

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 gödelienne, 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 ,