CSE 531: Computability and Complexity — Autumn 2004

Problem Set #5 — Instructor: Venkatesan Guruswami

Due on Thursday, **December 9, 2004** in class.

Instructions: Same as Problem Set 1.

---

1. Prove that $\mathsf{P} \neq \mathsf{SPACE}(n)$.

2. 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

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

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

3. Prove that if $\mathsf{NEXPTIME} \neq \mathsf{EXPTIME}$, then $\mathsf{P} \neq \mathsf{NP}$. (Problem 9.19, Sipser's book)

4. Prove that if $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{NP} = \mathsf{RP}$.

5. (30 points) In this exercise, by circuits we imply Boolean circuits with NOT, AND, and OR gates of fan-in 2, and we measure the size of a circuit by the number of gates in it.

   (a) Prove that there exists a Boolean function $f : \{0,1\}^n \to \{0,1\}$ which cannot be computed by any circuit of size less than $\frac{2^n}{9n}$. (Hint: Use a circuit counting argument.)

   (b) Let $s : \mathbb{N} \to \mathbb{N}$ be a function such that $n \leq s(n) < \frac{2^n}{9n}$ for $n \geq 10$. Prove that for all large enough n, there exists a function $g : \{0,1\}^n \to \{0,1\}$ that can be computed by a circuit of size $2 \cdot s(n) + O(1)$ but not by a circuit of size $s(n)$.

   (c) Prove that for every $k \geq 1$, $\mathsf{EXPTIME} \not\subseteq \mathsf{SIZE}(n^k)$, in other words there is a language that can decided in exponential time but cannot be decided by a circuit family of size $O(n^k)$. (Hint: Use Part (b) above.)

   (d) Prove that $\mathsf{EXPSPACE} \not\subseteq \bigcup_{k \geq 1} \mathsf{SIZE}(n^k)$. In other words, show that some language in $\mathsf{EXPSPACE}$ does not have a polynomial sized circuit family deciding it.

   (e) **(Extra Credit)** Strengthen the result of Part (b) above by proving that there is a function $g : \{0,1\}^n \to \{0,1\}$ that can be computed by a circuit of size $s(n) + n + O(1)$ but not by a circuit of size $s(n)$.