Le théorème de cardinalité

Michaël Monerau
Janvier 2008

1. La conjecture
   - Oracles et objectifs de l'étude
   - Nonspeedup theorem
   - La conjecture de cardinalité
2. Le théorème de cardinalité
   - Enoncé du théorème
   - Fonctions calculées par requêtes bornées
   - Preuve de la conjecture
3. Preuve du théorème de cardinalité
   - Codage
   - Branches récursives
   - Rang d'un arbre binaire
   - Arbres de rang fini
   - La preuve

Objectifs

Un ***oracle*** est une machine de Turing qui permet de décider un certain problème en une étape de calcul. Un oracle renvoie donc toujours 0 ou 1.

Objectif

Mesurer la décidabilité d'une partie A de $\mathbb{N}$ selon le nombre de requêtes nécessaires à un oracle fixé pour répondre à des questions précises sur A.

Théorème de Beigel

Théorème (Nonspeedup theorem, Beigel, 1987)

Soit A une partie de $\mathbb{N}$. Soit la fonction :

$$f_n^A : \left| \begin{array}{ccc} \mathbb{N}^{2^n} & \longrightarrow & \{0,1\}^{2^n} \\ (x_1, \dots, x_{2^n}) & \longmapsto & (\chi_A(x_1), \dots, \chi_A(x_{2^n})) \end{array} \right.$$

Si f_n^A peut être calculée avec au plus n requêtes à un oracle B, alors A est récursif.

Si A est *trop compliqué*, il faut beaucoup de requêtes à un oracle pour répondre à une question le concernant.

La conjecture de cardinalité

Calcul des 2^n valeurs de la fonction indicatrice

$$\downarrow$$

Calcul du nombre d'éléments parmi $(x_1, \ldots, x_{2^n})$ qui sont dans A

$$\#^A_{2^n} : \left| \begin{array}{ccc} \mathbb{N}^{2^n} & \longrightarrow & \{0 \ldots 2^n\} \\ (x_1, \ldots, x_{2^n}) & \longmapsto & \#\{i \in \mathbb{N} \mid x_i \in A\} \end{array} \right.$$

Conjecture de la cardinalité, Beigel, 1987

Si $\#^A_{2^n}$ peut être calculée en faisant au plus n requêtes à un oracle B, alors A est récursif.

La conjecture de cardinalité

Calcul des 2^n valeurs de la fonction indicatrice

$$\downarrow$$

Calcul du nombre d'éléments parmi $(x_1, \ldots, x_{2^n})$ qui sont dans A

$$\#^A_{2^n} \quad : \left| \begin{array}{ccc} \mathbb{N}^{2^n} & \longrightarrow & \{0 \ldots 2^n\} \\ (x_1, \ldots, x_{2^n}) & \longmapsto & \#\{i \in \mathbb{N} \mid x_i \in A\} \end{array} \right.$$

Conjecture de la cardinalité, Beigel, 1987

Si $\#^A_{2^n}$ peut être calculée en faisant au plus n requêtes à un oracle B, alors A est récursif.

Fonctions n-énumérables

Définition (fonction n-énumérable)

On dit qu'une fonction $f : \mathbb{N}^p \longrightarrow \mathbb{N}$ est n-énumérable s'il existe une machine de Turing M telle que, sur chaque entrée $(x_1, \ldots, x_p)$, M écrit sur sa bande de sortie au plus n entiers tels que l'un d'eux au moins est $f(x_1, \ldots, x_p)$.
M ne termine pas forcément, mais elle écrit nécessairement $f(x_1, \ldots, x_p)$ au bout d'un certain temps.

n-énumérabilité : calcul approché.

Le théorème de cardinalité

$$\#_m^A : \left| \begin{array}{ccc} \mathbb{N}^{2^n} & \longrightarrow & \{0 \ldots m\} \\ (x_1, \ldots, x_m) & \longmapsto & \#\{i \in \mathbb{N} \mid x_i \in A\} \end{array} \right.$$

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

$\#_m^A$ est « moins » que récursive, mais on aboutit toujours à la récursivité de A.

Requêtes bornées et fonctions récursives

Lemme (Lien avec les fonctions partielles récursives)

Soient $p \geq 1$, et une fonction $f : \mathbb{N}^p \longrightarrow \mathbb{N}$. On suppose que f peut être calculée avec au plus n requêtes à un oracle B.

Alors il existe un ensemble S de fonctions partielles récursives tel que $\#S \leq 2^n$ et :

$$\forall x \in \mathbb{N}^p, \quad \exists h \in S \quad tq \quad f(x) = h(x)$$

Preuve de la conjecture à partir du théorème

Conjecture de la cardinalité, Beigel, 1987

Si $\#_{2^n}^A$ peut être calculée en faisant au plus n requêtes à un oracle B, alors A est récursif.

Démonstration.

1. $\#_{2^n}^A$ calculable avec au plus n requêtes à un oracle $B \Rightarrow$ ensemble S de fonctions partielles récursives de cardinal au plus 2^n et tel que :

$$\forall x \in \mathbb{N}^{2^n},\ \exists h \in S, \quad \#_{2^n}^A(x_1 \ldots x_{2^n}) = h(x_1 \ldots x_{2^n})$$

2. Pour énumérer $\#_{2^n}^A$, exécution en parallèle de toutes les fonctions de S.
3. $\#_{2^n}^A$ est 2^n-énumérable (car $\#S \leq 2^n$), d'où la conjecture par le théorème.

$\square$

Preuve de la conjecture à partir du théorème

Conjecture de la cardinalité, Beigel, 1987

Si $\#_{2^n}^A$ peut être calculée en faisant au plus n requêtes à un oracle B, alors A est récursif.

Démonstration.

1. $\#_{2^n}^A$ calculable avec au plus n requêtes à un oracle $B \Rightarrow$ ensemble S de fonctions partielles récursives de cardinal au plus 2^n et tel que :

$$\forall x \in \mathbb{N}^{2^n},\ \exists h \in S, \quad \#_{2^n}^A(x_1 \ldots x_{2^n}) = h(x_1 \ldots x_{2^n})$$

2. Pour énumérer $\#_{2^n}^A$, exécution en parallèle de toutes les fonctions de S.
3. $\#_{2^n}^A$ est 2^n-énumérable (car $\#S \leq 2^n$), d'où la conjecture par le théorème.

$\square$

Preuve de la conjecture à partir du théorème

Conjecture de la cardinalité, Beigel, 1987

Si $\#^A_{2^n}$ peut être calculée en faisant au plus n requêtes à un oracle B, alors A est récursif.

Démonstration.

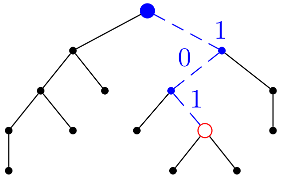
1. $\#^A_{2^n}$ calculable avec au plus n requêtes à un oracle $B \Rightarrow$ ensemble S de fonctions partielles récursives de cardinal au plus 2^n et tel que :

$$\forall x \in \mathbb{N}^{2^n},\ \exists h \in S, \quad \#^A_{2^n}(x_1 ... x_{2^n}) = h(x_1 ... x_{2^n})$$

2. Pour énumérer $\#^A_{2^n}$, exécution en parallèle de toutes les fonctions de S.
3. $\#^A_{2^n}$ est 2^n-énumérable (car $\#S \leq 2^n$), d'où la conjecture par le théorème.

$\square$

Codage des arbres binaires sur l'alphabet $\{0, 1\}$



Codage d'un arbre : ensemble des codages de tous ses noeuds. Codage de cet arbre :

$$\{\underbrace{0, 00, 01, 000, 001, 0000}_{\text{sous-arbre gauche}}, \underbrace{1, 10, 11, 100, 101, 110, 1010, 1011}_{\text{sous-arbre droit}}\}$$

Un ensemble de mots sur $\{0, 1\}$ est un arbre s'il est clos par préfixe.

Branches récursives

Branche infinie = mot infini sur le langage $\{0,1\}$, donc *fonction indicatrice* d'une certaine partie X de $\mathbb{N}$:

Définition (branche récursive)

Soient $T \subset \{0,1\}^*$ un arbre et b une branche de T. On note :

$$X = \{i \in \mathbb{N} \quad | \quad b[i] = 1\} \subset \mathbb{N}$$

On dit que b est une branche récursive de T si X est un ensemble récursif.

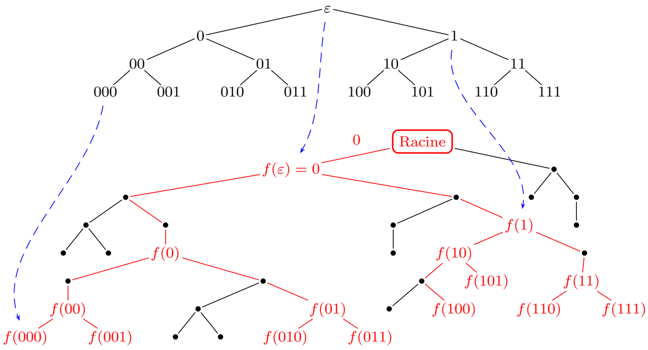
Nous allons voir que A est l'ensemble sous-jacent d'une branche récursive d'un arbre bien choisi.

Plongements

Définition (plongement)

$f : B_n \longrightarrow T$ est un plongement si pour $|w| \leq n-1$:

- $f(w).0$ est préfixe de $f(w.0)$
- $f(w).1$ est préfixe de $f(w.1)$



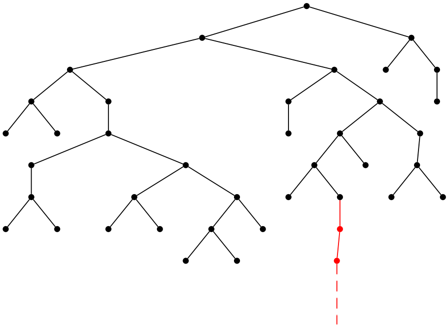
Rang

Définition (Rang)

Soit T un arbre. On définit le rang (fini ou non) de T par :

$$\operatorname{rg} T \quad = \quad \sup_{n \geq 1} \{ n \in \mathbb{N}^* \mid B_n \text{ est plongeable dans } T \}$$

Arbre de rang 3 :



Intérêt du rang fini

Lemme (Branches récursives et rang fini)

Soit T un arbre de rang fini. On suppose de plus qu'il est récursivement énumérable, c'est-à-dire que c'est un ensemble récursivement énumérable vu comme langage sur $\{0, 1\}$.

Alors chacune des branches de T est récursive.

La preuve

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

Démonstration.

1. $\#_m^A$ m-énumérable par φ.
2. $T_A = \{t \in \{0,1\}^* \mid \forall (x_1 \ldots x_m), \sum_{i=1}^m t[x_i] \in \varphi(x_1 \ldots x_m)\}$
3. T_A est un arbre récursivement énumérable et de rang fini.
4. χ_A en est une branche.
5. Donc χ_A est récursive, et A est récursif.

$\square$

La preuve

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

Démonstration.

1. $\#_m^A$ m-énumérable par φ.
2. $T_A = \{t \in \{0,1\}^* \mid \forall (x_1 \ldots x_m), \sum_{i=1}^m t[x_i] \in \varphi(x_1 \ldots x_m)\}$
3. T_A est un arbre récursivement énumérable et de rang fini.
4. χ_A en est une branche.
5. Donc χ_A est récursive, et A est récursif.

$\square$

La preuve

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

Démonstration.

1. $\#_m^A$ m-énumérable par φ.
2. $T_A = \{t \in \{0,1\}^* \mid \forall(x_1...x_m), \sum_{i=1}^m t[x_i] \in \varphi(x_1...x_m)\}$
3. T_A est un arbre récursivement énumérable et de rang fini.
4. χ_A en est une branche.
5. Donc χ_A est récursive, et A est récursif.

$\square$

La preuve

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

Démonstration.

1. $\#_m^A$ m-énumérable par φ.
2. $T_A = \{t \in \{0,1\}^* \mid \forall(x_1 \ldots x_m), \sum_{i=1}^m t[x_i] \in \varphi(x_1 \ldots x_m)\}$
3. T_A est un arbre récursivement énumérable et de rang fini.
4. χ_A en est une branche.
5. Donc χ_A est récursive, et A est récursif.

$\square$

La preuve

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

Démonstration.

1. $\#_m^A$ m-énumérable par φ.
2. $T_A = \{t \in \{0,1\}^* \mid \forall (x_1 \ldots x_m), \sum_{i=1}^m t[x_i] \in \varphi(x_1 \ldots x_m)\}$
3. T_A est un arbre récursivement énumérable et de rang fini.
4. χ_A en est une branche.
5. Donc χ_A est récursive, et A est récursif.

$\square$

Conclusion

Théorème (de cardinalité, Kummer, 1992)

Soient A une partie de $\mathbb{N}$ et $m \geq 1$.
Si $\#_m^A$ est m-énumérable, alors A est récursif.

Conjecture de la cardinalité, Beigel, 1987

Si $\#_{2^n}^A$ peut être calculée en faisant au plus n requêtes à un oracle B, alors A est récursif.