

2. Sphères empilées

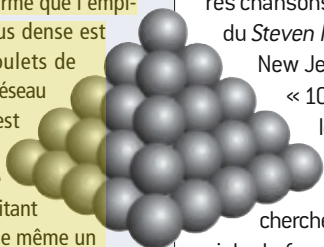
Le travail d'écriture de preuves formelles en utilisant les assistants de preuve informatiques est parfois considéré avec méfiance et scepticisme. L'idée est que, pour peu que les démonstrations mathématiques soient écrites avec suffisamment de soin et contrôlées par des experts humains, on élimine tout 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 meilleurs 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 : $\pi/4 = 1 - 1/3 + 1/5 - 1/7 + 1/9 - \dots$

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

– 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 $e = 2,7182818284590\dots$ 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-

dinateurs pour une partie de la preuve de 1976. Cette utilisation était en fait seulement l'indice que l'on avait affaire à un résultat particulièrement compliqué.

Notons aussi que le logiciel *Coq* est souple et adaptable à de nombreux problèmes, et que José Grimm de l'INRIA a pu grâce à lui entreprendre de formaliser les *Éléments de mathématique* de Bourbaki. L'idée n'est pas de suivre exactement le formalisme décrit dans le traité – nous avons vu que ce n'était pas envisageable –, mais de concevoir un formalisme équivalent permettant d'exprimer tous les résultats que l'on y trouve en même temps qu'on formalise le détail des preuves. En janvier 2011, une grande partie du livre I du traité de Bourbaki avait été formalisée.

Des théorèmes encore trop complexes

Parmi les 15 résultats de la liste des 100 théorèmes qui restent trop difficiles à formaliser aujourd'hui, même en utilisant des assistants de preuve, citons en deux.

– La transcendance du nombre π . C'est l'affirmation que π n'est racine d'aucun polynôme à coefficients entiers (ce résultat montre que l'antique problème de la quadrature du cercle est insoluble). Le théorème a été démontré par Lindemann en 1882 et on peut dire qu'il est à la limite de ce que peuvent faire les assistants de preuve actuels. Il est probable qu'il sera rapidement prouvé de manière formelle.

– Le théorème de Fermat-Wiles. C'est l'affirmation, démontrée en 1993 par Andrew Wiles, qu'il n'existe pas de solutions à l'équation $x^n + y^n = z^n$ où x, y, z sont des entiers positifs et n un entier fixé supérieur à 2.

Sa preuve est extrêmement difficile. Elle avait été recherchée pendant 350 ans et elle n'est vraiment comprise que par quelques spécialistes. En produire une version formelle serait intéressant.

Même si les erreurs sont fréquentes, le fait qu'une démonstration soit faite et refaite par de nombreux mathématiciens assure qu'aucun résultat classique n'est faux. Jamais dans les parties centrales des mathématiques une erreur grave n'est

restée longtemps cachée. Aussi le délicat, long et pénible travail de formalisation des mathématiques avec assistant informatique est-il vraiment utile ? La réponse est deux fois « oui ».

Vraiment utiles ?

Oui, la formalisation est utile, car certaines démonstrations récentes sont si longues que personne n'est entièrement persuadé de leur exactitude. C'est le cas du théorème de Thomas Hales qui résout la conjecture de Kepler concernant l'empilement optimal des sphères dans l'espace. Personne ne peut dire que la preuve de Hales a été contrôlée. Mener la vérification formelle d'une telle preuve n'est donc pas un luxe, mais une nécessité (voir la figure 2). La situation est pire encore dans le cas du théorème de classification des groupes simples, dont la première démonstration a été annoncée en 1983. Elle s'étend sur des dizaines d'articles mathématiques écrits par plus d'une centaine de mathématiciens différents et couvre un total de plus de 10 000 pages. Un trou important y a été découvert, qu'un complément de 1 300 pages est venu combler dans les années 1990. La seconde version de cette démonstration est en cours d'élaboration et s'étendra sur environ 5 000 pages. Bien qu'impossible à envisager dans l'immédiat, il est clair que seule la mise au point d'une preuve formelle sera susceptible de rassurer définitivement les mathématiciens qui, comme Jean-Pierre Serre, contestent l'affirmation que ce théorème « monstrueux » a été démontré.

Oui, la formalisation des démonstrations mathématiques est utile, car elle sert à certifier des logiciels ou des puces informatiques ainsi d'ailleurs qu'à y repérer des erreurs. Les « assistants de preuve » utilisés pour la mise au point des preuves formelles sont des outils puissants exploités par l'industrie du logiciel pour les morceaux de programme dont on veut avoir la certitude qu'ils font correctement certaines tâches cruciales. Aujourd'hui, assez peu de logiciels sont ainsi validés par la formalisation complète de la démonstration qu'ils font ce qu'on attend et rien d'autre, et de nombreuses autres méthodes de contrôle et de certification sont utilisées.

3. Démonstrations

Les démonstrations formelles sont peu lisibles et même souvent illisibles. Cela ne doit pas surprendre, car, sans qu'on ait toujours bien fait la distinction, les démonstrations mathématiques possèdent deux fonctions.

La première fonction d'une démonstration est de garantir que l'affirmation exprimée dans l'énoncé du théorème est exacte. C'est la fonction de certification.

La seconde fonction est de permettre au mathématicien de percevoir et de comprendre pourquoi les choses sont comme le théorème l'énonce. C'est la fonction didactique.

Lorsque les démonstrations ne sont pas trop compliquées, les deux fonctions peuvent être envisagées simultanément : le texte de la démonstration assure la validité de l'énoncé et, en même temps, il en explique les raisons profondes.

Lorsqu'on a affaire à des résultats vraiment difficiles, un double travail est nécessaire. La complexité dans le cas des mathématiques a donc pour conséquence la nécessité d'une part, de mener un contrôle formel (par l'utilisation des assistants de preuve), d'autre part de présenter un texte non formel illustré et largement commenté expliquant les idées mises en œuvre dans la démonstration.

C'est ce second texte qui permettra aux mathématiciens de saisir le sens du théorème... et d'imaginer le prochain théorème et la façon dont il faudra à son tour le démontrer.

