Retour sur « Que vaut une preuve assistée par ordinateur ? »

Par André Boileau, Professeur retraité, UQAM

Dans sa chronique de mars dernier [1], Jean-Philippe Villeneuve nous a posé la question suivante : que vaut une preuve assistée par ordinateur? Cette chronique a le mérite de poser plusieurs questions intéressantes, mais les éléments de réponses fournis sont parfois discutables, en ce sens qu'ils m'ont amené à proposer des réponses différentes.

Ainsi, prenons la question « comment être certain de ce calcul produit par un outil technologique, s'il ne peut pas être calculé à la main? » Ce qui est sous-entendu ici, me semble-t-il, c'est que le calcul à la main apporte un degré de certitude supérieur à un calcul par une machine. Cette impression semble d'ailleurs confirmée quand, plus loin, on affirme que les connaissances mathématiques doivent être indépendantes de l'expérience et que « l'utilisation de circuits électroniques lie le calcul à une expérience physique ». Comme si les circuits neuronaux humains ne constituaient pas une expérience physique!

D'ailleurs, la triste histoire de William Shanks [2], qui consacra 15 années de sa vie à calculer les 707 premières décimales du nombre π, illustre bien que les calculs à la main sont loin de constituer une panacée. En effet, Ferguson découvrit 70 ans plus tard, en utilisant une calculatrice mécanique, que seules les 527 premières décimales de Shanks étaient correctes. D'ailleurs [3], tous les calculs subséquents de nouvelles décimales de π ont été réalisés à l'aide de machines.

Une autre question soulevée par Villeneuve est « qu'est-ce qu'une preuve? ». Est-ce « un argument dont l'objectif est de convaincre » (Wittgenstein), ou encore doit-elle être « révisable par un mathématicien et formalisable » (Tymoczko) ? Notons au passage la subjectivité de ces points de vue. Qui au juste une preuve doit-elle convaincre : un quidam dans la rue, tous les mathématiciens, ou quelques mathématiciens spécialistes dans le domaine ? Et l'histoire donne plusieurs exemples de preuves erronées produites par des mathématiciens, parfois même parmi les plus grands : preuves fausses de Kempe et de Tait du théorème des quatre couleurs [4], conclusions erronées de Poincaré sur le problème des trois corps [5] et [6], preuve initiale de Wiles du dernier théorème de Fermat [7] et [8], etc. Une révision par un (ou même plusieurs) mathématicien(s) ne nous met donc pas nécessairement à l'abri d'erreurs…

Bien entendu, ces points de vue recèlent aussi leur part de sagesse. Pour un mathématicien, une « bonne » preuve non seulement convainc, mais fait comprendre le phénomène étudié. Qui d'entre nous n'a pas tenté de reformuler une preuve (trouvée par nous ou produite par quelqu'un d'autre) pour voir plus clairement ce qui se passe, pour ressentir cette illumination face à l'énoncé à démontrer. Malheureusement, notre expérience nous montre qu'il n'est pas toujours possible de trouver une preuve aussi simple et aussi éclairante qu'on le voudrait. On peut se demander si ceci ne reflète qu'une myopie temporaire et qu'on finira par trouver une preuve ayant les caractéristiques voulues, ou si cela ne correspond pas plutôt à une difficulté fondamentale liée à la nature même des mathématiques.

Pour tenter de répondre un tant soit peu à cette dernière question, je vais adopter un point de vue plus interne aux mathématiques. Les logiciens ont défini très explicitement le concept de preuve formelle d'un résultat ψ : c'est une suite de formules, dans le langage associé à une théorie donnée, de telle sorte que la dernière de ces formules est le résultat ψ et chaque formule de la suite est soit un axiome, soit une formule obtenue en appliquant une règle logique à des formules la précédant dans la suite. On peut décrire le tout de façon encore plus précise, à tel point qu'on peut alors programmer un ordinateur pour décider si une suite de formules donnée est une preuve ou pas.

On a donc ainsi transformé le concept intuitif de preuve en un objet formel. On imagine qu'on perd beaucoup du côté intuitif, mais on gagne aussi, car on peut maintenant étudier de façon mathématique le concept de preuve. Dans ce contexte, Kurt Gödel a pu démontrer un théorème dit de **complétude**, que l'on peut énoncer ainsi pour la théorie des groupes

> Il existe une preuve formelle d'un énoncé ψ de la théorie des groupes si et seulement si l'énoncé ψ est vérifié dans tous les modèles de la théorie des groupes (c.-à.-d dans tous les groupes).

et qui reste vrai pour toutes les théories

> Il existe une preuve formelle d'un énoncé ψ d'une théorie donnée si et seulement si l'énoncé ψ est vérifié dans tous les modèles de cette théorie.

Ce théorème est remarquable en ce qu'il nous assure que si un énoncé est vrai (c.-à.-d. vérifié dans tous les modèles d'une théorie), alors on peut en trouver une preuve formelle.

De même, Gödel a montré un théorème dit d'**incomplétude**, qui dit essentiellement que toute théorie assez complexe pour « inclure » l'arithmétique est indécidable dans le sens suivant : il est impossible de programmer un ordinateur[1] pour qu'il puisse décider, pour toute formule ψ de notre théorie, si cette formule est prouvable ou pas. Par contre, on peut imaginer l'algorithme suivant : on énumère systématiquement toutes les preuves formelles[2], et on déclare notre formule prouvable dès qu'une preuve de ψ est trouvée. L'indécidabilité viendra du fait que, parfois, il n'existera pas de preuve de ψ et que notre algorithme continuera sans jamais s'arrêter, et donc sans jamais donner de réponse.

Un corollaire intéressant du théorème d'incomplétude est le suivant : dans le cas d'une théorie assez complexe pour « inclure » l'arithmétique, il n'existe pas de fonction f calculable par ordinateur vérifiant

> si une formule ψ de longueur n est prouvable,
> alors il existe une preuve de longueur $< f(n)$.

En effet, si par hypothèse une telle fonction existait, elle permettrait à notre algorithme précédent de s'arrêter et de conclure que notre formule n'est pas prouvable dès que toutes les preuves formelles de longueur $< f(n)$ ont été examinées sans qu'une preuve soit trouvée, ce qui contredit le théorème d'incomplétude.

---

[1] Il s'agit ici d'ordinateurs théoriques, qui ont une mémoire illimitée et qui disposent d'un temps illimité pour leurs calculs.

[2] Bien entendu, un tel algorithme est très inefficace. Mais on s'intéresse ici seulement à l'existence ou non de tels algorithmes.

Appliquons ceci à un cas particulier en choisissant une fonction calculable f qui croît très rapidement

$$f(n) = n^{n^{\cdot^{\cdot^{\cdot^{n^n}}}}} \Big\}n \text{ niveaux}$$

et une théorie permettant de parler de coloriage des cartes, par exemple la théorie des graphes. Comme cette théorie est assez complexe pour « inclure » l'arithmétique, le corollaire précédent nous assure qu'il existe une formule prouvable ψ de longueur *n* telle que la preuve de longueur minimale de ψ est au moins de longueur f(*n*).

En d'autres mots : il existe des formules prouvables dont les preuves « minimales » sont énormément plus longues que lesdites formules! Bien entendu, il s'agit là d'un résultat purement existentiel, qui ne dit rien de la nature de telles formules. Mais il serait quand même étonnant d'imaginer que **toutes** les formules nous apparaissant intéressantes et pertinentes admettent des preuves courtes…

Quoi qu'il en soit, les mathématiciens rencontrent de plus en plus d'énoncés relativement courts dont les seules preuves connues sont très très longues. Il m'apparaît souhaitable de continuer à chercher de nouvelles preuves plus courtes et plus éclairantes de ces énoncés, mais, face au résultat que nous venons de décrire, il est loin d'être certain que nous réussirons toujours à en trouver.

Alors, que devons-nous faire? Je crois que l'ordinateur peut nous être d'un grand secours dans notre recherche de preuves. Oui, tout système physique peut avoir des défaillances, qu'il s'agisse d'ordinateurs ou d'humains. Mais on peut (en partie) remédier à ceci en vérifiant de plusieurs façons et avec plusieurs ordinateurs ou plusieurs humains. Oui, il peut y avoir des pépins dans la conception des circuits et les logiciels utilisés : après tout, ces circuits et ces logiciels ont été conçus par des humains, tout comme les preuves mathématiques d'ailleurs. Encore là, ces circuits et ces logiciels, tout comme ces preuves, peuvent être vérifiés et contre-vérifiés.

J'aimerais cependant contester l'affirmation « chacun des cas doit être vérifié ». Je crois que ce sont plutôt les algorithmes, et non le détail de leur exécution, qui doivent être vérifiés. Et comme ces algorithmes ont été écrits par des humains, il devrait être possible à d'autres humains de les vérifier. Prenons le calcul des décimales de π comme exemple : dans ce cas, nous devrions vérifier que la formule utilisée pour le calcul est correcte, et que les ressources informatiques utilisées pour les calculs (c.-à.-d. le calcul à précision multiple) ont été bien implantées. Mais on ne devrait certainement pas vérifier le détail arithmétique de tous les calculs : comme nous le montre l'exemple de Shanks, l'humain risquerait beaucoup plus de se tromper que la machine.

En terminant, un peu de *mathématique fiction*… Dans un avenir plus ou moins éloigné, imaginons qu'on arrive à créer des programmes informatiques permettant aux ordinateurs de prouver, sans intervention humaine, des résultats mathématiques qu'aucun humain n'a jamais réussi à établir. Certaines de ces preuves pourraient même être incompréhensibles aux humains, en raison de leur complexité. La situation serait alors comparable au jeu

d'échecs, où les meilleurs programmes battent actuellement les meilleurs joueurs humains. Même si je trouve que cette perspective est loin d'être réjouissante, je vois mal les mathématiciens ignorer ou rejeter complètement les résultats obtenus par les machines : ils tenteraient plutôt de les comprendre du mieux qu'ils peuvent. Tout comptes faits, ils se comporteraient comme plusieurs d'entre nous actuellement face à certains résultats dans des domaines où nous ne sommes pas spécialistes et dans le cas de preuves particulièrement complexes (théorème des quatre couleurs, dernier théorème de Fermat, classification des groupes finis, conjecture de Poincaré, etc.), à la différence que ces résultats ont été prouvés par des humains (bien que parfois aidés de machines)…

Références

[1] Jean-Philippe Villeneuve, La banalité des outils technologiques : que vaut une preuve assistée par ordinateur?, *Bulletin AMQ*, Vol LV, n° 1, pp 56-59, mars 2015.

[2] « William Shanks », article de l'encyclopédie *Wikipedia*, consulté le 21 mars 2015.

[3] « Chronology of computation of π », article de l'encyclopédie *Wikipedia*, consulté le 21 mars 2015.

[4] « Théorème des quatre couleurs », article de l'encyclopédie *Wikipedia*, consulté le 21 mars 2015.

[5] Diacu, Florin, Henri Poincaré et la découverte du chaos, *Bulletin AMQ*, Vol LIII, n° 2, mai 2013.

[6] Cédric Villani, La meilleure et la pire des erreurs de Poincaré, *Conférence donnée à l'Université de Lille1*, septembre 2012. Vidéo disponible à l'adresse suivante : http://lille1tv.univ-lille1.fr/tags/video.aspx?id=6844d847-df95-4808-adeb-c3b51241dbbd

[7] « Andrew Wiles », article de l'encyclopédie *Wikipedia*, consulté le 21 mars 2015.

[8] Simon Singh, Le dernier théorème de Fermat, Documentaire *BBC*, 1997. Vidéo disponible à l'adresse suivante : http://www.dailymotion.com/video/xmr2gr_simon-singh-le-dernier-theoreme-de-fermat-d-t-f_creation