Low Degree Testing

Reminder We proved $NP \subseteq PCP[O(\log n), O(1)]_{\{0,1\}^{\text{polylog}\, n}}$ modulo low degree testing.

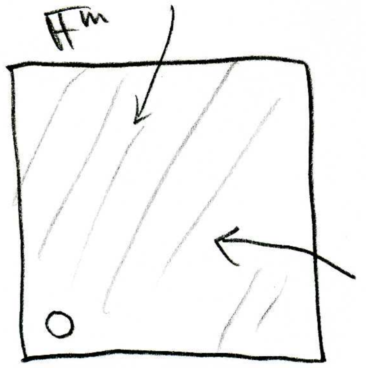
That is, we assumed the proof contains the tables of poly $\{p_i\}$. $p_i \in \mathbb{F}_{\leq d}[x_1, \ldots, x_m]$, where $m, d \ll |\mathbb{F}|$.

To remove assumption, need to devise a verifier that accesses a function $f: \mathbb{F}^m \to \mathbb{F}$, as well as a proof π over alphabet $\{0,1\}^{\text{polylog}\, n}$ in $O(1)$ places.

- Completeness $f \in \mathbb{F}_{\leq d}[x_1, \ldots, x_m] \Rightarrow \exists \pi\ P(Ver^{f,\pi} acc) = 1$.
- Soundness $f \notin \mathbb{F}_{\leq d}[x_1, \ldots, x_m] \Rightarrow \forall \pi\ P(Ver^{f,\pi} acc) \leq 0.9$

Rem Will insist on fraction $> \frac{1}{9}$. Recall that we can amplify

Observe Can't do it!



Take $p \in \mathbb{F}_{\leq d}[x_1, \ldots, x_m]$, $\vec{x}_0 \in \mathbb{F}^m$

Define

$$f(\vec{x}) = \begin{cases} p(\vec{x}) & x \neq \vec{x}_0 \\ 1 + p(\vec{x}) & x = \vec{x}_0 \end{cases}$$

- $f \notin \mathbb{F}_{\leq d}[x_1, \ldots, x_m]$
- $P(Ver^{f,\pi} acc) \geq P(Ver^{p,\pi} acc) - \frac{9}{|\mathbb{F}^m|} \geq 1 - \frac{9}{|\mathbb{F}^m|}$

# of queries Ver makes

"needle in a haystack" argument

However, we will be able to show a <u>property tester</u> with proof.

- <u>Completeness</u> $f \in \mathbb{F}_{\leq d}[x_1, \dots, x_m] \Rightarrow \exists \pi \quad P(\mathrm{Ver}^{f,\pi} \text{ acc}) = 1$

- <u>Soundness</u> f is 20%-far from $\mathbb{F}_{\leq d}[x_1, \dots, x_m] \Rightarrow \forall \pi$

$$P(\mathrm{Ver}^{f,\pi} \text{ acc}) \leq 0.9$$

<u>Def</u> (Hamming distance) The <u>normalized Hamming distance</u> between $f, g : \mathbb{F}^m \to \mathbb{F}$ is the fraction of points on which they <u>disagree</u>,

$$\Delta(f,g) \doteq P_{\vec{x} \in \mathbb{F}^m}(f(\vec{x}) \neq g(\vec{x}))$$ → We say f, g are $\Delta(f,g)$-far

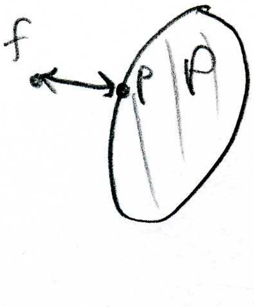
The <u>agreement</u> of f, g is

$$\mathrm{agr}(f,g) \doteq P_{\vec{x} \in \mathbb{F}^m}(f(\vec{x}) = g(\vec{x}))$$ → We say f, g are $\mathrm{agr}(f,g)$-close

The <u>normalized Hamming distance</u> between $f : \mathbb{F}^m \to \mathbb{F}$ and a set P of functions $\mathbb{F}^m \to \mathbb{F}$ is

$$\Delta(f, P) = \min_{p \in P} \Delta(f, p).$$

$$\mathrm{agr}(f, P) = 1 - \Delta(f, P).$$



<u>Note</u> • Hamming distance is a metric.

• We already saw the Hamming distance.

Observe for every $f: \mathbb{F}^m \to \mathbb{F}$, there is at most one $p_f \in \mathbb{F}_{\le d}[x_1, \ldots, x_m]$, s.t. $agr(f, p_f) \ge 0.8$.

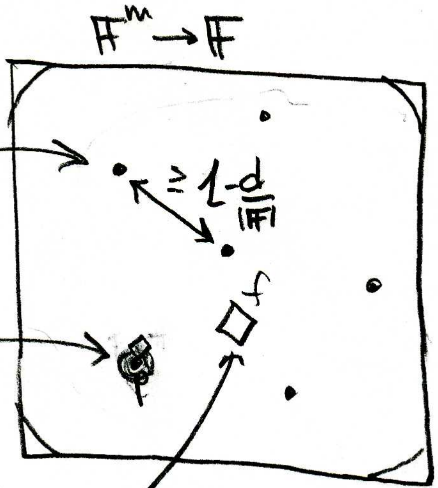
Pf Otherwise, if there's p_f'

$\Delta(p_f, p_f') \le \Delta(p_f, f) + \Delta(p_f', f)$

$\le 2 \cdot 0.2$ $\square$

$\mathbb{F}_{\le d}[x_1 \ldots x_m]$

Cannot dist. f from p if they are very close

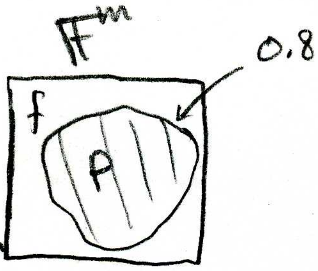


So, we'll concentrate on f's that are far from $\mathbb{F}_{\le d}[x_1, \ldots, x_m]$

$\text{Query}^{f,\pi}(\vec{x})$

1. Test f is 80%-close to $p \in \mathbb{F}_{\le d}[x_1, \ldots, x_m]$. If not, reject.
2. Evaluate p_f on $\vec{x}$. $\to$ How?

- $f(\vec{x})$ is the right eval w.p ≥ 0.8 over unif. dist. $\vec{x} \in \mathbb{F}^m$



- But: We don't eval. only on unif. dist. points in $\mathbb{F}^m$

  We need to eval at points of the form

  $(r_1, \ldots, r_{m-1}, a)$

  $a \in H$

Average-Case $\longrightarrow$ Worst-Case

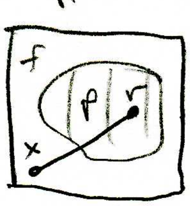
assume cannonical rep as $l : \mathbb{F} \to \mathbb{F}^m$

$l \subseteq \mathbb{F}^m \longleftrightarrow$

$Eval^{f,\pi}(\vec{x})$ $\rightarrow$

Assume proof contains for every line l, $\mathbb{F}^m$ a univariate deg-d poly. q_l

Honest prover: $q_l = p_f|_l$



1. Pick uniformly at random $\vec{r} \in \mathbb{F}^m$

2. Let l be line through $\vec{x}$ and $\vec{r}$.
   Assume $l(t_0) = \vec{x}$. Pick u.a.r $t \in \mathbb{F} \setminus \{t_0\}$,

3. Check that $q_l(t) = f(l(t))$. If not, rej.

4. Output $q_l(t_0)$.

Lemma For every $\vec{x} \in \mathbb{F}^m$

1. (Comp) For the honest prover, $Eval^{f,\pi}(\vec{x}) = p_f(\vec{x})$.
2. (Sound) For any proof π, the probability the verifier accepts, but $Eval^{f,\pi}(\vec{x}) \neq p_f(\vec{x})$ is at most 0.3.

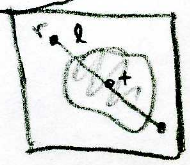
Pf Completeness is clear. Let us prove soundness.

Fix a proof π. If $Eval^{f,\pi}(\vec{x}) \neq p_f(\vec{x})$, then $q_l \neq p_f|_l$.

The prob. that this happens but $q_l(t) = p_f(l(t))$ is $\leq \frac{d}{|\mathbb{F}|-1}$

Let us concentrate on the event that $q_l(t) \neq p_f(l(t))$ but the verifier accepts $\Rightarrow \underbrace{f(l(t)) \neq p_f(l(t))}_{\text{happens w.p. } \leq 0.2}$.

Claim $l(t)$ is unif. dist. in $\mathbb{F}^m$

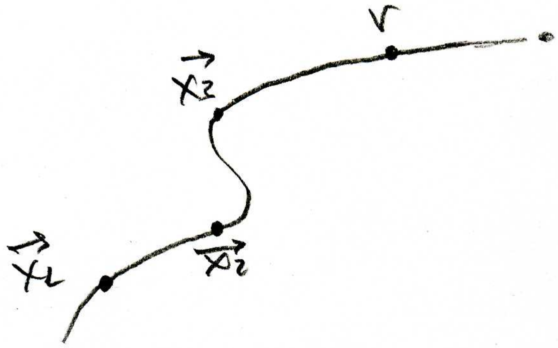


Remark

I Can extend this procedure to evaluate k points $\vec{x}_1, \dots, \vec{x}_k \in \mathbb{F}^m$ instead of one:

Use curves instead of lines.

Prove that for unif. dist. $\vec{r} \in \mathbb{F}^m$, for a unif. dist $t \in \mathbb{F} \setminus \{t_1, \dots, t_k\}$, the curve $c: \mathbb{F} \to \mathbb{F}^m$ through $\vec{x}_1, \dots, \vec{x}_k, \vec{r}$ $(c(t_i) = \vec{x}_i \;\; \forall i \in [k])$ is such that $c(t)$ is unif. dist. in $\mathbb{F}^m$.

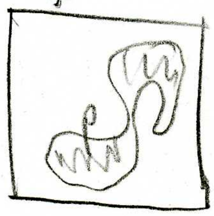


II The Eval func. we showed is an instance of a general idea "self-correction".

Low Degree Testing

Def

$$\mathrm{agr}_{\le d}(f) \doteq \max \mathrm{agr}(f, \mathbb{F}_{\le d}[x_1 \ldots x_m])$$



Def $\vec{x}_1 \ldots \vec{x}_k$ lin ind. $\{ \vec{x}_0 + t_1\vec{x}_1 + t_2\vec{x}_2 + \ldots + t_k\vec{x}_k \mid t_i \in \mathbb{F} \}$

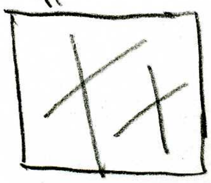
$S_k^m = \{$all k-dimensional affine subspaces in $\mathbb{F}^m\}$

Examples S_1^m = the set of all lines

S_2^m = the set of all planes

Claim I $|S_k^m| \le O(|\mathbb{F}|^{m(k+1)})$

II $\forall s \in S_k^m$, $|s| = |\mathbb{F}^k|$



Theorem For any $f: \mathbb{F}^m \to \mathbb{F}$, for any $k \ge 2$,

$$\left| \mathrm{agr}_{\le d}(f) - \mathop{\mathbb{E}}_{s \in S_k^m}[\mathrm{agr}_{\le d}(f_{|s})] \right| \le m^{O(1)} \cdot \left(\frac{d}{|\mathbb{F}|}\right)^{O(1)}$$

In ex., the easy part - (for the special case $k=1$)

$$\mathop{\mathbb{E}}_{s \in S_1^m}[\mathrm{agr}_{\le d}(f_{|s})] \ge \mathrm{agr}_{\le d}(f)$$

Next class, will prove the other part ($\lesssim$)

The Plane vs. Point Tester

Assume canonical representation

Assume proof π contains for every plane $s \in S_2^m$,
a bivariate poly. $q_s \in \mathbb{F}_{\leq d}[t_1, t_2]$.

<u>Honest prover</u> $q_s = f_{|s}$

<u>Test</u>$^{f,\pi}$

1. Pick u.a.r $s \in S_2^m$, $\vec{x} \in s$, denote $\vec{x} = x_0 + \sum_{i=1}^{2} t_i \vec{x}_i$
2. Check if $q_s(t_1, t_2) = f(\vec{x})$

<u>Lemma</u>

1. <u>Completeness</u> $f \in \mathbb{F}_{\leq d}[x_1 \ldots x_m] \Rightarrow$ for the honest prover, verifier always accepts.
2. <u>Soundness</u> $\Delta(f, \mathbb{F}_{\leq d}[x_1 \ldots x_m]) \geq 0.2 \Rightarrow$ for any prover, verifier accepts w.p $\leq 0.8 + m^{O(1)} \left(\frac{d}{|\mathbb{F}|}\right)^{O(1)}$

<u>Note</u> The theorem is <u>stronger</u> than we need.

Bibliographical Notes

- The Theorem we presented is by Raz-Safra, 97.
- It was proven (as a special case) by M.-Raz, 06.
- For slightly diff. parameters $\left(m^{O(k)} \frac{d^{O(1)}}{|\mathbb{F}|^{\Omega(1)}} \right)$, it is known for $k=1$ (Arora-Sudan, 97).
- For the simpler sub-case $\mathop{\mathbb{E}}_{s \in S_1^m} [agr_{\le d}(f_{|s})] \ge 0.9$, there are simple analyses (Friedl-Sudan, 93).
- The theorem also holds for smaller families S_k^m of affine subspaces (M.-Raz, 06).