Lecture B.3

Low-Degree Testing

(Locality of the Reed-Muller code)

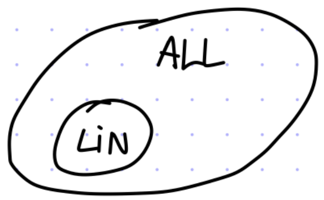
Tom Gur

Summer Graduate School on
Foundations and Frontiers of Probabilistic Proofs
July 28, 2021

Recap

Linearity Testing

A function $f: \mathbb{F}^n \to \mathbb{F}$ is linear if $\exists c \in \mathbb{F}^n$ s.t. $f(x) = \sum_{i=1}^{n} c_i x_i$.
Equivalently, if $\forall x, y \in \mathbb{F}^n$ $f(x) + f(y) = f(x+y)$.



$ALL = \{ f: \mathbb{F}^n \to$

$LIN = \{ f: \mathbb{F}^n \to$

We want a $O(1)$-query test that, give

But this is impossible: if f differs

but we can

So we relax the question: given

say YES if $f \in LIN$ and NO if

We count in Hamming distance:

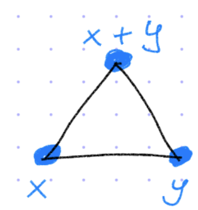
$\Delta(f,g) := \Pr_{x \in \mathbb{F}^n}[f(x) \neq g(x)]$ and

Q1: can we solve the relaxed problem?

Proof overview

$V_{BLR}^{f:\mathbb{F}^n \to \mathbb{F}} :=$ 1. sample $x, y \in \mathbb{F}^n$
2. check that $f(x) + f(y) = f(x+y)$

theorem: $\Pr[V_{BLR}^f = 0] \geq \min\{1/6, \frac{1}{2} \cdot \Delta(f, LIN)\}$



$g_f: \mathbb{F}^n \to \mathbb{F}$ is defined as $g_f(x) := \underbrace{\arg\max_{v \in \mathbb{F}} \left| \{ y \in \mathbb{F}^n \mid v = f(x+y) - f(y) \} \right|}_{\text{this is the plurality value}}$

Step 1: ※Bad-triangle is captured by distance from plurality vote

$$\Pr[V_{BLR}^f = 0] \geq \frac{1}{2} \cdot \Delta(g_f, f)$$

Step 2: plurality implies overwhelming majority

$$\Pr_{y \in \mathbb{F}^n}[g_f(x) = f(x+y) - f(y)] \geq 1 - 2 \cdot \Pr[V_{BLR}^f = 0] \geq \frac{2}{3}$$

Step 3: plurality vote (g_f) is a linear function

$$\text{if } \Pr[V_{BLR}^f = 0] < \tfrac{1}{6} \text{ then } \forall x, y \;\; g_f(x) + g_f(y) = g_f(x+y)$$

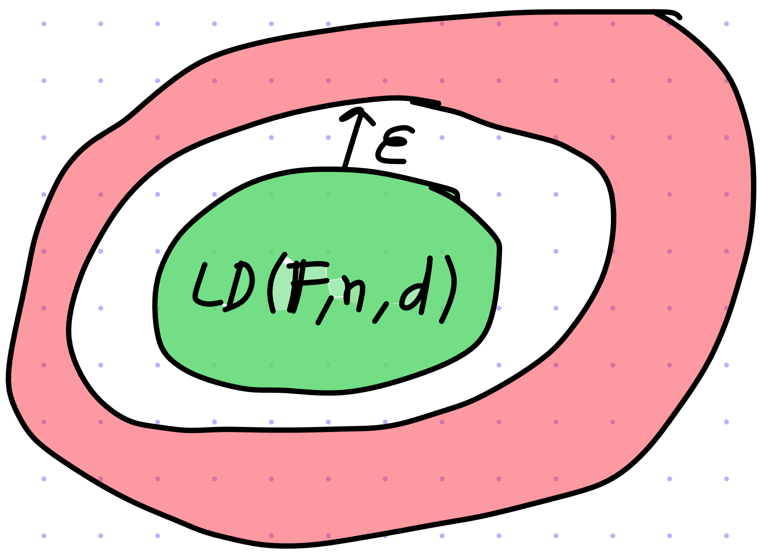
Low-Degree Testing

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. $\frac{1}{2}$ 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. $\frac{1}{2}$ if f is $\frac{1}{10}$-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.

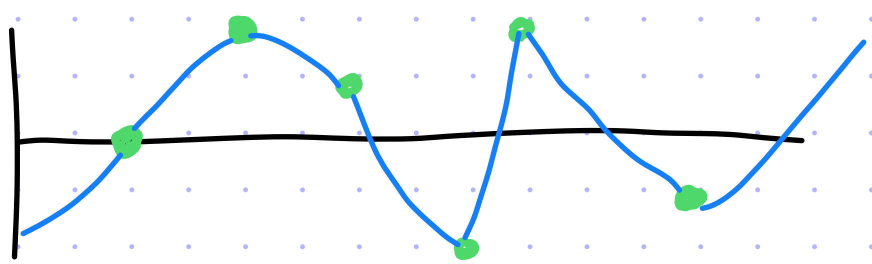
Either way in most applications to PCPs the difference does not matter.

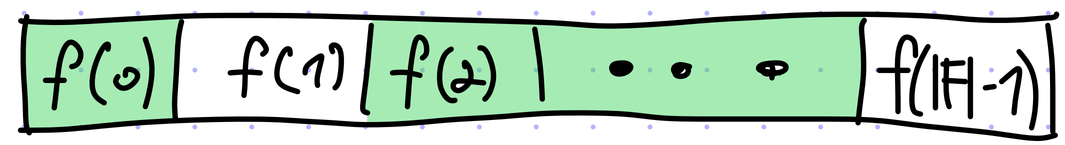
Today we study total degree:

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

Interlude: the magic of polynomials

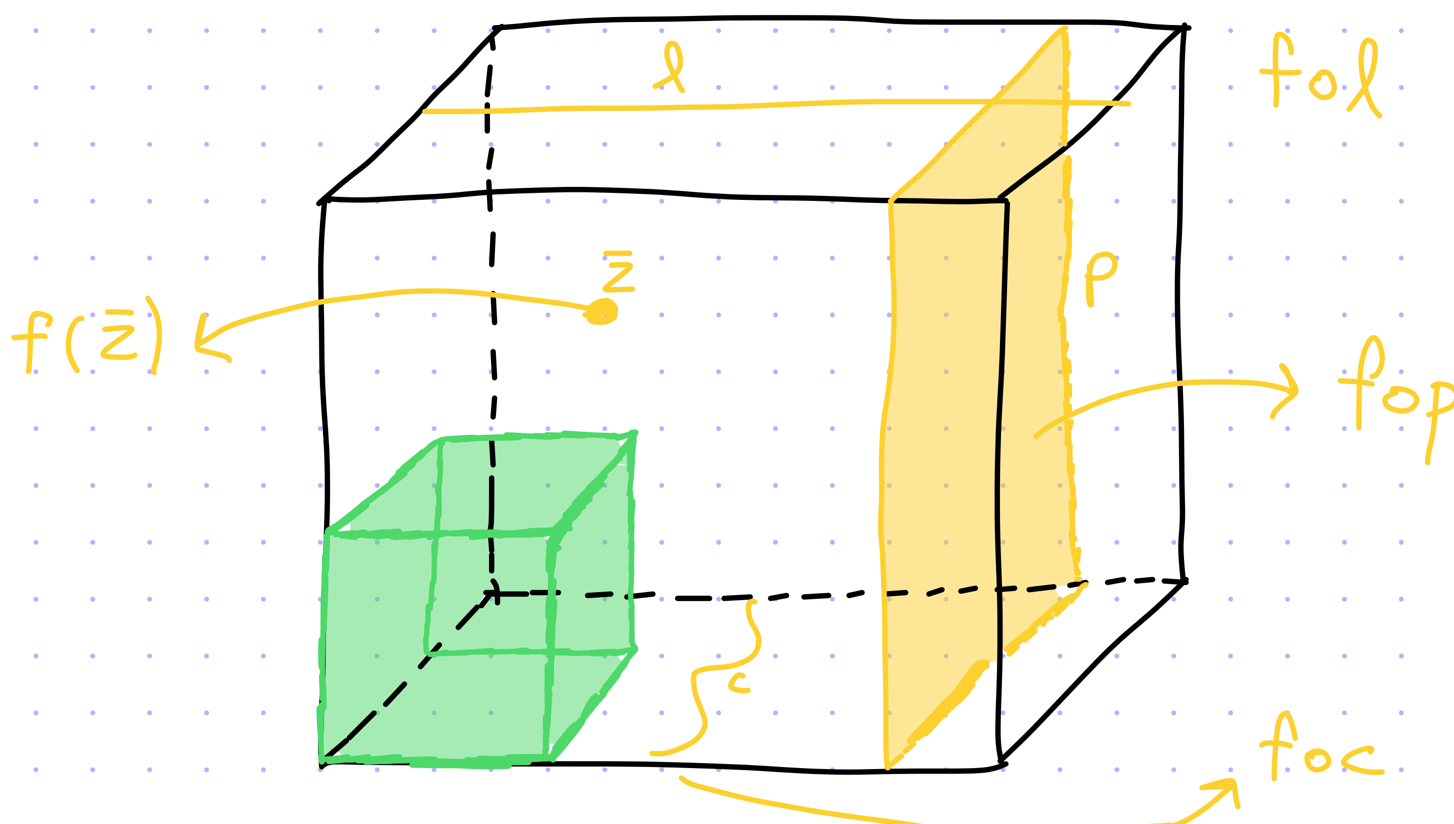
Univariate polynomials of degree d extend the values of $d+1$ points to a field $\mathbb{F}$.





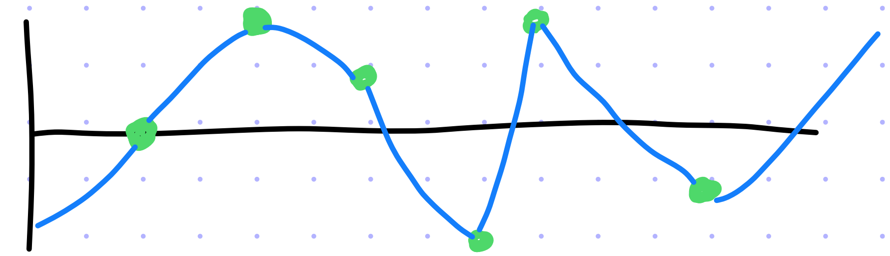
consider a polynomial $f:\mathbb{F}^n \to \mathbb{F}$ s.t. $\deg(f)=d$.

all affine subspaces are codes!



lines
planes
hyperplanes
curves
manifolds

Univariate Polynomials: a Basic Test

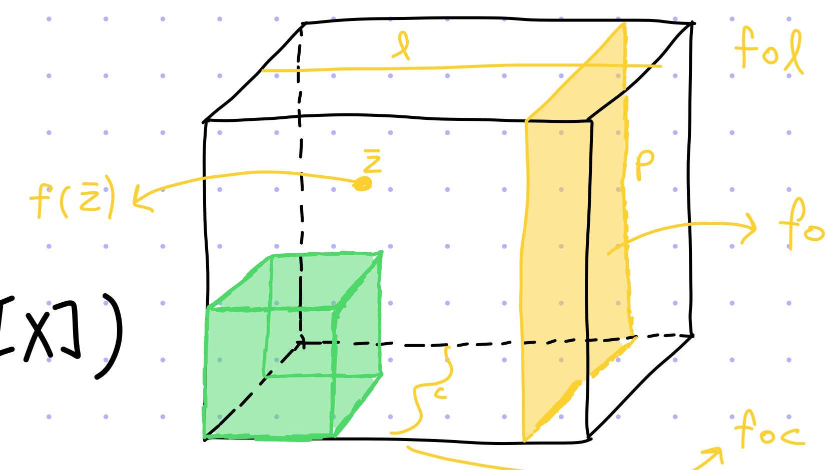


Idea: any $d+1$ locations determine a polynomial

$T^{f:\mathbb{F}\to\mathbb{F}}(\mathbb{F},d) :=$ 1. sample $r \in \mathbb{F}$
2. query f at $a_0, a_1, \dots, a_d, r$
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 $i = 0, 1, \dots, d+1$ $\quad c_i := (-1)^{i+1}\binom{d+1}{i} \in \mathbb{F}_p$.

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

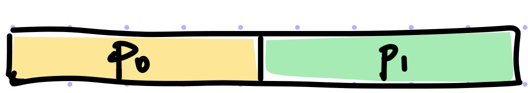
<u>proof</u>: Induction and formal derivatives. Ex for $d=0$: $(c_0, c_1) = (-1, 1) \to -f(a) + f(a+1) = 0$.

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., $\frac{f(a+1) - f(a)}{(a+1) - a} = \frac{f(a+2) - f(a+1)}{(a+2) - (a+1)}$.

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 $r, r+1, \dots, r+(d+1)$
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 $\approx d/(|\mathbb{F}|/2)$.

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

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

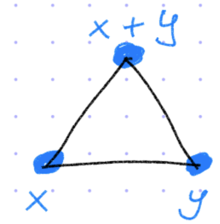
Recall the linear testing analysis

Proof overview

$V_{BLR}^{f:\mathbb{F}^n\to\mathbb{F}} :=$ 1. sample $x,y \in \mathbb{F}^n$
2. check that $f(x)+f(y)=f(x+y)$

<u>theorem:</u> $\Pr\left[V_{BLR}^{f}=0\right] \geq \min\left\{ 1/6 , \frac{1}{2}\cdot\Delta(f,\mathrm{LIN})\right\}$

$g_f:\mathbb{F}^n \to \mathbb{F}$ is defined as $g_f(x) := \underbrace{\arg\max_{v\in\mathbb{F}} \left|\left\{ y\in\mathbb{F}^n \mid v=f(x+y)-f(y)\right\}\right|}_{\text{this is the plurality value}}$



Step 1: ※Bad-triangle is captured by distance from plurality vote

$$\Pr\left[V_{BLR}^{f}=0\right] \geq \frac{1}{2}\cdot\Delta(g_f,f)$$

Step 2: plurality implies overwhelming majority

$$\Pr_{y\leftarrow\mathbb{F}^n}\left[g_f(x)=f(x+y)-f(y)\right] \geq 1-2\cdot\Pr\left[V_{BLR}^{f}=0\right] \geq \frac{2}{3}$$

Step 3: plurality vote (g_f) is a linear function

$$\text{if } \Pr\left[V_{BLR}^{f}=0\right]<\frac{1}{6} \text{ then } \forall x,y \;\; g_f(x)+g_f(y)=g_f(x+y)$$

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

If g_f is far from f then 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 $S = \{ r \in \mathbb{F}_p \text{ s.t. } \Pr_s[f(r) \neq \sum_{i=1}^{d+1} c_i \cdot f(r+is)] \geq \frac{1}{2} \}$, we get

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

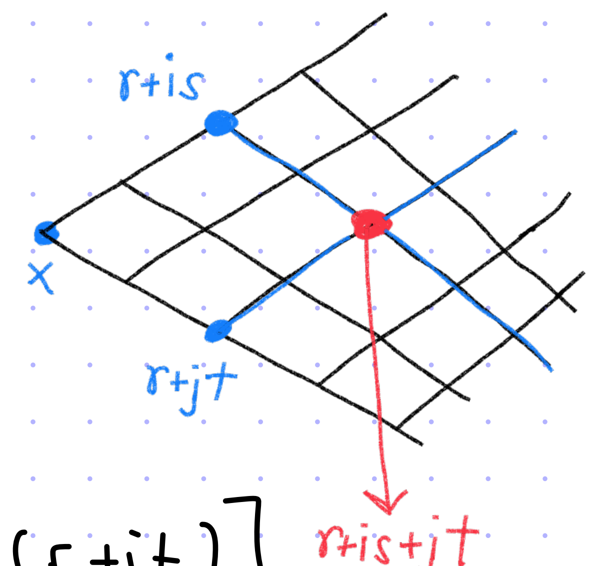
$$\geq \frac{|S|}{|\mathbb{F}|} \cdot \min_{r \in S} \left\{ \Pr_s \left[f(r) \neq \sum_{i=1}^{d+1} c_i \cdot f(r+is) \right] \right\} + 0 \geq \frac{|S|}{|\mathbb{F}|} \cdot \frac{1}{2}.$$

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

Analysis of the RS Test - Part 2

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

<u>proof:</u>



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

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

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

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

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

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

Let $g_f(x) := \arg\max_{v\in\mathbb{F}} \left|\left\{s\in\mathbb{F} \mid v = \sum_{i=1}^{d+1} c_i \cdot f(x+is)\right\}\right|$ 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 $\Pr[T^f=0] \geq \frac{1}{2}\Delta(g_f, f) = \frac{1}{2}\cdot\Delta(f, \mathbb{F}_p^{\leq d}[x])$.

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

proof: 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:

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

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

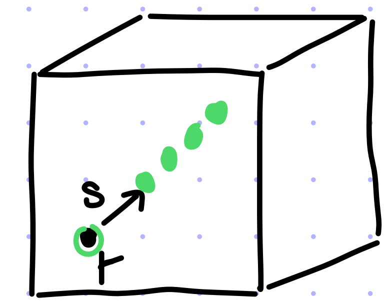
Extending the RS Test to Multivariate Polynomials

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 $d+2=O(d)$

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



random-line test

The theorem for soundness is also similar:

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

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.

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 application[s]

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 ha...
(probabilistic) characterizations of t...
classes. These characterizations invo...
tween an untrustworthy prover (or ...
polynomial-time verifier. In MIP= ...
NP = PCP($\log n$, 1) [6, 5] the verifi...
cally verify the satisfiability of a boo...
ing very few bits in a "proof string" ...
In IP=PSPACE [24, 31] the verifier h...

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).