Homework 4

Due Saturday, 09/22/2012

You may use any result discussed in class. Unless explicitly stated otherwise, you should not use other sources. Whenever you do use other source (even the textbook), you need to reference them.

Problem 4.1 (30 points)**.** Show that if there exist one-way permutations, then **P** $\neq$ **NP**.

Problem 4.2 (30 points)**.** Prove the easy direction of Yao's Theorem. That is, prove that if a distribution X over $0,1^n$ is pseudorandom[1] then there is no polynomial-time machine M, and $i \in [n]$ such that

$$\mathbb{P}\left\{M(X_1,\ldots,X_{i-1}) = X_i\right\} \geqslant 1/2 + n^{-O(1)}$$

Problem 4.3 (30 points)**.** Show the following limitation on combinatorial designs: If $S_1,\ldots,S_k$ are subsets of a universe U such that for some $\rho > 0$, $|S_i| = \rho|U|$ and $|S_i \cap S_j| \leqslant \rho^2|U|/2$ for every distinct $i, j \in [k]$ then $k \leqslant 2/\rho$.

Problem 4.4 (3×10 points)**.** For $\alpha \in \mathbb{F}_2^n$, let $\chi_\alpha \colon \mathbb{F}_2^n \to \mathbb{R}$ be the function $\chi_\alpha(r) = (-1)^{\langle \alpha, r\rangle}$. For functions $f, g \colon \mathbb{F}_2^n \to \mathbb{R}$, define the inner product $\langle f, g\rangle = \mathbb{E}_{r\in\mathbb{F}_2^n} f(r)g(r)$. (1) Show that $\{\chi_\alpha\}$ is an orthonormal basis with respect to this inner product. (2) Show that if $f = \sum_\alpha c_\alpha\chi_\alpha$ and $g = \sum_\alpha d_\alpha\chi_\alpha$, then $\langle f, g\rangle = \sum_\alpha c_\alpha d_\alpha$. (3) For $i \in [n]$, let $E_i = \{(x, x + 1_i) \mid x \in \mathbb{F}_2^n\}$. Let G be the graph on $\mathbb{F}_2^n$ with edge set $E = E_1 \cup \ldots \cup E_n$ (the n-dimensional *hypercube*). Show that $\{\chi_\alpha\}$ is an eigenbasis of G.

[1] Here, the notion of pseudorandomness is that polynomial-size circuits cannot distinguish the distribution from the uniform distribution with polynomial advantage