INFO-F408: Computability & complexity

Rémy Detobel

16 Octobre, 2017

1 Théorème de Rice

Pour P n'importe quelle propriété "non triviale" d'un langage d'une machine de Turing :

$$\exists M_1 \text{ tel que } L(M_1) \in P$$
$$\wedge \exists M_2 \text{ tel que } L(M_2) \notin P$$

— Problème de décision ($\equiv$ Langages)
— DFA (machine de turing déterministe)
— Non déterministes
— Power set construction : DFA (équivalent à NFA)
— Langage régulier ("Regular languages"), est l'ensemble des langages reconnus par un automate déterministe

— Machines de Turing / Church-T thesis
— Multitape Turing Machine / Machine de Turing non déterministe
— Décidabilité VS reconnaissable ("recognizable") $\Leftrightarrow$ $\exists$ un énumérateur ("enumerator")

Un langage A est :

$$\text{reconnaissable ("recognizable")} \Leftrightarrow \exists M : L(M) = A$$
$$\text{décidable} \Leftrightarrow \exists M : \text{ M est un "decider" } L(M) = A$$

— Cantor's Diagonalization argument :
$\Rightarrow$ $\exists$ langage L $\in$ Reconnaissable
— Problème de l'arrêt (Halting problem)
$A_{TM} = \{\langle M, w\rangle | \text{M est une machine de Turing qui accepte } w\}$
Reconnaissable et pas décidable $\overline{A_{TM}}$ n'est pas reconnaissable.
— Théorème de Rice.

2 Un problème indécidable simple

Voir livre chapitre 5.2

$$\left\{ \left[\frac{ab}{abab}\right], \left[\frac{b}{a}\right], \left[\frac{aba}{b}\right], \left[\frac{aa}{a}\right] \right\}$$

(Emil) Post correspondence problem
Théorème 5.15 PCP est indécidable (Post correspondence problem)

$$M, w \in \Sigma^* \rightarrow (Q, \Sigma, \Gamma, \delta, q_0, q_{accept}, q_{reject})$$

Construit une instance P du problème PCP.
P ("has a match") à une correspondance $\Leftrightarrow$ M accepte w.

1. Les premiers dominos sont :

$$\frac{\#}{\# q_0 w_1 w_2 ... w_n \#}$$

2. Pour chaque $a, b \in \Gamma$ et $q, r \in Q$ où $q \neq q_{reject}$
   Si $\delta(q, a) = (r, b, R)$ on ajoute $\left[\frac{qa}{br}\right]$
3. $a, b, c \in \Gamma; q, r \in Q$
   Si $\delta(q, a) = (r, b, L)$ on ajoute $\left[\frac{cqa}{rcb}\right]$
4. Pour chaque $a \in \Gamma$, on ajoute $\left[\frac{a}{a}\right]$
5. Ajouter : $\left[\frac{\#}{\#}\right]$ et $\left[\frac{\#}{\_\#}\right]$
6. $\left[\frac{aq_{accept}}{q_{accept}}\right] \forall a \in \Gamma$ et $\left[\frac{q_{accept}a}{q_{accept}}\right]$
7. $\left[\frac{q_{accept}\#\#}{\#}\right]$

Hypothèse : une correspondance doit commencer par le premier domino (Modified PCP)

Exemple :

$>\#$
$>\#q_0 0100\#$
$\delta(q_0, 0) = (q_7, 2, R)$
$$\left[\frac{q_0 0}{2q_7}\right]$$

$>\#q_0 0$
$>\#q_0 0100\#2q_7$

$>\#q_0 0100$
$>\#q_0 0100\#2q_7 100$

$>\#q_0 0100\#$
$>\#q_0 0100\#2q_7 100\#$
$\delta(q_7, 1) = (q_1, 3, L)$

$c = 2$
$$\left[\frac{2q_7 1}{q_1 23}\right]$$

$>\#q_0 0100\#2q_7 100\#$
$>\#q_0 0100\#2q_7 100\#q_1 2300\#$

Comment supprimer la condition de M PCP ? Posons :

$$\circledast w = *u_1 * u_2 * u_3 ... * u_n$$
$$u\circledast = u_1 * u_2 * ... u_n *$$
$$\circledast u \circledast = *u_1 * u_2 * u_3 ... * u_n *$$

On remplace donc :

$$\left\{\left[\frac{t_1}{b_1}\right], \left[\frac{t_2}{b_2}\right], \dots, \left[\frac{t_k}{b_k}\right]\right\}$$

Par :

$$\left\{\left[\frac{\circledast t_1}{\circledast b_1 \circledast}\right], \left[\frac{\circledast t_2}{b_2 \circledast}\right], \dots, \left[\frac{\circledast t_k}{b_k \circledast}\right]\right\}$$

Avec cela ils doivent donc être en premier. Mais on doit en plus rajouter :

$$\left[\frac{\circledast\lozenge}{\lozenge}\right].$$

3 Reducibility (Mapping/Many-One)

Définition : $f : \Sigma^* \to \Sigma^*$ est exécutable (computable) si et seulement s'il existe une machine de Turing M telle que pour n'importe quel entrée w, M s'arrête avec seulement $f(w)$ sur son stack/ruban (tape)

Définition : Un langage A est réductible dans un langage B, si il existe une fonction f exécutable ("computable") telle que

$$\forall w \in \Sigma^* : f(w) \in B \Leftrightarrow w \in A.$$

On note cela : $A \leqslant_M B$

Théorème : Si $A \leqslant_M B$ et B est décidable, alors A est décidable.

Théorème : Si $A \leqslant_M B$ et B est reconnaissable ("recognizable"), alors A est reconnaissable.