

se faire une idée, voici quelques détails sur le problème et sur le travail de l'ordinateur de W. McCune.

LES ALGÈBRES DE BOOLE

La conjecture de Robbins indique que toute structure définie par une opération d'addition, $x+y$, et une opération de complémentation, $n(x)$, qui vérifie les trois propriétés suivantes :

- commutativité (C) : $x+y = y+x$
- associativité (A) : $(x+y)+z = x+(y+z)$
- équation de Robbins (R) :

$$n(n(x+y) + n(x+n(y))) = x,$$

vérifie nécessairement toutes les propriétés que possède l'opération de réunion ensembliste et celle de complémentation dans un ensemble.

Les structures vérifiant les axiomes (C), (A) et (R) s'appellent des *algèbres de Robbins*. Celles vérifiant les propriétés que possèdent la réunion et la complémentation dans un ensemble

(liste indiquée sur la figure 3) s'appellent des *algèbres de Boole*, du nom de George Boole, mathématicien irlandais du XIX^e siècle, auteur du célèbre ouvrage *Les lois de la pensée*, qui décrit un calcul algébrique nouveau à la base de la logique moderne et de la théorie des ensembles.

La conjecture de Robbins affirme donc que «toute algèbre de Robbins est une algèbre de Boole», et la démontrer consiste à utiliser uniquement les trois propriétés (C), (A) et (R) pour en déduire celles de la figure 3. Essayez, par exemple, de déduire $x + x = x$. Il est facile de montrer qu'une algèbre de Boole est une algèbre de Robbins ; c'est la réciproque qui est difficile.

En fait, l'ordinateur n'a pas démontré exactement cette réciproque. Il a utilisé un résultat établi par S. Winker au début des années 1980 : si, dans une algèbre de Robbins, on peut trouver deux éléments a et b vérifiant l'équa-

tion de Winker (W) : $n(a + b) = n(a)$, alors l'algèbre en question est une algèbre de Boole.

L'ordinateur n'a donc eu qu'à établir l'implication : si (C), (A) et (R), alors il existe a et b tels que (W).

Bien des tentatives avaient été faites à la main, mais personne n'avait jamais réussi. Le programme EQP (*Equational Prover*) de W. McCune aboutit en octobre 1996, après un calcul ininterrompu d'une durée de huit jours sur une machine utilisant un processeur RS/6000, en consommant 30 mégaoctets de mémoire et en passant en revue plus de 2 612 977 expressions intermédiaires.

L'assaut final fut précédé de plusieurs autres, durant lesquels le programme était paramétré de façon différente et dont l'examen des résultats a conduit à un ajustement judicieux. Si on prend en compte la durée de cette phase de mise au point de la recherche, le déroulement du calcul a occupé le puissant microprocesseur cinq semaines entières.

VÉRIFICATION ET MISE À DISPOSITION DES DONNÉES

Les deux millions de termes manipulés pendant l'assaut d'octobre ne sont pas tous indispensables à l'écriture de la démonstration que (C), (A) et (R) implique (W). Loin s'en faut ! Ce que l'ordinateur a trouvé se résume en quatre pages vérifiables à la main, contrairement aux deux exemples de démonstration sur ordinateur cités précédemment. Une esquisse de cette démonstration est donnée en figure 4.

Le programme vainqueur EQP est un programme de démonstration automatique spécialisé qui a été développé à partir d'un autre programme de W. McCune, plus général, appelé OTTER. Pour passer du premier programme à EQP, on a amélioré l'efficacité du traitement des équations dans une algèbre où l'opération de base est commutative et associative, et l'on a multiplié les «paramètres de réglages».

Ces paramètres déterminent la stratégie de manipulation des équations que le programme engendre et combine lors de sa recherche. L'un d'eux, par exemple, indique qu'il ne faut pas prendre en considération les équations de longueur supérieure à une borne fixée. Ce paramètre était fixé à 70 dans la recherche d'octobre 1996. Quand ce paramètre est fixé trop bas, la recherche n'aboutit pas, car la démonstration recherchée passe par de longues équations ; quand le paramètre est fixé trop

4. LA DÉMONSTRATION DU 2 OCTOBRE 1996

Voici la preuve de la conjecture de Robbins trouvée par programme. La première étape a été détaillée. Pour les autres, des indications sommaires sont données. La dernière formule en changeant l'ordre de quelques termes est de la forme $n(a + b) = n(a)$; elle montre donc qu'il existe a et b vérifiant l'équation de Winker. Les numérotations des formules sont celles du programme. Les étapes inutiles ont été omises, d'où la discontinuité de la numérotation.

3 [équation de Robbins] $n(n(n(x)+y)+n(x+y)) = y$.

5 [3,3] $n(n(n(x+y)+n(x+y)+y) = n(x+y)$.

Le crochet [3,3] indique qu'on est parti de l'équation 3 et qu'on a simplifié grâce à 3. Voici le détail de cette première étape :

- on part de 3 : $n(n(n(x)+y)+n(x+y)) = y$.

- on remplace x par $n(x)+y$ et y par $n(x+y)$; cela donne :

$$n(n(n(n(x)+y)+n(x+y))+n(n(x)+y+n(x+y))) = n(x+y)$$

- on reconnaît le premier membre de l'équation de Robbins, qu'on

remplace par y : $n(y+n(n(x)+y+n(x+y))) = n(x+y)$

- on change l'ordre ce qui est autorisé à cause de l'axiome (C),

$$n(n(n(x+y)+n(x+y)+y) = n(x+y))$$

6 [3,3] $n(n(n(n(x)+y)+x+y)+y) = n(n(x)+y)$.

24 [6,3] $n(n(n(n(n(x)+y)+x+y+y)+n(n(x)+y))) = y$.

47 [24,3] $n(n(n(n(n(n(x)+y)+x+y+y)+n(n(x)+y)+z)+n(y+z)) = z$.

48 [24,3] $n(n(n(n(n(x)+y)+n(n(x)+y)+x+y+y)+y) = n(n(x)+y)$.

146 [48,3] $n(n(n(n(n(x)+y)+n(n(x)+y)+x+y+y+y)+n(n(x)+y))) = y$.

250 [47,3] $n(n(n(n(n(n(x)+y)+x+y+y)+n(n(x)+y)+n(y+z)+z)+z) = n(y+z)$.

996 [250,3] $n(n(n(n(n(n(n(x)+y)+x+y+y)+n(n(x)+y)$

$$+ n(y+z)+z)+z+u)+n(n(y+z)+u)) = u$$

16379 [5,996,3] $n(n(n(n(n(x)+x)+x+x+x)+x) = n(n(x)+x)$.

16387 [16379,3] $n(n(n(n(n(n(n(x)+x)+x+x+x)+x+y)+n(n(n(x)+x)+y))) = y$.

16388 [16379,3] $n(n(n(n(n(x)+x)+x+x+x+x)+n(n(n(x)+x))) = x$.

16393 [16388,3] $n(n(n(n(n(n(x)+x)+n(n(n(x)+x)+x+x+x+x)+x) = n(n(n(x)+x)$.

16426 [16393,3] $n(n(n(n(n(n(n(x)+x)+n(n(n(x)+x)+x+x+x+x)+x+y)$

$$+ n(n(n(n(x)+x)+y))) = y$$

17547 [146,16387] $n(n(n(n(n(n(n(x)+x)+n(n(n(x)+x)+x+x+x+x)+n(n(n(n(x)+x)$

$$+x+x+x)+x)+x) = n(n(n(n(x)+x)+n(n(n(x)+x)+x+x+x+x))$$

17666 [24,16426,17547] $n(n(n(n(x)+x)+n(n(n(x)+x)+x+x+x+x)$

$$= n(n(n(n(x)+x)+x+x+x+x))$$