Modèles de calcul, TD numéro 11
Natacha Portier
lundi 29 avril 2002

Question 1

La classe **P/poly** est l'ensemble des langages L tels qu'il existe une machine de Turing travaillant en temps polynomial M et une suite de mots booléens $(\bar{a}_n)$ où pour tout n le mot $\bar{a}_n$ est de longueur $q(n)$ et q est un polynôme et $\bar{x} = x_1...x_n \in L$ si et seulement si M accepte $\bar{x}\bar{a}_n$.

Montrer que **P/poly** est l'ensemble des langages reconnus par une suite de circuits de taille polynomiale.

Question 2,1

Nous considérons des machines de Turing non-déterministes telles que le temps de calcul ne dépende que de la longueur de l'entrée et qu'à chaque pas de calcul il y ait exactement deux calculs possibles. La classe **RP** (*randomized polynomial time*) est l'ensemble des problèmes X tels qu'il existe une machine de Turing polynomiale de Monte Carlo M qui décide X, c'est à dire une machine de Turing comme ci-dessus travaillant en temps polynomial et qui vérifie : si $\bar{x} \notin X$ alors tous les calculs de M refusent $\bar{x}$ et si $\bar{x} \in X$ alors au moins la moitié des calculs de M acceptent $\bar{x}$. C'est une classe de complexité sémantique. Bien sur, $\mathbf{P} \subseteq \mathbf{RP} \subseteq \mathbf{NP}$.

Montrer que pour tout problème X dans **RP** et pour tout ϵ strictement compris entre 0 et 1 il existe une machine de Turing polynomiale de Monte Carlo M qui décide X avec une proportion d'erreur au plus ϵ, c'est à dire telle que pour tout $\bar{x} \in X$ la proportion de calculs qui refusent $\bar{x}$ est au plus ϵ.

Question 2,2

On considère une machine non-déterministe qui effectue un calcul de longueur k sur une entrée de longueur n comme une machine déterministe qui utilise les bits (aléatoires) $a_1...a_k$ pour faire ses choix. Si $a_1...a_k$ est donné alors la machine est déterminisée pour les entrées de longueur n.

Soit L un langage et M une machine de Monte Carlo qui décide L avec une proportion d'erreur au plus ϵ, et qui effectue un calcul de longueur k pour les entrées de longueur n. Monter que pour ϵ suffisamment petit, il existe des bits $a_1...a_k$ tel que la machine déterminisée pour les entrées de longueur n décide de L pour les entrées de longueur n.

Question 2,3

Montrer que $\mathbf{RP} \subseteq \mathbf{P/poly}$.

Question 3

La classe **BPP** (*Bounded Probability of error*) est l'ensemble des problèmes X tels qu'il existe une machine de Turing non-déterministe polynomiale M qui décide X avec une proportion d'erreur au plus $1/4$, i.e. si $\bar{x} \in X$ alors plus de $3/4$ des calculs de M acceptent $\bar{x}$ et si $\bar{x} \notin X$ alors plus de $3/4$ des calculs de M rejettent $\bar{x}$. Il est clair que $\mathbf{RP} \subseteq \mathbf{BPP}$ et que $\mathbf{BPP} = \mathbf{co} - \mathbf{BPP}$. On ne sait pas si $\mathbf{BPP} \subseteq \mathbf{NP}$. Nous allons montrer que $\mathbf{BPP} \subseteq \mathbf{P/poly}$.

Question 3,1

Soit X un problème **BPP** décidé par la machine M. Considérons la machine de Turing non-déterministe M' qui simule 3 fois la machine M puis choisit le résultat le plus fréquent. Quelle est sa proportion d'erreur ? Généraliser à une machine qui simule $2m+1$ fois la machine M puis choisit le résultat le plus fréquent. On pourra utiliser la formule de Stirling.

Question 3,2

Montrons que tout problème **BPP** est décidé par une suite de circuits polynomiale. Soit L un langage **BPP** décidé par une machine non-déterministe M avec une proportion d'erreur au plus ϵ. Donner des conditions suffisantes pour qu'il existe un uple de choix pour lesquels la machine déterminisée M décide de L pour les entrées de longueur n. Conclure.

Question 4,1

La classe **PP** est l'ensemble des problèmes X tels qu'il existe une machine de Turing non-déterministe polynomiale M telle que $\bar{x} \in X$ si et seulement si strictement plus de la moitié des calculs de M acceptent $\bar{x}$. C'est une classe de complexité syntaxique. Il est clair que $\mathbf{BPP} \subseteq \mathbf{PP}$. Montrer que $\mathbf{NP} \subseteq \mathbf{PP}$.

Question 4,2

Soit ϵ un nombre strictement compris entre 0 et 1. La classe $\mathbf{PP}_\epsilon$ est l'ensemble des problèmes X tels qu'il existe une machine de Turing non-déterministe polynomiale M telle que $\bar{x} \in X$ si et seulement si la proportion des calculs de M qui acceptent $\bar{x}$ est au moins ϵ. Montrer que $\mathbf{PP}_\epsilon = \mathbf{PP}$.

Question 4,3

Montrer que $\mathbf{PP} = \mathbf{co} - \mathbf{PP}$.