Theory of Computation

Homework 5
Due: 2008/01/06

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

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?)