La fonction du castor affairé n'est pas calculable

Léo Gayral

2017-2018

ref : Dehornoy – Mathématiques de l'informatique – p.186

Définition 1 (Fonction calculable)**.** Soit $f : \mathbb{N} \to \mathbb{N}$. On dit que cette fonction est calculable si il existe une machine de Turing *unaire*, à un seul ruban bi-infini, qui termine sur toute entrée 1^n avec $1^{f(n)}$ sur le ruban, aligné en première position.

Notons que cette notion est en réalité équivalente au cas plus général, en fixant un codage $\mathbb{N} \to \Sigma^*$.

Définition 2 (Fonction du castor affairé)**.** Soit M une machine unaire. On définit $\Phi(M)$ comme le nombre de 1 écrits sur le ruban lorsque la machine termine sur l'entrée vide, fixé par convention à 0 lorsque la machine boucle.

La fonction du castor affairé est alors définie par :

$$U(n) = \max_{M \text{ à } n \text{ états}} \Phi(M)\,.$$

Étant donné le nombre fini de telles machines à n fixé, ce maximum est bien atteint.

Lemme 1. U est strictement croissante sur $\mathbb{N}^*$.

Démonstration.
On a naturellement $U(0) = U(1) = 0$.

Soit $M = (Q, q_0, F, \delta)$ qui réalise le maximum dans $U(n)$ pour $n \geq 1$. On considère alors M' définie comme M, avec un état $q_F \notin Q$ supplémentaire pour état final, et les transitions suivantes sur tout état $q \in F$ final dans M :

$$\delta(q, 1) = (q, 1, \rightarrow), \delta(q, 0) = (q_F, 1, \rightarrow)$$

de sorte que, dès que M termine sur une entrée, M' ajoute un 1 supplémentaire sur la première case libre à sa droite.

Il en découle $U(n) = \Phi(M) < \Phi(M) + 1 = \Phi(M') \leq \Phi(n+1)$. $\square$

Lemme 2 (admis)**.** La fonction $n \mapsto n^2$ est calculable.

Idée.
L'idée derrière la construction d'une telle machine se base sur la relation $(n+1)^2 = n + n + 1 + n^2$.

Sur l'entrée 1^n, on commence par vérifier si $n = 0$:
— Sur l'entrée $n + 1 > 0$, on effectue trois copies de n sans jamais écrire à gauche du mot, pour obtenir $1^n01^n01^n$, puis on complète le premier blanc par un 1, de sorte à avoir $1^{2n+1}01^n$. On peut alors s'aligner au début de 1^n, revenir à l'état initial de la machine, et recommencer le raisonnement.
— Sur l'entrée *vide* ($n = 0$), on élimine les 0 de la chaîne sur la gauche, jusqu'à obtenir une suite de 1 consécutifs sur le ruban.

En procédant ainsi, on finit effectivement par écrire 1^{n^2} sur le ruban. $\square$

Théorème 1. Soit $F : \mathbb{N} \to \mathbb{N}$ croissante, calculable. Alors à partir d'un rang, on a $F(n) < U(n)$.

Démonstration.
Soit M une machine qui calcule F.

On considère la machine C_n qui écrit 1^n sur le ruban, le rembobine, calcule son carré, puis applique la machine M. Ce faisant, on peut trouver une constante $K \in \mathbb{N}^*$ telle que C_n a moins de $K + n$ états. On en déduit donc que $F\left(n^2\right) = \Phi\left(C_n\right) \leq U(K+n)$.

Par stricte croissance de U, on cherche un rang à partir duquel $K + n < (n-1)^2$, ou de façon équivalente $n^2 - 2n + 1 - K > 0$. Cette fonction est croissante sur $\mathbb{N}^*$, et positive en $2K$, d'où $F\left(n^2\right) < U\left((n-1)^2\right)$ pour $n \geq 2K$.

Pour étendre le résultat de n^2 à n, il suffit d'avoir $n \geq 4K^2$, car alors on a $m \geq 2K$ tel que $n \in \rrbracket (m-1)^2, m^2 \rrbracket$ et donc $F(n) \leq F\left(m^2\right) < U\left((m-1)^2\right) < U(n)$. $\square$

Corollaire 1. La fonction U du castor affairé n'est pas calculable.