Somewhat incorrect recap of last two lectures

Every $f : \mathbb{F}_2^n \to \mathbb{F}_2$ expressible as polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]$ of degree n

$$\mathcal{P}_d = \{ f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid \deg(f) \leq d \}$$

LOW-DEGREE TESTING

Will soon switch to δ

Input: Table of $f : \mathbb{F}_2^n \to \mathbb{F}_2$
Parameters $d \in \mathbb{N}^+$, $\varepsilon \in \mathbb{R}^+$

Task: Query f in $O_n(1)$ positions and
(1) If $f \in \mathcal{P}_d$, always output "yes"/accept
(b) If $\delta(f, \mathcal{P}_d) \geq \varepsilon$, output "no"/reject with probability $\geq 2/3$

Recall $\delta(f,g) = \Pr_{x \sim \mathbb{F}_2^n} [f(x) \neq g(x)]$

$$\delta(f, \mathcal{G}) = \min_{g \in \mathcal{G}} \{ \delta(f,g) \}$$

But wait... Didn't we test low-degree polynomials with constant term 0?

$$\mathcal{P}_d^* = \mathcal{P}_d \cap \{ f : \mathbb{F}_2^n \to \mathbb{F}_2 \mid f(0) = 0 \}$$

Yes, but this difference doesn't matter much

Exercise Go over AKKLR proof and verify this

Idea behind AKKLR-tester

Repeat the following basic test a sufficient # times
- Pick a random affine subspace A of dimension exactly $d+1$
- Check if $f \upharpoonright A$ is a degree-d polynomial

Affine subspace of dimension ℓ

Pick full-rank matrix $M \in \mathbb{F}_2^{n \times \ell}$

Pick $b \in \mathbb{F}_2^n$

Then $A = \{ Mx + b \mid x \in \mathbb{F}_2^\ell \}$ is an affine subspace of dimension ℓ

But wait... Our subspace wasn't affine?
Well, no, but now we are testing general polynomials with any constant term.

More importantly: Was our subspace of degree exactly $d+1$. Actually, no. So let us be a bit more precise

Test $T_{d,\ell}$

Pick uniformly at random full-rank $M \in \mathbb{F}_2^{n \times \ell}$, $b \in \mathbb{F}_2^n$

Check if $f \upharpoonright A$ degree-d poly; if so accept, else reject

where $A = \{ Mx + b \mid x \in \mathbb{F}_2^\ell \}$

Test $T_{d, \leq \ell}$

Pick uniformly at random $M \in \mathbb{F}_2^{n \times \ell}$, $b \in \mathbb{F}_2^n$

Let $A = \{ Mx + b \mid x \in \mathbb{F}_2^\ell \}$

Accept iff $f \upharpoonright A$ degree-d poly

The basic AKKLR-test that we looked at last time was (almost) $T_{d,\le \ell}$

In the final two lectures, we will instead analyze $T_{d,\ell}$.

Essentially no difference, since random subspace is likely to be of full dimension

LEMMA 1 Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ for $n \ge d+1$.
Then

$$\Pr[T_{d,d+1} \text{ rejects } f] \ge \Pr[T_{d,\le d+1} \text{ rejects } f]$$
$$\ge \frac{1}{4} \Pr[T_{d,d+1} \text{ rejects } f].$$

Proof Exercise.

So there really is not much of a difference, and from now on we'll focus on (affine) subspaces of maximal dimension.

The heart of the AKKLR proof is to analyze rejection probability η of $T_{d,d+1}$, and then simply repeat basic test $O(1/\eta)$ times to make sure rejection probability is $\ge 2/3$

Outline of AKKLR proof

(1) Define "self-corrected" version g of f by letting subspaces containing $\vec{y}$ vote by majority what $g(\vec{y})$ should be given f evaluated on rest of subspace

(2) Show that f and g are close (easy).

(3) Show that if detection probability is small enough, then g degree-d polynomial (harder).

Main result in [AKKLR05]:

If $\delta(f, \mathcal{P}_d) \geq \delta$, then

$$\Pr[T_{d,d-1} \text{ rejects } f] = \Omega\left(\min\left\{\delta \cdot 2^d, \frac{1}{d \cdot 2^d}\right\}\right)$$

Leads to tester with query cplx $\Theta\left(\frac{1}{\delta} + d \cdot 2^{2d}\right)$ for degree d and distance parameter δ.

[AKKLR05] also shows that

$\Omega\left(\frac{1}{\delta} + 2^d\right)$ queries necessary for any tester (even with two-sided error).

Slightly more that quadratic gap here:

- $\approx 2^d$ queries necessary
- AKKLR does $\approx d \cdot 2^{2d}$ queries

Which bound is right?

THEOREM 2 [Bhattacharyya, Kopparty, Schoenebeck,
(MAIN) Sudan, Zuckerman 2010]

There exists a constant $\varepsilon_1 > 0$ such that for all $d, n \in \mathbb{N}^+$ and all functions $f: \mathbb{F}_2^n \to \mathbb{F}_2$ it holds that

$$\Pr\left[T_{d,d+1} \text{ rejects } f \right] \geq \min\{2^d \cdot \delta(f, P_d), \varepsilon_1\}$$

COROLLARY 3

Low-degree testing of degree-d polynomials can be done with $O(2^d + 1/\delta)$ queries

Proof

It is sufficient to repeat $T_{d,d+1}$ for

$$O(\ 1/ \min\{2^d \cdot \delta(f, P_d), \varepsilon_1\})$$

$$= O\left(1 + \frac{1}{2^d \cdot \delta}\right) \text{ times } [\text{for } \delta = \delta(f, P_d)]$$

queries per test $= 2^{d+1}$

Hence total query cplx is $O(2^d + 1/\delta)$ $\square$

So we can run (essentially) the AKKLR-tester significantly fewer times, and by the new analysis still be sure that the tester rejects with high enough probability.

Furthermore, this new analysis is right (hence the title "Optimal testing of Reed-Muller codes")

Last two lectures on the course dedicated to proving Theorem 2. Interestingly, very different analysis from [AKKLR05]

But first a detour, to present another context in which low-degree testing is important

GOWERS NORMS

An arithmetic progression of length k is a sequence $b, b+d, b+2d, \ldots, b+(k-1)d$ for $b, d, k \in \mathbb{Z}$, $(k>0)$.

Suppose that $A \subseteq \mathbb{N}$ has positive density, i.e.

$$\liminf_{n\to\infty} \frac{|\{s \in A \mid s \le n\}|}{n} > 0$$

Does such a set A have to contain arithmetic progressions of arbitrarily large length k?
Important question in ADDITIVE COMBINATORICS

$k = 1$ or 2: Trivial
$k = 3$: Yes, Roth '53
Arbitrary k: Yes! Szemerédi '75
Further improvements by Gowers.
Important tool: Uniformity ~~norms~~
(now called Gowers norms, except by Gowers)

For $f: \mathbb{F}^n \to \mathbb{F}$ and $y \in \mathbb{F}^n$
the DIRECTIONAL DERIVATIVE of f in direction y
is

$$f_y(x) = f(x+y) - f(x)$$

Can take iterated derivatives for $y_1, \ldots, y_k \in \mathbb{F}^n$
by defining

$$f_{y_1, \ldots, y_{k-1}, y_k} = (f_{y_1, \ldots, y_{k-1}})_{y_k}$$

(Order does not matter)

If f has degree d, then $f_y(x)$ has
degree at most $d-1$. Hence $(d+1)$-fold
derivative is 0.

The AKKLR-test (in the general, affine case)
is to set $k = d+1$, pick a point x and
k directions $y_1, \ldots, y_k$ at random, evaluate
$f_{y_1, \ldots, y_k}(x)$ and accept if this is 0

The kth Gowers norm of $f: \mathbb{F}_2^n \to \mathbb{F}_2$ is

$$\|f\|_{U^k} = \mathop{E}_{x, y_1, \ldots, y_k}\left[(-1)^{f_{y_1, \ldots, y_k}(x)}\right]^{1/2^k}$$

$$= \left(\Pr\left[T_{d, \leq d+1} \text{ accepts } f\right] - \Pr\left[T_{d, \leq d+1} \text{ rejects } f\right]\right)^{1/2^k}$$

Gowers showed that correlation of f to closest degree-d polynomial is at most $\|f\|_{U^{d+1}}$

<u>Inverse Conjecture for the Gowers norm</u>

If $\|f\|_{U^{d+1}} = \Omega(1)$ (i.e., is bounded away from zero), then the correlation between f and some degree-d polynomial is $\Omega(1)$.

True for linear functions ($d=1$) by analysis of BLR-test

Also for quadratic functions ($d=2$)

But FALSE for $d=3$ over $\mathbb{F}_2$! [Lovett, Meshulam, Samorodnitsky '08] [Green & Tao '09]

Modified versions of the conjecture have been proven in higher characteristics.

Gowers norms have turned out to be very useful. [Green and Tao '09] used them to show that the primes contain arbitrarily long arithmetic progressions

Also used in TCS for hardness of approximation (e.g., [Samorodnitsky & Trevisan '06]) and to construct pseudorandom generators that generate what looks like true randomness to low-degree polynomials over $\mathbb{F}_2$ [Bogdanov & Viola '07]

Gowers norm often used in "1% setting": correlation of function f to low-degree polynomial is non-negligible, but small

Can also look at "99% setting": correlation of f to low-degree poly is close to 1

This is the setting analyzed in [AKKLR05] and also in [BKSSZ10].

Latter paper gives optimal analysis of test $T_{d, \leq d+1}$ and tight connection in 99% setting

Theorem 2 says that functions accepted by $T_{d, \leq d+1}$ with (high) constant probability are (highly) correlated with degree-d polynomials.

What more could we ask for? Perhaps that

$$\Pr[\text{acceptance}] \geq 1/2 + \text{small constant} \Rightarrow \text{some kind of nontrivial correlation with degree-}d\text{ poly}$$

But this is ruled out by counterexamples to inverse conjecture for Gowers norm given in [LMS08], [GT09]

We won't talk more about Gowers norms, but let us just state the connection established in [BKSSZ10]

<u>THEOREM 4</u> There exists $\varepsilon > 0$ such that if $\|f\|_{U^{d+1}} \geq 1 - \varepsilon/2^d$, then

$$\delta(f, P_d) = \Theta(1 - \|f\|_{U^{d+1}})$$

So Gowers norm and distance are tightly related in "99% setting".

But now let's get back to proof of our main theorem.

Proceeds by induction over dimension n.
Suppose f δ-far from every degree-d poly

We can implement test $T_{d,d+1}$ in following way:

(1) Pick random hyperplane (i.e., $(n-1)$-dimensional affine subspace $A \subseteq \mathbb{F}_2^n$)

(2) Pick random affine subspace $A' \subseteq A$ of dimension $d+1$ and test if $f\restriction_{A'}$ is degree-d poly

Suppose that on (almost) all hyperplanes A $f\restriction_A$ is δ-far from P_d. Then by induction tester will reject with sufficiently high probability and we are done.

Suppose, however, that there are several ($O(2^d)$) hyperplanes A such that $f \upharpoonright_A$ is close to some polynomial P_A. Then we will "sew" the different P_A, each defined on some $(n-1)$-dimensional subspace, into degree-d polynomial P that agrees with <u>all</u> of these P_A's. Then we will show that P is close to f (which was not supposed to be the case).

<u>Compare to AKKLR:</u>

(1) Self-correct f to get g.
(2) Argue that f & g close (easy)
(3) Argue that g polynomial (harder)

<u>Instead what BKSSZ does is:</u>

(1) Look at hyperplanes A on which f agrees locally with polynomials P_A
(2) Sew P_A together to global polynomial P (degree d by construction)
(3) Argue that f and P are close (harder).

<u>PLAN FOR THE REST OF TODAY</u>

- Provide some formal definitions
- Give even more detailed proof overview
- State formal lemmas
- Prove main theorem given lemmas.

Recall: Affine subspace of dimension k

$$A = \{ Mx + b \mid x \in \mathbb{F}_2^k \}$$

$M \in \mathbb{F}_2^{n \times k}$ full-rank, $b \in \mathbb{F}_2^k$

(linear subspace if $b = 0$).

Will refer to affine subspace of dimension k as a k-FLAT

A HYPERPLANE is an $(n-1)$-flat.

We will study a slightly generalized version of the basic test that ~~might~~ looks at a larger subspace

DEFINITION 5 (k-FLAT TEST $T_{d,k}$)
The test $T_{d,k}$ picks a random k-flat $A \subseteq \mathbb{F}_2^n$ and accepts iff $f\restriction_A$ is a polynomial of degree d.

We write $Rej_{d,k}(f)$ to denote the rejection probability of this test (which is = probability that $f\restriction_A$ is not a degree-d poly on a uniformly randomly chosen k-flat A).

Though it won't be needed, we can note that $T_{d,d+1}$ accepts f if for the chosen $(d+1)$-flat A it holds that

$$\sum_{y \in A} f(y) = 0$$

The following proposition is (essentially) Lemma 2 in our lecture notes for [AKKLR05]

PROPOSITION 6

For every $k \geq d+1$ it holds that $Rej_{d,k}(f) = 0$ iff $f \in \mathcal{P}_d$.

The analysis of the k-flat test goes as follows.

(A) If f is really close to $\mathcal{P}_d$ but not in $\mathcal{P}_d$, then $Rej_{d,k}(f) \gtrsim \delta(f, \mathcal{P}_d)$ for any k (and we're in good shape).
The idea here is that with good probability the flat will contain exactly one point where f and closest $P \in \mathcal{P}_d$ differ, and so f will be rejected

(B) If $k \gtrsim d + 10$, then $T_{d,k}$ rejects f with constant probability if $\delta(f, \mathcal{P}_d) = \Omega(2^{-d})$
In some sense, the tester is good enough to provide us some slack here

(C) The tester $T_{d,k-1}$ can't be much worse than $T_{d,k}$ for $k \geq d+2$, and using the slack from (B) this can take us down from dimension $d+10$ to $d+1$.

The crucial part of the argument is B
Recall that we want to show that $\delta(f, P_d)$ and $Rej_{d,k}(f)$ are closely related.

Let A be a hyperplane.
Our inductive hypothesis will say that $\delta(f\restriction_A, P_d)$ and $Rej_{d,k}(f\restriction_A)$ are closely related for each A.

Easy to see that $Rej_{d,k}(f)$ is average of $Rej_{d,k}(f\restriction_A)$ over all hyperplanes A.

We need to prove similar relationship between $\delta(f, P_d)$ and $\delta(f\restriction_A, P_d)$ as A ranges over all hyperplanes.

The idea (again) is that if $\delta(f\restriction_A, P_d)$ is too small for sufficiently many hyperplanes A (ca 2^k), then the local polynomials P_A to which $f\restriction_A$ is close can be merged into polynomial $P \in P_d$ that is (too) close to f.
Crucially, the degree doesn't increase when we compose the P_A's to get P.

Let us now state the formal lemmas.

LEMMA A

For every $k, l, d \in \mathbb{N}^+$ such that $k \geq l \geq d+1$, if $\delta(f, P_d) = \delta$ then

$$Rej_{d,k}(f) \geq 2^l \cdot \delta\left(1 - (2^l - 1)\delta\right).$$

In particular, if $\delta \leq 2^{-(d+2)}$, then

$$Rej_{d,k}(f) \geq \min\left\{\frac{1}{8}, 2^{k-1} \cdot \delta\right\}$$

LEMMA B (KEY LEMMA)

There exist positive constants $\beta < 1/4$, ε_0, γ, and c such that the following holds for every $d, k, n \in \mathbb{N}^+$ such that $n \geq k \geq d+c$:

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be such that $\delta(f, P_d) \geq \beta \cdot 2^{-d}$. Then

$$Rej_{d,k}(f) \geq \varepsilon_0 + \gamma \cdot 2^d / 2^n.$$

LEMMA C

For every $d, k, k', n \in \mathbb{N}^+$ such that $n \geq k \geq k' \geq d+1$ and every $f : \mathbb{F}_2^n \to \mathbb{F}_2$ it holds that

$$Rej_{d,k'}(f) \geq Rej_{d,k}(f) \cdot 2^{-(k-k')}$$

Proof of main theorem (assuming Lemmas A–C)

Let ε_0 and c be constants as in Lemma B. Set $\varepsilon_1 = \varepsilon_0 \cdot 2^{-(c-1)}$.

If $\delta(f, P_d) \le 2^{-(d+2)}$, then by Lemma A ("in particular"-part)

$$Rej_{d,d+1}(f) \ge 2^d \cdot \delta(f, P_d).$$

Hence, assume $\delta(f, P_d) \ge 2^{-(d+2)} \ge \beta \cdot 2^{-d}$, with β from Lemma B. Then by Lemma B

$$Rej_{d,d+c}(f) \ge \varepsilon_0$$

Lemma C now yields that

$$Rej_{d,d+1}(f) \ge \varepsilon_0 \cdot 2^{-(c-1)} = \varepsilon_1$$

and the theorem follows $\blacksquare$

In the next and final lecture, we will prove Lemmas A, B, and C.