

LA CONJECTURE DE LA SENSITIVITÉ

3

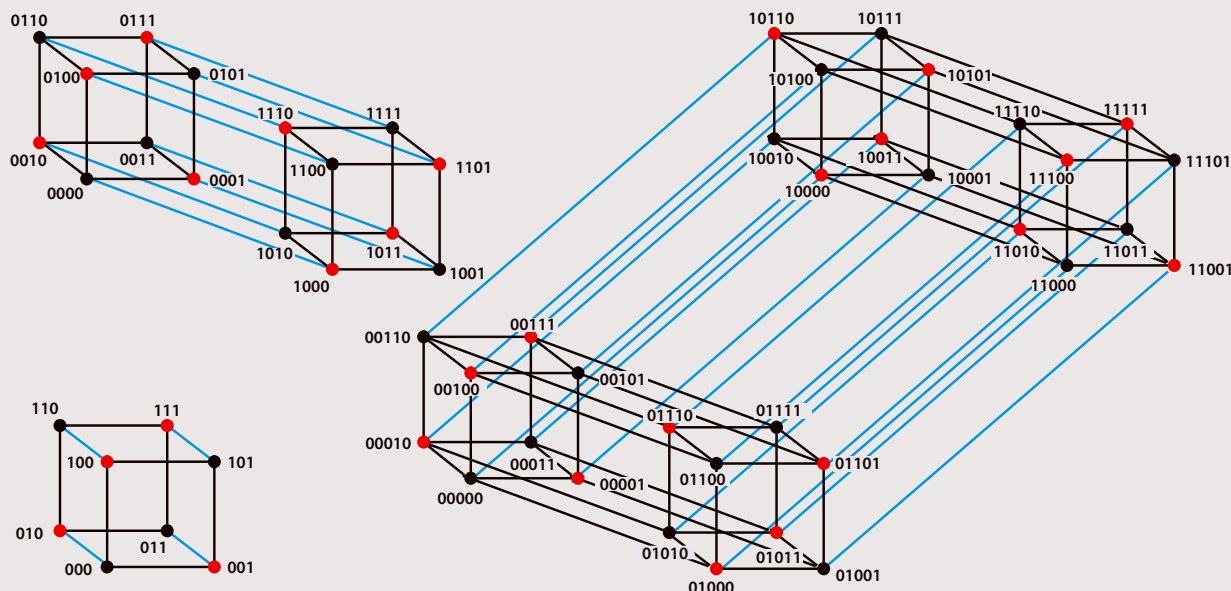
On avait montré que la conjecture de la sensibilité, qui porte sur les mesures de complexité des fonctions booléennes, est équivalente à une conjecture sur les sommets de l'hypercube H_n et c'est cette dernière formulation que Hao Huang a démontrée. Il a montré que si l'on prend $2^{n-1} + 1$ sommets de H_n , alors l'un au moins de ces sommets est relié à au moins $\sqrt{n}$ autres sommets parmi ceux retenus.

Autrement dit : dès qu'on prend 5 sommets du cube H_3 , l'un des sommets est lié à 2 autres ; dès qu'on prend 9 sommets de H_4 , l'un des sommets est lié à 2 autres ; dès qu'on prend 17 sommets de H_5 , l'un des sommets est lié à 3 autres ; et ainsi de suite.

Cette affirmation est d'autant plus étonnante que l'on peut trouver 4 sommets du cube H_3 sans aucun lien, 8 sommets de H_4 sans

aucun lien, 16 sommets de H_5 sans aucun lien, etc.

Les dessins ci-dessous représentent ces façons de choisir 2^{n-1} sommets de H_n sans liens entre eux. La méthode utilisée pour ces choix est assez simple : prendre les sommets dont les coordonnées comportent un nombre pair de 1 (en noir sur le dessin).



de trouver 9 sommets et en constatant que l'on n'y arrive jamais. Cependant, pour l'établir en toute rigueur, il faut soit trouver un raisonnement mathématique, soit envisager tous les sous-ensembles de 9 sommets pris dans les 16 sommets de H_4 et constater pour chacun que l'on a deux sommets reliés par une arête. Cela exige d'envisager $16!/(9!7!) = 11\,440$ cas (nombre de sous-ensembles de 9 éléments pris parmi un ensemble de 16 éléments).

Ce travail d'exploration de 11 440 cas est difficilement envisageable à la main. J'ai écrit un programme qui réalise cette énumération et, effectivement, il m'a indiqué que pour chacune des 11 440 façons de prendre 9 sommets de H_4 , il y a au moins un sommet relié à un autre. Mon programme m'a aussi signalé que dans chaque cas, il y a au moins un sommet relié à deux autres !

Problème 3. Quel est le plus grand nombre de sommets que l'on peut choisir dans H_5 de telle façon qu'aucun ne soit relié à un autre par une arête ?

La réponse est 16. D'une part, en s'inspirant de ce qui s'est passé pour la dimension 4, il est assez facile de choisir 16 sommets sans

que deux soient reliés par une arête. On prend la solution à 8 éléments pour le premier hypercube H_4 , qui engendre H_5 . On prend la solution complémentaire pour le second et tout est bon (voir l'encadré 3). On remarque alors que les sommets retenus sont ceux dont les coordonnées comportent un nombre pair de 1. Il est clair qu'un sommet ayant un nombre pair de 1 dans ses coordonnées n'est relié qu'à des sommets ayant un nombre impair de 1 dans ses coordonnées, ce qui confirme que la solution proposée est satisfaisante. Elle se généralise et montre que l'on peut toujours choisir 2^{n-1} sommets du graphe H_n sans que deux soient reliés.

Bien sûr, pour démontrer que 17 est impossible, le problème combinatoire est devenu colossal, car il y a $32!/(17!15!) = 565\,722\,720$ cas à envisager.

Ce qui s'est passé pour le problème 2 se reproduit en plus étonnant encore. Dès que l'on prend 17 sommets, on ne peut éviter qu'un sommet soit lié à trois autres. Le nombre maximum de voisins d'un sommet d'un graphe se nomme le « degré du graphe ». Le plus petit degré possible pour un sous-graphe de 16 sommets de H_4 , qui est 0, passe donc à 3 avec un

> sous-graphe de 17 sommets. De 16 sommets à 17 sommets, le degré minimum passe brusquement de 0 à 3.

Cette fois, ce n'est pas mon ordinateur qui m'a donné cette information, car mon programme n'était pas assez rapide: c'est le théorème de Hao Huang, qui résout la conjecture de la sensibilité.

Le résultat démontré par Hao Huang en 2019, qui a surpris tous les spécialistes, est maintenant facile à comprendre. Il s'énonce ainsi: «Si l'on choisit $2^{n-1}+1$ sommets dans l'hypercube H_n , alors l'un au moins des sommets est relié à au moins $\sqrt{n}$ autres sommets par des arêtes.»

Lorsque $n=3$, on retrouve qu'avec H_3 , dès que l'on prend 5 sommets, l'un est relié à deux autres ($\sqrt{3}=1,7320\dots$), qu'avec H_4 , dès que l'on prend 9 sommets, l'un est relié à deux autres ($\sqrt{4}=2$) et qu'avec H_5 , dès que l'on prend 17 sommets, l'un est relié à trois autres ($\sqrt{5}=2,2360\dots$).

L'intérêt du résultat de Hao Huang est qu'il est vrai pour tout entier positif n , ce qu'aucun ordinateur procédant par énumération ne pourra jamais établir. En soi, le résultat est surprenant puisque, associé à celui indiquant que

2^{n-1} sommets de H_n peuvent n'avoir aucun lien entre eux, il montre que, par exemple pour $n=100$, dès qu'on veut prendre un sommet de plus que 2^{99} (soit $6,338\dots \times 10^{29}$) sommets dans H_{100} , alors on crée toujours un sommet lié à dix autres au moins. De 2^{99} à $2^{99}+1$, c'est-à-dire en ajoutant un seul sommet, on passe du degré minimal 0 au degré minimal 10...

COMPLEXITÉ DES FONCTIONS BOOLÉENNES

Cependant, l'intérêt principal du résultat de Hao Huang n'est pas dans ce petit problème combinatoire relatif à l'hypercube, mais dans ses conséquences sur la mesure de la complexité des fonctions booléennes.

Les fonctions booléennes sont utiles pour la conception des circuits électroniques et en particulier des microprocesseurs. Elles servent aussi en cryptographie pour concevoir des fonctions pseudoaléatoires ou des fonctions de chiffrement. Ce sont simplement des fonctions dont l'ensemble de départ est H_n , l'hypercube de dimension n , et qui prennent une valeur qui peut être 0 ou 1. Le 0 et le 1 sont assimilés à *Faux* et *Vrai* quand on envisage les variables des fonctions booléennes.

Un exemple de fonction booléenne est:

$$f(A, B, C) = ((A \text{ ET } B) \text{ OU } (\text{NON}(A) \text{ ET } \text{NON}(B))) \text{ IMPLIQUE } C.$$

Les variables A , B et C peuvent chacune prendre deux valeurs 0 ou 1, ce qui donne 8 valeurs possibles pour le triplet (A, B, C) .

Les connecteurs **OU**, **ET** et **IMPLIQUE** sont définis par leur sens logique habituel:

0 **OU** 0 = 0; 0 **OU** 1 = 1; 1 **OU** 0 = 1; 1 **OU** 1 = 1;
0 **ET** 0 = 0; 0 **ET** 1 = 0; 1 **ET** 0 = 0; 1 **ET** 1 = 1;
0 **IMPLIQUE** 0 = 1; 0 **IMPLIQUE** 1 = 1;
1 **IMPLIQUE** 0 = 0; 1 **IMPLIQUE** 1 = 1,

On en tire par exemple que $f(1, 1, 1)$
= $((1 \text{ ET } 1) \text{ OU } (\text{NON}(1) \text{ ET } \text{NON}(1))) \text{ IMPLIQUE } 1$
= $(1 \text{ OU } (0 \text{ ET } 0)) \text{ IMPLIQUE } 1$
= $(1 \text{ OU } 0) \text{ IMPLIQUE } 1 = 1 \text{ IMPLIQUE } 1 = 1.$

Les fonctions booléennes utilisées en informatique peuvent comporter des milliers de variables et avoir des expressions comportant des milliers de connecteurs logiques. Chaque fonction s'écrit d'une multitude de façons et, bien sûr, on recherche les écritures les plus simples, car elles conduisent aux circuits et aux programmes les plus petits et les plus efficaces. Il est important de mesurer la complexité des fonctions booléennes; en cryptographie, c'est essentiel, car des fonctions booléennes trop simples seraient faciles à attaquer.

On a donc introduit des mesures de complexité des fonctions booléennes. Plusieurs se présentent naturellement. Quand on veut disposer d'une fonction booléenne avec la certitude qu'elle est complexe, il faut que toutes les mesures de complexité de cette fonction soient élevées, sinon cela signifie sans doute

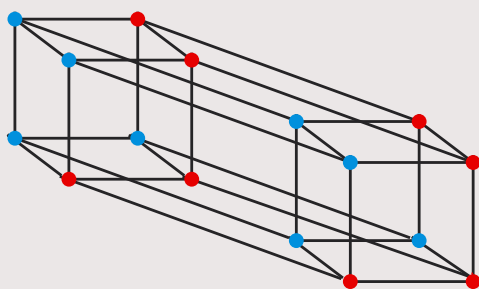
LA SENSITIVITÉ, MESURE DE COMPLEXITÉ

Une fonction booléenne de n variables est une fonction qui associe un 0 ou un 1 à chaque sommet de l'hypercube H_n . On peut représenter une fonction booléenne de n variables en dessinant H_n et en coloriant en bleu les sommets où la fonction prend la valeur 1, les autres étant en rouge.

La sensibilité d'une fonction booléenne en un point est le nombre de sommets liés à ce point où la fonction change (de rouge à bleu ou de bleu à rouge). La sensibilité d'une fonction f est le maximum

de la sensibilité de f en x , quand on fait varier x . C'est une sorte de dérivée, liée aux mouvements plus ou moins nombreux de la fonction quand on se déplace sur l'hypercube en suivant les arêtes.

La fonction représentée ci-dessous a une sensibilité égale à 2, car les sommets rouges ne sont jamais liés à plus de 2 sommets bleus, et les sommets bleus ne sont jamais reliés à plus de 2 sommets rouges. La sensibilité est une mesure de complexité pour les fonctions booléennes.



4