

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