COS 522 Complexity — Homework 6.

Boaz Barak

Total of 110 points. Due May 8th, 2006.

Exercise 1 (20 points)**.** Let $f, g : \{\pm 1\}^n \to \mathbb{R}$ be two functions. We define the *convolution* of f and g, $h : \{\pm 1\}^n \to \mathbb{R}$ in the following function: $h(x) = \mathbb{E}_{y \leftarrow_{\mathrm{R}} \{\pm 1\}^n}[f(x)g(x \oplus y)]$ (recall that we use $\oplus$ to denote componentwise multiplication).

1. Compute the Fourier expansion of h in terms of the Fourier expansions of f, g.
2. For a function $f : \{\pm 1\}^n \to \mathbb{R}$ and number $\epsilon < 1/2$ define $f'(x) = \mathbb{E}_{z \leftarrow_{\mathrm{R}} M_\epsilon}[f(x \oplus z)]$ where $z \leftarrow_{\mathrm{R}} M_\epsilon$ is chosen in the following way: for each i independently choose $z_i = +1$ with probability $1 - \epsilon$ and $z_i = -1$ with probability ϵ. Compute the Fourier expansion of f' in terms of the Fourier expansion of f.
3. Write a function g such that the convolution of f and g yields f'.

Exercise 2 (20 points + 10 points bonus)**.** Let $f : \{\pm 1\}^n \to \mathbb{R}$ and let $I \subseteq [n]$. Let M_I be the following distribution: we choose $z \leftarrow_{\mathrm{R}} M_I$ by for $i \in I$, choose z_i to be $+1$ with probability $1/2$ and -1 with probability $1/2$ (independently of other choices), for $i \notin I$ choose $z_i = +1$. We define the *variation of f on I* to be $\Pr_{x \leftarrow_{\mathrm{R}} \{\pm 1\}^n, z \leftarrow_{\mathrm{R}} M_I}[f(x) \neq f(x \oplus y)]$.

Suppose that the variation of f on I is less than ϵ. Prove that there exists a function $g : \{\pm 1\}^n \to \mathbb{R}$ such that **(1)** g does not depend on the coordinates in I and **(2)** g is 10ϵ-close to f (i.e., $\Pr_{x \leftarrow_{\mathrm{R}} \{\pm 1\}^n}[f(x) \neq g(x)] < 10\epsilon$). Can you come up with such a g that outputs values in $\{\pm 1\}$ only? (Bonus 10 points).

Exercise 3 (20 points)**.** For $f : \{\pm 1\}^n \to \{\pm 1\}$ and $x \in \{\pm 1\}^n$ we define $N_f(x)$ to be the number of coordinates i such that if we let y to be x flipped at the i^{th} coordinate (i.e., $y = x \oplus e^i$ where e^i has -1 in the i^{th} coordinate and $+1$ everywhere else) then $f(x) \neq f(y)$. We define the *average sensitivity* of f, denoted by $as(f)$ to be the expectation of $N_f(x)$ for $x \leftarrow_{\mathrm{R}} \{0, 1\}^n$.

1. Prove that for every balanced function $f : \{\pm 1\}^n \to \{\pm 1\}$ (i.e., $\Pr[f(x) = +1] = 1/2$), $as(f) \geq 1$.
2. Let f be balanced function from $\{\pm 1\}^n$ to $\{\pm 1\}$ with $as(f) = 1$. Prove that f is a dictatorship or its complement. (i.e., $f(x) = x_i$ or $f(x) = -x_i$)

Exercise 4 (20 points)**.** The *depth* of a directed acyclic graph G is the length of the longest path in the graph. Prove that for every constants $c > 1$ and $\epsilon > 0$, for sufficiently large n and G be an n-vertex graph with depth $c \log n$, and each vertex having in-degree and out-degree at most two, there exists a set B of edges such that:

- $|B| \leq \epsilon n$.

- The depth of the graph $G \setminus B$ (i.e., G with all edges in B removed) is at most $\epsilon \log n$.

Exercise 5 (20 points)**.** An $n \times n$-matrix A over $\mathsf{GF}(2)$ is called *ϵ-rigid* if there do not exist two $n \times n$ matrices B and C such that **(1)** the rank of B is at most ϵn **(2)** each row of C contains at most n^ϵ nonzero entries and **(3)** $A = B + C$. Prove that:

1. For every fixed ϵ, a random $n \times n$ matrix A is ϵ-rigid with probability $1 - o(1)$ (i.e., probability tending to 1 as n grows to infinity).

2. Define a *linear* circuit over $\mathsf{GF}(2)$ to be a circuit whose gates consist only of the operation $\oplus$. Let $\epsilon > 0$ be a constant and let $\{A_n\}$ be a sequence of ϵ-rigid matrices. Then there do *not* exist constants c, d and a sequence of linear circuits $\{C_n\}$ such that **(1)** C_n computes the linear function $\vec{v} \mapsto A_n \vec{v}$ and **(2)** the size of C_n is at most cn and **(3)** the depth of C_n (the length of longest input to output path) is at most $d \log n$.

Note that this means that an explicit construction of a sequence of rigid matrices would give an explicit linear function that cannot be computed by linear circuits of linear sized and logarithmic depth.[1]

[1] Note that the term "linear" was used in two different senses in the last sentence.