Low Degree Testing

Reminder: We proved $\text{NP} \subseteq \text{PCP}[O(\log n), O(1)]_{\frac{1}{2}, \frac{1}{2}, \text{polylog} n}$
modesto low degree testing.

That is, we assumed the proof contains the tables of poly $f(p, \pi)$, $\pi \in \mathbb{F}_{dqd}[x_0 \rightarrow x_n]$, where $m, d < \text{polylog} n$.

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

\textbf{Completeness} \quad \forall f \in \mathbb{F}_{dqd}[x_0, \ldots, x_n] \Rightarrow \exists \Pi \forall (\text{Ver} f_{\Pi}) \text{ acc } = 1.

\textbf{Soundness} \quad \forall f \in \mathbb{F}_{dqd}[x_0, \ldots, x_n] \Rightarrow \forall \Pi \forall (\text{Ver} f_{\Pi}) \text{ acc } \leq 0.9.

Observe: Can't do it!

Take $p \in \mathbb{F}_{dqd}[x_0, \ldots, x_n]$, $x_0 \in \mathbb{F}^m$.

Define $f(x) = \begin{cases} p(x) & x \neq x_0 \\ 0 & x = x_0 \end{cases}$.

\textbf{f & \mathbb{F}_{dqd}[x_0, \ldots, x_n]}

$P(\text{Ver} f_{\Pi}) \text{ acc } \geq P(\text{Ver} p_{\Pi}) - \frac{q}{\mathbb{F}^m} \geq 1 - \frac{q}{\mathbb{F}^m}$.
However, we will be able to show a property tester with proof.

- **Completeness** \( f \in \mathbb{P}^d [x_1, ..., x_m] \rightarrow \) \( \mathbb{T} \) \( \mathbb{P}(\text{Ver}^{f, \pi} \text{ acc}) = 1 \)

- **Soundness** \( f \) is \( \leq \) \( 0.9 \) \( \mathbb{P}(\text{Ver}^{f, \pi} \text{ acc}) \leq 0.9 \)

**Def (Hamming distance)**

The **Hamming distance** between \( f, g : \mathbb{F}^m \rightarrow \mathbb{F} \) is the fraction of points on which they disagree,

\[ \Delta(f, g) = \mathbb{P}(f(x) \neq g(x)) \quad \text{We say } f, g \text{ are } \Delta(f, g) \text{-far} \]

The **agreement of** \( f, g \) is

\[ \text{agr}(f, g) = \mathbb{P}(f(x) = g(x)) \quad \text{We say } f, g \text{ are } \text{agr}(f, g) \text{-close} \]

The normalized **Hamming distance** between \( f : \mathbb{F}^m \rightarrow \mathbb{F} \) and a set \( P \) of functions \( \mathbb{F}^m \rightarrow \mathbb{F} \) is

\[ \Delta(f, P) = \min_{p \in P} \Delta(f, p) \]

\[ \text{agr}(f, P) = 1 - \Delta(f, P) \]

\[ f \rightarrow \begin{array}{c}
\vdots \\
\end{array} \]

**Note**. **Hamming distance is a metric**.

- We already saw the Hamming distance.
Observe for every $f: F^m \rightarrow F$, there is at most one $p \in F_{\leq d}[x_1, \ldots, x_m]$, s.t.

$$\text{agr}(f, p) \geq 0.8.$$ 

\text{If otherwise, if there's } p',

$$\Delta(p, p') \leq \Delta(p, f) + \Delta(f, p') \leq 0.2.$$ 

So, we'll concentrate on $f$'s that are far from $F_{\leq d}[x_1, \ldots, x_m]$.

**Query** $f(x^?)$

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

- $f(x^?)$ is the right eval w.p. $\geq 0.8$ over unif. dist. $x \in F^m$.
- But: We don't eval. only on unif. dist. points in $F^m$.
  - We need to eval at points of the form
    $$(x_1, \ldots, F \alpha)$$
    $$\in H$$
Average-Case $\rightarrow$ Worst-Case

Assume proof contains for every line $l \in \mathcal{F}^m$

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

a univariate deg-$d$ poly. $q_l$

Honest prover: $q_l = p_l$

Pick uniformly at random $v \in \mathcal{F}^m$

Let $l$ be line through $x$ and $v$.
Assume $q(l(t)) = x$. Pick $w.r.t. t \in \mathcal{F}^m$

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

Output $q_e(t_0)$.

---

Lemma For every $v \in \mathcal{F}^m$

1. For the honest prover, $\text{Eval}^{f,\pi}(x) = p_f(x)$.

2. For any proof $\pi$, the probability the verifier accepts, but $\text{Eval}^{f,\pi}(x) \neq p_f(x)$ is at most 0.3.

---

PF Completeness is clear. Let us prove soundness.

Fix a proof $\pi$. If $\text{Eval}^{f,\pi}(x) \neq p_f(x)$, then $q_e \neq q_e$

The prob. that this happens but $q_e(t) = p_f(l(t))$ is $\leq \frac{1}{10^{-1}}$

Let us concentrate on the event that $q_e(t) \neq p_f(l(t))$

but the verifier accepts $\Rightarrow f(l(t)) \neq p_f(l(t))$.

Claim $l(t)$ is unif. dist. in $\mathcal{F}^m$ happens w.p

$\leq 0.2$. 

---
Remark

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

Use curves instead of lines.

Prove that for uniform distribution $\mathbf{x} \in \mathbb{F}^m$, for a uniform distribution $\mathbf{x} \in \mathbb{F} \setminus \{t_i, \ldots, t_k\}$, the curve through $\mathbf{x}_1, \ldots, \mathbf{x}_k, \mathbf{v}$ ($c(t_i) = \mathbf{x}_i; \forall i \in [k]$) is such that $c(t)$ is uniform distribution in $\mathbb{F}^m$.

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

\[ \def \agrd_d(f) = \max \ agr(f, \mathbb{F}_d[x_1, \ldots, x_n]) \]

\[ \def \agrd_d(f) = \max \ agr(f, \mathbb{F}_d[x_1, \ldots, x_n]) \]

\[ \text{Def} \quad \max \ \text{lin ind.} \left\{ \sum_{j=0}^{k} a_j x_j \right\} + \text{eff} \]

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

Examples

\[ S_1^m = \text{the set of all lines} \]
\[ S_2^m = \text{the set of all planes} \]

Claim I \( |S_k^m| \leq O(\#^{\#(k)}) \)

\[ \forall S \subseteq S_k^m, \ |S| = \#^{\#(k)} \]

Theorem For any \( f: \mathbb{F}^m \rightarrow \mathbb{F} \), for any \( k \geq 2 \),

\[ |\agrd_d(f) - \mathbb{E}_{S \subseteq S_k^m} [\agrd_d(f_{|S})]| \leq m^{O(1)} \left( \frac{d}{\#} \right)^{O(1)} \]

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

\[ \mathbb{E}_{S \subseteq S_1^m} [\agrd_d(f_{|S})] \geq \agrd_d(f) \]

Next class, will prove the other part (\( \leq \))
The Plane vs. Point Tester

Assume $\pi$ contains for every plane $s \in S_2^m$, a bivariate poly. $q_s \in \mathbb{F}_2[x, t_1, t_2]$.

**Honest prover** $q_s = f_{1s}$

**Test** $f, \pi$

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

**Lemma**

1. **Completeness** $f(\bar{x}) \Rightarrow$ for the honest prover, verifier always accepts.
2. **Soundness** $\Delta(f, f_{\mathbb{F}_2[x]} - x) \leq 0.2 \Rightarrow$ for any prover, verifier accepts w.p. $\leq 0.8 + m o(1)$

**Note** The theorem is stronger 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 \( m^{-\Omega(\cdot)} \frac{\mu_{\vee}(1)}{\mu_{\wedge}(1)} \), it is known for \( k=1 \) (Arora-Sudan, 97).
- For the simpler sub-case \( E \left[ \xi_{\beta}(f_{15}) \right] \geq 0.9 \), there are simple analyses (Friedl-Sudan, 93).
- The theorem also holds for smaller families \( S_k \) of affine subspaces (M.-Raz, 06).