Calculabilité
Cours 3 : les limites du calcul

Kévin Perrot – Aix Marseille Université – printemps 2021

Table des matières

4 Les limites du calcul

Attention. Dans la suite du cours, il sera beaucoup question de machines de Turing qui « prennent en entrée une autre machine de Turing ». On aura une machine A, qui tente de réponse à une question du genre : est-ce que la machine B qui t'es donnée en entrée accepte le mot vide ? Gare aux confusions ! On considère ici **une** machine A, qui doit pouvoir répondre à la question pour **toute** machine B qui lui est donnée en entrée.

4.1 Code d'une machine de Turing

Les résultats fondamentaux sur les limites du calcul sont liés à des problèmes dans lesquels une machine de Turing doit répondre à une question sur les machines de Turing. Pour cela, il faut pouvoir donner en entrée à une machine de Turing la définition (le code, le programme) d'une autre machine de Turing. Deux possibilités :

— en donnant le numéro de la machine dans une énumération des machines de Turing,
— en écrivant le code de la machine sur la ruban.

Pour la première possibilité, il faut fixer une *énumération* des machines de Turing, c'est-à-dire fixer une bijection entre $\mathbb{N}$ et l'ensemble des machines de Turing, afin de pouvoir désigner *la* machine numéro 0, *la* machine numéro 1, *la* machine numéro 2, etc.

Pour la seconde possibilité, il faut *encoder* la définition d'une machine de Turing dans le mot d'entrée. Ce mot correspondra au *code* de la machine de Turing donnée en entrée.

Notation 1. *Nous noterons* $\langle M \rangle$ *le* **code d'une machine de Turing**.

Il y a de nombreuses façons d'encoder les machines de Turing sur le ruban. Par exemple, en numérotant de q_1 à q_n les états (avec q_1 l'état initial et q_n l'état final) et de a_1 à a_m les symboles de ruban (avec a_1 le sumbole blanc B) d'une machine M, et en fixant $D = 0$ et $L = 00$, il est possible d'encoder chaque transition $\delta(q_i, a_j) = (q_k, a_\ell, L)$ de M par la séquence

$$\text{transition} = \underbrace{0\dots0}_{i}1\underbrace{0\dots0}_{j}1\underbrace{0\dots0}_{k}1\underbrace{0\dots0}_{\ell}1\underbrace{00}_{L}$$

On peut alors encoder une machine complète en commençant par dire combien elle a d'états, combien elle a de symboles de ruban, puis en listant ses x transitions une à une :

$$\langle M\rangle = 111\underbrace{0\dots0}_{n}11\underbrace{0\dots0}_{m}11\text{transition}_1 11\text{transition}_2 11\dots 11\text{transition}_x 111.$$

Par convention, nous pouvons énumérer les transitions dans l'ordre lexicographique selon l'état courant et le symbole lu (pratique pour décoder, mais pas nécessaire). Un tel codage est injectif, c'est-à-dire qu'une suite de bits correspond à au plus une machine de Turing. On se convaincra que le résultat suivant est vrai.

Lemme 2. *Le langage $L_{enc} = \{w \in \{0,1\}^* \mid w = \langle M\rangle$ pour une MT $M\}$ est décidable.*

4.2 Théorème de l'arrêt

Théorème 3. *La fonction* **halt** : $(\langle M\rangle, w) \mapsto \begin{cases} 0 \text{ si } M(w)\uparrow \\ 1 \text{ sinon} \end{cases}$ *n'est pas calculable.*

Démonstration. Par l'absurde, supposons qu'il existe une machine de Turing M_{halt} qui calcule la fonction *halt*. Nous pouvons alors sans difficulté construire la machine M_{diag} suivante :

$$M_{diag}(i) = \begin{cases} 1 \text{ si } M_{halt}(i,i) = 0 \\ \uparrow \text{ si } M_{halt}(i,i) = 1 \end{cases}$$

où $\uparrow$ signifie que M_{diag} entre dans une boucle infinie (et ne termine donc pas). Considérons à présent l'entrée $\langle M_{diag}\rangle$ donnée à la machine M_{diag}. Deux cas sont possibles.

— Si $M_{diag}(\langle M_{diag}\rangle) = 1$ alors, par définition de M_{diag}, nous avons $M_{halt}(\langle M_{diag}\rangle, \langle M_{diag}\rangle) = 0$ ce qui signifie, par définition de M_{halt}, que $M_{diag}(\langle M_{diag}\rangle)\uparrow$, une contradiction.

— Si $M_{diag}(\langle M_{diag}\rangle)\uparrow$ alors, par définition de M_{diag}, nous avons $M_{halt}(\langle M_{diag}\rangle, \langle M_{diag}\rangle) = 1$ ce qui signifie, par définition de M_{halt}, que $M_{diag}(\langle M_{diag}\rangle)$ s'arrête, une contradiction.

Dans les deux cas nous arrivons à une contradiction. $\square$