Lecture 12

Foundations of Probabilistic Proofs
Fall 2020
Alessandro Chiesa

Low-Degree Testing

Recall the goal of linearity testing:

input: $\mathbb{F}, n$
oracle: $f: \mathbb{F}^n \to \mathbb{F}$
requirement: YES w.p. 1 if $f \in LIN(\mathbb{F}, n)$
YES w.p. ½ if f is $\frac{1}{10}$-far from $LIN(\mathbb{F}, n)$

The goal of low-degree testing is:

input: $\mathbb{F}, n, d$
oracle: $f: \mathbb{F}^n \to \mathbb{F}$
requirement: YES w.p. 1 if $f \in LD(\mathbb{F}, n, d)$
YES w.p. ½ if f is $1/10$-far from $LD(\mathbb{F}, n, d)$

What does degree d mean?

- total degree (e.g. in this case $LD(\mathbb{F}, n, tot \leq 1) = LIN(\mathbb{F}, n)$)
- individual degree (e.g. in this case $LD(\mathbb{F}, n, ind \leq 1)$ is multilinear polys)

A test for individual degree can be derived from a test for total degree.

Either way in most applications to PCPs the difference does not matter.

Today we study total degree:

Step 1: understand $n=1$ (univariate polys) Step 2: extend to $n>1$ (multivariate polys)

Univariate Polynomials: a Basic Test

Idea: any $d+1$ locations determine a polynomial

$T^{f:\mathbb{F}\to\mathbb{F}}(\mathbb{F},d) :=$ 1. sample $r \in \mathbb{F}$
2. query f at $a_0, a_1, \ldots, a_d, r$
3. let $\tilde{p}(x)$ be the interpolation of $\{(a_i, f(a_i))\}_{i=0}^{d}$
4. check that $\tilde{p}(r) = f(r)$

query complexity:
$d+2 = O(d)$
[& non-adaptive]

Completeness: if $f \equiv p$ for a polynomial $p(x)$ of degree $\leq d$
then $\tilde{p} = p$ and so $\forall r \in \mathbb{F}$ $\tilde{p}(r) = p(r) = f(r)$

Soundness: $\Pr[\text{accept}] = \Pr_r[\tilde{p}(r) = f(r)] \leq 1 - \Delta(f, \mathbb{F}^{\leq d}[X])$

The query complexity of $O(d)$ could be much less than $|\mathbb{F}|$ (reading all of f).
Also, one can prove that a query complexity of $\Omega(d)$ is necessary.

Univariate Polynomials: a Different Attempt

We focus on a special case: $\mathbb{F} = \mathbb{F}_p$ for prime $p \geq d+2$.

The test is inspired by a different local characterization of low-degree polynomials:

<u>def</u>: For $i = 0, 1, \ldots, d+1$ $\quad c_i := (-1)^{i+1} \binom{d+1}{i} \in \mathbb{F}_p$.

<u>lemma</u>: $\forall\, d < p$, $\forall\, f : \mathbb{F}_p \to \mathbb{F}_p$ $\quad f \in \mathbb{F}^{\leq d}[X]$ iff $\forall a \in \mathbb{F}_p \quad \sum_{i=0}^{d+1} c_i \cdot f(a+i) = 0$

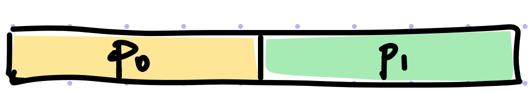
<u>proof</u>: Induction and formal derivatives. Ex for $d=0$: $(c_0, c_1) = (-1, 1) \to -f(a) + f(a+1) = 0$.

Ex for $d=1$: $(c_0, c_1, c_2) = (-1, 2, -1) \to -f(a) + 2f(a+1) - f(a+2) = 0$, i.e., $\frac{f(a+1) - f(a)}{(a+1) - a} - \frac{f(a+2) - f(a+1)}{(a+2) - (a+1)} = 0$.

A new proposal:

$T^{f : \mathbb{F}_p \to \mathbb{F}_p}(\mathbb{F}_p, d) :=$
1. sample $r \leftarrow \mathbb{F}_p$
2. query f at $r, r+1, \ldots, r+(d+1)$
3. check that $\sum_{i=0}^{d+1} c_i \cdot f(r+i) = 0$

Problem: it does not work. [Not all local characterizations do!]

Consider f: 

, which has distance $1/2$ to $\mathbb{F}^{\leq d}[X]$.

But the test rejects only with probability $\approx d/(|\mathbb{F}|/2)$.

A Refined Local Characterization

def: For $i = 0, 1, \dots, d+1$ $\quad c_i := (-1)^{i+1}\binom{d+1}{i} \in \mathbb{F}_p$.

lemma: $\forall d < p$, $\forall f: \mathbb{F}_p \to \mathbb{F}_p$ $\quad f \in \mathbb{F}^{\leq d}[X]$ iff $\forall a \in \mathbb{F}_p$ $\sum_{i=0}^{d+1} c_i \cdot f(a+i) = 0$

corollary: $\forall d < p$, $\forall f: \mathbb{F}_p \to \mathbb{F}_p$

$$f \in \mathbb{F}^{\leq d}[X] \text{ iff } \forall a, b \in \mathbb{F}_p \ \sum_{i=0}^{d+1} c_i f(a+ib) = 0$$

proof: For the direction "$\Leftarrow$" set $b = 1$ and invoke lemma.
For the direction "$\Rightarrow$", fix $a, b \in \mathbb{F}_p$ and consider $g(x) := f(a+xb)$.
The degree of g is at most d. Hence, by lemma,

$$\forall e \in \mathbb{F}_p \quad 0 = \sum_{i=0}^{d+1} c_i g(e+i) = \sum_{i=0}^{d+1} c_i \cdot f(a+(e+i)b) = \sum_{i=0}^{d+1} c_i \cdot f((a+eb)+ib).$$

Now set $e = 0$, and we get the condition for a, b. $\blacksquare$

We have increased from $|\mathbb{F}_p|$ local conditions to $|\mathbb{F}_p|^2$.
The choice of b randomizes the "step size" and seems to rule out the prior counterexample.

Univariate Polynomials: the Rubinfeld-Sudan Test

Check one of the $|\mathbb{F}_p|^2$ local conditions at random:

$T^{f:\mathbb{F}_p\to\mathbb{F}_p}(\mathbb{F}_p, d) :=$ 1. sample $r, s \leftarrow \mathbb{F}_p$
2. query f at $r, r+s, \ldots, r+(d+1)\cdot s$
3. check that $\sum_{i=0}^{d+1} c_i \cdot f(r+i\cdot s) = 0$

query complexity: $d+2 = O(d)$
[& non-adaptive]

Completeness: if $f \in \mathbb{F}_p^{\leq d}[X]$ then $\Pr_{r,s}[T^f = 1] = 1$ by corollary

Soundness: if f is $\frac{1}{10}$-far from $\mathbb{F}_p^{\leq d}[X]$ then $\Pr[T^f = 1] \leq 1 - O\left(\frac{1}{d^2}\right)$.

theorem: $\Pr[T^f = 0] \geq \min\left\{\Omega\left(\frac{1}{d^2}\right), \frac{1}{2}\cdot\Delta\left(f, \mathbb{F}_p^{\leq d}[X]\right)\right\}$

Isn't this test worse?

- lose a factor of 2 in distance (previously, $\Pr[T^f = 0] \geq \Delta(f, \mathbb{F}_p^{\leq d}[X])$)
- high agreement regime: even if f is $\frac{1}{10}$-far we only get error $\leq 1 - O\left(\frac{1}{d^2}\right)$, so we need to repeat the test $O(d^2)$ times for constant error $\Rightarrow O(d^3)$ queries

But: this test will extend to multivariate polynomials with no changes

Analysis of the RS Test - Part 1

$\sum_{i=0}^{d+1} c_i \cdot f(r+is) = 0 \Leftrightarrow f(r) = \sum_{i=1}^{d+1} c_i f(r+is)$

The analysis is analogous to the combinatorial analysis of the BLR test.
We consider the plurality (most popular) values:

$g_f : \mathbb{F}_p \to \mathbb{F}_p$ is defined as $g_f(x) := \arg\max_{v \in \mathbb{F}_p} \left| \left\{ s \in \mathbb{F}_p \mid v = \sum_{i=1}^{d+1} c_i \cdot f(x+is) \right\} \right|$.

If g_f is far from f then T must reject with high probability:

<u>claim:</u> $\Pr[T^f = 0] \geq \frac{1}{2} \cdot \Delta(g_f, f)$

<u>proof:</u> Letting $S = \left\{ r \in \mathbb{F}_p \text{ s.t. } \Pr_s\left[f(r) \neq \sum_{i=1}^{d+1} c_i \cdot f(r+is) \right] \geq \frac{1}{2} \right\}$, we get

$$\Pr[T^f = 0] = \Pr_r[r \in S] \Pr_{r,s}[T^f = 0 \mid r \in S] + \Pr_r[r \notin S] \cdot \Pr_{r,s}[T^f = 0 \mid r \notin S]$$

$$\geq \frac{|S|}{|\mathbb{F}|} \cdot \min_{r \in S} \left\{ \Pr_s\left[f(r) \neq \sum_{i=1}^{d+1} c_i \cdot f(r+is) \right] \right\} + 0 \geq \frac{|S|}{|\mathbb{F}|} \cdot \frac{1}{2}.$$

Also, for every $r \notin S$ we have $\Pr_s\left[f(r) = \sum_{i=1}^{d+1} c_i f(r+is) \right] > \frac{1}{2}$ so $f(r) = g_f(r)$.
This tells us that $\frac{|S|}{|\mathbb{F}|} \geq \Delta(g_f, f)$.

$\blacksquare$

Analysis of the RS Test - Part 2

claim: $\forall r \in \mathbb{F}_p,\ \Pr_s\left[g_f(r) = \sum_{i=1}^{d+1} c_i f(r+is)\right] \geq 1 - 2\cdot(d+1)\cdot \Pr\left[T^f = 0\right]$

proof:

$$\Pr_s\left[g_f(r) = \sum_{i=1}^{d+1} c_i f(r+is)\right] = \max_{v\in\mathbb{F}_p} \Pr_s\left[v = \sum_{i=1}^{d+1} c_i\cdot f(r+is)\right]$$

$\sum_i p_i^2 \leq \max_i\{p_i\}\cdot \sum_i p_i$

$$\geq \sum_{v\in\mathbb{F}_p} \Pr_s\left[v = \sum_{i=1}^{d+1} c_i f(r+is)\right]^2$$

$$= \Pr_{s,t}\left[\sum_{i=1}^{d+1} c_i f(r+is) = \sum_{i=1}^{d+1} c_i f(r+it)\right]$$

Union bounds $\longrightarrow$ $\geq 1 - 2(d+1)\Pr\left[T^f = 0\right]$

For any $s,t\in\mathbb{F}$ if $\begin{cases} \forall i\in\{1,\dots,d+1\}\ f(r+is) = \sum_{j=1}^{d+1} c_j\cdot f((r+is)+jt) \\ \forall j\in\{1,\dots,d+1\}\ f(r+js) = \sum_{i=1}^{d+1} c_i\cdot f((r+jt)+is) \end{cases}$,

then $\sum_{i=1}^{d+1} c_i\cdot f(r+is) = \sum_{i=1}^{d+1} c_i \sum_{j=1}^{d+1} c_j f((r+is)+jt) = \sum_{j=1}^{d+1} c_j \sum_{i=1}^{d+1} c_i f((r+jt)+is) = \sum_{j=1}^{d+1} c_j f(r+jt)$

Hence:

$$\Pr_{s,t}\left[\sum_{i=1}^{d+1} c_i f(r+is) \neq \sum_{i=1}^{d+1} c_i f(r+it)\right] \leq \Pr_{s,t}\left[\begin{array}{l} \exists i\ f(r+is) \neq \sum_{j=1}^{d+1} c_j f((r+is)+jt) \\ \text{or} \\ \exists j\ f(r+jt) \neq \sum_{i=1}^{d+1} c_i f((r+jt)+is) \end{array}\right] \leq 2(d+1)\Pr\left[T^f = 0\right].$$

Analysis of the RS Test - Part 3

Let $g_f(x) := \arg\max_{v \in \mathbb{F}} \left| \left\{ s \in \mathbb{F} \;\middle|\; v = \sum_{i=1}^{d+1} c_i \cdot f(x+is) \right\} \right|$ be the plurality correction of f.

We proved that $\Pr[T^f=0] \geq \frac{1}{2} \cdot \Delta(g_f, f)$ & $\forall r \in \mathbb{F}_p, \Pr_s\left[g_f(r) = \sum_{i=1}^{d+1} c_i f(r+is)\right] \geq 1 - 2\cdot(d+1)\Pr[T^f=0]$.

$> 1 - \frac{1}{2\cdot(d+2)}$

If $\Pr[T^f=0] \geq \frac{1}{4(d+2)^2}$ then we are done. So assume that $\Pr[T^f=0] < \frac{1}{4\cdot(d+2)^2}$.

We prove that $g_f \in \mathbb{F}_p^{\leq d}[X]$, so we are done as $\Pr[T^f=0] \geq \frac{1}{2}\Delta(g_f, f) = \frac{1}{2}\cdot\Delta(f, \mathbb{F}_p^{\leq d}[X])$.

<u>claim</u>: if $\Pr[T^f=0] < \frac{1}{4\cdot(d+2)^2}$ then $\forall r, s \in \mathbb{F}_p \; \sum_{i=0}^{d+1} c_i g_f(r+is) = 0$

<u>proof</u>: If $\exists t_1, t_2 \in \mathbb{F}_p$ s.t. $\begin{cases} \forall i \in \{0,1,\dots,d+1\} \; g_f(r+is) = \sum_{j=1}^{d+1} c_j f((r+is)+j(t_1+it_2)) \\ \forall j \in \{1,\dots,d+1\} \; \sum_{i=0}^{d+1} c_i f((r+jt_1)+i(s+jt_2)) = 0 \end{cases}$

then $\sum_{i=0}^{d+1} c_i g_f(r+is) = \sum_{i=0}^{d+1} c_i \cdot \left[\sum_{j=1}^{d+1} c_j f((r+is)+j(t_1+it_2))\right] = \sum_{j=1}^{d+1} c_j \left[\sum_{i=0}^{d+1} c_i f((r+jt_1)+j(t_1+it_2))\right] = \sum_{j=1}^{d+1} c_j \cdot 0 = 0$.

Hence by union bound:

$$\Pr_{t_1,t_2}\left[\sum_{i=0}^{d+1} c_i \cdot g_f(r+is) \neq 0\right] \leq \Pr_{t_1,t_2}\left[\begin{array}{l} \exists i \in \{0,1,\dots,d+1\} \; g_f(r+is) \neq \sum_{j=1}^{d+1} c_j \cdot f((r+is)+j\cdot(t_1+it_2)) \\ \text{or} \\ \exists j \in \{1,\dots,d+1\} \; \sum_{i=0}^{d+1} c_i \cdot f((r+jt_1)+i\cdot(s+jt_2)) \neq 0 \end{array}\right]$$

$$\leq (d+2)\cdot\frac{1}{2(d+2)} + (d+1)\cdot\frac{1}{4\cdot(d+2)^2} < 1$$

$\blacksquare$

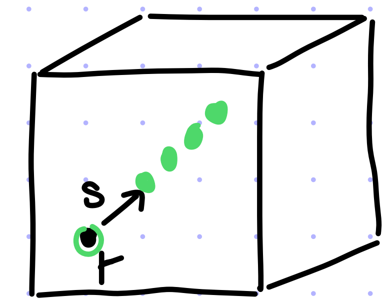
Extending the RS Test to Multivariate Polynomials

The local characterization holds similarly: refers to total degree

$$\forall d<p,\ \forall f:\mathbb{F}_p^n\to\mathbb{F}_p \quad f\in\mathbb{F}^{\leq d}[X_1,\dots,X_n] \text{ iff } \forall a,b\in\mathbb{F}_p^n\ \sum_{i=0}^{d+1} c_i f(a+ib)=0$$

The test is also similar: query complexity is $d+2=O(d)$

$T^{f:\mathbb{F}_p^n\to\mathbb{F}_p}(\mathbb{F}_p,d):=$
1. sample $r,s\leftarrow\mathbb{F}_p^n$
2. query f at $r, r+s, \dots, r+(d+1)\cdot s$
3. check that $\sum_{i=0}^{d+1} c_i\cdot f(r+i\cdot s)=0$



random-line test

The theorem for soundness is also similar:

theorem: $\Pr[T^f=0]\geq\min\left\{\Omega\left(\frac{1}{d^2}\right),\frac{1}{2}\cdot\Delta\left(f,\mathbb{F}_p^{\leq d}[X_1,\dots,X_n]\right)\right\}$

And its proof is the same up to synctactic modifications!

In sum, by repeating the test $O(d^2)$ times, we get:
a low-degree test with query complexity $O(d^3)$ [independent of n!] where constant relative distance → constant soundness error.