Problem 1 (20 pts.)

Let $A$ be an oracle such that when input a boolean formula $\phi$ in 3CNF, $A(\phi)$ gives a 2-approximation to the number of satsifying assignments to $\phi$. 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.

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 $\left(\frac{1}{3}\right)^k$. 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 $f : \{0, 1\}^* \rightarrow \mathbb{N}$ is in $\#L_1$ 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 $f : \{0, 1\}^* \rightarrow \mathbb{N}$ is in $\#L_2$ 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 $\#L_1$ can be computed in polynomial time, and that $\#L_2 = \#P$.

Problem 4  (20 pts.)

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

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

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

Show that $\#P \subseteq \text{FP}^{\text{PP}}$. (Hint: Show that you can solve $\#\text{CircuitSAT}$ 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 $x > 0$. 

Computational Complexity  

CS 579