CS 294-92 Analysis of Boolean Functions
Problem Set 3

Due: Mar 31, 2020, 11:59 PM.

You are encouraged to discuss the problems and solve them in groups (over Zoom, Slack, Skype, Hangouts, etc.). However, the solutions are to be written up alone, listing all the collaborators.

1. **Correlation Bounds of Majority against DNFs.** Let $g : \{-1,1\}^n \to \{-1,1\}$ be a width-w DNF. Recall that we showed that:

$$\forall k : \quad \mathbf{W}^{\geq k}[g] \leq 2 \cdot 2^{-k/(10w)} \qquad \text{and} \qquad \sum_{S:|S|=k} |\widehat{g}(S)| \leq (20w)^k.$$

   In particular, the first item implies that any such g has a small correlation with the Parity function. In this exercise, we show similar results for the Majority function, and more generally for any symmetric balanced function. Let $f : \{-1,1\}^n \to \{-1,1\}$ be a symmetric balanced function (i.e., $\widehat{f}(\emptyset) = \mathbf{E}[f] = 0$).

   (a) Show that for all $S \subseteq [n]$ it holds that $|\widehat{f}(S)| \leq 1/\sqrt{\binom{n}{|S|}}$.

   (b) Show that for any k

$$\left| \sum_{S:|S|=k} \widehat{f}(S) \cdot \widehat{g}(S) \right| \leq (20w)^k \cdot \frac{1}{\sqrt{\binom{n}{k}}}.$$

   (c) Show that for any k

$$\left| \sum_{S:|S|=k} \widehat{f}(S) \cdot \widehat{g}(S) \right| \leq \sqrt{2 \cdot 2^{-k/(10w)}}.$$

   (d) Assuming $w \leq n^{1/4}$ and n large enough, show that $|\langle f, g \rangle| \leq 40w/\sqrt{n}$.

2. **(k,δ)-wise Independent Generators:** In this exercise, you will prove the beautiful result of Naor-Naor, constructing (k,δ)-wise independent generators using $O(k+\log\log n+\log(1/\delta))$ random bits. For constant k and δ, this generator uses only $O(\log\log n)$ random bits!

   We start by describing a well-known construction of $(k,0)$-wise independent generators. Let n be a power of 2, i.e., $n = 2^\ell$. Let $T : \mathbb{F}_{2^\ell} \to \mathbb{F}_2$ be a non-trivial linear function. Consider the generator K that on seed $a = (a_0, a_1, \ldots, a_{k-1}) \in (\mathbb{F}_{2^\ell})^k$, treats the seed as the coefficients of a univariate polynomial p_a of degree $k-1$ over $\mathbb{F}_{2^\ell}$:

$$p_a(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_{k-1} x^{k-1}.$$

   and outputs the tuple $(T(p_a(z)) : z \in \mathbb{F}_{2^\ell})$. Note that $K : (\mathbb{F}_{2^\ell})^k \to \mathbb{F}_2^n$.

(a) Show that for any fixed distinct $k' \leq k$ points $x_1, \ldots, x_{k'} \in \mathbb{F}_{2^\ell}$ the distribution of $(p_{\mathbf{a}}(x_1), p_{\mathbf{a}}(x_2), \ldots, p_{\mathbf{a}}(x'_k)))$ on a random $\mathbf{a} \sim (\mathbb{F}_{2^\ell})^k$ is the uniform distribution over $(\mathbb{F}_{2^\ell})^{k'}$.

(b) Show that K generates a $(k, 0)$-wise independent distribution. (Hint: It suffices to prove that $K(\mathbf{a})$, on a uniform $\mathbf{a} \sim (\mathbb{F}_{2^\ell})^k$, is pseudorandom against parity functions on at most k variables with 0-error.)

(c) Let ϕ be a $\mathbb{F}_2$-linear bijection from $\mathbb{F}_2^{\ell k}$ to $(\mathbb{F}_{2^\ell})^k$, that is, $\phi(a+b) = \phi(a) + \phi(b)$ for all $a, b \in \mathbb{F}_2^{\ell k}$. (Such a bijection always exists.) Let $K' : \mathbb{F}_2^{\ell k} \to \mathbb{F}_2^n$ defined by $K'(a) = K(\phi(a))$. Show that K' is linear over $\mathbb{F}_2$.

(d) Let $B : \mathbb{F}_2^s \to \mathbb{F}_2^{\ell k}$ be a $(2^{-k/2} \cdot \delta)$-biased generator. Prove that $G(x) = K'(B(x))$ is a (k, δ)-wise independent generator. (Hint: Vazirani's XOR Lemma).

(e) Using the constructions of Naor-Naor or Alon-Goldreich-Håstad-Peralta (that we saw in class) for B, deduce that G has seed-length $s = O(k + \log\log(n) + \log(1/\delta))$.

3. **Derandomized BLR Test:** The following exercise is based on the Derandomized Linearity Test by Ben-Sasson, Sudan, Vadhan, and Wigderson. Let D be an ε-biased distribution over $\{-1, 1\}^n$. Given black-box access to a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the test:

- Picks $x \sim U_n$ uniformly at random.
- Picks $y \sim D$.
- Accepts if and only if $f(x) + f(y) = f(x + y)$.

For convenience, denote by $F(x) = (-1)^{f(x)}$, so that $F : \mathbb{F}_2^n \to \{-1, 1\}$. In this exercise, we show that if the Derandomized BLR Test accepts with probability at least $\frac{1+\delta}{2}$, then there exists a Fourier coefficient $\widehat{F}(S)$ with $|\widehat{F}(S)| \geq \sqrt{\delta^2 - \varepsilon}$. (Put differently, in this case the function either correlates well with some linear function χ_S or its negation $-\chi_S$.)

(a) Show that the probability that the test accepts f equals

$$\frac{1}{2} \cdot \left(1 + \mathop{\mathbf{E}}_{\substack{\mathbf{x} \sim U_n, \\ \mathbf{y} \sim D}} [F(\mathbf{x})F(\mathbf{y})F(\mathbf{x}+\mathbf{y})] \right).$$

(b) Assuming that the test accepts f with probability at least $(1 + \delta)/2$, deduce that

$$\delta \leq \mathop{\mathbf{E}}_{\mathbf{y} \sim D} [F(\mathbf{y}) \cdot (F * F)(\mathbf{y})].$$

(c) Show that $\delta^2 \leq \mathbf{E}_{\mathbf{y} \sim D}[(F * F)(\mathbf{y})^2]$ (Hint: Cauchy-Schwarz).

(d) Show that $\mathbf{E}_{\mathbf{y} \sim D}[(F * F)(\mathbf{y})^2] \leq \sum_S \widehat{F}(S)^4 + \varepsilon$.

(e) Deduce that there exists a Fourier coefficient $\widehat{F}(S)$ with $|\widehat{F}(S)| \geq \sqrt{\delta^2 - \varepsilon}$.