les lois de la nature telles que nous les comprenons aujourd'hui, il faudrait à un ordinateur une infinité d'opérations logiques pour décrire ce qui se produit dans une région finie de l'espace et dans un intervalle de temps borné, et cela aussi petits qu'ils soient. Comment cela se passe-t-il donc dans le petit espace? Pourquoi faudrait-il une quantité infinie d'opérations logiques pour rendre compte de ce qui se déroule au sein d'un tout petit morceau de l'univers?»

2. Réseau d'automates cellulaires

Un réseau d'automates cellulaires sur le plan est un quadrillage dont chaque case est occupée par un automate. L'automate du *Jeu de la vie* de Conway est un exemple merveilleux d'automate cellulaire susceptible d'engendrer de la complexité à partir de presque rien. Le monde du *Jeu de la vie* est un plan infini quadrillé, dont chaque case (ou cellule) est soit occupée, soit vide. Chaque case

possède huit voisines et d'une génération à l'autre des naissances et des décès s'y succèdent mécaniquement selon la règle: si une case est vide et que 3 de ses voisines sont occupées, alors une naissance s'y produit; si une case est occupée, la survie n'y est possible que si 2 ou 3 cases voisines sont occupées; dans tous les autres cas, la case se retrouve vide à la génération suivante. En



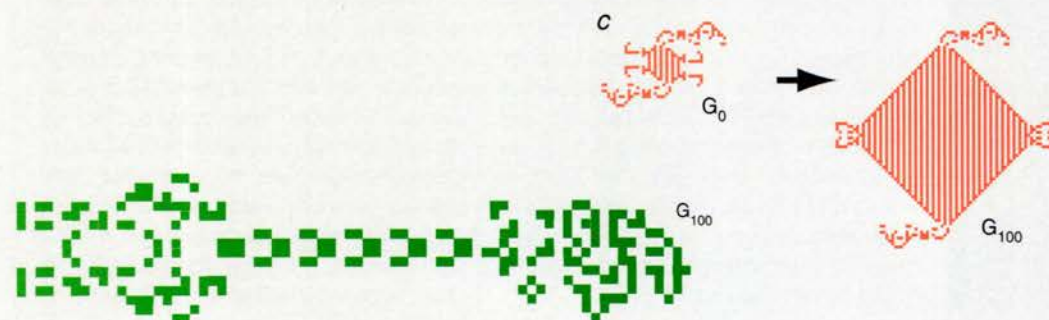
Les réseaux d'automates cellulaires inventés dans les années 1940 par Stanislas Ulam et John von Neumann – ce dernier les utilisant pour établir la possibilité logique d'organismes autorépliqueurs dans un monde déterministe – sont le modèle de calcul discret le plus simple qu'on puisse imaginer et, comme nous le verrons, c'est à eux que nous pensons en premier quand nous envisageons une physique débarrassée du continu et ramenée à un immense calcul.

Dans le modèle des automates cellulaires, l'espace (de dimension 1, 2, 3 ou même plus) est divisé en cases dénommées cellules, par exemple un pavage par des carrés ou des cubes. Chaque case ou cellule est occupée par un automate qui peut prendre deux états différents (disons 0 pour vide, et 1 pour occupé) ou plus, et qui, d'une étape à l'autre – d'un instant au suivant – change d'état en tenant compte de ses voisins – par exemple ses 8 voisins si nous sommes dans un plan divisé en cellules carrées. À chaque pas de l'évolution du réseau, chaque automate, partant de son état présent et de son environnement proche, détermine son nouvel état en appliquant des règles fixées une fois pour toutes, règles qui sont les mêmes pour toutes les cellules du réseau. Les règles du *Jeu de la vie* de John Conway – le réseau d'automates cellulaires le plus célèbre – sont explicitées sur la figure 2 et peuvent se résumer, pour les cases vides, par « Naissance si 3 voisins » et, pour les cases pleines, « Survie si 2 ou 3 voisins, mort sinon ».

Notons bien que, dans un tel monde, le temps est discret, l'espace est discret, et l'évolution se fait localement en opérant un calcul élémentaire décrit par un calcul fini identique pour toutes les cases : aucun infini, aucune transmission instantanée d'information à distance. Tout y est granulaire et borné sauf peut-être l'étendue de l'espace qu'on peut imaginer illimitée, mais ce n'est même pas nécessaire, car on peut décréter que tout se déroule dans un grand rectangle dont les bords se rejoignent (tore). Pour Zuse, ces modèles résoudreient peut-être l'interrogation sur le continu : « Il apparaît qu'une question justifiée est de savoir si des quantités indéfiniment divisibles (en d'autres termes des

résumé, naissance si 3 voisins ; survie si 2 ou 3 voisins. Ces règles, choisies parce qu'elles sont naturelles (la vie nécessite déjà de la vie, mais trop de vie provoque l'étouffement) et qu'elles engendrent un monde inattendu, ont dépassé toutes les espérances de leur inventeur. Certaines configurations ont la propriété de se déplacer, on les dénomme navire, un exemple

étant représenté en (a). D'autres configurations s'étendent indéfiniment (b). D'autres pavent le plan (c) avec une densité 1/2, d'autres réalisent des calculs complexes comme simuler le hasard ou énumérer les nombres premiers. Cette diversité répond à Leibniz qui s'étonnait que des lois globales engendrent un monde différencié.



quantités continues) ont une réalité dans la nature. Quelles seraient les conséquences si nous adoptions une discrétisation totale pour les lois de la nature et supposions que, par principe, toutes les valeurs physiques sont discrétisées ? »

Ce livre visionnaire examine alors un modèle d'interaction entre particules décrit dans un formalisme d'automates cellulaires. L'« espace calculant » comme il le nomme, semble, d'après ces premiers essais, capable de modéliser des phénomènes physiques complexes. Cependant Zuse est conscient des difficultés qu'introduit ce modèle et que l'on examine encore aujourd'hui : « Une structure de grille abolirait la structure isotrope de l'espace. » C'est bien un grave problème puisque, remarque-t-il : « Nous ne disposons d'aucune expérience physique qui indiquerait des directions privilégiées comme il y en a nécessairement dans un espace découpé en cases. [...] L'hypothèse d'une grille entraîne celle d'un système de coordonnées privilégiées, ce qui contredit la théorie de la relativité. »

Fredkin et la mécanique digitale

Pour Zuse, l'idée que la physique pourrait se réduire aux calculs d'automates cellulaires est intéressante par l'économie de moyens qu'elle permet. Il n'en fait cependant pas un credo comme plusieurs de ses successeurs et est bien conscient des doutes qu'on peut avoir sur le succès d'une telle entreprise.

Après Zuse, le premier, et peut-être le plus acharné, des adeptes de l'idée d'un monde à base d'automates cellulaires – donc d'un univers-ordinateur – est Edward Fredkin qui explorera plus avant l'idée d'un monde physique réduit à un mécanisme localement fini de calcul.

Dans son essai intitulé *Finite Nature*, E. Fredkin proclame : « Jusqu'à présent toutes les questions concernant l'opposition discret/continu à propos des propriétés de notre monde

3. Konrad Zuse



Konrad Zuse a conçu de véritables ordinateurs et imaginé que le monde dans sa totalité pourrait être un ordinateur.

En 1941, Konrad Zuse est mobilisé dans les usines allemandes d'aviation *Henschel* qui travaillent pour le Troisième Reich. Avec une dizaine de personnes, il conçoit et met au point une machine qu'il nomme Z3 et qui est le premier ordinateur général fonctionnant avec des programmes enregistrés. La machine comporte 2600 relais, une console de commande et un lecteur de bande perforée avec les instructions à exécuter, c'est-à-dire le programme qui est donc indépendant du reste de la machine. La mémoire de la machine est de 64 nombres de 22 bits, c'est-à-dire de 176 octets ! La Z3, qui exécute une addition en un quart de seconde et une multiplication en moins de 5 secondes, est détruite dans un bombardement allié en avril 1945.

Le modèle suivant, le Z4, est plus performant. Zuse et son équipe évitent sa destruction : en 1945, ils le démontent et fuient Berlin avant l'arrivée de l'armée russe. Les troupes alliées le trouvent, mais ne s'y intéressent pas. Après la guerre, le Z4 est installé à l'École polytechnique de Zurich, puis à Bâle dans un institut de recherche aérodynamique où il est utilisé jusqu'en 1960.

Parallèlement à son travail de concepteur et de réalisateur d'ordinateurs, Zuse se demande si le monde n'est pas au fond une sorte de grand ordinateur. Son livre *Rechnender Raum* (*L'espace calculateur*) de 1969 propose d'utiliser les réseaux d'automates cellulaires pour décrire les phénomènes physiques et, pourquoi pas, une physique ultime du monde où tout ce qui se déroule est ramené à un calcul discret et local. Cette idée sera reprise par Edward Fredkin et suscite encore aujourd'hui travaux et débats.

sont restées ouvertes ou résolues en faveur du discret [...] Dans l'hypothèse d'une nature finie, cette évolution historique se poursuivra jusqu'à sa conclusion logique : à un niveau suffisamment fin, tout se révélera atomique ou discret, y compris l'espace et le temps. »

E. Fredkin a écrit une série d'articles et une ébauche de livre pour rendre hommage à Zuse. Il y développe ce qu'il nomme la *Mécanique digitale* (voir : <http://www.digital-philosophy.org/>) et explore l'hypothèse qu'on ramènera un jour tout à un réseau d'automates cellulaires... lequel reste à découvrir. Les difficultés créées par l'isotropie de notre monde, l'absence de repères fixes énoncée comme principe par la théorie de la relativité et d'autres ennuis soulevés par la mécanique quantique (où l'intrication est une sorte de lien entre des parties éloignées d'un système physique apparemment incompatible avec un modèle d'automates cellulaires) y sont examinés. La réponse est en gros que l'espace cellulaire du réseau n'est pas nécessairement identique à l'espace modélisé par le réseau. L'argument s'appuie sur le fait que certains automates cellulaires – comme le *Jeu de la vie* de Conway – ont la propriété d'être universels, c'est-à-dire de pouvoir simuler n'importe quel calcul ; donc n'importe quel espace peut être simulé, au moins de manière approchée, par de tels réseaux d'automates.

Nous n'examinerons pas cet argument peu satisfaisant (car si l'espace des automates cellulaires n'est pas celui de la physique, à quoi sert d'utiliser un réseau d'automates cellulaires ?). Plus proches des véritables problèmes de la modélisation des systèmes physiques, Tommaso Toffoli, Norman Margolus et d'autres chercheurs ont utilisé les réseaux d'automates cellulaires pour modéliser divers problèmes précis : particules en mouvement avec collisions, phénomènes d'hydrodynamique, transitions de phase, ondes diverses, réseaux de spins, diffusion de la chaleur, etc. Les automates cellulaires sont ainsi devenus au cours des années un outil de modélisation reconnu et accepté. Aujourd'hui, des réunions scientifiques régulières permettent aux chercheurs intéressés de se retrouver. La septième conférence internationale *Cellular Automata for Research and Industry* s'est par exemple réunie en septembre 2006 à Perpignan.

Stephen Wolfram

À côté de ces travaux d'un intérêt pratique indubitable, d'autres chercheurs plus spéculatifs, préoccupés par l'idée d'une physique authentiquement finie et discrète, et donc informatique, ont continué à s'interroger et à explorer toutes sortes de pistes pour éliminer le continu. Citons parmi eux Donald Greenspan (*Discrete Models*), Pierre Noyes (*Bit-string Physics*), David Hiebeler (*Discrete Physics*), Bohdan Shepelavey et Felix Lev (*Finite Physics*), Stanly Steinberg (*Mimetic Discretizations of Continuum Mechanics*) qui tous s'opposent à l'utilisation du continu en physique et proposent des méthodes pour l'éviter partiellement ou totalement. Un adepte du finitisme en physique mérite une mention spéciale, car il a beaucoup fait parler de lui en publiant un étrange livre : il s'agit de Stephen Wolfram.

Après une brève et brillante carrière de chercheur en physique théorique (où il étudia entre autres les réseaux d'automates cellulaires), Stephen Wolfram a dirigé et développé l'entreprise informatique qui vend le logiciel de calcul formel *Mathematica*. En 2002, après des années de silence scientifique et devenu riche grâce à son entreprise, il publie à compte d'auteur un énorme ouvrage dont une campagne publicitaire soigneusement orchestrée réussit à faire un succès. Le texte principal du livre, modestement intitulé *A New Kind of*

Science, ne mentionne pratiquement pas d'autres chercheurs que S. Wolfram, même quand il reprend leurs idées. Le livre se présente comme l'acte de naissance d'une nouvelle science dont le leitmotiv – répétitif donc ennuyeux – est : de l'application de règles de calcul simples et déterministes peuvent naître des phénomènes complexes et même aléatoires.

Ce dernier point est faux, puisqu'une suite calculée par algorithme ne peut pas être aléatoire au sens mathématique précis défini par le mathématicien Martin-Löf (qui utilise l'idée que l'aléatoire est incompressible). Mais surtout, le slogan que le simple peut engendrer le complexe, présenté par S. Wolfram comme sa découverte révolutionnaire, remonte en réalité au moins à Alan Turing qui, dès 1950, s'appuyant sur son expérience de programmeur d'un des premiers ordinateurs britanniques (qu'il avait contribué à mettre au point), écrivait : « J'ai conçu pour l'ordinateur de Manchester un petit programme de 1 000 unités de mémoires à peine qui, à chaque fois qu'on lui donne un nombre de 16 chiffres, en renvoie un autre [...]. Je défie quiconque, n'ayant connaissance que des réponses du programme à certaines valeurs, de deviner ce qu'il donnera pour une valeur qui n'a pas déjà été essayée. » Que le simple engendre le complexe est aussi bien connu des mathématiciens et pour ne citer qu'un exemple, n'est-il pas merveilleux que le nombre $\sqrt{2}$, défini avec quatre symboles $x^2 = 2$, possède une suite de décimales d'une complexité extrême que rien *au premier abord* ne distingue d'une suite de tirages au hasard ?

Sous la forme plus précise de la possibilité d'obtenir un comportement complexe avec un simple automate cellulaire, la « découverte géniale » de S. Wolfram doit être attribuée à John Conway. C'est lui, en effet, qui vers 1970 en étudiant le *Jeu de la vie* avec un groupe de passionnés mit en évidence à quel point des comportements imprévisibles résultent de petites configurations initiales de cet automate cellulaire d'une simplicité extrême.

Un réductionnisme trop radical

L'apport du livre de S. Wolfram sur ces questions, malgré ses 1 197 pages, est insignifiant : il présente une multitude d'exemples de combinatoires élémentaires produisant des configurations compliquées qui pour lui sont les briques de sa nouvelle science, alors qu'on ne voit pas très bien à quoi de telles énumérations peuvent servir, théoriquement ou pratiquement. Les volumineuses notes qui complètent le texte principal sont d'une utilité douteuse puisque la mégalomanie de l'auteur fait qu'il n'indique pas la moindre référence bibliographique !

Parmi les idées discutées par S. Wolfram, il y a celle (déjà énoncée par Zuse) qu'il existe peut-être un système de règles simples de nature finie et essentiellement locales (du type de celles utilisées pour les automates cellulaires, mais pas nécessairement en se limitant strictement à eux, car S. Wolfram semble admettre qu'on doit aller voir un peu au-delà) donnant, une fois pour toutes, les clefs du monde physique et à partir duquel tout se déduirait. S. Wolfram déclare sur ce sujet : « Tout ceci étaye ma conviction qu'il se confirmera que chaque détail de notre univers suit effectivement des règles représentables par un programme simple et que tout ce que nous voyons émergera en faisant tourner ce programme. »

Outre que ce réductionnisme extrême est jugé peu vraisemblable par nombre de scientifiques et d'épistémologues, il semble incompatible avec la physique actuelle en particulier à cause de la non-localité de la mécanique quantique. La question a été soigneusement (et âprement) discutée par Scott Aaronson, de l'Université de Waterloo

4. Des singes tapant sur un ordinateur quantique ?

Pour Seth Lloyd et de nombreux chercheurs s'occupant de complexité, notre univers n'est pas un chaos complet dont par hasard certaines parties sont organisées (celle où nous nous trouvons par exemple), mais le résultat d'une sorte de calcul multiple à partir de programmes qui eux seraient tirés au hasard. À l'image – proposée par Émile Borel en 1913 – d'un million de singes tapant au hasard sur des machines à écrire et produisant parfois des structures organisées, ils préfèrent celle d'un million de singes tapant au hasard des programmes lesquels, en fonctionnant, produisent alors des résultats imprimés dont la plupart sont structurés. L'image des singes programmeurs (fondée sur l'idée que le monde réalise un calcul, c'est-à-dire est une sorte

d'ordinateur) s'accorde mieux avec ce que nous observons autour de nous (qui est très loin d'être un chaos général) que l'image d'un monde engendré au hasard par des singes dactylographes.

Abandonnant l'idée d'un univers de type automate cellulaire techniquement insoutenable pour les raisons évoquées ici, Seth Lloyd préfère l'idée que l'univers pourrait n'être qu'un grand ordinateur quantique. Tout dans l'univers ne serait que le résultat d'un immense calcul quantique. Au slogan proposé en 1989 par Archibald Wheeler « It from bit » (L'être à partir du bit) pour mettre en avant la nature informationnelle de la physique, Lloyd répond par un nouveau slogan « It from qubit » (L'être à partir du bit quantique).



au Canada, qui conclut que les propositions de S. Wolfram pour résoudre cette difficulté – des graphes dynamiques – ne résistent pas à l'examen technique.

L'idée que l'univers pourrait n'être qu'un ordinateur de type réseau d'automates cellulaires semble gravement mise en doute par la mécanique quantique. Pourtant on peut imaginer de nouveaux types d'ordinateurs, exploitant la superposition des états quantiques et l'intrication des particules, qui autoriseraient une nouvelle conception d'un monde informatique: l'univers ne serait alors qu'un immense ordinateur quantique.

Telle est la thèse de S. Lloyd qui présente et explore l'affirmation que tout dans l'univers n'est que de l'information – donc se ramène à du discret et du fini –, mais de l'information quantique, donc en oubliant la localité et les automates cellulaires.

S. Lloyd, sans s'interdire le délicieux jeu des spéculations, étudie avec lucidité les capacités d'un tel ordinateur quantique total et la simulation (pour S. Lloyd, il n'y a pas de différence entre un système quantique et sa simulation): il envisage aussi les conséquences de l'hypothèse d'un univers-ordinateur-quantique sur ce que nous observons.

Singes programmeurs ?

S. Lloyd qui s'intéresse aux théories de la complexité – celles-ci entretiennent de nombreux liens avec les mathématiques du calcul, les technologies informatiques et la recherche sur les ordinateurs quantiques – insiste dans son livre sur une idée profonde: «les singes programmeurs». On attribue à Émile Borel l'image d'un million de singes placés devant des machines à écrire et qui, frappant les touches au hasard, finissent sur l'une des machines par écrire le texte d'une tragédie de Shakespeare. Cette idée que le désordre total produit tout, et donc, qu'avec de la patience, la pièce *Hamlet* finit par apparaître sur les feuillets dactylographiés d'une machine, n'est pas fausse, c'est même une

évidence de la théorie des probabilités. En revanche, l'idée que l'univers n'est qu'un chaos total, mais que, par chance, nous sommes dans une petite partie localement organisée, semble improbable. Une bien meilleure explication du désordre entraînant l'ordre est celle des singes programmeurs qui produisent notre univers en tapant au hasard des programmes dont les calculs fournissent des données constituant l'univers.

En plaçant un million de singes devant des claviers d'ordinateurs et en les persuadant d'écrire chacun un programme, les résultats des calculs faits avec ces programmes ressembleront plus à ce que nous observons. Certains programmes très simples, qui apparaîtront donc avec une forte probabilité sous les doigts des singes, feront apparaître une longue série de 0, ou une longue série périodique ABCABCABCA..., ou la suite des entiers 0, 1, 2... L'ensemble des résultats calculés et imprimés constituera non pas un ensemble de données aléatoires parsemé de rares petits morceaux structurés, mais un ensemble de textes, chacun organisé de manière plus ou moins complexe.

Un tel ensemble de résultats organisés est effectivement ce que nous observons quand nous examinons notre environnement. Nous ne voyons pas une masse d'objets aléatoires interrompue par quelques rares objets structurés, mais plutôt un monde organisé où le hasard est rarement dominant. En clair : le monde se présente à nous, bien plus comme le résultat d'un zoo de singes programmeurs que comme le résultat d'un zoo de singes dactylographes.

Cette idée, d'après S. Lloyd, nous conduit à croire que l'univers pourrait bien être une sorte de grand ordinateur nourri par des programmes plus ou moins tirés au hasard dont nous observons les productions. Nous expliquerions ainsi que le monde est compréhensible, car les programmes simples sont majoritaires. Quant à l'origine des choix aléatoires, S. Lloyd formule l'hypothèse que l'univers entreprend simultanément tous les calculs possibles avec le parallélisme quantique. Pour lui : « Les capacités fondamentales de calcul de l'univers au niveau le plus fondamental donnent naissance à toutes les formes possibles de traitement de l'information. Après le Big Bang, les différentes parties de l'univers tentent tous les calculs possibles. »

Peut-on éviter la mort thermique ?

Revenons maintenant à la dernière question (c'est-à-dire à celle posée à l'ordinateur dans la nouvelle d'Asimov). Peut-on inverser l'entropie ou plus exactement en éviter la conséquence ultime, la mort thermique et donc la fin de toute vie ?

La question appartient à ce qu'on nomme aujourd'hui l'eschatologie scientifique, domaine inauguré en 1979 par Freeman Dyson dans un article optimiste qui proposait des stratégies de refroidissement et d'interruption prolongée par hibernation permettant de tirer indéfiniment du travail d'un univers dont l'expansion irait diminuant. Malheureusement une série d'observations a montré depuis que l'expansion accélère. Les idées de Dyson doivent donc être réexaminées. Beaucoup pensent aujourd'hui que les données et théories dont nous disposons nous conduisent à croire que notre univers en expansion accélérée ne permet pas à une forme de vie de perdurer infiniment. D'une part, la matière devenant de plus en plus éparse, il devient impossible d'en accumuler une quantité suffisante pour alimenter la mémoire d'une vie qui se prolongerait indéfiniment ; or si cette mémoire accessible est bornée, la vie finit par tourner en rond, ce qui n'est pas vraiment conforme à l'idée d'une vie indéfiniment prolongée. D'autre part, il semble impossible

d'extraire une quantité infinie de travail d'un univers en expansion accélérée : la réponse de la cosmologie moderne au problème de l'entropie posé par Asimov est négative.

Sur ce dernier point, la thermodynamique de l'information développée autour des années 1980 par Rolf Landauer et Charles Bennett, et en particulier celle du calcul quantique, montre que tout calcul peut être mené de manière réversible et qu'en conséquence un calcul n'entraîne pas nécessairement un accroissement de l'entropie. À la condition donc que la vie ultime se déroule sous la forme d'un calcul réversible, elle pourrait être illimitée dans le temps. Pour cela une solution serait que cette vie migre à l'intérieur d'un ordinateur... ce qui nous ramène encore à la nouvelle d'Asimov et à son ordinateur *AC*.

Ce type d'idées qui fait d'Asimov un précurseur scientifique de nos actuels cosmologues prête à sourire. Pourtant un tel transfert est explicitement mentionné dans un article, paru en 2003, de Katherine Freese, de l'Université du Michigan, et de William Kinney, de l'Université Columbia. Leur travail envisage aussi d'autres pistes nous permettant d'échapper à la mort thermique dans le cas des univers en expansion accélérée. Il conclut donc d'une manière bien plus optimiste que L. Krauss et G. Starkman quelques années auparavant : il est, selon eux, possible d'imaginer divers scénarios pour notre futur compatibles avec nos connaissances actuelles et dans lesquels la vie perdure indéfiniment. Nous l'avons échappé belle...

Libre arbitre et mécanique quantique

John Conway et Simon Kochen démontrent un théorème qui signifie que si nous sommes libres, alors les particules élémentaires le sont aussi.

1. Le skieur quantique

La mécanique quantique indique que le trajet d'une particule n'est pas localisé. Lorsqu'une particule contourne un obstacle, une « partie » de la particule peut emprunter une trajectoire, l'autre « partie » en emprunter une autre. Après le passage de l'obstacle, la particule se recompose par interférence. Tant que l'on ne mesure pas la position de la particule, elle existe en différents endroits, comme les physiciens l'ont observé en la faisant interférer avec elle-même.

L'extension des propriétés quantiques à des objets macroscopiques, tel le skieur, surprend. La démarche de J. Conway et S. Kochen décrite dans ce chapitre procède dans le sens inverse : des propriétés macroscopiques, tel le libre arbitre d'un individu, ont des conséquences quantiques sur le comportement des particules.



Un des plus grands mathématiciens vivants s'est associé à un spécialiste respecté de mécanique quantique pour mettre en évidence l'étrangeté de notre monde ! Dans un article publié en 2006, puis épuré et perfectionné en 2009, John Conway, de l'Université de Princeton (inventeur du *Jeu de la vie*), associé dans l'aventure à Simon Kochen, aussi mathématicien à Princeton, présentent le théorème du libre arbitre (*The Free Will Theorem*). L'article est fondé sur trois axiomes en partie testables, liés à la mécanique quantique et à la relativité. Sur la base de ces axiomes, les auteurs démontrent que si un expérimentateur dispose du libre arbitre, alors les particules elles-mêmes disposent aussi de libre arbitre !

L'utilisation du concept de libre arbitre peut choquer, mais nous verrons qu'en prenant le terme *libre arbitre* dans le sens donné par J. Conway et S. Kochen, l'expression est bien choisie : elle force à repenser l'indéterminisme de la mécanique quantique sans l'associer à des probabilités, ce qui en éclaire le sens et la portée.

Indétermination logique

Selon J. Conway et S. Kochen, une entité dispose de libre arbitre à l'instant t si son état ne peut pas être décrit comme résultat de l'application d'une fonction, au sens mathématique, portant sur l'état de l'Univers avant l'instant t . Ce libre arbitre, qui n'a rien à voir avec les probabilités puisqu'il affirme juste la non-existence d'une certaine fonction, est un indéterminisme logique (ou si l'on veut préciser, fonctionnel).

Bien sûr, ce libre arbitre-là n'est pas exactement celui qu'on évoque en philosophie et en droit où, par exemple, il fonde la notion de responsabilité. Cependant, J. Conway considère qu'il n'est pas sans rapport et met en évidence un

2. La détermination impossible avant la mesure

Le théorème de Kochen-Specker est illustré par un polyèdre représenté sur la figure ci-dessous. En s'appuyant sur ce polyèdre, on définit 33 axes de l'espace. Le théorème énonce qu'il est impossible d'attribuer une valeur 0 ou 1 à chacun des 33 axes de façon que, pour tout triplet d'axes orthogonaux x, y, z , les valeurs attribuées soient 1-1-0, 1-0-1 ou 0-1-1.

Selon la mécanique quantique, quand on mesure selon trois axes orthogonaux le carré du spin d'une particule de spin unité, on trouve toujours 1-1-0, 1-0-1, ou 0-1-1.

Si le spin est fixé avant qu'on en mesure le carré, cela signifie que pour toute direction, il y a un résultat déterminé avant la mesure et que ce résultat est conforme à ce qu'indique la mécanique quantique (c'est-à-dire 1-1-0, 1-0-1, ou 0-1-1 pour trois axes orthogonaux).

L'existence du résultat avant qu'on en prenne connaissance par la mesure implique donc, en particulier (en prenant en

compte uniquement les 33 directions), qu'il est possible d'attribuer des 0 et des 1 aux 33 directions de façon que trois axes orthogonaux donnent toujours 1-1-0, 1-0-1, ou 0-1-1. (Si le spin est déterminé avant la mesure, la mécanique quantique nous dit plus, elle dit que cette histoire de 1-1-0, 0-1-1, 1-0-1 est vraie pour tout triplet orthogonal sans qu'il faille se limiter aux 33 axes.)

Il existerait donc une façon de mettre des 0 et des 1 aux 33 directions avec la propriété 1-1-0, 0-1-1, 1-0-1. Mais cela contredit le théorème de Kochen-Specker qui ne peut être faux (on l'a démontré). Ce qui est faux, c'est que nous avons supposé que le spin avait une valeur selon chaque axe et respectait la mécanique quantique.

Comme on a supposé que la mécanique quantique sur ce point était valide, c'est donc que le spin n'a pas de valeur déterminée avant qu'on le mesure : le spin se « décide » au moment de la mesure, pas avant.

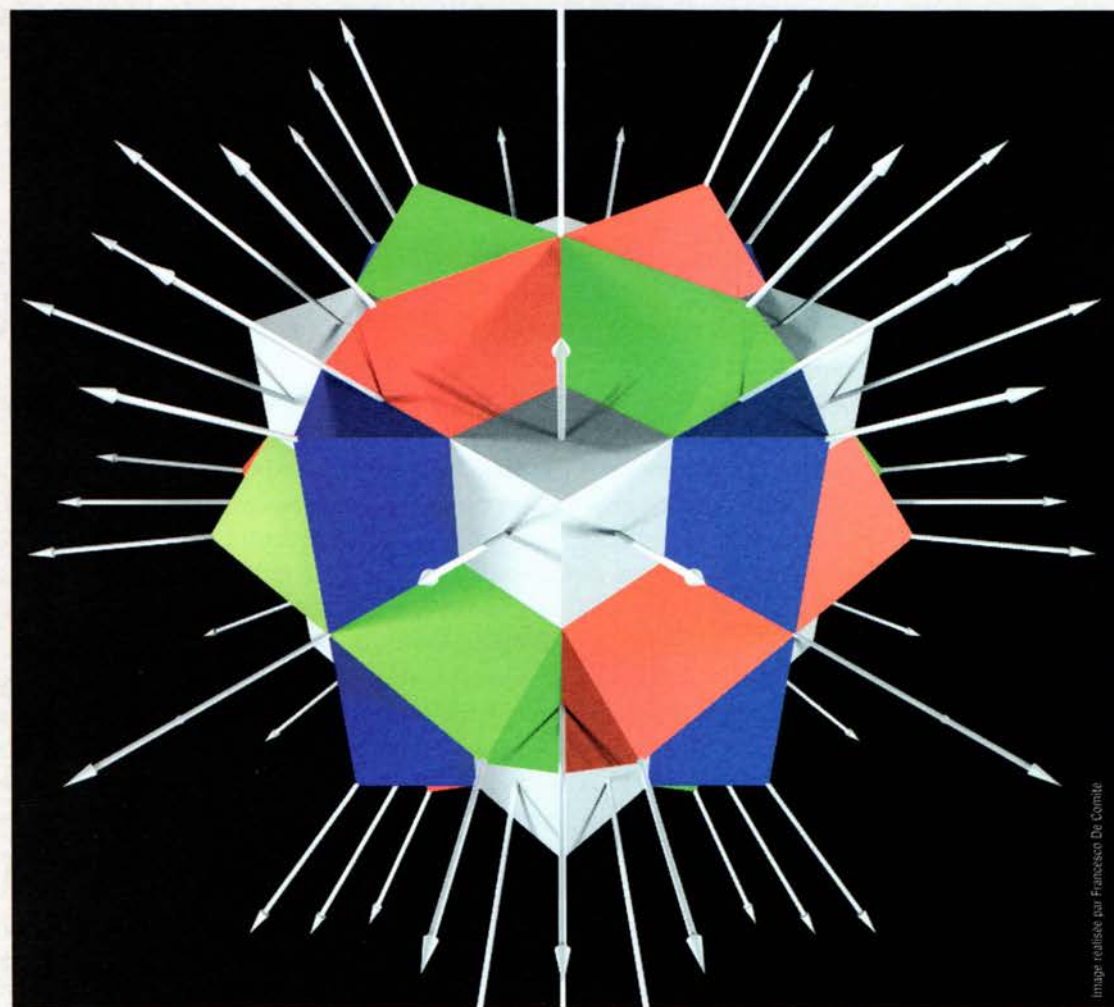


Image réalisée par Francesco De Comite

point qui n'était pas clair avant ces travaux : l'indéterminisme que la physique moderne semble obligée d'accepter est une notion fonctionnelle et logique. Cet indéterminisme est l'impossibilité logique qu'il existe certaines fonctions reliant les états de l'univers, impossibilité qui signifie que d'instant en instant l'Univers n'est pas contraint par son passé, mais libre de son évolution.

Pour J. Conway et S. Kochen, quiconque accepte leurs trois axiomes nommés SPIN, TWIN (tous deux liés à la mécanique quantique) et MIN (lié à la relativité et à l'idée qu'un expérimentateur est libre de ses choix), doit aussi admettre que l'état d'une particule à l'instant t n'est pas logiquement déterminé par l'état de l'Univers autour de la particule avant l'instant t . Dit simplement, s'il y a un peu de libre arbitre pour les gros systèmes physiques que nous sommes, alors l'univers est plein de libre arbitre et celui-ci est microscopique.

Tous les commentaires s'accordent sur l'importance de ce résultat qui complète d'autres contributions classiques comme le paradoxe EPR (présenté en 1935 par Albert Einstein, Boris Podolsky et Nathan Rosen), les inégalités de John Bell de 1964, et surtout le paradoxe de Kochen-Specker que le nouveau raisonnement utilise d'ailleurs comme élément central de la démonstration. Le théorème du libre arbitre, contribution majeure à la compréhension de la mécanique quantique, est un pas vers une situation où personne ne pourra plus dire, comme Richard Feynman : « Si quelqu'un vous affirme qu'il comprend la mécanique quantique, vous avez affaire à un menteur. »

L'axiome SPIN

Le premier axiome, SPIN, concerne le résultat de la mesure du spin d'une particule. Le spin est parfois assimilé à un moment cinétique, mais la seule chose qui compte pour nous est que, parmi les conséquences de la mécanique quantique, il y a l'énoncé SPIN, lequel stipule que :

Axiome SPIN. *La mesure du carré du spin d'une particule de spin unité, selon trois axes orthogonaux x , y et z donne toujours deux 1 et un 0, soit 1-0-1, 0-1-1, ou 1-1-0.*

Cette conséquence testable de la mécanique quantique, et admise comme axiome, est bien sûr moins forte que l'ensemble de la mécanique quantique : en bons mathématiciens, nos deux auteurs minimisent les hypothèses qu'ils utilisent. Pourtant, à elle seule, elle est déjà troublante, car nous allons voir qu'elle implique que le spin d'une particule de spin unité n'existe pas avant d'avoir été mesuré. En effet, le théorème de Kochen-Specker de 1967, simplifié par Asher Peres en 1991, stipule que :

Si on considère les 33 axes du schéma de la figure 2, il n'existe aucune façon de leur attribuer des valeurs 0 ou 1 qui soit telle que chaque triplet d'axes orthogonaux donne les valeurs 1-0-1 dans cet ordre ou un autre.

Démontrer le théorème de Kochen-Specker consiste simplement à traiter un puzzle géométrique et combinatoire. On essaie de placer des 1 et des 0 aux extrémités des 33 axes de la figure de Peres en respectant la règle des trois directions orthogonales, toujours 1-0-1 dans cet ordre ou un autre, et on s'aperçoit qu'on n'y arrive pas.

Il existe des démonstrations directes de ce théorème, mais vous pouvez écrire un programme qui essaie toutes les combinaisons possibles de 0 et de 1 pour les 33 axes de Peres (il y en a 2^{33}), et qui, pour chaque combinaison, teste la propriété des trois axes orthogonaux. Votre programme conclura que parmi les 2^{33} combinaisons, aucune n'est satisfaisante.

Ce théorème, associé à SPIN, montre que les objets de la mécanique quantique ont des comportements inattendus. On pourrait penser que, quel que soit l'axe choisi pour mener la mesure, le spin d'une particule de spin unité est fixé avant l'opération. L'idée est naturelle : avant la mesure et indépendamment de ce que prévoit l'expérimentateur, le résultat serait inscrit dans la particule et son environnement.

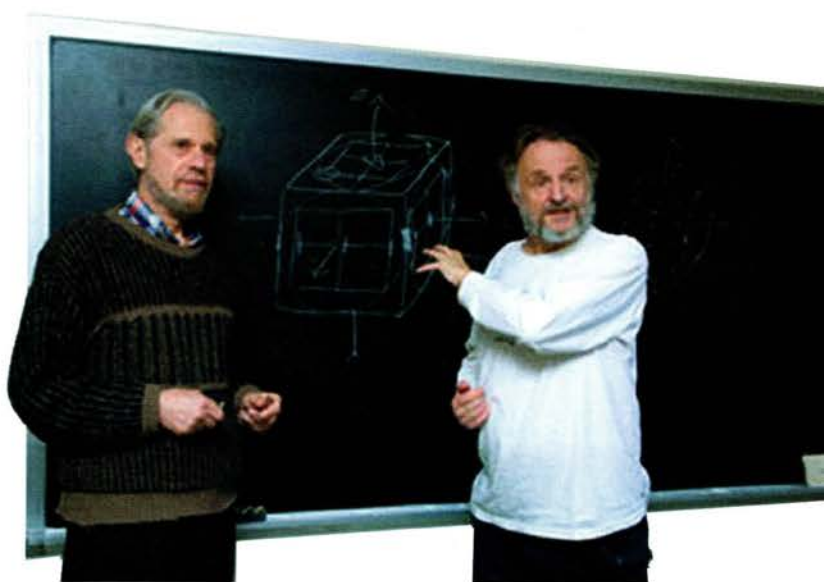
Pour connaître la réponse, il faudrait faire intervenir des variables dont nous n'avons pas connaissance et que l'on nomme *variables cachées*. La mécanique quantique ne dirait pas précisément ce qu'on va trouver, car elle ne serait, dans cette hypothèse, pas assez précise. Toutefois, en ajoutant d'autres variables, c'est-à-dire en complétant la mécanique quantique, on saurait proposer une théorie où ce que l'on observe est bien déterminé avant qu'on en fasse l'observation.

Le théorème de Kochen-Specker est fatal à une telle conception dite *réaliste*, car si une théorie à variables cachées (connue ou inconnue de nous) était vraie, alors l'ensemble des résultats des valeurs de spin déterminées par ces variables cachées quand on fait varier l'axe de mesure vérifierait la propriété 1-0-1 pour tout triplet d'axes orthogonaux. Or, en ne considérant que les 33 directions de Peres (et non pas l'infinité des directions possibles), c'est déjà mathématiquement impossible.

Le théorème de Kochen-Specker implique la fausseté de toutes les théories à variables cachées. Imaginer des variables non décrites par la mécanique quantique ne permettra jamais de proposer un complément à cette théorie (par ailleurs toujours vérifiée) qui soit compatible avec ce qu'on en sait déjà, et cela uniquement à cause de l'affirmation SPIN.

Pour être précis, il faut indiquer que nous avons uniquement envisagé des variables cachées *non contextuelles*, c'est-à-dire qui fixent les résultats de la mesure selon un axe x , sans prendre en compte que l'observateur est aussi en train de mener des mesures selon les axes y et z . Qu'il puisse y avoir des variables cachées contextuelles (dans ce cas, le résultat de la mesure selon x ne dépend pas seulement de l'environnement de la particule et de x , mais aussi du fait que vous tentez en même temps de mesurer selon d'autres axes y et z) ne semble pas sérieusement envisageable, et en tout cas n'est pas conforme à l'idée d'une réalité autonome que soutiennent les défenseurs des variables cachées.

Quand on mesure le poids et la couleur d'un objet, le résultat pour le poids est le même que lorsque l'on mesure le poids et la longueur ; envisager qu'il puisse en être autrement – c'est-à-dire envisager des variables contextuelles – apparaît absurde. C'est pourtant ce à quoi le théorème de Kochen-Specker accule ceux qui tentent à tout prix de concevoir des théories où les résultats d'une mesure sont fixés avant que la mesure soit



3 Simon Kochen (à gauche) et John Conway (à droite) exposant le théorème du libre arbitre.

menée. Ou bien il n'y a pas de variables cachées, ou bien elles sont contextuelles, mais le réaliste ne retombe jamais sur ses pieds, et le monde quantique n'aura donc jamais les bons comportements qu'il attend. Le plus simple est d'accepter que le résultat d'une mesure n'est pas déterminé avant la mesure.

Notons, avant de poursuivre, que le théorème du libre arbitre ne dépend pas de la position que l'on adopte à propos des variables cachées, contextuelles ou non. Il dépend uniquement de l'axiome SPIN testable expérimentalement, du théorème de Kochen-Specker, qui n'est pas une hypothèse, mais une affirmation élémentaire et démontrée de combinatoire géométrique, et des deux autres axiomes auxquels nous arrivons.

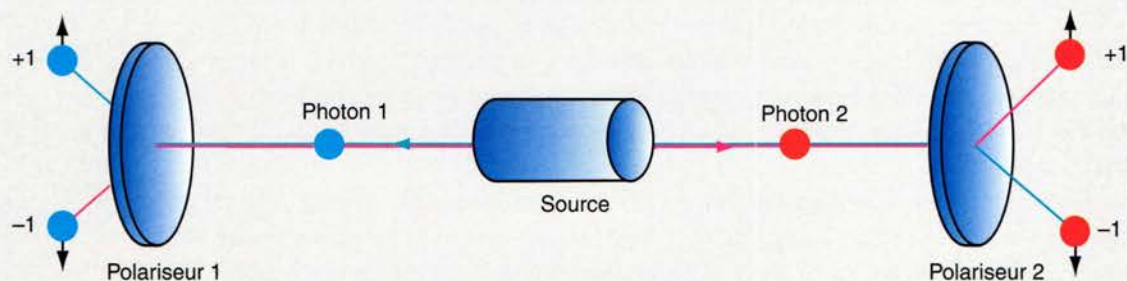
Particules jumelles

On sait produire des particules jumelles dont la théorie quantique indique que, même éloignées l'une de l'autre, elles fourniront des résultats identiques si on les soumet à des opérations de mesure identiques.

Si l'on accepte que les résultats d'une mesure ne sont pas fixés à l'avance, les deux particules d'une paire de particules jumelles «communiqueraient instantanément» pour s'entendre sur le résultat qu'elles doivent rendre! Sans approfondir ce que signifie dans un tel contexte «communiquer instantanément», l'axiome TWIN prend en compte un fait expérimental testable, dans le cadre d'une expérience de pensée, que nous nommerons A-B-a-b.

Axiome TWIN. *Considérons une paire de particules jumelles a et b de spin unité. Si l'expérimentateur A mesure le carré du spin de a selon trois axes orthogonaux x, y, z, pendant que l'expérimentateur B mesure le carré du spin de b selon l'axe w, alors, si w est l'un des trois axes*

4. Le paradoxe EPR (Einstein, Podolsky et Rosen)



La mécanique quantique indique comment fabriquer des paires de particules jumelles, qui sont par ailleurs utilisées pour la réalisation de certains protocoles de cryptographie quantique. L'expérience de pensée décrite ici est celle du paradoxe de Einstein, Podolsky et Rosen; elle a été réalisée par le physicien français Alain Aspect en 1982.

Une paire de particules jumelles est fabriquée, ici deux photons. Elles s'éloignent l'une de l'autre à la vitesse de la lumière si bien que toute communication est impossible entre elles. Même si celles-ci sont très éloignées l'une de

l'autre, toute mesure (ici une mesure de polarisation de valeur +1 ou -1) faite sur les deux particules donne des résultats identiques. Donc si l'on fait la mesure sur l'une, on sait le résultat qu'a donné la mesure sur l'autre. Le fait est troublant: l'interprétation classique de la mécanique quantique considère que l'état d'une particule n'est pas déterminé avant qu'on opère la mesure, cela contrairement aux théories à variables cachées qui soutiennent que le résultat est fixé (même si la mécanique quantique ne le donne pas du fait de son incomplétude).

x , y ou z , le résultat que découvrira B sera le même que celui que découvrira A pour l'axe correspondant.

L'existence et les propriétés de telles particules jumelles sont aujourd'hui une certitude. L'axiome TWIN doit donc être considéré non pas comme une propriété hypothétique et théorique, mais comme une propriété certaine de notre monde physique, indépendamment du reste de la mécanique quantique.

Le dernier axiome est le plus délicat, car il se réfère à la relativité et qu'il tente de rendre précise l'idée de localité, c'est-à-dire l'idée que ce qui se passe en un point de l'espace ne peut pas avoir d'influence causale sur ce qui se passe au même instant en un point éloigné.

Il est naturel d'admettre la forme élémentaire suivante du principe de causalité, car cela semble une question de bon sens : *il est impossible à un événement d'influer sur un événement passé.*

Grâce à cette évidence, on peut déduire une forme de localité. En effet, selon la théorie de la relativité, tous les repères inertiels (en mouvement uniforme l'un par rapport à l'autre) sont équivalents du point de vue des lois de la physique. De plus, si deux événements E_1 et E_2 se déroulent simultanément dans un certain repère inertiel, on peut trouver un autre repère inertiel dans lequel E_2 se déroule avant E_1 , et un autre encore dans lequel E_1 se déroule avant E_2 . Le principe de causalité (pas d'influence en arrière dans le temps) et le simple fait d'être éloigné dans l'espace entraînent donc, du fait des changements de repères possibles, l'impossibilité d'une influence de E_2 sur E_1 et réciproquement.

L'axiome relativiste

Une affirmation du type « E influence F » n'a un sens précis que dans un monde où tout n'est pas fixé à l'avance, car si tout est parfaitement déterminé, les notions d'indépendance et d'influence ne signifient rien. Du coup, pour formuler précisément l'idée de localité qui fait intervenir la notion d'influence, il faut admettre que l'expérimentateur fait des choix qui ne sont pas déterminés : il faut admettre qu'il dispose de libre arbitre dans le sens fonctionnel que J. Conway et S. Kochen donnent à ces mots. La formulation d'un axiome de localité, exprimant ce qui semble résulter de la théorie de la relativité, oblige à faire l'hypothèse du libre arbitre des expérimentateurs.

Pour J. Conway, la question n'est pas de savoir si le déterminisme est vrai ou faux. Pour lui, comme le solipsisme (l'affirmation que rien d'autre n'existe en dehors de moi), le déterminisme n'est pas réfutable. Si quelqu'un pense que ce qui se passe dans le monde est déjà fixé, rien ne pourra l'en dissuader. La mécanique quantique suggère que le déterminisme est faux (et c'est l'avis de J. Conway et S. Kochen), mais ne le prouve pas, car c'est impossible à prouver. J. Conway et S. Kochen s'intéressent à la relation entre le libre arbitre des expérimentateurs (s'ils en ont) et celui des particules.

Ces remarques expliquent la formulation du troisième axiome, qui affirme que dans l'expérience de pensée $A-B-a-b$ (déjà utilisée pour TWIN), ce que choisit A n'influe pas sur b et que ce que choisit B n'influe pas sur a .

Axiome MIN. *Supposons que les expériences menées par A et B soient spatialement séparées et simultanées dans un certain repère inertiel. Le choix par B de l'une des 33 directions de Peres, w , est libre, et le résultat de l'expérience pour a est indépendant de ce choix. De même, le choix par A d'un repère orthogonal x, y, z est libre et le résultat pour b est indépendant de ce choix.*

Enfin, le théorème !

Nous sommes maintenant prêts pour l'énoncé et la démonstration du théorème du libre arbitre.

Théorème du libre arbitre. *Les axiomes SPIN, TWIN et MIN impliquent que la réponse d'une particule de spin unité à une expérience de mesure du carré du spin selon trois axes orthogonaux est libre, c'est-à-dire n'est pas une fonction de l'état de l'univers avant l'instant de la réponse.*

La démonstration peut se formuler de manière plus ou moins technique en utilisant un appareillage de notations plus ou moins complexes. Nous en donnerons une version qui nous semble adaptée; ceux qui la trouveront trop vague pourront lire celle de J. Conway et S. Kochen en : <http://www.ams.org/notices/200902/rtx090200226p.pdf>.

L'idée est d'utiliser l'axiome MIN qui indique que les choix faits par A et par B sont libres et de supposer que ceux faits par les particules jumelles a et b ne le sont pas, puis d'aboutir à une contradiction par l'utilisation du théorème de Kochen-Specker.

Si le choix fait par la particule a n'est pas libre, cela signifie que ce choix est une fonction de l'état de l'univers avant la mesure faite par l'expérimentateur A , état qui bien sûr dépend en particulier du choix opéré par A des trois axes orthogonaux x , y et z , retenus librement par lui, mais, d'après l'axiome MIN, ne dépend pas de l'axe w choisi par B .

De même, la réponse donnée à la mesure opérée par B sur b selon l'axe w ne dépend que de l'état de la partie de l'univers autour de b avant la mesure, partie qui inclut l'information w , mais n'inclut pas les informations x , y et z d'après l'axiome MIN.

L'axiome TWIN indique, lui, que si w est parallèle à l'un des axes x , y ou z choisis par A , la mesure faite par B sur b donnera le même résultat que la mesure faite par A sur a pour l'axe correspondant. Cela signifie que si A change de triplet x , y , z , les valeurs trouvées par A pour un axe donné ne changeront pas.

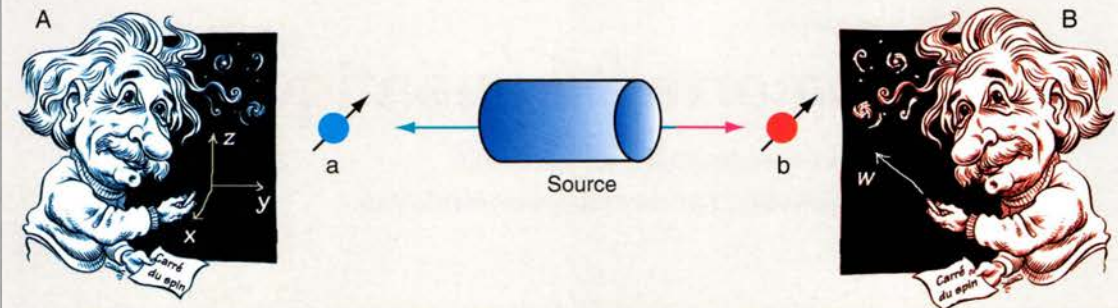
L'axiome SPIN indique alors qu'il existe une attribution des valeurs 0 et 1 aux 33 axes de Peres telle que chaque triplet d'axes orthogonaux reçoive les valeurs 1-0-1, 1-1-0 ou 0-1-1. L'existence d'une telle attribution contredit le théorème de Kochen-Specker. Nous sommes arrivés à une contradiction, qui signifie que l'hypothèse «les choix des particules a et b ne sont pas libres» est fausse.

Libre arbitre et hasard

Il ne fait pas de doute que l'effort nécessaire pour suivre l'argument de J. Conway et S. Kochen est assez important, c'est souvent le cas en mécanique quantique, mais si la chose avait été totalement évidente, on n'aurait pas attendu 2006 pour découvrir cette conséquence inattendue de deux des théories les mieux vérifiées de la physique. Comme le raisonnement isole parfaitement les points de ces théories nécessaires pour le mener et qu'il ne présuppose donc aucune des autres affirmations de ces théories, c'est l'intérêt de la mobilisation des esprits mathématiques, on découvre que les difficultés créées par les théories physiques modernes résultent d'un nombre très limité d'affirmations.

Parmi les trois axiomes, deux sont testables. Le troisième ne l'est pas, car la propriété de localité qu'il exprime est aussi impossible à prouver que la fausseté du solipsisme. Il est cependant en parfaite conformité avec toutes les expériences qu'on peut mener et qui

5. L'expérience de pensée de John Conway et Simon Kochen



Voici l'expérience de pensée $A-B-a-b$ qui, selon J. Conway et S. Kochen, prouve que si les expérimentateurs A et B disposent de libre arbitre pour mener leurs mesures, alors les deux particules jumelles en disposent aussi. Leur raisonnement montre que si A et B choisissent librement – sans que cela soit déterminé par l'état de l'univers avant l'instant de leur choix – les axes x , y et z (pour A) et l'axe w (pour B), alors il en va de même pour les particules a et b dont il est impossible que les réponses qu'elles donnent aux mesures soient entièrement déterminées par l'état de l'univers avant l'instant de la mesure.

n'ont jamais permis le transfert instantané d'informations d'un point de l'univers à un autre. Précisons que les expériences dites de téléportation quantique n'ont jamais pour conséquence le transfert instantané d'informations choisies ou la mise en évidence d'actions causales instantanées, mais qu'elles réalisent seulement, comme dans le cas des particules jumelles (qu'elles utilisent), la révélation d'informations partagées inconnues et sans doute indéterminées... ce qui est très différent.

L'utilisation du terme libre arbitre par les deux mathématiciens est une provocation délibérée dont le but est de faire comprendre que l'indéterminisme a été, à tort, lié aux probabilités, alors que sa véritable nature réside dans la définition fonctionnelle de la non-détermination d'un fait ou d'une information relativement à un contexte physique. Voici ce qu'en disent J. Conway et S. Kochen : « Certains pensent que la seule alternative au déterminisme est l'aléatoire de la théorie des probabilités et ajoutent pourtant qu'autoriser l'aléatoire dans le monde n'aide pas vraiment à comprendre le libre arbitre. Nous pensons que les processus probabilistes classiques comme le lancer d'une pièce parfaite n'aident pas à expliquer le libre arbitre, mais nous pensons qu'il se pourrait bien aussi qu'utiliser l'aléatoire de la théorie de probabilités n'aide pas plus à expliquer les effets quantiques que notre théorème met en avant.

Le type de liberté des particules jumelles, et plus généralement l'intrication quantique, montre que quelque chose de très différent de l'aléatoire classique des probabilités joue ici. [...] Dans l'état actuel des connaissances, il est certainement au-delà de nos capacités de compréhension d'établir un lien entre les décisions libres des particules et celles des humains, mais l'aléatoire de la théorie de probabilités ne rend compte ni du libre arbitre des humains ni de celui des particules. »

L'indéterminisme de la mécanique quantique est bien plus subtil et profond que celui décrit par les probabilités et c'est ce que le théorème du libre arbitre montre de manière flagrante, changeant sans doute profondément les analyses qu'on fera à partir de maintenant de la mécanique quantique.

Suicide et immortalité quantiques

La logique des univers multiples de Hugh Everett
introduit des possibilités d'action totalement inattendues.

Lorsqu'il touche des sujets trop graves, le raisonnement semble outrepasser ses droits et apparaît intolérable. Aux yeux de certains, on n'est pas autorisé à jouer avec toutes les idées. Précisons que nous allons traiter, en logicien froid et décharné, des thèmes qui peuvent choquer, comme celui du suicide collectif ou de l'immortalité, et que nous ne nous interdirons aucune considération, même la plus démente. Nous examinerons ici les conséquences d'une idée de science-fiction introduite en physique par Hugh Everett, et nous ferons cela comme nous le ferions pour un jeu abstrait, même si le détachement sera parfois difficile.

Simplification

Au fil des années, l'interprétation des mondes multiples de la mécanique quantique gagne des partisans. Plusieurs enquêtes parmi les physiciens ont montré qu'elle arrivait en seconde position derrière l'interprétation classique dite de Copenhague. Selon cette interprétation de Copenhague, élaborée en 1927 par Niels Bohr et Werner Heisenberg, au moment où l'observateur effectue une mesure, les diverses possibilités décrites par la fonction d'onde se « réduisent » à une seule. Cette réduction explique que, contrairement au monde quantique qui accepte l'existence d'états « superposés », le monde de notre expérience quotidienne n'en exhibe jamais de trace. Le célèbre chat de Schrödinger dans sa boîte (*voir la figure 1*) avant l'observation est à la fois mort et vivant du point de vue de la mécanique quantique, mais une fois la boîte ouverte, nous le trouvons mort ou nous le trouvons vivant.

Cette réduction de la fonction d'onde est parfois jugée insatisfaisante, car elle introduit une complication *ad hoc*, une discontinuité et du non-déterminisme. De plus, elle oblige à faire intervenir de manière essentielle l'observateur dans la description de l'évolution d'un système physique. Cela conduit à des considérations subjectivistes (ou pire...), ce qui réjouit quelques philosophes, mais s'oppose aux points de vue réalistes, selon lesquels le monde physique existe indépendamment de l'observateur, points de vue que l'on a toujours préférés en science.

Le 23 avril 1957, Hugh Everett soutenait à l'Université de Princeton sa thèse *Sur les fondements de la mécanique quantique* (*On the Foundations of Quantum Mechanics*). Il y décrivait une façon d'éviter la réduction de la fonction d'onde. Dans son manuscrit et

1. La roulette russe quantique

Dans l'expérience de pensée du chat de Schrödinger, un mécanisme quantique aléatoire – une désintégration radioactive – a une probabilité $1/2$ de se produire en une heure. La particule émise par cette désintégration ouvre une fiole de poison qui tue le chat. Le chat est dans la boîte pendant une heure et, avant l'ouverture de la cage, l'état chat mort et chat vivant sont «superposés». Une heure après, l'observateur ouvre la trappe de la boîte où réside le chat et examine s'il est mort ou non : dans l'interprétation de Copenhague, les deux possibilités décrites par la fonction d'onde du chat se rédui-

sent à une seule à l'instant où l'observateur ouvre la boîte. Dans l'univers des «mondes multiples», l'univers se dédouble à l'ouverture de la boîte, créant un univers où le chat est vivant et un autre où le chat est mort.

Pour prouver la justesse de l'interprétation des mondes multiples, un expérimentateur prend la place du chat et fait fonctionner plusieurs fois le mécanisme quantique qui le tue avec une probabilité $1/2$ à chaque expérience. Si l'interprétation usuelle de Copenhague de la mécanique quantique est la bonne, sa probabilité de survie est $1/2^n$, où n est le nombre de fois qu'il fait fonctionner le dispositif. En revanche, si l'hypothèse des mondes multiples proposée par Hugh Everett est correcte, à chaque tirage, l'univers avec l'observateur donne deux univers différents, l'un où le premier des résultats possibles est la survie, l'autre où la mort est survenue ; l'expérimentateur survit de manière certaine dans une branche de l'univers et ne se préoccupe pas des autres où il a été annihilé. Le fait pour l'observateur de se retrouver vivant après l'expérience lui prouverait la justesse de l'idée d'Everett. L'hypothèse des mondes multiples est donc bien testable. Ce procédé inhabituel (et dangereux !) permettant de prouver une théorie physique était sans doute connu par Everett quand il présenta sa thèse en 1957, mais c'est en 1985 seulement qu'apparaît la première mention de la roulette russe quantique, dans une nouvelle de science-fiction de John Gribbin. Depuis, cette idée a été redécouverte un grand nombre de fois.

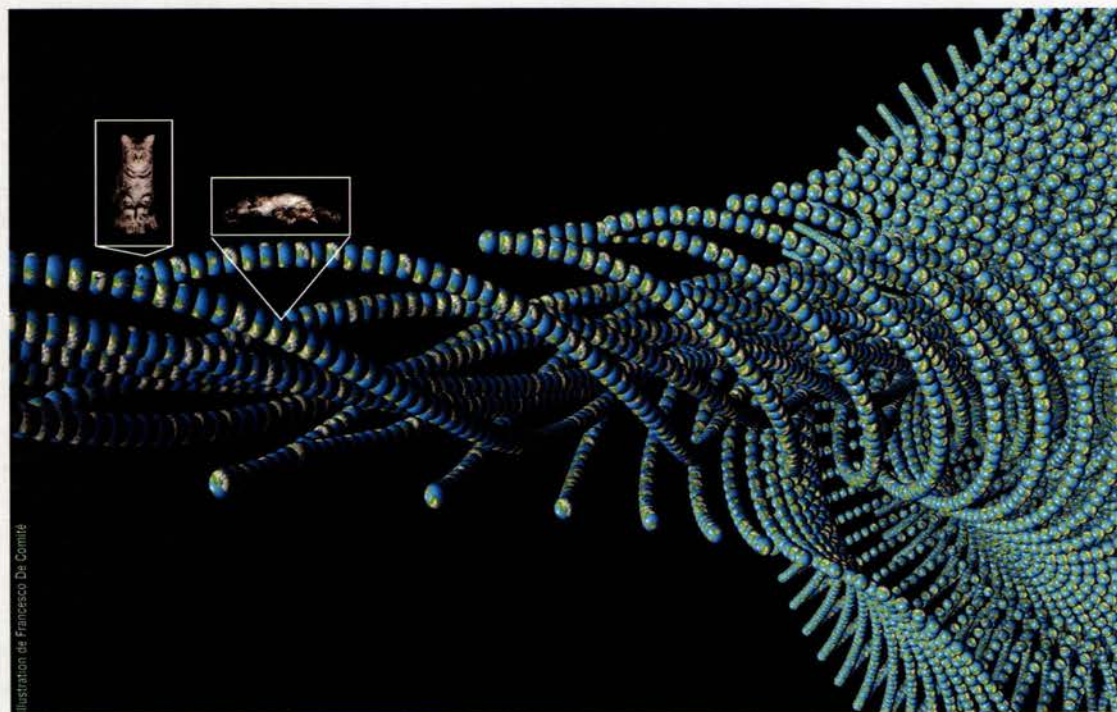
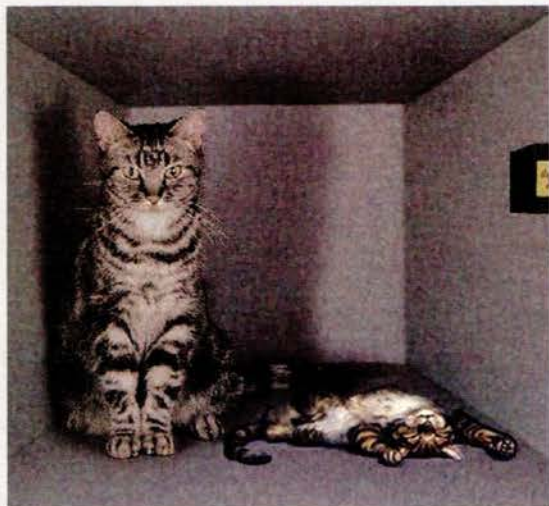


Illustration de Francesco De Gennaro

l'article qu'il en a tiré, sa théorie de ce que l'on dénomme aujourd'hui les « mondes multiples » y est exprimée avec prudence et en termes aussi techniques que possibles, sans doute pour ne pas choquer. L'idée, aussi simple que téméraire, a été reprise avec moins de détours par Bryce DeWitt. Pour Everett, DeWitt et leurs partisans, lors d'une mesure de la nature du chat par exemple, il n'y a pas réduction du paquet d'ondes, mais un dédoublement de l'univers. Dans l'une des branches de l'univers, l'observateur voit le résultat *A* (le chat mort), dans l'autre il voit *B* (le chat vivant). Chaque branche déroule sa propre histoire, indépendante de l'autre, en produisant alors d'autres bifurcations. L'évolution du monde physique est une explosion ininterrompue, engendrant par duplication répétée des milliards de milliards de copies nouvelles de l'univers tel que nous le concevons et dont nous ne voyons qu'une infime partie.

Des tests possibles

Depuis quelques années, une série de publications soutient que toutes les interprétations de la mécanique quantique ne sont pas équivalentes et qu'il se pourrait qu'on réussisse à mener des expériences décisives conduisant à déterminer quelle est la bonne; dans ce cas, il ne faudrait plus parler d'interprétations différentes de la mécanique quantique, mais de théories quantiques différentes.

David Deutsch, Don Page, Frank Tipler, Rainer Plaga et quelques autres proposent des méthodes pour départager les « interprétations ». Rien n'est tranché aujourd'hui et nous n'allons nous intéresser qu'à l'un des tests envisagés : le plus fou, dénommé la *roulette russe quantique*.

Eugene Shikhovtsev, le biographe d'Everett, soutient qu'Everett en aurait eu l'idée. La première mention imprimée de la roulette quantique est due à John Gribbin dans sa nouvelle de science-fiction intitulée *The Doomsday Device* publiée dans la revue *Analog* du 22 janvier 1985. L'idée est d'entrer dans la boîte du chat de Schrödinger, de prendre sa place et de faire fonctionner le mécanisme non pas une fois, mais plusieurs fois.

La boîte contient un dispositif quantique qui peut donner deux résultats équiprobables *A* et *B*. Si *A* se produit, le dispositif vous tue. Si le résultat est *B*, rien ne se passe et vous survivez dans votre univers. Vous recommencez dix fois de suite l'expérience de la roulette russe quantique; dans l'interprétation de Copenhague, votre probabilité de survie est égale à $(1/2)^{10}$, soit une chance sur 1 000 environ ($2^{10} = 1 024$). En revanche, si l'interprétation des mondes multiples est correcte, vous continuez de vivre dans votre univers et vous ne souffrez pas de ce qui se passe dans les autres.

Le fait que vous ayez survécu à dix expériences vous montre que l'interprétation des mondes multiples est très probablement correcte. Pour que l'interprétation de Copenhague soit juste, il faudrait que vous ayez eu beaucoup de chance et que, dix fois de suite, la réduction du paquet d'ondes ait donné *B*. Si l'expérience réussit, le risque que l'interprétation des mondes multiples soit fausse est donc de $1/1 024$.

Si ce risque d'erreur vous semble trop élevé et que vous désirez une confirmation plus fine de la théorie des mondes multiples, faites l'expérience 20 ou 30 fois : le risque d'erreur deviendra un millionième ou un milliardième. Au bout du compte, vous sortirez donc de la boîte persuadé de la justesse de l'interprétation d'Everett, qui sera donc pour vous quasi certaine.

Communicable ou pas ?

Cette certitude que vous avez acquise de la justesse de l'existence des mondes multiples d'Everett possède un défaut : elle vous est propre et vous ne pouvez pas la communiquer, car nul n'est obligé de vous croire. Ceux qui veulent savoir ce qu'il en est de l'interprétation d'Everett doivent personnellement affronter la roulette russe quantique dix fois de suite ou plus.

En réalité, cette incommunicabilité n'est pas absolue... pourvu qu'on y pense à l'avance. En effet, si vous avez prévu votre coup, vous avez pu installer une caméra infalsifiable (par exemple enfermée dans une boîte blindée avec une clef que vous avez confiée à un huissier). Elle a pu filmer à travers un hublot la séance des dix tirages de roulette russe quantique que vous avez courageusement enclenchée. Ces données soigneusement enregistrées et dont l'exactitude est certifiée par le protocole rigoureux constituent une preuve que l'expérience a bien été menée et qu'elle a donné un résultat favorable. Après l'expérience, dans la branche d'univers où vous survivez (la seule qui compte pour vous), vous disposerez donc d'une preuve matérielle de la justesse de la théorie d'Everett que vous pouvez transmettre à tous les autres physiciens de votre univers, ce qui les persuadera que l'hypothèse des mondes multiples est juste.

Vous avez pris un risque, celui qu'il n'y ait pas de mondes multiples, mais un succès bénéficie à tout le monde autour de vous. Qui veut être un héros de la science ?

Imaginons maintenant que, par d'autres moyens, on arrive à la certitude que la théorie des mondes multiples d'Everett est juste, ne pourra-t-on pas alors utiliser la roulette russe quantique de manière utile ?

Devenir riche

La réponse est oui. Nous verrons comment devenir riche grâce à elle et comment traiter tous les problèmes NP en temps raisonnable, ce qui sera une forme concrète de résolution de la fameuse énigme fondamentale de l'informatique théorique « $P = NP$? ».

Si vous êtes certain que l'interprétation des mondes multiples est juste, voici comment devenir riche. Réunissez 19 amis ayant la même conviction, déposez chacun 10 000 euros dans un coffre à combinaison, dont chacun de vous connaîtra le code, puis opérez la variante suivante de la roulette quantique. Après vous être attribué un numéro de 1 à 20 pour chacun, sans répétition, vous entrez tous dans un dispositif qui, par un procédé quantique semblable à celui du chat de Schrödinger, tire un nombre entre 1 et 20 de manière équiprobable et tue les 19 personnes dont le numéro n'est pas celui tiré. Les participants sont dans un état quantique de superposition de 20 états et, dans chacun, un participant a gagné. Le survivant dans son univers va alors retirer l'argent du coffre qui lui est acquis. Si vous pensez que 10 000 euros ne sont pas assez, proposez 100 000 ou 1 000 000 euros à vos amis. Tout le monde est gagnant, car chacun des 20 participants survit dans la branche où il gagne. N'est-ce pas formidable ? Dans les univers multiples, tout le monde devient riche.

Une autre méthode consiste à jouer une grille de loto (voir l'encadré 2).

Posez-vous maintenant la question : quelqu'un, certain de la validité de l'interprétation des mondes multiples, peut-il avoir des raisons sérieuses de refuser de jouer au jeu de la roulette quantique des 20 amis, ou à la variante loto de la roulette quantique ?

2. Pour devenir riche...

Si quelqu'un avait une confiance totale en la justesse de l'hypothèse des mondes multiples, il gagnerait au loto en ne jouant qu'une seule fois. Voyons le mode opératoire.

– L'expérimentateur, comme le chat, entre dans la boîte.



– Il utilise un dispositif quantique pour choisir une grille de loto. Le dispositif est conçu de façon à ce que chaque grille possible soit tirée avec la même probabilité.

– Le dispositif joue alors par Internet la grille choisie par le dispositif quantique (c'est possible aujourd'hui).

– Dès que le tirage est effectué, le dispositif consulte les résultats et ne laisse en vie l'expérimentateur que s'il a gagné un million d'euros ou plus.

Toujours sous réserve de la justesse de l'interprétation des mondes multiples, en entrant dans la variante loto de la roulette quantique, tout expérimentateur est certain d'en ressortir gagnant.

D'autres méthodes du même type font gagner aux courses ou à la Bourse.

Chacun est tenté de répondre «non». Pourtant, la question a été débattue par plusieurs philosophes, dont Peter Lewis, de l'Université de Hong Kong, et Davis Papi-neau, du *King College* de Londres, qui ne sont pas d'accord.

Tout d'abord, le moindre doute qui pourrait persister sur la validité de l'interprétation des mondes multiples est évidemment suffisant pour justifier un refus. Supposons que vous soyez absolument certain de la justesse de la théorie d'Everett; vous pourriez néanmoins refuser de jouer pour une raison éthique. Vous ne connaîtrez que les mondes où vous gagnez, mais puisque les autres mondes existent, vous créerez des situations où vos proches découvriront que vous les avez quittés sans vous préoccuper d'eux. Jouer au loto quantique est donc profondément égoïste, même si vous ne voyez jamais le mal qui résulte de votre choix!

Devenir riche n'est pas le seul but possible de la vie: résoudre des problèmes difficiles est un autre objectif que les chercheurs considèrent plus important. Une variante de la roulette quantique les aidera.

Imaginons d'abord le cas simple d'un chercheur qui se pose une question *Q* dont il peut avoir la réponse, *oui* ou *non*, à la condition de mener une expérience avec un réactif chimique extrêmement coûteux. Si la réponse est positive, cela aura été intéressant de faire l'expérience et en plus on pourra récupérer le réactif, mais si l'expérience échoue ce sera très ennuyeux, car le réactif chimique aura été utilisé pour rien et sera devenu irrécupérable. L'expérience donne son résultat instantanément et, *a priori*, elle a une chance de réussir non négligeable, disons 1/2. Voici ce que doit faire le chercheur qui croit aux mondes multiples d'Everett.

– Il lance un tirage au sort quantique entre deux options A et B, mais avec des probabilités très inégales: A sera obtenu dans 999 999 cas sur un million et B dans 1 cas sur un million. Autrement dit, la roulette provoque la création d'un million de branches parallèles: 999 999 avec A, et 1 avec B. Ensuite:

– Si A sort, il mène l'expérience qui lui permet de répondre à *Q*: il fait fonctionner la roulette russe qui le tue si l'expérience échoue et le laisse indemne si elle réussit.

– Si B sort, il ne mène pas l'expérience pour répondre à la question *Q*.

Quelle est la situation pour un expérimentateur qui a survécu ?

Si c'est A, comme il est en vie, cela signifie que l'expérience a réussi, il peut alors récupérer le réactif chimique et sait que la réponse à sa question Q est positive.

Si c'est B, cela signifie que très probablement la réponse à la question Q est négative. En effet, quand la réponse à Q est positive, il n'y a qu'une chance sur un million d'obtenir B et quand la réponse à Q est négative, il y a 100 pour cent de chance d'obtenir B.

La méthode comporte un petit risque d'erreur, car lorsque la réponse à Q est positive, on peut croire faussement qu'elle est négative, car on serait dans le cas B. La probabilité d'erreur est $1/1\,000\,000$. Comme précédemment, si ce risque vous semble trop grand, choisissez un risque plus faible. Il s'agit là, comme à la page 97, d'une application de la formule de Bayes.

Résoudre tous les problèmes NP

La méthode s'adapte à chaque fois que vous vous interrogez sur une question Q qui, si elle possède une réponse négative, entraîne un coût que vous voulez éviter. On peut donc l'utiliser pour jouer en Bourse (vous faites l'hypothèse que telle action va monter, et vous ne perdez rien si elle baisse), et faire des paris de toute nature. Dans le domaine scientifique et technique, elle permet de tester sans coût la solidité des ponts, et toutes sortes d'hypothèses en se dispensant de payer les conséquences des cas où l'hypothèse est fausse. Le suicide quantique n'est-il pas merveilleux ?

Un problème NP est un problème que quelqu'un ayant une chance parfaite et absolue résout rapidement (c'est-à-dire en temps polynomial en fonction de la taille des données). L'idée précédente se généralise et rend possible le traitement rapide (c'est-à-dire en temps polynomial) de tout problème NP, ce qui constitue une résolution pratique de la fameuse énigme « $P = NP$? » (les problèmes P se

3. L'éthique du suicide quantique



La roulette quantique (pour prouver l'hypothèse des mondes multiples, pour gagner au loto, etc.) présente l'inconvénient de laisser l'expérimentateur mort dans un grand nombre de branches de l'univers. Il peut décider de s'en moquer, car les branches où il survit sont les seules qu'il connaîtra. Est-ce pour autant moralement acceptable ? La question semble devoir être posée puisque ses proches le trouveront mort dans un grand nombre d'univers parallèles, et donc son suicide quantique engendre une grande quantité de mondes où il les fait souffrir.

Peut-on être indifférent à ces univers qu'on sait réels ? Cette question d'éthique, ainsi que le problème général de la rationalité (pour un égoïste certain de la vérité des mondes multiples) du choix de jouer, est l'objet de débats entre philosophes. Pour l'instant, ils n'ont pas réussi à se mettre d'accord. Jacques Mallah, effrayé de ce que le suicide quantique pourrait attirer quelques esprits fragiles, tente par toutes sortes d'arguments plus ou moins subtils de démontrer qu'il ne faut surtout pas essayer.

4. Hugh Everett



Hugh Everett est né le 11 novembre 1930 à Washington. Après avoir passé sa thèse de physique à Princeton sous la direction de John Wheeler et publié un article sur son interprétation des mondes multiples, il

ne réussit pas à obtenir le poste universitaire qui lui aurait permis de poursuivre ses travaux sur les fondements de la mécanique quantique. Il travaille alors pour la Défense américaine et contribue en particulier au projet des missiles nucléaires *Minuteman*. Après une période d'oubli, ses travaux sur les mondes multiples sont reconnus et plusieurs physiciens de premier plan, dont David Deutsch, en défendent les conclusions : ils émettent l'idée que sa conception doit être considérée comme une théorie ayant des conséquences observables et qu'on pourra soumettre un jour à des tests. Everett disparaît dans la nuit du 18 au 19 juillet 1982.

Quinze ans avant la thèse de Hugh Everett, l'écrivain argentin Jorge Luis Borges a décrit une des conceptions possibles de l'univers pour les physiciens quantiques et qu'il attribue à un imaginaire Ts'ui Pên :

« Le jardin aux sentiers qui bifurquent est une image incomplète, mais assez exacte de l'univers tel que le concevait Ts'ui Pên. À la différence de Newton et de Schopenhauer, votre ancêtre ne croyait pas à un temps uniforme et absolu. Il croyait à des séries infinies de temps, à un réseau croissant et vertigineux de temps divergents, convergents et parallèles. Cette trame de temps qui s'approchent, bifurquent, se coupent ou s'ignorent pendant des siècles, embrasse toutes les possibilités. Nous n'existons pas dans la majorité de ces temps ; dans quelques-uns vous existez et moi pas ; dans d'autres, moi, et pas vous ; dans d'autres, tous les deux. Dans celui-ci, que m'accorde un hasard favorable, vous êtes arrivé chez moi ; dans un autre, en traversant le jardin, vous m'avez trouvé mort ; dans un autre, je dis ces mêmes paroles, mais je suis une erreur, un fantôme. »

Le jardin aux sentiers qui bifurquent, 1941

résolvent en temps de calcul polynomial, donc pas trop difficilement). Voici, en même temps que nous précisons sur le sens des termes utilisés, comment procéder.

Le problème du chemin hamiltonien, où il faut passer par chaque nœud d'un graphe en suivant les arêtes du graphe et sans passer deux fois par le même nœud, est un problème NP (NP provient des initiales de *Non determinist Polynomial*). Celui qui a une chance parfaite le résout en procédant comme suit : il se place sur un nœud du graphe tiré au hasard, puis il tire au hasard un nœud relié à son nœud de départ et il y va ; il poursuit ainsi sans jamais accepter de passer par un nœud déjà visité. S'il existe un chemin hamiltonien, puisqu'il a une chance parfaite, il le trouve dès le premier essai et donc rapidement (en N étapes de calcul, N étant le nombre de nœuds du graphe).

Le problème de savoir si un graphe possède un chemin hamiltonien est donc un problème NP, et même un problème NP-complet. Les problèmes NP-complets sont les plus difficiles des problèmes NP : en résoudre un seul efficacement (en temps polynomial) permettrait de résoudre tous les problèmes NP efficacement. Comme on juge cela peu vraisemblable, on les considère comme intrinsèquement difficiles, ce qui veut dire qu'on pense qu'aucune méthode ne pourra jamais résoudre rapidement les problèmes NP-complets.

Avec la roulette quantique, on fait comme pour l'expérience chimique, sauf qu'on prend comme probabilité pour l'option B une probabilité très sensiblement inférieure à la probabilité d'échec *a priori* du problème NP auquel on s'intéresse. Si la probabilité qu'il n'existe pas de chemin hamiltonien pour le graphe qui vous intéresse est évaluée à $1/1000$, on prendra par exemple pour l'option B une probabilité $1/1\,000\,000$. Si p est la probabilité que se produise B, la probabilité de A sera bien sûr $1 - p$.

– Si c'est A qui est choisi par la roulette quantique, on cherche à résoudre le problème en procédant à une série de tirages aléatoires quantiques qui, soit (a) conduisent à un échec, auquel cas on est tué par la machine ; soit (b) conduisent à un succès.

– Comme précédemment, si B est choisi, aucun calcul n'est opéré.

Les choix conduisant à un succès permettent la survie, ainsi que le choix B qui marque que la réponse est négative. Le survivant sait donc s'il existe un chemin hamiltonien pour le graphe dont il s'occupe et quand tel est le cas, il le connaît.

Grâce au suicide quantique, tout problème NP est donc rapidement résolu avec un risque d'erreur aussi petit qu'on le veut.

5. L'immortalité...

La plus étonnante et démente des idées tirées des sélections quantiques nous fait croire à notre immortalité.

Bien que nous voyions mourir des gens autour de nous, à titre personnel les branchements créés par la mécanique quantique qui sont extrêmement nombreux impliquent qu'aussi proche que nous soyons de la mort, il y a toujours une éventualité qui nous fait y échapper. Même si l'événement quantique qui nous évite tel accident a une probabilité $1/10^{10\,000\,000}$ de se produire (par exemple parce qu'il s'agit d'un cas massif d'effet tunnel), c'est lui seul qui nous importe. Quelles que soient les situations de mort imminente que nous rencontrerons, il y aura toujours une solution quantique qui permettra la survie (dans une branche de l'univers au moins). D'instant en instant, cela nous assure l'immortalité.

Malheureusement, comme dans de nombreuses branches où je survis, cela résulte d'événements aléatoires quantiques favorables m'ayant sauvé la vie d'extrême justesse, je me retrouve vivant... mais mal en point, voire agonisant. Certes, à chaque fois que je manque de perdre la vie, cela ne se produit pas (dans les branches d'univers où je continue à percevoir le monde), mais je suis de plus en plus fragile et souffrant.

Ce type de raisonnements et de conclusions est controversé et ne fait pas partie de la théorie d'Everett. Rares sont les partisans des univers multiples qui donnent leur opinion ou expliquent pourquoi il ne faut pas croire à cette immortalité quantique de science-fiction.



Immortalité de Fantin-Latour
[1836-1904].

Sur un plan mathématique, on n'aura pas vraiment traité le problème central de l'informatique théorique « $P = NP?$ » (est-ce que tout problème NP peut être résolu en temps polynomial par un algorithme déterministe?), mais, sur un plan pratique, cela n'aura pas d'importance puisqu'à chaque fois qu'on aura à résoudre un problème NP, on pourra lancer la roulette quantique qui donnera rapidement la solution.

Ne pas entrer seul dans la machine

Reste la grave question morale que nous avons évoquée.

Pour ne pas risquer de laisser votre cadavre traîner dans une multitude d'univers où vos proches vous maudiront de les avoir abandonnés, il faut leur demander de monter dans la machine avec vous. Et pour éviter de créer des remous sociaux qui pourraient devenir graves, il faut que toute l'humanité participe au protocole de suicide quantique à chaque fois qu'on trouve intéressant de l'employer.

Il n'est sans doute pas très facile de réaliser cela en pratique, mais il n'y a pas d'impossibilité de principe à ce que chaque être humain soit impliqué dans le fonctionnement de ces roulettes générales, qui dans les cas d'échecs tueront tout le monde instantanément, ce qui évitera la douleur des survivants, et réconciliera donc le suicide quantique avec l'éthique.

L'idée de ce suicide quantique par civilisation entière a été étudiée par Paul Almond : « Une civilisation avancée pourrait utiliser le suicide quantique au niveau de la civilisation comme méthode d'action sur la réalité et pour disposer d'un pouvoir de calcul accru, ce qui pourrait aussi faciliter ses propres processus de pensée. »

L'immortalité en plus

Tout ce que nous venons de dire vous semble dément et peut-être n'en pouvez-vous plus de ce délire spéculatif. Pourtant, je commettrais un grave oubli si j'omettais de mentionner l'immortalité quantique qui procède du même type de logique.

À chaque instant, et en particulier lorsque vous êtes mourant, toutes sortes d'événements quantiques imperceptibles se produisent, créant des milliards de bifurcations. Certains sont sans doute bénéfiques et par exemple, un effet quantique d'une probabilité extrêmement faible pourrait détruire le caillot sanguin qui allait faire cesser de battre votre cœur. En acceptant de considérer des événements d'une probabilité extrêmement faible, il y a toujours une possibilité quantique qui vous fait survivre. Dans une des branches de l'univers d'Everett, vous ne mourrez pas. Dit autrement, l'hypothèse des mondes multiples entraîne que je ne meurs jamais : nous sommes tous immortels. Cela ne veut pas dire que nous ne voyons pas des gens mourir, mais que chaque seconde de vie que nous ressentons à titre individuel est suivie d'une autre. Aussi fou que cela paraisse, Everett lui-même semble avoir pensé à cela et il n'est pas impossible qu'il y ait cru.

En général, les physiciens partisans des mondes multiples n'approuvent pas le raisonnement ci-dessus... ou en tout cas n'y pensent pas et ne précisent pas comment ils le réfutent. Des discussions sont en cours sur ce sujet entre philosophes spécialistes des probabilités et de physique quantique. Espérons qu'ils trouveront un accord... au moins dans notre branche de l'Univers.

Quand la physique démontre des théorèmes mathématiques

Des raisonnements de physique permettent parfois de prouver rapidement des théorèmes difficiles et d'éviter de longs calculs.

N ombreuses sont les disciplines mathématiques nées de questions que la physique posait. Cependant, les mathématiciens revendiquent une autonomie totale et ont toujours prétendu donner des démonstrations ne s'appuyant que sur des axiomes choisis sans qu'il faille les justifier par des considérations physiques ou expérimentales. De cela, il résulte que même si, pour l'historien, la physique précède souvent les mathématiques, pour le logicien c'est l'inverse : quand le mathématicien écrit ses articles et ses livres, il produit les résultats, puis, seulement après, ceux-ci sont appliqués à tel ou tel problème physique.

Cette conception des mathématiques comme une science pure qui ne met pas les mains dans le cambouis des réalités terrestres et se donne comme un outil théorique indépendant est préjudiciable, d'abord pour le mathématicien lui-même, ensuite pour l'élégance de ses démonstrations et leur communicabilité, et enfin pour la puissance et la pertinence des intuitions.

Un livre de Mark Levi, professeur de mathématiques à l'Université d'État de Pennsylvanie, vient nous en faire une singulière démonstration et nous incitera peut-être à revoir le dogme axiomatique, ou au moins à le tempérer. Le titre du livre annonce la couleur : *The Mathematical Mechanic: Using Physical Reasoning to Solve Problems* (La mécanique des mathématiques : l'utilisation du raisonnement physique pour la résolution des problèmes, Princeton University Press, 2009).

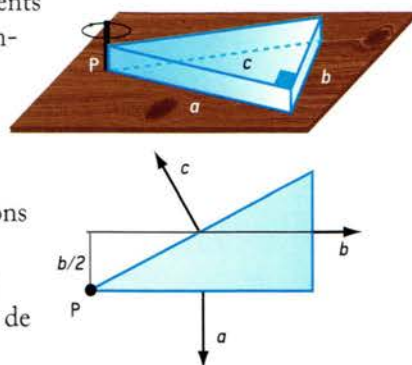
L'ouvrage recense une grande variété de problèmes mathématiques dont la solution s'obtient par des méthodes de raisonnements physiques. De telles démonstrations physiques n'ont bien sûr d'intérêt que lorsqu'elles font mieux, c'est-à-dire lorsqu'elles sont plus simples et plus claires, que les démonstrations « internes » aux mathématiques. C'est le cas de la plupart des exemples retenus par l'auteur.

Plusieurs questions se posent à propos de ces « démonstrations physiques ».

Question 1 : En quoi est-ce que ce sont des démonstrations ?

Question 2 : Pourrait-on en tirer des preuves susceptibles de satisfaire un mathématicien, et est-ce souhaitable ?

Question 3 : Ces preuves physiques de résultats mathématiques sont-elles utiles ?



1 Pythagore démontré par l'hydrostatique.

Avant de tenter des réponses, donnons quelques exemples des raisonnements physiques collectionnés par M. Levi.

Pythagore et l'eau qui dort

On connaît de nombreuses démonstrations géométriques du théorème de Pythagore. Elles procèdent souvent par découpage et surgissent comme une évidence d'un dessin sans qu'aucun commentaire ne soit nécessaire. Vous trouverez aussi des démonstrations particulièrement frappantes de ce théorème procédant par dessins animés.

La démonstration physique que propose M. Levi est d'une autre nature et d'une singulière beauté : elle s'appuie sur l'idée qu'une boîte triangulaire remplie d'eau posée sur une table... reste immobile.

Considérons une boîte de la forme du triangle rectangle qui nous intéresse (*voir la figure 1*) de côtés a , b et c , et dont on veut montrer que $a^2 + b^2 = c^2$. On remplit cette boîte d'eau, et bien sûr, elle reste immobile sur la table : elle ne glisse ni ne tourne !

La pression exercée sur les parois de la boîte est équivalente à une force perpendiculaire à la paroi, s'exerçant au centre. Cela est vrai des trois parois. Puisque la boîte ne tourne pas autour de l'axe correspondant au point P, c'est que les moments de ces trois forces vis-à-vis de cet axe s'annulent (le moment de la force F par rapport à l'axe X est le produit de la distance du point d'appui de la force par l'intensité de la composante tangentielle de la force).

Ici il y a trois forces, chacune d'entre elles est proportionnelle à la surface correspondante, elle-même proportionnelle à la longueur du côté du triangle concerné. Les distances des points d'appuis (ramenés à des droites passant par P) sont respectivement $a/2$, $b/2$ et $c/2$. En prenant en compte les directions des forces (les mêmes directions pour a et b qui s'opposent à la direction de c) le fait que les trois forces s'annulent s'écrit :

$$a(a/2) + b(b/2) = c(c/2), \text{ soit } a^2 + b^2 = c^2.$$

Comme l'écrit M. Levi, le théorème de Pythagore est une conséquence de la remarque peu intéressante au premier abord que l'eau tranquille... reste tranquille.

Que la géométrie bénéficie de la physique n'est peut-être pas étonnant, aussi, pour le second exemple, nous allons envisager une question purement algébrique.

Moyenne électrique

Chacun sait que la moyenne arithmétique des nombres $a_1, a_2, \dots, a_n$ est, par définition :

$$MA = (a_1 + a_2 + \dots + a_n)/n.$$

La moyenne harmonique (qui évite que quelques grands nombres perturbent trop le résultat d'une moyenne entre une majorité de petits nombres) est, par définition, l'inverse de la moyenne (arithmétique) des inverses :

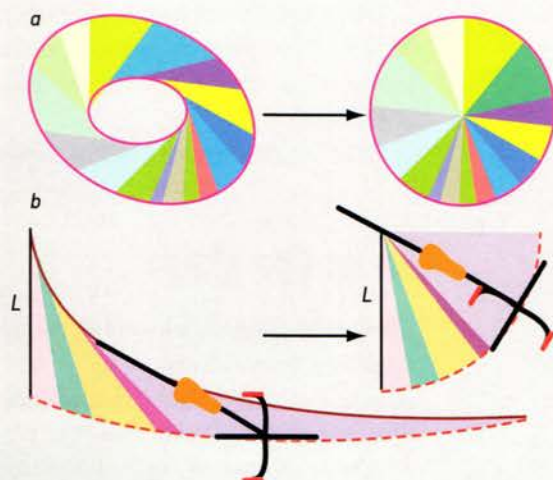
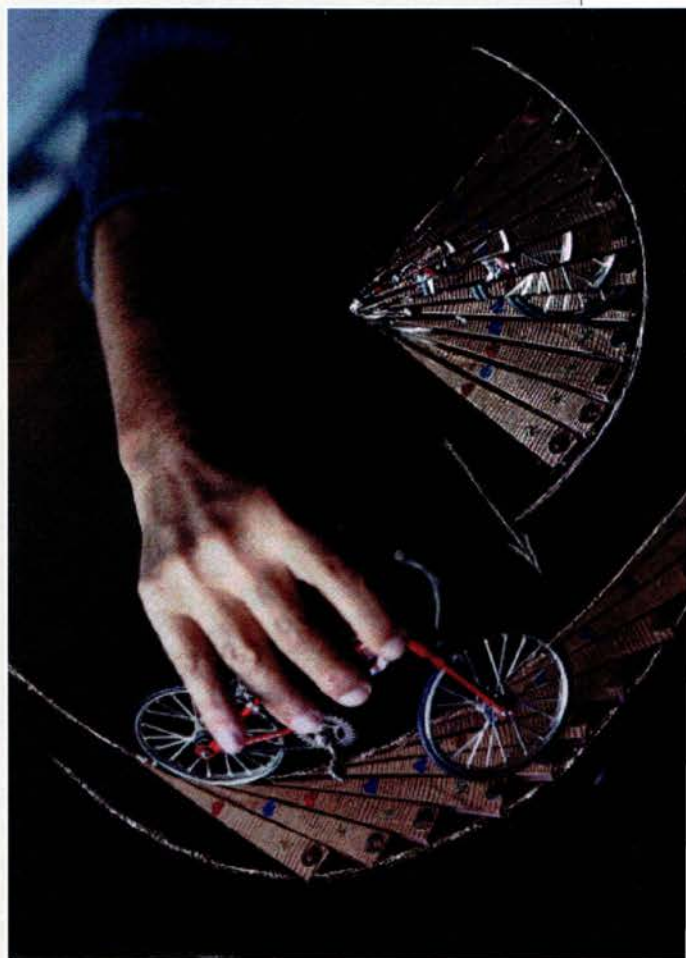
$$MH = 1/[(1/a_1 + 1/a_2 + \dots + 1/a_n)/n] = n/(1/a_1 + 1/a_2 + \dots + 1/a_n).$$

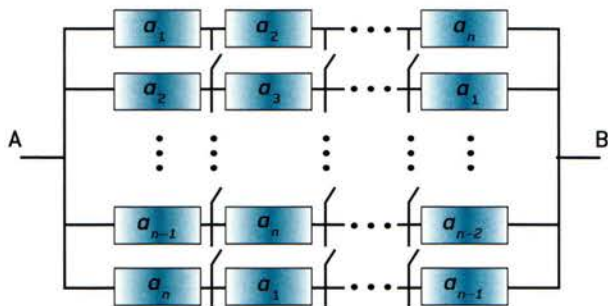
Existe-t-il une relation entre ces deux moyennes ? La réponse est oui et le mathématicien démontre que si tous les nombres auxquels on s'intéresse sont positifs, alors on a toujours $MH \leq MA$. Voici la « démonstration électrique » qu'on peut en faire.

Souvenons-nous : dans un circuit électrique, la résistance de plusieurs éléments $a_1, a_2, \dots, a_n$ mis en série est la somme $a_1 + a_2 + \dots + a_n$ des résistances de chacun des éléments. La résistance R de plusieurs résistances mises en parallèle $a_1, a_2, \dots, a_n$ est

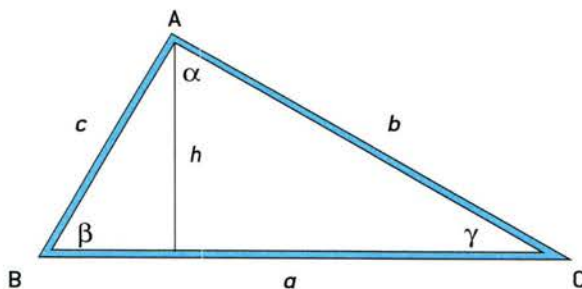
2. L'aire entre deux courbes

Le calcul de l'aire comprise entre les traces de deux roues d'une bicyclette semblait bien compliqué jusqu'à ce que l'on applique une méthode mise au point par Mamikon Mnatsakanian alors qu'il était étudiant en Arménie. Il a montré, dans le cas de l'anneau de la figure *a*, que l'on pouvait résoudre les problèmes de calcul intégral en ramenant l'origine de tous les segments tangents à la courbe intérieure (constitution d'un «hodogramme») et en calculant l'aire balayée par ces segments dans le mouvement. La méthode s'applique à l'aire entre les deux traces des roues de bicyclettes de la figure *b* : l'aire balayée est égale au secteur de cercle d'angle égal à la rotation de l'axe de la bicyclette ; le rayon du cercle est égal à la distance L entre les moyeux des roues.





3 Moyennes arithmétique et harmonique comparées par l'électricité.



4 La loi des sinus démontrée par l'hydrostatique.

donnée par la relation $1/R = 1/a_1 + 1/a_2 + \dots + 1/a_n$. On sait également que si, dans un circuit, on relie certains points par de nouveaux fils, par exemple si on ferme certains interrupteurs, la résistance totale diminue. La raison est que cela crée de nouveaux chemins pour les électrons, ce qui facilite la circulation et réduit donc la résistance totale.

Nous avons tout en main pour comparer les moyennes arithmétiques et harmoniques. Intéressons-nous au circuit de la figure 3, en supposant que les composants $a_1, a_2, \dots, a_n$ ont respectivement pour résistance $a_1, a_2, \dots, a_n$.

Chaque ligne a pour résistance $S = a_1 + a_2 + \dots + a_n$. Il y a n lignes en parallèle, donc, quand les interrupteurs sont ouverts, la résistance R_1 entre A et B est S/n (car $1/R_1 = 1/S + 1/S + \dots + 1/S$). Autrement dit, $R_1 = MA = (a_1 + a_2 + \dots + a_n)/n$.

Le circuit calcule la moyenne arithmétique : si vous êtes fatigué de calculer des moyennes à la main, construisez ce circuit et mesurez la résistance. Le calcul se fera tout seul !

Quand les interrupteurs sont fermés, la résistance R_2 entre A et B est celle d'un circuit comportant en série n fois les circuits composés des résistances $a_1, a_2, \dots, a_n$ mises en parallèle (car chaque colonne du tableau comporte des éléments de résistance $a_1, a_2, \dots, a_n$). On a donc :

$$R_2 = n / (1/a_1 + 1/a_2 + \dots + 1/a_n) = MH.$$

Puisque la fermeture des interrupteurs a diminué la résistance, $R_2 \leq R_1$, ou encore : $MH \leq MA$. Sans avoir fait le moindre calcul, nous avons démontré que la moyenne harmonique de n nombres positifs est toujours inférieure ou égale à leur moyenne arithmétique.

Passons maintenant à la trigonométrie.

La loi des sinus

Dans un triangle quelconque, il existe une relation entre les longueurs des côtés et les angles correspondants :

$a/\sin \alpha = b/\sin \beta = c/\sin \gamma$. En considérant à nouveau la physique des liquides, nous allons démontrer cette double égalité.

On se donne un tube de section constante, composé de trois segments, qui a la forme du triangle étudié (voir la figure 4). La pression P_B en B et la pression P_C en C sont égales ; en soustrayant la pression en A, on obtient donc : $P_B - P_A = P_C - P_A$.

Mais la différence de pression $P_C - P_A$ entre C et A est proportionnelle à la hauteur de la colonne d'eau au-dessus de C, c'est-à-dire à $b \sin \gamma$. De même, la différence de pression $P_B - P_A$ entre B et A est proportionnelle à $c \sin \beta$, avec bien sûr la même constante de proportionnalité (qui dépend de la section du tube et du liquide utilisé). Puisque ces différences sont égales, nous avons $b \sin \gamma = c \sin \beta$. Cela donne la seconde égalité recherchée, $b/\sin \beta = c/\sin \gamma$. La première égalité se déduit de la même façon en plaçant horizontalement le côté AB de notre tube triangulaire.

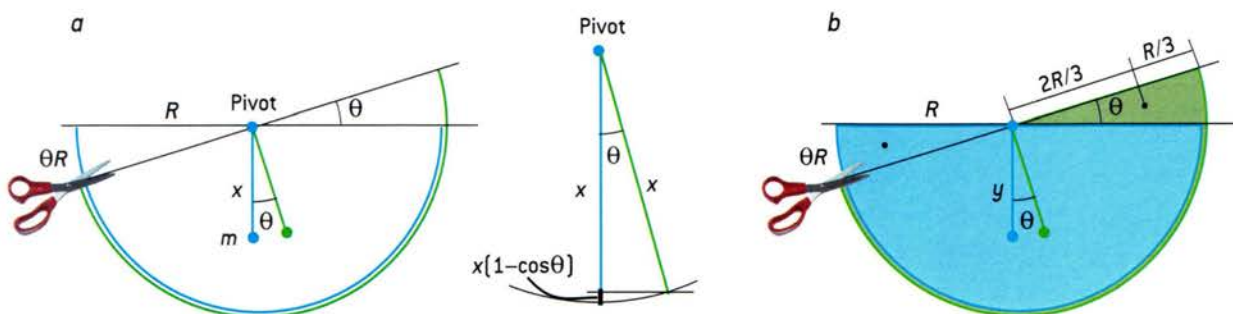
Le centre de gravité d'un secteur de cercle et d'un disque

Le calcul d'un centre de gravité se fait à l'aide d'intégrales. Parfois, cependant, une idée physique dispense de tout calcul. Considérons par exemple le demi-périmètre d'un cercle de rayon R supposé fait d'une tige courbée pesant un kilogramme par mètre (voir la figure 5). Pour une raison de symétrie, le centre de gravité de la tige en demi-cercle est sur le rayon passant par le centre du cercle support et coupant le demi-périmètre en deux quarts de périmètre. La question posée est : à quelle distance x du centre du cercle est situé le centre de gravité que nous recherchons ?

Pour le savoir, plaçons la tige (supposée tenue par des fils) dans la position représentée sur la figure 5a. En faisant légèrement tourner le demi-périmètre d'un angle ϑ (supposé petit), on déplace le centre de gravité vers le haut de $x(1 - \cos \vartheta)$, et le travail effectué est égal à $\pi R x(1 - \cos \vartheta)$.

Le travail fourni pour ce déplacement est le même que celui qu'il faut fournir pour déplacer le petit arc de cercle de masse ϑR , d'une hauteur de ϑR . Cela signifie que $\pi R x(1 - \cos \vartheta) = (\vartheta R)^2$, d'où l'on déduit que $x = \vartheta^2 R / \pi(1 - \cos \vartheta)$. Comme $(1 - \cos \vartheta)$, pour les petites valeurs de ϑ , équivaut à $\vartheta^2/2$, l'expression se simplifie et donne finalement : $x = 2R/\pi$.

Le même raisonnement s'applique quand, au lieu de considérer un demi-périmètre, on considère un demi-disque (voir la figure 5b). Cette fois, le travail effectué lors de la montée du centre de gravité quand on tourne le demi-disque est équivalent au travail à produire pour déplacer le petit triangle déterminé par l'angle de rotation. Ce petit triangle monte d'une hauteur de $2/3 \vartheta R$, car le centre de gravité d'un triangle est situé à une hauteur égale au tiers de celle d'un triangle (les médianes se coupent au tiers). Le



5 Calculs des positions des centres de gravité d'un demi-cercle et d'un demi-disque.

résultat final est donc le même que précédemment, multiplié par $2/3$. Autrement dit, cette fois : $x = 4R/3\pi$.

La chaînette

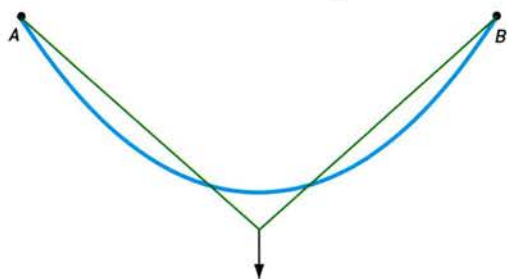
Une chaîne homogène qui pend entre deux points fixés prend la forme d'une courbe en U. Galilée s'y est intéressé et pensait, à tort, que la forme de la courbe était celle d'une parabole. À la suite d'un défi lancé par Jacques Bernoulli en 1691, trois mathématiciens trouvèrent simultanément la solution : Gottfried Leibniz, Jean Bernoulli et Christiaan Huygens. La forme que prend la courbe est celle définie par la fonction cosinus hyperbolique $\text{ch}(x) = (e^x + e^{-x})/2$, qu'on appelle aussi chaînette.

Une question simple se pose, dont la réponse demande *a priori* un calcul assez compliqué : en tendant le point bas de la chaînette, la courbe devient une réunion de deux droites obliques ; ces deux droites ont-elles un centre de gravité plus haut ou plus bas que celui de la chaînette (voir la figure 6) ?

Ne vous lancez surtout pas dans un calcul, la réponse est évidente. Si la position d'équilibre de la courbe est la chaînette, c'est qu'elle minimise l'énergie potentielle de la chaîne ; donc, en tirant la pointe de la chaîne, le centre de gravité remonte. Non seulement le centre de gravité est plus haut quand vous avez obtenu les deux segments de droite, mais pour chacune des positions intermédiaires prise par la chaîne quand vous opérez la traction, les

deux bouts de chaînette qui se rejoignent au point de traction ont un centre de gravité plus haut que celui de la chaînette initiale. Remarquons aussi que Galilée, sans connaître la vraie nature de la courbe, pouvait répondre correctement.

Dans le problème suivant aussi, une solution mathématique traditionnelle nécessiterait des calculs épouvantables alors que des considérations simples vont le résoudre.



6 La chaînette et le déplacement du centre de gravité.

Le vélo qui tourne

Imaginons une bicyclette qui exécute un parcours en revenant à sa position initiale. On suppose que la roue avant suit une trajectoire T_1 tandis que la roue arrière suit une trajectoire T_2 . Le problème est de démontrer que l'aire délimitée par les deux trajectoires T_1 et T_2 ne dépend pas des trajectoires particulières suivies par la roue avant et la roue arrière (voir la figure 2).

Il résulte de la propriété demandée que si vous faites avec votre bicyclette le tour d'une chaise ou de votre village, l'aire entre T_1 et T_2 sera la même !

La solution est que l'aire entre les deux courbes est toujours πL^2 , où L est la distance séparant la roue avant de la roue arrière. L'axe de la bicyclette est toujours tangent à la courbe de la roue arrière (car la roue arrière ne pivote pas). L'aire balayée par le segment de droite AB reliant le centre de la roue avant et le centre de la roue arrière est l'aire que nous devons évaluer. On peut imaginer que le déplacement de ce segment AB est décomposé en déplacements infinitésimaux et qu'on opère cette

décomposition en distinguant déplacements dans le sens de l'axe AB et déplacements laissant B fixe (rotation de AB). Les déplacements du premier type ne balayent aucune aire. Seuls les seconds déplacements comptent donc pour notre problème, et globalement l'aire balayée par AB lors de ces déplacements est celle que parcourt le segment AB quand il fait un tour complet, B restant fixé. L'aire recherchée est donc l'aire du disque de rayon L , qui est πL^2 .

Le type de raisonnement donné dans cet exemple est à rapprocher des raisonnements utilisés par les physiciens pour calculer des aires, des volumes, des attractions gravitationnelles ou électriques engendrées par des corps sphériques ou autres quand on les imagine décomposés en petits morceaux (raisonnements qui ont été inventés par les mathématiciens grecs). Les mathématiciens contemporains savent rendre ces raisonnements conformes aux exigences de rigueur qu'ils s'imposent. Malheureusement, cela se fait bien souvent au prix de complications, voire de très grosses complications, où, malheureusement, l'intuition initiale se perd.

Après ces exemples pris parmi une cinquantaine proposés par M. Levi, revenons aux trois questions posées initialement au sujet des preuves «physiciennes» de résultats mathématiques.

Question 1 : En quoi est-ce que ce sont des démonstrations ?

Les raisonnements physiques sont des démonstrations dans le sens suivant : s'appuyant sur des évidences sensibles (de nature physique) et procédant étape par étape, ils font passer d'un certain nombre d'affirmations acceptées à une affirmation nouvelle qui est la conclusion. Or ce passage contrôlé d'une série d'affirmations à une autre correspond à la définition même d'une démonstration. Ce n'est pas parce que les mathématiques ont identifié certains ensembles de vérités primaires, nommées axiomes ou postulats, et qu'elles réussissent à faire assez bien tout ce qu'elles souhaitent en se limitant à ces vérités primaires-là, qu'on doit s'interdire d'envisager d'autres ensembles d'affirmations de base, surtout quand il s'agit d'enseignement.

Qu'est-ce qu'une démonstration ?

Ce qui compte, c'est le chemin suivi et l'articulation persuasive des propositions d'une démonstration. Les «chemins» s'appuyant sur les concepts et lois physiques (ou géométriques) produisent une meilleure compréhension à ceux qui les parcourent, que ceux parfois pénibles et inutilement difficiles que les mathématiciens modernes retiennent prioritairement. Il est certes intéressant de tout enfermer dans un nombre limité de formalismes fixés une fois pour toutes (par exemple celui de la théorie des ensembles qui est puissant et assez commode), mais cela se fait trop souvent au prix d'une moindre clarté, et en mettant en œuvre des artifices, dont la valeur pédagogique est médiocre. N'oublions pas que la démonstration est un moyen de communication ! Les démonstrations physiques constituant véritablement des démonstrations corrigeront parfois l'abs traction et la complication déraisonnables des démonstrations «officielles».

Question 2 : Pourrait-on en tirer des preuves susceptibles de satisfaire un mathématicien, et est-ce souhaitable ?

La réponse est sans doute oui pour la première partie de la question, mais à vouloir replacer dans les formalismes standards du mathématicien contemporain les preuves de type physique (après avoir identifié ce qui doit être pris comme axiomes, et comme règles), on risque de perdre une bonne part du bénéfice heuristique de ces preuves et leur agrément. De plus, on découvrira qu'après « transcription », les preuves provenant des raisonnements physiques sont devenues longues et souvent sans doute plus longues que les preuves que le mathématicien a pris l'habitude de retenir. Les preuves physiques ne sont brèves et éclairantes que quand elles sont exprimées directement dans le langage et avec les concepts de la physique. Retraduites, elles risquent de devenir contournées et plus assez directes pour aider à la compréhension des propositions visées.

Question 3 : Ces preuves physiques de résultats mathématiques sont-elles utiles ?

Oui, de plusieurs façons. En restant plus proches des concepts que le physicien retient, elles aident à une meilleure perception physique des situations et dispositifs concernés. Quand une figure interprétée physiquement démontre, au sens de M. Levi, une affirmation mathématique, cela produit une clarté que ne donne pas la réduction formaliste et axiomatique chère au mathématicien.

Plus important peut-être : en permettant une pensée directe et en construisant une intuition fine et précise en prise immédiate avec les objets physiques, les méthodes des raisonnements physiques aident à trouver d'autres résultats inconnus et à les démontrer. On peut ainsi imaginer des généralisations faciles (pour le physicien) du théorème de la bicyclette donné en exemple.

Il est plusieurs fois arrivé que les formalismes mathématiques soient en retard sur les pratiques de raisonnement des physiciens. Un travail important de formalisation a parfois été nécessaire pour rattraper ce retard et mettre en place un formalisme conforme aux critères de rigueur du mathématicien. La théorie des distributions, qui étend la notion de dérivée, est un exemple récent d'une telle situation, où, avec une certaine peine, les mathématiciens, en l'occurrence le Russe Serge Sobolev (1908-1989) et le Français Laurent Schwartz (1915-2002), justifiaient les raisonnements des physiciens, mais largement après coup. L'analyse non standard, qu'on peut voir comme la théorie des raisonnements utilisant les infinitésimaux si chers aux physiciens, est un autre exemple de justification tardive.

Les mathématiques ne sont pas une doctrine définitivement fixée et fossilisée dans quelques systèmes d'axiomes qu'on n'a plus le droit de discuter et de revoir. Il y a mille façons de pratiquer les parcours d'affirmations en affirmations que sont les démonstrations mathématiques : accepter leur diversité est conforme à la véritable nature des mathématiques.

Il est sans doute dommage que, dans l'enseignement, la géométrie ait perdu ce rôle d'exemple : une discipline où, à l'aide de règles limitées, on déduit toutes sortes d'affirmations nouvelles et souvent inattendues, en s'appuyant sur la force imaginative que donne l'intuition du plan et de l'espace dont chacun dispose avant même d'entrer dans le cours de mathématiques. Les méthodes de raisonnement physique sont comparables et leur puissance mérite d'être utilisée dans l'enseignement des mathématiques où elles aideront les élèves à comprendre l'intérêt général du raisonnement rigoureux et l'agrément qu'il y a à tirer, comme par magie, des énoncés nouveaux d'énoncés admis.

I - La logique de l'infini

L'infini est-il paradoxal en mathématiques ?

- A. KANAMORI, *The Higher Infinite*, Springer-Verlag, 1994.
 J.W. DAUBEN, *Georg Cantor: His Mathematics and Philosophy of the Infinite*, Harvard University Press, 1979.
 J.-L. KRIVINE, *Théorie des ensembles*, Cassini, Paris, 1998.
 B. BOLZANO, *Les paradoxes de l'infini*, introduction, traduction de l'allemand et notes par Hourya Sinaceur, Seuil, 1993.
 J.-P. DELAHAYE, *Jeux mathématiques et mathématiques des jeux*, chapitre 7: *Des jeux infinis aux grands ensembles*, Belin/Pour la science, 1998.
Infini des mathématiciens, infini des philosophes, ouvrage collectif sous la direction de F. Monnoyeur, Belin, 1992.

Imaginer l'infini, ou le découvrir ?

- J. BAGARIA, *Natural Axioms of Set Theory and the Continuum Problem*, 2007 :
www.crm.es/publications/04/pr591.pdf
 P. DEHORNOY, *Au-delà du forcing: la notion de vérité essentielle en théorie des ensembles*, in *Logique, Dynamique et Cognition*, 2007.
<http://www.math.unicaen.fr/~dehornoy/Surveys/>
 L. BELLOTTI, *Woodin on the continuum problem: an overview and some objections*, in *Logic and Philosophy of Science*, III-1, 2005.
 H. WOODIN, *Set Theory after Russell. The Journey Back to Eden. In One Hundred Years of Russell's Paradox*, De Gruyter, Berlin, 2004.
 P. DEHORNOY, *Progrès récents sur l'Hypothèse du Continu [d'après Woodin]*, Séminaire Bourbaki, 55^e année, 915, 2002-2003.
 H. WOODIN, *The continuum hypothesis, Parts I and II*, in *Notices of the Amer. Math. Soc.* 48, n° 6 et 7, pp. 567-576 et 681-690, 2001.
 P. COHEN, *Set Theory and the Continuum Hypothesis*, Benjamin 1966.

L'ensemble de tous les ensembles

- R. HOLMES, *Elementary set theory with a universal set*, 1998/2010 :
<http://math.boisestate.edu/~holmes/holmes/head.ps>
 L. MOSS, *Non-wellfounded set theory*, Stanford Encyclopedia of Philosophy, 2008 :
<http://plato.stanford.edu/entries/nonwellfounded-set-theory/>
 R. HOLMES, *Alternative Axiomatic Set Theories*, Stanford Encyclopedia of Philosophy, 2006 :
<http://plato.stanford.edu/entries/settheory-alternative/>
 J. BARWISE et L. MOSS, *Vicious circles*, CSLI Lecture Notes n° 60, CSLI Publications, 1996.
 Th. FORSTER, *Set Theory with a Universal Set*, Oxford

Logic Guides, n° 31 (2^e édition), Cambridge University Press, 1995.

P. ACZEL, *Lectures on nonwellfounded sets*, CSLI Lecture Notes n° 9, 1987.

J. BARWISE et J. ETCHEMENDY, *The Liar. An Essay on Truth and Circularity*, Oxford University Press, 1987.

W. QUINE, *New foundations for mathematical logic*, *American Mathematical Monthly*, vol. 44, pp. 70-80, 1937.

II - L'incomplétude et les limites logiques

L'incomplétude, le hasard et la physique

- G. GUERRERIO, *Gödel, Logique à la folie*, in *Les Génies de la Science*, n° 20, Belin/Pour la Science, 2004.
 L. LEVIN, *Forbidden information*, in *Proc. Annual IEEE Symp. on Foundations of Computer Science*, 2002.
<http://arXiv.org/abs/cs.CC/0203029>
 J.-P. DELAHAYE, *L'intelligence et le calcul. De Gödel aux ordinateurs quantiques*, Belin/Pour la Science, 2002.
 R. SMULLYAN, *Les théorèmes d'incomplétude de Gödel*, Masson, Paris, 1993.
 K. GÖDEL, *Collected Works*, Volume I (Publications 1929-1936), Oxford University Press, 1986.

Presque tout est indécidable !

- C. S. CALUDE, *Incompleteness: A Personal Perspective*, Centre for Discrete Mathematics and Theoretical Computer Science, in *Research Report Series CDMTCS 324*, juin 2008.
 J.-P. DELAHAYE, *L'incomplétude, le hasard et la physique*, in *Pour la Science*, pp. 90-95, mai 2007.
 J.-P. DELAHAYE, *Omega Numbers, Randomness and Complexity. From Chaitin To Leibniz*, sous la direction de C. S. CALUDE, World Scientific, pp. 343-358, 2007.
 C. S. CALUDE et H. JÜRGENSEN, *Is complexity a source of incompleteness?*, in *Advances in Applied Mathematics* 35, pp. 1-15, 2005.
 C. S. CALUDE, *Chaitin numbers, Solovay machines and incompleteness*, in *Theoretical Comput. Sci.* 284, pp. 269-277, 2002.
 C. S. CALUDE, H. JÜRGENSEN et M. ZIMAND, *Is independence an exception?*, in *Appl. Math. Comput.* 66, pp. 63-76, 1994.

III - La logique du désordre et des probabilités

L'étonnante loi de Benford

- C. CALDWELL, *Does Benford's law apply to prime numbers?*, 2006 :
<http://primes.utm.edu/notes/faq/Benford'sLaw.html>
 P. JOLISSAINT, *Loi de Benford, relations de récurrence et suites équidistribuées*, 2005 : w3.jura.ch/ijsla/Benford.pdf
 P. N. POSCH, *A survey on sequences and distribution functions satisfying the first-digit-law*, 2004 :
<http://www.posch.net/>

E. JANVRESSE et T. de la RUE, *La loi de Benford*, in *Quadrature* n° 48, pp. 5-9, avril-juin, 2003.

P. D. SCOTT et M. FASLI, *Benford's law: an empirical investigation and a novel explanation*, 2001 : <http://citeseer.ist.psu.edu/709593.html>

T. HILL, *A statistical derivation of the significant-digit law*, in *Statistical Science*, 10(4) pp. 354-363, 1995.

V. ARNOLD et A. AVEZ, *Ergodic Problems of Classical Mechanics*, Benjamin, 1968.

F. BENFORD, *The law of anomalous numbers*, in *Proc. American Philosophical Society*, 78(4) pp. 551-772, 1938.

S. NEWCOMB, *Note on the frequency of the use of the digits in natural numbers*, in *Amer. Jour. Math.*, 4, pp. 39-40, 1881.

Le désordre total n'existe pas...

A. SOIFER, *The Mathematical Coloring Book*, Springer, 2009.

T. GERKEN, *Empty convex hexagons in planar point sets*, in *Discrete Comput. Geom.*, vol. 39, pp. 239-272, 2008.

Carlos M. NICOLAS, *The empty hexagon theorem*, in *Discrete Comput. Geom.*, vol. 38, n° 2, 2007.

V. A. KOSHELEV, *On the Erdős-Szekeres Problem*, in *Doklady Mathematics*, vol. 76, n° 1, 2007.

J.D. HORTON, *Sets with no empty convex 7-gon*, in *Canad. Math. Bull.*, vol. 26, pp. 482-484, 1983.

M.H. OVERMARS, *Finding sets of points without empty convex 6-gons*, in *Discrete Comput. Geom.*, vol. 29, pp. 153-158, 2003.

A. SÁRKÖZY, *On difference sets of sequences of integers III*, in *Acta Math. Acad. Sci. Hungar.*, vol. 31, pp. 355-386, 1978.

P. ERDŐS et G. SZEKERES, *A combinatorial problem in geometry*, in *Compositio Mathematica*, vol. 2, pp. 463-470, 1935.

Pierre, feuille, ciseaux...

C. MEYER, *Sagace* : <http://ch.meyer.free.fr/favorite.htm>

G. SZABÓ, A. SZOLNOKI, et R. IZSÁK, *Rock-scissors-paper game on regular small-world networks*, in *J. Phys. A: Math. Gen.*, 37, pp. 2599-2609, 2004.

B. SIVERO et C.M. LIVELY, *The rock-paper-scissors game and the evolution of alternative male reproduction strategies*, in *Nature*, vol. 380, pp. 240-243, 1996.

B. KERR, M. RILEY, M. FELDMAN et J. M. BOHANNAN, *Local dispersal promotes biodiversity in a real-life game of rock-paper-scissors*, in *Nature*, vol. 418, pp. 171-174, 11 juillet 2002.

A. SZOLNOKI et G. SZABÓ, *Phase transitions for rock-scissors-paper game on different networks*, in *Phys. Rev. E* 70, 2004.

La Belle au bois dormant, la fin du monde et les extraterrestres

J.-P. DELAHAYE, *Logique, informatique et paradoxes*. Le chapitre III traite du paradoxe de l'Apocalypse. Éditions Belin/Pour la science, 1995.

N. BOSTROM, *Anthropic Bias. Observation Selection Effects in Science and Philosophy*, Routledge, New York, 2002.

J. LESLIE, *The End of the World. The Science and Ethics of Human Extinction*, Routledge, New York, 1996.

P. FRANCESCHI, Thèse : <http://www.univ-corse.fr/~franceschi/index-fr.htm>

IV - Logiques de graphes et de nombres

Une priorité cachée des graphes

R. DIESTEL, *Graph Theory*, Springer, 2006. Version électronique en : <http://www.math.uni-hamburg.de/home/diestel/books/graph.theory/>

L. LOVASZ, *Graph minor theory*, in *Bulletin of the American Mathematical Society*, vol. 42-1, pp. 75-86, 2005.

N. ROBERTSON et P. SEYMOUR, *Graph minors XX. Wagner's conjecture*, in *Journal of Combinatorial Theory*, B 92-2, pp. 325-357, 2004 (dernier article de la série de 20, donnant la démonstration de la conjecture de Wagner).

B. HOHAR et C. THOMASSEN, *Graphs on Surfaces*, The Johns Hopkins University Press, 2001.

D. ARCHDEACON, *Variations on a theme of Kuratowski*, in *Discrete Mathematics*, vol. 302, pp. 22-31, 2005.

Graphes et algorithmes pour ballons

E. DEMAINE, M. DEMAINE et V. HART, *Computational Balloon Twisting: The Theory of Balloon Polyhedra* in *Proceedings of the 20th Canadian Conference on Computational Geometry*, Montréal, Québec, Canada, August 13-15, 2008 : <http://cccg.ca/proceedings/2008/paper34full.pdf>

D. ALAN, *Rubber Circus*, Magic Inc., Chicago, 1958.

A. KOTZIG, *The Theory of Finite Regular Graphs of Degree Three and Four*, Casopis Pestov. Mat., 82 : 76-92, 1957.

Un terrain de course numérique

A. GRANVILLE et G. MARTIN, *Prime number races*, in *American Mathematical Monthly*, vol. 113-1, pp. 1-33, 2006.

P. BORWEIN et al., *The Riemann Hypothesis: a Resource for the Afficionado and Virtuoso Alike*, Springer-Verlag, 2007.

J.-P. DELAHAYE, *Merveilleux nombres premiers*, Pour la Science/Belin, 2000.

J. KACZOROWSKI, *On the distribution of primes (mod 4)*, in *Analysis*, vol. 15, pp. 159-171, 1995.

M. RUBINSTEIN et P. SARNAK, *Chebyshev's bias*, in *Experiment. Math.*, vol. 3, pp. 173-197, 1994.

S. KNAPOWSKI et P. TURAN, *On prime Numbers 1 resp. 3 mod 4*, in *Number Theory and Algebra*, Academic Press, New York, pp. 157-165, 1977.

J. E. LITTLEWOOD, *Distribution des nombres premiers*, in *C. R. Acad. Sci.*, Paris, vol. 158, pp. 1869-1872, 1914.

V - Logique sociale, économique et humaine

La répartition idéale des biens existe-t-elle ?

K. ARROW, *Social Choice and Individual Values*, Yale University Press, 1963.

U. ENDRIS, N. MAUDET, F. SADRI et F. TONI, *Negotiating socially optimal allocations of resources*, in *Journal of Artificial Intelligence Research*, 25, 315-348, 2006.

T. SANDHOLM, *Contract types for satisfying task allocation: theoretical results*, AAAI Spring Symposium: Satisfying Models, USA, California, Stanford University, 23-25, 1998.

A. NONGAILLARD, P. MATHIEU et B. JAUMARD, *A multi-agent resource negotiation for the utilitarian welfare*, ESAW'08

(Engineering Societies in the Agents World), et LNAI 5485, Springer-Verlag, 2009.

Escroquerie ou jeu risqué ?

R. GUBERT et E. SAINT-SIMON, « Et surtout n'en parlez à personne... » *Au cœur du Gang Madoff*, Albin Michel, Paris, 2009.

Marc ARTZOUNI, *The Mathematics of Ponzi Schemes*, Department of Mathematics, Université de Pau, avril 2009.

M. ZUCOFF, *Ponzi's Scheme: The True Story of a Financial Legend*, Random House, New York, 2005.

U. BHATTACHARYA, *The optimal design of Ponzi schemes in finite economies*, in *Journal of Financial Intermediation*, vol. 12, pp. 2-24, 2003.

K. SADIRAJ et A. SCHRAM, *Informed and Uninformed Investors in an Experimental Ponzi Scheme*, Department of Economics and Econometrics, University of Amsterdam, 1998.

S. A. O'CONNELL et S. P. ZELDES, *Rational Ponzi games*, in *International Economics Review*, vol. 29-3, pp. 431-350, 1988.

Tao : l'éducation réussie d'un surdoué

T. TAO, *Poincaré's legacies: Pages from Year Two of a Mathematical Blog in American Mathematical Society*, 2009.

A. GRANVILLE, *Prime number patterns*, in *The American Mathematical Monthly*, vol. 115, pp. 279-296, 2008.

T. TAO, *Structure and Randomness: Pages from Year One of a Mathematical Blog*, in *American Mathematical Society*, 2008.

B. GREEN et T. TAO, *The primes contain arbitrarily long arithmetic progressions*, in *Annals of Math.*, vol. 167, pp. 481-547, 2008.

T. TAO, *A remark on primality testing and decimal expansions*, in *Journal of the Australian Mathematical Society*, 2008. Voir : <http://arxiv.org/abs/0802.3361>

T. TAO, *Solving Mathematical Problems: A Personal Perspective*, Oxford University, Press, 2006.

M. A. (Ken) CLEMENTS, *T. Tao*, in *Educational Studies in Mathematics*, vol. 15, n° 3, pp. 213-238, août 1984.

B. TAO, *Parental involvement in gifted education*, in *Educational Studies in Mathematics*, vol. 17, n° 3, pp. 313-321, août 1986.

VI - La logique rencontre la physique

Concevoir l'univers comme un ordinateur ?

S. LLOYD, *Programming the Universe. A quantum computer scientist takes on the cosmos*, Knopf, New York, 2006.

J.-P. DELAHAYE, *Complexités. Aux limites des mathématiques et de l'informatique*. Belin/Pour la Science (voir le chapitre 11 sur le point de vue « uniformiste » et le chapitre 18 sur les capacités de l'univers vu comme un ordinateur), 2006.

S. LLOYD et Y. JACK NG, *L'univers, un monstre informatique*, in *Pour la Science*, novembre 2004.

K. FRESE et W. KINNEY, *The ultimate fate of life in an accelerating Universe*, in *Phys. Lett.*, B558, 1, 2003.

S. AARONSON, Book Review on « A New Kind of Science » par S. Wolfram, in *Quantum Information and Computation*, vol. 2, n° 5, 410-423, 2002.

S. WOLFRAM, *A new kind of science*, Wolfram media Inc. 2002.

E. FREDKIN, *Digital Mechanics*, 2000 : <http://www.digital-philosophy.org/>

I. ASIMOV, *Le robot qui rêvait*, Éditions J'ai lu, Paris, 1988.

K. ZUSE, *Calculating space*, 1969 :

<http://www.idsia.ch/~juergen/digitalphysics.html>

Libre arbitre et mécanique quantique

J. CONWAY et S. KOCHEN, *The strong free will theorem*, in *The Notices of the American Mathematical Society*, vol. 56, n° 2, pp. 1441-1473, février 2009.

J. CONWAY et S. KOCHEN, *The free will theorem*, in *Found. Phys.*, vol. 36, 1441-1473, 2006.

S. KOCHEN et E. SPECKER, *The problem of hidden variables in quantum mechanics*, in *J. Math. Mech.*, vol. 17, pp. 59-88, 1967.

J. BARRETT, *Quantum Mechanics of Minds and Worlds*, Oxford University Press, 1999.

J. CONWAY, *Free Will and Determinism in Science and Philosophy*. Conférences filmées :

http://www.princeton.edu/WebMedia/flash/lectures/2009_03_04_conway_free_will.shtml.

H. ZWIRN et J. BRICMONT, *Philosophie de la mécanique quantique*, Éditions Vuibert, 2009.

Suicide et immortalité quantiques

S. AARONSON, *Quantum complexity and anthropic principle*, consulté en juin 2010 :

<http://www.scottaaronson.com/talks/anthropic.html>

P. J. LEWIS, *What is it to be a Schrödinger Cat?*, in *Analysis*, vol. 60(1), pp. 22-29, 2000.

P. ALMOND, *Civilization level quantum suicide*, 2008 : www.paul-almond.com/CivilizationLevelQuantumSuicide.doc

J. MALLAH, *Many-worlds interpretation can not imply « Quantum immortality »*, 2009 :

B. DEWITT et N. GRAHAM (éds.), *The Many-Worlds Interpretation of Quantum Mechanics*, Princeton University Press, 1973.

J. HIGGO, *Quantum theory of immortality*, 2001 :

<http://www.higgo.com/qti/>

M. TEGMARK, *The interpretation of quantum mechanics, many worlds or many words*, in *Fortschritte der Physik*, vol. 46, pp. 855-862, 1998 :

Quand la physique démontre des théorèmes mathématiques

M. LEVI, *The Mathematical Mechanic: Using Physical Reasoning to Solve Problems*, in *Princeton University Press*, 2009.

J.-M. KANTOR, *Mathématiques d'Est en Ouest - Théorie et pratique: l'exemple des distributions*, in *Gazette des Mathématiciens*, 2004.

T. APOSTOL, *A Visual Approach to Calculus Problems*, in *Caltech's Engineering & Science*, vol. 63 (3), pp. 22-31, 2000. <http://www.mamikon.com/VisualCalc.pdf>

P. BOULANGER, *Les données inutiles*, in *Dossier Pour la Science* n° 59, 2008.

A

actuel (infini) 12-24
 Aczel (Peter) 39
 AF et AFA 38-39, 41, 43
 aiguille de Kakeya 153, 155, 157
 aleph 16-17, 21
 algorithme probabiliste 47, 51
 Allen (Woody) 12
 allocation 132-140
 anamorphose probabiliste 90, 93-95
 antinomie 20, 34
 Asimov (Isaac) 160-169
 automate cellulaire 162-164
 axiome 11, 17, 22, 36-39, 57-58, 172-175
 axiome d'antifondation 38-39
 axiome de compréhension 36
 axiome de fondation 38-39
 axiome de la réunion 36
 axiome de l'infini 37
 axiome de remplacement 37
 axiome DP 31
 axiome du choix 30, 38
 axiome MMW 32
 axiomes SPIN TWIN MIN 172-176

B

balloonerie 111-119
 bande de Möbius 105-106, 109-110
 Barwise (Jon) 38
 Bell (John) 172
 Belle au bois dormant 90-99
 Benford (Franck) 64-72
 Bennett (Charles) 169
 Big bang 168
 bijection 16, 19, 30
 Bolzano (Bernard) 17, 18, 34
 Borel (Émile) 167
 Borge (Jorge Luis) 184
 bouteille de Klein 106

C

Calude (Cristian) 55-61
 Cantor (Georg) 13-14, 17, 19-20, 25-33
 carré magique 151
 Carter (Brandon) 95-98
 Cesàro (Ernesto) 69
 Chaitin (Gregory) 55-61

chat de Schrödinger 178-181
 classes P et NP 46, 102, 117-119, 183-184
 Cohen (Paul) 22, 23, 28-29
 complexité de Kolmogorov 52-53, 58-60, 80
 Conway (John) 163-166, 170-177

D

Dedekind (Richard) 19, 37
 Dehornoy (Patrick) 26
 Demaine (Eric et Martin) 111-119
 dénombrable 14, 26
 désordre total 73-80
 DeWitt (Brice) 180
 diagonal (raisonnement) 14, 19
 don social 138-140
 Dyson (Freeman) 59, 168

E

effet de filtre 93-94
 effet de loupe 93-94, 97
 effet de sélection 93-99
 égalitarisme 133-136
 Einstein (Albert) 51, 172-174
 ensemble de tous les ensembles 34-43
 ensemble d'obstructions 104-110
 ensembles magiques et supermagiques 156
 Erdős (Paul) 73-80
 Euclide 14
 Euler (Leonard) 113
 Everett (Hugh) 178-186
 extraterrestres 78, 90-99

F

Feynman (Richard) 162, 172
 fin du monde 90-99
 forcing 28-29
 formule de Bayes 94, 97-98
 formule stratifiée 42
 fraude 70, 72
 Fredkin (Edward) 164
 Frege (Gottlob) 39

G

Gauss (Carl) 18
 Gödel (Kurt) 11, 19, 22, 23, 27, 45-61

grand cardinal 22-24, 29-30
 graphe 78, 83-89, 102-119
 graphe eulérien 112
 graphe planaire 102-103, 107
 Green (Ben) 152

H

Hart (Vi) 111-119
 Hilbert (David) 27, 50, 55
 Holmes (Randall) 41-42
 hyperensemble 38-40
 hypothèse de Riemann 120-129, 157
 hypothèse du continu 12, 17, 21, 25-33

I

immortalité 185-186
 incomplétude 45-61
 indécidabilité 22, 30, 54, 57-58, 60
 indécidable 22, 45-61, 78
 indéterminisme 170, 172, 177
 infini 11-33
 interprétation de Copenhague 178-180
 interprétation des mondes multiples 178-186

J

Jeu de la vie 163-166

K

Klein (Esther) 73-77
 Kochen (Simon) 170-177
 Kolmogorov (Andrei) 46, 52-53, 58-60, 80
 Kronecker (Leopold) 19, 27
 Kuratowski (Kazimierz) 102

L

Landauer (Rolf) 169
 Leibniz (Gottfried) 17, 18
 Leslie (John) 95-98
 Levi (Mark) 187-194
 Levin (Leonid) 45-61
 libre arbitre 170-177
 Lloyd (Seth) 160-169
 localité 174
 loi de Benford 64-72
 loi de conservation 52-53

loi des sinus 190
loi du premier chiffre significatif 66
loterie 147, 149
loto quantique 181-182

M

Madoff (Bernard) 141-149
Martin-Löf (Per) 55, 60-61, 166
maximalisme ontologique 27-29
mécanique quantique 51, 170-186
médaille Field 151, 156
mort thermique 160-168

N

Newcomb (Simon) 66
NF, NFU 41-43
nombre oméga 60-61
nombres premiers 47, 120-129, 150-157

O

oméga-logique 32

P

P NP 46, 118, 183-184
paradoxe 12, 13, 17, 20-21, 34-43, 57, 90-99, 172-174
paradoxe de Banach-Tarski 17
paradoxe de la Belle au bois dormant 90-99
paradoxe de l'Apocalypse 95-99
paradoxe de l'autoréférence 21
paradoxe de Russell 20
paradoxe du menteur 38
paradoxe EPR 172, 174
Peano (arithmétique de) 46-50
Pierre-feuille-ciseaux 81-89
Plouffe (Simon) 66, 69, 72
Podolsky (Boris) 172, 174
polyèdre 111-119
polygone 73-77
Ponzi (Charles) 141-149
principe de conservation 52-53
problème à l'heureuse issue 73-75
problème d'allocation 132-140
problème de l'arrêt 52
programmation multi-agents 140
progression arithmétique 79, 152-154
pyramide de Ponzi 141-149

Q

Quine (Willard) 41-42

R

Ramsey (Frank) 77-80
réaction de Belousov-Zhabotinskii 87
réflexivité (paradoxes de la) 187
Robertson (Neil) 102-107
Rosen (Nathan) 172, 174
roulette quantique 178-186
Russell (Bertrand) 20, 34-43

S

Saint Thomas d'Aquin 16
Sárközy (András) 79-80
Schwartz (Laurent) 194
Seymour (Paul) 102-107
singé dactylographe 167, 168
singé programmeur 167, 168
solipsisme 176
Solovay (Richard) 55-61
stratégie mixte 81
suicide quantique 178-186
suite aléatoire 60-61, 166
suite monotone 76
surdoué 150-157
système formel 46-48
système non contradictoire 48
Szekeres (George) 73-77

T

Tao (Terence) 150-157
Tchebychev (Pafnouti) 121, 123, 126
théorème de Fary-Wagner 103
théorème de Green-Tao 152-154
théorème des sous-suites monotones 76
théorème de Kochen-Specker 171
théorème de Kuratowski 102-103
théorème des nombres premiers 123
théorème de l'hexagone vide 73-77
théorème de Pythagore 187-188
théorème de Ramsey 77-80
théorème de Robertson et Seymour 102-110
théorème des mineurs 102-110
théorème d'Euler 113, 116
théorème d'incomplétude 44-61

théorème du libre arbitre 170-177
théorie des ensembles 12-43
théorie des types 40-41
tore 105-106, 108
tout (le – et la partie) 12, 16
Turing (Alan) 51-53, 55, 162, 166

U

Ulam (Stanislaw) 163
utilitarisme 134-136

V

van den Waerden (Bartel) 79
variables cachées 173
von Neumann (John) 35, 162-163

W

Wolfram (Stephen) 165, 166
Woodin (Hugh) 26-33

Z

ZF, Zermelo-Fraenkel 20, 23, 27-43
Zuse (Konrad) 162, 167



Imprimé en France par Clerc à Saint-Amand-Montrond
N° d'édition : 84245115-02 / juin 2014 - N° d'imprimeur : 13985
Dépôt légal : avril 2012

La logique, un aiguillon pour la pensée

La logique – prise dans un sens large – a connu d'incroyables progrès depuis deux siècles. On y a découvert l'infinie variété des infinis si grands qu'on en a le vertige ; les étranges hyperensembles qui forment toutes sortes de boucles ; l'ensemble de tous les ensembles avec ses paradoxes ; l'incomplétude de Gödel et l'indécidabilité de Turing ; la troublante loi de Benford et de déconcertants paradoxes probabilistes , etc.

Ces thèmes, parmi d'autres, constituent la matière de l'ouvrage. Une place y est laissée aux raisonnements ludiques et parfois spéculatifs – il est dans la nature de la logique de s'y intéresser. De ce fait, cette logique moderne des sciences s'adresse aussi bien au mathématicien qu'au philosophe et au curieux intrigué par le monde abstrait des raisonnements.

La science logique évolue, se renouvelle et, abordant parfois des questions étonnantes, amuse autant qu'elle intrigue par sa puissance et la témérité de ses méthodes.

Jean-Paul Delahaye est professeur d'informatique à l'Université des sciences et technologies de Lille et chercheur au Laboratoire d'informatique fondamentale du CNRS, à Lille. Il tient la rubrique « Logique et calcul » de la revue *Pour la Science*.

www.pourlascience.fr

ISBN 978-2-84245-115-8



9 782842 451158

84245115

27 €