Theory of Computation

Solutions to Homework 4

Problem 1. Let A be an algorithm that correctly determines whether a given Boolean circuit is satisfiable. Assume that the expected running time of A is polynomial in its input length, so A solves CIRCUIT-SAT in expected polynomial time. Argue whether NP $\subseteq$ BPP.

Proof. Let $p(n)$ be a polynomial bounding the expected running time of A on inputs of length n. By Markov's inequality, the probability that the running time of A exceeds $3p(n)$ given an input of length n is at most $1/3$. Hence, by running A for $3p(n)$ steps on inputs of length n, one can determine with probability at least $1 - 1/3$ whether an input is satisfiable. We therefore obtain a polynomial-time algorithm for CIRCUIT-SAT which errs with probability at most $1/3$ on each input. As CIRCUIT-SAT is NP-complete, NP $\subseteq$ BPP. □

Problem 2. Should all languages that have polynomial circuits be in PSPACE? Briefly justify your answer.

Proof. No. There exist undecidable languages with polynomial circuits, but PSPACE contains only decidable languages. □