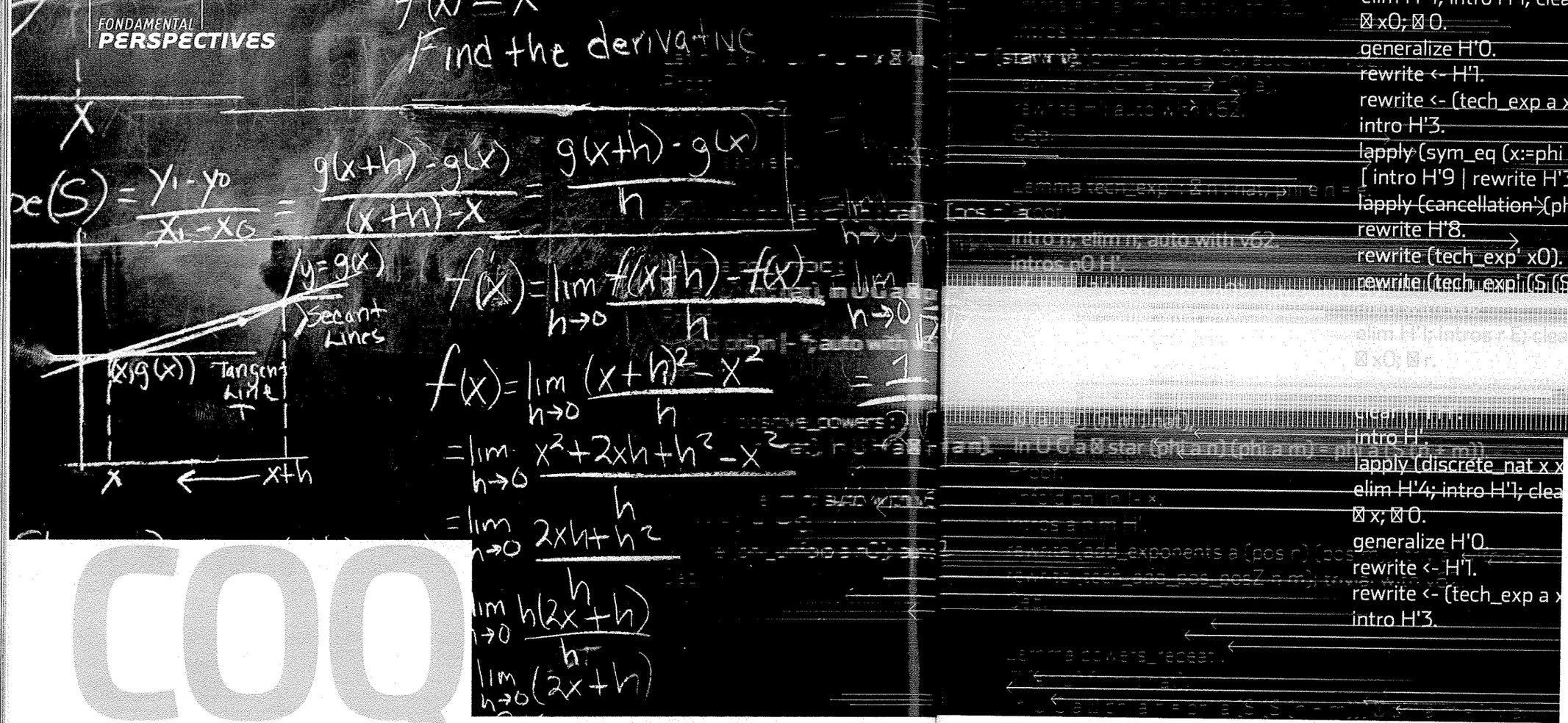


COQ LES MATHS ONT TROUVÉ LEUR MAÎTRE

Pour qu'un théorème soit juste, il faut qu'il soit démontré. Ce qui nécessite des dizaines et des dizaines de pages de raisonnement… qu'un logiciel, baptisé Coq, permet aujourd'hui de vérifier automatiquement et, surtout, de valider, sans erreur possible. De quoi révolutionner les maths !

PAR PHILIPPE PAJOT

Vingt septembre 2012. La dizaine d'informaticiens œuvrant autour de Georges Gonthier, au centre de recherche commun Inria-Microsoft de Saclay, termine l'écriture du dernier programme. A l'ordinateur de jouer maintenant. Celui-ci assemble les milliers de briques informatiques déjà écrites, les passe en revue une à une et, en moins de cinq secondes, donne son verdict final : tous les voyants passent au vert. L'opération est un succès ! Au terme de six ans d'efforts, l'équipe a conçu un programme informatique qui vérifie chacune des étapes du raisonnement permettant de démontrer un théorème. En l'occurrence, pas n'importe quel théorème : celui de Feit-Thompson, dont la démonstration, longue et complexe, est l'un des résultats phares de l'algèbre du XXe siècle. Et voici qu'un ordinateur prouve que cette démonstration est bel et bien valide ! Impossible, désormais, de la mettre en doute. L'exploit a été salué comme un jalon décisif dans les méthodes de vérification des preuves. Surtout, au-delà de la simple prouesse, il présage une façon radicalement nouvelle de faire des mathématiques…

Mais pourquoi demander à une machine de vérifier le travail de mathématiciens ? Simple : les maths sont le fruit de raisonnements humains qui sont, par définition, faillibles, puisque s'y mêle une part d'intuition. Et même si la suite de raisonnements logiques permettant d'affirmer un résultat peut être explicitée de manière exhaustive, personne ne le fait, ce qui laisse une part de non-dit et d'interprétation à toute démonstration. Il suffit de regarder la preuve présentée en septembre dernier de la "conjecture abc", un important résultat qui généralise notamment le théorème de Fermat : le Japonais Shinichi Mochizuki ayant travaillé seul pendant douze ans, aucun autre mathématicien ne peut juger du bien-fondé de cette démonstration en 500 pages bien tassées.

CORBIS - GETTY

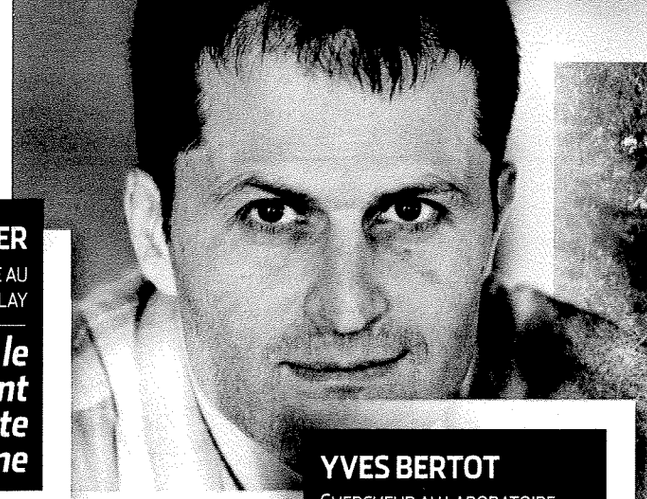
UNE IDÉE QUI DATE DE 30 ANS

C'est justement ici qu'entrent en scène les informaticiens : il y a trente ans, ils ont imaginé un moyen de s'assurer qu'il n'y a pas d'erreur ni de trou dans de tels raisonnements, aussi longs et complexes soient-ils. Tout commence lorsque, dans les années 1980, Gérard Huet et Thierry Coquand, alors à l'Institut national de recherche en informatique et en automatique (Inria), élaborent une méthode de traduction de toute démonstration en calculs. Bien que difficile à mettre en œuvre, cette méthode permet de développer un logiciel baptisé "Coq", en référence au "calcul des constructions" (CoC) à partir duquel il est construit, mais également au nom d'un de ses fondateurs (Coquand) et à sa nationalité (française). Coq est un "assistant de preuve" : il guide pas à pas la transcription de toutes les étapes d'un raisonnement mathématique en un programme informatique ; une fois la transcription achevée, il suffit de lancer le programme pour vérifier mécaniquement la justesse du raisonnement d'origine (voir *S&V* n° 1013, p. 55).

Aujourd'hui, il existe différents assistants de preuve : HOL-Light, Isabelle, Mizar… Coq, lui, en est à sa huitième version ! Enseigné dans plusieurs universités en Europe et aux Etats-Unis, il a déjà certifié des dizaines de démonstrations. Mais sa mise en œuvre est si fastidieuse que les théorèmes concernés sont longtemps restés assez élémentaires. Avec celui de Feit-Thompson, →

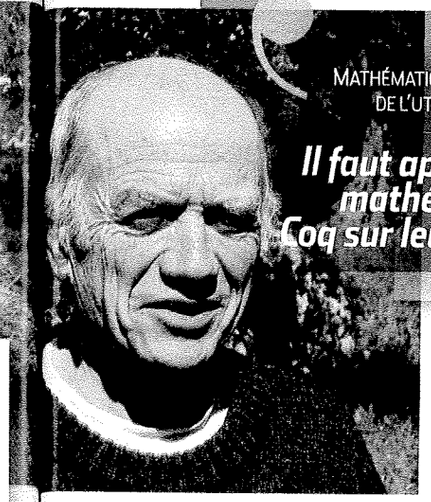
GEORGES GONTHIER
CHERCHEUR EN INFORMATIQUE AU CENTRE INRIA-MICROSOFT DE SACLAY

Nos travaux avec le logiciel Coq couvrent pratiquement toute l'algèbre moderne



YVES BERTOT
CHERCHEUR AU LABORATOIRE INRIA DE SOPHIA-ANTIPOLIS

Coq nous a permis de valider un résultat majeur du XXe siècle



ANDRÉ HIRSCHOWITZ
MATHÉMATICIEN À L'UNIVERSITÉ DE NICE, PIONNIER DE L'UTILISATION DES ASSISTANTS DE PREUVE

Il faut apprendre aux jeunes mathématiciens à utiliser Coq sur leurs propres travaux

CÉDRIC VILLANI
MATHÉMATICIEN, DIRECTEUR DE L'INSTITUT HENRI-POINCARÉ À PARIS

Cela devrait changer la manière de travailler des mathématiciens

→ Coq vient de passer dans une dimension supérieure.

Georges Gonthier n'en est pas à son coup d'essai. En 2005, il avait déjà vérifié un autre problème célèbre, le théorème des quatre couleurs, qui stipule qu'il est possible de colorier toute carte découpée en régions avec seulement quatre couleurs, de telle sorte que deux régions adjacentes soient toujours de couleurs différentes (voir *S&V* n° 1056, p. 90). Mais les chercheurs voulaient aller plus loin et attaquer un "vrai" problème mathématique. *"Le théorème des quatre couleurs était un problème difficile, mais pas très intéressant sur le plan des mathématiques*, souligne Georges Gonthier. *La plupart des outils utilisés dans la preuve ne font pas partie du bagage habituel des matheux."*

250 PAGES DE DÉMONSTRATION

Mais où choisir un théorème reconnu comme ardu et utilisant une grande variété de notions de haut niveau ? Finalement, le choix s'est arrêté sur l'algèbre, c'est-à-dire l'étude des équations et, plus généralement, de toutes les structures algébriques, comme les "groupes", une notion centrale des mathématiques modernes. Dans la théorie des groupes, la classification de ceux ayant un nombre fini d'éléments a été un travail monumental qui s'est étendu de 1955 à 1983, rassemblant des centaines de mathématiciens dans le monde. Et le théorème de Feit-Thompson est en quelque sorte la pierre angulaire de ce travail (voir "Repère").

Lorsque le théorème fut publié en 1963 par les Américains Walter Feit et John Thompson, sa démonstration en 250 pages était si complexe que, dans les livres de l'époque, les résultats qui en découlaient étaient notés avec un astérisque, au cas où le raisonnement serait finalement faux… Même si la dernière version de la preuve, publiée en 1995 et 2000, a été corrigée, simplifiée, et que sa validité n'est plus mise en doute, il y avait là une démonstration qui permettrait de montrer le potentiel des assistants de preuve.

Lorsque les informaticiens se sont attaqués à cette montagne, en 2006, très peu de mathématiques avaient été formalisées. *"La plus grosse partie du travail a consisté à traduire en un programme vérifiable toutes les théories sur lesquelles la démonstration s'appuie. Et avec Feit-Thompson, cela couvre pratiquement toutes les bases de l'algèbre moderne, en gros tout ce qu'un étudiant de fin de licence doit savoir dans ce domaine"*, raconte Georges Gonthier. Son collègue Laurent Théry résume à sa manière le travail accompli pendant ces six années : *"Nombre de lignes : environ 170 000 ; nombre de définitions : environ 15 000 ; nombre de théorèmes : environ 4 200 ; plaisir : énorme !"*

Assez pour convaincre les mathématiciens que leurs raisonnements seront bientôt validés automatiquement par des assistants informatiques ? André Hirschowitz, de l'université de Nice, l'un des pionniers de l'utilisation des assistants de preuve, pense que l'heure a sonné : *"Si l'on veut que des mathématiciens adoptent ce logiciel, il faut aller chercher des jeunes spécialistes de la théorie des groupes, par exemple, puisque Coq est en pointe sur ce sujet, et leur apprendre à utiliser Coq sur leurs propres mathématiques."* Yves Bertot, membre de l'équipe de vérification, au laboratoire Inria de Sophia-Antipolis, est plus patient : *"Le côté positif, c'est que nous avons vérifié un théorème reconnu comme un résultat majeur du XXe siècle ; mais cela a demandé plusieurs années de préparation, de sorte qu'il y a encore peu de mathématiciens qui pensent que cet outil puisse les aider au quotidien."*

REPÈRE

Le ***théorème de Feit-Thompson*** énonce que tout groupe d'ordre impair est résoluble. Sachant qu'un groupe est une structure mathématique, que son ordre désigne son nombre d'éléments et qu'il est résoluble s'il peut être décomposé en une série de groupes cycliques, ce théorème stipule que l'étude de ces groupes est relativement simple à mener.

UNE SCIENCE PROMETTEUSE

Pour que le mouvement s'enclenche, d'autres parties des mathématiques doivent encore être traduites en langage informatique. *"Une première étape, qui semble réalisable d'ici quelques années, serait d'entrer dans Coq toutes les mathématiques enseignées dans les trois années de licence*, poursuit l'informaticien. *Grâce aux travaux autour de Feit-Thompson, c'est quasiment fait pour l'algèbre. Du côté de l'analyse, de la topologie ou de la géométrie, il ne devrait pas y avoir de problème insurmontable."* Le projet européen ForMath, porté par Thierry Coquand, s'attaque par exemple à des questions d'analyse.

Même s'il reste encore du travail pour que Coq devienne aussi simple et naturel qu'une calculatrice graphique moderne, ces bibliothèques de théorèmes vérifiés favorisent l'émergence d'une communauté de mathématiciens qui utiliseront Coq ou d'autres systèmes de manière routinière. Georges Gonthier réfléchit ainsi à la façon de présenter une théorie mathématique comme une brique autonome, utilisable pour construire d'autres théories, en s'inspirant des composants logiciels que les informaticiens utilisent pour construire de nouveaux programmes. De gros efforts sont aussi consacrés aux fonctionnalités et à l'interface, afin de diminuer la distance entre le raisonnement humain et les détails que la machine peut vérifier.

Cédric Villani, médaille Fields et directeur de l'Institut Henri-Poincaré, est convaincu de l'importance que va prendre cette science de la vérification automatique dans les décennies à venir : *"Les mathématiciens seront capables de vérifier des théorèmes de plus en plus complexes, s'assurant qu'ils sont exempts d'erreurs, même quand les démonstrations sont longues de plusieurs milliers de pages. Cela devrait changer leur manière de travailler."*

Et l'on se prend à imaginer un futur où l'assistant de preuve deviendra un outil aussi banal qu'une calculatrice. Où la publication d'un nouveau résultat consistera à le faire valider par un assistant de preuve. Et où un mathématicien pourra pianoter sur son ordinateur une vague intuition que la machine transformera en théorème. *"Les mathématiciens qui ont les idées les plus créatrices doivent garder cette liberté, tout en utilisant le support de rigueur qu'est l'ordinateur le plus vite possible dès qu'ils ont une ébauche d'idée"*, estime Yves Bertot. Une idée que partage l'informaticien Serge Abiteboul, de l'Inria : *"On peut imaginer des outils qui aideront les mathématiciens en vérifiant leurs hypothèses, en proposant des pistes, en développant des preuves formelles. Le mathématicien serait libéré de la partie fastidieuse des démonstrations."* Des mathématiques non fastidieuses ? Le rêve. ■

DR - C.LEBEDINSKY/INRIA - DR - O.ROLLER

* EN SAVOIR PLUS

La vérification par Coq de la démonstration du théorème de Feit-Thompson est accessible en ligne : http://ssr2.msr-inria.inria.fr/~jenkins/current/progress.html