CS 579. Computational Complexity
Problem Set 3

Alexandra Kolla

due March 3, 2017

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 names and netids 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, March 3. 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 (20 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 $\phi_1, \ldots, \phi_{10}$, describe a polynomial time algorithm that uses only a single query to A to decide which of $\phi_1, \ldots, \phi_{10}$ are satisfiable. (Note: You may assume that A can operate on any boolean formulas of any sort, so that you don't have to worry about coming up with a 3CNF formula to give to A. Getting to a 3CNF formula is fairly tricky.)

Problem 2 (20 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 $x \notin L$ 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 (20 pts.)

Consider the following two definitions of log-space counting problems. A function $f : \{0,1\}^* \to \mathbb{N}$ is in $\#\mathbf{L}_1$ if there is a non-deterministic Turing machine M_f such that on input x of length n uses $O(\log n)$ space is such that the number of accepting paths of $M_f(x)$ equals $f(x)$. A function $f : \{0,1\}^* \to \mathbb{N}$ is in $\#\mathbf{L}_2$ if there is a relation $R(\cdot,\cdot)$ that is decidable in log-space and a polynomial p such that if $R(x,y)$ then $|x| \leq p(|x|)$ and such that $f(x)$ equals $|\{y \mid R(x,y)\}|$. Prove that all functions in $\#\mathbf{L}_1$ can be computed in polynomial time, and that $\#\mathbf{L}_2 = \#\mathbf{P}$.

Problem 4 (20 pts.)

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

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

Intuitively, a problem is in **PP** if it corresponds to computing the most significant bit of a function in $\#\mathbf{P}$. We also write **FP** to denote the class of functions computable in polynomial time.

Show that $\#\mathbf{P} \subseteq \mathbf{FP}^{\mathbf{PP}}$. (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 5 (20 pts.)

Let $X_1, \ldots, X_n$ be iid Bernoulli random variables so that $X_i = 1$ with probability p and $X_i = 0$ with probability $1 - p$. Let $X = \sum_{i=1}^{n} X_i$. Let $\mu = E[X]$. Prove that

$$\Pr(X \geq (1+\delta)\mu) \leq e^{-\frac{\delta^2}{2+\delta}\mu} \text{ for all } \delta > 0$$

and that

$$\Pr(X \leq (1-\delta)\mu) \leq e^{-\mu\delta^2/2} \text{ for all } 0 < \delta < 1.$$

Use Markov's inequality with the random variable e^{sX} where $s > 0$ is a parameter you can choose at the end to get the desired bound. You'll also probably want to use the following two inequalities: $1 + y \leq e^y$ for all y and $\ln(1+x) \geq \frac{x}{1+x/2}$ for $x > 0$.