PRINCETON UNIVERSITY COS 522: COMPUTATIONAL COMPLEXITY

Homework 2

Out: *March 5* Due: *March 14*

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 there is a language in **PH** that is not decidable by circuits of size n^k. (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 The XOR casino offers the following game. A sequence of k cards all labelled with 0 or 1 is laid on the table face-down. The cards are chosen by the casino, with just one restriction (under state gambling laws): with probability at least p, all k cards must be 1. Now a card is picked uniformly at random and all the other cards are turned face up. You are asked to guess the number on the hidden card; if you guess correctly you receive a payoff of \$ 1.

This question explores what your expected payoff can be.

(a) Suppose the casino's strategy is the following: with probability p make all cards 1 and otherwise make each card 1 with probability 1/2 and 0 with probability 1/2. Show that your expected payoff then is at most $1/2 + p/2$, and that you have a strategy that achieves this payoff.

(b) Now suppose the casino strategy is unknown to you (except you know that it obeys state laws). Suppose you use the following guessing strategy: if all $k-1$ cards you saw had a 1, you guess that the k'th one is 1, otherwise you guess 0 or 1 with equal probability.

Show that then the casino has a strategy to make your expected payoff at most

$$\frac{1}{2} + \frac{p}{2} - \frac{1-p}{2k}.$$

(c) Now suppose you adopt the following strategy: if among the $k-1$ cards revealed to you, t cards have a 0 on them, then you guess with probability $(1+2^{-t})/2$ that the kth card has a 1 and with probability $(1-2^{-t})/2$ that it has a 0.

Show that with this strategy your expected payoff is at least $1/2 + p/2 - 2^{-k/3}$, irrespective of the casino's strategy (so long as it obeys state laws).

§5 Use the previous question to prove the following version of the Yao XOR Lemma. Suppose $f : \{0,1\}^n \to 0,1$ is a function such that no circuit of size $S(n)$ can, given a random x, predict $f(x)$ with probability 3/4. Let $f^{\oplus k} : \{0,1\}^{(n+1)k} \to 0,1$ be the function that breaks its input into k parts $y_1, y_2, \ldots, y_k$ of n bits each and one part r of k bits. It computes the k-tuple $(f(y_1), f(y_2), \ldots, f(y_k))$ and outputs its inner product (mod 2) with r.

Then no circuit of size $t(nk)$ can predict $f^{\oplus k}$ for more than $1/2 + s(nk)$ fraction of inputs, where $poly(s(nk)t(nk)) \leq T(n)$. (Hint: The circuit could have hardwired answers to quite a few random inputs; think of these as the $k-1$ cards of the casino game.)