CSE 531: Computability and Complexity — Autumn 2005

Problem Set #5 — Instructor: Paul Beame

Due on Thursday, **December 8, 2005** in class.

Instructions: Same as Problem Set 1.

---

1. (10 points) Define $UNIQUESAT = \{\langle\phi\rangle \mid \phi$ has precisely one satsifying assignment$\}$. Prove that $UNIQUESAT \in \mathsf{P}^{\mathsf{SAT}}$.

2. (10 points) Prove that an oracle C exists such that $\mathsf{NP}^{\mathsf{C}} \neq \mathsf{coNP}^{\mathsf{C}}$.

3. (10 points) 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 (the sum of the degrees of all variables in each monomial is at most 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.

4. (10 points) Prove that if $\mathsf{NEXPTIME} \neq \mathsf{EXPTIME}$, then $\mathsf{P} \neq \mathsf{NP}$. (Problem 9.19, Sipser's 1st edition; Problem 9.14 Sipser's 2nd edition.) Use the function *pad* as described in the hint from Sipser's book.

5. (10 points) Prove that evey language in BPP can be decided by a polynomial-size family of Boolean circuits. (Hint: use the amplification lemma to reduce the error on input x to smaller than $2^{-|x|}$ and then show that one can "hardwire" values into the circuit that can replace the randomness used.)

6. (10 points) Prove that if the polynomial-time hierarchy $\mathsf{PH} = \mathsf{PSPACE}$ then it has only a finite number of levels, i.e. $\mathsf{PH} = \Sigma_k^{\mathsf{P}}$ for some integer $k \geq 0$.

7. (Extra credit) Prove that if $\mathsf{NP} \subseteq \mathsf{BPP}$, then $\mathsf{NP} = \mathsf{RP}$.