On comprend sans mal qu'une machine simple, avec peu d'états et peu d'instructions, placée sur un ruban couvert uniquement de 0, va soit s'engager dans un calcul infini (par exemple parcourir le ruban en changeant les 0 en 1, ou osciller entre deux cases sans rien y faire), soit calculer un petit moment puis s'arrêter. Une machine simple produit soit un calcul infini, soit un calcul court, et on verra que c'est justement ce qui pose un défi aux mathématiciens et les expose aux formes les plus élémentaires d'indécidabilité.

En 1962, le mathématicien hongrois Tibor Radó s'est intéressé au nombre maximal, noté $s(n)$, de mouvements qu'exécute une machine de Turing à n états avant de s'arrêter (dans le cas où elle s'arrête).

Les castors affairés

Les machines M à n états qui atteignent ce maximum sont dénommées « castors affairés ». Le nombre $s(n)$ est un nombre parfaitement défini, puisqu'il n'y a qu'un nombre fini de machines à n états n'utilisant que les symboles 0 et 1. Le nombre de machines à n états a d'ailleurs été déterminé : il est égal à $(4n+4)^{2n}$.

Pour calculer $s(n)$ pour un n donné, il suffit de faire fonctionner toutes les machines à n états en repérant celles qui calculent le plus longtemps et s'arrêtent. Avec les incroyables ordinateurs dont nous disposons, il semblerait facile d'obtenir rapidement les valeurs de $s(n)$.

Grave erreur ! Aujourd'hui, malgré de considérables efforts, on ne connaît que $s(1) = 1$, $s(2) = 6$, $s(3) = 21$ et $s(4) = 107$. On sait aussi que $s(5) \geqslant 47\,176\,870$, et que $s(6) \geqslant 7{,}4 \times 10^{36\,534}$, mais personne n'est certain que ces valeurs sont définitives. Pourquoi est-il si difficile d'évaluer $s(n)$?

La raison est double. D'abord, le nombre de machines à n états augmente très rapidement quand n augmente et on ne sait guère faire mieux, pour calculer $s(n)$, que de les prendre une à une. Ensuite, et c'est encore plus ennuyeux, les machines qui ne s'arrêtent pas sont délicates à traiter. Il faut en effet raisonner sur leurs instructions ou leur comportement pour être sûr qu'elles ne s'arrêtent pas. Pour certaines, c'est facile, mais on tombe rapidement sur des machines dont le comportement est complexe et dont on n'arrive pas à déterminer si elles s'arrêteront et donc si elles interviennent pour la détermination de $s(n)$, ou si elles poursuivent indéfiniment leurs calculs – auquel cas elles sont sans importance pour $s(n)$. On sait par ailleurs qu'aucune méthode algorithmique générale ne permet de répondre à la question. C'est la fameuse indécidabilité de l'arrêt démontrée par Turing en 1936 : aucun algorithme ne peut déterminer, pour toute machine de ce type placée sur un ruban ne comportant que des 0, si oui ou non elle finira par s'arrêter.

Une conséquence de ce résultat, qui est la raison de l'introduction par Radó de sa fonction $s(n)$, est que $s(n)$ n'est pas calculable par algorithme. Plus intéressant

Les castors affairés calculent l'entropie

La connaissance des valeurs de la fonction $s(n)$ de Radó, dont il vient d'être démontré que $s(1\,919)$ est indécidable, est utile pour certains calculs fondamentaux de la théorie de la complexité. En utilisant la valeur conjecturée comme la bonne pour $n = 5$, $s(5) = 47\,176\,870$, une équipe réunie autour de Fernando Soler-Toscano a calculé l'entropie algorithmique, qui généralise l'entropie statistique de Shannon, des suites courtes de 0 et de 1.

Cette entropie est aussi nommée complexité de Kolmogorov : pour une suite donnée, c'est la taille du plus court programme qui produit la suite. Plus une suite est complexe, plus son entropie algorithmique est grande *(voir l'article indiqué en bibliographie de F. Soler-Toscano et al.)*. La méthode est la suivante. On fait calculer chacune des 26 559 922 791 424 (26 000 milliards) machines de Turing à 5 états jusqu'à ce qu'elle s'arrête où jusqu'à l'étape $s(5)$, ce qui signifie que la machine ne s'arrête jamais. Le nombre k de fois où est obtenue une suite donnée (par exemple la suite $t = 01010$) est directement lié à son entropie algorithmique $K(t)$ par une formule de Leonid Levin, $K(t) \approx -\log_2[k/N(5)]$, où $N(5)$ désigne le nombre de machines à 5 états, et donne donc une valeur approchée de l'entropie.

La formule de Leonid Levin est remarquable et très profonde. Elle signifie que les suites complexes (c'est-à-dire celles dont le plus court programme de création est long) sont aussi celles qu'une machine tirée au hasard produit avec la plus faible probabilité.

Quelques valeurs ainsi obtenues sont présentées ci-dessous.

SUITE	FRÉQUENCE	ENTROPIE
1	0,175036	2,51428
0	0,175036	2,51428
11	0,0996187	3,32744
10	0,0996187	3,32744
01	0,0996187	3,32744
00	0,0996187	3,32744
111	0,0237546	5,3962
000	0,0237546	5,3962
110	0,0229434	5,44578
100	0,0229434	5,44578
011	0,0229434	5,44578
001	0,0229434	5,44578
101	0,0220148	5,5038
010	0,0220148	5,5038
1111	0,0040981	7,03083
0000	0,0040981	7,03083
1110	0,00343136	8,187
1000	0,00343136	8,187
0111	0,00343136	8,187
0001	0,00343136	8,187

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