

5. Les ordinateurs prendront-ils le pouvoir ?

Les logiciels de calcul formel, de démonstration automatique et les assistants de preuve (qui aident le mathématicien à écrire des démonstrations sans erreur) conduisent à une pratique des mathématiques où l'ordinateur tient un rôle de plus en plus important.

Dans un article intitulé *Post-Human Mathematics*, le mathématicien-physicien David Ruelle, professeur honoraire à l'IHÉS, s'interroge sur l'avenir des mathématiques quand les ordinateurs y joueront un rôle peut-être devenu dominant (<http://arxiv.org/pdf/1308.4678.pdf>).

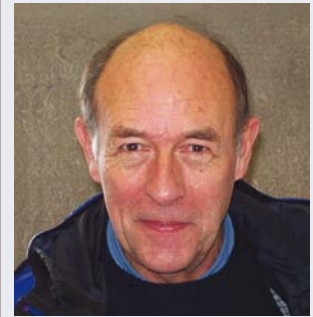
« Ma conclusion temporaire est que nous ne pouvons pas exclure que les ordinateurs puissent penser, mais que s'ils y

arrivent, alors ce sera d'une façon très différente de celle des humains. La situation est un peu semblable à celle de la chimie organique de synthèse : la synthèse de composés organiques n'est pas impossible, loin de là, mais on y arrive en général en procédant d'une façon très différente des organismes vivants. [...] Les mathématiques d'aujourd'hui sont une construction humaine où les

ordinateurs sont de plus en plus utilisés, mais ne jouent pas un rôle créatif.

La situation pourrait changer : les ordinateurs pourraient devenir créatifs, et puisqu'ils fonctionnent d'une manière très différente des cerveaux humains, ils pourraient produire des mathématiques très différentes. [...] Je ne suis pas impatient de voir les ordinateurs remplacer les mathématiciens humains. Ce serait, ou ce sera, une chose triste à certains égards, mais je ne veux pas être aveugle à cette éventualité. Les effets de la synthèse organique industrielle sur l'humanité ont été

énormes, ce fut parfois bien et parfois terrible, mais aucun retour en arrière à l'époque pré-Wohler n'est possible. De même, les mathématiques entrent probablement dans une ère nouvelle, et il est sans aucun doute intéressant de deviner ce qu'elle sera. »



partie entière de x , utilisée ici pour avoir des suites de nombres rationnels].

L'équation dont Ω est solution est donc insoluble en ce sens qu'aucune méthode ne sera jamais efficace pour en calculer la solution même de manière approchée. Cette forme d'insolubilité pratique que la théorie du calcul et la logique mathématique nous offrent ici est loin d'être la seule que le XX^e siècle a mise en évidence. Elle prolonge les résultats d'insolubilité de Ruffini, Abel et Galois.

Des algorithmes pour toute équation ?

Nous qualifierons cependant tous ces cas d'insolubilité de bénins : on sait que l'équation n'a pas de solution ou on sait que, du fait de sa nature, elle a des solutions qu'on ne connaîtra que de manière approchée et même parfois sans pouvoir contrôler l'erreur, mais au fond, l'équation est quand même traitée. Ce qui importe pour le mathématicien et encore plus pour l'ingénieur qui perfectionne les programmes de calcul formel est la mise au point de méthodes générales permettant de résoudre une famille d'équations.

En algèbre linéaire, on sait par exemple comment s'y prendre face à n'importe quel système d'équations du type :

$$x + 2y + 3z = 1,$$

$$x + 3y + 2z = 1,$$

$$3x + y + 2z = 1,$$

dont $x = y = z = 1/6$ est l'unique solution, ce qu'un logiciel de calcul formel trouve immédiatement. La présence de coefficients irrationnels ne gêne pas un bon logiciel, qui résoudra sans plus de peine un système tel que :

$$x + 2y + 3z = \pi + 5,$$

$$2x + 3y + 2z = 2\pi + 5,$$

$$3x + \pi y + \pi z = 5\pi,$$

dont les solutions sont $x = \pi, y = z = 1$.

Des algorithmes mis au point par les mathématiciens sont introduits dans le programme des logiciels de calcul formel. Ils traitent donc parfaitement des familles entières d'équations et de systèmes d'équations, voire d'inéquations. La question est alors de savoir si on pourra toujours aller plus loin dans la mise au point d'algorithmes qui fonctionneraient pour des familles variées d'équations et d'inéquations, de plus en plus vastes.

Par expérience, on sait depuis longtemps qu'il est difficile de résoudre les équations

polynomiales à coefficients entiers comme $X^2 + 5Y^3 + 2Z^4 = 11$ dont on cherche des solutions entières. Ces équations sont dites diophantiennes (en l'honneur du mathématicien grec Diophante d'Alexandrie). David Hilbert affirma en 1900 qu'il n'existait probablement pas de méthode générale pour les résoudre. L'un des grands succès de la logique mathématique fut de donner un sens et une démonstration à cette intuition. Achievant un travail commencé par les chercheurs américains Martin Davis, Hilary Putnam et Julia Robinson, le mathématicien russe Yuri Matiyasevich prouva en 1970 qu'il n'existe pas d'algorithme permettant de savoir, pour toute équation diophantienne, si elle a ou non des solutions entières.

Cette « indécidabilité du dixième problème de Hilbert » signifie que les logiciels de calcul formel ne sont pas tout-puissants. Jamais on n'en programmera un qui, face à n'importe quelle équation diophantienne, saura dire si elle possède des solutions entières, et *a fortiori* les déterminer quand il y en a.

Aujourd'hui encore, on s'intéresse aux équations diophantiennes. On recherche non plus des solutions qui soient des nombres entiers, mais des nombres appartenant à d'autres structures algébriques. Des résultats

positifs et négatifs sont obtenus, précisant le paysage de l'insolubilité selon les familles de nombres que l'on considère. Le travail du mathématicien est devenu double : trouver des méthodes algorithmiques de résolution pour des familles d'équations les plus larges possible et, le cas échéant, démontrer que de telles méthodes n'existent pas.

Kirsten Eisenträger et Alexandra Shlapentokh ont ainsi établi en 2013 un résultat très général résolvant le dixième problème de Hilbert pour les équations diophantiennes dont on recherche les solutions parmi les fonctions. Assez étrangement, un problème très simple de cette catégorie reste obstinément mystérieux : celui des nombres rationnels. En effet, on ignore s'il existe oui ou non un algorithme permettant de trouver les solutions rationnelles de toute équation polynomiale à coefficients rationnels.

Simplifier n'importe quelle expression ?

Terminons en mentionnant un résultat inattendu qui montre que même la vérification d'une formule ou sa simplification pose parfois d'insurmontables difficultés.

Si on vous souffle que $X = 1$, $Y = 2$ et $Z = 3$ est une solution de l'équation diophantienne $X^2 + 2Y^3 - 3Z - 8 = 0$, vous n'aurez aucun mal à le vérifier (il suffit de remplacer les variables de la partie gauche par les valeurs proposées, et de faire le calcul). Vérifier une identité semble être une simple question de patience qu'un ordinateur sera toujours capable de mener. Contrôler que des solutions proposées pour une équation sont correctes est une tâche plus facile qu'en trouver les solutions : c'est la fameuse asymétrie entre « trouver » et « vérifier », si utile en cryptographie. Pourtant, même le travail de vérification peut être difficile : il existe des familles de problèmes de vérifications qu'aucun algorithme ne traitera jamais parfaitement.

Parmi les identités faisant intervenir les fonctions $\sin x$ et $\cos x$, on a la fameuse relation $\sin^2 x + \cos^2 x = 1$, ainsi que $\sin 2x = 2 \sin x \cos x$, dont on déduit par exemple : $4 \sin^2 x \cos^2 x + \cos^2 2x - 1 = 0$. Un logiciel de calcul formel trouve effectivement 0 quand on lui demande de simplifier

$4 \sin^2 x \cos^2 x + \cos^2 2x - 1$. Plus compliqué (j'ai essayé !), il trouve aussi que $2 \sin x \cos x + 4 \cos^3 x - 3 \cos x - \sin 2x - \cos 3x$ vaut 0 pour tout x .

Face à de telles identités, dispose-t-on de méthodes de simplification efficaces et générales, c'est-à-dire garantissant que si on leur donne une expression identiquement nulle, elles s'en apercevront ?

Le théorème de Daniel Richardson, démontré en 1968 et récemment perfectionné par Mikloz Laczkovich, indique que, là encore, le pouvoir des algorithmes est limité. Ce théorème décrit une catégorie de problèmes de simplification qu'aucun algorithme ne sera jamais capable de traiter parfaitement.

D. Richardson considère toutes les expressions désignant des fonctions d'une variable réelle et construites en utilisant des nombres rationnels, les constantes π et $\ln(2)$, les fonctions $\sin x$, $\exp x$ et $|x|$ (valeur absolue de x), et les opérations d'addition, de soustraction, de multiplication et de composition de fonctions. Il démontre qu'aucun algorithme ne peut reconnaître toutes les expressions désignant la fonction nulle. Autrement dit, aucune méthode automatique ne sera jamais capable de simplifier toutes les formules qui peuvent l'être.

Une multitude de résultats de ce type sont maintenant connus concernant les équations entre mots, entre matrices, entre fonctions, ou concernant le calcul automatique des primitives. Ils nous apprennent que l'automatisation des tâches de calculs et de résolution d'équations est limitée dans toutes les directions. Cela n'empêche pas des progrès continus dans la programmation des calculs mathématiques et, au contraire, permet d'y être plus efficaces.

Le travail de ceux qui améliorent les logiciels de calcul formel présente un double visage : d'une part, identifier ce qui est impossible en prouvant des résultats comme ceux de Y. Matiyasevich et de D. Richardson, afin d'en déduire des objectifs raisonnables ; d'autre part, rechercher des bons algorithmes qui mèneront des calculs de plus en plus complexes, rapides et variés. Les équations insolubles sont au cœur des mathématiques depuis l'Antiquité. C'est en les maîtrisant et en les comprenant que, bien souvent, les mathématiciens avancent.

L'AUTEUR



J.-P. DELAHAYE est professeur émérite à l'Université de Lille et chercheur au Laboratoire d'informatique fondamentale de Lille (LIFL).

Le blog de Jean-Paul Delahaye sur SciLogs.fr : www.scilogs.fr/complexites/

BIBLIOGRAPHIE

E. Reiter, *Limits of Computation : An Introduction to the Undecidable and the Intractable*, CRC Press, 2013.

J. Koenigsmann, *Undecidability in number theory*, prépublication [<http://arxiv.org/abs/1309.0441>], 2013.

M. Suvakov et V. Dmitrasinovic, *Three classes of Newtonian three-body planar periodic orbits*, *Phys. Rev. Lett.*, vol. 110, 114301, 2013.

B. Poonen, *Undecidable problems : A sampler*, prépublication [[arXiv:1204.0299](http://arxiv.org/abs/1204.0299)], 2012.

C. Calude *et al.*, *Computing a glimpse of randomness*, *Experimental Mathematics*, vol. 11(3), pp. 361-370, 2002.

M. Henkel, *Sur la solution du problème des trois corps de Karl Sundman en 1909*, *Philosophia Scientiae*, vol. 5(2), pp. 161-184, 2001.

M. Petkovšek *et al.*, *A = B*, AK Peters, 1996.



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