18.405J/6.841J Advanced Complexity Theory	April 25, 2001
Lecture 20	
Lecturer: Dan Spielman	*Scribe: Jan Vondrák*

The Multilinearity Test

In this lecture, we describe the *multilinearity test* which is used by the verifier in the proof of NEXP $\subseteq$ PCP(poly,poly).

For a finite field F and a function $f : F^n \to F$, given by a table of values, we want to decide if f is "close" to a multilinear function, by looking at a polynomial number of entries in the table. Our test will be randomized and we would like to have the following properties:

- If f is multilinear then $Pr[\text{test accepts}] = 1$.
- If $Pr[\text{test accepts}] > \frac{1}{2}$ then there is a multilinear function L which differs from f at most in a $\frac{1}{n^k}$-fraction of places (for some k fixed).

The test is surprisingly simple. However, its analysis is more difficult.

The Test:

Repeat t times:

- Choose $(x_1, \ldots, x_n) \in F^n$ uniformly at random.
- For $i = 1 \ldots n$, let $a_i(z) = f(x_1, \ldots, x_i' = z, \ldots, x_n)$.
- If for any i, $a_i(x_i) \neq a_i(0) + x_i(a_i(1) - a_i(0))$, stop and reject.

Accept if all iterations have been completed successfully.

Definition 1 *Let ML_n denote the class of all multilinear functions from F^n to F. For functions $f, g : F^n \to F$, define their distance as*

$$d(f,g) = \Pr_{x \in F^n}[f(x) \neq g(x)].$$

Lemma 2 *If $|F| = q > 6n$ then for any two different $L_1, L_2 \in ML_n$,*

$$d(L_1, L_2) > \frac{5}{6}.$$

Proof: If $L_1 \neq L_2$ then $L_1 - L_2$ is a non-zero multilinear function. By Schwartz's lemma (with degree at most 1 in each variable),

$$\Pr_{x \in F^n}[(L_1 - L_2)(x) = 0] \leq \frac{n}{q} < \frac{1}{6}.$$

As a corollary, for any f there can be at most one multilinear function "close" to f (satisfying $d(f, L) < \frac{1}{3}$, for instance).

First, we demonstrate how the test works in two variables. Let $f : F^2 \rightarrow F$. If f is multilinear then the test clearly accepts with probability 1.

So suppose f is not multilinear. From f, we derive two functions which are linear in x_1 and x_2, respectively.

$$f^1(x_1, x_2) = f(0, x_2) + x_1(f(1, x_2) - f(0, x_2)),$$
$$f^2(x_1, x_2) = f(x_1, 0) + x_2(f(x_1, 1) - f(x_1, 0)).$$

The way the test works, we are actually testing the difference between f and f^1, f^2. If $d(f, f^i) = \epsilon_i$, the test for the i-th coordinate rejects with probability ϵ_i. Therefore,

$$Pr[\text{test accepts}] \leq (1 - \max\{d(f, f^1), d(f, f^2)\})^t.$$

Our goal is to show that if the test accepts with high probability, f is not only close to f^1 and f^2 but it is close to some multilinear function. Call $(x_1, x_2) \in F^2$ *good* if $f(x_1, x_2) = f^1(x_1, x_2) = f^2(x_1, x_2)$. In other words, the test passes an iteration iff it chooses a good point.

Lemma 3

$$\Pr_{x_1, x_2}[(x_1, x_2) \textit{ is good}] > 1 - \epsilon \Rightarrow \exists L \in ML_2; d(f, L) < 5\epsilon.$$

Proof: If

$$\Pr_{x_1, x_2}[(x_1, x_2) \text{ is good}] > 1 - \epsilon$$

then

$$\Pr_{x_1, x_2}[(x_1, x_2) \text{ is bad}] < \epsilon$$

and by Markov's inequality, for at least 1/2 values of x_1,

$$\Pr_{x_2}[(x_1, x_2) \text{ is bad}] < 2\epsilon.$$

Let c, d be two values of x_1 for which this is true and define a multilinear function

$$L(x_1, x_2) = f^2(c, x_2) + \frac{f^2(d, x_2) - f^2(c, x_2)}{d - c}(x_1 - c).$$

At least a $(1 - 4\epsilon)$-portion of x_2's are good for both c and d; i.e., $f^1(c, x_2) = f^2(c, x_2) = L(c, x_2)$ and $f^1(d, x_2) = f^2(d, x_2) = L(d, x_2)$. For such x_2, $L(x, x_2)$ and $f^1(x, x_2)$ are equal as functions of x (because a linear function is determined by its values at two points). Thus

$$d(f^1, L) = \Pr_{x_1, x_2}[L(x_1, x_2) \neq f^1(x_1, x_2)] \leq 4\epsilon.$$

Obviously, $d(f, f^1) \leq \epsilon$ and so

$$d(f, L) \leq 5\epsilon.$$

For $\epsilon = \frac{1}{n^k}$, we repeat our test n^k times and then if the acceptance probability is still high, the lemma implies that f is closer than $O(\frac{1}{n^k})$ to a multilinear function. Unfortunately, this proof does not generalize to an arbitrary number of variables. We sketch out how the test can be analyzed for n variables.

From $f : F^n \rightarrow F$, we derive $f^1, \ldots, f^n$ linear in $x_1, x_2, \ldots, x_n$ respectively. They key observation is that $d(f^1, ML_n)$ is reasonably approximated by $d(f^1_{x_1=c}, ML_{n-1})$, i.e. instead of f^1 we consider the slice taken at a random point $x_1 = c$, which reduces the number of variables by one.

More precisely, we give the following without proof.

Lemma 4 *If f^1 is linear in x_1, then either*

$$\Pr_{c \in F}[d(f^1, ML_n) - d(f^1_{x_1=c}, ML_{n-1}) \leq \frac{1}{\sqrt{q}}] \geq 1 - \frac{1}{\sqrt{q}}$$

or $d(f^1_{x_1=c}, ML_{n-1}) > \frac{1}{6}$ for all but one value of c_1.

For now, we ignore the latter possibility and apply this idea successively to all variables. For "most" values of $c_1, c_2, \ldots$, we have

$$d(f, ML_n) \leq d(f, f^1) + d(f^1, ML_n) \leq d(f, f^1) + d(f^1_{x_1=c_1}, ML_{n-1}) + \frac{1}{\sqrt{q}}$$

$$\leq d(f, f^1) + d(f^1_{x_1=c_1}, f^2_{x_1=c_1}) + d(f^2_{x_1=c_1}, ML_{n-1}) + \frac{1}{\sqrt{q}}$$

$$\leq d(f, f^1) + d(f^1_{x_1=c_1}, f^2_{x_1=c_1}) + d(f^2_{x_1=c_1, x_2=c_2}, ML_{n-2}) + \frac{2}{\sqrt{q}}$$

$$\cdots$$

$$\leq d(f, f^1) + d(f^1_{x_1=c_1}, f^2_{x_1=c_1}) + d(f^2_{x_1=c_1, x_2=c_2}, f^3_{x_1=c_1, x_2=c_2}) + \ldots + \frac{n}{\sqrt{q}}.$$

This holds for all but a $\frac{1}{\sqrt{q}}$-fraction of each c_i; by averaging over the c_i's, we get an additional error term of $\frac{1}{\sqrt{q}}$ for each variable:

$$d(f, ML_n) \leq d(f, f^1) + d(f^1, f^2) + d(f^2, f^3) + \ldots + d(f^{n-1}, f^n) + \frac{2n}{\sqrt{q}}$$

$$\leq 2 \sum_{i=1}^{n} d(f, f^i) + \frac{2n}{\sqrt{q}}.$$

So far, we have ignored the possibility that $d(f^i, ML_{n-i}) > 1/6$ for all but one value of c_i. However, if we multiply the right hand side by a factor of 6, the inequalities will be satisfied trivially in this case.

Theorem 5

$$d(f, ML_n) \leq 12 \left(\sum_{i=1}^{n} d(f, f^i) + \frac{n}{\sqrt{q}} \right).$$

This means that if our test accepts with high probability and the distances $d(f, f^i)$ are small then f must be very close to a multilinear function.