

– On peut écrire un programme *pro* (ou une machine de Turing) qui ne s'arrête pas, mais tel que l'énoncé de *S* qui exprime «*pro* ne s'arrête pas» est indécidable dans *S*. Dit en bref dans le cas particulier du système formel de Bourbaki : Bourbaki n'est pas assez puissant pour comprendre le comportement du programme *pro*.

– On peut construire un ensemble fini de formes géométriques simples *ens* (chaque forme a un bord polygonal, possède des sommets à coordonnées entières et est disponible en quantité illimitée) avec lesquelles on peut paver le plan sans interstice ni chevauchement, et pourtant l'énoncé qui exprime l'existence de ce pavage n'est pas démontrable dans *S* : Bourbaki ne voit pas qu'avec les formes de *ens* on pave le plan.

– On peut définir un jeu à information complète *jic* (le jeu de dame ou le jeu d'échecs sont de tels jeux) tel que le second joueur possède une stratégie gagnante, mais telle aussi que *S* soit incapable de voir comment répliquer correctement à certains coups initiaux du premier joueur. Bourbaki, même s'il continue à développer son traité pendant plus de 1 000 ans, ne connaîtra jamais la stratégie gagnante au jeu *jic*... alors qu'elle existe.

– Certaines égalités algébriques ne sont pas vraies, mais *S* ne sait pas le démontrer. En bref, les méthodes de preuves qu'utilise le traité de Bourbaki, même lorsqu'il s'intéresse à des problèmes algébriques simples, sont parfois aveugles.

– Certaines propriétés élémentaires concernant des produits de matrices sont indécidables dans *S* (il s'agit d'un résul-

tat récent de V. Blondel et J. Tsitsiklis). Même dans des parties élémentaires des mathématiques, Bourbaki ne pourra jamais démontrer tout ce qui est vrai.

LA COMPLEXITÉ EST INDÉCIDABLE

D'autres avancées de la théorie du calcul ont conduit depuis 1965 au développement de la théorie de la complexité de Kolmogorov, où l'on définit la complexité d'une séquence *s* composée uniquement de 0 et de 1, par la taille *K(s)* du plus court programme qui engendre *s*.

Cette théorie, pourtant importante sur le plan pratique (car c'est la théorie mathématique de la compression de données qui, on le sait, concerne toutes les technologies de l'information), est un remarquable nid d'indécidabilité. Certaines situations sont même profondément troublantes, comme celle-ci. Il existe une infinité de propositions du type «la séquence *s* possède la complexité *n*», certaines sont exactes et d'autres fausses. Non seulement un système formel donné passe à côté de certaines formules vraies de ce type, mais il ne peut en démontrer qu'un nombre fini (ces résultats ont été établis pas N. Kolmogorov et G. Chaitin). La complexité de Kolmogorov échappe gravement à tout système formel qui, par nature, n'en connaîtra qu'une partie finie.

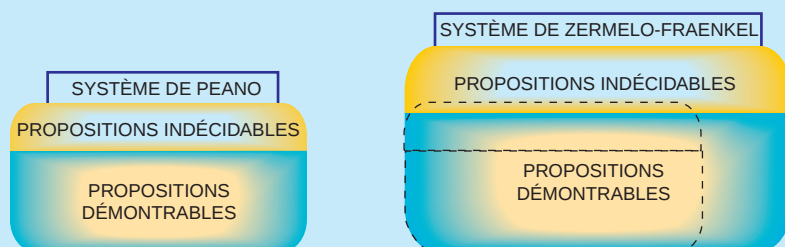
En particulier, en exploitant au mieux les ressources que donne le traité de Bourbaki, il arrivera un moment où il aura déduit tout ce qu'il pouvait sur la complexité des séquences *s* : il aura réussi à identifier quelle était la complexité *K(s)* pour certaines suites *s* en nombre fini, par exemple $K(010101) = 3$, $K(01101001110) = 12$, mais il ne pourra pas prouver un seul résultat de plus de ce type. Récemment, certains travaux de G. Chaitin conduisent à évaluer que Zermelo-Fraenkel (donc cela s'applique à Bourbaki) ne pourrait jamais démontrer qu'aucune séquence *s* ne possède une complexité de Kolmogorov supérieure à 100 000. Notons pourtant que Zermelo-Fraenkel permet de montrer l'énoncé «il existe une infinité de *s* ayant une complexité supérieure à 100 000».

La situation n'est pas la marque d'une contradiction dans Zermelo-Fraenkel, mais celle de l'incomplétude.

EFFROYABLE ÉQUATION

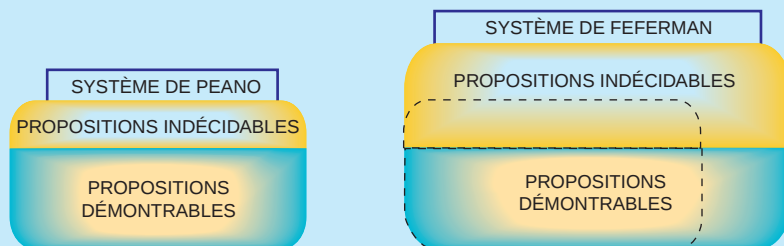
Un autre domaine où l'indécidabilité a été explicitée par la théorie du calcul est celui des équations arithmétiques. Citons le résultat de G. Chaitin, qui a construit explicitement et a fait imprimer pour de vrai (j'en ai une copie que je garde

3. CONSERVER LES MÊMES INDÉCIDABLES



EXTENSION NON CONSERVATIVE

Quand on passe de l'arithmétique de Peano (PA) à la théorie des ensembles de Zermelo-Fraenkel (ZF), on étend le domaine des objets que l'on peut traiter. On augmente alors le nombre de formules d'arithmétique que la théorie peut démontrer, et il y a donc moins de formules arithmétiques indécidables. Hélas, ce faisant, on risque de démontrer des formules absurdes telles que $0 = 1$, ce qui signifierait que le nouveau système est inconsistent. L'augmentation du pouvoir de preuve que donne une telle extension dite non conservatrice s'accompagne d'une prise de risque.



EXTENSION CONSERVATIVE

En revanche, quand on passe de l'arithmétique de Peano (PA) à une extension conservatrice du type de celles proposées par S. Feferman ou S. Simpson, on étend le domaine d'objets que l'on peut traiter (ce qui permet, par exemple, de développer l'analyse classique), mais cette fois sans augmenter le nombre de formules arithmétiques que la théorie peut démontrer (les formules arithmétiques indécidables restent donc les mêmes). Cette attitude prudente empêche d'introduire une inconsistance (si le nouveau système était inconsistent, on y démontrerait la formule $0 = 1$, ce qui signifierait que PA le démontre aussi : donc si PA est consistant, le nouveau système aussi). La découverte qu'on pouvait mener l'essentiel des mathématiques utiles aux sciences de la nature dans de telles extensions prudentes conduit à s'interroger sur le sens des autres extensions : en plus d'être dangereuses, ne sont-elles pas illusoires ?

précieusement) une équation terriblement indécidable (voir l'encadré 5).

L'équation est terriblement indécidable, car G. Chaitin a démontré qu'un système formel donné S ne peut jamais résoudre qu'un nombre fini de cas de l'équation, tous les autres cas étant indécidables dans S . Les moyens de preuve définis au début du traité de Bourbaki atteindront donc un jour une limite absolue face à cette équation. Même si le traité se développe pendant un milliard d'années, au-delà d'un certain point d'élucidation maximale, il ne permettra plus jamais de régler un seul cas supplémentaire de l'équation.

QUE RÉPONDEZ-VOUS DONC À ÇA ?

Quelle est la réponse des mathématiciens face à cet arsenal de résultats d'indécidabilité qui ont envahi chaque spécialité mathématique ?

Ils répondent qu'à chaque fois tout cela est construit sur du codage. Le programme qui ne s'arrête pas, le jeu à information complète que Bourbaki ne réussit pas à analyser, l'équation indécidable dont on ne peut traiter qu'un nombre fini de cas, etc., tout cela provient à chaque fois du déguisement avec les notations de divers domaines mathématiques, des indécidables originaux trouvés par Gödel et Turing. À chaque fois, les objets en cause sont complexes et longs à écrire (l'équation de Chaitin, avec ses 12 000 variables, battant tous les records). Les mathématiciens spécialistes d'équations diophantiennes ne se seraient jamais intéressés d'eux-mêmes aux équations que les logiciens aidés de la théorie du calcul leur mettent sous le nez. Les mathématiciens répondent donc : «Les indécidables que vous construisez sont artificiels et toutes vos constructions ne peuvent nous forcer à croire que nos propres problèmes, ceux que nous rencontrons dans le cours normal du développement de nos théories, risquent d'être indécidables.»

Face à cette réponse, les logiciens devaient dégager les indécidables de tout codage.

INDÉCIDABLES DE J. PARIS ET L. HARRINGTON

Cela se produisit, il y a une vingtaine d'années, quand plusieurs énoncés arithmétiques simples et dégagés de tout codage furent démontrés indécidables vis-à-vis de l'arithmétique de Peano (voir l'énoncé indécidable concernant les hydres cité dans la rubrique du mois de novembre).

Nombreux furent ceux, y compris parmi les mathématiciens, qui reconnurent alors qu'un pas important avait été franchi.

Malgré ces progrès, certains mathématiciens ont eu beau jeu de remarquer que les indécidables arithmétiques dégagés du codage inventés par les logiciens n'avaient jamais été envisagés spontanément par les mathématiciens. On parla d'énoncés «cuisinés exprès».

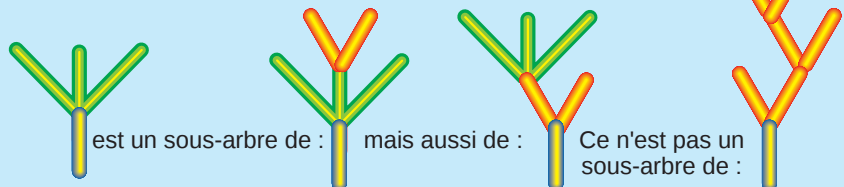
Ces énoncés sont, là encore, des constructions de logiciens. De plus, dans la grande majorité des cas, il s'agit d'indécidables de l'arithmétique de Peano décidables dans Zermelo-Fraenkel, et non pas d'indécidables de Zermelo-Fraenkel. Il manque donc encore un cas incontestable d'énoncé que les spécialistes d'arithmétique considèrent intéressant avant que les logiciens ne s'y intéressent et sur lequel ils travaillent, que les logiciens démontreraient indécidable vis-à-vis de l'arithmétique de Peano (qui

est la théorie naturelle pour écrire les raisonnements d'arithmétique) ou, mieux, indécidable avec Zermelo-Fraenkel.

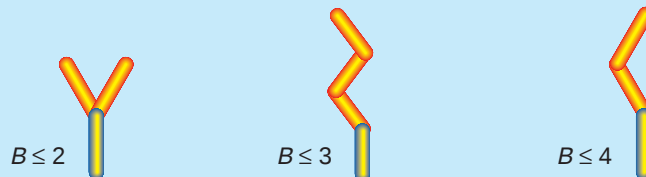
Les candidats ne manquent pas. Il y a d'une part les résultats d'arithmétique qu'on démontre avec des outils plus puissants que ceux de l'arithmétique de Peano. C'est le cas de nombreux théorèmes concernant les nombres premiers dont les premières démonstrations – qualifiées de transcendantes – utilisaient des techniques d'analyse formalisable dans la théorie Zermelo-Fraenkel, mais pas dans Peano. Pour plusieurs d'entre eux, on sait aujourd'hui que l'on peut en fait les démontrer dans l'arithmétique de Peano. Ces énoncés ne constitueront donc pas des propositions envisagées spontanément par les mathématiciens, démontrables dans Zermelo-Fraenkel, indécidables dans

4. LES ARBRES DE KRUSKAL

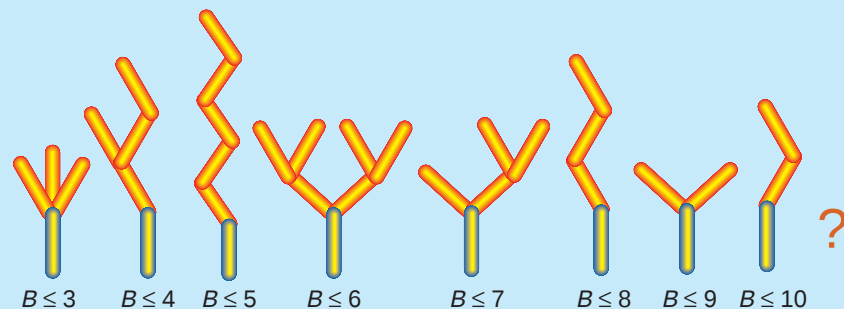
Un arbre est dit sous-arbre d'un autre si on peut retrouver la forme du premier dans le second.



On cherche à construire des séries d'arbres tels qu'aucun ne soit le sous-arbre d'un arbre placé plus loin. Une telle série d'arbres est dite correcte.



On dit qu'une série est de type 2 si le premier arbre possède deux branches au plus, le second trois branches au plus, etc. En construisant des séries correctes de type 2, on s'aperçoit qu'elles n'ont jamais plus de quatre arbres.



Une série est de type 3 si le premier arbre possède trois branches au plus, le second quatre branches au plus, etc. On s'aperçoit, là aussi, qu'on ne peut jamais prolonger indéfiniment les séries correctes de type 3.

Le théorème de Kruskal indique que, «pour tout entier n supérieur à 1, il existe une limite k à la longueur des séries correctes de type n ».

Cet énoncé ne contient aucun codage déguisé de proposition logique. C'est pourtant un énoncé indécidable de l'arithmétique de Peano. Cet énoncé est l'un de ceux qui auraient dû convaincre les mathématiciens que, même à propos de problèmes simples et naturels, l'indécidabilité peut surgir.