

Complexité avancée 2008-2009

TD 8

14 janvier 2009

I. Multi-Prover Interactive Systems. Let P_1, \dots, P_k be infinitely powerful 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. 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.

II. Zero-Knowledge Interactive Systems. Loosely speaking, we say that an interactive proof system (P, V) , for a language L , is zero-knowledge if whatever can be efficiently computed after interacting with P on input $x \in L$, can also be efficiently computed from x (without interaction).

Formally, we say that a prover strategy P is (perfect) zero-knowledge over a language L if for every probabilistic polynomial time interactive machine V^* there exists an (ordinary) probabilistic polynomial time machine M^* (that could answer \perp) such that for every $x \in L$ the following two conditions hold :

- $M^*(x)$ outputs \perp with probability at most $\frac{1}{2}$;
- The random variables $(P, V^*)(x)$ and $(M^*(x) | M^*(x) \neq \perp)$ are identically distributed.

An interactive proof system (P, V) for L is zero-knowledge if P is zero-knowledge for L . We call ZK the class of languages that have zero-knowledge interactive proof systems.

1. Show that $BPP \subseteq ZK$.
2. Let $view_{(P,V^*)}(x)$ be the final view of V^* after running (P, V^*) on x . Show that we can replace $(P, V^*)(x)$ by $view_{P,V^*}(x)$ above to get an equivalent definition.
3. Construct a perfect zero-knowledge interactive protocol for the problem of graph isomorphism.