CS 351: Problem Set 5

(assigned 10/31/2002; due 11/14/2002)

Some hints for PS5.

(1a) An $O(\log n)$ communication protocol for equality using polynomials over finite fields.

Treat the coefficients as polynomials with 0–1 coefficients over the field $\mathbf{Z}_p$, and let Alice send the evaluation of her polynomial on a random point of $\mathbf{Z}_p$. Make sure that p is large enough to make the protocol succeed, and small enough to keep the communication low.

(1b) A randomized *simultaneous protocol* with $o(n)$ communication for equality.

Multiple evaluations *a la* (1a), sufficiently many to ensure that with high probabilty, Alice and Bob evaluate their polynomials on a common point.

(2) If NP $\subseteq$ BPP, then NP $=$ RP.

Use the reduction from search to decision to construct satisfying assignments; you'll need some amplification too.

(3) Hitting sets and RP, BPP.

(No new hints here) Revisit the proof of BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$, and note that the "existence" proofs are really "abundance" proofs. Use this idea to define a set A and build a one-sided error randomized algorithm (RP type) for L that, on input x, tosses a set of coins y, and then needs to decide if (x, y) belongs to A. Then show that the instance (x, y) of A can be solved by a one-sided error randomized algorithm (again, RP type, but note that I am not claiming that $A \in$ RP). Use the hitting set to derandomize each step in turn.

(4) Approximate counting of satisfying assignments.

Suppose $2^k \leq N_\varphi < 2^{k+1}$. Let $h : \{0,1\}^n \longrightarrow \{0,1\}^\ell$ be chosen from a pairwise independent hash function family. Analyze the following cases separately: $\ell \geq k+3$ and $\ell \leq k-3$. In the first case, prove that with high probability, the element 0^ℓ will not have a pre-image a under h that is also a satisfying assignment of φ. (Idea: compute the expected number of satisfying assignments in $h^{-1}(0^\ell)$, and apply Markov's inequality.) In the second case, prove that with high probability, the element 0^ℓ will have a pre-image a under h that is also a satisfying assignment of φ. (Idea: compute the expected number of satisfying assignments in $h^{-1}(0^\ell)$, compute its variance, and apply Chebyshev's inequality, which says that for any r.v. X, $\Pr[|X - \mathrm{E}[X]| > \tau] < \mathrm{Var}[X]/\tau^2$. Chebyshev's inequality is an easy consequence of Markov's inequality applied to $(X - \mathrm{E}[X])^2$.) Then suppose you can answer the question "$(\exists a)[h(a) = 0^\ell \wedge \varphi(a)]$" for each ℓ; argue that 2^{ℓ^*}, where ℓ^* is the largest ℓ for which the answer to this question is "yes," is a good approximation to N_φ. This will give you something like a BPP algorithm using an NP oracle; then suitably replace randomness by quantifiers, as in the proof of BPP $\subseteq \Sigma_2^p \cap \Pi_2^p$.

(5) A one-way logspace probabilistic proof system for SAT.

Suppose the proof is an assignment; pick a random clause and check if it is satisfied, and then amplify (by suitably enhancing the proof system).