Des machines pour Goldbach et Riemann

Tout comme on peut envisager d'écrire explicitement une machine de Turing qui recherche une contradiction dans la théorie des ensembles ZFC et qui n'en trouvera pas, on peut expliciter une machine de Turing qui recherche un contre-exemple à la conjecture de Goldbach, c'est-à-dire un entier pair supérieur à 2 qui ne s'écrit pas comme somme de deux nombres premiers.

Une telle « machine de Goldbach » ne s'arrête que si la conjecture de Goldbach est fausse. Le nombre d'états de cette machine de Turing qu'on tente de rendre le plus petit possible est une mesure de la difficulté de la conjecture. Le record obtenu tout récemment est 47. Une machine à 27 états est en cours de vérification (www.scottaaronson.com/blog/?m=201605).

L'hypothèse de Riemann est une conjecture centrale de la théorie des nombres, formulée en 1859 par le mathématicien allemand Bernhard Riemann. Elle énonce que les zéros non triviaux de la fonction zêta de Riemann ont tous pour partie réelle 1/2 et donne des précisions sur la densité des nombres premiers.

On recherche des machines de Turing qui ne s'arrêtent que si la conjecture est fausse. La plus petite connue aujourd'hui est à 744 états. Si la conjecture de Riemann est indécidable dans ZFC (c'est une éventualité parfois envisagée), on pourra alors affirmer que $s(744)$ est indécidable dans ZFC, ce qui serait un progrès.

De même, si la conjecture de Goldbach se révélait indécidable dans ZFC, on saurait alors que $s(47)$ est indécidable dans ZFC.

encore, cette fonction croît plus rapidement que n'importe quelle fonction calculable par algorithme.

Voici le raisonnement de Radó. Soit $f(n)$ une fonction calculable par algorithme dont on suppose qu'elle majore $s(n)$, c'est-à-dire que pour tout entier n, $f(n) \geqslant s(n)$. En l'utilisant, on pourrait savoir par algorithme si une machine donnée M à n états s'arrête ou non. En effet, on calcule $f(n)$, puis on calcule $f(n)$ étapes du fonctionnement de M ; si M s'est arrêtée pendant ces $f(n)$ étapes, c'est qu'elle s'arrête, sinon c'est qu'elle ne s'arrête jamais, par définition de $s(n)$. Une fonction calculable par algorithme et qui majore $s(n)$ ne peut donc pas exister. Autrement dit : pour toute fonction $f(n)$ calculable par algorithme, il existe un n tel que $f(n) < s(n)$. Sans beaucoup d'effort, on montre même qu'il existe une infinité de n tels que $f(n) \leqslant s(n)$, et en outre que c'est le cas pour tous les entiers à partir d'une certaine valeur.

Voyons maintenant le rapport entre cette fonction de Radó et la théorie des ensembles, ce qui nous mènera aux nouveaux indécidables courts découverts il y a quelques mois.

Des indécidables grâce à la fonction de Radó

La théorie des ensembles permet de représenter pratiquement tous les objets mathématiques et tous les raisonnements qu'on fait avec eux. Sa version la plus utilisée (par exemple dans le traité *Éléments de mathématique,* de Nicolas Bourbaki) est notée ZFC, pour « Zermelo-Fraenkel avec axiome du choix » (Ernst Zermelo et Abraham Fraenkel sont deux mathématiciens qui ont contribué à sa définition). L'axiome du choix stipule que pour toute famille F d'ensembles non vides et disjoints deux à deux, par exemple $\{\{a\}, \{1, 2, 3\}, \{X, Y\}, \{p, q, r, s\}\}$, il existe un ensemble C de « choix » contenant un élément exactement de chaque ensemble de F ($C = \{a, 2, X, r\}$ conviendrait pour notre exemple). Depuis un siècle qu'on utilise ZFC, on n'y a jamais trouvé de contradiction et nous supposerons qu'il n'y en a pas.

On montre que lorsqu'une fonction $f(n)$ n'est pas calculable par algorithme, la théorie des ensembles ZFC ne peut pas en connaître certaines valeurs. Autrement dit il existe au moins un entier n tel que l'énoncé $f(n) = k$ qui en donne la valeur est un indécidable de ZFC. C'est vrai aussi pour n'importe quelle autre théorie non contradictoire utilisée à la place de ZFC, mais bien sûr pas nécessairement avec le même entier n.

Concernant la fonction $s(n)$ de Radó, on sait donc depuis 1962 qu'avec la théorie ZFC, il existe au moins un entier n_0 tel qu'on ne peut déterminer la valeur de $s(n_0)$: l'énoncé $s(n_0) = k$, pour la bonne valeur de k, n'est pas démontrable dans ZFC, et sa négation non plus. La théorie ZFC est impuissante pour $s(n_0)$, qui échappe à son pouvoir déductif.

La question que se sont récemment posée Scott Aaronson, professeur au MIT, et Adam Yedidia, l'un de ses étudiants, est la suivante : est-ce que ce n_0 qui marque l'impuissance de ZFC vaut 10, 1 000, 100 milliards ou autre chose ? Répondre en proposant une valeur aussi petite que possible de n_0 est une façon parfaitement concrète de mesurer la proximité des indécidables de ZFC.

Le résultat auquel ils sont parvenus est que $s(7\,918)$ échappe à ZFC : jamais un mathématicien travaillant avec la théorie classique des ensembles ne pourra connaître $s(7\,918)$. Dit autrement, parmi les machines de Turing à 7 918 états qui ne s'arrêtent pas, certaines le font pour des raisons que la théorie n'est pas capable d'analyser. C'est la première fois qu'on réussit à avoir une précision de ce type sur l'indécidabilité dans la théorie des ensembles.

Chose amusante, ce travail, rendu public en mai 2016, a aussitôt suscité d'autres travaux sur la même question, lesquels ont abouti à son amélioration. Stefan O'Rear a établi dans un premier temps que $s(5\,349)$ échappe à ZFC, résultat encore amélioré quelques jours plus tard pour arriver cette fois à la démonstration que $s(1\,919)$ est hors d'atteinte de ZFC.

Désormais, personne ne pourra plus dire que les indécidables de la théorie des

ensembles ne concernent que des problèmes alambiqués et si complexes qu'aucun mathématicien ne s'y intéressera jamais de lui-même : s'interroger sur $s(1\,919)$ est naturel, car cela concerne la partie la plus élémentaire de la théorie mathématique du calcul…

Notons que ce record $n_0 = 1\,919$ est sans doute améliorable, car, comme le savent bien ceux qui tentent de connaître les valeurs de $s(n)$, les difficultés concrètes commencent dès $s(5)$, qui reste inconnu à ce jour. Une bonne marge de travail est donc disponible entre 5 et 1 919, marge que l'on réduira soit en progressant dans le calcul des $s(n)$, soit en réussissant à prouver l'indécidabilité d'énoncés de la forme $s(n) = k$ pour des valeurs encore plus petites que $n_0 = 1\,919$.

La machine Z ne s'arrête jamais

La méthode utilisée par Adam Yedidia et Scott Aaronson est intéressante. L'idée la plus naturelle serait de mettre en œuvre les techniques d'arithmétisation de la syntaxe de Gödel et donc de construire une machine de Turing M qui recherche une contradiction dans ZFC en énumérant toutes les démonstrations de ZFC et en tentant d'y reconnaître une preuve de l'énoncé « 0 = 1 ». Une telle machine ne trouvera pas de contradiction, et pourtant ZFC ne pourra pas le démontrer (sinon, cela signifierait que ZFC démontre qu'elle n'est pas contradictoire, ce que le second théorème d'incomplétude de Gödel interdit). Cependant, cette méthode par l'arithmétisation de la syntaxe conduirait à une machine de Turing à plusieurs centaines de milliers d'états, voire des millions, et l'on ne démontrerait donc l'indécidabilité de $s(n) = k$ que pour un n très grand.

La méthode utilisée par Scott Aaronson et Adam Yedidia évite cette explosion du nombre d'états de la machine de Turing dont ZFC ne peut prouver le non-arrêt. Elle se fonde sur des travaux récents de Harvey Friedman, de l'université d'État de l'Ohio, qui élabore depuis des années des énoncés d'arithmétiques indécidables dans ZFC ou d'autres théories. L'un d'eux concerne une propriété des graphes et cette propriété, trop abstraite pour être décrite ici, est équivalente à celle exprimant la non-contradiction de ZFC. Cette propriété s'écrit assez facilement en termes arithmétiques et la machine, notée Z, qui cherche un contre-exemple à cet énoncé est donc relativement simple comparée à celle qu'on aurait obtenue par arithmétisation de la syntaxe : elle énumère des séries d'entiers et effectue des tests sur eux. Le fait que Z ne s'arrête pas dans cette recherche de contre-exemple est nécessairement un indécidable de ZFC, sinon, encore une fois, ZFC démontrerait d'elle-même qu'elle est non contradictoire.

Soit n_0 le nombre d'états de Z. Puisque pour connaître $s(n_0)$, ZFC doit savoir prouver le non-arrêt de chaque machine à n_0 états qui ne s'arrête pas, il en résulte que ZFC ne peut pas démontrer $s(n_0) = k$ pour la bonne valeur k. Précisons que la propriété en question des graphes est démontrable dans une théorie un peu plus forte que ZFC, et donc qu'on a toutes les raisons de la croire vraie. Notons aussi qu'une fois leur machine Z programmée, Scott Aaronson et Adam Yedidia l'ont effectivement lancée pour voir si elle s'arrêtait ; au bout de plusieurs heures, elle ne s'était pas arrêtée.

Sans effort particulier, utiliser ce raccourci déduit des travaux de Friedman n'aurait cependant pas permis à lui seul d'arriver aux petites valeurs de n_0 aujourd'hui connues. Scott Aaronson et Adam Yedidia ont, et c'est la seconde idée originale de leur travail, conçu un langage informatique nommé Laconic permettant d'exprimer la propriété de Friedman de manière concise. Ils ont aussi écrit et utilisé le traducteur des programmes écrit en Laconic qui en tire des machines de Turing du type considéré par Radó. C'est ainsi qu'ils ont obtenu la machine de Turing Z à 7 918 états qui ne s'arrête jamais, mais dont ZFC ne peut pas démontrer qu'elle ne s'arrête jamais. Le passage de 7 918 états à 1 919 états s'est fait en améliorant le langage et les opérations de transformation des programmes en machines de Turing.

Saura-t-on faire encore mieux et trouver des valeurs encore plus petites que le $n_0 = 1\,919$ d'aujourd'hui ? C'est probable, et peut-être qu'à l'heure où vous lirez ce texte, le record sera déjà battu. Pour le savoir, consultez le blog de Scott Aaronson ! ■

L'AUTEUR

J.-P. DELAHAYE est professeur émérite à l'université de Lille et chercheur au Centre de recherche en informatique, signal et automatique de Lille (CRISTAL).

BIBLIOGRAPHIE

S. Aaronson, **The 8000th Busy Beaver number eludes ZF set theory : New paper by Adam Yedidia and me**, blog de mai 2016, www.scottaaronson.com/blog/?m=201605

H. Marxen, **List of the known Busy Beaver values**, 2016, www.drb.insel.de/ffheiner/BB/

P. Michel, **The Busy Beaver competition : A historical survey**, 2016, http://export.arxiv.org/pdf/0906.3749v4

A. Yedidia et S. Aaronson, **A relatively small Turing machine whose behavior is independent of set theory**, 2016, https://arxiv.org/pdf/1605.04343.pdf

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

C. S. Calude et E. Calude, **Evaluating the complexity of mathematical problems : Part 1 & Part 2**, *Complex Systems*, vol. 18, pp. 267-285, 2009 et pp. 387-401, 2010.

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