EPFL - Information, Calcul et Communication - Partie théorique

Complexité : l'argument de la diagonale de Cantor

Pour montrer que certains problèmes ne sont pas solubles par un algorithme, on peut utiliser un autre argument que celui du problème de l'arrêt : c'est l'argument de la diagonale de Cantor, qui montre que l'univers contient *plus* de problèmes que d'algorithmes, et donc que forcément, certains de ces problèmes ne sont pas solubles par un algorithme (nous allons encore préciser ci-dessous ce que veut dire ce *plus*),

Pour ce faire, on se restreint à nouveau aux *problèmes de décision* : un problème de décision est un problème qui, pour des données d'entrée, demande une réponse oui ou non (de manière équivalente, 1 ou 0). Pour rappel, un exemple est le problème de la primalité : "Etant donné un nombre entier $N \geq 1$, ce nombre est-il premier ou non ?"

L'idée est maintenant de montrer que :

- d'une part, l'ensemble des algorithmes est dénombrable (c'est-à-dire en bijection avec l'ensemble des nombres entiers naturels $\mathbb{N}$) ;

- d'autre part, l'ensemble des problèmes de décision ne l'est pas, ce qui implique qu'il existe *plus* de problèmes que d'algorithmes.

Observons tout d'abord que l'ensemble des algorithmes est dénombrable : en effet, un algorithme consiste toujours en un suite finie de symboles. Or comme nous le verrons dans le prochain chapitre consacré à la représentation binaire, tout symbole peut être représenté (de manière univoque) par une suite finie de 0 et de 1. En conséquence, tout algorithme peut également être représenté (de manière univoque) par une suite finie de 0 et de 1 (par simple concaténation des représentations des symboles pris séparément). Or il se trouve que toute suite finie de 0 et de 1 peut à son tour être encodée par un seul nombre entier (à nouveau, voir le prochain chapitre à ce sujet). Ainsi, on peut faire correspondre à tout algorithme un unique nombre entier (certes très grand), ce qui établit l'existence d'une bijection entre l'ensemble des algorithmes et l'ensemble des entiers naturels $\mathbb{N}$, et par là-même le fait que l'ensemble des algorithmes est dénombrable.

D'autre part, qu'en est-il de l'ensemble des problèmes de décision ? Comme vu plus haut, on peut représenter un problème de décision comme une fonction f associant à des données d'entrée une valeur 0 ou 1. Dans l'exemple du problème de la primalité, les données d'entrée sont simplement un nombre entier naturel. Or il se trouve que n'importes quelles données d'entrée peuvent également être représentées par un unique nombre entier naturel ! En effet, il suffit pour cela d'utiliser la représentation binaire de ces données et de rassembler celles-ci pour former une suite de 0 et de 1, qui peut à nouveau être encodée par un seul nombre entier.

La question qui reste donc maintenant est : l'ensemble des fonctions $f : \mathbb{N} \to \{0, 1\}$ est-il dénombrable ? L'argument de la diagonale de Cantor, qui est un raisonnement par l'absurde, permet de montrer que ce n'est pas le cas (et donc qu'il existe plus de problèmes de décision que d'algorithmes pour les résoudre). Voici cet argument en détail :

Supposons que l'ensemble des fonctions $f : \mathbb{N} \to \{0, 1\}$ soit dénombrable : nous allons voir que ceci mène à une contradiction. Si cet ensemble est dénombrable, il est possible d'énumérer la liste $\{f_1, f_2, f_3, \ldots\}$ de toutes ces fonctions. Définissons alors une nouvelle fonction $g : \mathbb{N} \to \{0, 1\}$ ainsi :

$$g(n) = 1 - f_n(n), \quad \text{pour } n \in \mathbb{N}$$

Ainsi $g(n)$ prend la valeur 1 si et seulement si $f_n(n) = 0$ (et réciproquement). La fonction g est donc parfaitement bien définie comme fonction allant de $\mathbb{N}$ dans $\{0, 1\}$. Comme nous avons supposé que l'ensemble de ces fonctions est dénombrable, g doit forcément faire partie de la liste $\{f_1, f_2, f_3, \ldots\}$. Mais c'est impossible, car on sait par construction que pour toute valeur de n, la fonction f_n ne peut être égale partout à g, car elle diffère justement de g en position n. Nous avons donc trouvé une fonction $g : \mathbb{N} \to \{0, 1\}$ qui ne fait pas partie de la liste $\{f_1, f_2, f_3, \ldots\}$, ce qui est en contradiction avec notre hypothèse de départ que l'ensemble des fonctions $f : \mathbb{N} \to \{0, 1\}$ est dénombrable. QED