LOGIQUE & CALCUL

Du rêve à la réalité des preuves

Les ordinateurs ne savent pas prouver seuls des théorèmes profonds. Cependant, grâce aux assistants de preuve, ils garantissent les démonstrations découvertes par les mathématiciens.

Jean-Paul DELAHAYE

Il y a 100 ans paraissait le premier des trois tomes des *Principia Mathematica* d'Alfred Whitehead et Bertrand Russell. En s'appuyant sur les travaux de Gottlob Frege, Giuseppe Peano, Richard Dedekind et Georg Cantor, cet ouvrage montre comment réduire les mathématiques à la logique symbolique. L'ouvrage est l'un des plus importants de l'histoire des mathématiques, car il montre pour la première fois qu'un savoir scientifique peut être entièrement formalisé.

Avant le travail de Whitehead et Russell, écrire une démonstration mathématique était un exercice de nature littéraire où il fallait convaincre les lecteurs d'une affirmation abstraite. L'acceptation d'une preuve ou son refus résultait d'un consensus entre spécialistes conduisant le plus souvent à un accord unanime. Dans toutes les sciences, cette situation prévaut : il n'y a pas de procédure automatique et absolue de validation d'un résultat ou d'une théorie. On dispose de méthodes de contrôle, variées selon les disciplines, mais l'affaire reste humaine et dans certaines situations, les désaccords persistent longuement.

Avec les *Principia,* la formalisation des mathématiques fait basculer ces dernières dans une situation différente : vérifier si un résultat mathématique est juste peut être confié à un opérateur ignorant de ce dont traite la démonstration et qui se contentera de contrôler si les règles de manipulations symboliques des *Principia*, en nombre fini et fixées à l'avance, ont été respectées.

Cette formalisation est un immense progrès, puisque plus aucune controverse ne peut exister sur la validité d'une preuve écrite dans le langage des *Principia*. Si quelqu'un prétend qu'une preuve est fausse, l'opérateur ignorant trouvera l'erreur. Tout se passe comme pour un calcul arithmétique : aucune faute ne peut se dissimuler. Grâce à la formalisation, et comme l'avait imaginé Leibniz avec sa *characteristica universalis* au XVII^{e} siècle, démontrer est devenu un simple calcul.

Tout cela est très beau, mais c'est un rêve : la formalisation proposée par Whitehead et Russell est trop complexe pour être pratiquée dès qu'on aborde autre chose que des théorèmes élémentaires de logique ou d'arithmétique. Dans les *Principia,* les preuves formelles sont rarement écrites entièrement, les auteurs se contentant de montrer qu'elles existent et d'indiquer ce qu'il faudrait faire pour les écrire.

Avec les *Principia*, les mathématiques deviennent formalisables *en principe*, mais pas en réalité. S'en tenir au langage des *Principia* conduit à des preuves dont la longueur empêche leur écriture effective et donc leur contrôle. Le formalisme des *Principia* n'est pas praticable et la garantie qu'aurait dû donner le formalisme ne fonctionne pas.

D'autres formalisations générales des mathématiques ont été proposées, dont celle de Bourbaki, le célèbre mathématicien français polycéphale. Sa proposition, qui date des années 1930, s'appuie sur la théorie des ensembles et le logicien Adrian Mathias en a révélé une propriété cocasse. Dans le formalisme de Bourbaki, la notation complète pour désigner le nombre « 1 » est une longue suite de symboles et Bourbaki indiquait que si l'on tentait de la déployer sans utiliser aucun raccourci, l'écriture complète du « 1 » comporterait quelques dizaines de milliers de symboles. A. Mathias a montré que la situation était pire et qu'écrire le nombre « 1 », en respectant à la lettre le formalisme de Bourbaki, nécessiterait 4 523 659 424 929 symboles, soit l'équivalent de quatre millions de livres de 400 pages.

L'informatique rend-elle tout simple ?

Les premiers formalismes complets proposés pour les mathématiques ne sont pas destinés aux mathématiciens terrestres ! Pourtant, l'informatique et un siècle de travail de la part des logiciens ont maintenant transformé le rêve en réalité. Le *en principe* qui était juxtaposé à « mathématiques formalisables » peut être enlevé.

L'informatique n'a pas peur des grandes quantités de données. La formalisation des

Principia ou celle du traité de Bourbaki à l'aide des ordinateurs fonctionnerait-elle sans peine ?

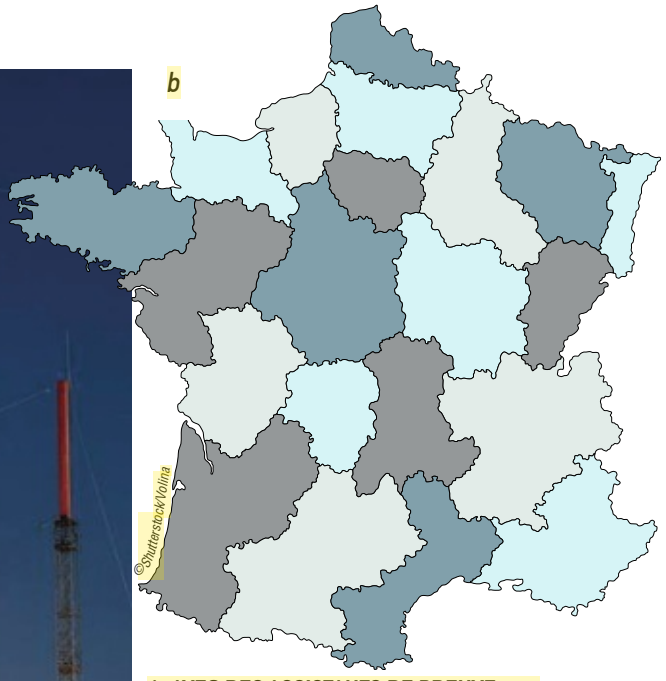
Non. Les calculs informatiques ne peuvent tout affronter et la formidable puissance des ordinateurs ne dispense pas d'être intelligent. Nos machines sont de capacité limitée et ce n'est pas parce que le progrès est rapide que l'on dispose d'une puissance infinie. Ainsi, on ne sait aujourd'hui ni trouver un nombre premier de plus de 13 millions de chiffres, ni calculer un million de milliards de décimales de π, on en est seulement à 5 000 milliards de décimales. Le formalisme des *Principia* ou du traité de Bourbaki est bien trop gourmand en puissance, même pour les plus puissants des ordinateurs ou des réseaux informatiques.

Attendre serait une solution, mais il n'est pas certain que les progrès technologiques ne buttent pas sur une limite ultime : il est probable, au contraire, que la miniaturisation ne pourra aller en deçà de la taille des atomes. Le plus sage pour obtenir une formalisation pratique et réelle des mathématiques est donc de mener une double attaque : améliorer les formalismes en les simplifiant pour les rendre praticables et profiter des gains de puissance que la technologie nous offre. C'est ce que l'on a fait et l'heure du succès est maintenant arrivée.

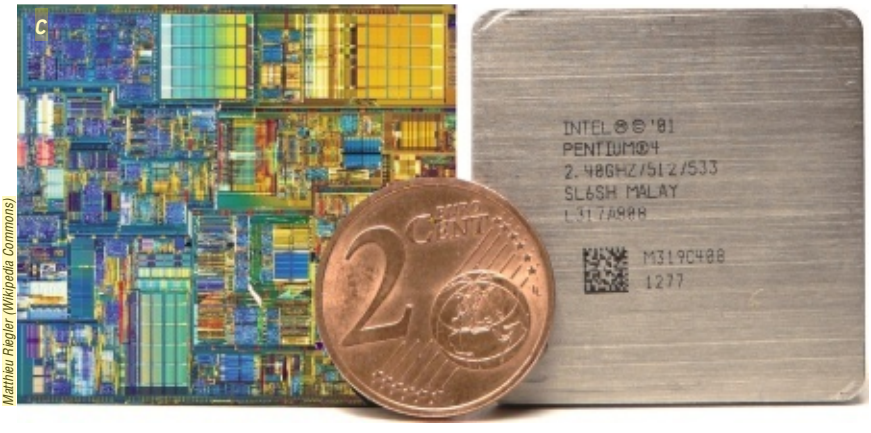
Assistant de preuve

Le premier travail de formalisation des mathématiques fut le projet *Automath* conçu et développé aux Pays-Bas à partir de 1966 par Nicolaas de Bruijn. Il fut suivi par une série de projets dont les plus avancés sont, en Pologne le projet *Mizar*, en Grande-Bretagne et aux États-Unis le projet *HOL-Isabelle* et, en France, le projet *Coq*.

L'idée est de mettre à la disposition du mathématicien un système informatique interactif et un formalisme de démonstration qui lui permettent d'élaborer une version formelle du résultat auquel il s'intéresse en dialoguant avec le logiciel *(voir la figure 4)*. Le logiciel libère le mathématicien d'une partie du fastidieux travail d'écriture et opère les contrôles minutieux nécessaires à



1. AVEC DES ASSISTANTS DE PREUVE, des erreurs auraient été évitées. Le 4 juin 1996, la fusée *Ariane 5* explosait 40 secondes après son décollage *(a)*. La catastrophe résultait d'une erreur de programmation. On peut colorier une carte, comme celle des régions de France, avec quatre couleurs seulement *(b)* : le « théorème des quatre couleurs » a été définitivement prouvé par un assistant de preuve, ce qui a mis fin à une controverse sur les premières démonstrations. Ces logiciels, qui aident à produire des démonstrations formalisées de théorèmes, sont aussi utilisés pour démontrer que certains circuits de microprocesseurs, dont le *Pentium 4 (c)*, fonctionnent correctement. La démarche est prudente, car, en octobre 1994, Thomas Nicely, de l'Université de Lynchburg (États-Unis), a dévoilé un dysfonctionnement dans l'unité de calcul en virgule flottante du *Pentium* : il s'est rendu compte que certaines opérations du processeur renvoyaient une valeur erronée par excès.



Matthieu Riegler (Wikipedia Commons)

2. Sphères empilées

Le travail d'écriture de preuves formelles en utilisant les assistants de preuve informatiques est parfois considéré avec méfiance et scepticisme. L'idée est que, pour peu que les démonstrations mathématiques soient écrites avec suffisamment de soin et contrôlées par des experts humains, on élimine tout risque d'erreur. Cette idée n'est plus défendable depuis que Thomas Hales a proposé une démonstration (non formelle) de la conjecture de Kepler, jugée impossible à contrôler par les experts à qui on l'avait confiée.

Cette conjecture affirme que l'empilement de sphères le plus dense est celui utilisé pour les boulets de canon ou les oranges : un réseau triangulaire de boulets est créé sur le sol plat ; on pose dessus un autre réseau analogue en exploitant les creux du premier et de même un troisième réseau, etc.

La démonstration de Th. Hales a été publiée par le prestigieux *Annals of Mathematics* en 2005 avec la mise en garde que, du fait de la complexité de la démonstration et de l'utilisation pour certaines de ses parties de programmes informatiques, le comité d'experts chargé de l'examiner ne pouvait pas en garantir l'exactitude. Devant cette situation inédite, Th. Hales a entrepris le projet de produire une preuve formelle (et donc mécaniquement vérifiable) de son théorème. Son programme de travail, qui pourrait occuper son équipe pour une durée de dix années ou plus avance régulièrement. Il a déjà donné lieu à deux doctorats de mathématiques et à la mise au point d'une preuve formelle d'un résultat à l'énoncé simple, mais dont la démonstration formelle posait des difficultés : le théorème de Jordan.

Celui-ci indique que lorsqu'on enlève les points d'une courbe plane continue et fermée qui ne se recoupe pas (une boucle), la partie du plan qui reste est composée de deux morceaux disjoints, chacun d'un seul tenant.

Les mathématiques donnent lieu à des démonstrations de plus en plus longues et difficiles et l'utilisation de preuves formalisées pourrait bien devenir routinière.

chaque étape de l'explicitation d'une démonstration formelle. Le logiciel stocke aussi les résultats démontrés formellement par d'autres mathématiciens lors de séances antérieures, et ces résultats sont utilisables pour des preuves nouvelles.

Pour mesurer le succès des logiciels assistants de preuve qui formalisent de vraies mathématiques, nous examinerons la liste des théorèmes centraux des mathématiques dont on a aujourd'hui réussi à produire une preuve formalisée qui en garantit de manière quasi absolue l'exactitude.

Imitant l'idée de la liste des 100 meilleures chansons, Nathan Kahn, mathématicien du *Steven Institute of Technology,* dans le New Jersey, a composé une liste des « 100 théorèmes mathématiques les plus importants ». Cette liste, subjective, a cependant été adoptée comme repère par les chercheurs qui mettent au point les logiciels de formalisation des mathématiques et elle permet d'en comparer les succès.

Formalisation de 85 théorèmes sur 100

Au cours du temps, le nombre des théorèmes que l'on a formalisés dans la liste de Kahn augmente et, aujourd'hui, on en est à 85 sur les 100 de sa liste.

Citons quelques-uns de ces théorèmes maintenant garantis par la machine.

– Irrationalité de la racine carrée de 2 : $\sqrt{2}$ n'est pas égal à un quotient de deux nombres entiers.

– Infinité des nombres premiers : la suite des nombres entiers n'ayant pas d'autres diviseurs que 1 et eux-mêmes est une suite infinie (2, 3, 5, 7, 11, 13,...).

– Impossibilité de la trisection d'un angle par une construction exacte menée avec seulement une règle et un compas.

– Théorème des quatre carrés de Lagrange : tout nombre entier s'écrit comme la somme de quatre carrés (par exemple $23 = 3^2+3^2+2^2+1$).

– Formule de Leibniz :
$\pi/4 = 1 - 1/3 + 1/5 - 1/7 + 1/9 - \ldots$

– Divergence de la série harmonique
$1 + 1/2 + 1/3 + 1/4 + \ldots$

– Théorème fondamental de l'algèbre : un polynôme de degré n à coefficients complexes possède n racines.

– Théorème fondamental de l'analyse : la dérivée de l'intégrale, prise entre une constante a et x, de la fonction continue f, est égale à $f(x)$.

– Transcendance de e : le nombre $e = 2{,}182818284590\ldots$ n'est racine d'aucun polynôme à coefficients entiers.

– Premier théorème d'incomplétude de Gödel : tout système formel non contradictoire pour l'arithmétique ou une théorie plus puissante laisse sans démonstration certains énoncés vrais.

– Théorème des nombres premiers par Hadamard et par de La Vallée Poussin : la densité des nombres premiers autour de n est $1/\log(n)$.

– Théorème des quatre couleurs : toute carte dessinée sur un plan peut être coloriée avec quatre couleurs de façon que deux pays voisins soient de couleurs différentes.

Ce dernier théorème est le plus difficile de tous ceux dont la démonstration a pu être contrôlée par la méthode de l'écriture complète d'une preuve formelle. La preuve formelle a été obtenue en 2004 par Georges Gonthier et Benjamin Werner avec le logiciel *Coq* de l'INRIA (Institut national de la recherche en informatique et automatique).

Précisons que ce théorème avait été démontré en 1976 en utilisant une démonstration comportant deux parties. Une partie de la preuve était informelle, c'est-à-dire exposée dans un texte en langue naturelle (l'anglais) comme le sont toutes les preuves mathématiques publiées dans les journaux et livres mathématiques. Une autre partie de la démonstration était un calcul mené par ordinateur, calcul trop long pour qu'on puisse le réaliser sans machine. La preuve de 1976 n'était en rien formalisée et elle pouvait parfaitement comporter des erreurs, soit dans la partie informelle, soit dans la partie informatique si les programmes utilisés étaient incorrects ou que la machine avait commis des erreurs.

Le travail consistant à prouver le théorème des quatre couleurs de façon formelle n'était donc pas du tout réglé d'avance ni même rendu plus facile par l'utilisation d'or-