Assignment III

1. A language L is in the class S_2^p if the following holds: there exists a polynomially balanced relation V such that If $x \in L$, then there exists y such that for all z, $V(x, y, z) = 0$ whereas, if $x \notin L$, there exists an z such that for all y, $V(x, y, z) = 0$. Intuitively, this means that if $x \in L$, a prover can send V a proof y such that all test runs z of V are accepting whereas, if $x \notin L$, then V has a special test run z (which depends on x only and not on the proof supplied by the prover) which will reject any y supplied by the prover.

    1. Show that S_2^p is closed under union, intersection and complementation.
    2. Show that NP$\subseteq$ $S_2^p \subseteq \Sigma_2^p \cap \Pi_2^p$.
    3. Use the technique in Sipser Gacs theorem to show that MA$\subseteq$ S_2^p.
    4. If NP$\subseteq$ P/POLY show that PH= S_2^p. (See Wiki - Karp Lipton Theorem for hint).

    (Note: It can be shown that BPP$\subseteq$ S_2^p. The proof is more involved).

2. Prove the following inclusions. (Some of them follow from the previous problem).

    1. BPP$\subseteq$ MA
    2. NP$\subseteq$ MA.
    3. MA$\subseteq$ $\Sigma_2^p \cap \Pi_2^p$.
    4. AM$\subseteq$ Π_2^p.

3. Prove that If PSPACE$\subseteq$P/POLY then PSPACE=MA. (Hint: Any problem in PSPACE will have polynomial sized circuit which Merlin can sent to Arthur).

4. Recall that AM_ϵ and MA_ϵ were defined as the version of AM and MA with imperfect completeness. That is, if $x \in L$, the AM/MA protocol accepts only with probability $1 - \epsilon$ where as if $x \notin L$, the protocol rejects with probability at least ϵ.

    1. Show that the value of ϵ can be brought down to $\frac{1}{2^n}$.
    2. Show that MA$_\epsilon$=MA and AM$_\epsilon$=AM.
    3. Show that MA $\subseteq$ AM.
    4. Show that AM[k] $\subseteq$ AM[2], where k denotes the number of message exchanges between the two parties.

5. If $S_1, S_2, .., S_m$ be a collection of subsets of $\{1, 2, .., n\}$. Suppose we assign each number between 1 and n a weight uniformly at random between 1 and t, where $t > n$, then show that with probability at least $1 - \frac{n}{t}$, there is a subset S_i of unique minimum weight. This is a general form of the isolation lemma proved in class. (The proof is identical).

6. Let p be a large prime. Let Z_p denote the field $\{0, 1, 2, .., p - 1\}$ with addition and multiplication modulo p. Consider the map $h_{a,b}(x) = ax + b \mod p$, $a, b \in \{0, 1, 2, .., p - 1\}$ mapping elements in Z_p to Z_p. Clearly, for each $a, b \in Z_p$, we can define such a function and there are p^2 such functions. Let us collect all of them to the set $\mathcal{H} = \{h_{a,b}, 0 \leq a, b \leq p - 1\}$.

    1. Fix arbitrary $a, b \in Z_p$. Show that given any $c, d \in Z_p$, there exists unique x, y such that $h_{a,b}(x) = c$ and $h_{a,b}(y) = d$.
    2. Given any $x \neq y$, and any arbitrary $c, d \in Z_p$, suppose we choose a, b at random. show that $Pr(h_{a,b}(x) = c \wedge h_{a,b}(y) = d) = Pr((a = r) \wedge (b = s)) = \frac{1}{p^2}$, where $r = \frac{c-d}{x-y}$ and $s = \frac{xd-yc}{x-y}$. Hence conclude that $\mathcal{H}$ is a pair-wise independent hash family.