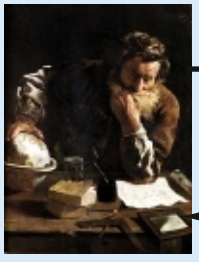
4. Les assistants de preuve

Un logiciel assistant de preuve est destiné à aider un mathématicien à écrire des démonstrations formelles lors de cessions de travail interactives. Pour ce faire, le mathématicien traducteur de la démonstration classique en démonstration formelle doit avoir une parfaite connaissance de la preuve, ce qui n'est pas facile dans le cas d'une démonstration complexe. De plus, la traduction est difficile et lente : un ou plusieurs jours par page.

La partie du programme informatique qui gère les interactions est longue et délicate et, de ce fait, peut comporter des erreurs. C'est sans importance, car la preuve produite à l'issue du dialogue sera vérifiée par le cœur du système, qui lui seul doit être correct. Cette partie centrale est courte et vérifiée de façon indépendante par plusieurs spécialistes. On utilise parfois un autre logiciel assistant de preuve pour démontrer que ce cœur fonctionne correctement. La petite taille des parties centrales, et le soin particulier à les vérifier et à les prouver n'annulent pas le risque d'erreur finale (et donc de validation de preuves erronées), mais réduisent de plusieurs ordres de grandeur ce risque. Avec la formalisation des preuves, on améliore donc sensiblement la garantie de justesse de ce qui est démontré.



Cependant on a là, venue des mathématiques et de la logique, une technique quasi définitive permettant d'assurer l'absence de bogues dans les parties clefs d'un programme ou d'un microprocesseur. En 1993, la firme *Intel* avait mis en circulation une puce qui commettait des erreurs arithmétiques ennuyeuses ; elle utilise aujourd'hui la méthode des assistants de preuve pour éviter que cela se reproduise.

Récemment dans un article du *New York Times*, Adi Shamir (le *S* du système de cryptage RSA) faisait remarquer que la présence d'une seule erreur dans une puce informatique largement utilisée mettrait en danger la sécurité de millions de machines ; elle rendrait peut-être manipulables frauduleusement toutes les transactions faussement sécurisées du commerce électronique.

Non seulement la présence d'erreurs dans les logiciels et les puces peut faire tomber la fusée *Ariane*, ce qui s'est produit le 4 juin 1996, mais elle peut aussi être à l'origine de problèmes économiques majeurs. Les difficultés qu'on a en mathématiques à garantir l'exactitude des longues démonstrations et les méthodes élaborées pour résoudre ce qui ne semblait devoir n'intéresser qu'une petite communauté de chercheurs se révèlent importantes pour tout le monde. C'est là un exemple nouveau et spectaculaire de l'utilité des théories abstraites, ici la logique mathématique.

Quelle certitude ?

Certains voient un paradoxe dans l'idée d'utiliser l'informatique pour contrôler des démonstrations mathématiques, car notre expérience des ordinateurs montre que loin d'être des outils fiables, ce sont des sources nouvelles et incontrôlables d'erreurs dont on ne comprend souvent pas l'origine : on redémarre sa machine et ça s'arrange (parfois...) sans que personne ne sache pourquoi. Comment, dès lors, croire que les preuves formelles par ordinateur sont plus sûres que les preuves informelles et humaines ?

La réponse est que les assistants de preuve reposent sur des noyaux logiciels, la partie qui mène le contrôle des preuves produites lors des séances de travail interactif, aussi petits que possible et que l'on contrôle minutieusement :

– En s'arrangeant pour que leur présentation soit la plus lisible et la plus simple possible, et en demandant ensuite à un nombre aussi grand que possible de spécialistes de relire ces programmes clefs.

– En testant ces noyaux logiciels sur de très nombreux exemples : si une erreur persistait, elle aurait très probablement des conséquences et aurait produit des effets visibles lors des essais.

– En démontrant formellement que ces noyaux logiciels sont corrects à l'aide de versions différentes du même noyau ou, mieux encore, avec d'autres assistants de preuve écrits par des groupes de chercheurs indépendants.

Bien sûr, on n'arrive pas à une certitude totale que le noyau de l'assistant de preuve est sans erreur, mais à une très faible probabilité qu'il en contienne. Tout le risque se concentre sur un petit nombre de lignes de programmes (moins de 500 dans le cas de l'assistant *HOL*) et sur lui seul. Au total, on a considérablement gagné en sûreté et sans doute réduit le risque d'erreur de plusieurs ordres de grandeur. De même que les théorèmes les plus anciens des mathématiques ayant été redémontrés (sans utiliser d'assistant de preuve) un grand nombre de fois ne contiennent certainement aucune

erreur, les noyaux des assistants de preuve gagnent en fiabilité de jour en jour. Toutes les autres preuves reposent sur eux, et l'on atteint donc une certitude de correction quasi absolue.

Les assistants de preuve ne seraient-ils pas susceptibles de changer notre façon de faire des mathématiques ? C'est l'idée du manifeste QED dont le nom vient de l'expression latine *Quod Erat Demonstrandum* (Ce qu'il fallait démontrer). Formulé en 1994 par des chercheurs qui ont souhaité rester anonymes, ce manifeste énonce l'objectif de mettre au point un assistant de preuve général pour toutes les mathématiques, de manière à garantir la totalité de tout ce qui se fait dans la discipline.

L'assistant de preuve envisagé serait à la fois puissant, fonctionnant avec un formalisme proche du langage qu'utilisent les mathématiciens, et évidemment serait aussi sûr que possible. Avec un tel assistant de preuve, on formaliserait toutes les mathématiques existantes et à chaque fois qu'un nouveau résultat serait proposé, le chercheur qui le soumettrait en donnerait une preuve formelle, ce qui dispenserait de le faire expertiser par d'autres chercheurs. La pratique de la recherche mathématique en serait transformée.

Aujourd'hui, cet assistant de preuve idéal n'existe pas. Les assistants de preuve actuels restent trop compliqués et les langages qu'ils utilisent souvent éloignés de celui pratiqué par les mathématiciens. Formaliser une preuve reste un énorme travail et il faut un ou plusieurs jours par page pour traduire une preuve classique d'un article mathématique en preuve formelle.

Tout cela fait que les chercheurs en mathématiques n'utilisent que très rarement les assistants de preuve disponibles et que la communication entre mathématiciens continue de fonctionner par échange de preuves informelles et sans processus de validation informatique. Le chemin menant à une nouvelle pratique des mathématiques n'est pas achevé et il n'est pas sûr qu'on atteindra l'idéal imaginé par le manifeste QED.

Toutefois, Henk Barendregt et Freek Wiedijk, deux spécialistes des preuves formelles, prédisent que le changement dans la recherche mathématique se produira dans la prochaine décennie.

Mentionnons encore deux points. Il n'est pas question de laisser à la machine l'initiative de la recherche mathématique : sauf dans des cas exceptionnels ou à propos de problèmes se réduisant à du calcul, les méthodes de recherche automatique de preuves ne trouvent que des résultats faciles et ne peuvent donc pas se substituer au mathématicien humain, qui reste la clef des découvertes.

Les assistants de preuve permettent d'accroître la sûreté des démonstrations, mais la fonction d'une démonstration, en particulier dans l'enseignement, est aussi de faire comprendre ce qui se passe mathématiquement dans l'univers des objets abstraits. Or les preuves formelles, désagréables à lire, entravent la compréhension plus qu'elles ne l'aident. Même si les objectifs du manifeste QED sont un jour atteints, on continuera d'écrire des preuves informelles, car ce sont elles qui font passer les idées d'un cerveau de mathématicien à un autre.

Prouver ainsi tous les résultats ?

D'ici quelques années, les assistants de preuve seront probablement en mesure de prouver l'ensemble des résultats mathématiques classiques.

Aujourd'hui, des théorèmes très difficiles ont pu être validés par la méthode des preuves formelles. C'est le cas du théorème des nombres premiers de Jacques Hadamard et Charles de La Vallée Poussin (qui précise la densité asymptotique des nombres premiers), dont deux démonstrations différentes ont été formalisées et validées.

Il n'en est pas de même pour des résultats plus avancés comme le grand théorème de Fermat, qui reste trop complexe pour les outils actuels. Mais F. Wiedijk et d'autres chercheurs du domaine considèrent que ce n'est qu'une question de moyens, et que même les plus difficiles des grands théorèmes sont maintenant à portée de main. ■

L'AUTEUR

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

BIBLIOGRAPHIE

F. Wiedijk, **Formalizing the « top 100 » of mathematical theorems**, 2011 : http://www.cs.ru.nl/~freek/100/

H. Geuvers, **Proof assistants : History, ideas and future**, *Sadhana*, vol. 34-1, pp. 3-25, février 2009 : http://www.ias.ac.in/sadhana/Pdf2009Feb/3.pdf

G. Gonthier, **The four-color theorem**, *Notices of the AMS*, vol. 55, n° 11, pp. 1382-1393, 2008.

Th. Hales, **A proof of the Kepler conjecture**, *Annals of Mathematics*, vol. 162, pp. 1065-1185, 2007.

F. Wiedijk, **Formal proof - Getting started**, *Notices of the AMS*, vol. 55, n° 11, pp. 1408-1414, 2008.

Th. Hales, **Formal proof**, *Notices of the AMS*, vol. 55, n° 11, pp. 1370-1380, 2008.

F. Wiedijk, **The QED manifesto revisited**, *Studies in Logic, Grammar and Rhetoric*, vol. 10(23), pp. 121-133, 2007.

F. Wiedijk (éd.), **The Seventeen Provers of the World**, Springer, 2006.