Analysis of Boolean Functions

CMU 18-859S, Spring 2007

PROBLEM SET 1

Due: Thursday, February 1

Homework policy: I encourage you to try to solve the problems by yourself. However, you may collaborate as long as you do the writeup yourself and list the people you talked with.

Notation used:

$[n]$	:	the set $\{1, 2, \ldots, n\}$
$x^{(i)}$	:	the n-bit string x with its ith bit flipped, where $i \in [n]$
S	:	always a subset of $[n]$, unless otherwise specified
$\mathbb{F}_2^n$	:	the n-dimensional vector space over the 2-element field $\mathbb{F}_2$
$H^\perp$	:	the orthogonal complement of the subspace H of $\mathbb{F}_2^n$; i.e., the subspace $\{x \in \mathbb{F}_2^n : \langle x, h\rangle = 0 \quad \forall h \in H\}$
$\mathbf{Pr}_{\boldsymbol{x}}$, $\mathbf{E}_{\boldsymbol{x}}$, $\mathbf{Var}_{\boldsymbol{x}}$	:	always denotes Probability, Expectation, Variance with respect to the *uniform* probability distribution of $\boldsymbol{x}$ on its range, unless otherwise specified

1. Poincaré Inequality I. Let $f : \{\mathrm{T}, \mathrm{F}\}^n \to \{\mathrm{T}, \mathrm{F}\}$. As in Lecture 1, define the *total influence* of f to be

$$\mathbb{I}(f) = \mathop{\mathbf{E}}_{\boldsymbol{x}}\left[\#\{i \in [n] : f(\boldsymbol{x}) \neq f(\boldsymbol{x}^{(i)})\}\right].$$

Show that

$$4 \mathop{\mathbf{Pr}}_{\boldsymbol{x}}[f(x) = \mathrm{T}] \mathop{\mathbf{Pr}}_{\boldsymbol{x}}[f(x) = \mathrm{F}] \leq \mathbb{I}(f).$$

(Please give a self-contained proof.)

2. Flipping Coins. Suppose you have a biased coin which has probability p of coming up heads. You try to approximate a fair coin toss by flipping the biased coin n times and declaring "overall heads" if the number of heads you flipped was odd. Show that the probability of "overall heads" is $\frac{1}{2} - \frac{1}{2}(1 - 2p)^n$.

3. Lagrange Interpolation. A multivariate polynomial with real coefficients is said to be *multilinear* if no variable in it is raised to a power greater than 1; e.g., $x_1x_2 + 3x_1x_3x_4 - .4x_2x_4 + 1.1$. In this problem we will give an alternate, direct proof (no linear algebra) that every function $f : \{-1,1\}^n \to \mathbb{R}$ can be uniquely expressed as an n-variate multilinear polynomial.

(a) Show existence by explicit construction. Use expressions like

$$\left(\frac{x_1+1}{2}\right)\left(\frac{x_2-1}{2}\right)\left(\frac{x_3-1}{2}\right),$$

which is 1 when $x = (1,-1,-1)$ and 0 elsewhere on the discrete cube.

(b) Show uniqueness by arguing that any nonzero n-variate multilinear polynomial must have a nonzero value somewhere in $\{-1,1\}^n$. *(Hint: Induction on n.)*

4. No Weight Beyond Level 1.
(a) Suppose $f : \{-1,1\}^n \to \{-1,1\}$ satisfies

$$\sum_{|S|>1} \hat{f}(S)^2 = 0.$$

Show that f is a 1-junta (i.e., a constant function, a dictator, or an anti-dictator).

(b) Show that the above result is not true if 1 is replaced by 2.

5. Odd Functions. A function $f : \{-1,1\}^n \to \mathbb{R}$ is said to be *odd* if $f(-x) = -f(x)$ for all $x \in \{-1,1\}^n$. Show that f is odd if and only if "f only has odd Fourier coefficients" — i.e., $\hat{f}(S) = 0$ for all S of even cardinality.

6. Indicators of Subspaces. Let H be a subspace of $\mathbb{F}_2^n$ of *codimension* d; i.e., $\dim(H^\perp) = d$. Let $f : \mathbb{F}_2^n \to \{0,1\}$ denote the indicator function of H (here 0 and 1 in f's range are treated as real numbers).

(a) Show that for all $S \subseteq [n]$,

$$\hat{f}(S) = \begin{cases} 2^{-d} & \text{if } S \in H^\perp, \\ 0 & \text{else,} \end{cases}$$

where in "$S \in H^\perp$" we identify the subset S with its 0-1 characteristic vector.

(b) Derive from (a) the Fourier transform of the AND function AND : $\{-1,1\}^n \to \{-1,1\}$, where -1 is interpreted as True and 1 as False.

(c) Derive the Fourier transform of the OR function OR : $\{-1,1\}^n \to \{-1,1\}$.

7. Testing 1-Resiliency. In cryptography, a boolean function $f : \{-1,1\}^n \to \{-1,1\}$ is said to be *dth order correlation-immune* if $\mathbf{E}[g] = \mathbf{E}[f]$ for every function g which is a restriction of f gotten by fixing up to d coordinates. If in addition $\mathbf{E}[f] = 0$, f is said to be *d-resilient*.

(a) Show that f is dth order correlation-immune if and only if $\hat{f}(S) = 0$ for all $1 \leq |S| \leq d$.

(b) Give a $\mathrm{poly}(1/\epsilon)$-query test with the following properties: If f is 1-resilient, the test outputs YES with probability at least $2/3$; if $\hat{f}(S)^2 \geq \epsilon$ for some $|S| \leq 1$, the test outputs NO with probability at least $2/3$. (NB: This is not quite the same thing as a “2-sided test for the property of being 1-resilient”.)

(Hint: You’ll probably need the following Chernoff bound: If $\boldsymbol{X}$ is a random variable with values in $[-1,1]$, then the empirical average of $\boldsymbol{X}$ after $O(\log(1/\delta)/\gamma^2)$ samples is within $\pm\gamma$ of $\mathbf{E}[\boldsymbol{X}]$, with probability at least $1-\delta$.)