PRINCETON UNIVERSITY COS 522: COMPUTATIONAL COMPLEXITY

Homework 2

Out: *March 7* Due: *March 26*

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 for each $k > 0$ there is a language in **PH** that is not decidable by circuit families of size n^k. For full credit prove the existence of such a language in Σ_2^p. (Hint: Diagonalization.)

§2 Let $\mathcal{H}$ be a family of 2-universal hash functions mapping $\{0,1\}^n$ to $\{0,1\}^m$ where $n > m$. Let $S \subseteq \{0,1\}^n$ have size at least 2^m. Show that

$$\Pr_{h \in \mathcal{H}}[h(S) \neq \{0,1\}^m] \leq \frac{2^{2m+1}}{|S|}.$$

§3 Let $f, g : \{0,1\}^* \to \mathbf{N}$ be functions and $c > 1$. We say that f *approximates* g *within a factor* c if for every string x, $g(x) \leq f(x) \leq c \cdot g(x)$. Show that for every $g \in \#\mathbf{P}$ and every $\epsilon > 0$, there is a function in $\mathbf{FBPP}^{\mathrm{SAT}}$ that approximates g within a factor $1 + \epsilon$. (Hint: Use the previous Problem.)

§4 A *formula* is a circuit in which every node (except the input nodes) has outdegree 1. Show that a language is computable by polynomial-size formulae iff it is in (nonuniform) NC^1. (Hint: a formula may be viewed —once we exclude the input nodes—as a directed binary tree, and in a binary tree of size m there is always a node whose removal leaves subtrees of size at most $2m/3$ each.)

§5 Show that every for every language in AC^0 there is a depth 3 circuit of $n^{\mathrm{poly}(\log n)}$ size that decides it on $1 - 1/\mathrm{poly}(n)$ fraction of inputs and looks as follows: it has a single $\oplus$ gate at the top and the other gates are $\vee, \wedge$ of fanin at most $\mathrm{poly}(\log n)$.

§6 (a) Show that if f is a one-way permutation then so is f^k (namely, $f(f(f(\cdots(f(x)))))$ where f is applied k times).

(b) Show that the above fails for one-way functions. (You may assume that one-way functions exist.)

(c) Let $\{f_n\}$ be a family of pseudorandom generators where $f_n : \{0,1\}^n \to \{0,1\}^{2n}$. Let $T_{m,n}(x)$ for $x \in \{0,1\}^n$ be a complete binary tree of depth m whose each node is labelled with an n-bit string. The root is labelled x. If a node in the tree has label y then its left child is labelled with the first n bits of $f_n(y)$ and the right child is labelled with the last n bits of $f_n(y)$. Define a family of functions $g : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ where $m = \mathrm{poly}(n)$ as follows: for any $s \in \{0,1\}^m, x \in \{0,1\}^n$, interpret s as a label for a path from root to leaf in $T_{m,n}(x)$ in the obvious way and output the label at the leaf.

Show that for any probabilistic polynomial-time adversary A and every $c > 0$:

$$\left| \Pr_{s,x}[A(x, g(s,x)) = 1] - \Pr_{h \in \mathcal{F}_n}[A(x, h(x)) = 1] \right| \leq \frac{1}{n^c}, \tag{1}$$

where $\mathcal{F}_n$ is the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$.