

qu'on peut la casser. Pour en être certain, le plus simple est de disposer de résultats mathématiques généraux reliant les diverses mesures de complexité les unes aux autres et qui assureront que, dès qu'une mesure pour f est élevée, c'est aussi le cas pour les autres.

De tels résultats servent à concevoir aisément des fonctions booléennes résistantes aux attaques. Mais un autre motif pour rechercher des liens entre les diverses mesures de complexité des fonctions booléennes est simplement que les mathématiciens aiment savoir, quand ils introduisent des notions portant sur les mêmes objets, quelles relations les lient.

Le résultat de Hao Huang sur les hypercubes a justement comme conséquence qu'une mesure naturelle de complexité, la «sensitivité» (définie plus loin) est liée aux autres. Les travaux antérieurs avaient relié toutes les mesures naturelles de complexité des fonctions booléennes, sauf la sensibilité, qui faisait bande à part.

LA SENSITIVITÉ BOOLÉENNE

Pour saisir l'éclaircissement que Hao Huang a apporté, considérons trois des mesures de complexité les plus courantes et indiquons où le résultat de Huang intervient. Commençons par la mesure de complexité récalcitrante, la «sensitivité».

La sensibilité d'une fonction booléenne f au point $x = (b_1, b_2, \dots, b_n)$ est le nombre de x' liés à x sur l'hypercube H_n tels que $f(x') \neq f(x)$; autrement dit, c'est le nombre de coordonnées de x qui changent la valeur $f(x)$ quand on les modifie. Cette mesure est une sorte de dérivée de f en x : si f bouge beaucoup quand on envisage des points proches de x sur H_n , alors la sensibilité de f est élevée en x .

Par définition, la sensibilité d'une fonction booléenne f est le maximum de la sensibilité de f en x quand on fait varier le point x dans H_n . Cette mesure est une évaluation globale de l'agitation de f : on la note $s(f)$.

Par exemple, la fonction booléenne $f(A, B) = (A \text{ ou } B)$ a une sensibilité 0 en $x = (1, 1)$; en effet, $(1 \text{ ou } 1) = 1$ et quand on change la première coordonnée ou la seconde, le résultat ne change pas, puisque $(0 \text{ ou } 1) = (1 \text{ ou } 0) = 1$. Elle a en revanche une sensibilité égale à 2 en $x = (0, 0)$, car $(0 \text{ ou } 0) = 0$, valeur qui change en modifiant la première ou la seconde coordonnée: $(1 \text{ ou } 0) = 1$, $(0 \text{ ou } 1) = 1$. La sensibilité de la fonction booléenne $f(A, B) = (A \text{ ou } B)$ est donc 2: $s(f) = 2$.

Une deuxième mesure de complexité pour les fonctions booléennes est la «complexité en arbre de décision». Une fonction booléenne étant fixée, on considère les algorithmes qui posent des questions de type: «Quelle est la valeur de la variable X ?» puis, prenant en compte les réponses précédentes, «Quelle est la

valeur de la variable Y ?», etc., jusqu'à avoir assez d'information pour déterminer $f(x)$. Le meilleur algorithme est celui qui sait déterminer $f(x)$ pour tout x en un minimum de questions; ce minimum est la complexité en arbre de décision de f , notée $ad(f)$.

Prenons l'exemple $f(A, B, C, D, E) = (A \text{ ET } B \text{ ET } E) \text{ OU } (C \text{ ET } D \text{ ET NON}(E))$.

Bien qu'il y ait cinq variables, trois questions suffiront toujours pour connaître la valeur de f en un point, car selon que E est vrai (1) ou faux (0), il faut s'intéresser à la première partie de l'expression définissant f ou à la seconde. Le meilleur algorithme d'interrogation est donc:

- 1) Demander la valeur de E ;
- 2) Si E est vrai, demander A , puis, si A est vrai, demander B ;
- 3) Si E est faux, demander C , puis, si C est vrai, demander D .

En trois questions et parfois deux, on connaît ainsi la valeur de f . On ne peut pas faire mieux que 3, donc $ad(f) = 3$.

Une troisième mesure de complexité d'une fonction booléenne est le «degré» défini de la façon suivante. Toute fonction booléenne peut s'écrire de façon unique comme une somme de conjonctions du type:

$$f(A, B, C) = (A \text{ ET } B) + (B \text{ ET } C) + (A \text{ ET } C)$$

où le + désigne le «ou exclusif»: $P + Q$ est vrai si « P est vrai et Q faux», ou si « P est faux et Q vrai». Le degré de f , noté $deg(f)$, est le plus grand nombre de variables qu'on trouve dans un terme de cette expression de f . Ici, c'est 2: $deg(f) = 2$.

Quels sont les liens entre ces trois mesures de complexité et d'autres encore? Pour les deux dernières et les autres, la réponse était connue: chacune est majorée par un polynôme en fonction de l'autre, puisque l'on a toujours:

$$deg(f) < ad(f) < 16 [deg(f)]^8.$$

Pour avoir des relations liant la sensibilité $s(f)$ aux autres mesures de complexité, il était établi que la question se ramenait à celle concernant les sous-graphes de H_n que Hao Huang a résolue et que nous avons expliquée. Ce travail a permis de savoir que $[s(f)]^2 \geq deg(f)$, ce qui, avec les autres résultats connus, permet de conclure à l'équivalence, à un polynôme près, des mesures de complexité des fonctions booléennes.

Le résultat de Hao Huang est théorique, mais il est aussi pratique puisque la vitesse optimale de calcul de certains circuits électroniques est directement liée à ces mesures de complexité. La preuve en deux pages de Hao Huang est assez simple. En une heure de lecture, un mathématicien connaissant le sujet peut la vérifier.

Scott Aaronson, de l'université du Texas à Austin, remarque qu'une recherche pendant trente ans par des dizaines de mathématiciens, certains très brillants, a été nécessaire pour aboutir à une preuve qui se vérifie en une heure: prouver est bien plus difficile que vérifier! ■

BIBLIOGRAPHIE

R. Karthikeyan et al., **On the resolution of the sensitivity conjecture**, *Bull. of the Amer. Math. Soc.*, vol. 57(4), pp. 615-638, 2020.

H. Huang, **Induced subgraphs of hyper-cubes and a proof of the sensitivity conjecture**, *Ann. of Math.*, vol. 190(3), pp. 949-955, 2019.

D. Knuth, **A computational proof of Huang's degree theorem** (démonstration en une page du résultat de Hao Huang), 2019 : <https://www.cs.stanford.edu/~knuth/papers/huang.pdf>

S. Jukna, **Boolean Function Complexity**, Springer, 2012.

H. Buhrman et R. de Wolf, **Complexity measures and decision tree complexity : a survey**, *Theoret. Comput. Sci.*, vol. 288(1), pp. 21-43, 2002.

C. Gotsman et N. Linial, **The equivalence of two problems on the cube**, *J. Combin. Theory Ser. A*, vol. 61(1), pp. 142-146, 1992.

N. Nisan et M. Szegedy, **On the degree of Boolean functions as real polynomials**, *Computational Complexity*, vol. 4, pp. 301-313, 1994.