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 $1/2^m$.

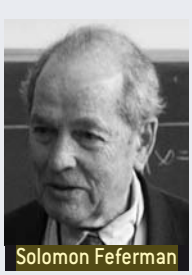
Comme il est facile d'écrire un programme de longueur proche de n qui produit une suite s de longueur n donnée (on prend le programme « PRINT s »), la complexité de Kolmogorov d'une suite de longueur n est, sauf rares exceptions, très proche de n.

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,