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.