PRINCETON UNIVERSITY COS 522: COMPUTATIONAL COMPLEXITY

Homework 3

Out: *March 28* Due: *April 4*

You can collaborate with your classmates, but be sure to list your collaborators with your answer. Also, limit your answers to one handwritten page, preferably less —you just need to give enough detail to convince me. If some question doesn't seem correct or solvable, indicate why.

§1 (a) Show that $\mathbf{AM}[2] \subseteq \mathbf{NP}/\text{poly}$. (b) Show that if $\overline{SAT} \in \mathbf{NP}/\text{poly}$ then $\mathbf{PH} = \mathbf{\Sigma}_3^p$. (c) Conclude that if Graph Isomorphism is **NP**-complete under polynomial time reductions, then $\mathbf{PH} = \mathbf{\Sigma}_3^p$

§2 A *program checker* for a computational problem π is a probabilistic algorithm C. Given any program P that supposedly computes π and an input x, the checker calls P at most poly($|x|$) times, and runs in poly($|x|$) time (this does not include the time required by P).

(a) If P correctly computes π on every input, then with probability at least 0.99, C outputs "CORRECT" on x.

(b) If $P(x) \neq \pi(x)$, then with probability at least 0.99, C outputs "BUGGY" on x.

Show that Graph Isomorphism and Discrete Log (for a specific prime p) have program checkers. What about SAT?

§3 A degree d polynomial is one whose degree in each variable is at most d. Let the *distance* between two functions f, g (denoted $\Delta(f, g)$) be the fraction of points on which f, g disagree. Show that if f, g are degree d polynomials in m variables, then $\Delta(f, g) \geq 1 - md/|F|$. (Hint: Use induction on m.)

§4 Let $\Delta_d(f)$ denote the distance of f to the nearest degree d polynomial.

Suppose we are given the table of values of a function $f : F^m \to F$. Supposedly this function is a degree d polynomial in m variables over field $F = Z_q$, but this needs to be checked. Let $q = \Omega(m^3 d^3)$. Consider the following tester:

Pick $i \in_R \{1, \ldots, m\}$ *and* $a_1, a_2, \ldots, a_m \in_R F$ *randomly. For* $s = 0, 1, \ldots, d$, *read* $f(a_1, \ldots, a_{i-1}, s, a_{i+1}, \ldots, a_m)$ *from the table. Let these values be* $b_0, \ldots, b_d$ *respectively. Let* $g(x)$ *be a degree* d *univariate polynomial such that* $g(i) = b_i$. *ACCEPT iff* $f(a_1, a_2, \ldots, a_m) = g(a_i)$.

Show that there is a constant $c > 0$ such that the probability this test accepts is at most $1 + \sqrt{\frac{md}{q}} - \min\left\{c\Delta_d(f), \frac{1}{10md}\right\}$. Report partial progress on this problem too, but keep it brief. (Hint: Use some kind of induction on m and also use Problem 3. Note that the test is implicitly defining m functions, one for each value of i. The ith function has the property that fixing all but the ith coordinate gives a polynomial of degree d in that variable. The induction should use properties of such functions.)