IP = PSPACE

Soutenance de langages formels, calculabilité, complexité

Jean Bastien Grill

Ecole Normale Supérieure

Jeudi 6 janvier 2010

Système de preuve interactive

Définition d'un système de preuve interactive

C'est un couple de machines de Turing $\mathcal{V}$,$\mathcal{P}$.
Ces deux machines de Turing échangent des messages de tailles polynomiale en l'entrée. $\mathcal{V}$ dispose d'un temps de calcul polynomial.
Aucune hypothèse n'est fait sur $\mathcal{P}$.

Définition de NP

Définition de NP

Soit un langage $\mathbb{L}$,

1. $\exists\, \mathcal{P}$, $x \in \mathbb{L} \Longrightarrow \mathcal{V}$ décide que la preuve est correcte
2. $\forall\, \mathcal{P}$, $x \notin \mathbb{L} \Longrightarrow \mathcal{V}$ décide que la preuve est incorrecte

Définition de IP

Définition de IP

Soit un langage $\mathbb{L}$,

1. $\exists\, \mathcal{P}$, $x \in \mathbb{L} \Longrightarrow \mathcal{V}$ décide que la preuve est correcte
2. $\forall\, \mathcal{P}$, $x \notin \mathbb{L} \Longrightarrow \mathcal{V}$ décide avec une probabilité supérieure à $1/2$ que la preuve est incorrecte

Démonstration

Transformation en polynôme

Déterminer de façon probabiliste si deux polynômes sont égaux

Problème

On genère une nombre, uniformément aléatoire sur un ensemble fini, et on teste si les deux polynômes coïncident sur cette valeur.

Preuve

La probabilité d'erreur est de $\frac{n}{|E|}$, où n est le degré du polynôme et E l'ensemble des valeurs.

Propriétés

1. NP ⊆ IP

Propriétés

1. NP ⊆ IP
2. Co-NP ⊆ IP

La taille d'une formule est polynomiale

Lemme

Le degré du polynôme associé à une formule logique est polynomial en la taille de la formule logique.

Remarque - Prevue

La degré est en fait majoré par la taille de la formule.

Propriétés

1. NP ⊆ IP
2. Co-NP ⊆ IP
3. IP est clos par complémentation

Résultat

$$IP = PSPACE$$