Theory of Computation

Final Examination on January 13, 2009

Problem 1 (25 points)**.** Show that if SAT $\in$ P, then FSAT has a polynomial-time algorithm. (Hint: You may want to use the self-reducibility of SAT.)

Proof. Assume SAT $\in$ P. We describe below how to find a truth assignment to an input Boolean expression ϕ in time polynomial in $|\,\phi\,|$. If $\phi \notin$ SAT then it does not have a satisfying truth assignment. So we assume otherwise. Denote the variables of ϕ by $x_1, \ldots, x_n$. Let t be the empty truth assignment to $x_1, \ldots, x_n$. For $i = 1$ up to n, we expand t to include the assignment $x_i =$ true if $\phi[\,t \cup \{x_i = \text{true}\}\,] \in$ SAT and $x_i =$ false otherwise. Clearly, after n iterations, t will end up being a satisfying assignment of ϕ. It is also clear that the above procedure runs in time polynomial in $|\,\phi\,|$. □

Problem 2 (25 points)**.** Let x be a random variable taking positive integer values. Show that for any $k > 0$, $\text{prob}[x \geq kE[\,x\,]] \leq 1/k$.

Proof. Let p_i be the probability that $x = i$. Then

$$\begin{aligned} E[\,x\,] &= \sum_i i p_i \\ &= \sum_{i<kE[x]} i p_i + \sum_{i \geq kE[x]} i p_i \\ &\geq kE[\,x\,] \times \text{prob}\,[\,x \geq kE[\,x\,]\,]\,. \end{aligned}$$

□

Problem 3 (25 points)**.** In the slides, we have shown a 2-round interactive proof system for GRAPH NONISOMORPHISM. Hence GRAPH NONISOMORPHISM is in IP. But is GRAPH ISOMORPHISM also in IP? Briefly justify your answer.

Proof. Let $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ be isomorphic graphs. A permutation π on V with $(u, v) \in E_1 \Leftrightarrow (\pi(u), \pi(v)) \in E_2$ constitutes a succinct certificate for $G_1 \cong G_2$. Nonisomorphic graphs cannot have such certificates. □

Problem 4 (25 points)**.** Show that if #SAT $\in$ FP, then P = NP.

Proof. Given a Boolean formula ϕ, we calculate its number of satisfying truth assignments, k, in polynomial time. Then we declare $\phi \in$ SAT if and only if $k \geq 1$. As SAT is NP-complete, P = NP. □