CS 880: Pseudorandomness and Derandomization 3/6/2013

Homework 1

Instructors: Holger Dell and Dieter van Melkebeek

This homework is due at the beginning of class on 4/3/2013. Good luck!

1. An exact-k-CNF formula is a CNF-formula in which every clause consists of exactly k literals involving k distinct variables.

   Let $k(n) = \lceil c \cdot \log n \rceil$, where c is an arbitrary positive constant. Given an exact-$k(n)$-CNF formula φ on n variables, show how to find an assignment that satisfies at least a fraction $1 - \frac{1}{2^{k(n)}}$ of the clauses of φ on a deterministic machine with a polynomial number of processors in polylogarithmic parallel time.

2. In class we constructed a β-bias generator on $\{0,1\}^r$ with seed length $2\log(r) + O(\log(1/\beta))$. The goal of this problem is to improve the seed length to $\log(r) + O(\log(1/\beta))$. In order to do so, you can make use of a polynomial-time computable linear error-correcting code $\mathcal{C} = (C_k)_{k\in\mathbb{N}}$ with $C_k : \{0,1\}^k \to \{0,1\}^{n(k)}$ such that the rate and relative distance of C_k are at least some positive constant.

   (a) Given a positive integer k and a positive real ϵ, construct a linear error-correcting code $C'_k : \{0,1\}^k \to \Sigma^{n(k)}$ with relative distance at least $1-\epsilon$, where Σ is an alphabet of size $(\frac{1}{\epsilon})^{O(1)}$. The family $\mathcal{C}' = (C'_k)_{k\in\mathbb{N}}$ should be computable in time polynomial in k and $\frac{1}{\epsilon}$. *Hint:* Expander-based confidence boosting.

   (b) Construct a β-bias generator over $\{0,1\}^r$ with seed length $\log(r) + O(\log(1/\beta))$ that is computable in time polynomial in r and $\frac{1}{\beta}$.

3. Consider the following randomized affinity test for a function $f : \{0,1\}^n \to \{0,1\}$: Pick x and y uniformly from $\{0,1\}^n$, and accept if and only if $f(x) + f(y) = f(0) + f(x+y)$.

   (a) Show that the probability of acceptance equals $\frac{1}{2} \cdot \left(1 + g(0)\sum_{a\in\{0,1\}^n} \hat{g}(a)^3\right)$, where $g(x) \doteq (-1)^{f(x)}$.

   (b) Conclude that if the probability of acceptance is at least p then there exists an affine function that agrees with f in at least a fraction p of the domain $\{0,1\}^n$.

   (c) Suppose that we pick x from the uniform distribution as before, but y from a β-bias distribution. Generalize the arguments from parts (a) and (b) to this setting.

4. Recall the problem from the first lecture about approximating the average μ of a function $f : \{0,1\}^n \to \{0,1\}$ with respect to the uniform distribution.

   For any positive reals δ and ϵ, give a randomized algorithm that outputs an estimate that, with probability at least $1-\delta$, differs from μ by no more than ϵ. Your algorithm should use no more than $n + O(\log\frac{1}{\delta})$ random bits, query f in no more than $O(\frac{1}{\epsilon^2}\log\frac{1}{\delta})$ points, and run in time polynomial in n, $\frac{1}{\epsilon}$ and $\log\frac{1}{\delta}$.

   For every positive integer n and positive real λ, you can assume the existence of a regular graph on 2^n vertices with spectral expansion at least $1-\lambda$ and degree $O(1/\lambda^2)$ such that the neighbors of a given vertex can be computed in time polynomial in n and $1/\lambda$.

5. [optional]

   In Lecture 4 we saw two different constructions of pairwise independent generators, namely a simple one in Theorem 2, and a somewhat more involved one in Lemma 5 and Theorem 6 (for $k = 2$). I believe the two constructions are related, but I currently do not know the precise connection. This problem asks you to investigate it.

   For the construction from Theorem 2, you can consider its generalization $G_r : \Sigma^{(m+1)} \to \Sigma^r$ with $\Sigma = \mathbb{F}_{2^p}$ and $r = 2^m$ that takes $\sigma = (\sigma_i)_{i=1}^{m+1}$ to $(\sum_{i=1}^m x_i \sigma_i + \sigma_{m+1})_{x \in \{0,1\}^m}$. For the other construction, consider the mapping $G : \mathbb{F}_q^2 \to \mathbb{F}_q^q$ with $q = (2^p)^m$ that takes (a, b) to $(ay + b)_{y \in \mathbb{F}_q}$, where the arithmetic is over $\mathbb{F}_q$.

   Feel free to make further simplifying assumptions, like an appropriate choice of an irreducible polynomial for the underlying field operations.