Lecture 6

1. (O 3.29) Let $\phi : \mathbb{F}_2^n \to \mathbb{R}^{\geq 0}$ be a probability density function corresponding to probability distribution Φ on $\mathbb{F}_2^n$. Let $J \subseteq [n]$.

   (a) Consider the marginal probability distribution of Φ on coordinates J. What is its probability density function (a function $\mathbb{F}_2^J \to \mathbb{R}^{\geq 0}$) in terms of ϕ?

   Solution:

   (b) Consider the probability distribution of ϕ conditioned on a substring $s \in \mathbb{F}_2^{\overline{J}}$. Assuming it's well defined, what is its probability density function in terms of ϕ?

   Solution:

2. (O 3.16/3.38) Let $f : \{-1,1\}^n \to \mathbb{R}$ and let $\varepsilon > 0$. Show that f is ε-concentrated on a collection $\mathcal{F} \subseteq 2^{[n]}$ with $|\mathcal{F}| \leq \hat{\|} f \hat{\|}_1^2/\varepsilon$.

   Let $\mathcal{C}$ be the set of functions f such that $\hat{\|} f \hat{\|}_1 \leq s$. Show that $\mathcal{C}$ can be learned with error ε in time $\text{poly}(n, s, 1/\varepsilon)$.

   Solution:

3. (O 3.44) Let $\tau \geq 1/2 + \varepsilon$ for some constant $\varepsilon > 0$. Give an algorithm simpler than Goldreich and Levin's that solves the following problem with high probability: Given query access to $f : \{-1,1\}^n \to \{-1,1\}$, in time $\text{poly}(n, 1/\varepsilon)$ find the unique $U \in [n]$ such that $|\widehat{f}(U)| \geq \tau$ assuming it exists. (Hint: First, consider the case $\varepsilon = 1/2$. Use the local correction algorithm from Lecture 2 to generalize this.)

   Solution:

4. (O 3.45) Informally: a "one-way permutation" is a bijective function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ that is easy to compute on all inputs but hard to invert on more than a negligible fraction of inputs; a "pseudorandom generator" is a function $f : \mathbb{F}_2^k \to \mathbb{F}_2^m$ for $m > k$ whose output on a random input "looks unpredictable" to any efficient algorithm. Goldreich and Levin proposed the following construction of the latter from the former: for $k = 2n, m = 2n + 1$, define

   $$g(r, s) = (r, f(s), r \cdot s),$$

   where $r, s \in \mathbb{F}_2^n$. When g's input (r, s) is uniformly random, then so is the first $2n$ bits of its output (using the fact that f is a bijection). The key to the analysis is showing that the final bit, $r \cdot s$, is highly unpredictable to efficient algorithms even given the first $2n$ bits$(r, f(s))$. This is proved by contradiction.

(a) Suppose that an adversary has a deterministic, efficient algorithm A good at predicting the bit $r \cdot s$:

$$\Pr_{r,s \sim \mathbb{F}_2^n}[A(r, f(s)) = r \cdot s] \geq \frac{1}{2} + \gamma.$$

Show there exists $B \subseteq \mathbb{F}_2^n$ with $|B|/2^n \geq \frac{1}{2}\gamma$ such that

$$\Pr_{r \sim \mathbb{F}_2^n}[A(r, f(s)) = r \cdot s] \geq \frac{1}{2} + \frac{1}{2}\gamma.$$

for all $s \in B$.

Solution:

(b) Switching to ± 1 notation in the output, deduce $\widehat{A_{|f(s)}}(s) \geq \gamma$ for all $s \in B$.

Solution:

(c) Show that the adversary can efficiently compute s given $f(s)$ (with high probability) for any $s \in B$. If γ is nonnegligible, this contradicts the assumption that f is "one-way". (Hint: Use the Goldreich–Levin Algorithm.)

Solution:

Lecture 7

1. (O 4.1) Show that every function $f : \{0,1\}^n \to \{0,1\}$ can be represented by a DNF formula of size at most 2^n and width at most n.

Solution:

2. (O 4.3) A DNF formula is said to be *monotone* if its terms contain only unnegated variables. Show that monotone DNFs compute monotone functions and that any monotone function can be computed by a monotone DNF.

Solution:

3. (O 4.9) Give a direct (Fourier-free) proof of the following Corollary. (Hint: Condition on whether $i \in J$.)

Fix $f : \{-1,1\}^n \to \mathbb{R}$ and $i \in [n]$. If $(j|x)$ is a δ-random restriction, then $\mathbb{E}[\mathrm{Inf}_i[f_{J|x}]] = \delta \mathrm{Inf}_i[f]$. Hence also $\mathbb{E}[\mathbf{I}[f_{J|x}]] = \delta \mathbf{I}[f]$.

Solution:

4. (Based on O 4.12)

   (a) Show that the parity function $\chi_{[n]} : \{-1, 1\}^n \to \{-1, 1\}$ can be computed by a DNF (or a CNF) of size 2^{n-1}.

   Solution:

   (b) Show that the bound 2^{n-1} above is exactly tight. (Hint: Show that every term must have width exactly n.)

   Solution:

   (c) Show that there is a depth-4 circuit of size $O(n^{1/2} 2^{2n^{1/2}})$ computing $\chi_{[n]}$. (Hint: Break up the input into $n^{1/2}$ blocks of size $n^{1/2}$ and use (a) twice.)

   Solution:

   (d) More generally, show there is a depth-$2d$ circuit of size $O(n^{1-1/d} 2^{dn^{1/d}})$ computing $\chi_{[n]}$.

   Solution: