Theory of Computation

Solutions to Homework 5

Problem 1. Do zero-knowledge proofs exist for every language in BPP? Briefly justify your answer.

Proof. Yes. In an interactive proof system for any language in BPP, the prover needs to do nothing. The verifier itself can determine whether to accept the input. Clearly, the empty transcript of interaction can be output by a polynomial-time Turing machine. □

Problem 2. It is known that there exists a polynomial-time algorithm R with the following properties.

(i). Given a satisfiable boolean expression, R outputs a satisfiable CNF with exactly 3 literals in each clause.

(ii). Given an unsatisfiable boolean expression, R outputs a CNF ϕ with exactly 3 literals in each clause such that no truth assignment can satisfy more than a 0.9 fraction of the clauses of ϕ.

Prove that if there exists a polynomial-time approximation scheme for MAX3SAT, then SAT $\in$ P. (Hint: Let M be a polynomial-time, 0.01-approximation algorithm for MAX3SAT. For a CNF x, how many clauses of $R(x)$ are satisfied by $M(R(x))$ if $x \in$ SAT? How many are satisfied otherwise?)

Proof. If $x \in$ SAT, then $R(x)$ is satisfiable. So $M(R(x))$ satisfies at least a 0.99 fraction of the clauses of $R(x)$ because M is a 0.01-approximation algorithm. If $x \notin$ SAT, item (ii) forbids $M(R(x))$ or any truth assignment from satisfying more than a 0.9 fraction of the clauses of $R(x)$. To determine whether $x \in$ SAT, therefore, one computes the fraction f of the clauses of $R(x)$ satisfied by $M(R(x))$. Then one accepts if $f \geq 0.99$ and rejects otherwise. □