Advanced Complexity Theory
6.841/18.405J
Due: Wednesday, May 8, 2002

Madhu Sudan

Problem Set 4

Problems

1. (a) Show that if co-SAT is in AM (one-round interactive proofs with public coins), then the PH collapses.

   (b) Show that AMAM (the class of languages with two round interactive proofs with public coins) is contained in AM.

   (c) Show that AM with two-sided error is contained in AM with one-sided error.

2. (a) In the lecture on showing PSPACE $\subseteq$ IP, we showed that evaluation of straightline programs of polynomials with width $w = 2$ is in IP. (I.e., the ith polynomial can be computed with two oracle calls to the $(i-1)$th polynomial.) Generalize this to the case of straightline programs of polynomials with arbitrary (polynomial) width.

   (b) Using Part (a), give a direct proof that the permanent is in IP.

3. A p-prover 1-round proof system consists of a probabilistic polynomial time verifier V interacting with p provers $P_1, \ldots, P_p$. On input x of length n, the verifier tosses $r(n)$ coins, generates queries $q_1, \ldots, q_p$ and send q_i to P_i who responds with a_i, a string of length $a(n)$. The verifier then determines whether to accept or not based on x, the random string and the answers $a_1, \ldots, a_p$. Completeness and soundness are defined as usual.

   Show that SAT has a 3-prover 1-round proof system with perfect completeness, soundness bounded away from 1, where the verifier tosses $O(\log n)$ coins and the answers are poly $logn$ bits long.

   You may use the following version of the low-degree test.

   Let $\mathcal{L}_m$ be the space of lines in $\mathbb{F}^m$ and let $\mathbb{F}^{(d)}[x]$ denote the set of univariate polynomials of degree at most d. Given a function $f : \mathbb{F}^m \to \mathbb{F}$, let $f_{\text{aux}} : \mathcal{L}_m \to \mathbb{F}^{(d)}[x]$ be a function that maps lines in $\mathbb{F}^m$ to degree d polynomials. Consider the test that picks a random line $\ell \in \mathcal{L}_m$ and a point $x \in \ell$ at random, and then verifies if $(f_{\text{aux}}(\ell))(x)$ agrees with $f(x)$. Then this test has the following properties:

   Completeness If f is a degree d polynomial, then there exists a function f_{aux} such that the test accepts with probability 1.

   Soundness There exists $\delta_0 > 0$ such that the following is true: If f differs from every degree d polynomial in at least δ-fraction of the places, then for every f_{aux} the test rejects with probability at least $\min\{\delta_0, \delta/2\}$.

4. Show that the error of an $r(n)$-round interactive proof system can be amplified while preserving the number of rounds. Specifically suppose ω is the maximum (over all provers)

probability that V accepts an input x. Let V^2 be the verifier that picks two independent random strings R_1 and R_2 according to the distribution used by V and carries out two instances of the interactive protocol $V \leftrightarrow P$ in parallel with a prover P^2; and accepts if both instances accept. Show that the maximum probability with which V^2 accepts is exactly ω^2.

Does the error of a 2-prover 1-round interactive proof system also get amplified similarly under parallel repetition? Give your guess on the answer. For extra credit, prove your answer!

Instructions:

- Usual rules on collaboration.
- You may consult any material whatsoever! However cite all sources.
- Turn in the solutions to the above problems by 11am on Wednesday, May 8, 2002.