Assignment II

1. Show that if SAT$\in$ BPP, then SAT$\in$ RP. (Use self reducibility).

2. Show that for any language L in NP, there is a polynomially balanced binary relation V such that if $x \in L$, $Pr_r(V(x,r) = 1) > \frac{1}{2}$ and if $x \notin L$, $Pr_r(V(x,r) = 0) > \frac{1}{2}$.

3. Let X be a non-negative random variable with mean μ. Show that $Pr(X > t\mu) < \frac{1}{t}$. This result is known as the Markov Inequality. Using this, Prove that ZPP=RP $\cap$ coRP.

4. Let L be accepted by a BPP algorithm A such that $Pr(A(x) \neq (x \in L)) < 1 - \frac{1}{n^c}$. Show that for any $1 > \epsilon > 0$, we can construct a polynomial time algorithm A' such that $Pr(A'(x) \neq (x \in L)) < \epsilon$

5. Show that PP$\subseteq$ PSPACE.

6. Show that $P^{PSPACE} = P^{TQBF} = NP^{TQBF} = NP^{PSPACE} = PSPACE^{PSPACE} = PSPACE$. Show that EXP^{EXP} $\neq$ EXP. (Hint for the second part: you can solve languages complete for $2^{2^{O(n^k)}}$ time. The trick is that with exponential time, one can write an exponentially long string on the query tape to the oracle. Now use a padding argument.)

7. A language L is in the class AC_i if there is a uniform circuit family $(C_1, C_2, ...)$ of polynomial size and $O(\log^i n)$ depth with unbounded fan-in and fan out that accepts L. Show that $NC_i \subseteq AC_i \subseteq NC_{i+1}$.

8. Show that L has a polynomial sized non-uniform circuit family (that is $L \in$ P/POLY) if and only if there exists a polynomial time deterministic algorithm V such that $x \in L$ and a function $f : \mathbf{N}^+ \longrightarrow \Sigma^*$ such that $|f(n)|$ is polynomially bounded and $x \in L$ if and only if $V(x, f(|x|)) = 1$. (If V is allowed to be a non-deterministic algorithm, we get the class NP/POLY and if V is allowed to use exponential time, we get EXP/POLY.)

9. A language L is in the class MA if there exists a polynomially balanced relation V on three inputs satisfying the following conditions: if $x \in L$, there exists y such that $Pr_z(V(x,y,z) = 1) \geq 1 - \epsilon$ and if $x \notin L$, for every y $Pr_Z V((x,y,z) = 1) < \epsilon$, where $0 < \epsilon < \frac{1}{2}$

    1. Show that given any constant $0 < \epsilon < \frac{1}{2}$, we can get the error margin down to $\frac{1}{2^n}$.
    2. Use the idea in Sipser Gacs theorem to achieve perfect completeness. That is, show that there exists a verifier V' such that if $x \in L$, there exists y such that $Pr_z(V(x,y,z) = 1) = 1$ and if $x \notin L$, for every y $Pr_Z V((x,y,z) = 1) < \epsilon$, where $0 < \epsilon < \frac{1}{2}$

10. A language A Turing reducible to a language B (written $A \preceq_T^p B$) if $A \in P^B$. That is, A can be solved in polynomial time provided an oracle for B is available.

    1. If $L_1, L_2 \in$ NP $\cup$ coNP, then show that $L_1 \cup L_2 \preceq_T^p$ SAT and $L_1 \cap L_2 \preceq_T^p$ SAT
    2. For any language L, $\overline{L} \preceq_T^p L$.

11. Show that UDepth($f(n)$)$\subseteq$ DSPACE($f^k(n)$)) for some $k > 0$ when $f(n) \geq \log n$ is fully space constructible. Show that DSPACE($f(n)$))$\subseteq$ UDepth($f^c(n)$)) for some $c > 0$ when $f(n) \geq \log n$ is fully space constructible. Note that the proof uses the fact that a uniform circuit family is log-space computable.

12. (Reading assignment) Let R be a polynomially balanced binary (two input strings) relation. The counting problem associated with R is the following: Given $x \in \Sigma^*$, find $|\{y : R(x,y) = 1\}|$. The class #P is defined as the class of all counting problems associated with polynomially balanced binary relations. Let R and S be two relations. A polynomial time algorithm A that maps from Σ^* to Σ^* is called a **parsimonious** reduction if for each $x \in \Sigma^*$, $|\{y : R(x,y) = 1\}| = |\{z : S(A(x), z) = 1\}$. Define the problem #SAT as: given a boolean formula, find the number of satisfying truth assignments. Show that #SAT indeed can be framed as a #P problem.

1. Let V be any deterministic polynomial time verifier for any language L in NP, show that there is a parsimonious reduction from V to #SAT. A problem in #P with this property is said to be #P complete.
2. Show that parsimonious reductions are closed under composition.
3. Show that the problem of counting the number of k cliques in a given graph is #P complete.
4. Show that $P^{PP} \subseteq P^{\#P}$. (Hint: PP requires only testing whether positive certificates form a majority, which is easier than counting the exact number of certificates)