cantorienne des ensembles, théorie des grands cardinaux) à nourrir la notion d'infini et à constituer une série de domaines mathématiques nouveaux où le concept d'infini dévoile une richesse que la philosophie n'avait su déceler.

Au début du XX^{e} siècle, la logique mathématique a précisé la notion de preuve mathématique et a permis à la pensée philosophique sur les mathématiques de s'appuyer sur une multitude de notions précises (systèmes formels, calcul propositionnel et calcul de prédicats, modèles, etc.) et de résultats profonds (théorèmes de complétude, théorèmes de limitation, etc.). La philosophie des mathématiques en a été transformée, et si le débat y est devenu plus technique, la réflexion des philosophes qui acceptent ces avancées mathématiques n'en a été que plus pertinente et plus incisive (voir, par exemple, *The Philosophy of Mathematics*, W. H. Hart ed., Oxford University Press, 1996).

L'éclaircissement de la notion de calcul mécanique vers 1936 (par K. Gödel, A. Church, A. Turing) a posé le socle d'une discipline nouvelle (appelée théorie de la récursivité ou théorie de la calculabilité) qui a récemment conduit à de miraculeuses applications dans le domaine de la philosophie des sciences. La théorie de la complexité de Kolmogorov, un développement récent de la théorie de la calculabilité, est, de ce point de vue, d'une remarquable efficacité. On lui doit nombre de propositions dont la portée philosophique est incontestable et qui, dans certains cas, ont résolu des problèmes posés par les philosophes eux-mêmes.

Avant de donner quelques détails sur l'une des dernières contributions de ces théories à l'étude de la question «est-ce que les résultats mathématiquement difficiles sont pratiquement utiles ?», question incontestablement philosophique et intéressante, nous allons survoler rapidement les idées de base de la théorie de la complexité de Kolmogorov.

LE COMPLEXE, LE SIMPLE, LE HASARD

Formulée par R. Solomonoff, A. Kolmogorov et G. Chaitin vers 1965, la théorie de la complexité algorithmique, dénommée aujourd'hui complexité de Kolmogorov, a pour ambition de définir ce qu'est un objet simple, et propose une mesure absolue de la complexité.

L'idée est de donner un sens à l'évidence : la suite 01010101010101010101 est plus simple que la suite 10000100110101110110. Pourquoi donc ? Parce que la première suite peut se définir brièvement, c'est «dix fois 01», alors que la seconde n'est pas exprimable avec la même concision : pour la décrire, on ne pourra guère faire mieux que d'en énumérer les éléments : «1, puis 0, puis 0, puis 0, etc.», ce qui est beaucoup plus long.

La théorie de la calculabilité, pour définir plus précisément la simplicité en termes de programmes, utilise les machines de Turing universelles, qui sont des sortes d'ordinateurs abstraits dont chaque ordinateur réel est une réalisation particulière, à un détail près : l'ordinateur réel ne possède qu'une mémoire de travail finie, alors que la machine de Turing est munie d'un ruban de mémoire indéfiniment extensible. La théorie suggère de choisir une machine de Turing universelle, *U*, et de dire qu'un objet *O*, représenté sous forme d'une suite de 0 et de 1 (ce qui est toujours possible comme l'informatique le démontre chaque jour), est simple s'il existe un programme court *P* pour la machine *U* qui engendre l'objet *O*. Un objet sera complexe si, au contraire, aucun programme court pour *U* ne donne *O*.

Cette définition ne dépend pratiquement pas de la machine *U* choisie, ce qui est rassurant et garantit l'invariance de la notion. La complexité de Kolmogorov de *O*, *K (O)*, est la taille (mesurée en nombre de chiffres binaires) du plus petit programme qui permet à la machine *U* d'engendrer *O*.

Cette idée très naturelle : «est simple ce qui s'exprime brièvement» a en particulier permis de définir la notion de suite aléatoire, problème que la théorie des probabilités avait contourné en utilisant une notion collective de probabilité qui interdisait qu'on puisse dire, d'une suite donnée, qu'elle est aléatoire. La définition individuelle d'objet aléatoire avait été longuement recherchée par les philosophes, et par exemple Karl Popper, dans son ouvrage fondamental de 1934, *La logique de la découverte scientifique* (que Jacques Monod admirait beaucoup) y consacre plusieurs pages.

D'après la théorie de la complexité de Kolmogorov, une suite infinie de chiffres binaires est aléatoire si, par définition, à chaque fois qu'on en prend *n* chiffres, on obtient un objet dont la complexité de Kolmogorov est approximativement *n*. Dit autrement encore, il est impossible de comprimer les données contenues dans $(a_0a_1a_2...a_n...)$: être aléatoire, c'est être incompressible.

Des liens ont alors été établis entre l'incompressibilité et l'imprévisibilité : une suite aléatoire est, par nature, imprévisible, et donc incompressible. Ces définitions ont donné un sens mathématique à tout un ensemble d'idées philosophiques vagues, et ce succès remarquable est apparu comme un petit miracle après les nombreuses tentatives infructueuses passées.

La théorie de la complexité de Kolmogorov a atteint une remarquable maturité dans les années 1990, et les lecteurs intéressés trouveront un tour d'horizon complet de cette merveilleuse théorie dans le livre profond et synthétique de Ming Li et Paul Vitanyi cité en bibliographie, et une présentation plus concise se trouve dans mon ouvrage *Information, complexité et hasard,* également cité en bibliographie. Parmi les progrès philosophiques que la

2. Inutilité des résultats mathématiques difficiles

Dans la grande majorité des cas, les résultats mathématiques possédant des preuves compliquées sont d'une faible utilité pratique. Les résultats que l'on n'a pas encore prouvés aujourd'hui (qu'on dénomme des conjectures) n'ont sans doute pas de preuves simples. Malgré la fascination qu'exercent ces énigmes sur les mathématiciens et les amateurs, on ne peut attendre que peu de retombées concrètes de leurs solutions. Parmi les conjectures les plus étudiées dont l'inutilité pratique est presque certaine, indiquons :

– la conjecture de Goldbach : tout nombre pair est somme de deux nombres premiers (un million de dollars à gagner) : 24 = 11 + 13 ;

– la conjecture des nombres premiers jumeaux : il existe une infinité de paires de nombres premiers espacés de deux unités (comme 11 et 13 ou 17 et 19) ;

– la conjecture des nombres parfaits impairs : il n'existe aucun nombre parfait impair (un nombre parfait est un nombre comme 6 = 1 + 2 + 3 ou 28 = 1 + 2 + 4 + 7 + 14, qui est égal à la somme de ses diviseurs autres que lui-même). C'est sans doute la plus vieille de toutes les conjectures mathématiques.

– la conjecture de l'équirépartition des chiffres de π : la fréquence de chacun des chiffres dans le développement décimal de π est 1/10.

Plus étrange, il semble que la démonstration de la grande conjecture de l'informatique «*P* = *NP* ?» (qui concerne la classification des problèmes en fonction de la difficulté de leur résolution et qui a été dotée de un prix d'un million de dollars cette année) n'aurait pas de conséquences concrètes. Si on démontre que P est différent de *NP* (ce que les spécialistes pensent en général), aucun algorithme nouveau n'en résultera. Si l'on montre que *P* = *NP*, il apparaît probable que cela se fera d'une telle façon que rien de concrètement utile n'en sortira.

théorie de la complexité de Kolmogorov a apportés, on remarque ceux-ci.

1) Une nouvelle compréhension du sens des théorèmes d'incomplétude de Gödel : les propositions indécidables (ni elles, ni leur négation ne sont démontrables) dans une théorie donnée doivent leur existence au fait que le contenu en information de la théorie (qu'on mesure par la complexité de Kolmogorov des axiomes de la théorie) limite son pouvoir de preuve : l'incomplétude est un problème de contenu en information des théories, ce qui n'apparaissait pas clairement dans les travaux antérieurs des logiciens.

2) Une conception objective de l'entropie physique : l'entropie physique, lorsqu'on la définit traditionnellement, comporte une composante subjective (elle semble dépendre de l'observateur, ce qui est gênant) qu'évite la définition proposée par le physicien W. Zurek, définition fondée sur la prise en compte de la complexité de Kolmogorov des informations mémorisée par l'observateur.

3) Le nombre *Oméga* de Chaitin est le seul nombre réel qu'on peut définir précisément et dont on peut montrer qu'il est équiréparti dans toutes les bases (en base 10, par exemple, son écriture comporte autant de 0 que de 1, que de 2, etc.), ce qui éclaire à nouveau les phénomènes d'incomplétude et d'indécidabilité algorithmique et rassure sur la cohérence de la théorie de la mesure (laquelle indique qu'il existe des nombres équirépartis, mais ne propose aucune méthode pour en définir).

4) Une nouvelle compréhension du problème de l'induction scientifique (que le philosophe Hume considérait comme impossible et qui fut à l'origine des travaux de K. Popper), de la règle de Bayes et du principe du rasoir d'Ockam (qui indique que, dans une explication, il faut éviter autant qu'on le peut de multiplier les entités et les concepts) et des mises en relation précises de toutes ces notions.

5) La proposition par Charles Bennett d'une distinction mathématique entre complexité aléatoire et complexité organisée (utilisant la complexité de Kolmogorov), distinction qui semble essentielle pour expliquer la complexification des structures de l'Univers au cours du temps qui passe (évolution stellaire, évolution du vivant, etc.).

LA QUESTION DE L'UTILITÉ DES RÉSULTATS DIFFICILES

L'énumération pourrait se poursuivre, mais nous allons nous arrêter sur une des applications toute récente de la théorie de la complexité à l'étude d'un problème d'épistémologie des sciences : est-ce que les résultats mathématiquement difficiles sont ceux qui ont le plus de chances d'être utiles dans les applications ou, au contraire, un résultat mathématiquement difficile est-il toujours condamné à avoir peu d'incidences concrètes?

Bien sûr, tous les mathématiciens souhaitent et tentent de défendre l'idée que démontrer des résultats difficiles est important et très utile. Bien sûr aussi, personne ne conteste que les théories abstraites, les résultats complexes ou très longs à démontrer sont souvent d'une grande beauté et constituent des accomplissements humains remarquables. De même, personne ne met en doute que la compréhension profonde du monde physique ou mathématique nécessite des concepts et des théories qui peuvent être d'une grande abstraction et vraiment très difficiles. On disait à un moment (ce qui est sans doute exagéré) que seul Einstein comprenait la théorie de la relativité, dont l'utilité est incontestable.

Ce dont il s'agit ici c'est seulement la question de savoir si les résultats difficiles parce que longs à démontrer sont utiles, sans prendre en compte la difficulté de la compréhension, qui est un autre problème (chacun sait d'ailleurs que certains résultats de démonstration simple sont difficiles à comprendre).

Il faut reconnaître que les résultats incontestablement difficiles n'ont que peu d'applications concrètes précises. Inversement, les théorèmes les plus utiles des mathématiques semblent être tous assez simples à prouver. Citons quelques exemples confirmant cette remarque, que le mathématicien J. Hartmanis a récemment développée.

FACILE ET TRÈS UTILE, OU DIFFICILE MAIS INUTILE?

Rares sont ceux qui prétendent qu'on trouvera une application concrète au théorème de Fermat (il n'existe pas de solution entière de l'équation $x^n + y^n = z^n$, pour n supérieur à 2), dont on chercha la démonstration pendant des siècles avant de la trouver, il y a six ans, à l'aide d'un raisonnement d'une extrême difficulté, à la fois long et faisant usage de concepts d'une grande abstraction. Aujourd'hui le théorème de Fermat est l'exemple type d'un résultat mathématique difficile, mais sans utilité concrète.

Parmi les résultats difficiles des mathématiques, il y a le fameux théorème de raréfaction des nombres premiers, qui indique que la proportion de nombres premiers parmi les entiers proches de n est environ $1/\ln(n)$. Longtemps recherchée, la preuve de ce théorème fut découverte en 1896 par Jacques Hadamard et Charles de La Vallée-Poussin. Cette preuve, longue et complexe, a été très soigneusement étudiée. Des variantes évitant le recours aux concepts abstraits, dont il semblait étrange que la preuve fasse usage, ont été mises au point, mais ces variantes élémentaires, dans leurs concepts, sont toujours longues et complexes. On peut donc dire, sans risque de se tromper, que ce résultat fait bien partie de la classe des résultats complexes à démontrer. Pourtant son utilité pratique semble réduite, et je crois qu'aucun commerçant, assureur, chimiste ou physicien ne trouvera jamais la moindre utilité à ce théorème : même s'il aide à la conception de certains algorithmes, il n'est jamais utile pour en garantir le bon fonctionnement.

Les résultats d'arithmétique qui sont les plus utiles, par exemple en cryptographie, sont tous d'une relative simplicité et, par exemple, les résultats qui justifient l'algorithme *RSA* (voir *La cryptographie RSA vingt ans après*, *Pour la*

3. Les théorèmes mathématiques utiles sont faciles à démontrer

On a constaté que les résultats mathématiques les plus utiles sont souvent relativement simples à démontrer, ce qui n'empêche pas qu'ils peuvent passer inaperçus durant des siècles. Le cas le plus étonnant est celui de la règle de calcul de Karatsuba, qui permet de réaliser des multiplications entre grands nombres plus rapidement que la méthode classique. Cette règle s'écrit :

$$(a + b \times 10^k)\,(c + d \times 10^k) = ac - [(a - b)\,(c - d) - ac - bd] \times 10^k + bd \times 10^{2k}$$

On peut la démontrer en classe de troisième. Cette identité, lorsqu'on multiplie deux entiers de longueur 2k, ramène le calcul à 3 multiplications entre entiers de taille k, ce qui fait gagner 25 pour cent du temps de calcul par rapport à l'identité classique à la base de la méthode usuelle :

$$(a + b \times 10^k)\,(c + d \times 10^k) = ac + (ad + bc) \times 10^k + bd \times 10^{2k}$$

Les additions sont plus nombreuses dans la formule de Karatsuba, mais elles sont d'un coût négligeable à côté des multiplications.

Directement sous cette forme ou sous des formes un peu plus élaborées (mais toujours faciles à démontrer), l'identité de Karatsuba est l'un des résultats le plus concrètement utiles des mathématiques, car de nombreux logiciels de calcul en font usage. Or elle est à la portée d'un élève de troisième...