Le théorème de cardinalité

François-Régis André

27 janvier 2010

Machines de Turing avec oracle

Definition

Une machine de Turing avec oracle est une machine de Turing qui a de plus une bande particulière, l'oracle, qui lui permet de calculer instantanément une fonction à valeurs dans $\{0, 1\}$.

Machines de Turing avec oracle

Definition

Une machine de Turing avec oracle est une machine de Turing qui a de plus une bande particulière, l'oracle, qui lui permet de calculer instantanément une fonction à valeurs dans $\{0,1\}$.

Definition

Soient A une partie de $\mathbb{N}$ et $n \in \mathbb{N}$. On note :

$$\chi_{A,n} : \mathbb{N}^n \to \{0,1\}^n \ , \ (x_1, x_2, \ldots, x_n) \mapsto (\chi_A(x_1), \ldots, \chi_A(x_n))$$
$$\#_{A,n} : \mathbb{N}^n \to \mathbb{N} \ , \ (x_1, x_2, \ldots, x_n) \mapsto$$
$$\sum_{i=1}^{n} \chi_A(x_i) = \#\{i \in \{1, \ldots, n\} \,|\, x_i \in A\}$$

où χ_A désigne la fonction caractéristique de A.

Théorème de non-accélération et conjecture de Beigel

Théorème

(théorème de non-accélération) Si $\chi_{A,2^n}$ *peut être calculée par une machine de Turing avec oracle qui ne fait pas plus de* n *appels à cet oracle, alors* A *est récursif.*

Théorème de non-accélération et conjecture de Beigel

Théorème

(théorème de non-accélération) Si $\chi_{A,2^n}$ peut être calculée par une machine de Turing avec oracle qui ne fait pas plus de n appels à cet oracle, alors A est récursif.

En 1987, Beigel énonce une conjecture qui renforce ce théorème :

Proposition

Si $\#_{A,2^n}$ peut être calculée par une machine de Turing avec oracle qui ne fait pas plus de n requêtes à cet oracle, alors A est récursif.

Théorème de cardinalité

Ce résultat est une conséquence du théorème de cardinalité :

Théorème

Si pour $m \in \mathbb{N}$, il existe une fonction G récursive $\mathbb{N}^m \to \mathcal{P}(\{0, \ldots, m\}) - \{\{0, \ldots, m\}\}$, telle que pour tous $(x_1, \ldots, x_m) \in \mathbb{N}^m$:

$$\#_{A,m}(x_1, \ldots, x_m) \in G(x_1, \ldots, x_m)$$

alors A est récursive.

Le théorème de cardinalité implique la conjecture de Beigel

Lemme

Si une fonction f peut être calculée grâce à moins de n requêtes à un oracle pour un certain entier n, alors il existe un ensemble S d'au plus 2^n fonctions partielles récursives tel que :

$$\forall x \in \mathbb{N}, \exists g \in S, f\left(x\right) = g\left(x\right)$$

Le théorème de cardinalité implique la conjecture de Beigel

Lemme

Si une fonction f peut être calculée grâce à moins de n requêtes à un oracle pour un certain entier n, alors il existe un ensemble S d'au plus 2^n fonctions partielles récursives tel que :

$$\forall x \in \mathbb{N}, \exists g \in S, f(x) = g(x)$$

On se place dans les hypothèses de la conjecture de Beigel : $\#_{A,2^n}$ est calculée par une machine de Turing qui ne fait pas plus de n appels à son oracle. La fonction G demandée par le théorème de cardinalité est calculée en prenant l'ensemble des valeurs retournée par les 2^n fonctions partielles récursives obtenues grâce au lemme.

Arbres binaires

On considère des arbres binaires éventuellement infinis représentés par l'ensemble de leurs nœuds. On représente un nœud par le chemin fait depuis la racine pour l'atteindre, c'est-à-dire par un mot sur $\{0, 1\}$. Un arbre est donc un ensemble de mot clos par préfixe. On appelle branche d'un arbre infini T tout mot infini dont les préfixes sont tous des nœuds de T.

Arbres binaires

On considère des arbres binaires éventuellement infinis représentés par l'ensemble de leurs nœuds. On représente un nœud par le chemin fait depuis la racine pour l'atteindre, c'est-à-dire par un mot sur $\{0,1\}$. Un arbre est donc un ensemble de mot clos par préfixe. On appelle branche d'un arbre infini T tout mot infini dont les préfixes sont tous des nœuds de T.

Definition

Soient T_1 et T_2 deux arbres, on dit que $f : T_1 \to T_2$ est un plongement de T_1 dans T_2 lorsque pour tout $t_1 \in T_1$,t_1 est un sous-mot de $f\,(t_1)$.

Lorsqu'un arbre se plonge dans un autre, on retrouve donc sa structure dans celle du second. On note B_n l'arbre binaire complet de profondeur n et on appelle rang d'un arbre T l'entier n maximal s'il existe tel que B_n se plonge dans T.

Arbres récursivement énumérables de rang fini

Lemme

Si T est un arbre récursivement énumérable de rang fini alors toutes les branches de T sont récursives.

Arbres récursivement énumérables de rang fini

Lemme

Si T est un arbre récursivement énumérable de rang fini alors toutes les branches de T sont récursives.

Démonstration.

On construit un algorithme qui calcule à partir d'une profondeur donnée le nœud de la branche t à cette profondeur. $\square$

Lemme

Pour tout $n \in \mathbb{N}$ *et tout 2-coloriage* $c : B_{2n} \to \{0, 1\}$, *il existe un plongement* g *monochromatique de* B_n *dans* B_{2n}.

Propriétés combinatoires des arbres binaires

Lemme

Pour tout $n \in \mathbb{N}$ *et tout 2-coloriage* $c : B_{2n} \to \{0,1\}$, *il existe un plongement* g *monochromatique de* B_n *dans* B_{2n}.

Lemme

Pour tout $n \geq 1$ *et tout arbre* T *de rang* $rg(T) \geq 4^n - 2$, *il existe des nœuds* $t_1, \ldots, t_{(n+1)}$ *de* T, *des entiers* $x_1 \leq \ldots \leq x_n$ *et* $b \in \{0,1\}$ *tels que :*

$$\text{pour tous } i = 1, \ldots, n,\ j = 1, \ldots, n+1 : t_j(x_i) = \begin{cases} b & \text{si } i \geq j \\ 1 - b & \text{si } i < j \end{cases}$$

Propriétés combinatoires des arbres binaires

Lemme

Pour tout $n \in \mathbb{N}$ et tout 2-coloriage $c : B_{2n} \to \{0,1\}$, il existe un plongement g monochromatique de B_n dans B_{2n}.

Lemme

Pour tout $n \geq 1$ et tout arbre T de rang $rg(T) \geq 4^n - 2$, il existe des nœuds $t_1, \ldots, t_{(n+1)}$ de T, des entiers $x_1 \leq \ldots \leq x_n$ et $b \in \{0,1\}$ tels que :

$$\text{pour tous } i = 1, \ldots, n,\ j = 1, \ldots, n+1 : t_j(x_i) = \begin{cases} b & \text{si } i \geq j \\ 1-b & \text{si } i < j \end{cases}$$

En particulier, $\{\sum_{i=1}^{n} t_j(x_i) \,|\, 1 \leq j \leq n+1\} = \{0, \ldots, n\}$.

Démonstration du théorème de cardinalité

Théorème

Si pour $m \in \mathbb{N}$*, il existe une fonction* G *récursive* $\mathbb{N}^m \to \mathcal{P}\left(\{0, \ldots, m\}\right) - \{\{0, \ldots, m\}\}$*, telle que pour tous* $(x_1, \ldots, x_m) \in \mathbb{N}^m$ *:*

$$\#_{A,m}\left(x_1, \ldots, x_m\right) \in G\left(x_1, \ldots, x_m\right)$$

alors A *est récursive.*

Démonstration.

D'après l'hypothèse on peut construire un arbre récursivement énumérable :

$$T_G = \left\{ t \in \{0,1\}^* \,|\forall x_1 \leq \ldots \leq x_m \leq |t|, \sum_{i=1}^{m} t\,(x_i) \in G\,(x_1, \ldots, x_m) \right\}$$

Cette définition contredit la conclusion du précédent lemme, donc l'hypothèse du lemme n'est pas vérifiée par T_G : T_G est donc de rang inférieur à $4^m - 2$ donc fini ! Or χ_A est une branche de T_G, arbre récursivement énumérable de rang fini, donc χ_A est récursive. $\square$