Advanced Complexity Theory 18.405/6.841 Due: Thursday, May 17th, 2001 — Dan Spielman

no extensions available!

Problem Set 4

1 Let f be a function from $\{0,1,\ldots,d\}^n$ into a field $\mathbf{F}$. Show that, when $\mathbf{F}$ is the field of real numbers or a field $\mathbf{Z}/p$ for a prime $p > d$, there is a unique polynomial Q over $\mathbf{F}$ of degree at most d in each of its variables such that

$$f(x_1,\ldots,x_n) = Q(x_1,\ldots,x_n) \text{ for all } (x_1,\ldots,x_n) \in \{0,1,\ldots,d\}^n.$$

Partial credit will be given for the case $d = 1$.

Note: $3x^2 + 2yz^2 + 1$ has degree at most two in each of its variables.

2 Minimum set cover is the following problem: given a collection of sets $\{S_1, S_2 \ldots, S_m\}$, each a subset of U, determine the minimum number of the S_i's needed to cover every element of U. (the collection covers an element if it is in the union of the sets in the collection). Prove that there is some constant c such that it is NP-hard to approximite minimum set cover to within a factor of c.

In our proof that $NEXP \subseteq PCP(poly, poly)$, the PCP that we constructed contained a table

$$\hat{A} : \mathbf{F}^n \to \mathbf{F}.$$

We sketched a proof of a multilinearity test for $\hat{A}$ such that if the probability that $\hat{A}$ passes the test is greater than 1/4 (arbitrary constant), then there exists a multilinear L such that

$$\operatorname*{Prob}_{\vec{x} \in S^n}[L(x) \neq \hat{A}(x)] < 1/n^{10},$$

where $S = \mathbf{F}$ if $\mathbf{F}$ is a finite field. If $\mathbf{F}$ is the reals (or integers), then S is just $\{0,1,\ldots,N\}$ for some large N that we can represent with a polynomial number of bits.

Assuming that $\hat{A}$ passes the test, we will assume that the above condition holds. We still need to verify that

$$\text{for all } \vec{x} \in \{0,1\}^n,\ \hat{A}(\vec{x}) \in \{0,1\} \tag{1}$$

3a. Describe a protocol for a verifier V and a proof format Π such that

$$\begin{aligned} \operatorname{Prob}[V^{\hat{A},\Pi}\text{accepts}] &= 1 \qquad \text{if (1) holds, and} \\ \operatorname{Prob}[V^{\hat{A},\Pi}\text{accepts}] &< 1/2 \qquad \text{if (1) does not hold.} \end{aligned}$$

You may assume that $\hat{A}$ is multilinear. For this part, assume that $\mathbf{F}$ is the reals or integers. Prove that your protocol is correct. Hint: consider the polynomial $(x(1-x))^2$.

3b. Same as 3a, but with $\mathbf{F}$ a finite field. You can assume that $\mathbf{F} = \mathbf{Z}/p$ for a prime $p > poly(n)$ for any *poly* you like. Hint: consider multiplying $\hat{A}$ by the multilinear poly

$$\prod_{i=1}^{n}(1 + x_i(a_i - 1)),$$

for randomly chosen $a_1, \ldots, a_n \in S$.

Let $\mathbf{F}$ be the field $\mathbf{Z}/p$, where p is a prime. A function $f : \mathbf{F}^n \to \mathbf{F}$ is called *multilinear* if there exists a polynomial q that has degree at most one in each variable and is equal to f on all of $\mathbf{F}^n$. By ML_n, we denote the set of all multilinear functions from $\mathbf{F}^n \to \mathbf{F}$. By $d(f, g)$, we mean $\text{Prob}_{\vec{x} \in \mathbf{F}^n}[f(\vec{x}) \neq g(\vec{x}))]$. Assume in the following problems that $n/p < 1/6$.

4 Assume that $f : \mathbf{F}^n \to \mathbf{F}$ has degree at most one in x_1. Prove that one of the following must hold:

a. the inequality $|d(f, ML_n) - d(f_{x_1=c}, ML_{n-1})| \leq 1/\sqrt{p}$ holds with probability at least $1 - \frac{1}{\sqrt{p}}$ for a random $c \in \mathbf{F}$, or

b. $d(f_{x_1=c}, ML_{n-1}) > 1/6$ for all c except at most one.

Note: by $f_{x_1=c}$, we mean the function of $n-1$ variables obtained from f by fixing $x_1 = c$.

5 Julia's due date was the same day this problem set is due. She was born on April 30th. How early was she?

Homework policy:

If you work with anyone else on the homework, please give them due credit (i.e., list who you worked with on which problems). Cite any sources you use, but please don't look up the answer. If you don't know the answer to a problem, then just don't answer it. Do not write anything you don't believe. Avoid making yourself believe a false proof—it damages your brain.