*CS 262: Computational Complexity* *Instructor: Sandy Irani*

# Final Exam

**Due: Friday, June 15, 2018, Noon**

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

2. 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.

3. A language L is said to be *downward self-reducible* if there's a polynomial-time algorithm R that for any $n$ and any $x \in \{0,1\}^n$, $R^{L^{n-1}}(x) = L(x)$, where by $L_k$ we denote an oracle that solves L on inputs of size at most $k$. Prove that if L is downward self-reducible then L is in PSPACE.

4. Define $\mathbf{L}_i$ to be the class of languages decidable by a deterministic Turing Machine using at most $O(\log^i n)$ space, and $\mathbf{NL}_i$ to be the class of languages decidable by a non-deterministic Turing Machine using at most $O(\log^i n)$ space. The classes $\mathbf{L}_1$ and $\mathbf{NL}_1$ should be familiar – they are just deterministic logspace and nondeterministic logspace, respectively.

   (a) Show that for all $i$, $\mathbf{NL}_i$ has $O(\log^{2i} n)$ depth, fan-in 2, Boolean circuits. Your circuits do not need to be uniform.

   (b) It is tempting to try to show that for all $i$, $\mathbf{NL}_i \subseteq \mathbf{NC}_{2i}$ (since this holds for $i = 1$). Show that this would imply that $\mathbf{L} \neq \mathbf{P}$.

5. Recall that a *clique* in an undirected graph $G = (V, E)$ is a subset $V' \subseteq V$ with edges between every pair of vertices in $V'$. We know that the language

   $$\text{CLIQUE} = \{(G, k) : G \text{ has a clique of size } k\}$$

   is **NP**-complete. You will show that there is some constant $\delta > 0$ for which CLIQUE is **NP**-hard to approximate to within $N^\delta$ in the following sense: if there is an $N^\delta$-approximation algorithm for CLIQUE, then $\mathbf{NP} = \mathbf{ZPP}$. Here $N$ is the length of the input $(G, k)$.

   The PCP Theorem implies that there is some constant $\epsilon > 0$ for which given a 3-CNF formula $\phi$ it is **NP**-hard to distinguish between the following two cases:

   YES : $\phi$ is satisfiable

   NO : every assignment to $\phi$ satisfies at most a $(1 - \epsilon)$ fraction of the clauses

Below you will describe a *randomized* transformation from an instance $\phi$ into a graph $G$ whose intended effect is that a YES instance produces a graph with a large clique, while a NO instance produces a graph with only a very small clique. Here $n$ is the number of variables in $\phi$.

(a) Suppose $\phi$ is a NO instance, and consider the following probabilistic experiment: pick $\log_2 n$ clauses from $\phi$ uniformly at random, take their conjunction, and call this CNF $\phi_1$; repeat $n^3$ times to get CNFs $\phi_1, \phi_2, \ldots, \phi_{n^3}$. Show that for a fixed assignment $A$:

$$\Pr[A \text{ satisfies at least } n^{3-\epsilon} \text{ of the } \phi_i] < e^{-n^2}.$$

Hint: What is the probability that $A$ satisfies a given $\phi_i$? What is the expected number of $\phi_i$ satisfied by $A$? You may want to use the fact that $(1-\epsilon)^{1/\epsilon} \leq 1/e$ for $1 > \epsilon > 0$, and the Chernoff bound: if $X$ is the sum of independent 0/1 random variables with expected value $\mathrm{E}[X] \leq \mu$, then $\Pr[X > 2\mu] \leq e^{-\mu/3}$.

(b) Argue that the above randomized procedure produces from $\phi$ a collection of 3-CNFs $\phi_1, \phi_2, \ldots, \phi_{n^3}$ for which

i. $\phi$ is a YES instance $\Rightarrow \Pr[\exists$ assignment $A$ simultaneously satisfying all of the $\phi_i] = 1$, and

ii. $\phi$ is a NO instance $\Rightarrow \Pr[$no assignment satisfies more than $n^{3-\epsilon}$ of the $\phi_i] \geq 1/2$.

(c) Describe an efficient deterministic procedure to construct a graph $G$ from the collection of 3-CNFs in part (b) for which

i. $\exists$ assignment $A$ simultaneously satisfying all of the $\phi_i \Rightarrow G$ has a clique of size $n^3$, and

ii. no assignment satisfies more than $n^{3-\epsilon}$ of the $\phi_i \Rightarrow$ no clique in $G$ has size greater than $n^{3-\epsilon}$.

(d) Prove that there exists a constant $\delta > 0$ for which an $N^\delta$-approximation algorithm for CLIQUE implies that $\mathbf{NP} = \mathbf{ZPP}$, where $N$ is the length of the input. (Hint: first show that if there is an $N^\delta$-approximation algorithm for CLIQUE then $\mathbf{NP} \subseteq$ **co-RP**.)