Thm: [Lecture 24]

$NP \subseteq PCP[\text{poly}(n), 1]$.

① NP-complete Problem: satisfiable quadratic equations

\# variables $x_1, \dots, x_n$ \# of equations

$$\left\{ \sum_{i,j=1}^{n} \underbrace{c^{(k)}_{i,j}}_{n^2} \cdot \underbrace{x_i \cdot x_j}_{\text{unknowns}} = \underbrace{c^{(k)}}_{n} \right\}_{k=1}^{m} = z$$

$z \in SQE \iff \exists\, x \in \{0,1\}^n$ s.t.

$$z(x) = \left(c^{(1)}, \dots, c^{(k)}\right)$$

satisfying

Idea: Let $a \in \{0,1\}^n$ s.t.

$$\underbrace{\sum c_{i,j}^{(k)} a_i a_j}_{} = c^{(k)} \quad \forall k \in [m]$$

$$\sum c_{i,j}^{(k)} \cdot a_{i,j} = \langle \vec{c}, \vec{a} \rangle$$

$$a_{i,j} = a_i \cdot a_j$$
$$= a_{i,i} \cdot a_{j,j}$$

Proof String

$$\Pi \in \{0,1\}^{2^{n^2}}$$

$$\Pi : \{0,1\}^{n^2} \longmapsto \{0,1\}$$

$$\Pi(\vec{v}) = \sum_{i,j=1}^{n} a_i \cdot a_j \cdot v_{i,j}$$

$$\vec{v} = (v_{1,1}, v_{1,2}, \ldots, v_{2,1}, \ldots, v_{n,n})$$

$$\vec{a} = (a_{1,1}, a_{1,2}, \ldots, a_{2,1}, \ldots, a_{n,n})$$

$$\Pi(c_{1,1}^{(k)}, \ldots, c_{n,n}^{(k)}) = c^{(k)} \quad \forall k$$

$$\Pi(\vec{v}) = \langle \vec{v}, \underline{\vec{a}} \rangle$$

$$\Pi : \{0,1\}^{n^2} \longmapsto \{0,1\} \longrightarrow \in \{0,1\}^{2^{n^2}}$$

$$\pi[\vec{v}] = \pi(\vec{v})$$

<u>Verification</u>

① π encodes a <u>linear function</u>

$$\pi(\vec{v}) = \langle \vec{v}, \vec{\lambda} \rangle$$

$$= \sum_{i,j=1}^{n} v_{i,j} \cdot \lambda_{i,j}$$

$\pi(a \cdot x) = a\,\pi(x)$

$\pi(x+y) =$
$\pi(x) + \pi(y)$

$\lambda_{i,j} \in \{0,1\} \quad \forall i,j.$

② $\lambda_{i,j}$ are <u>consistent</u>

$$\lambda_{i,j} = \lambda_{i,i} \cdot \lambda_{j,j} \quad \forall i,j$$

③ The equations are satisfied by $\lambda_{i,i} = a_i \;\; \forall i.$

Linearity Test

$f : \{0,1\}^N \to \{0,1\}$ is linear if

$\exists r$ s.t. $f(x) = \langle x, r \rangle$
$= \sum x_i \cdot r_i$

- Goal: Test if Π is close to f (linear above)

Test:

1. Sample $x, y \xleftarrow{\$} \{0,1\}^N$
2. Query $\Pi(x)$, $\Pi(y)$, $\Pi(x+y)$
3. Accept iff $\Pi(x+y) = \Pi(x) + \Pi(y)$

Distance:

If $\Pr_x [f(x) \neq g(x)] = \delta$

for any $f, g : \{0,1\}^n \to \{0,1\}$, then

f, g have distance δ $(\Delta(f,g) = \delta)$

- We say g is δ-far from linear

if $\forall$ linear f,

$$\Delta(f,g) \geq \delta$$

Lemma: If π is ε-far from linear,

then the linearity test

$$\left(\underset{x,y \leftarrow^{\$} \{0,1\}^n}{\pi(x+y) = \pi(x) + \pi(y)} \right)$$

rejects w.p. $\geq \varepsilon$.

If Π not linear, then

Π is ε-far for some $\varepsilon \in (0, \frac{1}{2})$

* we assume Π is $\frac{1}{48}$-close to linear

Consistency Test

$$f(\vec{v}) = \sum_{i,j=1}^{n} \lambda_{i,j} \cdot V_{i,j} \quad \text{s.t.}$$

$$\underline{\lambda_{i,j} = \lambda_{i,i} \cdot \lambda_{j,j}} \quad \forall\, i,j$$

$$M = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ \vdots & \vdots & & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,n} \end{pmatrix}$$

$$\vec{\lambda} = (\lambda_{1,1}, \lambda_{2,2}, \ldots, \lambda_{n,n})$$

$$M = \vec{\lambda}^T \cdot \vec{\lambda} \iff \lambda_{i,j} = \lambda_{i,i} \cdot \lambda_{j,j} \quad \forall\, i,j$$

$\lambda_{i,i}^2 = \lambda_{i,i}$ over $\{0,1\}$

<u>Claim:</u> Let $M \neq M'$ be $n \times n$ binary matrices. Then,

$$\Pr_{\vec{x},\vec{y} \xleftarrow{\$} \{0,1\}^n} \left[\vec{x} M \vec{y}^T = \vec{x} M' \vec{y}^T \right] \le \frac{3}{4}$$

<u>Proof:</u> $\vec{x} M \vec{y}^T = \vec{x} M' \vec{y}^T \Longleftrightarrow$

$$\vec{x} \underbrace{(M - M')}_{A \neq 0^{n \times n}} \vec{y}^T = 0 \qquad M \neq M'$$

$$\Pr_{\vec{x},\vec{y}} \left[\vec{x} A \vec{y}^T = 0 \mid A \neq 0^{n \times n} \right]$$

- $A y^T = \vec{0}$ w.p. $\le \frac{1}{2}$

  $\Updownarrow$

  $\langle A_i, \vec{y} \rangle = 0$ $\forall$ rows i

$$\Pr_{\vec{y}}\left[\langle A_i, \vec{y}\rangle = 0\right] = \frac{1}{2}$$

- Otherwise, $A\vec{y}^T = \vec{z} \neq \vec{0}$

$$\Pr_{\vec{x}}\left[\langle \vec{x}, \vec{z}\rangle = 0 \mid \vec{z} \neq \vec{0}\right] = \frac{1}{2}$$

$$\Rightarrow \Pr_{x,y}\left[\vec{x} A \vec{y}^T = 0 \mid A \neq 0\right] \leq \frac{1}{2} + \frac{1}{4}$$

$$= \frac{3}{4}$$

How to do above w/ Π?

$$f(\vec{v}) = \underline{\sum \lambda_{i,j}} \cdot \underline{v_{i,j}}$$

suppose we have access to this

① $\vec{x} M \vec{y} = \sum_{i,j=1}^{n} \underline{\lambda_{i,j}}\, \underline{x_i \cdot y_j} = f(\vec{v})$

$v_{i,j} = x_i \cdot y_j$

② $\vec{x}(\vec{\lambda}^T \cdot \vec{\lambda})\vec{y}$

$\parallel$

$$\parallel$$

$$\left(\vec{x}\,\vec{\lambda}^T\right)\left(\vec{\lambda}\,\vec{y}\right)$$

$$= \langle \vec{x}, \vec{\lambda} \rangle \cdot \langle \vec{\lambda}, \vec{y} \rangle = \left(\sum_i x_i \cdot \lambda_{ii}\right)\left(\sum_i y_i \cdot \lambda_{ii}\right)$$

$\langle \vec{x}, \vec{\lambda} \rangle = f(\vec{v}_1)$ $(\vec{v}_1)_{i,i} = x_i$ and

0 otherwise

$\langle \vec{y}, \vec{\lambda} \rangle = f(\vec{v}_2)$ for $(\vec{v}_2)_{i,i} = y_i$ and

0 otherwise ✓

But we have Π, not f!

- Sample $\vec{r} \xleftarrow{\$} \{0,1\}^{n^2}$
- Define $\tilde{f}(\vec{v}) = \Pi(\vec{r}) + \Pi(\vec{v} + \vec{r})$
  - If Π is linear, then

self correction

$\tilde{f}(\vec{v}) = \Pi(\vec{v})$

$\Pi(\vec{r}) + \Pi(\vec{v} + \vec{r})$

$= \cancel{\pi(\vec{r})} + \cancel{\pi(\vec{r})} + \pi(\vec{v})$

- If $\pi(\vec{r}) = f(\vec{r})$ and
$\pi(\vec{r}+\vec{v}) = f(\vec{r}+\vec{v})$, then
$\hat{f}(\vec{v}) = f(\vec{v})$

Consistency Test:

① Sample $\vec{x}, \vec{y} \xleftarrow{\$} \{0,1\}^n$
$\vec{r}_{1,2,3} \xleftarrow{\$} \{0,1\}^{n^2}$

② Query $\pi(\vec{v}_1 + \vec{r}_1) = a_{1,1}$
$(\vec{v}_1)_{i,j} = x_i \cdot y_j$

$\pi(\vec{v}_2 + \vec{r}_2) = a_{2,1}$
$(\vec{V}_2)_{i,i} = x_i$ (0 o.w.)

$\pi(\vec{v}_3 + \vec{r}_3) = a_{3,1}$
$(v_3)_{i,i} = y_i$

$a_{1,2} = \pi(\vec{r}_1)$ $a_{2,2} = \pi(\vec{r}_2)$

$a_{3,2} = \pi(\vec{r}_3)$

Compute

$a_1 = a_{1,1} + a_{1,2} = \tilde{f}(v_1)$

$a_2 = a_{2,1} + a_{2,2}$ $\vdots$

$a_3 = a_{3,1} + a_{3,2}$

Accept iff

$a_1 = a_2 \cdot a_3$

we correctly compute f ✓

except w.p. $\leq \frac{1}{24} = \frac{2}{48}$

Thm: If π is $\frac{1}{48}$-close to a linear f, then if f is not consistent, this above test rejects w.p. $\geq \frac{1}{8}$

Satisfiability Test

- Know

π is close to a consistent linear

$$f(\vec{v}) = \sum_{i,j} \lambda_{i,j} v_{i,j}$$

$$\lambda_{i,j} = \lambda_{i,i} \cdot \lambda_{j,j} \quad \forall i,j$$

$$\underbrace{\lambda_{i,i} = a_i \quad \forall i}_{\text{prover claims}}$$

Using Π, check that

$$\sum c_{i,j}^{(k)} \, a_i \cdot a_j = c^{(k)} \quad \forall k$$

$$\rightarrow \underbrace{c^{(k)} + \sum_{i,j=1}^{n} c_{i,j}^{(k)} \cdot a_i \cdot a_j}_{y_k} = 0 \qquad \forall k$$

$\vec{y} \in \{0,1\}^k$

Claim $\vec{y} = \vec{0}$

- Verifier will check if $\langle \vec{y}, \vec{r} \rangle = 0$ for random $\vec{r} \xleftarrow{\$} \{0,1\}^k$

$$\langle \vec{y}, \vec{r} \rangle = 0 \iff \sum_{i=1}^{n} y_i r_i = 0$$

$$= \sum_{k \in S} y_k \qquad S = \{ i \mid r_i \neq 0 \}$$

$$= \sum_{k \in S} \left(c^{(k)} + \sum_{i,j=1}^{n} c_{i,j}^{(k)} a_i \cdot a_j \right)$$

$$= \underbrace{\sum_{k \in S} c^{(k)}}_{\text{V computes directly}} + \sum_{i,j=1}^{n} \underline{a_i \cdot a_j} \left(\underline{\sum_{k \in S} c_{i,j}^{(k)}} \right)$$

$$f(\vec{v}) \sum a_i \cdot a_j \cdot V_{i,j}$$

$$V_{i,j} = \sum_{k \in S} c_{i,j}^{(k)}$$

- Done w/ 2 queries!

Thm: If π is $\frac{1}{48}$-close to consistent f, then if equations are not sat, V rejects w.p. $\geq \frac{1}{8}$

Verifier all together

Given π:

1. Perform linearity test (3 queries)
2. Perform consistency (6 queries)
3. Perform SAT Test (2 queries).

Soundness error $\leq \frac{47}{48}$.

Lecture 24