Assignment 2 : Complexity Theory

April 6, 2018

1. Show that if $EXP \subseteq P/poly$, then $EXP = MA$. (Hint : What is the complexity of the prover needed for the interactive protocol in $TQBF$?)

2. Recall the definition of MA : A language $L \in MA$ if there exists a BPP Turing machine V s.t.
$$x \in L \implies \exists m, Pr_r[V(x,m,r) = 1] \geq 2/3$$
$$x \notin L \implies \forall m, Pr_r[V(x,m,r) = 1] \leq 1/3$$
Suppose we define a new class MA' where the first condition has perfect completeness (i.e) $L \in MA'$ if there exists a BPP Turing machine V s.t.
$$x \in L \implies \exists m, Pr_r[V(x,m,r) = 1] = 1$$
$$x \notin L \implies \forall m, Pr_r[V(x,m,r) = 1] \leq 1/3$$
Show that $MA = MA'$

3. Show a similar result for AM.

4. Let $\mathbb{F}$ be a finite field. Define the family of functions $\mathcal{H} = \{h_{a_0,a_1,\cdots,a_{k-1}} : \mathbb{F} \to \mathbb{F}\}$ where $h_{a_0,a_1,\cdots,a_{k-1}}(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}$ and $a_0, a_1, \cdots, a_{k-1} \in \mathbb{F}$.
Prove that $\mathcal{H}$ is k-wise independent.

5. Let $\mathcal{H} = \{h : [n] \to [m]\}$ be a pairwise independent family of functions.
   (a) Prove that if $n \geq 2$, then $|\mathcal{H}| \geq m^2$
   (b) Prove that if $m = 2$, then $|\mathcal{H}| \geq n + 1$ (Hint : Construct a sequence of orthogonal vectors $v_x \in \{\pm 1\}^{\mathcal{H}}$ parameterized by $x \in [n]$)
   (c) Prove that for arbitrary M, we have $|\mathcal{H}| \geq N(M-1) + 1$

6. Show that if there is a polynomial time algorithm that approximates $\#CYCLE$ within a factor of $1/2$, then $P = NP$.

7. Show that if $P = NP$, then for every $f \in \#P$, there is a polynomial time algorithm that approximates f within a factor of $1/2$.

8. It was mentioned but not proved in class that every connected graph has second largest eigenvalue upper bounded by $1 - 1/poly(n)$. Complete this proof and find the exact bound.[1] Hence complete the proof that undirected st-connectivity is in RL.

[1] You may look-up a reference for this, *after making an attempt yourself* but do write your own proof, and mention the reference.