Homework 2

Out: *April 4* Due: *April 16*

You are encouraged to collaborate with your classmates, but be sure to list your collaborators with your answers and write your final solutions on your own. (Note that no credit is lost due to collaboration.) Remember: False proofs cause brain damage. Do not ever attempt to write down a proof that you are unsure about. It is better to write down your thoughts, and point out where you are stuck. Please be concise in your answers. If you suspect a problem is open, just say so and give reasons for your suspicion.

§1 Show that $PCP \subset NEXPTIME$.

§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 (as an oracle) at most $poly(|x|)$ times, and runs in additional $poly(|x|)$ time (this does not include the time required by P). The checker has the following properies:

(a) If P corectly computes π on every input, then for every input x, with probability at least 2/3, C outputs "Correct".

(b) If for a given x, it is the case that $P(x) \neq \pi(x)$, then with probability at least 2/3, C outputs "Buggy".

Show that Graph Isomorphism has a program checker (Note that the program only (supposedly) outputs whether two graphs are isomorphic; it does not have to reveal an isomorphism.) Does SAT have a program checker?

§3 Let f, g be functions defined over a finite field F. Let $\Delta(f, g)$ be the fraction of input points on which f and g disagree. Show that if f, g are degree d multivariate polynomials in m variables, then $\Delta(f, g) \geq 1 - md/|F|$. (Hint: induction on m).

§4 Let $\Delta_d(f)$ denote the distance of f to the nearest degree d polynomial. Suppose we are given an oracle for a function $f : F^m \to F$. We want to test if this oracle is really a degree d polynomial over a prime field F with $\Omega(m^3 d^3)$ elements, or if it is far away from being one.

We consider the following tester:

Choose $i \in_R 1, \ldots, m$, and $a_1, a_2, \ldots, a_m \in_R F$ randomly. For $s = 0, 1, \ldots, d$, query for $f(a_1, \ldots, a_{i-1}, s, a_{i+1}, \ldots, a_m)$. From these $d+1$ values interpolate the degree d univariate polynomial $g(x)$. Accept if $g(a_i) = f(a_1, \ldots, a_m)$.

Show that if $\Delta_d(f)$ is large enough, then this test will reject with noticeable probability. Try to show the most nontrivial statement you can. Can you show that for some constant $c > 0$, if the probability of the test rejecting is smaller than c/md, then there exists a degree d polynomial $O(1/md)$-close to f? (Hint: Use previous problem. This is pretty non-trivial.)

§5 Prove that all nontrivial monotone graph properties on graphs over v vertices require decision trees of depth $\Omega(v^2)$. Recall that in class, we already showed that this is true when v is a power of 2; we also showed that any property f over n variables, where $f(\overline{\mathbf{0}}) \neq f(\overline{\mathbf{1}})$ and n is a prime power, such that the property is invariant under the action of a transitive group on its variable names, is evasive.