UN CLASSIQUE REVISITÉ

Rêvée par Alan Turing dans les années 40, développée par des spécialistes de logique mathématique, *boostée* par l'essor de l'informatique, la science de la vérification automatique poursuit son impressionnante avancée, partout où il importe de tester la rigueur d'un agencement logique complexe : puces électroniques, programmes informatiques, preuves mathématiques...

Régulièrement l'Institut national de recherche en informatique et automatique (Inria) présente des avancées fortes dans ce domaine : après la validation du controversé Théorème des Quatre Couleurs, puis le compilateur C certifié "sans bug" par l'équipe de Xavier Leroy, c'était, voici deux semaines à peine, la validation de la preuve d'un théorème célèbre du XX^{e} siècle, le Théorème de Thompson–Feit.

Pour comprendre l'importance symbolique de cette validation, replaçons le théorème dans son contexte. Née au XIX^{e} siècle avec Abel et Galois pour résoudre les équations polynomiales, la notion de groupe est la plus fondamentale des structures de l'algèbre. Un groupe est défini par une opération réversible, comme l'addition des entiers, la composition de rotations, etc. Les groupes sont associés aux symétries, que l'on trouve partout en mathématique, mais aussi dans la physique des particules élémentaires, dans la chimie des cristaux, etc.

Un exemple simplissime est le groupe des restes modulo 2 : seulement 2 éléments, à savoir les restes dans la division par 2 (0 pour pair, 1 pour impair), et les règles pair + pair = pair, pair + impair = impair, impair + impair = pair. On peut de même considérer des groupes de restes modulo n, avec un nombre n arbitraire d'éléments.

Il existe beaucoup d'autres familles de groupes finis (groupes de Conway, de Chevalley, etc.) Peut-on en dresser une classification exhaustive ? En 1954, Thompson & Feit font sensation en prouvant un théorème aussi simple à énoncer, que compliqué à démontrer (250 pages !) : tout groupe contenant un nombre impair d'éléments se décompose comme un produit de groupes de restes modulo n. C'était la première brique de la classification des groupes finis, monument de plus de 10 000 pages réparties dans des centaines d'articles. La validité de cette preuve titanesque est régulièrement mise en doute; on a d'ailleurs éprouvé le besoin de publier en 2000 une preuve révisée du Théorème de Thompson–Feit.

Ce sujet emblématique, complexe et controversé, était un terrain idéal pour les outils de vérification de preuve comme le langage Coq. Georges Gonthier, qui s'est déjà illustré dans le Théorème des Quatre Couleurs, se lance donc en 2006, avec son équipe mixte Microsoft–Inria, dans la validation informatique du Théorème de Thompson–Feit. Personne n'a jamais tenté de vérifier informatiquement une preuve aussi complexe. Comme on pouvait le craindre, des erreurs sont rapidement repérées... elles s'avèrent sans gravité. Six ans plus tard, la preuve est complètement validée par l'oracle de silicium. Nul ne pourra plus jamais la mettre en doute !

Cédric Villani, Professeur de l'Université de Lyon, Directeur de l'Institut Henri Poincaré (CNRS/UPMC)
— Carte blanche du supplément *Sciences & Technologie* du Monde, 2 novembre 2012