TESTING OF LOW-DEGREE POLYNOMIALS — FINAL LECTURE

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

Want to test with few queries whether

(a) f is degree-d polynomial ($f \in \mathcal{P}_d$), or

(b) f far from all degree-d polynomials ($\delta(f, \mathcal{P}_d) \geq$ some constant ε)

Basic test $T_{d,k}$ (k-flat test)

- Pick random k-flat $A \subseteq \mathbb{F}_2^n$ (affine subspace of dimension k)
- Reject if $f \restriction A$ not degree-d polynomial

$Rej_{d,k}(f)$ = rejection probability of $T_{d,k}$ for f

k-flat $A \subseteq \mathbb{F}_2^n$ is

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

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

hyperplane: $(n-1)$-flat

Question: What does it mean, actually, that "$f \restriction A$ is a degree-d polynomial"?

Let $M = (m_{ij})$

Suppose we have $f(y_1, \ldots, y_n)$

Define $g(x_1, \ldots, x_k) = f(y_1, \ldots, y_n)$ for (†)

$$y_i = \sum_{j=1}^{k} m_{ij} x_j + b_i. \quad f \restriction A = g$$

MAIN THEOREM [BKSSZ 10]

$\exists\, \varepsilon_1 > 0$ s.t. $\forall\, d, n \in \mathbb{N}^+$, $f : \mathbb{F}_2^n \to \mathbb{F}_2$ it holds that

$$Rej_{d,d+1}(f) \geq \min\{ 2^d \cdot \delta(f, P_d), \varepsilon_1 \}$$

COROLLARY

Testing of degree-d polynomials doable with $O(2^d + 1/\delta)$ queries (and this is optimal

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

(A) If f is really close to P_d but not in P_d, then $Rej_{d,k}(f) \gtrsim \delta(f, P_d)$ 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 $P \in P_d$ differ, and so f will be rejected

(B) If $k \gtrsim d + 10$, then $T_{d,k}$ rejects f with constant probability if $\delta(f, P_d) = \Omega(2^{-d})$
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 $d+1$.

LEMMA A

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

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

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

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

We need to talk a bit more about hyperplanes

$A, B \subseteq \mathbb{F}_2^n$ are COMPLEMENTARY HYPERPLANES if $A \cup B = \mathbb{F}_2^n$

Not hard to verify that any hyperplane can be described as set of points

$$\{ x \in \mathbb{F}_2^n \mid L_c(x) = b \} \qquad (*)$$

for some $L_c(x) = \sum_{i=1}^n c_i x_i = \langle c, x \rangle$ for $c \in \mathbb{F}_2^n$, $c \neq 0$
and $b \in \mathbb{F}_2$

Refer to L_c as linear part of hyperplane

We say that hyperplanes $A_1, \ldots, A_\ell$ are linearly independent if the corresponding linear parts are linearly independent (i.e., the vectors c for the L_c are independent)

<u>PROPOSITION 1</u> (Properties of hyperplanes)

1. There are exactly $2^{n+1} - 2$ distinct hyperplanes in $\mathbb{F}_2^n$

2. Among any $2^\ell - 1$ distinct hyperplanes there are at least ℓ independent hyperplanes

3. There is an affine invertible transform that maps linearly independent hyperplanes $A_1, \ldots, A_\ell$ to the hyperplanes $x_1 = 0, \ldots, x_\ell = 0$
[i.e., $M \in \mathbb{F}_2^{n \times n}$ full-rank, $b \in \mathbb{F}_2^n$, such that $x \in \mathbb{F}_2^n$ is sent to $y = Mx + b$]

<u>Proof</u> Exercise.

Proof of Lemma A "If f close to P_d, we're good"

In one line: With good probability a random flat will contain exactly one point where f and closest degree-d polynomial disagree, which will cause test to reject.

We will prove

$$\mathrm{Rej}_{d,\ell}(f) \geq 2^{\ell}\delta(1-(2^{\ell}-1)\delta) \qquad (1)$$

CLAIM(i) ← All such claims will have proofs left as exercises

If $k \geq \ell$, then $\mathrm{Rej}_{d,k}(f) \geq \mathrm{Rej}_{d,\ell}(f)$

(Looking at larger subspace can never hurt.)

Given (1) and CLAIM(i), second part follows

Namely, assume $\delta(f, P_d) = \delta \leq 2^{-(d+2)}$.
If $\delta \leq 2^{-(k+1)}$, set $\boxed{k = \ell}$.
Otherwise, choose ℓ such that $2^{-(\ell+2)} < \delta \leq 2^{-(\ell+1)}$
(which is possible since $\delta \leq 2^{-(d+2)}$.

Former case:

$$\begin{aligned}\mathrm{Rej}_{d,k}(f) &\geq 2^{k}\delta(1-(2^{k}-1)\delta) \\ &\geq 2^{k}\delta(1-2^{k}\delta) \\ &\geq 2^{k}\cdot\delta\cdot(1-1/2) \\ &= 2^{k-1}\delta\end{aligned}$$

Latter case

$$\begin{aligned}\mathrm{Rej}_{d,k}(f) &\geq 2^{\ell}\delta(1-(2^{\ell}-1)\delta) \\ &\geq 2^{\ell}2^{-(\ell+2)}(1-2^{\ell}\cdot 2^{-(\ell+1)}) \\ &= 2^{-2}\cdot(1-1/2) = \frac{1}{8}\end{aligned}$$

Let $M \in \mathbb{F}_2^{n \times \ell}$ random full-rank matrix
Let $b \in \mathbb{F}_2^n$ random
Denote

$$a_x = Mx + b \qquad (2)$$

Then the random ℓ-flat A is

$$A = \{ a_x \mid x \in \mathbb{F}_2^\ell \}$$

Let $g \in P_d$ be such that $\delta(f, g) = \delta$
Define events

$$E_x = \text{"} f(a_x) \neq g(a_x) \text{"}$$

$$F_x = \text{"} f(a_x) \neq g(a_x) \text{ and } \forall y \neq x \; f(a_y) = g(a_y) \text{"}$$

If any F_x occurs, then $T_{d,\ell}$ rejects
This is because distinct degree-d polynomials differ in at least a 2^{-d} fraction of points [Lecture 9, page $\overline{\text{XII}}$], so no two degree-d polynomials can disagree in a single point in $\ell > d$.

<u>CLAIM (ii)</u>
Fix $x, y \in \mathbb{F}_2^\ell$, $x \neq y$. Then for random M and b as above a_x is distributed uniformly over $\mathbb{F}_2^n$ and a_y is distributed uniformly over $\mathbb{F}_2^n \setminus \{a_x\}$

Hence (with probabilities over choice of M and G, i.e., of random ℓ-flat):

$$\Pr[E_x] = \delta$$

$$\Pr[E_x \text{ and } E_y] = \Pr[E_x] \cdot \Pr[E_y \mid E_x] \leq \delta \cdot \delta = \delta^2$$

From this we get

$$\begin{aligned}\Pr[F_x] &= \Pr\Big[E_x \setminus \bigcup_{y \neq x} (E_x \cap E_y)\Big] \\ &\geq \Pr[E_x] - \sum_{y \neq x} \Pr[E_x \text{ and } E_y] \\ &\geq \delta - (2^\ell - 1)\,\delta^2 \\ &= \delta\,(1 - (2^\ell - 1)\,\delta)\end{aligned}$$

Since events F_x are mutually exclusive, we obtain

$$\begin{aligned}Rej_{d,\ell}(f) &\geq \Pr\Big[\bigcup_x F_x\Big] \\ &= \sum_x \Pr[F_x] \\ &\geq 2^\ell\,\delta\,(1 - (2^\ell - 1)\,\delta)\end{aligned}$$

and Lemma 4 follows $\square$

Proof of Lemma C

" If for $k \geq k'$, $k' = k - O(1)$, k-flat test good, ~~then~~ k'-flat test must also be fairly good "

Need Proposition 1 and two lemmas

LEMMA 2

Let $k \geq d+1$ and suppose $f : \mathbb{F}_2^{(k+1)} \to \mathbb{F}_2$ has degree $\deg(f) > d$. Then
$\mathrm{Rej}_{d,k}(f) \geq 1/2$.

Proof By contradiction. Suppose not. Means that on strict majority of hyperplanes A $f\restriction_A$ has degree d.

In particular, exist complementary hyperplanes A, $\bar{A}$ s.t. $f\restriction_A$, $f\restriction_{\bar{A}}$ both degree-d polynomials, say $g_A : \mathbb{F}_2^k \to \mathbb{F}_2$ $g_{\bar{A}} : \mathbb{F}_2^k \to \mathbb{F}_2$.

If ~~for~~ a matrix $M \in \mathbb{F}^{n \times \ell}$ has full column-rank ($n \geq \ell$), then there exists a pseudoinverse $M^+ \in \mathbb{F}^{\ell \times n}$ such that

$$M^+ M = I$$

Suppose $$A = \{ Mx + b \mid x \in \mathbb{F}_2^{n \times (n-1)} \}$$

Then for a point $a_x \in A$ (as in (2)) we have

$$a_x = \mathcal{M} x + b$$

$$\mathcal{M}^+ a_x = x + \mathcal{M}^+ b = x + b^+$$

i.e. we can express $x \in \mathbb{F}_2^{n-1}$ in terms of $y \in \mathbb{F}_2^n$ as

$$x = \mathcal{M}^+ y + b^+$$

and this map is bijective for y restricted to A

In this way from $g_A \in \mathbb{F}_2[x_1, \dots, x_{n-1}]$ we obtain a polynomial $p_A \in \mathbb{F}_2[y_1, \dots, y_n]$ by

$$p_A(y) = g_A(\mathcal{M}^+ y + b^+)$$

such that $\deg(p_A) \leq d$ and

$$\forall y \in A \quad f(y) = p_A(y)$$

Construct $p_{\bar{A}}(y)$ in the same way

Suppose (using $(*)$)

$$A = \{ y \in \mathbb{F}_2^n \mid \alpha(y) = 0 \}$$

$$\bar{A} = \{ y \in \mathbb{F}_2^n \mid \alpha(y) = 1 \}$$

Then

$$P(y) = (\alpha(y) - 1) \, P_A(y) + \alpha(y) \cdot P_{\bar{A}}(y)$$

is a polynomial of degree $\leq d+1$ that equals f <u>everywhere</u>, i.e. $f = P$.

If $\deg(P) \leq d$, we get a contradiction.

Hence suppose $\deg(P) = d+1$.

Since $\mathrm{Rej}_{d,k}(f) < 1/2$, on a strict majority of hyperplanes A we have that $f \restriction A = P \restriction A$ has degree d.

Strict majority means (by Proposition 1(1)) at least

$$\frac{1}{2}(2^{k+2} - 2) + 1 > 2^{k+1} - 1$$

hyperplanes, i.e., (by Proposition 1(2)) at least $k+1 \geq d+2$ linearly independent hyperplanes. $A_1, \ldots, A_{d+2}$.

<u>Claim (iii)</u>

Let $y = Mx + b$ full-rank (invertible) affine transform on $\mathbb{F}_2^n$. Let $Q(x) = P(Mx+b)$

Then $\deg(Q) = \deg(P)$

Using this and Prop 1(3), we can assume that the hyperplanes are $x_1 = 0, \ldots, x_{d+2} = 0$.

Using (†) again, we see that

$$f\restriction_{A_i} = P\restriction_{A_i} = P(x_1,\dots,x_n)\restriction_{x_i=0}$$

Write

$$P = P_h + P'$$

where P_h homogenous part of deg $d+1$ and $\deg(P') \leq d$.

Since $\deg(P\restriction_{A_i}) \leq d$, we have that $P_h\restriction_{x_i=0}$ vanishes for every x_i.

In other words, $x_i \mid P_h$

But then $\prod_{i=1}^{d+2} x_i \mid P_h$

which contradicts $\deg(P_h) \leq d+1$.

Lemma 2 follows $\square$

<u>LEMMA 3</u>

Let $n \geq k \geq d+1$ and let $f\ \mathbb{F}_2^n \to \mathbb{F}_2$ have $\deg(f) > d$. Then $Rej_{d,k}(f) \geq 2^{k-n}$

<u>Proof</u> Induction on n. Base case $n=k$ is obvious.

Assume Lemma holds for $n-1$.

Pick random hyperplane $A \subseteq \mathbb{F}_2^n$

By Lemma 2,

by def

$$\Pr[\, f \upharpoonright A \text{ not degree-}d \text{ polynomial} \,]$$

$$= \mathrm{Rej}_{d,n-1}(f)$$

$$\geq \ 1/2$$

Now a random k-flat in A will detect that $f \upharpoonright A$ is not degree-d with probability $\geq 2^{k-(n-1)}$.

Claim (iv)

Consider the following two experiments

(1) Pick uniformly random k-flat B in $\mathbb{F}_2^n$

(2) Pick uniformly random hyperplane C' in $\mathbb{F}_2^n$
Pick uniformly random k-flat C in C'.

Then B and C have exactly the same distribution

Using Claim (iv) and above reasoning, we get

$$\mathrm{Rej}_{d,k}(f) \geq \mathrm{Rej}_{d,n-1}(f) \cdot \mathrm{Rej}_{d,k}(f \upharpoonright A)$$

$$\geq \frac{1}{2} \cdot 2^{k-(n-1)}$$

$$= 2^{k-n}$$

(assuming $f \upharpoonright A$ is not degree-d poly) $\boxed{\equiv}$

Proof of Lemma C

For $k > k'$, we view k'-flat test as follows
(a) Pick random k-flat $A_1 \subseteq \mathbb{F}_2^n$
(b) Pick random k'-flat $A \subseteq A_1$
(c) Accept if $f \restriction A$ is degree-d polynomial

By a generalization of Claim (iv), this is exactly the same as the standard description of the k'-flat test.

$$\Pr[f \restriction A_1 \text{ not degree-}d] = Rej_{d,k}(f)$$

by definition. By Lemma 3

$$\Pr[(f \restriction A_1) \restriction A \text{ not degree-}d \mid f \restriction A_1 \text{ not degree-}d]$$
$$\geq 2^{-(k-k')}$$

Hence,

$$Rej_{d,k'}(f) = \Pr[(f \restriction A_1) \restriction A \text{ not degree-}d]$$
$$\geq Rej_{d,k}(f) \cdot 2^{-(k-k')}$$

and Lemma C follows. $\boxtimes$

Good, so now we're done with the easy Lemmas A and C.

Time to move on to Lemma B!

Proof of Lemma B

Prove lemma for any

$$\beta < 1/24$$
$$\varepsilon_0 < 1/8$$
$$\gamma \geq 72$$
$$c \geq \log_2\left(\max\left\{\frac{4\gamma}{1-8\varepsilon_0}, \frac{\gamma}{1-\varepsilon_0}, \frac{2}{\beta}\right\}\right)$$

In particular, $\beta = 1/25$, $\varepsilon_0 = 1/16$, $\gamma = 72$, $c = 10$ works.

The proof is by induction over $(n-k)$

Want to prove $\forall n \geq k \geq d+c$ that if $\delta(f, P_d) \geq \beta \cdot 2^{-d}$, then $Rej_{d,k}(f) \geq \varepsilon_0 + \gamma \cdot 2^d/2^n$

Base case $n - k = 0$

Then $Rej_{d,k}(f) = 1 \geq \varepsilon_0 + \gamma \cdot 2^{d-k}$

since
$$2^{d-k} \leq 2^{-c} \leq \cancel{\frac{\gamma}{1-8\varepsilon_0}} \quad \frac{1-\varepsilon_0}{\gamma}$$

Inductive step

Let $\mathcal{H} = \{\text{hyperplanes in } \mathbb{F}_2^n\}$

$|\mathcal{H}| = N = 2(2^n - 1)$ [by Prop 1 (1)]

Let $\mathcal{H}^*$ set of all hyperplanes $A \in \mathcal{H}$ such that

$$\delta(f|_A, P_d) < \beta \cdot 2^{-d}$$

Let $K = |\mathcal{H}^*|$

Since a random k-flat of a random hyperplane is a random k-flat (Claim (iv)) we have

$$Rej_{d,k}(f) = \underset{A \sim \mathcal{H}}{E}\left[Rej_{d,k}(f\upharpoonright_A)\right]$$

By induction, for $A \in \mathcal{H} \setminus \mathcal{H}^*$ we have

$$Rej_{d,k}(f\upharpoonright_A) \geq \varepsilon_0 + \gamma \cdot \frac{2^d}{2^{n-1}}$$

and hence

$$Rej_{d,k}(f) \geq \left(1 - \frac{K}{N}\right) \cdot \left(\varepsilon_0 + \gamma \cdot \frac{2^d}{2^{n-1}}\right)$$

$$\geq \varepsilon_0 + \gamma \cdot \frac{2^d}{2^{n-1}} - \frac{K}{N} \qquad (3)$$

We get a case analysis depending on whether $K = |\mathcal{H}^*|$ is small or large

Case 1 $K \leq \gamma \cdot 2^d$ [f far from degree-d poly on almost all hyperplanes]

then massaging (3) further we obtain

$$(3) \geq \varepsilon_0 + \gamma \cdot \frac{2^d}{2^n} \cdot 2 - \gamma \cdot \frac{2^d}{2(2^n - 1)}$$

$$\geq \varepsilon_0 + \gamma \frac{2^d}{2^n} \cdot 2 - \gamma \frac{2^d}{2^n}$$

$$= \varepsilon_0 + \gamma \cdot \frac{2^d}{2^n}$$

Case 2 $K > \gamma \cdot 2^d$ [f is close to degree-d polynomial on uncomfortably many hyperplanes]

If this happens, for many hyperplanes A there are polynomials p_A s.t. $\delta(f, p_A) \leq$ small

We want to show that these local polynomials p_A can be sewn together to global polynomial that is close to f on all of $\mathbb{F}_2^n$.

LEMMA 4 ("SEWING LEMMA")

For $f: \mathbb{F}_2^n \to \mathbb{F}_2$, let $A_1, \ldots, A_K$ be hyperplanes such that $f \restriction A_i$ is α-close to some degree-d polynomial on A_i. Then if $K > 2^{d+1}$ and $\alpha < 2^{-(d+2)}$, it holds that

$$\delta(f, P_d) \leq \frac{3}{2}\alpha + \frac{9}{K}.$$

In (3), set $\alpha = \beta \cdot 2^{-d} < 2^{-(d+2)}$

Note that $K > \gamma \cdot 2^d > 2^{d+1}$

Hence

$$\delta(f, P_d) \leq \frac{3}{2}\beta 2^{-d} + \frac{9}{\gamma \cdot 2^d} =: \delta_0$$

Since

$$\beta < 1/24$$

$$9/\gamma < 1/8$$

we get $\delta_0 \leq \frac{1}{16}2^{-d} + \frac{1}{8}2^{-d} < 2^{-(d+2)}$

Lemma A now implies that

$$\mathrm{Rej}_{d,k}(f) \geq \min\left\{ 2^{k-1}\delta(f, P_d) ,\ \frac{1}{8} \right\}$$

We claim both terms on RHS are

$$\geq \varepsilon_0 + \gamma / 2^{c+1} \geq \varepsilon_0 + \gamma\ 2^d/2^n$$

(since $n > k \geq d+c$)

By the setting of parameters at start of proof, we have

$$2^c \geq \frac{4\gamma}{1-8\varepsilon_0}$$

$$1 - 8\varepsilon_0 \geq \frac{4\gamma}{2^c}$$

$$\frac{1}{8} \geq \varepsilon_0 + \gamma/2^{c+1}$$

taking case of the second term. Since also $2^c \geq 2/\beta$ we have $\beta \geq 2^{-c+1}$ and

$$2^{k-1}\delta(f, P_d) \overset{\text{by assumption}}{\geq} 2^{k-1} \cdot \beta \cdot 2^{-d}$$

$$\geq 2^{c-1} \cdot \beta$$

$$\geq 2^{c-1} \cdot 2^{-c+1} = 1$$

Hence

$$\mathrm{Rej}_{d,k}(f) \geq \varepsilon_0 + \gamma \cdot 2^d/2^n$$

and Lemma B follows by the induction principle $\boxtimes$

We'll spend what remains of this lecture proving (or at least trying to prove) the Sewing Lemma.

High-level idea

- By assumption $\exists$ hyperplanes $A_1, \dots, A_K$ s.t. $f \upharpoonright A_i$ α-close to some polynomial P_{A_i} on A_i
- Use P_{A_i} to define $P \in \mathbb{F}_2[x_1, \dots, x_n]$ on whole space of degree $\deg(P) \leq \max_i \deg(P_{A_i}) \leq d$.
- Show that P agrees with P_{A_i} on A_i. Hence on every A_i f and P are α-close.
- Suppose A_i would cover $\mathbb{F}_2^n$ <u>exactly uniformly</u>

  $\forall z_1, z_2 \in \mathbb{F}_2^n \left(\left| \{A_i \mid z_1 \in A_i\} \right| = \left| \{A_j \mid z_2 \in A_j\} \right| \right)$

  then we would get $\delta(f, P) \leq \alpha$ and be done (with same margin)
- This is a bit too much of wishful thinking, but the coverage is almost uniform so above argument kind of works if we allow for some slack

  $\delta(f, P) \leq \frac{3}{2}\alpha + 9/K$ instead of $\delta(f, P) \leq \alpha$.

And the Sewing Lemma follows.

For every A_i, fix P_i degree-d polynomial such that $f \upharpoonright A_i$ is α-close to P_i

SUBLEMMA 5

Suppose A_i, A_j non-complementary hyperplanes ($A_i \cup A_j \neq \mathbb{F}_2^n$). Then $P_i \restriction_{A_i \cap A_j} = P_j \restriction_{A_i \cap A_j}$ if $\alpha < 2^{-(d+2)}$.

$$|A_i \cap A_j| = |A_i|/2 = |A_j|/2$$

This is so since

$$A_i = \{x \mid L_i(x) = b_i\}$$
$$A_j = \{x \mid L_j(x) = b_j\}$$

Since $A_i \neq \overline{A_j}$ there is non-empty intersection, say x^*. Then all points are given by $x^* + y$

where y solution to $\begin{cases} L_i(y) = 0 \\ L_j(y) = 0 \end{cases}$

2^{n-2} solutions. $|A_i| = |A_j| = 2^{n-1}$.

Worst case: all disagreements between f and P_i/P_j on $A_i \cap A_j$. If so still have

$$\delta(f \restriction A_i \cap A_j, P_i \restriction A_i \cap A_j) \leq 2\alpha$$
$$\delta(f \restriction A_i \cap A_j, P_j \restriction A_i \cap A_j) \leq 2\alpha$$

By Δ-inequality

$$\delta(P_i \restriction A_i \cap A_j, P_j \restriction A_i \cap A_j) \leq 4\alpha < 2^{-d}$$

But 2 degree-d polynomials agreeing in all but 2^{-d} fraction of points are the same $\boxtimes$

Let $\ell = \lfloor \log_2(K+1) \rfloor$

Then $\ell > d$

By Prop 11(2) $\exists$ ℓ linearly independent hyperplanes.

Assume wlog $A_1, A_2, \dots, A_\ell$.

By Prop 11(3), ~~assume~~ wlog for $i \in [\ell]$

$$A_i = \{ x \in \mathbb{F}_2^n \mid x_i = 0 \}$$

Can view P_i as polynomial $P_i \in \mathbb{F}_2[x_1, \dots, x_n]$ not containing any x_i

Let ~~us~~ write below

$$x = (x_1, \dots, x_\ell)$$
$$y = (x_{\ell+1}, \dots, x_n)$$

Can write any $f: \mathbb{F}_2^n \to \mathbb{F}_2$ as

$$f(x,y) = \sum_{S \subseteq [\ell]} P_{f,S}(y) \prod_{j \in S} x_j \qquad (4)$$

In particular write

$$P_i = P_i(x,y) = \sum_{S \subseteq [\ell]} P_{i,S}(y) \prod_{j \in S} x_j \qquad (5)$$

We have

$$\deg(P_{i,S}) \le d - |S| \qquad (6)$$

$$|S| > d \Rightarrow P_{i,S} = 0 \qquad (7)$$

Since x_i doesn't occur in P_i also

$$i \in S \Rightarrow P_{i,S} = 0 \qquad (8)$$

and so

$$P_i(x,y) = \sum_{S \subseteq [\ell] \setminus \{i\}} P_{i,S}(y) \prod_{j \in S} x_j \qquad (9)$$

SUBLEMMA 6

For every $S \subseteq [\ell]$, $i,j \in [\ell] \setminus S$ it holds that $P_{i,S}(y) = P_{j,S}(y)$

Proof To evaluate $P_{i,S}$ on $A_j = \{ x \in \mathbb{F}_2^n \mid x_j = 0 \}$ we simply set $x_j = 0$. Hence

$$P_i \restriction_{A_i \cap A_j} (x,y) = \sum_{S \subseteq [\ell] \setminus \{i,j\}} P_{i,S}(y) \prod_{m \in S} x_m$$

$$P_j \restriction_{A_i \cap A_j} (x,y) = \sum_{S \subseteq [\ell] \setminus \{i,j\}} P_{j,S}(y) \prod_{m \in S} x_m$$

Claim (v)

Any $f : \mathbb{F}_2^n \to \mathbb{F}_2$ has a unique representation as a multilinear polynomial over $\mathbb{F}_2[x_1, \ldots, x_n]$

By **Sublemma** 5, $P_i \restriction_{A_i \cap A_j} = P_j \restriction_{A_i \cap A_j}$

Combining this with Claim (v), these polynomials must be the same syntactically, and hence

$$P_{j,S}(y) = P_{i,S}(y)$$

as claimed $\square$

Hence, we can define for $S \subsetneq [\ell]$

$$P_S(y) = P_{i,S}(y) \quad \text{for any } i \in [\ell] \setminus S \qquad (10)$$

Now we can define our serving polynomial

$$P(x,y) = \sum_{S \subsetneq [\ell]} P_S(y) \prod_{j \in S} x_j \qquad (11)$$

By (6), (7), and (10) we have $\deg(P) \le d$.

We want to show that

$$\delta(f, P) \le \frac{3}{2}\alpha + \frac{9}{K}$$

Let us start by showing that P agrees with any P_i on A_i for $i = 1, \dots, K$ (not just for $i \le \ell$)

<u>SUBLEMMA 7</u>

For every $i \in [K]$, $P \restriction A_i = P_i \restriction A_i$

<u>Proof</u> For $i \in [\ell]$ we can just plug $x_i = 0$ into expressions (9) and (11) (using also (10)).

Consider $i \in [K] \setminus [\ell]$.

For any $x \in A_i \cap \bigcup_{j=1}^{\ell} A_j$, letting $j^* \in [\ell]$ be such that $x \in A_{j^*}$ we have

$$P_i(x) = P_{j^*}(x)$$

by Sublemma 5 and also

$$P_{j^*}(x) = P(x)$$

by what we just showed, since $j^* \in [\ell]$

Hence P_i and P agree on $A_i \cap \bigcup_{j=1}^{\ell} A_j$

Claim (vi)

Since $\ell > d$, it holds that

$$\frac{|A_i \cap \bigcup_{j=1}^{\ell} A_j|}{|A_i|} \geq 1 - 2^{-\ell} > 1 - 2^{-d}$$

Since $P\restriction_{A_i}$ and $P_i\restriction_{A_i}$ are both of degree $\leq d$, they must be identical. Hence $P\restriction_{A_i} = P_i\restriction_{A_i}$ for all i and the sublemma follows $\boxtimes$

Hence P is close to f on every hyperplane. Recall that if $A_1, \ldots, A_K$ covered all of $\mathbb{F}_2^n$ uniformly, then we would immediately get

$$\delta(f, P) \leq \alpha$$

We'll argue instead that
- most of $\mathbb{F}_2^n$
- is covered roughly uniformly

and this will be good enough.

To this end, let

$$BAD = \{ z \in \mathbb{F}_2^n \mid z \in A_i \text{ for less than } K/3 \text{ hyperplanes } A_i \}$$

$$\tau = \frac{|BAD|}{2^n}$$

We have two final sublemmas

SUBLEMMA 8

$$\delta(f, P) \le \frac{3}{2}\alpha + \tilde{\iota}$$

SUBLEMMA 9

$$\tilde{\iota} \le 9/K$$

Combining Sublemmas 8 and 9, the Sensing Lemma immediately follows.

Proof of Sublemma 8

Consider following experiment:

Pick $z \in \mathbb{F}_2^n$ and $i \in K$ uniformly and independently at random.

Let $E_{z,i}$: $z \in A_i$ and $f(z) \neq P_i(z)$

What is $\Pr_{z,i}[E_{z,i}]$?

On the one hand

$$\Pr[E_{z,i}] \le \max_i \left\{ \Pr_z[z \in A_i] \cdot \Pr_z[f(z) \neq P_i(z) \mid z \in A_i] \right\}$$

$$\le \frac{1}{2} \cdot \alpha \qquad (12)$$

On the other hand, since $P \restriction_{A_i} = P_i$ we can calculate the probability as

$$\Pr_{z,i}\left[E_i\right] = \Pr_{z,i}\left[z \in A_i \text{ and } f(z) \neq P(z)\right]$$

$$\geq \Pr_{z,i}\left[z \in A_i \wedge f(z) \neq P(z) \wedge z \notin BAD\right]$$

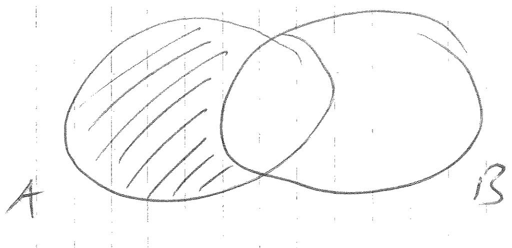
$$= \Pr_{z}\left[f(z) \neq P(z) \wedge z \notin BAD\right] \cdot \Pr_{z,i}\left[z_i \in A_i \mid f(z) \neq P(z) \wedge z \notin BAD\right]$$

$$\geq \Pr_{z}\left[f(z) \neq P(z) \wedge z \notin BAD\right] \cdot \min_{\substack{z : z \notin BAD \\ f(z) \neq P(z)}} \Pr_{i}\left[z \in A_i\right]$$

$$\geq \left(\delta(f,P) - \tau\right) \cdot \min_{z : z \notin BAD} \Pr_{i}\left[z \in A_i\right]$$

$$\geq \left(\delta(f,P) - \tau\right) \cdot \frac{1}{3}$$

using $\Pr\left[A \wedge \neg B\right] \geq \Pr[A] - \Pr[B]$ (13)



Combining (12) and (13) we get that

$$\left(\delta(f,P) - \tau\right)/3 \leq \alpha/2$$

from which the sublemma follows $\boxed{}$

Proof of Sublemma 9

Let $z \sim \mathbb{F}_2^n$ uniformly randomly distributed
For $i \in [K]$ define

$$Y_i = Y_i(z) = \begin{cases} 1 & \text{if } z \in A_i \\ -1 & \text{otherwise} \end{cases}$$

$$z \in BAD \text{ iff } \sum_{i=1}^{K} Y_i(z) \leq -K/3$$

Hence

$$\tau = \Pr_z \left[\sum_{i=1}^{K} Y_i \leq -K/3 \right] \qquad (14)$$

Since A_i is exactly half of $\mathbb{F}_2^n$ we have

$$\mathbb{E}[Y_i] = 0$$

$$Var(Y_i) = \mathbb{E}[Y_i^2] - (\mathbb{E}[Y_i])^2 = 1$$

Claim (vii)

If A_i and A_j are not complementary hyperplanes, then Y_i and Y_j are independent and so $\mathbb{E}[Y_i Y_j] = \mathbb{E}[Y_i]\,\mathbb{E}[Y_j] = 0$.

If A_i and A_j are complementary, then

$$\mathbb{E}[Y_i Y_j] = -1 \leq 0$$

Hence

$$\mathbb{E}\left[\sum_{i=1}^{K} Y_i\right] = 0 \qquad (15)$$

$$Var\left(\sum_{i=1}^{K} Y_i\right) \leq K \qquad (16)$$

(Recall that

$$Var\left(\sum_i Y_i\right) = \sum_i Var(Y_i) + 2\sum_{i<j} Cov(X_i, X_j)$$

and we have

$$Cov(Y_i, Y_j) = E[Y_i Y_j] - E[Y_i]E[Y_j]$$
$$= E[Y_i Y_j]$$
$$\leq 0 \quad)$$

CHEBYSHEV'S INEQUALITY

If X is a random variable with $Var(X) = \sigma^2$, then for every $k > 0$ it holds that

$\sigma > 0$, of course

$$Pr\left[\,|X - E[X]| > k\sigma\right] \leq \frac{1}{k^2}$$

Using Chebyshev's inequality we get

$$\gamma = Pr\left[\sum_i Y_i \leq -K/3\right]$$
$$\leq Pr\left[\left|\sum_i Y_i - E\left[\sum_i Y_i\right]\right| \geq K/3\right]$$

$\left[\text{setting } k \cdot \sqrt{Var(\sum_i Y_i)} = K/3\right]$

$$\leq \frac{Var\left(\sum_i Y_i\right)}{(K/3)^2}$$

$$\leq \frac{9 \cdot K}{K^2} = \frac{9}{K}$$

This establishes the Scaling Lemma, and hence Lemma B, and hence the main thm in [BKSSZ10]