PRINCETON UNIVERSITY COS 522: COMPUTATIONAL COMPLEXITY

Homework 3

Out: *April 9* Due: *April 18*

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 Show that if SAT $\in$ PCP$(r(n), 1)$ for $r(n) = o(\log n)$ then P = NP. (Thus the PCP Theorem is probably optimal up to constant factors.)

§2 These little problems introduce you to the reasoning used in the analysis of the low degree test. In all of them assume that the field size q is at least quadratic in the degree in question.

(a) Show that if $f : F^m \to F$ is described by a univariate polynomial of degree $\leq d$ on all lines in F^m, then f is a polynomial of degree at most d.

(b) Suppose $f : F^2 \to F$ and for each $a \in F$ let C_a, R_a be two univariate degree d polynomials. Suppose these satisfy for at least $(1 - \frac{1}{20d})$ fraction of $(a, b) \in F^2$,

$$f(a, b) = R_a(b) = C_b(a).$$

Then show that f is 0.2-close to a bivariate polynomial whose degree in each variable is at most d.

(c) Show that if $f, g : F^m \to F$ are δ-close (i.e., agree on δ fraction of points) then on at least $1 - 1/K^2$ fraction of lines in F^m, functions f, g agree on between $\delta(1 - \frac{2K}{\sqrt{\delta q}})$ and $\delta(1 + \frac{2K}{\sqrt{\delta q}})$ fraction of points on the line. (Hint: A random line is picked by picking two random points, so the set of points on it are roughly pairwise independent. Check this by computing the variance!)

§3 Using the fact that a correct tableau can be verified in logspace, we saw the following exact characterization of NP:

$$\text{NP} = \{L : \text{ there is a logspace machine } M \text{ s.t } x \in L \text{ iff } \exists y \ : \ M \text{ accepts } (x, y).\}.$$

Note that M has two-way access to y.

Let L-PCP$(r(n))$ be the class of languages whose membership proofs can be probabilistically checked by a logspace machine that uses $O(r(n))$ random bits but makes only one pass over the proof. (To use the terminology from above, it has 2-way access to x but 1-way access to y.) As in the PCP setting, "probabilistic checking of membership proofs" means that for $x \in L$ there is a proof y that the machine accepts with probability 1 and if not, the machine rejects with probability at least 1/2. In this problem we prove NP = L-PCP$(\log n)$.

Assume the following fact (which is only asymptotically correct) from now on: The number of primes in the interval $[l, 2l]$ is exactly $\frac{l}{\log l}$.

(a) Show that L-PCP$(\log n) \subseteq$ NP.

(b) Show that if x and y are distinct n-bit numbers, and p is a prime chosen randomly from among the first $2n$ primes, then

$$Pr[x = y \bmod p] \leq \frac{1}{2}.$$

(c) Let S_1 and S_2 be two given multisets with at most m elements, each of which is an n-bit numbers. Describe a probabilistic algorithm that tests whether or not S_1, S_2 are equal using $O(\log n + \log m)$ random bits and using only one pass over S_1, S_2. If $S_1 = S_2$ the algorithm must accept with probability 1 and if $S_1 \neq S_2$ it must reject with probability at least $1 - 1/n$. (Hint: Interpret a multiset as a multivariate polynomial and use Schwartz-Zippel.) In order to be useful below, your algorithm should work even if the elements of S_1, S_2 are arbitrarily interspersed.

(d) Let ψ be a $3SAT$ formula. This part concerns a special representation of a satisfying assignment. In the rest of the question, "pair" refers to some (n, v) where n is a variable in ψ and $v \in \{0, 1\}$.

A *triple* for a clause in ψ is a tuple of the type:

$$< (n_1, v_1), (n_2, v_2), (n_3, v_3) >$$

where n_1, n_2 and n_3 are variables occuring in the clause. The triple is *valid* if the assignment v_1, v_2 and v_3 to these variables makes the clause true.

A "valuation sequence" σ for ψ consists of two parts:

- A sequence of pairs (n, v) where n is a variable of ψ. Call this sequence the *assignment part* of σ.
- A sequence of valid triples, each representing some clause of ψ. Call this part the *evaluation part* of σ.

σ is *complete* if there each variable is assigned exactly once in its assignment part, and each clause is evaluated exactly once in its evaluation part.

It is *globally consistent* if for each variable n, every pair (n, v) appearing in σ has the same value of v. (Intuition: A pair (n, v) occuring anywhere implies that variable n has been assigned value v, and consistency demands that this value is the same throughout σ).

Convince yourself that φ is satisfiable iff it has a complete and globally consistent valuation sequence.

Now you have all ingredients to complete the proof of NP $\subseteq$ L-PCP($r(n)$).

§4 Suppose we define $J - PCP(r(n))$ similarly to $L - PCP(r(n))$, except the verifier is only allowed to read $O(r(n))$ successive bits in the membership proof. (It can decide which bits to read.) Show that $J - PCP(\log n) =$ L.