CS 262: Computational Complexity *Instructor: Sandy Irani*

Homework 5

Due: June 13, 2013

1. This question fills in some of the holes of the proof of IP = PSPACE which we did in class.

   (a) Prove that any quantified boolean formula can be transformed to one in which the occurance of any variable is seperated by at most one $\forall$ from its point of quantification. The transformation requires at most a polynomial expansion in the size of the formula and the new formula evaluates to true if and only if the original formula evaluates to true.

   (b) Prove that the above transformation give a bound on the degree of the polynomials sent by the prover to the verifier in the proof of IP = PSPACE.

2. Prove that PCP(0, $\log n$) = P. Prove that PCP(0, poly(n)) = NP.

3. The PCP model defined in class allows for *adaptive* queries in which the bits that the verifier requests to see depend on the values of previously requested bits. Suppose instead that the queries the verifier asks must be *non-adaptive* in that the verifier uses its random bits to select the bits of the proof she would like to see and sends the request for those bits all at once. Prove that any language that has a PCP-verifier using r coins and q adaptive queries has a PCP-verifier using r coins and 2^q non-adaptive queries.

4. Linearity Testing. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function, and suppose that

$$\Pr_{x,y}[f(x) + f(y) = f(x + y)] \geq 1 - \delta, \tag{1}$$

   where x, y are chosen uniformly in $\mathbb{F}_2^n$. Define $\tilde{f} : \mathbb{F}_2^n \to \mathbb{F}_2$ by

$$\tilde{f}(x) = \text{majority}_y(f(x + y) - f(y)),$$

   where we set $\tilde{f}(x) = 0$ if there is a tie.

   (a) Prove that for all $x \in \mathbb{F}_2^n$, we have

$$\Pr_y[f(x + y) - f(y) = \tilde{f}(x)] \geq 1 - 4\delta.$$

   Hint: start by relating the probability that the a random voter disagrees with the majority to the probability that two random voters disagree.

   (b) Show that $\Pr_x[f(x) \neq \tilde{f}(x)] \leq 2\delta$. Hint: use Eq. (1) and the definition of $\tilde{f}$.

(c) Assume that $\delta < 1/14$. Prove that $\tilde{f}$ is linear; i.e., for all x, y we have

$$\tilde{f}(x) + \tilde{f}(y) = \tilde{f}(x+y).$$

Hint: Eq. (1) gives us

$$\begin{aligned} \Pr_{w,z}[f(w) + f(z) = f(w+z)] &\geq 1-\delta \\ \Pr_{w,z}[f(x+w) + f(y+z) = f(x+y+w+z)] &\geq 1-\delta. \end{aligned}$$

Now use part (a) to obtain statements about $\tilde{f}(x)$, $\tilde{f}(y)$ and $\tilde{f}(x+y)$.

(d) Given a function $f : \mathbb{F}_2^n \to \mathbb{F}$, the BLR linearity test on f is the following procedure: pick $x, y \in \mathbb{F}_2^n$ randomly; f passes the test if $f(x) + f(y) = f(x+y)$. Prove the following two statements:

Completeness: If f is linear, then f passes the test with probability 1.

Soundness: If f passes the test with probability $1-\delta$, then there exists a *linear* function $\tilde{f}$ satisfying $\Pr_x[f(x) = \tilde{f}(x)] \geq 1 - O(\delta)$.