Foundations of Probabilistic Proofs

A course by **Alessandro Chiesa**

Lecture 09

Low-Degree Testing

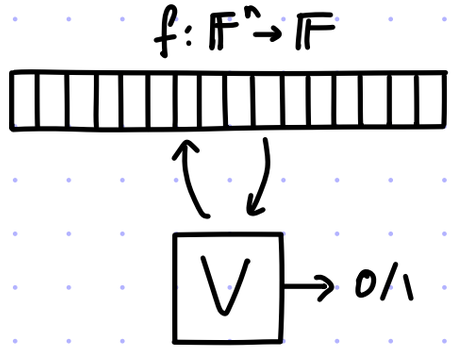
These slides are licensed under the CC BY-SA 4.0 license.

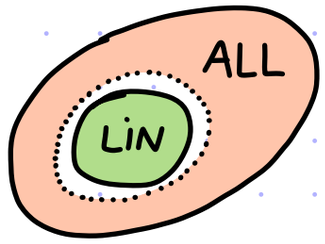
Low-Degree Testing

Recall the goal of LINEARITY TESTING:

A test V_{LIN} s.t. $\forall f: \mathbb{F}^n \to \mathbb{F}$

- completeness: $f \in LIN[\mathbb{F}, n] \to Pr[V_{LIN}^f = 1] = 1$
- soundness: $\Delta(f, LIN[\mathbb{F}, n]) \geq \delta \to Pr[V_{LIN}^f = 1] \leq \varepsilon(\delta)$

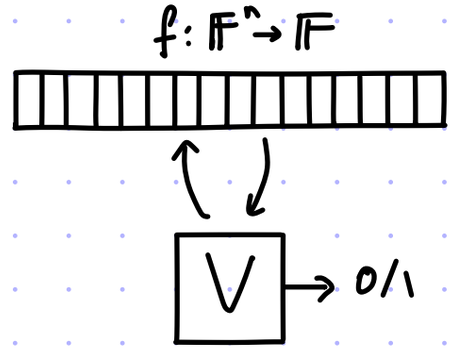


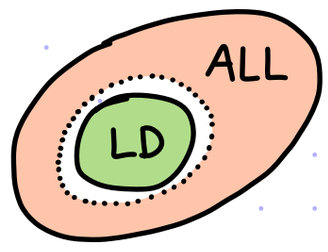


The goal of LOW-DEGREE TESTING is:

A test V_{LD} s.t. $\forall f: \mathbb{F}^n \to \mathbb{F}$

- completeness: $f \in LD[\mathbb{F}, n, d] \to Pr[V_{LD}^f = 1] = 1$
- soundness: $\Delta(f, LD[\mathbb{F}, n, d]) \geq \delta \to Pr[V_{LD}^f = 1] \leq \varepsilon(\delta)$





What does degree d mean?

- total degree (e.g. in this case $LD[\mathbb{F}, n, tot \leq 1] = AFFINE[\mathbb{F}, n]$)
- individual degree (e.g. in this case $LD[\mathbb{F}, n, ind \leq 1] =$ "multilinear polynomials")

EXERCISE: derive a test for individual degree from a test for total degree.

In most applications the difference total-vs-individual does not matter much.

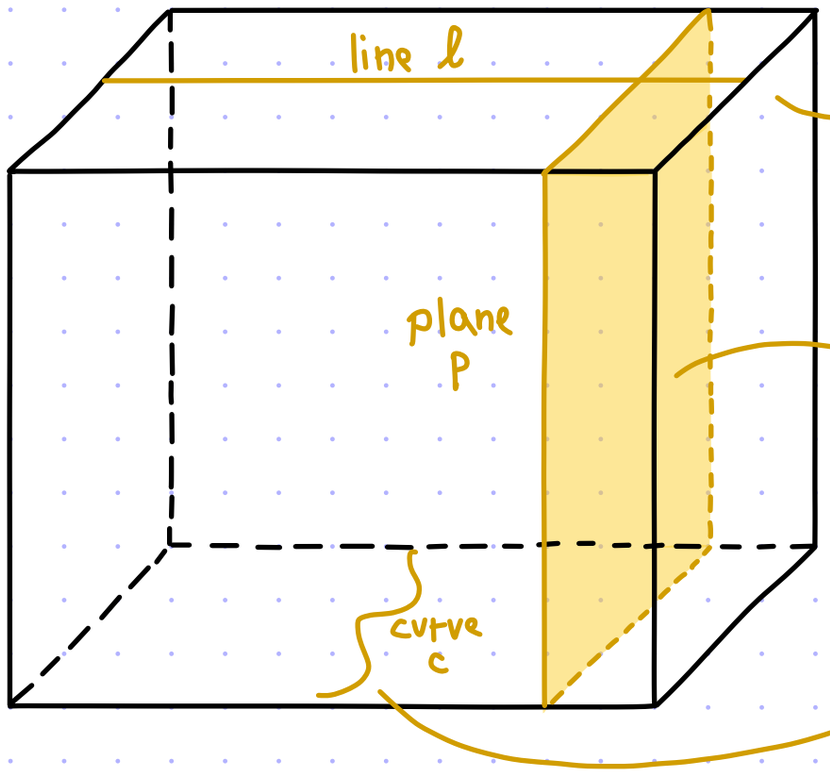
Total Low-Degree Testing

Today we study TOTAL low-degree testing:

$$LD[\mathbb{F}, n, d] = \{ f : \mathbb{F}^n \to \mathbb{F} \mid \exists\, p \in \mathbb{F}[X_1, \ldots, X_n] \text{ of TOTAL degree } \leq d \text{ s.t. } p \equiv f \}.$$

This set of functions is a linear error-correcting code with rich structure:

$f : \mathbb{F}^3 \to \mathbb{F}$



many subcodes by restrictions:

$f \circ \ell : \mathbb{F} \to \mathbb{F}$

has degree $\leq d$

$f \circ p : \mathbb{F}^2 \to \mathbb{F}$

ha total degree $\leq d$

$f \circ c : \mathbb{F} \to \mathbb{F}$

has total degree $\leq d \cdot \deg(c)$

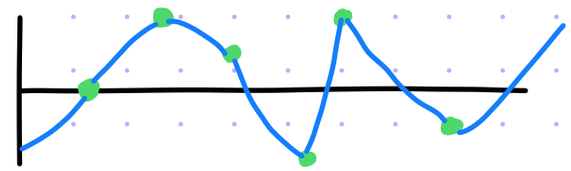
Reed-Muller code:

- message length $= \binom{n+d}{d}$ if $d < |\mathbb{F}|$
- block length $= |\mathbb{F}|^n$
- relative distance $\geq 1 - \frac{d}{|\mathbb{F}|}$

Next: ① low-degree testing for $LD[\mathbb{F}, n=1, d]$ (univariate polynomials)

② extend to $n > 1$ (multivariate polynomials)

Univariate Polynomials: a Trivial Test



Fact: any $d+1$ locations $a_0, a_1, \ldots, a_d \in \mathbb{F}$ determine a polynomial

A natural idea is to interpolate and test at a random point:

$V^{f:\mathbb{F}\to\mathbb{F}}(\mathbb{F}, d) :=$
1. Sample $r \leftarrow \mathbb{F}$
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: $\Pr[V^f = 1] = \Pr_r[\tilde{p}(r) = f(r)] \leq 1 - \Delta(f, \mathbb{F}^{\leq d}[x])$

The query complexity $O(d)$ can be much less than $|\mathbb{F}|$ (reading all of f).

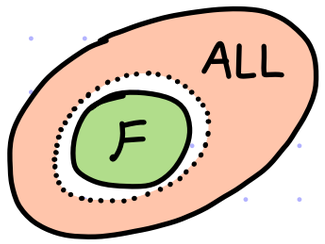
Exercise: prove that a query complexity of $\Omega(d)$ is necessary.

PROBLEM: the straightforward extension of this idea to $n>1$ yields large query complexity.

Trivial Test for Multivariate Polynomials

The "interpolate-and-test" idea is an example of a TRIVIAL TEST.

We describe a trivial test for any property $F = \{f : D \to \Sigma\}$.



A fixing set $S \subseteq D$ for F is such that, $\forall a : S \to \Sigma$, $|\{f \in F \mid f(S) = a\}| \leq 1$.

$V_S^{f:D\to\Sigma}$:
1. Sample $r \leftarrow D$.
2. Query f at S and r. ← query complexity is $|S|+1$
3. Let $\tilde{p}$ be the unique function in F s.t. $\tilde{p}(S) = f(S)$.
4. Check that $\tilde{p}(r) = f(r)$.

Completeness: if $f \in F$ then $\Pr[V_S^f = 1] = \Pr[\tilde{p}(r) = f(r)] = 1$.

Soundness: $\Pr[V_S^f = 1] = \Pr[\tilde{p}(r) = f(r)] \leq 1 - \Delta(f, F)$.

Examples of trivial tests:

F	ALL-ZERO	CONST	LIN(𝔽,n)	LD[𝔽,n=1,d]	LD[𝔽,n,tot≤d]	LD[𝔽,n,ind≤d]
$\lvert S\rvert$	0	1	n	d+1	$\binom{n+d}{d}$	$(d+1)^n$

(LIN(𝔽,n): Lecture 7; LD[𝔽,n=1,d]: prior slide)

The BLR test for LIN(𝔽,n) has 3 queries, much better than the (n+1)-query trivial test.

The (d+2)-query trivial test for LD[𝔽,n=1,d] is optimal.

The trivial tests for LD[𝔽,n,tot≤d] and LD[𝔽,n,ind≤d] have large query complexity.

Today we see a low-degree test that is much better than the trivial test.

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

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

The proof is by induction, using 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., $\frac{f(a+1)-f(a)}{(a+1)-a} - \frac{f(a+2)-f(a+1)}{(a+2)-(a+1)} = 0$.

New proposal: $V^{f:\mathbb{F}_p \to \mathbb{F}_p}(\mathbb{F}_p, d) :=$

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 $\geq \frac{1}{2} - \frac{d}{|\mathbb{F}|}$ to $\mathbb{F}^{<d}[x]$.

This test rejects with probability only $\Theta(d/|\mathbb{F}|)$.

A Refined Local Characterization

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

lemma: $\forall f:\mathbb{F}_p\to\mathbb{F}_p \quad f\in \mathbb{F}_p^{\le d}[x] \leftrightarrow \forall a\in\mathbb{F}_p \quad \sum_{i=0}^{d+1} c_i\cdot f(a+i)=0$

corollary: $\forall f:\mathbb{F}_p\to\mathbb{F}_p \quad f\in \mathbb{F}_p^{\le d}[x] \leftrightarrow \forall a,b\in\mathbb{F}_p \quad \sum_{i=0}^{d+1} c_i\cdot f(a+i\cdot b)=0$

proof:

For the direction "$\leftarrow$" set $b=1$ and invoke the lemma.

For the direction "$\rightarrow$", fix $a,b\in\mathbb{F}_p$ and consider $g(x):=f(ax+b)$.

The degree of g is at most d. Hence, by the lemma,

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

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

The local constraints increased from $|\mathbb{F}_p|=p$ to $|\mathbb{F}_p|^2=p^2$.

The choice of b randomizes the "step size" and seems to rule out the counterexample.

Univariate Polynomials: the Rubinfeld-Sudan Test

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

$V_{RS}^{f:\mathbb{F}_p\to\mathbb{F}_p}(\mathbb{F}_p, d) :=$ 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 $f \in \mathbb{F}_p^{\le d}[x]$ then $\Pr_{r,s}[V_{RS}^f = 1] = 1$ by corollary

Soundness: **theorem:** $\Pr[V_{RS}^f = 0] \ge \min\left\{\Omega\left(\frac{1}{d^2}\right), \frac{1}{2}\cdot\Delta(f, \mathbb{F}_p^{\le d}[x])\right\}$

Equivalently: $\Pr[V_{RS}^f = 1] \le \max\left\{1 - O\left(\frac{1}{d^2}\right), 1 - \frac{1}{2}\cdot\Delta(f, \mathbb{F}_p^{\le d}[x])\right\}$

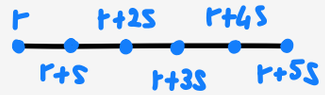
Isn't this test worse?

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

BUT: RS test extends to multivariate polynomials with no changes

Proof overview

$V_{RS}^{f:\mathbb{F}_p\to\mathbb{F}_p}$:= 1. Sample $r,s\in\mathbb{F}_p$



2. Check that $\sum_{i=0}^{d+1} c_i \cdot f(r+i\cdot s) = 0$

Similar to the case of linearity testing.

theorem: $\Pr\left[V_{RS}^f = 0\right] \geq \min\left\{\frac{1}{4\cdot(d+2)^2},\ \frac{1}{2}\cdot\Delta\left(f,\mathbb{F}_p^{\leq d}[x]\right)\right\}$.

The plurality correction is

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

- Part 1: $\Pr\left[V_{RS}^f = 0\right] \geq \frac{1}{2}\cdot\Delta(f,g_f)$ far from plurality correction → many bad lines
- Part 2: $\Pr\left[V_{RS}^f = 0\right] < \frac{1}{4\cdot(d+2)^2} \to g_f\in\mathbb{F}_p^{\leq d}[x]$ few bad lines → plurality correction is low-degree

Conclusion:

- If $\Pr\left[V_{RS}^f = 0\right] \geq \frac{1}{4\cdot(d+2)^2}$ then we are done.
- If $\Pr\left[V_{RS}^f = 0\right] < \frac{1}{4\cdot(d+2)^2}$ then (by Part 2) g_f is low-degree and (by Part 1) we get

$$\Pr\left[V_{RS}^f = 0\right] \geq \frac{1}{2}\cdot\Delta(f,g_f) \geq \frac{1}{2}\cdot\Delta\left(f,\mathbb{F}_p^{\leq d}[x]\right).$$

■

Analysis of the RS Test - Part 1

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

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

If g_f is far from f then V_{RS}^f rejects with high probability:

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

<u>proof:</u> Define $S := \left\{ r \in \mathbb{F}_p \;\middle|\; \Pr_s\left[f(r) \neq \sum_{i=1}^{d+1} c_i \cdot f(r+i \cdot s) \right] \geq \frac{1}{2} \right\}$.

For every $r \notin S$, $\Pr_s\left[f(r) = \sum_{i=1}^{d+1} c_i \cdot f(r+is) \right] > \frac{1}{2}$ (more than half of s's vote for $f(r)$)

so $f(r) = g_f(r)$.

Hence $\Delta(f, g_f) \leq \frac{|S|}{|\mathbb{F}|}$ ($\forall r$ if $f(r) \neq g_f(r)$ then $r \in S$).

$$\begin{aligned}
\text{So } \Pr\left[V_{RS}^f = 0\right] &= \Pr_r[r \in S] \cdot \Pr_{r,s}\left[V_{RS}^f = 0 \mid r \in S \right] + \Pr_r[r \notin S] \cdot \Pr_{r,s}\left[V_{RS}^f = 0 \mid r \notin S \right] \\
&\geq \frac{|S|}{|\mathbb{F}|} \cdot \min_{r \in S} \left\{ \Pr_s\left[f(r) \neq \sum_{i=1}^{d+1} c_i \cdot f(r+is) \right] \right\} + 0 \\
&\geq \frac{|S|}{|\mathbb{F}|} \cdot \frac{1}{2} \geq \Delta(f, g_f) \cdot \frac{1}{2}.
\end{aligned}$$

■

Analysis of the RS Test - Collision Lemma

few bad lines imply many votes for the plurality correction

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

proof:

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

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

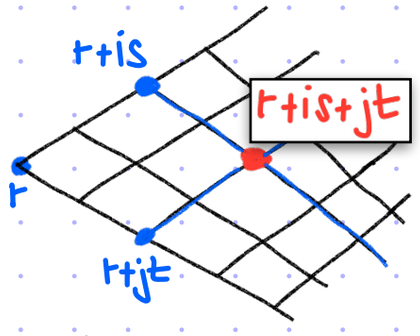
$$\geq \sum_{v\in\mathbb{F}_p} \Pr_s\left[v = \sum_{i=1}^{d+1} c_i \cdot f(r+i\cdot s)\right]^2$$

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

$$\geq 1 - 2\cdot(d+1)\cdot \Pr\left[V_{RS}^f = 0\right].$$

We now analyze the COLLISION PROBABILITY.

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



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

Hence

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

$$\leq 2(d+1)\cdot \Pr\left[V_{RS}^f = 0\right].$$

■

Analysis of the RS Test - Part 2

claim: if $\Pr\left[V_{RS}^{f}=0\right] < \frac{1}{4\cdot(d+2)^2}$ then $g_f \in \mathbb{F}_p^{\le d}[x]$

proof: Fix $r,s \in \mathbb{F}_p$. We show that $\sum_{i=0}^{d+1} c_i \cdot g_f(r+is) = 0$.

If $\exists\, t_1,t_2 \in \mathbb{F}_p$ s.t. $\begin{cases} \forall\, i \in \{0,1,\ldots,d+1\} \\ \forall\, j \in \{1,\ldots,d+1\} \end{cases}$ $\begin{array}{l} g_f(r+is) = \sum_{j=1}^{d+1} c_j \cdot f\left((r+is)+j\,(t_1+it_2)\right) \\ \sum_{i=0}^{d+1} c_i \cdot f\left((r+jt_1)+i\,(s+jt_2)\right) = 0 \end{array}$

then

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

Hence

$$\Pr_{t_1,t_2}\left[\sum_{i=0}^{d+1} c_i \cdot g_f(r+is) \neq 0\right] \overset{\text{union bound}}{\le} \Pr_{t_1,t_2}\left[\begin{array}{ll} \exists\, i \in \{0,1,\ldots,d+1\} & g_f(r+is) \neq \sum_{j=1}^{d+1} c_j \cdot f\left((r+is)+j\,(t_1+it_2)\right) \\ \text{OR} & \\ \exists\, j \in \{1,\ldots,d+1\} & \sum_{i=0}^{d+1} c_i \cdot f\left((r+jt_1)+i\,(s+jt_2)\right) \neq 0 \end{array}\right]$$

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

$$\Pr_{t_1,t_2}\left[g_f(r+is) \neq \sum_{j=1}^{d+1} c_j \cdot f\left((r+is)+j\cdot(t_1+it_2)\right)\right] \overset{\text{collision lemma}}{<} 2(d+1)\cdot\Pr\left[V_{RS}^{f}=0\right] < 2(d+1)\cdot\frac{1}{4\cdot(d+2)^2} \le \frac{1}{2\cdot(d+2)}$$

■

Extending the RS Test to Multivariate Polynomials

The local characterization holds similarly:

$$\forall\, d < p-2 \quad \forall\, f : \mathbb{F}_p^n \to \mathbb{F}_p, \quad f \in \mathbb{F}_p^{\leq d}[X_1,\dots,X_n] \iff \forall\, a,b \in \mathbb{F}_p^n \ \sum_{i=0}^{d+1} c_i \cdot f(a+i\cdot b) = 0$$

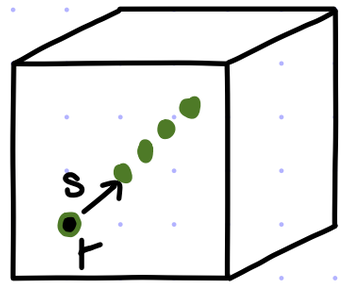
(total degree)

This directly motivates the following test:

query complexity is $d+2 = O(d)$

$V_{RS}^{f:\mathbb{F}_p^n \to \mathbb{F}_p}(\mathbb{F}_p, n, d) :=$

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



read $d+2$ locations on a random line

The theorem for soundness is also similar:

theorem: $\Pr\left[V_{RS}^{f} = 0\right] \geq \min\left\{\frac{1}{4\cdot(d+2)^2}, \frac{1}{2}\cdot\Delta\left(f, \mathbb{F}_p^{\leq d}[X_1,\dots,X_n]\right)\right\}$

The proof is the same up to syntactic modifications.

By repeating the test $O(d^2)$ times, we get:

a total low-degree test with query complexity $O(d^3)$ [independent of n]

where "constant relative distance" → "constant soundness error".

More on Total Low-Degree Testing [1/2]

A key structure that enables low-degree testing is a ROBUST LINES CHARACTERIZATION.

Suppose that $f:\mathbb{F}^n \to \mathbb{F}$ has total degree $\leq d$.

Then, $\forall a,b \in \mathbb{F}^n$, the univariate function $g_{a,b}(z) := f(a+z\cdot b)$ has degree $\leq d$.

Does the converse hold?

COUNTEREXAMPLE: Set $\mathbb{F} := \mathbb{F}_{p^e}$ and fix any d with $p^e - p^{e-1} - 1 < d < p^e$.

Consider the bivariate function $f(x_1,x_2) := (x_1^{p-1} x_2)^{p^{e-1}}$.

The total degree of f is $q > d$. Yet $\forall a,b$ $g_{a,b}(z) = f(a_1+zb_1, a_2+zb_2) = ((a_1+zb_1)^{p-1}(a_2+zb_2))^{p^{e-1}}$ has degree at most $(p-1)p^{e-1} = p^e - p^{e-1}$. (Indeed recall that $z^{p^e} \equiv z$ since p^e is the field size.)

The converse holds if $d \leq p^e - p^{e-1} - 1$. (E.g. if $\mathbb{F}$ has prime size p then the condition is $d \leq p-2$.) [Friedl, Sudan 1995] for a proof.

In this case, if $\{g_{a,b}(z) := f(a+zb)\}_{a,b\in\mathbb{F}^n}$ all have degree $\leq d$ then f has total degree $\leq d$.

Low-degree testing is based on distance variants of such results:

if $\{g_{a,b}(z) := f(a+zb)\}_{a,b\in\mathbb{F}^n}$ are close to degree $\leq d$ in expectation

then f is close to total degree $\leq d$

More on Total Low-Degree Testing [2/2]

These statements motivate the random-line test.

$V^{f:\mathbb{F}^n\to\mathbb{F}}$:=
1. Sample $r,s \leftarrow \mathbb{F}^n$.
2. Query f at the line $\ell_{r,s}(z) := r + z \cdot s$.
3. Check that $\deg(f \circ \ell_{r,s}) \leq d$.

query complexity is $|\mathbb{F}|$

theorem: $\exists\, \alpha \in (0,1]\ \forall\, \mathbb{F}\ \forall\, f:\mathbb{F}^n\to\mathbb{F} \quad \Pr[V^f = 0] \geq \Delta(f, LD[\mathbb{F},n,tot\leq d]) - \left(\frac{d}{|\mathbb{F}|}\right)^{\alpha}$

For every line ℓ, $p_\ell : \mathbb{F}\to\mathbb{F}$

Analyses focus on proving statements

A few words about low-degree testing

Low-degree testing for quantum states, and a quantum entangled games PCP for QMA

Anand Natarajan* Thomas Vidick†

Abstract

We show that given an explicit description of a multiplayer game, with a classical verifier and a constant number of players, it is QMA-hard, under randomized reductions, to distinguish between the cases when the players have a strategy using entanglement that succeeds with probability 1 in the game, or when no such strategy succeeds with probability larger than $\frac{1}{2}$. This proves the "games quantum PCP conjecture" of Fitzsimons and the second author (ITCS'15), albeit under randomized reductions.

The core component in our reduction is a construction of a family of two-player games for testing n-qubit maximally entangled states. For any integer $n \geq 2$, we give such a game in which questions from the verifier are $O(\log n)$ bits long, and answers are $\mathrm{poly}(\log \log n)$ bits long. We show that for any constant $\varepsilon \geq 0$, any strategy that succeeds with probability at least $1 - \varepsilon$ in the test must use a state that is within distance $\delta(\varepsilon) = O(\varepsilon^c)$ from a state that is locally equivalent to a maximally entangled state on n qubits, for some universal constant $c > 0$. The construction is based on the classical plane-vs-point test for multivariate low-degree polynomials of Raz and Safra (STOC'97). We extend the classical test to the quantum regime by executing independent copies of the test in the generalized Pauli X and Z bases

Low-degree tests at large distances

Alex Samorodnitsky*

September 27, 2018

Abstract

We define tests of boolean functions which distinguish between linear (or quadratic) ...te sense, from these poly- ...etween soundness and the ...ormity norms behave "ran- ...f of an inverse theorem for

Testing Low-Degree Polynomials over $GF(2)$

Noga Alon * Tali Kaufman † Michael Krivelevich ‡ Simon Litsyn § Dana Ron¶

July 9, 2003

Abstract

We describe an efficient randomized algorithm to test if a given *binary* function $f : \{0,1\}^n \to \{0,1\}$ is a low-degree polynomial (that is, a sum of low-degree monomials). For a given integer $k \geq 1$ and a given real $\epsilon > 0$, the algorithm queries f at $O(\frac{1}{\epsilon} + k4^k)$ points. If f is a polynomial of degree at most k, the algorithm always accepts, and if the value of f has to be modified on at least an ϵ fraction of all inputs in order to transform it to such a polynomial, then the algorithm rejects with probability at least 2/3. Our result is essentially tight: Any algorithm for testing degree-k polynomials over $GF(2)$ must perform $\Omega(\frac{1}{\epsilon} + 2^k)$ queries.

Improved low-degree testing and its applications

Sanjeev Arora* Princeton University Madhu Sudan† IBM T. J. Watson Research Center

Abstract

NP = PCP(log n, 1) and related results crucially depend upon the close connection between the probability with which a function passes a *low degree test* and the distance of this function to the nearest degree d polynomial. In this paper we study a test proposed by Rubinfeld and Sudan [29]. The strongest previously known connection for this test states that a function passes the test with probability δ for some $\delta > 7/8$ iff the function has agreement $\approx \delta$ with a

1 Introduction

The use of algebraic techniques has ... (probabilistic) characterizations of ... classes. These characterizations involve ... tween an untrustworthy prover (or ... polynomial-time verifier. In MIP= NP = PCP(log n, 1) [6, 5] the verifier ... cally verify the satisfiability of a boolean ... ing very few bits in a "proof string" ... In IP=PSPACE [24, 31] the verifier ...

A Sub-Constant Error-Probability Low-Degree Test, and a Sub-Constant Error-Probability PCP Characterization of NP *

Ran Raz † Shmuel Safra ‡

Abstract

We introduce a new low-degree–test, one that uses the restriction of low-degree polynomials to planes (i.e., affine sub-spaces of dimension 2), rather than the restriction to lines (i.e., affine sub-spaces of dimension 1). We prove the new test to be of a very small error-probability (in particular, much smaller than constant).

The new test enables us to prove a low-error characterization of NP in terms of PCP. Specifically, our theorem states that, for any given $\epsilon > 0$, membership in any NP language can be verified with $O(1)$ accesses,

of the most fundamental avenues of research in theory of computer-science.

Since the early days, when the classes P and NP were defined, and the question was posed as to whether they are the same or do they differ, many problems were shown to be NP-complete, thereby increasing the weight on finding stricter characterization for the class NP.

NP has since been given a few alternative characterizations. The one most commonly applied being Cook's [Coo71], which characterizes NP in terms of efficient verification of proofs (or nondeterministic computations).

Bibliography

Individual degree testing

- [BFL 1991]: Non-deterministic exponential time has two-prover interactive protocols, by László Babai, Lance Fortnow, Carsten Lund.
- [BFLS 1991]: Checking computations in polylogarithmic time, by László Babai, Lance Fortnow, Leonid Levin, Mario Szegedy.

Total degree testing

- [AS 1992]: Probabilistic checking of proofs; a new characterization of NP, by Sanjeev Arora, Madhu Sudan.
- [RS 1996]: Robust characterizations of polynomials with applications to program testing, by Ronitt Rubinfeld, Madhu Sudan.
- [Sudan 1992]: Efficient checking of polynomials and proofs and the hardness of approximation problems, by Madhu Sudan.
- [AS 1997]: Improved low-degree testing and its applications, by Sanjeev Arora, Madhu Sudan.
- [RS 1997]: A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP, by Ran Raz, Shmuel Safra.
- [FS 2013]: Some improvements to total degree tests, by Katalin Friedl, Madhu Sudan.
- [HKSS 2023]: An improved line-point low-degree test, by Prahladh Harsha, Mrinal Kumar, Ramprasad Saptharishi, Madhu Sudan.
- (▸On low-degree polynomials), (▸The power of algebra) by Madhu Sudan.

Boolean low-degree testing

- [AKKLR 2003]: Testing low-degree polynomials over GF(2), by Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, Dana Ron.
- [Samorodnitsky 2006]: Low-degree tests at large distances, by Alex Samorodnitsky.