CSCI 7000-005 Computational Complexity
Problem Set 4

Alexandra Kolla

Due November 8.

Collaboration Policy: The homework can be worked on in groups of up to 3 students each (2 would be optimal, but 1 and 3 are both accepted).

One submission per team is sufficient. Please write the solution for each of the problems on a separate sheet of paper. Write your team's names and id on each submission and please **staple** all the sheets together.

Submissions should be written in LaTeX, unless your handwriting is indistinguishable from LaTeX.

Homework is due before the end of class, October 18. Only one late homework per person will be allowed. If you submit more than one homework late, you will get no grade for the excess late homeworks.

Problem 1 (25 pts)

Let A be an oracle such that when input a boolean formula ϕ in 3CNF, $A(\phi)$ gives a 2-approximation to the number of satsifying assignments to ϕ. Given 10 3CNF formulas $\phi_1, \cdots, \phi_{10}$, describe a polynomial time algorithm that uses only a single query to A to decide which of $\phi_1, \cdots, \phi_{10}$ are satisfiable. (Note: You may assume that A can operate on any boolean formulas of any sort, so that you dont have to worry about coming up with a 3CNF formula to give to A. Getting to a 3CNF formula is fairly tricky.)

Problem 2 (25 pts)

Prove that for every AM[2] protocol for a language L, if the prover and the verifier repeat the protocol k times in parallel (so the verifier sends k independent random strings for their message) and the verifier accepts if all k parallel occurrences of the protocol accept, then the probability that the verifier accepts a string $x \in L$ is at most $(1/3)^k$. Note that you cannot assume the prover is acting independently in each execution. (Use definition 8.6 for IP from Arora-Barak.)

Problem 3 (25 pts)

We define the class of decision problems PP as follows:$L \in PP$ if there exists apolynomial time TM M and a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0,1\}^*$,

$$x \in L \Longleftrightarrow \left|\left\{y \in \{0,1\}^{p(|x|)} | M(x,y) = 1\right\}\right| \geq \frac{1}{2} 2^{p(|x|)}$$

Intuitively, a problem is in PP if it corresponds to computing the most significant bit of a function in #P. We also write FP to denote the class of functions computable in polynomial time. Show that $\#P \subseteq FP^{PP}$ (Hint: Show that you can solve #CircuitSAT using an oracle to decide whether a circuit with n inputs has at least 2^{n-1} satisfying assignments.)

Problem 4 (25 pts)

Alice and Bob share an arbitrarily long common string S. Alice is given as input a random bit x_A and Bob a random bit x_B. Without communicating with each other, Alice and Bob wish to output bits a and b respectively such that $x_A \wedge x_B = a \oplus b$. Prove that any protocol that Alice and Bob follow has success probability at most 3/4.