BIBLIOGRAPHIE

M. Rix, **The Golden Age of Botanical Art,** Univ. of Chicago Press, 2013.

T. Robinson, **William Roxburgh : the Founding Father of Indian Botany,** Phillimore and Co. / Royal Botanic Garden, 2008.

H. Noltie, **Indian Botanical Drawings, 1793-1868, from the Royal Botanic Garden,** Royal Botanic Garden, 1999.

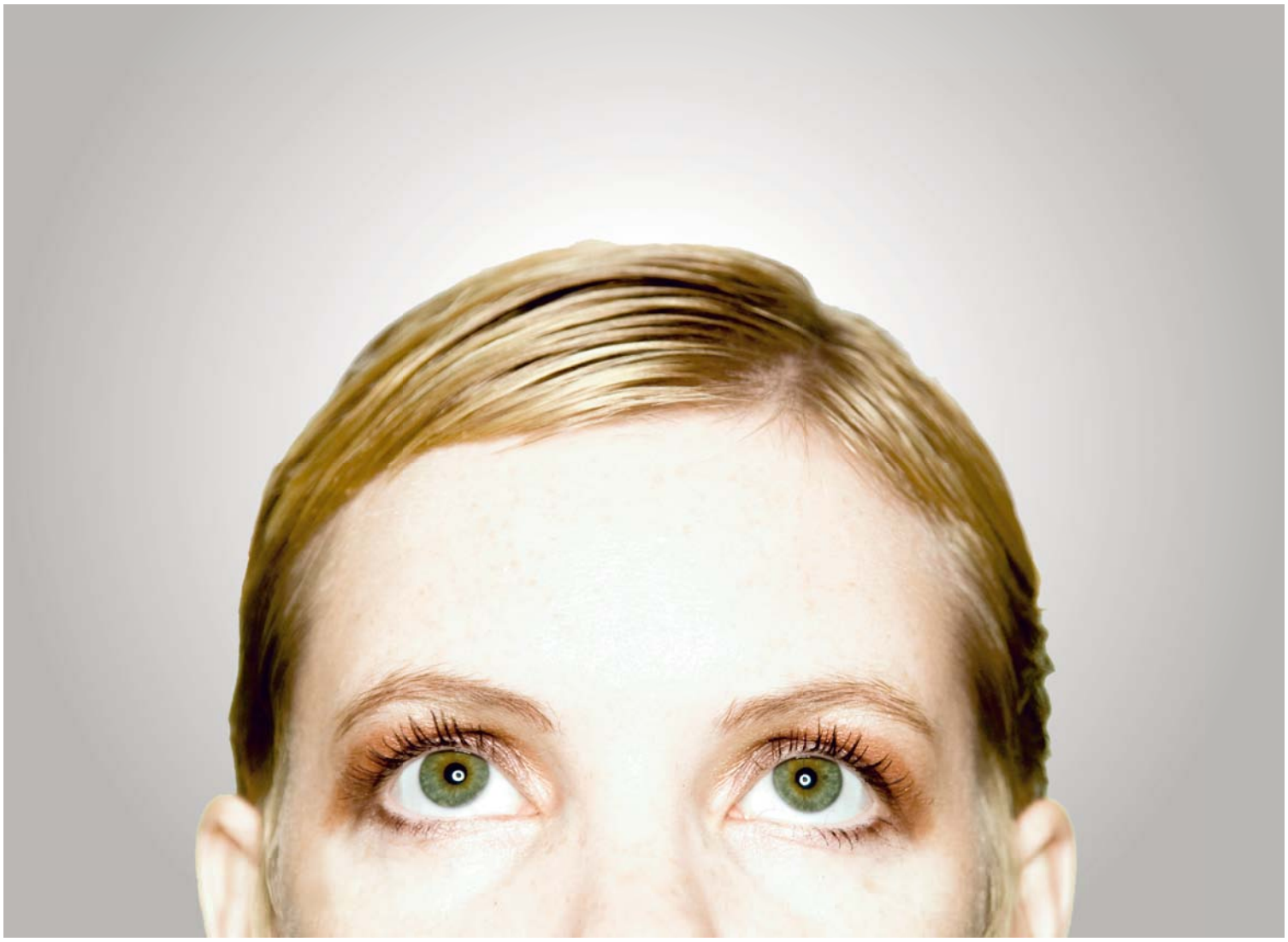
rapportées des campagnes napoléoniennes, et les nombreux présents que lui font les savants de retour d'expédition. Peu à peu, sous la supervision des botanistes Étienne Ventenat, puis Aimé Bonpland, le jardin de la Malmaison devient incontournable pour les botanistes d'Europe. En 1810, au sommet des guerres napoléoniennes, un arrangement spécial des amirautés britannique et française autorise l'horticulteur anglais John Kennedy à franchir le blocus anglais des ports français pour envoyer à Joséphine diverses plantes, dont le rosier thé chinois *Hume's Blush Tea-Scented China*.

En 1814, Bonpland, qui répertorie les plantes cultivées dans les jardins de Joséphine, se rend à Londres pour y comparer les relevés du peintre de Joséphine, Pierre-Joseph Redouté, aux dessins de la Compagnie des Indes. Il y retrouve la plupart des plantes chinoises cultivées à la Malmaison et à Navarre. La précision est telle qu'il perçoit même de subtiles différences entre les plantes d'origine et celles cultivées en France depuis plusieurs années, telle la pivoine moutan, arrivée en 1803 à la Malmaison.

Le travail des botanistes, des collectionneurs et des innombrables artistes anonymes de Chine et d'Inde qui ont peint les plantes recensées a contribué à établir de précieuses archives sur les plantes sauvages et cultivées de ces pays. La précision du détail et la fusion des styles artistiques orientaux et occidentaux confèrent à ces images un intérêt historique et archéologique remarquable. De telles collections nous rappellent l'origine de plantes désormais courantes partout dans le monde. Elles nous offrent aussi un plaisir intense : contempler l'art botanique dans sa plus belle expression. ■

AcademiaNet

La base de données qui rassemble toutes les femmes scientifiques de renommée internationale



AcademiaNet offre un service unique aux instituts de recherche, aux journalistes et aux organisateurs de conférences qui recherchent des femmes d'exception dont l'expérience et les capacités de management complètent les compétences et la culture scientifique.

AcademiaNet, base de données regroupant toutes les femmes scientifiques d'exception, offre:

- Le profil des femmes scientifiques les plus qualifiées dans chaque discipline – et distinguées par des organisations de scientifiques ou des associations d'industriels renommées
- Des moteurs de recherche adaptés à des requêtes par discipline ou par domaine d'expertise
- Des reportages réguliers sur le thème »Women in Science«

Robert Bosch Stiftung

Spektrum DER WISSENSCHAFT

nature

Une initiative de la Fondation Robert Bosch en association avec Spektrum der Wissenschaft et Nature Publishing Group

www.academia-net.org

LOGIQUE & CALCUL

Indécidables utiles et inutiles

Les affirmations sur la complexité sont souvent indécidables. D'où l'idée d'en utiliser comme axiomes pour limiter la désagréable incomplétude de toute théorie mathématique, découverte par Kurt Gödel il y a 80 ans.

Jean-Paul DELAHAYE

Ce qui est simple peut se dire en peu de mots et donc ce qui est complexe en demande beaucoup. Le hasard ne pouvant pas se résumer, il est incompressible et fournit les objets les plus complexes. Ces idées élémentaires servent de fondement à la « théorie algorithmique de l'information » ou théorie de la « complexité de Kolmogorov ». Créée il y a 50 ans par le mathématicien russe Andreï Kolmogorov et quelques autres théoriciens, son importance se confirme d'année en année : on l'utilise en physique pour définir l'entropie, en biologie pour concevoir des algorithmes de comparaison de séquences, en psychologie pour mesurer la capacité des humains à reconnaître et simuler le hasard, etc.

En logique mathématique et en philosophie des sciences, les multiples facettes de cette théorie définissent ce qu'est une suite infinie aléatoire ou une théorie complexe *(voir la rubrique du numéro de mai 2013 : « Qu'est-ce qu'un objet complexe ? »)*. Nous verrons ici que des axiomes portant sur le hasard et la complexité enrichissent une théorie mathématique et augmentent son pouvoir de démonstration. Cinq mathématiciens d'origines variées, Laurent Bienvenu et Antoine Taveneaux, de l'Université Paris 7, Andreï Romashchenko et Alexander Shen, aujourd'hui à l'Université de Montpellier, et Stijn Vemeeren, de l'Université de Leeds en Grande-Bretagne, ont dans un article récent fait avancer notre compréhension du hasard et du rôle logique de la complexité.

1. La complexité ne peut être calculée

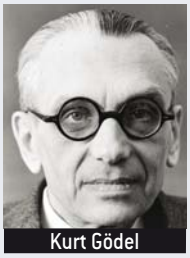
La complexité de Kolmogorov d'une suite finie s de 0 et de 1 est la taille du plus court programme écrit dans un langage assez puissant qui produit s. On la note $K(s)$. Une suite d'un million de 0 a une faible complexité de Kolmogorov, car il existe des programmes courts qui l'engendrent (par exemple : « Pour i de 1 à 1 000 000, print '0' »). C'est vrai aussi de la suite composée d'un million de chiffres de π ou de e, car, grâce aux nombreuses séries qui donnent π ou e, on sait écrire des programmes courts qui calculent un million de chiffres de π ou de e. Il existe un programme de moins de 200 caractères (J. Gibbons, *Amer. Math. Monthly*, vol. 113, pp. 318-328, 2006) qui réussit l'exploit de calculer indéfiniment des chiffres de π. Bien sûr, il les calcule de plus en plus lentement, mais il ne s'arrête que lorsque toute la mémoire de la machine a été utilisée. Il ne s'arrêterait pas si l'on ajoutait progressivement de la mémoire à la machine.

Il est assez facile de montrer qu'il existe des suites s de complexité $K(s)$ aussi grande qu'on le souhaite ; mais Gregory Chaitin a établi que si l'on se donne une théorie formalisée T, elle ne peut démontrer qu'un nombre fini de théorèmes de la forme « $K(s) = n$ » ou « $K(s) > n$ ». Cela signifie que, sauf pour un nombre fini de suites s, la théorie T ignore tout de la complexité de s : la complexité est, sauf rares exceptions, indécidable. La situation est presque paradoxale : une théorie T (par exemple l'arithmétique de Peano, formalisation la plus naturelle des modes de raisonnements en arithmétique) prouve qu'il existe des suites de grande complexité, mais n'en connaît aucune. Cette forme particulière de l'incomplétude est remarquable, car contrairement aux formules dont Kurt Gödel a démontré l'indécidabilité, les formules concernant la complexité de Kolmogorov sont immédiatement compréhensibles.


Andreï Kolmogorov


Gregory Chaitin


Giuseppe Peano


Kurt Gödel

Avant d'expliquer le détail de leurs travaux rappelons que la complexité d'un objet numérique (une suite finie s de 0 et de 1) est, d'après Kolmogorov, la taille du plus court programme d'ordinateur qui engendre s. On note cette taille $K(s)$ (elle dépend peu du langage de programmation choisi). Une suite finie s de longueur n est considérée comme aléatoire si elle a une complexité de Kolmogorov proche de sa taille (par exemple supérieure à $n - c$ pour une constante c fixée). Une suite infinie s de 0 et de 1 est considérée aléatoire (on dit aléatoire au sens de Martin-Löf car ce mathématicien est à l'origine de la notion) si c'est le cas de tous les débuts de s : la suite $(s_0, s_1, ..., s_n, ...)$ est aléatoire si et seulement s'il existe un nombre c tel que $K(s_0, s_1, ..., s_n) > n - c$ pour tout entier n.

Comment compléter une théorie ?

Grâce aux célèbres résultats d'incomplétude de Kurt Gödel, nous savons depuis maintenant plus de 80 ans qu'une théorie mathématique formalisée (par exemple la théorie des ensembles) comporte inévitablement des trous : pour toute théorie formalisée T, il existe des énoncés E qualifiés d'indécidables, dont la théorie T n'est capable ni de démontrer qu'ils sont vrais, ni de démontrer qu'ils sont faux. Parmi ces « indécidables » sur lesquels une théorie T est incapable de se prononcer, figure l'affirmation que dans la théorie T, il n'existe pas de théorème qui énonce le contraire d'un autre. On désigne cette propriété par la « consistance » de T. Une idée vient alors naturellement à l'esprit : pourquoi ne pas ajouter aux axiomes de T l'affirmation de sa consistance, *cons*(T) ? On obtient ainsi une théorie plus puissante que T dont on a réduit l'incomplétude.

La théorie de la démonstration – un domaine de la logique mathématique – a étudié ce procédé de complétion qu'on applique éventuellement plusieurs fois : on ajoute l'affirmation de la consistance de T, ce qui donne une nouvelle théorie T', on recommence avec T', et ainsi de suite.

Dès 1939, Alan Turing a étudié ce thème qui était le sujet de sa thèse de doctorat à Princeton. Les résultats obtenus sont difficiles, car liés à la théorie des ordinaux (les nombres transfinis). Ils ont été complétés depuis, en particulier par Solomon Feferman, un élève de Gödel.

Ce domaine est malgré tout un peu décevant, car les énoncés qui affirment des propriétés de consistance sont peu pratiques pour démontrer des théorèmes mathématiques, ce qui a pour conséquence qu'il faut en ajouter beaucoup (en fait jusqu'à l'infini, puis recommencer encore et encore en utilisant la théorie des ordinaux) pour que cette méthode de complétion produise des conséquences intéressantes. En résumé, en procédant par l'ajout d'axiomes de consistance, on complète bien les théories mathématiques, mais les théories obtenues ne sont pas très commodes pour ce qui intéresse les mathématiciens et les résultats obtenus délicats à interpréter. Il fallait donc imaginer d'autres méthodes de complétion.

Le mathématicien américain Gregory Chaitin, qui formula en même temps et indépendamment de Kolmogorov la théorie algorithmique de l'information, a suggéré une voie alternative à celle des axiomes de consistance. Il a en effet démontré que les affirmations concernant la complexité de Kolmogorov des suites finies (et donc leur nature aléatoire ou non) sont souvent des indécidables de Gödel. Il a en fait établi le

2. Réduire l'incomplétude en ajoutant des axiomes

La complexité de Kolmogorov, la taille $K(s)$ du plus court programme donnant une suite s, est rarement petite. Les programmes sont des suites de 0 et de 1. Chaque programme produit une suite binaire s et certains programmes n'en produisent pas, car ils ne s'arrêtent jamais.

Le nombre de programmes de taille 99 est au plus 2^{99} (il y a 2^{99} suites différentes de 0 et de 1). Le nombre de suites s produites par les programmes de taille 99 est donc inférieur ou égal à 2^{99}. Le même raisonnement montre que les programmes de taille 1, 2, ..., 99 produisent au plus $2^1 + 2^2 + 2^3 + 2^4 + ... + 2^{99}$ suites binaires différentes. La somme de cette série géométrique est égale à $2^{100} - 1$. On en déduit que le nombre de suites s, de longueur 110 par exemple, produites par un programme de longueur inférieur à 100 est au plus 2^{100}. Cela signifie aussi que le nombre (2^{110}) de suites de longueur 110 ayant une complexité $K < 100$ est inférieur à 2^{100}. La proportion de suites de longueur 110 ayant une complexité $K < 100$ est inférieure à $2^{100}/2^{110} = 1/2^{10} = 1/1024$: moins d'une suite sur mille de longueur 110 a une complexité $K < 100$. Plus généralement, la proportion de suites de longueur n ayant une complexité $K < n - m$ est au plus $1/2^m$.

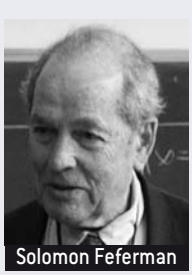
Comme il est facile d'écrire un programme de longueur proche de n qui produit une suite s de longueur n donnée (on prend le programme « PRINT s »), la complexité de Kolmogorov d'une suite de longueur n est, sauf rares exceptions, très proche de n.

Un axiome stipulant qu'une suite s de longueur n tirée au hasard a une complexité $K > n - m$ est très probablement vrai, en même temps qu'il est indécidable, car dès qu'une suite est longue on ne sait déterminer sa complexité de Kolmogorov *(voir l'encadré 1)*.

Cette façon d'ajouter comme axiomes des indécidables à une théorie T vient d'être étudiée.


Alan Turing


Per Martin-Löf


Solomon Feferman


Laurent Bienvenu

remarquable et étonnant théorème suivant : une théorie consistante donnée T ne peut démontrer qu'un nombre fini d'affirmations du type « $K(s) = n$ » ou du type « $K(s) > n$ ». Ainsi, au-delà d'un certain n_0 (qui dépend de la théorie T), tous les énoncés affirmant une complexité supérieure à n_0 sont des indécidables de la théorie T.

Éviter les indécidables

Toute théorie formalisée est donc gravement aveugle à la complexité, puisqu'elle ne sait pratiquement rien démontrer de la complexité des suites finies de 0 et de 1. Cela suggère, toujours pour éviter les indécidables, d'ajouter des axiomes de la forme « $K(s) = n$ » ou « $K(s) > n$ » pour des suites finies s et des entiers n choisis. Étudier la force axiomatique de la complexité et du hasard consiste donc à poser les questions « Est-ce que l'ajout de tels indécidables a des effets intéressants ? » et « Comment faire cela au mieux ? ». C'est exactement le sujet de l'article des chercheurs réunis autour de L. Bienvenu.

Insistons sur le fait que ces travaux, aussi abstraits qu'ils paraissent, renforcent notre compréhension philosophique et mathématique sur un sujet fondamental. On doit déjà beaucoup à la théorie algorithmique de l'information dans les progrès faits récemment concernant le hasard, car ce qu'elle montre va au-delà de la théorie des probabilités en établissant, ce qui était loin d'être évident, que les concepts de calculs, d'algorithmes et de programmes sont profondément liés à cette notion.

Les résultats obtenus par L. Bienvenu et ses collègues nous éclairent sur quatre points principaux.

1) Ajouter sans méthode des axiomes affirmant des propriétés presque certaines sur la complexité ne conduit pas à prouver des théorèmes nouveaux limitant l'incomplétude gödélienne, mais en revanche permet de raccourcir les démonstrations.

2) Ajouter comme axiomes des formules indiquant la complexité de séquences assez nombreuses du type « $K(s) = n$ » ou « $K(s) > n$ » supprime les indécidables de la forme « pour tout x : $P(x)$ » *(voir l'encadré 3 pour l'importance de telles formules)*. Cela constitue un renforcement considérable du pouvoir démonstratif de la théorie. L'affirmation « Tout nombre pair supérieur à 2 est somme de deux nombres premiers » (conjecture de Goldbach) est de la forme « Pour tout x : $P(x)$ » ; elle ne peut être indécidable dans une théorie complétée systématiquement par des axiomes concernant la complexité.

3) Tous les axiomes du type « $K(s) = n$ » n'ont pas la même force. Certains, assez rares, sont extrêmement puissants et rendent inutiles la plupart des autres.

4) Ajouter comme axiome qu'une séquence infinie s de 0 et de 1 est aléatoire au sens de Martin-Löf renforce la théorie, mais ne le fait jamais autant que la méthode précédente.

Parmi les 2^n suites de 0 et de 1 de longueur n (par exemple n = 100 000), on démontre qu'au plus une sur 1 024 ($= 2^{10}$) a une complexité de Kolmogorov inférieure à $n - 10$ (ici 99 990). Il n'y en a, au plus, qu'une sur un million (1 048 576 $= 2^{20}$ précisément) ayant une complexité inférieure à $n - 20$ (donc 99 980 pour notre exemple). L'énoncé général est : « Au plus une suite de longueur n sur 2^m a une complexité inférieure à $n - m$ » ; autrement dit, les suites peu complexes sont extrêmement rares *(voir l'encadré 2)*.

Si l'on choisit m = 100, que l'on tire uniformément une séquence s de 100 000 symboles 0 ou 1 (par exemple à l'aide d'une pièce de monnaie) et que l'on ajoute l'axiome « $K(s) > 99\,900$ » à une théorie T, alors sauf malchance extraordinaire (risque de $1/2^{100}$), on ajoute un indécidable vrai à la théorie T à laquelle on s'intéresse. Cela en accroît donc au moins un peu le pouvoir démonstratif : la théorie maintenant sait que $K(s) > 99\,900$.

On dispose ainsi d'une méthode de complétion qui, sauf au plus une fois sur 2^{100} (ce qu'on peut considérer comme totalement négligeable) améliore une théorie T en supprimant au moins un indécidable. La question est maintenant : avoir pris ce risque est-il utile, c'est-à-dire conduit-il à une théorie T' (comportant un axiome de plus) qui démontre des théorèmes nouveaux intéressants, que T était incapable de démontrer avant l'ajout ?

La réponse est négative pour l'essentiel. Cela résulte de la proposition suivante démontrée par le groupe des cinq chercheurs : si l'on ajoute un ou plusieurs axiomes du type envisagé en les choisissant au hasard (par exemple en tirant à pile ou face les suites s concernées) et en prenant un risque total inférieur à un seuil fixé ϵ (par exemple $1/2^{100}$), et si l'on ne considère que les théorèmes qui dans ce processus probabiliste de démonstration sont obtenus avec une probabilité supérieure à ϵ, alors les théorèmes qu'on découvre peuvent l'être sans ajout d'axiomes, autrement dit, pouvaient déjà l'être dans la théorie initiale.

Ajouter des axiomes peu risqués est inutile

Ajouter des informations presque certaines concernant la complexité n'est donc pas vraiment utile pour limiter l'incomplétude. En revanche, un second résultat sur ces processus de démonstration avec ajout aléatoire d'axiomes presque certains établit qu'on en tire un gain sur la taille des démonstrations : on n'a pas vraiment plus de théorèmes, mais les théorèmes de T sont maintenant obtenus par des démonstrations plus courtes.

La situation est analogue à celle déjà rencontrée en arithmétique à propos des tests de primalité probabilistes. Alors que démontrer sans accepter de prendre le moindre risque qu'un entier long (de 10 000 chiffres par exemple) est un nombre premier exige toujours un long calcul, on sait le faire rapidement si l'on accepte un risque d'erreur, même infinitésimal (par exemple inférieur à $1/2^{100}$). Ces tests probabilistes de primalité découverts dans les années 1980 sont d'une grande utilité en cryptographie.

Mis à part des gains sur la taille des démonstrations, ajouter des axiomes du type « $K(s) = n$ » ou « $K(s) > n$ » lorsque s est aléatoire n'est pas le bon moyen d'accroître le pouvoir de démonstration d'une théorie formalisée T. Qu'en est-il de l'ajout d'axiomes fournissant des informations précises sur la complexité, y compris concernant des suites finies s peu complexes ?

Cette fois, les résultats vont être positifs et très instructifs.

Le premier résultat dans cette direction indique ce que donne l'ajout, à une théorie T, de tous les axiomes concernant la complexité des suites finies : pour chaque suite finie s,

3. La classification des formules

En logique, on s'intéresse à la forme logique des affirmations mathématiques, ce qui conduit à une classification des formules. Chacun perçoit qu'en parcourant la liste suivante de formules, où chaque élément de la liste est comme un échelon, la difficulté de compréhension des affirmations mathématiques augmente.

Énoncé A : 2 + 11 = 13.

Énoncé B : Le carré de tout entier pair est aussi pair.

Énoncé C : Pour tout entier n donné, il existe un nombre entier $P > n$ qui est un nombre premier (autrement dit, il y a une infinité de nombres premiers).

Énoncé D : Pour tout entier k, il existe un entier n tel que pour tout entier $m > n$, on ait : $0 < 2^{1/m} - 1 < 1/k$ (autrement dit, la suite $2^{1/m}$ tend vers 1 quand m tend vers l'infini)

Énoncé E : Il existe un entier b et pour tout entier k, il existe un entier n tel que pour tout entier $m > n$: $b - 1/k < f(m) < b + 1/k$ (autrement dit, la suite $f(m)$ a une limite quand m tend vers l'infini et cette limite est un entier).

D'un énoncé au suivant, les formules contiennent de plus en plus de quantificateurs (« il existe », « pour tout ») et c'est ce qui rend leur compréhension plus difficile. Il y en a d'abord 0, puis 1, puis 2, puis 3, puis 4. Cette augmentation de difficulté est utilisée pour définir la hiérarchie arithmétique des formules.

Le premier niveau, noté Δ_0, ne contient que les affirmations arithmétiques immédiates à vérifier (même si parfois cela demande de la patience). D'autres exemples de formules Δ_0 sont « 1 048 576 est une puissance de 2 », « Il n'y a pas de nombres premiers entre 5 490 et 5 500 ». Pour chacune de ces affirmations, on peut entreprendre un calcul dont on sait évaluer la taille par avance et qui, achevé, indiquera si l'affirmation est vraie ou non.

Toutes les formules de Δ_0 vraies sont démontrables dans le système formel de l'arithmétique de Peano. En particulier, c'est le cas de toutes les affirmations vraies du type « n est un nombre premier ». De même, si une formule de Δ_0 est fausse (par exemple « 121 est un nombre premier »), l'arithmétique de Peano sait démontrer sa négation. Aucune des formules de Δ_0 n'est donc indécidable dans l'arithmétique de Peano (ou dans une théorie plus forte comme la théorie des ensembles).

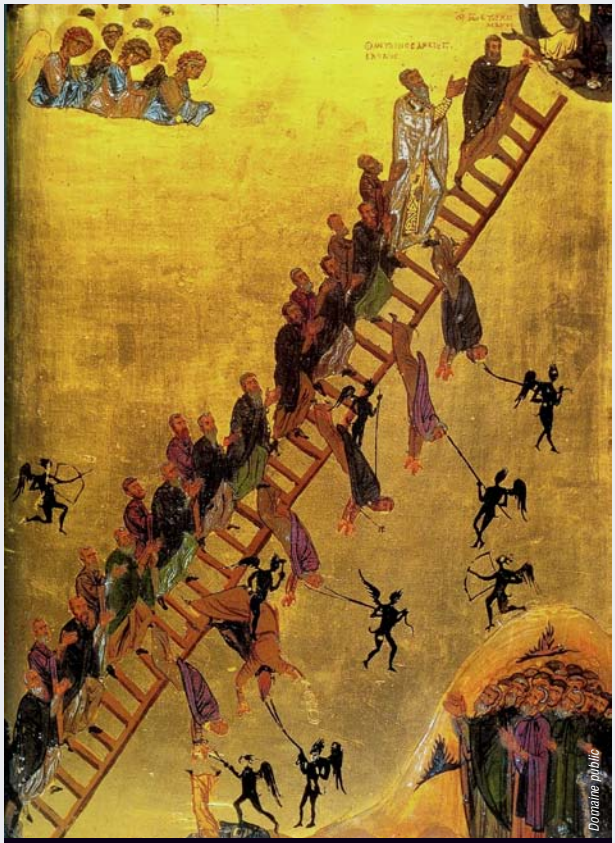
Au-dessus de Δ_0, il y a la classe très importante des formules Π_1. Ce sont les formules de la forme « Pour tout entier n, F(n) », où F(n) est une formule Δ_0. Au-dessus encore, il y a les formules Π_2 de la forme « Pour tout entier n, il existe un entier m tel que F(n, m) » où F(n, m) est une formule de Δ_0. Il y a ensuite les formules Π_3 de la forme « Pour tout entier n, il existe un entier m tel que, pour tout entier k, F(n, m, k) » où F(n, m, k) est une formule de Δ_0, etc.

La formule « Pour tout entier n, n est multiple d'un nombre premier » est Π_1, car si n est connu, la formule « n est multiple d'un nombre premier » est Δ_0. C'est une formule démontrable dans l'arithmétique de Peano.

Parmi les formules Π_1, certaines sont des indécidables. La formule exprimant que le système formel de l'arithmétique de Peano est consistant (c'est-à-dire non contradictoire) est Π_1, car elle signifie « Pour tout entier n, les démonstrations dans l'arithmétique de Peano de longueur au plus n ne conduisent jamais à démontrer que 0 = 1 ».

De nombreux énoncés sur lesquelles les mathématiciens s'interrogent sont équivalents à des formules Π_1. C'est le cas de la conjecture de Goldbach (tout nombre pair > 2 est somme de deux nombres premiers), mais aussi de la conjecture de Riemann (une fois correctement traduite). La formule arithmétique qui exprime le théorème des quatre couleurs (toute carte peut être coloriée avec quatre couleurs sans que deux pays voisins portent la même couleur) est aussi une formule Π_1.

Les énoncés du type « $K(s) \geq n$ » (s et n fixés) sont des formules Π_1. En effet, une telle affirmation indique qu'aucun programme de longueur inférieure à n ne donne s. À cause des programmes ne s'arrêtant pas, cet énoncé est du type « pour tout n, F(n) ».



« Échelle du paradis », selon la conception du moine Jean Climax (VI^e siècle) : la vie monastique s'échelonne comme sur les 30 barreaux d'une échelle. Les formules mathématiques s'échelonnent, elles, sur une infinité de degrés.

on ajoute l'axiome « $K(s) = n$ » qui donne sa complexité. La nouvelle théorie T' a le pouvoir de démontrer tous les énoncés de la forme « Pour tout x : $F(x)$ » où F est une formule testable par programme (par exemple, « x est un multiple de 7 »). Les énoncés de ce type constituent ce qu'on nomme la classe de formules Π_1, et on montre que la plupart des questions non résolues en mathématiques sont équivalentes à des énoncés de la classe Π_1.

C'est le cas de la conjecture de Goldbach (« Tout nombre pair supérieur à 2 est somme de deux nombres premiers. ») ; c'est aussi le cas de l'hypothèse de Riemann, qui concerne la répartition des nombres premiers.

Notons bien que l'idée d'ajouter comme axiomes tous les énoncés de la forme « $K(s) = n$ » est étudiée ici comme on étudie ce qui se passe quand deux particules isolées interagissent. Il n'existe aucun moyen pratique d'isoler parfaitement deux particules, mais c'est intéressant quand même de faire le calcul. Ici, il n'existe aucun moyen pratique de connaître la complexité de toutes les suites finies, qui conduirait à ajouter véritablement tous les axiomes envisagés.

On bouche un gros trou grâce à la complexité

Cependant, le résultat de cette expérience de pensée nous apprend quelque chose de profond sur l'indécidabilité : les trous que comporte toute théorie T correspondent (quand on se limite aux énoncés Π_1) à un manque d'information sur la complexité. L'indécidabilité de Gödel provient donc de ce qu'une théorie donnée T n'a jamais une assez bonne connaissance de la complexité et qu'il est impossible de mettre toute cette connaissance dans des axiomes simples. En deux mots : l'indécidabilité gödélienne provient de l'ignorance de la complexité.

L. Bienvenu et ses collègues se sont aussi interrogés sur ce que donnerait une information partielle sur la complexité, fournie par un nombre limité d'axiomes. Ils montrent que pour qu'une théorie soit capable de démontrer toutes les formules Π_1 de taille au plus n, il suffit d'ajouter un axiome unique de la forme $K(s) > n$ pour une suite finie s bien choisie de longueur n. Les suites s utilisables pour cet ajout concentrent en elles l'information nécessaire pour connaître la complexité de toutes les suites de longueur au plus n.

Quand on veut rendre décidables toutes les formules Π_1, cette façon de procéder est beaucoup plus économique en axiomes que la précédente (qui ajoutait tous les « $K(s) = n$ »). Les cinq chercheurs en déduisent le beau théorème suivant : pour tout entier n, il existe un indécidable dont la taille est approximativement n, qui est une formule Π_1 et qui, ajoutée aux axiomes de l'arithmétique de Peano, supprime tous les indécidables Π_1 de taille inférieure à n. En clair, pour boucher tous les trous correspondant à des formules Π_1 précisée et qui est donc une séquence concentrant toute l'information jusqu'au niveau n qu'il faut connaître pour supprimer les indécidables Π_1 de complexité inférieure à n.

Un tel théorème, contrairement aux résultats envisageant d'ajouter une infinité d'axiomes pour supprimer tous les indécidables Π_1, permet d'envisager réellement une complétion progressive de l'arithmétique de Peano dans le but de supprimer petit à petit les indécidables Π_1.

Kurt Gödel a défendu l'idée qu'il fallait tenter de compléter les axiomes de nos théories pour en limiter l'incomplétude. Ce théorème indique une voie possible et montre qu'il existe des méthodes systématiques pour ce faire (au moins pour les formules Π_1).

4. Le rôle des formules Π_1

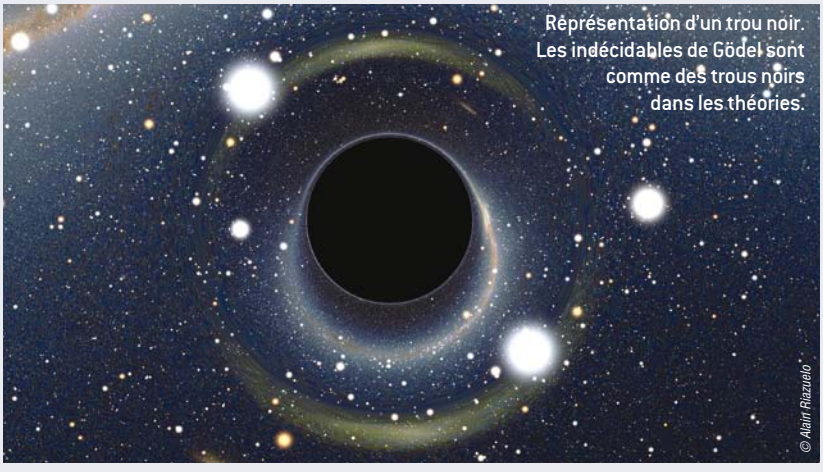
Un théorème central figure dans le travail de Laurent Bienvenu, Andrei Romashchenko, Alexander Shen, Antoine Taveneaux et Stijn Vermeeren. Ce théorème indique non seulement que pour une théorie T, connaître la complexité de toutes les séquences finies permet de supprimer tous les indécidables Π_1 et réciproquement ; il indique aussi ce qui se passe quand T ne connaît que partiellement ce type d'information.

Le théorème utilise la notion de complexité d'une formule (fondée sur la même idée que la définition de la complexité de Kolmogorov) et il énonce que les trois méthodes suivantes pour compléter une théorie T sont équivalentes :

a) Ajouter aux axiomes toutes les formules indiquant la complexité de séquences s qui ont une complexité $K(s)$ inférieure à n.

b) Ajouter aux axiomes toutes les formules Π_1 vraies dont la complexité (comme formule) est inférieure à n ;

c) Ajouter un seul axiome $K(r_n) > n$ pour une séquence r_n dont la construction est



Représentation d'un trou noir. Les indécidables de Gödel sont comme des trous noirs dans les théories.

© Alain Riazuelo

de taille inférieure à n, un seul axiome supplémentaire assez court suffit.

Les séquences finies s qui permettent ces complétions efficaces sont-elles nombreuses ? La réponse à cette question a été trouvée et, sans surprise, elle est négative : pour compléter efficacement, il faut bien choisir s et c'est difficile, car les s qui conviennent sont en petit nombre.

Un effet limité…

Un autre théorème intéressant généralise le théorème de G. Chaitin mentionné plus haut. Il affirme que, même très efficaces, ces complétions par des axiomes bien choisis n'ont qu'un effet fini, et qu'il faut donc ajouter une infinité d'axiomes pour faire disparaître les indécidables Π_1. Voici l'énoncé : « Il existe une constante c (qui dépend seulement de la théorie T) telle que, pour tout d fixé, l'ensemble des axiomes vrais de la forme $K(s) > d$ ne peut pas prouver des propriétés de la forme $K(s) > c + d$. »

Autrement dit, la connaissance requise pour savoir quelles suites ont une complexité supérieure à d ne permet pas de savoir quelles suites ont une complexité supérieure à $c + d$: une connaissance « locale » jusqu'à d de la complexité n'est jamais en mesure d'en fournir une connaissance dépassant $c + d$.

La conclusion de cet ensemble de résultats, dont nous n'avons reproduit ici qu'une petite partie, est que, d'une part, l'information sur la complexité des suites finies est bien au cœur de l'indécidabilité (au moins pour les formules Π_1), et que, d'autre part, la force axiomatique d'information sur la complexité est puissante et est susceptible d'une certaine concentration.

La définition des suites infinies aléatoires rappelée au début suggère une idée : trouver une suite infinie aléatoire (au sens de Martin-Löf) unique s et ajouter à T les axiomes indiquant que cette suite particulière est aléatoire. Cet ajout limité correspondant à une affirmation portant sur une unique suite infinie peut-il dire tout ce qui est nécessaire pour que toutes les formules Π_1 deviennent décidables ?

La réponse est négative. Cet objectif ne peut être atteint ; aucune suite infinie aléatoire ne le permet. Cela résulte d'un théorème des cinq chercheurs : l'ensemble d'axiomes affirmant qu'une suite est aléatoire au sens de Martin-Löf n'est jamais suffisant pour supprimer tous les indécidables Π_1.

Une multitude d'autres résultats affinant notre compréhension de la force axiomatique du hasard sont présentés et démontrés. Précisons qu'à côté de ces résultats de limitation, des résultats expérimentaux d'une équipe réunie autour de Fernando Soler-Toscano, à laquelle je participe, montrent qu'à condition d'accepter d'effectuer des calculs massifs, une certaine connaissance approchée robuste de la complexité de Kolmogorov est possible et que cette connaissance qui s'applique y compris aux séquences courtes est utile aujourd'hui et sert d'étalon pour mener des expériences en psychologie *(voir la bibliographie)*.

Une méthode automatique d'ajouts progressifs d'axiomes utiles (pour rendre décidables les formules indécidables de Π_1) pourrait s'en déduire pour celui qui disposerait d'une capacité de calcul indéfiniment croissante. En utilisant la technique de cette équipe, on obtiendrait pour des suites finies de plus en plus nombreuses des approximations de $K(s)$ qui s'amélioreraient et qu'on ajouterait et modifierait au fur et à mesure du déroulement du calcul.

Des liens devenant précis

Le phénomène de l'incomplétude découvert et démontré par Gödel en 1930 est troublant et toute philosophie des mathématiques (et même des sciences) se doit d'en rendre compte et d'en fournir la compréhension. Les liens établis entre cette incomplétude, la complexité et le hasard que plusieurs résultats de G. Chaitin, Per Martin-Löf et Leonid Levin avaient déjà fait apparaître deviennent maintenant très précis, grâce aux théorèmes établis par l'équipe réunie autour de L. Bienvenu. On sait désormais que ce qui manque dans une théorie formalisée, c'est essentiellement de l'information sur la complexité et le hasard, et on commence à comprendre comment on peut ajouter cette information de façon plus ou moins efficace. ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

BIBLIOGRAPHIE

L. Bienvenu *et al.*, **The axiomatic power of Kolmogorov complexity**, *Annals of Pure and Applied Logic*, à paraître, 2014 (arxiv.org/pdf/1301.3392.pdf).

F. Soler-Toscano *et al.*, **Calculating Kolmogorov complexity from the output of frequency distributions of small Turing machines**, *PLoS ONE*, vol. 9(5), e96223, 2014.

A. Taveneaux, **Puissance logique et calculatoire de l'aléa algorithmique**, Thèse de doctorat, Université Paris 7, 2013.

S. Vermeeren, **Notions and Applications of Algorithmic Randomness**, Thèse de doctorat, Université de Leeds, 2013.

N. Gauvrit *et al.*, **Algorithmic complexity for short binary strings applied to psychology : a primer**, *Behavior Research Methods*, en ligne le 6/12/2013 (http://tiny.cc/7ahehx).

Retrouvez la rubrique Logique & calcul sur www.pourlascience.fr

SCIENCE & FICTION

Des vampires pas si imaginaires

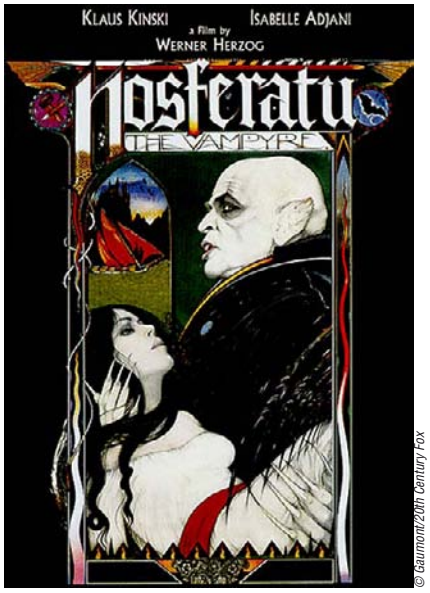
Personnage incontournable de la culture fantastique, le vampire se comporte tel un parasite se nourrissant du sang de ses victimes. Bien réels, les moustiques, les tiques et certaines chauves-souris en font tout autant.

Jean-Sébastien STEYER et Roland LEHOUCQ

Dracula, Nosferatu, Vlad l'empaleur, Lestat, Carmilla… ont des noms variés, mais ne forment qu'une seule et même entité gothique issue de lointains folklores ou d'anciennes superstitions. Le vampire (*vampyre* en vieux français, *upir* en slave) est un mort-vivant qui se nourrit du sang des vivants et en tire sa force vitale.

Ces êtres ont fait parler d'eux au XVIII[e] siècle. La population croyait que ces monstres rôdaient parmi les hommes. En 1751, le moine bénédictin Augustin Calmet a expliqué comment reconnaître un vampire dans son *Traité sur les apparitions*. Il y affirmait qu'un vampire a la peau violacée ou pâle à cause de son penchant pour le sang. Tantôt très pileux tantôt chauve, il peut avoir des oreilles pointues. Dans une vision plus moderne, le vampire arbore un aspect gothique élégant pour mieux attirer ses proies, en majorité de jeunes adolescents. Mais la caractéristique commune demeure des canines longues et pointues, utilisées lors du « baiser ». Notons cependant que, chez le *Nosferatu* de Werner Herzog, interprété par Klaus Kinski, ce sont les incisives qui sont hypertrophiées (comme chez les rongeurs et les lapins !) et non les canines.

Dans les films et les livres, la survie du vampire dépend des humains, alors que la réciproque est fausse : le vampire répond donc à la définition du parasite. Le fait qu'il ne soit pas en permanence en train de s'abreuver au cou d'un homme en fait un parasite temporaire. Il existe bien sûr des variantes selon les histoires : certains vampires se compliquent la vie en ne sélectionnant que du sang de jeunes filles vierges (comme c'est le cas du *Nosferatu* de Werner Herzog), tandis que d'autres ne sortent que la nuit. Notons que le *Dracula* de Bram Stoker (1897) arpente les rues de Londres en plein jour. Ces contraintes d'approvisionnement en sang, même si elles ajoutent du piment au scénario, diminuent la probabilité d'une rencontre entre le parasite et sa victime et réduisent d'autant les chances de survie du vampire. Elles illustrent le fait qu'un organisme hyperspécialisé est beaucoup plus fragile qu'un individu généraliste.



1. DANS LE FILM *NOSFERATU* (1979) de Werner Herzog, Klaus Kinski joue le rôle du comte Dracula qui chasse la nuit, à la recherche d'une victime pour se nourrir de son sang.

Un parasite hématophage

Autre caractéristique, le vampire est un parasite externe, ou ectoparasite, qui puise le sang de l'extérieur. Ce n'est pas le cas des micro-organismes qui vivent dans le sang de leur hôte : ces endoparasites, tels que le protozoaire *Plasmodium* ou le ver *Onchocerca*, sont responsables de graves maladies – respectivement le paludisme et la « cécité des rivières ». Ils sont véhiculés par des moustiques ou autre suceurs de sang externes.

Dans le monde réel, les hématophages (littéralement « mangeurs de sang ») ne