Computational complexity: Assignment 4

Due date: November 20, 2013

General instructions:

- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly urged to solve the problems by yourself.
- If you discuss with someone else or refer to any material (other than the course notes) then please put a reference in your answer script stating clearly whom or what you have consulted with and how it has benifited you. We would appreciate your honesty.
- If you need any clarification, please ask the instructor.

Total: 50 points

In the following problems, n stands for length of input string (unless mentioned otherwise in the problem).

1. (**4 points**) [Excercise-7.5 from Arora-Barak's book] Describe a real number ρ such that given a random coin that comes up with "Heads" with probability ρ, a Turing machine can decide an undecidable language in (probabilistic) polynomial time.

2. (**7 points**) [Excercise-7.6 from Arora-Barak's book]

   (a) (**3 points**) Prove that a language L is in ZPP iff there exists a polynomial-time PTM M with outputs in $\{0, 1, ?\}$ such that for every $x \in \{0,1\}^*$, with probability 1, $M(x) \in \{L(x), ?\}$ and $\Pr[M(x) = ?] \leq \frac{1}{2}$.

   (b) (**4 points**) Show that $\mathsf{ZPP} = \mathsf{RP} \cap \mathsf{coRP}$.

3. (**6 points**) [Excercise-7.7 from Arora-Barak's book] A nondeterministic circuit has two inputs x, y. We say that C accepts x iff there exists y such that $C(x, y) = 1$. The size of the circuit is measured as a function of $|x|$. Let $\mathsf{NP}_{/\mathsf{poly}}$ be the languages that are decided by polynomial size nondeterministic circuits. Show that $\mathsf{BP} \cdot \mathsf{NP} \subseteq \mathsf{NP}_{/\mathsf{poly}}$.

4. (**8 points**) [Excercise-7.8 from Arora-Barak's book] Show that if $\overline{3\ \mathrm{SAT}} \in \mathsf{BP} \cdot \mathsf{NP}$, then PH collapses to Σ_3^p. (Thus it is unlikely that $\overline{3\ \mathrm{SAT}} \leq_r 3\ \mathrm{SAT}$)

5. (**6 points**) [Excercise-7.9 from Arora-Barak's book] Show that $\mathsf{BPL} \subseteq \mathsf{P}$.

6. (**5 points**) [Excercise-7.10 from Arora-Barak's book] Show that the random walk idea for solving connectivity does not work for directed graphs. In other words, describe a directed graph on n vertices and a starting point s such that the expected time to reach t is $\Omega(2^n)$, even though there is a directed path from s to t.

7. (**14 points**) [Excercise-8.1 & 8.2 from Arora-Barak's book] Prove the following assertions about class IP:

   (a) (**3 points**) Let IP' denote the class obtained by allowing the prover to be probabilistic, i.e. the prover's strategy can be chosen at random from some distribution on functions. Prove that $\mathsf{IP}' = \mathsf{IP}$.

   (b) (**6 points**) Prove that $\mathsf{IP} \subseteq \mathsf{PSPACE}$.

   (c) (**2 points**) Let IP' denote the class obtained by changing the 'soundness' constant $1/3$ to 0. Prove that $\mathsf{IP}' = \mathsf{IP}$.

   (d) (**3 points**) Let IP' denote the class obtained by requiring in the 'completeness condition' that there exists a single prover P for every $x \in L$ (rather than for every $x \in L$ there is a prover). Prove that $\mathsf{IP}' = \mathsf{IP}$.