CSE 531: Computability and Complexity — Autumn 2002

Problem Set #5 — Instructor: Venkatesan Guruswami

Due on Tuesday, **December 10, 2002** in class.

Instructions: You are permitted (though not exactly encouraged) to collaborate with fellow students taking the class in solving problem sets. If you do so, *please indicate for each problem the people you worked with on that problem.* Note that you must write down solutions on your own and collaboration must be restricted to a discussion of solution ideas. Solutions are expected to be your original work and so you must refrain from looking up solutions or solution ideas from websites or other literature.

---

1. Define the class polyL $= \bigcup_{k\geq 1} \text{SPACE}(\log^k n)$ consisting of languages that can decided in polylogarithmic space.
   (a) Prove that NL $\neq$ polyL.
   (b) Prove that polyL $\neq P$.
   (Hint: You are permitted to to use the result of Theorem 10.40 from Sipser's book, or that of Problem 7 from Problem Set 4.)

2. (a) Prove that if NEXPTIME $\neq$ EXPTIME, then P $\neq$ NP. (Problem 9.19, Sipser's book)
   (b) Prove that if BPP = EXPTIME, then P $\neq$ NP.

3. Prove that there exists an oracle C for which $\text{NP}^C \neq \text{coNP}^C$. (Problem 9.12, Sipser's book)

4. Prove the following version of the Schwarz-Zippel lemma. Let $\mathbb{F}$ be any field (finite or infinite) and let $Q(x_1, x_2, \ldots, x_m) \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be a non-zero m-variate polynomial over $\mathbb{F}$ of *total* degree d. Fix any finite set $S \subseteq \mathbb{F}$. Prove that

$$\textbf{Prob}[Q(r_1, r_2, \ldots, r_m) = 0] \leq \frac{d}{|S|}$$

   where the probability is taken over $r_1, r_2, \ldots, r_m$ that are chosen independently and uniformly at random from S.

5. State and prove a hierarchy theorem for circuit size. Your result should at least prove that circuits of size $O(n^a)$ are strictly more powerful than circuits of size $O(n^{a-1})$ for every integer $a \geq 2$ (and this will receive a good portion of the credit). The question as posed is deliberately vague, and solutions which are creative and/or establish the finest hierarchies will receive bonus points.

6. (a) Prove that if $L \in$ BPP, then there is a polynomially bounded function $p : \mathbb{N} \to \mathbb{N}$ and a polynomial time *deterministic* Turing machine V such that

$$x \in L \implies \text{Prob}_{r\in\{0,1\}^{p(|x|)}}[V \text{ accepts } (x,r)] \geq (1 - 2^{-2|x|})$$
$$x \notin L \implies \text{Prob}_{r\in\{0,1\}^{p(|x|)}}[V \text{ accepts } (x,r)] \leq 2^{-2|x|} \ .$$

   (b) Prove that every language in BPP has a circuit family of polynomial size that decides it. (Hint: Use (a) above)