

Complexité avancée 2008-2009

TD 7

15 décembre 2008

Exercice 1. Montrer que :

- $NP^{BPP} \subseteq MA$.
- $AM \subseteq BPP^{NP}$.
- Si $NP \subseteq P/Poly$ alors $MA = AM$.

Exercice 2. On considère les variantes de $AM[k]$ suivantes :

- $AM[k]$ avec *complétude parfaite* : si l'entrée x est dans le langage, alors le verifieur A doit en être convaincu avec probabilité 1.
- $AM[k]$ avec *correction parfaite* : si l'entrée x n'est pas dans le langage, alors A doit rejeter avec probabilité 1.

Montrer que :

- Si $L \in AM[k]$, alors $L \in AM[k+1]$ avec complétude parfaite.
- Si $L \in AM[k]$ avec correction parfaite, alors L est dans une classe de complexité familière.

Exercice 3 : Multi-Prover Interactive Systems. Let P_1, \dots, P_k be infinitely powerfull machines and V be a probabilistic polynomial-time machine. The verifier V shares communication tapes with each P_i , but different provers P_i and P_j have no tapes they can both access besides the input tape. A round of a multi-prover interactive protocol consists of messages from the verifier to some or all of the provers followed by messages from these provers to the verifier.

P_1, \dots, P_k and V form a multi-prover interactive protocol for a language L if :

- If $x \in L$, then $Pr[(P_1, \dots, P_k, V)(x) = acc] > 1 - 2^{-n}$.
- If $x \notin L$, then for all provers P'_1, \dots, P'_n , $Pr[(P'_1, \dots, P'_n, V)(x) = acc] < 2^{-n}$.

In this case, we note $L \in MIP_k$.

1. Show that $L \in MIP_k \implies L \in MIP_2$.
2. Let M be a probabilistic polynomial-time Turing machine with access to an oracle. We say that a language L is accepted by M iff
 - If $x \in L$, then there is an oracle O s.t. M^O accepts x with probability greater than $1 - 2^{-n}$
 - If $x \notin L$, then for any oracle O' , $M^{O'}$ accepts x with probability smaller than 2^{-n}

Show that L is accepted by a multi-prover interactive protocol if and only if L is accepted by a probabilistic oracle machine.