

RECAP OF LAST LECTURE

Every function $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ can be expressed as polynomial $f \in \mathbb{F}_2[x_1, \dots, x_n]$ of degree $\leq n$

$$\mathcal{P}_r^* = \{ f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \mid \deg(f) \leq r, f(\vec{0}) = 0 \}$$

LOW-DEGREE TESTING

Input: Table of $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$
Parameters $r \in \mathbb{N}^+$, $\epsilon \in \mathbb{R}^+$

Task: Query f in $O_n(1)$ positions and output "yes"/"no" so that

- (a) If $f \in \mathcal{P}_r^*$, then output always "yes"
- (b) If $\delta(f, \mathcal{P}_r^*) \geq \epsilon$, then output "no" with probability $\geq 2/3$ (over internal randomness)

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

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

For $f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ and $\vec{y}_1, \dots, \vec{y}_\ell \in \mathbb{F}_2^n$, define

$$T_f(\vec{y}_1, \dots, \vec{y}_\ell) = \sum_{\emptyset \neq I \subseteq [\ell]} f\left(\sum_{i \in I} \vec{y}_i\right) \quad (2)$$

LEMMA 2

$f \in \mathcal{P}_r^*$ iff $\forall \vec{y}_1, \dots, \vec{y}_{r+1} \in \mathbb{F}_2^n \quad T_f(\vec{y}_1, \dots, \vec{y}_{r+1}) = 0$.

Idea behind AKKLR-tester:

- Pick random subspace $S \in \mathbb{F}_2^n$ of dimension $r+1$
- Check if $f|_S$ is degree- r polynomial with constant term zero ($f(\vec{0}) = 0$).

AKKLR-TESTER (f, r, ϵ)

Repeat $\Theta\left(\frac{1}{\epsilon \cdot 2^r} + r \cdot 2^r\right)$ times

- Uniformly and independently at random select $\vec{y}_1, \dots, \vec{y}_{r+1} \in \mathbb{F}_2^n$
- Reject if $T_f(\vec{y}_1, \dots, \vec{y}_{r+1}) \neq 0$

If all tests passed, then accept.

MAIN THEOREM [AKKLR05]

The AKKLR-tester

- (a) has query complexity $\Theta\left(\frac{1}{\epsilon} + r \cdot 2^{2r}\right)$
- (b) always accepts $f \in \mathcal{P}_r^*$
- (c) rejects f such that $\delta(f, \mathcal{P}_r^*) \geq \epsilon$ with probability $\geq 2/3$.

Query complexity: Clear from description

Completeness: $f \in \mathcal{P}_r^*$ always accepted by lemma 2

Soundness: Need to prove that if $\delta(f, \mathcal{P}_r^*) \geq \epsilon$, then AKKLR-tester rejects with high probability.

Or, viewed differently: Show that if rejection probability too low, then $\exists g \in \mathcal{P}_r^*$ such that $\delta(f, g)$ small.

Argument in two steps:

- ① Show that f is close to function g deciding by "majority vote" at each point $\vec{y}$ what $f(\vec{y})$ should be to satisfy Lemma 2
- ② Prove that majority vote function g is a degree- r polynomial

Define

$$T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_r) = T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_r) + f(\vec{y}) \quad (3)$$

$T_f^{\vec{y}}$ evaluates f on whole subspace except $\vec{y}$ (and $\vec{0}$)
if $f \in P_r^*$, by lemma 2 this allows us to evaluate f on $\vec{y}$ without looking up $f(\vec{y})$ in table

OBSERVATION 3

If $f \in P_r^*$, then $\forall \vec{y}_2, \dots, \vec{y}_{r+1} \in \mathbb{F}_2^n$ it holds that

$$T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1}) = f(\vec{y})$$

Let "majority vote" function g be defined by

$$g(\vec{y}) = \begin{cases} 1 & \text{if } \Pr_{\vec{y}_2, \dots, \vec{y}_{r+1} \sim \mathbb{F}_2^n} [T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1}) = 1] \geq \frac{1}{2} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

Define "error detection probability" of single iteration of AKKLR-test

$$\begin{aligned} \eta &= \Pr_{\vec{y}_2, \dots, \vec{y}_{r+1} \sim \mathbb{F}_2^n} [T_f(\vec{y}_1, \dots, \vec{y}_{r+1}) \neq 0] \\ &= \Pr_{\vec{y}, \vec{y}_2, \dots, \vec{y}_{r+1}} [T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1}) \neq f(\vec{y})] \end{aligned} \quad (5)$$

We concluded last lecture by stating a few more lemmas and then showed how the main theorem follows

IV

LEMMA 5 (f and g are close)

With definitions as above, $\delta(f, g) \leq 2\eta$

LEMMA 6 (g is decided by overwhelming majority)

$$\forall \vec{y} \Pr_{\vec{y}_2, \dots, \vec{y}_{r+1}} [g(\vec{y}) = T_f(\vec{y}_2, \dots, \vec{y}_{r+1})] \geq 1 - 2r\eta$$

LEMMA 7 (g is a low-degree polynomial)

If $\eta < \frac{1}{(4r+2)2^r}$, then $g \in \mathcal{P}_r^*$

LEMMA 8 (f is likely to be wrong exactly once on random subspace)

Suppose $0 < \eta < \frac{1}{(4r+2)2^r}$. The probability over

random $\vec{y}_1, \dots, \vec{y}_{r+1}$ that exactly one point

$$\vec{v} \in \left\{ \sum_{i \in I} \vec{y}_i \mid \emptyset \neq I \subseteq [r+1] \right\} \text{ has}$$

$f(\vec{v}) \neq g(\vec{v})$ is at least

$$\frac{1}{3} (2^{r+1} - 1) \delta(f, g)$$

COROLLARY 9 (Detection probability lower-bounded by distance)

If $\eta < \frac{1}{(4r+2)2^r}$, then $\eta \geq \frac{1}{3} (2^{r+1} - 1) \delta(f, g)$

Putting all of this together, the main theorem follows.

Proof of main theorem

V

Query cplx clear by description.

If $f \in P_r^*$, then test always accepts by Lemma 2.

Suppose $\delta(f, P_r^*) \geq \epsilon$.

If we run tester for $\Theta(1/\eta)$ iterations, it will reject with (any) constant probability.

By statement of thm, # iterations $\Theta(\frac{1}{\epsilon \cdot 2^r} + r \cdot 2^r)$
Need to show this is upper bound for $1/\eta$
That is

$$\eta = \Omega\left(\min(\epsilon \cdot 2^r, \frac{1}{r \cdot 2^r})\right)$$

If $\eta \geq \frac{1}{(4r+2) \cdot 2^r}$ this holds and we are done

Suppose $\eta < \frac{1}{(4r+2) \cdot 2^r}$

By Corollary 9

$$\eta \geq \frac{1}{3} (2^{r+1} - 1) \delta(f, g)$$

By Lemma 7 we have $g \in P_r^*$ and hence

$$\delta(f, g) \geq \delta(f, P_r^*) \geq \epsilon$$

so

$$\eta \geq \frac{1}{3} (2^{r+1} - 1) \cdot \epsilon = \Omega(\epsilon \cdot 2^r) \quad \square$$

Lemmas 2 and 5 left as exercises.

Today, we will prove Lemmas 6, 7, and 8

Problem:

$g(\vec{y}_1)$ is defined for fixed point $\vec{y}_1$ w.r.t. random
 $\vec{y}_2, \dots, \vec{y}_{r+1}$

Tester chooses all points $\vec{y}_1, \vec{y}_2, \dots, \vec{y}_{r+1}$ uniformly
at random

Need a way to transition between these two settings

CLAIM 10

For all $\vec{y}, \vec{z}, \vec{w}, \vec{y}_2, \dots, \vec{y}_r \in \mathbb{F}_2^n$ it holds that

$$\begin{aligned} & T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_r, \vec{w}) + T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_r, \vec{z}) = \\ &= T_f(\vec{y} + \vec{w}, \vec{y}_2, \dots, \vec{y}_r, \vec{y} + \vec{w} + \vec{z}) + T_f(\vec{y} + \vec{z}, \vec{y}_2, \dots, \vec{y}_r, \vec{y} + \vec{z} + \vec{w}) \quad (6) \end{aligned}$$

Proof Well, we just need to verify that this is indeed an equality... Fix $Y = \{\vec{y}_2, \dots, \vec{y}_r\}$ and consider any $I \subseteq \{2, 3, \dots, r\}$. Let

$$f_{Y,I}(x) = f\left(\sum_{i \in I} \vec{y}_i + x\right)$$

For every $I \neq \emptyset$, $f_{Y,I}(\vec{0}) = f\left(\sum_{i \in I} \vec{y}_i\right)$ appears twice on both sides and cancels out. For sums that involves vectors in first or last position we get on the left-hand side of (6) for every $I \subseteq \{2, \dots, r\}$ including $I = \emptyset$

$$\begin{aligned}
& f_{Y,I}(\vec{y}) + f_{Y,I}(\vec{w}) + f_{Y,I}(\vec{y} + \vec{w}) + \\
& f_{Y,I}(\vec{y}) + f_{Y,I}(\vec{z}) + f_{Y,I}(\vec{y} + \vec{z}) = \\
& = f_{Y,I}(\vec{w}) + f_{Y,I}(\vec{y} + \vec{w}) + f_{Y,I}(\vec{z}) + f_{Y,I}(\vec{y} + \vec{z}) \quad (7)
\end{aligned}$$

On the right-hand side we get

$$\begin{aligned}
& f_{Y,I}(\vec{y} + \vec{w}) + f_{Y,I}(\vec{y} + \vec{w} + \vec{z}) + f_{Y,I}(\vec{z}) + \\
& f_{Y,I}(\vec{y} + \vec{z}) + f_{Y,I}(\vec{y} + \vec{w} + \vec{z}) + f_{Y,I}(\vec{w}) = \\
& = f_{Y,I}(\vec{y} + \vec{w}) + f_{Y,I}(\vec{z}) + f_{Y,I}(\vec{y} + \vec{z}) + f_{Y,I}(\vec{w}) \quad (8)
\end{aligned}$$

What luck! (7) and (8) are the same! $\square$

Proof of Lemma 6

Fix $\vec{y} \in \mathbb{F}_2^n$. Let us denote

$$K = \Pr_{\vec{y}_2, \dots, \vec{y}_{r+1}} \left[g(\vec{y}) = T_{\vec{f}}(\vec{y}_2, \dots, \vec{y}_{r+1}) \right] \quad (9)$$

We want to prove $K \geq 1 - 2^{-r} \gamma$.

Recall again the problem

- Probability K defined for fixed $\vec{y}$ and $\vec{y}_2, \dots, \vec{y}_{r+1}$ random
- Probability γ defined for all points random

We somehow have to express K in terms of evaluations of $T_{\vec{f}}$ on random points.

These random points will not be independent, but we can always use the union bound (and hope that it will be enough). So, to this end...

Define

VIII

$$\lambda = \Pr_{\substack{\vec{y}_2, \dots, \vec{y}_{r+1} \\ \vec{z}_2, \dots, \vec{z}_{r+1}}} \left[T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1}) = T_f^{\vec{y}}(\vec{z}_2, \dots, \vec{z}_{r+1}) \right] \quad (10)$$

Then

$$\begin{aligned} \lambda &= \Pr \left[T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1}) = T_f^{\vec{y}}(\vec{z}_2, \dots, \vec{z}_{r+1}) = g(\vec{y}) \right] \\ &\quad + \Pr \left[T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1}) = T_f^{\vec{y}}(\vec{z}_2, \dots, \vec{z}_{r+1}) \neq g(\vec{y}) \right] \\ &= \cancel{\#} \kappa^2 + (1-\kappa)^2 \end{aligned}$$

Since $\kappa \geq 1/2$, we have

$$\kappa = \kappa^2 + \kappa(1-\kappa) \geq \kappa^2 + (1-\kappa)^2 = \lambda \quad (10\frac{1}{2})$$

and so it is sufficient to prove $\lambda \geq 1 - 2r\gamma$

Since we are in $\mathbb{F}_2$, it holds that

$$\lambda \cancel{\#} = \Pr_{\substack{\vec{y}_2, \vec{z}_2 \\ \vec{y}_3, \vec{z}_3 \\ \vdots \\ \vec{y}_{r+1}, \vec{z}_{r+1}}} \left[T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{r+1}) + T_f(\vec{y}, \vec{z}_2, \dots, \vec{z}_{r+1}) = 0 \right] \quad (11)$$

The sum in (11) can be massaged as

$$\begin{aligned} &T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{r+1}) + T_f(\vec{y}, \vec{z}_2, \dots, \vec{z}_{r+1}) = \\ &= T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_r, \vec{y}_{r+1}) + T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_r, \vec{z}_{r+1}) \\ &+ T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_r, \vec{z}_{r+1}) + T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{r-1}, \vec{z}_r, \vec{z}_{r+1}) \\ &+ T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{r-1}, \vec{z}_r, \vec{z}_{r+1}) + T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{r-2}, \vec{z}_{r-1}, \vec{z}_r, \vec{z}_{r+1}) \\ &+ \dots \\ &+ T_f(\vec{y}, \vec{y}_2, \vec{z}_3, \dots, \vec{z}_{r+1}) + T_f(\vec{y}, \vec{z}_2, \vec{z}_3, \dots, \vec{z}_{r+1}) \\ &\quad [r \text{ pairs of sums}] \end{aligned} \quad (12)$$

Consider a pair

$$T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{l-1}, \vec{y}_l, \vec{z}_{l+1}, \dots, \vec{z}_{r+1}) \\ + T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{l-1}, \vec{z}_l, \vec{z}_{l+1}, \dots, \vec{z}_{r+1})$$

in (12). The terms only differ in one parameter. Furthermore, T_f is a symmetric function.

Therefore, we can apply Claim 10 to obtain

$$\begin{aligned} & T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{l-1}, \vec{y}_l, \vec{z}_{l+1}, \dots, \vec{z}_{r+1}) \\ & + T_f(\vec{y}, \vec{y}_2, \dots, \vec{y}_{l-1}, \vec{z}_l, \vec{z}_{l+1}, \dots, \vec{z}_{r+1}) = \\ & = T_f(\vec{y} + \vec{y}_l, \vec{y}_2, \dots, \vec{y}_{l-1}, \vec{z}_{l+1}, \dots, \vec{z}_{r+1}, \vec{y} + \vec{y}_l + \vec{z}_l) \quad (13) \\ & + T_f(\vec{y} + \vec{z}_l, \vec{y}_2, \dots, \vec{y}_{l-1}, \vec{z}_{l+1}, \dots, \vec{z}_{r+1}, \vec{y} + \vec{y}_l + \vec{z}_l) \end{aligned}$$

Now, if $\vec{a} \in \mathbb{F}_2^n$ is fixed and $\vec{b} \in \mathbb{F}_2^n$ is chosen uniformly at random, then $\vec{a} + \vec{b}$ is also uniformly random.

And for independent, uniformly random $\vec{b}_1$ and $\vec{b}_2$, the two vectors $\vec{a} + \vec{b}_1$ and $\vec{a} + \vec{b}_1 + \vec{b}_2$ are also independent and uniformly random.

So the two $T_f(\dots)$ -terms in (13) are evaluated on random ~~points~~ subspaces. The two terms are not independent, but both for it holds that $T_f(\dots) = 0$ except with probability y .

The telescoping sum of $T_f(\dots)$ -terms in (12) has $2r$ terms, all evaluated on random subspaces (although different subspaces are dependent).

Hence (12) sums to 0 except with $\overline{X}$ probability $\leq 2r\eta$ by the union bound. Plugging this into (11), we get

$$\lambda \geq 1 - 2r\eta \quad (14)$$

Combining (10 $\frac{1}{2}$) and (14), the lemma follows. $\square$

So now we know that if the error detection probability η is small enough, then

$g(\vec{y})$ agrees with a random vote

$T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1})$ with overwhelming probability.

Now we want to prove that if η is small enough, then pointwise correction of $f(\vec{y})$ to $g(\vec{y})$ that satisfies

$$g(\vec{y}) = T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1})$$

i.e., the constraint to be a degree- r polynomial, works on the whole domain $\mathbb{F}_2^n$.

That is, local correction $g(\vec{y}) = \text{Most likely } T_f^{\vec{y}}(\vec{y}_2, \dots, \vec{y}_{r+1})$ turns slightly distorted degree- r polynomial f into perfect degree- r polynomial g !

Proof of Lemma 7

Suppose $\eta < \frac{1}{(4r+2)2^r}$. By Lemma 2,

sufficient to prove $\forall \vec{y}_2, \dots, \vec{y}_{r+1}$ that

$$T_f(\vec{y}_2, \dots, \vec{y}_{r+1}) = 0$$

What do we know about g ? Fixing $\vec{y}_1$,
for random $\vec{y}_2, \dots, \vec{y}_{r+1}$ it holds with
high probability ($\geq 1 - 2^{-r}$) that

$$T_f(\vec{y}_1, \vec{y}_2, \dots, \vec{y}_{r+1}) - f(\vec{y}_1) + g(\vec{y}_1) = 0$$

We want to prove something similar for all
 $\vec{y}_1, \dots, \vec{y}_{r+1}$ (not just most) and when changing
 f to g everywhere

So we will have to

- look at terms $g(\sum_{i \in I} \vec{y}_i)$ in the
expansion of $T_g(\vec{y}_1, \dots, \vec{y}_{r+1})$
- Expand every $g(\sum_{i \in I} \vec{y}_i)$ into summations
of f over new random subspaces
- Argue that with high probability these
expansions hold (since g is decided
by huge majorities)
- Reach the desired conclusion.

Here we go... Fix $\vec{y}_1, \dots, \vec{y}_{r+1}$. We have

$$T_g(\vec{y}_1, \dots, \vec{y}_{r+1}) = \sum_{\emptyset \neq I \subseteq [r+1]} g\left(\sum_{i \in I} \vec{y}_i\right) \quad (15)$$

For $i \in [r+1]$, $j \in [r]$ ^{independently and} uniformly at random XII
 select $\vec{z}_{ij} \in \mathbb{F}_2^n$. By Lemma 6, with
 probability $\geq 1 - 2ry$ it holds for a fixed
 $I \subseteq [r+1]$, $I \neq \emptyset$, that

$$g\left(\sum_{i \in I} \vec{y}_i\right) = T_f\left(\sum_{i \in I} \vec{y}_i, \sum_{i \in I} z_{i,1}, \dots, \sum_{i \in I} z_{i,r+1}\right) + f\left(\sum_{i \in I} \vec{y}_i\right) \quad (16)$$

Let E_1 be event that (16) holds for all
 $\emptyset \neq I \subseteq [r+1]$. By Lemma 6 and the union bound

$$\Pr[E_1] \geq 1 - (2^{r+1} - 1) 2ry \quad (17)$$

Suppose that ~~the~~ E_1 holds. Plugging (16) into (15)
 we get that

$$\begin{aligned} T_g(\vec{y}_1, \dots, \vec{y}_{r+1}) &= \sum_{\emptyset \neq J \subseteq [r]} T_f\left(\sum_{j \in J} \vec{z}_{1,j}, \dots, \sum_{j \in J} \vec{z}_{r+1,j}\right) \\ &\quad + \sum_{\emptyset \neq J \subseteq [r]} T_f\left(\vec{y}_1 + \sum_{j \in J} \vec{z}_{1,j}, \dots, \vec{y}_{r+1} + \sum_{j \in J} \vec{z}_{r+1,j}\right) \quad (18) \end{aligned}$$

by some calculations that we might
 have to skip depending on how we
 are doing on time. But they follow
 below anyway.

$$T_f(\vec{y}_1, \dots, \vec{y}_{r+1}) = [\text{assuming } \mathcal{L}_1]$$

XIII

$$\begin{aligned} & \sum_{\emptyset \neq I \subseteq [r+1]} \left[T_f \left(\sum_{i \in I} \vec{y}_i, \sum_{i \in I} \vec{z}_{i,1}, \dots, \sum_{i \in I} \vec{z}_{i,r} \right) + f \left(\sum_{i \in I} \vec{y}_i \right) \right] = \\ &= \sum_{\emptyset \neq I \subseteq [r+1]} \sum_{\emptyset \neq J \subseteq [r]} \left[f \left(\sum_{i \in I} \sum_{j \in J} \vec{z}_{ij} \right) + f \left(\sum_{i \in I} \vec{y}_i + \sum_{i \in I} \sum_{j \in J} \vec{z}_{ij} \right) \right] = \\ &= \sum_J \sum_I f \left(\sum_{i \in I} \sum_{j \in J} \vec{z}_{ij} \right) + \sum_J \sum_I f \left(\sum_{i \in I} \vec{y}_i + \sum_{i \in I} \sum_{j \in J} \vec{z}_{ij} \right) = \\ &= \sum_{\emptyset \neq J \subseteq [r]} T_f \left(\sum_{j \in J} \vec{z}_{1,j}, \dots, \sum_{j \in J} \vec{z}_{r+1,j} \right) + \\ & \sum_{\emptyset \neq J \subseteq [r]} T_f \left(\vec{y}_1 + \sum_{j \in J} \vec{z}_{1,j}, \dots, \vec{y}_{r+1} + \sum_{j \in J} \vec{z}_{r+1,j} \right) \end{aligned}$$

which is (18) above

But by the same observations as above, the T_f -evaluations in (18) are on random subspaces (not independent, but each single space is random).

Let $\mathcal{E}_2$ be event that all terms on right-hand side in (18) are 0. This we can estimate by $\eta = \Pr [\text{single } T_f(\dots) \neq 0] \text{ plus union-bounding}$

Hence

XIV

$$\Pr[E_2] \geq 1 - 2(2^r - 1)\gamma \quad (19)$$

And

$$\begin{aligned} \Pr[\text{not } E_1 \text{ or not } E_2] &\leq \\ \gamma \left[(2^{r+1} - 1)2^r + 2(2^r - 1) \right] &\leq \\ \gamma \left[2^r \cdot 4r + 2^r \cdot 2 \right] &= \\ \gamma \cdot 2^r (4r + 2) &\quad (20) \end{aligned}$$

If $\gamma < \frac{1}{(4r+2)2^r}$, this means that

there are vectors $\vec{Z}_{ij}$ such that equality in (18) holds and $\text{RHS in (18)} = 0$

But of course the value of LHS in (18) is fixed independently of random choices $\vec{Z}_{ij}$

Hence for arbitrary $\vec{y}_1, \dots, \vec{y}_{r+1}$

$$T_g(\vec{y}_1, \dots, \vec{y}_{r+1}) = 0$$

and g is a degree- r polynomial by Lemma 2 as claimed 

Only Lemma 8 left...

Proof of Lemma 8

XV

For each $I \subseteq [r+1]$, $I \neq \emptyset$, let X_I be indicator variable

$$X_I = \begin{cases} 1 & \text{if } f\left(\sum_{i \in I} \vec{y}_i\right) \neq g\left(\sum_{i \in I} \vec{y}_i\right) \\ 0 & \text{otherwise} \end{cases} \quad (21)$$

Obviously $\Pr_{\vec{y}_1, \dots, \vec{y}_{r+1}}[X_I = 1] = \delta(f, g)$ (this is by definition)

Let

$$X = \sum_{\emptyset \neq I \subseteq [r+1]} X_I \quad (22)$$

What we want to prove is that it is likely that f and g disagree on a unique point in the random subspace, or more precisely that

$$\Pr[X = 1] \geq \frac{1}{3} (2^r - 1) \delta(f, g) \quad (23)$$

Suppose for a moment all points

$\sum_{i \in I} \vec{y}_i$ fully independent (clearly not true)

Then probability of X being large goes down exponentially with $\delta(f, g)$

However, $E[X] = (2^r - 1) \delta(f, g)$ [true without assumptions]

$$E[X] \approx \sum_{s \text{ small}} s \cdot \Pr[X = s]$$

since $\Pr[X = s] \approx 0$ for s large.

If η , and hence $\delta(f, g)$ by Lemma 5, is small enough, then $\Pr[X=1]$ should be ^{largest probability} likeliest event among $X = \text{small}$, and so

$$\Pr[X=1] = \text{constant fraction of } E[X]$$

This is what Lemma 8 says, with "constant fraction" = $\frac{1}{3}$

Note that for $I_1 \neq I_2$, the points

$\sum_{i \in I_1} \vec{y}_i$ and $\sum_{i \in I_2} \vec{y}_i$ are completely independent. Hence X_{I_1} and X_{I_2} are independent, so the random variables X_I , $\emptyset \neq I \subseteq [r+1]$ are pairwise independent

$$E[X] = (2^r - 1) \delta(f, g) \quad (24)$$

one by linearity of expectation.

We will also need to discuss variance

$$\begin{aligned} \text{Var}(X) &= E[(X - E[X])^2] \\ &= E[X^2] - (E[X])^2 \end{aligned}$$

and covariance between X_i and X_j

$$\begin{aligned} \text{Cov}(X_i, X_j) &= E[(X_i - E[X_i])(X_j - E[X_j])] \\ &= E[X_i X_j] - E[X_i] E[X_j] \end{aligned}$$

which is $= 0$ if X_i & X_j independent

For $X = \sum_{i=1}^m X_i$ we have

$$\text{Var}(X) = \sum_{i=1}^m \text{Var}(X_i) + 2 \sum_{1 \leq i < j \leq m} \text{Cov}(X_i, X_j)$$

Since X_I for $\emptyset \neq I \subseteq [r+1]$ is essentially a coinflip we have

$$\begin{aligned} \text{Var}(X_I) &= \delta(f, g) (1 - \delta(f, g)) \\ &= \delta(1 - \delta) \end{aligned}$$

for brevity from now on. Since the X_I are pairwise independent, we get

$$\text{Var}(X) = (2^{r+1} - 1) \delta(1 - \delta) < \mathbb{E}[X] \quad (25)$$

We also need:

CLAIM 11

For a nonnegative random variable X it holds that

$$\Pr[X > 0] \geq \frac{(\mathbb{E}[X])^2}{\mathbb{E}[X^2]}$$

Proof of Claim 11

Let $p_i = \Pr[X = i]$. Then

$$(\mathbb{E}[X])^2 = \left(\sum_{i>0} i \cdot p_i \right)^2 = \left(\sum_{i>0} i \sqrt{p_i} \sqrt{p_i} \right)^2 \leq$$

$$[\text{Cauchy-Schwarz}] \leq \left(\sum_{i>0} i^2 p_i \right) \left(\sum_{i>0} p_i \right) = \mathbb{E}[X^2] \cdot \Pr[X > 0]$$

This implies

XVIII

$$\begin{aligned} \Pr[X=0] &\geq \frac{(E[X])^2}{E[X^2]} \quad \left[\text{Var}(X) \leq E[X] \right] \\ &\geq \frac{(E[X])^2}{E[X] + (E[X])^2} \\ &= \frac{E[X]}{1 + E[X]} \quad (26) \end{aligned}$$

Since X takes integer values, using (26) we get

$$\begin{aligned} E[X] &\geq \Pr[X=1] + \left(\frac{E[X]}{1 + E[X]} - \Pr[X=1] \right) \cdot 2 \\ &= \frac{2 E[X]}{1 + E[X]} - \Pr[X=1] \end{aligned}$$

or shifting things around

$$\begin{aligned} \Pr[X=1] &\geq E[X] \left(\frac{2}{1 + E[X]} - 1 \right) \\ &= E[X] \left(\frac{1 - E[X]}{1 + E[X]} \right) \quad (27) \end{aligned}$$

Substituting $E[X]$ from (24) we get

$$\Pr[X=1] \geq (2^{n+1} - 1) \delta \frac{1 - (2^{n+1} - 1) \delta}{1 + (2^{n+1} - 1) \delta} \quad (28)$$

Now we are almost done. We are in control of $\delta \leq 2\gamma$ (by Lemma 5), since we are assuming γ to be really small, and clearly

$$\frac{1 - (2^{r+1} - 1)\delta}{1 + (2^{r+1} - 1)\delta} \rightarrow 1$$

as $\delta \rightarrow 0$. In particular, if

$$(2^{r+1} - 1)\delta \leq \frac{1}{2} \quad (29)$$

we get the factor

$$\frac{1 - (2^{r+1} - 1)\delta}{1 + (2^{r+1} - 1)\delta} \geq \frac{1/2}{3/2} = \frac{1}{3}$$

claimed in the lemma we are proving. Using our assumption $\gamma = \frac{1}{(4r+2)2^r}$ and the fact $\delta \leq 2\gamma$ from Lemma 5, we get

$$\begin{aligned} (2^{r+1} - 1)\delta &\leq \frac{2^{r+1} - 1}{(4r+2)2^r} \leq \left[\begin{array}{c} \text{assuming} \\ r \geq 2 \end{array} \right] \\ &\leq \frac{2^{r+1}}{8 \cdot 2^{r-1}} \leq \frac{1}{2} \end{aligned}$$

and for $r=1$

$$\frac{2^2 - 1}{(4 \cdot 1 + 2)2^0} = \frac{3}{6} = \frac{1}{2}$$

The lemma follows



We will not show it here, but [AKKLR05] also contains a proof that the AKKLR-tester is nearly optimal in the following sense.

THEOREM 12 [AKKLR05]

Any tester for membership in $\mathcal{P}_r^*$ (even with two-sided error) with distance parameter ϵ must perform $\Omega(\max(\frac{1}{\epsilon}, 2^r))$ queries

So this result is nearly optimal... But not quite! We'll see how to do even better next time!