

Les ordinateurs mathématiciens !

JEAN-PAUL DELAHAYE

Après le jeu d'échecs, l'intelligence artificielle triomphera-t-elle des mathématiques ?

Il y a 40 ans que les calculatrices ont supplanté l'homme pour les calculs numériques. En revanche, c'est seulement depuis une dizaine d'années que le calcul symbolique par ordinateur (dérivation des fonctions, recherche de primitives, manipulation de polynômes, développements limités, etc.) a atteint une maturité qui en fait un allié de première importance dans certains domaines mathématiques et une aide appréciée des ingénieurs. La nouvelle formule de calcul de π , que nous avons traitée en janvier 1997, était un exemple frappant de cette avancée et des résultats produits par le calcul symbolique en mathématiques.

Un domaine mathématique subsiste où les progrès de la science informatique sont peu spectaculaires : la recherche de démonstrations par ordinateur.

Distinguons deux types de démonstrations mathématiques : celles qui ne sont que le développement de longs calculs (numériques ou symboliques) et celles qu'on obtient avec des méthodes où les raisonnements prédominent.

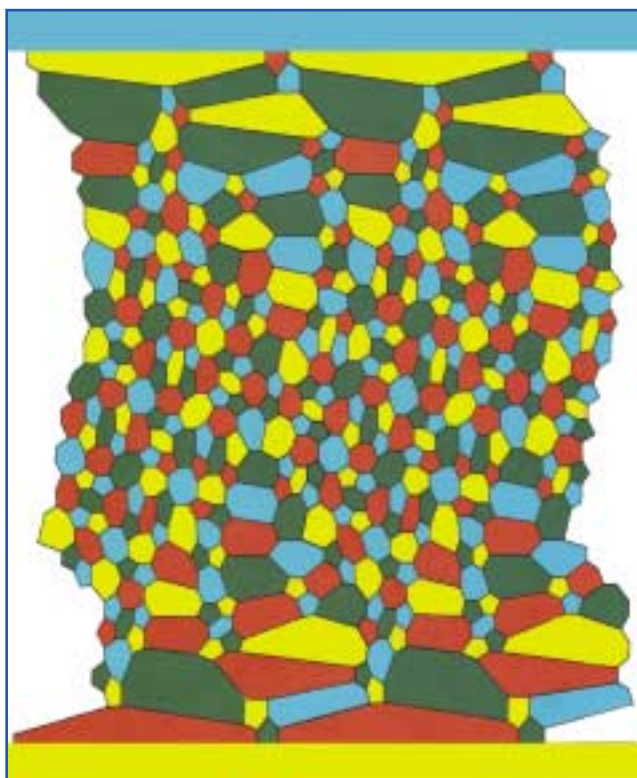
Pour le second type de démonstration, l'apport de l'informatique n'est pas convaincant : rares sont les énigmes anciennes intéressant vraiment les mathématiciens dont la réso-

lution a été obtenue par une démonstration automatique d'ordinateur.

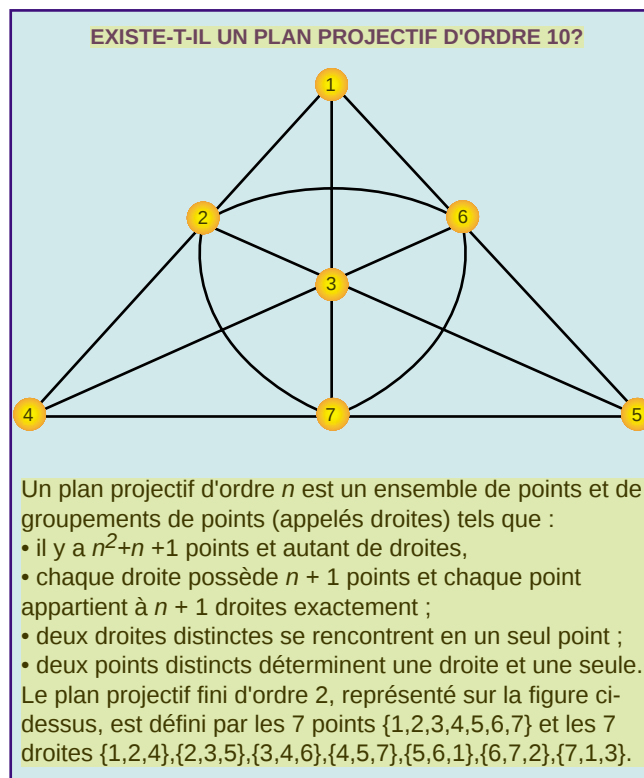
LE THÉORÈME DES QUATRE COULEURS

On cite fréquemment le théorème des quatre couleurs : avec quatre couleurs, on peut toujours colorier les pays d'une carte géographique sans que deux voisins portent des couleurs identiques. Ce résultat, conjecturé en 1852 par Francis Guthrie, ne fut démontré qu'en juin 1976 par Kenneth Appel et Wolfgang Haken à l'aide d'un calcul par ordinateur. Toutefois, les idées et la structure de la démonstration étaient dues aux mathématiciens qui, pendant plus d'un siècle, avaient travaillé sur le problème. L'ordinateur, en 1976, s'est chargé d'un travail de recherche et de vérification trop long pour être mené à la main par un humain, mais qu'on peut difficilement considérer comme un raisonnement et encore moins comme un raisonnement créatif. L'ordinateur, dans la démonstration du théorème des quatre couleurs, quoique irremplaçable, n'a été qu'un assistant fiable et obstiné.

La preuve de K. Appel et W. Haken n'a jamais été vérifiée à la main. En fait, elle n'avait pas été vérifiée du tout, car, pour le faire par machine, il fallait saisir la description de 1 476 graphes



1. Illustration du problème des quatre couleurs résolu par ordinateur en 1976 et vérifié en 1996: peut-on colorier toute carte de façon que deux pays contigus n'aient pas la même couleur ?



2. Les mathématiciens ne pouvaient déterminer s'il existait un plan projectif d'ordre 10. Cette inexistence a été démontrée en 1988 sur un ordinateur programmé par C. Lam, L. Thiel et S. Swiercz.

assez compliqués, ce qui, à cause du risque considérable d'erreurs et de la stupidité de cette étape de travail, n'a pas été tenté.

Neil Robertson, Daniel Sanders, Paul Seymour et Robin Thomas entreprirent, il y a quelques mois, de trouver une nouvelle preuve du théorème des quatre couleurs, afin de tranquilliser les mathématiciens qui niaient l'authenticité de la démonstration : en mathématiques, un résultat démontré une seule fois – par un humain ou par un ordinateur – reste incertain.

Après quelques mois de travail, l'équipe réunie autour de W. Robertson et leur ordinateur découvrirent une nouvelle preuve, plus courte que la précédente. Elle utilise un ensemble de 633 graphes, dont l'un au moins serait présent dans un contre-exemple au théorème des quatre couleurs, s'il en existait.

La méthode est en gros la même que celle de 1976, et la nouvelle preuve est encore impossible à vérifier à la main. Toutefois, avoir trouvé deux preuves différentes du théorème devrait rassurer les mathématiciens soupçonneux. De plus, puisque la nouvelle preuve est plus courte, elle sera aussi plus facile à vérifier; d'autant qu'un effort a été fait pour rendre disponibles les données nécessaires à la vérification sous une forme commode à manipuler et accessible à tous par *Internet*.

La communication généralisée des ordinateurs facilite l'échange des données et, donc, la vérification de ce type de résultats par d'autres équipes, tâche autrefois presque impossible.

LE PLAN PROJECTIF D'ORDRE 10

Un second exemple de résultat souvent mentionné comme une réussite des ordinateurs en mathématiques est la preuve qu'il n'existe pas de plan projectif fini d'ordre 10 (une explication de ce qu'est un plan projectif et un exemple sont indiqués sur la figure 2). Cette preuve a été obtenue à l'aide d'un programme, en 1988, par C. W. Lam, L. H. Thiel et S. Swiercz.

Le problème est intéressant, car il est lié à une conjecture formulée en 1782 par Léonard Euler concernant les carrés gréco-latins, qui, une fois qu'elle eut été montrée fautive (en 1959), amena à penser qu'il pouvait y avoir de tels plans projectifs d'ordre 10. L'échec des tentatives pour en construire ou pour démontrer qu'ils sont impossibles faisait de la question une énigme agaçante que l'informatique a résolue. Il s'agit donc, là encore, d'un

résultat sur lequel les mathématiciens s'interrogeaient (une thèse a même été soutenue sur le sujet à l'Université de Berkeley en 1974) et qui a été trouvé par ordinateur avant qu'aucun humain ne l'élucide.

L'ordinateur fut irremplaçable, mais son rôle fut d'explorer systématiquement et mécaniquement toutes les tentatives imaginables de construction d'un plan projectif d'ordre 10 et de constater qu'aucune n'aboutit. Le travail fait par l'ordinateur se réduisait à un calcul.

Comme pour le théorème des quatre couleurs, une telle preuve est, par sa longueur, impossible à vérifier à la main.

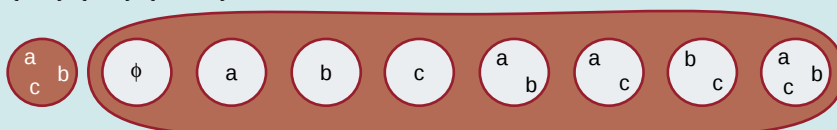
Il y a quelques mois, William McCune, du Département de mathématiques et d'informatique du Laboratoire Argonne, aux États-Unis, a démontré la conjecture de Robbins, sur laquelle des recherches vaines étaient menées depuis 1933.

L'ordinateur, cette fois-ci, a-t-il fait un peu plus que dans les deux cas précédents? Pour que chacun puisse

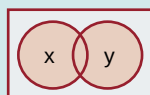
3. ALGÈBRE DE BOOLE ET AXIOME DE ROBBINS

ALGÈBRE DE BOOLE

Un exemple d'algèbre de Boole (et l'on peut montrer que toutes les algèbres de Boole finies se ramènent à cet exemple) est celui des parties d'un ensemble E . Les parties de $\{a, b, c\}$, par exemple, sont $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}$.



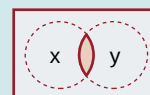
Dans une algèbre de Boole, deux opérations $x+y$ et $n(x)$ sont données ; elles permettent d'en définir une troisième en posant $x \bullet y = n(n(x) + n(y))$.



RÉUNION $x + y$



COMPLÉMENT $n(x)$



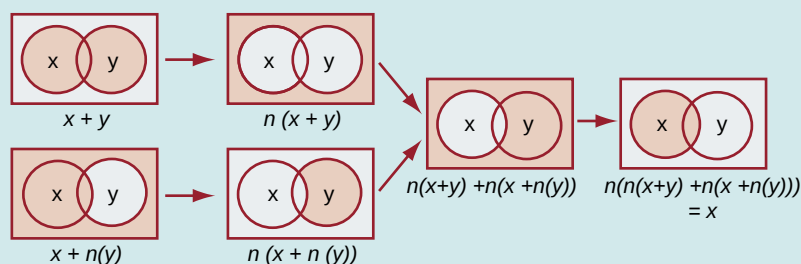
INTERSECTION $x \bullet y$

Ici, $+$ est l'opération de réunion ensembliste ; $n(x)$ est l'opération de passage au complémentaire, $\bullet$ est l'opération d'intersection, V est l'ensemble vide, etc. Une algèbre est de Boole si tous les axiomes suivants sont satisfaits.

$x+y=y+x$	$x \bullet y = y \bullet x$	(commutativité)
$x+(y+z)=(x+y)+z$	$x \bullet (y \bullet z) = (x \bullet y) \bullet z$	(associativité)
$x+T=T$	$x+V=x$	(propriétés de T et V)
$x \bullet T=x$	$x \bullet V=V$	(propriétés de T et V)
$x+n(x)=T$	$x \bullet n(x)=V$	(idempotence)
$x+x=x$	$x \bullet x=x$	(distributivité)
$x \bullet (y+z) = (x \bullet y) + (x \bullet z)$	$x+(y \bullet z) = (x+y) \bullet (x+z)$	(absorption)
$x+(x \bullet y)=x$	$x \bullet (x+y)=x$	(lois de Morgan)
$n(x+y)=n(x) \bullet n(y)$	$n(x \bullet y)=n(x)+n(y)$	

Certains des axiomes peuvent être démontrés à partir des autres : la commutativité de $\bullet$ résulte ainsi de sa définition et de la commutativité de $+$.

TOUTE ALGÈBRE DE BOOLE VÉRIFIE L'AXIOME DE ROBBINS : $n(n(x+y) + n(x+n(y))) = x$



La commutativité de $+$, l'associativité de $+$ et l'axiome de Robbins permettent seuls de démontrer tous les axiomes d'une algèbre de Boole. C'est un ordinateur qui a établi ce résultat conjecturé depuis 1933, mais resté indémontré jusqu'à présent.