Jean-Michel Thiriet

Mathématiques et philosophie

JEAN-PAUL DELAHAYE

Quelles leçons philosophiques peut-on tirer des mathématiques? Les résultats difficiles à démontrer mathématiquement sont-ils utiles?

Les rapports entre science et philosophie sont ambigus. La philosophie adopte souvent une attitude normalisatrice envers la science, fixant les critères de ce qui est «scientifique» : le philosophe se propose d'aider la science en lui donnant des conseils.

La philosophie a pu rendre d'authentiques services à la science, et de grands savants comme Albert Einstein, Kurt Gödel, Max Planck ou Jacques Monod ont accordé de l'importance à la pensée philosophique qui les a aidés à formuler et à défendre les audacieuses théories qu'ils proposaient.

Hélas, trop souvent, les conceptions avancées par la philosophie pour rendre compte de la science ont freiné ou retardé les nouveautés plutôt qu'elles ne les ont favorisées. Lors des développements de la théorie de l'évolution, de la théorie de la relativité, de la mécanique quantique et de la logique mathématique, la philosophie a constitué un obstacle plus qu'elle n'a été une aide à la découverte.

Cette affirmation provocante nécessiterait de longues analyses pour être pleinement justifiée. Évoquons simplement Henri Bergson, qui, au nom d'une certaine intuition du temps s'opposa à la théorie de la relativité et se mit dans l'impossibilité de la comprendre. Pensons aussi aux conceptions *a priori* de ce que sont les mathématiques : Henri Poincaré et d'autres refusèrent les progrès de la logique mathématique – en particulier, de la théorie des ensembles, aujourd'hui universellement adoptée et dont aucun mathématicien ne peut se passer.

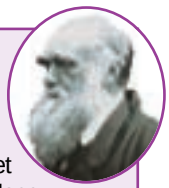
Pensons encore aux difficultés rencontrées par la théorie de l'évolution, au XIX^{e} siècle un peu partout, puis au XX^{e} siècle dans les pays communistes (dans l'affaire Lyssenko, c'est au nom d'une science prolétarienne fondée sur un matérialisme dialectique qu'on condamna la génétique moderne). Aujourd'hui encore, aux États-Unis, des idées philosophiques fausses sur la vie interdisent à la pensée scientifique de faire valoir ses vues et en entravent la diffusion.

Rappelons aussi que la conception de l'espace que défendait Kant est incompatible avec celle aujourd'hui universellement admise en physique, où l'on considère que la nature de la géométrie (euclidienne, hyperbolique ou sphérique) doit se déterminer par l'observation et l'expérimentation, et non par la simple analyse *a priori* des données immédiates de la raison.

La vérité est que la science enrichit la philosophie et la renouvelle, plus que l'inverse.

Ce constat, que certains philosophes acceptent presque (voir, par exemple, *La philosophie du non*, de Gaston Bachelard), fait apparaître la philosophie comme une entrave à la science, en même temps qu'elle rend inacceptables les prétentions de certains philosophes à dire aux chercheurs comment ils doivent travailler.

1. Science et philosophie

La science fait de la philosophie en remettant en cause les conceptions du sens commun. La philosophie ne peut se permettre de telles remises en cause, car son support concret est limité, ce qui nuit à sa force de persuasion et lui interdit une audace que la science est, quant à elle, contrainte de mettre en œuvre pour franchir les obstacles qu'elle rencontre. Ces audaces de la science constituent des avancées dont les conséquences philosophiques sont parfois importantes.

Voici quatre exemples de champs philosophiques qui ont été bouleversés par des progrès scientifiques :

– la conception de la vie et de l'homme, par la théorie Darwinienne;
– la conception du temps et de l'espace, par la théorie de la relativité ;
– la conception du déterminisme et des objets physiques, par la mécanique quantique ;
– la conception du raisonnement, de ses propriétés et de ses limitations, la conception du cerveau et de l'intelligence, par les avancées de la logique mathématique.


Bachelard avait perçu cette importance philosophique de la science : «Les progrès de la pensée scientifique contemporaine ont déterminé des transformations dans les principes mêmes de la connaissance.»

De la philosophie aux mathématiques

En mathématiques, en logique et en théorie de la calculabilité, des problèmes considérés comme philosophiques deviennent, à la suite d'un progrès scientifique, des problèmes techniques – en l'occurrence des problèmes mathématiques – dont les solutions (parfois inattendues) sont riches en contenus philosophiques ; l'impression qui se dégage est que la science fait de la philosophie et s'y substitue.

Parmi les avancées incontestables des mathématiques sur des sujets classés autrefois «purement philosophiques», il y a, bien sûr, celles concernant l'infini. Envisageant celui-ci comme un domaine réservé des philosophes ou même des théologiens, les mathématiciens ont réussi en plusieurs étapes (géométrie, théorie des nombres, calcul infinitésimal, théorie

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...

Science, février 2000) sont élémentaires, comparés à ceux nécessaires au théorème de raréfaction des nombres premiers. Relevons en passant un paradoxe : les résultats pour le *RSA,* bien plus simples et utiles que le théorème de raréfaction des nombres premiers, ont pourtant été formulés et démontrés bien après : ce qui était difficile, ce n'était pas démontrer de le résultat clef du *RSA*, mais de le découvrir et d'en comprendre l'intérêt.

La règle de calcul de Karatsuba est exactement dans la même situation, mais d'une façon plus nette encore. Elle permet des multiplications rapides de grands nombres, et c'est l'un des résultats les plus utiles de toutes les mathématiques (à chaque seconde qui passe, elle est utilisée par des milliers d'ordinateurs). Pourtant cette règle est véritablement facile à prouver.

Inversement, de nombreux autres grands résultats mathématiques (classification des groupes simples, démonstration de la transcendance de π, théorèmes de Gödel, etc.), et dont les démonstrations sont longues, semblent d'une utilité pratique nulle.

De même, les grandes conjectures indémontrées (dont on peut penser qu'elles sont indémontrées parce qu'elles n'ont pas de démonstrations simples) ne paraissent pas avoir d'applications potentielles. Si l'on réussissait à établir qu'il y a une infinité de nombres premiers jumeaux (conjecture des nombres premiers jumeaux), ou que tout nombre pair est somme de deux nombres premiers (conjecture de Goldbach), ou que l'algorithme de Syracuse conduit toujours à 1 (conjecture de Syracuse), rien de concret n'en résulterait, aucune *start-up* n'en sortirait et, abstraction faite des récompenses offertes par des mécènes sensibles aux mystères des mathématiques et des positions universitaires auxquelles pourront prétendre les génies qui résoudront ces problèmes, ce sont de purs défis sans conséquences économiques ou matérielles attendues.

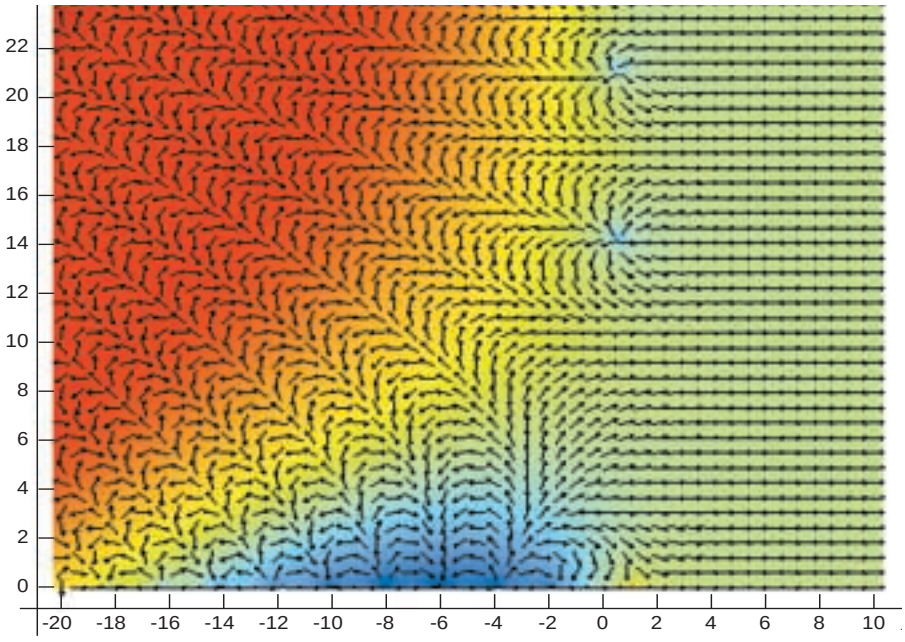
Les réflexions menées sur la célèbre conjecture *P* = *NP* (qui pourtant porte sur une question d'efficacité d'algorithmes) ont conduit le mathématicien J. Hartmanis à croire que sa solution (si on la trouve) ne changera concrètement pas grand-chose à la situation de l'informatique. Là encore, et même en informatique, on croit découvrir la confirmation que ce qui est difficile à prouver ne peut pas être concrètement utile.

Cette constatation ne doit pas nous décourager de faire des mathématiques, mais au contraire doit nous rassurer : si ce qui est utile est toujours assez facile à démontrer, c'est une raison de plus pour faire des mathématiques qui deviennent, pour ce qui est applicable, une science à la portée du plus grand nombre.

LA LOI DE L'INUTILITÉ DES PREUVES COMPLEXES

Les résultats mathématiques utiles semblent donc toujours simples, ou – ce qui revient au même – ce qui est mathématiquement complexe à démontrer apparaît toujours inutile sur le plan concret. Peut-on établir de telles affirmations générales et en apparence philosophiques? Oui, et c'est ce que viennent de faire Vladik Kreinovich et Luc Longpré, deux chercheurs de la théorie de la complexité. Ils ont prouvé que, si un résultat est potentiellement utile, alors il n'est pas possible qu'il possède une preuve complexe.

Le résultat technique est impossible à expliquer dans tous ses détails, mais



4. La conjecture de Riemann est-elle utile ?

Le théorème suivant est dû à G. Miller et E. Bach :

Si l'hypothèse de Riemann généralisée (une conjecture liée à la répartition des nombres premiers, qui stipule que les zéros de cette fonction, représentée ci-dessus, sont sur la droite d'abscisse 1/2) est vraie et si pour tout entier *a* entre 1 et $2.\ln^2(n)$ le nombre *n* est *a-fortement-probablement-premier*, alors, *n* est premier.

(Le nombre *n* est *a-fortement-probablement premier* si, après avoir écrit $n - 1 = 2^r q$ avec *q* impair, on constate que $a^q = 1 \bmod n$ ou que $a^{q\,2^i} = -1 \bmod n$ pour un entier $i = 0,1, ..., r - 1$.)

Considérons alors l'algorithme suivant :

Algorithme de Miller et Bach

• Pour tout $a = 2, 3,$ jusqu'à $2.\ln^2 (n)$, tester si *n* est *a-fortement-probablement premier ;*

• Dès que la réponse est non, répondre : *n* est composé ;

• Si la réponse a toujours été oui, répondre : *n* est premier.

Le résultat de Miller et Bach signifie que, si l'hypothèse de Riemann généralisée est vraie, cet algorithme ne se trompe jamais. Cet algorithme fonctionne en temps polynomial c'est-à-dire rapidement. Nous avons donc un algorithme rapide pour tester la primalité des nombres entiers (ce qui est incontestablement utile), mais la garantie de son bon fonctionnement n'est pas assurée, car l'hypothèse de Riemann généralisée reste non démontrée. Il semble donc que l'hypothèse de Riemann généralisée est un résultat à la fois difficile et utile concrètement : sa démonstration garantirait que l'algorithme de Miller et Bach fonctionne toujours.

Un théorème récent de Vladik Kreinovich et Luc Longpré indique que, malgré cette situation, l'hypothèse de Riemann généralisée n'est pas vraiment utile, car, en pratique, sans l'hypothèse de Riemann, on montre que, sauf pour des cas très rares, l'algorithme de Miller et Bach fonctionne correctement.

Leur théorème, dont le sens est plus général, signifie que, si un résultat ne possède que des démonstrations complexes, alors il ne peut être concrètement utile.

5. La loi de l'inutilité des preuves complexes

Vladik Kreinovich et Luc Longpré ont prouvé, en utilisant les concepts et méthodes de la théorie de la complexité, que :
– Si un résultat est potentiellement utile, alors il n'est pas possible qu'il possède une preuve complexe.
Leur travail a comporté plusieurs étapes.
– Formulation d'une définition mathématique de la notion de résultat potentiellement utile. Selon eux, un résultat est utile s'il permet de prouver le bon fonctionnement d'un algorithme et qu'on ne peut pas substituer à cet algorithme un algorithme probabiliste (c'est-à-dire fonctionnant avec un risque d'erreur aussi petit qu'on le souhaite) dont le bon fonctionnement soit simple à établir.
– Formulation d'une définition mathématique de la notion de preuve complexe. Leur définition prend en compte à la fois le nombre d'étapes élémentaires de raisonnement de la preuve et les possibilités de simplification dues à d'éventuelles parties répétitives. Pour eux, une preuve complexe est une preuve longue, et qui le reste même après exploitation des parties répétitives.
– Utilisation de la théorie de la complexité pour prouver leur affirmation.
Le résultat de Kreinovich et Longpré est un exemple récent provenant de la théorie de la complexité de résultats mathématiques ayant un contenu philosophique intéressant et inattendu. Il est probable qu'il déplaira aux mathématiciens qui aiment justifier leurs travaux, même les plus difficiles, en évoquant de possibles applications futures.

tentons tout de même de le présenter, il en vaut la peine.

Les deux chercheurs, pour arriver à leur résultat, ont d'abord donné une définition mathématique de la notion de résultat potentiellement utile.

Pour eux, un tel résultat est un énoncé *S*, qui permet d'établir une formule du type «pour tout *x*, *P(x)*», où *P(x)* est facilement vérifiable (par exemple, une formule du type «si la somme des chiffres de *x* est un multiple de 9, alors *x* est un multiple de 9»).

Leur définition est justifiée, car ce sont les résultats de ce type qui assurent que les méthodes algorithmiques fonctionnent correctement : algorithmes de codage, algorithmes de recherche dans une base de données, algorithmes de tri de données, algorithmes de calcul numérique, algorithmes de simulation, etc.

Ensuite les deux chercheurs définissent une preuve complexe d'une manière fine et subtile *(voir la figure 5)*.

Leur résultat, formulé avec plus de précision, est : si *S* n'a que des preuves complexes et permet de montrer que «pour tout *x P(x)*», alors pour la quasi-totalité des données de taille raisonnable (les seules qu'on rencontre en pratique) *P(x)* est vrai indépendamment de *S*. En quelques mots : si *S* est complexe, et que $S => $ (pour tout *x P(x)*) alors, sauf de manière exceptionnelle, on n'a pas besoin de *S* pour savoir que *P(x)* est vrai.

En très court, si *S* est complexe, alors ce n'est pas un résultat potentiellement utile.

Ce résultat s'applique en particulier à la conjecture de Riemann (un résultat qui concerne la répartition des nombres premiers et qui est considéré comme l'énoncé mathématique irrésolu le plus recherché des mathématiques aujourd'hui). Il a été prouvé par G. Miller et E. Bach que, si une forme généralisée de l'hypothèse de Riemann était vraie, alors il existait un algorithme efficace (l'algorithme de Miller et Bach) pour tester la primalité des nombres entiers en temps polynomial, c'est-à-dire efficacement. Cette situation a conduit de nombreux mathématiciens à croire que les recherches sur l'hypothèse de Riemann étaient utiles, même dans une optique d'applications pratiques.

Est-il vraiment utile de démontrer Riemann?

La situation créée par l'algorithme de Miller est qu'on dispose sans doute d'un algorithme efficace de test de primalité dont le bon fonctionnement dépend de la vérité de l'hypothèse de Riemann généralisée. Ce qu'énonce le résultat de Vladik Kreinovich et Luc Longpré est : si vraiment l'hypothèse de Riemann généralisée ne possède pas de preuve simple, alors l'algorithme de Miller pour des entiers de tailles raisonnables fonctionne correctement pour la quasi-totalité des cas qu'on peut lui soumettre. On n'a donc pas besoin en pratique de la démonstration de l'hypothèse de Riemann généralisée si l'on désire utiliser cet algorithme.

Cette inutilité pratique de l'hypothèse de Riemann dans le cas des tests de primalité est d'ailleurs corroborée par l'usage informatique réel : dans les applications cryptographiques où l'utilisation des nombres premiers est intensive, on se sert le plus souvent des méthodes probabilistes de test de primalité, c'est-à-dire de méthodes dont le bon fonctionnement est justifié par un raisonnement relativement simple, mais qui ne donnent un résultat que d'une manière probabiliste, autrement dit avec un risque, jugé négligeable, d'erreur.

Tout n'est pas terminé

Notons, pour l'amusement, que le résultat de Vladik Kreinovich et Luc Longpré possède une démonstration assez courte (environ une page) : il n'est donc pas impossible, d'après ce qu'il nous apprend, qu'il soit un résultat concrètement utile !

Notons aussi qu'en toute rigueur, malgré les longues recherches faites à son sujet, il n'est pas logiquement exclu que la conjecture de Riemann possède une démonstration simple. Si c'est le cas, l'hypothèse de Riemann pourrait être pratiquement utile. Nous devons continuer à en rechercher la preuve, même si l'intérêt mathématique pur ne nous semble pas une raison suffisante de nous y intéresser.

Précisons que, même si, après une traduction mathématique sous une certaine forme particulière, on a réussi à établir que le difficile est inutile, il ne faut pas donner une importance excessive au résultat de Vladik Kreinovich et Luc Longpré qui fixent, dans leurs définitions, le sens des mots peut-être un peu rapidement.

Dans le cœur de tous les mathématiciens est inscrite la conviction que plus c'est difficile, plus c'est beau et important, et donc utile au moins par l'approfondissement et une meilleure vision que cela procure à notre perception du monde des entités abstraites. «Le but unique de la science, c'est l'honneur de l'esprit humain», écrivait le mathématicien Jacobi dans une lettre adressée à son collègue Legendre en 1830. Il est peu vraisemblable que le formalisme mathématique s'empare un jour de cette vérité philosophique-là !

G. Bachelard, *La philosophie du non*, Presses Universitaires de France, Paris, 1940.

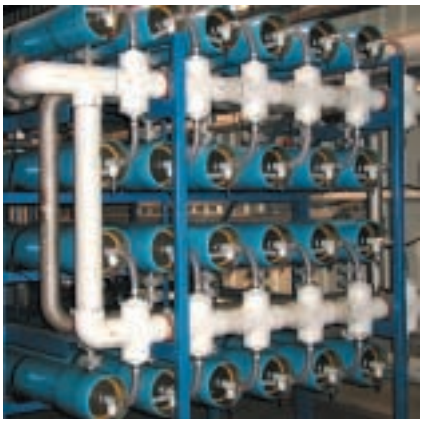
W. H. Zurek, *Algorithmic Randomness and Physical Entropy*, in *Physical Review A*, n° 8, vol. 40, pp. 4731-4751, 1989.

***The Philosophy of Mathematics*, sous la direction de W. H. Hart, Oxford University Press, 1996.**

Ming Li et Paul Vitanyi, *An Introduction to Kolmogorov Complexity and Its Applications*, Springer-Verlag, New York, 1997.

J.-P. Delahaye, *Information, complexité et hasard*, Hermès, Paris, 1999.

V. Kreinovich et L. Longpré, *How Important Is Theory for Practical Problems?*, in *Bulletin of the European Association for Theoretical Computer Science* (EATCS), n° 71, pp. 160-164, 2000.



Vivendi

Le droit au mélange

BERNARD CABANE • SYLVIE HÉNON

L'eau se déplace à travers les membranes par osmose. Ce phénomène permet de détruire les bactéries par déshydratation ou, en l'inversant, de dessaler l'eau de mer.

Aux temps héroïques de l'exploration pétrolière des régions tropicales, on protégeait de la gangrène les plaies infectées en les recouvrant de sucre, traitement encore utilisé aujourd'hui à l'hôpital pour les plaies profondes. Le sucre préserve aussi les confitures des proliférations bactériennes et le sel conserve viandes et poissons. Comment sel et sucre empêchent-ils la croissance bactérienne ? Par le phénomène d'osmose, important dans les mécanismes biologiques et industriels.

La plupart des bactéries sont des organismes unicellulaires. Remplies d'une solution aqueuse d'ions, d'acides aminés et de protéines, elles ne sont protégées de l'extérieur que par une membrane constituée d'une mince couche de lipides et de protéines, perméable à l'eau. Lorsque les bactéries sont plongées dans un milieu aqueux, l'eau entre et sort de la cellule à travers la membrane.

Plongeons une bactérie dans du sucre : comme il y a beaucoup plus de molécules de sucre à l'extérieur de la bactérie que de molécules à l'intérieur, la quasi totalité de l'eau traverse la membrane afin de diluer le sucre. La bactérie se déshydrate et meurt. En effet, selon le second principe de la thermodynamique, la situation la plus favorable est celle où les molécules d'eau se mélangent équitablement avec toutes les autres molécules (les molécules internes à la bactérie et le sucre externe).

Inversement, le contact avec l'eau pure est dangereux pour les cellules de notre corps, parce qu'elles contiennent des liquides salés. Dans notre corps, elles sont en contact avec les fluides physiologiques, salés eux aussi. Si nous introduisons de l'eau pure dans un de ces fluides, nous déclenchons un transfert d'eau vers l'intérieur des cellules. Par exemple si, pour nettoyer nos yeux ou nos lentilles de contact, nous utilisons de l'eau pure au lieu d'une solution saline, en vertu de son «droit au mélange», l'eau passe dans les cellules de la cornée, ce qui crée un œdème.

L'ÉQUILIBRE OSMOTIQUE

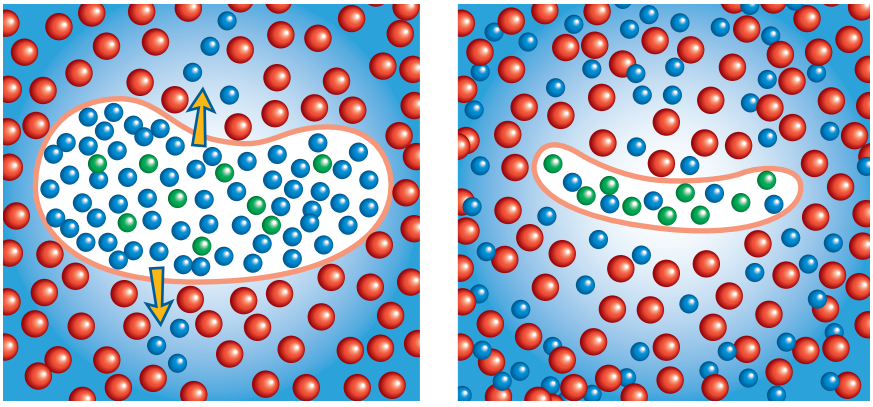
Pour éviter que nos cellules ne gonflent ou ne dégonflent par des transferts d'eau intempestifs, les mélanges de l'eau avec les sels, à l'intérieur et à l'extérieur des cellules, doivent être équivalents. Comme le métabolisme des cellules produit de l'eau, une régulation est nécessaire afin que notre teneur en eau n'augmente pas : cette régulation est assurée par les reins.

Si l'eau passe facilement à travers les membranes des cellules, le passage des sels et des molécules plus grosses est restreint. Ainsi, l'important pour l'équilibre osmotique n'est pas que les fluides interne et externe contiennent les mêmes composés en solution, mais que la proportion d'eau, en nombre de molécules, soit égale des deux côtés de la membrane. Par exemple, l'équilibre osmotique doit être assuré pour le sérum utilisé lors des perfusions, afin que les globules rouges du sang n'éclatent pas : on utilise des solutions salées, ou des solutions de glucose, qui nourrissent l'organisme tout en assurant son équilibre en eau.

Loin du monde médical, la culture des tomates dans le désert illustre le maintien de l'équilibre osmotique ; comme l'eau douce y est rare, on arrose les plantations avec des saumures. La forte concentration en sels à l'extérieur des cellules végétales pourrait entraîner la sortie de l'eau cellulaire : afin d'éviter la déshydratation, les cellules végétales sécrètent une grande quantité de sucres ou d'acides aminés qui équilibrent les concentrations en eau à l'intérieur et à l'extérieur des cellules. Les tomates ainsi cultivées dans le désert sont plus sucrées que celles qui sont alimentées avec de l'eau douce.

Les cellules végétales diffèrent toutefois des bactéries ou de nos propres cellules car leur concentration interne en espèces dissoutes reste supérieure à celle du milieu extérieur : l'eau externe devrait alors entrer dans les cellules et les faire gonfler, mais la pression à l'intérieur de la cellule, supérieure à la pression extérieure, l'en empêche. L'application d'une pression s'oppose ainsi à l'osmose.

Peut-on reproduire ce phénomène à grande échelle ? Oui, à l'aide de membranes qui laissent passer l'eau, mais ni le sel, ni le sucre. Imaginons un récipient empli d'eau pure divisé par une membrane en deux compartiments. Ajoutons du sucre dans un compartiment. L'eau se déplace alors vers le compartiment sucré toujours en vertu du «droit au mélange».



Dessins de Bruno Vacaro

Quand une bactérie est plongée dans une solution sucrée, la proportion d'eau à l'extérieur est inférieure à la proportion à l'intérieur *(à gauche)* : les molécules d'eau *(boules bleues)* traversent la paroi cellulaire jusqu'à rétablir l'équilibre. La bactérie se déshydrate et meurt *(à droite)*.