Lecture 22

<u>Goal</u> Encode $\phi$ as n-variable polynomial over $\mathbb{Z}_p$

$$Q_\phi(X_1, \dots, X_n)$$

- <u>Property</u>: $\forall \bar{b} \in \{0,1\}^n$

$$Q_\phi(\bar{b}) = \phi(\bar{b})$$

- Construct $Q_\phi$
- $\forall \ell \in [m]$
  - $\phi_\ell = (x_{\ell_1} \vee x_{\ell_2} \vee x_{\ell_3})$
  - write

$$Q_\ell(X_1, \dots, X_n) =$$
$$1 - (1 - X_{\ell_1}^{i})(1 - X_{\ell_2}^{j})(1 - X_{\ell_3}^{k})$$

- $\phi_\ell = (\overline{x}_{\ell_1} \vee x_{\ell_2} \vee x_{\ell_3})$

$Q_\ell(x_1, \dots, x_n) =$

$1 - x_{\ell_1}(1 - x_{\ell_2})(1 - x_{\ell_3})$

- $Q_\phi(x_1, \dots, x_n) :=$

$\prod_{\ell=1}^{m} Q_\ell(x_1, \dots, x_n)$

$\phi = \phi_1 \wedge \phi_2 \wedge \dots \wedge \phi_m$

$\log_2 |Q_\phi|$

$Q_\phi = \prod_{\ell=1}^{m} Q_\ell$

$Q_\ell$ has total degree $\leq 3$

$\forall \ell$

$\Rightarrow \Theta(1)$ field$/\mathbb{Z}_p$ elements to describe it

$\Rightarrow Q_\phi$ has total degree $\leq 3m$

$\Rightarrow \Theta(m \log p)$ bits

$\phi \longmapsto Q_\phi$

Want to prove

$$|\{x : \underline{\phi(x)=1}\}| = K$$

$$\longleftrightarrow K = \sum_{\bar{b} \in \{0,1\}^n} \underline{Q_\phi(\bar{b})} \mod p$$

## Sum-check protocol

$$g : \mathbb{Z}_p^n \longrightarrow \mathbb{Z}_p$$

polynomial s.t.

① $\deg_i(g) \le d \quad \forall i$

Ex $g(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1^2 + x_2^3$

$\deg_1(g) = 2$ $\quad \deg_3(g) = 1$

$\deg_2(g) = 3$

② $g(\alpha_1, \dots, \alpha_n)$ is computable in poly-time $\forall \bar{\alpha} \in \mathbb{Z}_p^n$

## Sum-check

P convinces V of the

claim $(g, K)$ s.t.

$$K = \sum_{\bar{b} \in \{0,1\}^n} g(\bar{b}) \bmod p$$

public

$P$ $\quad (K, g) \notin L \quad$ $V$

$K_1 = K$

Round 1

- Compute

$$g_1(X_1) = \sum_{\bar{b} \in \{0,1\}^{n-1}} g(X_1, \bar{b}) \qquad \alpha_1$$

$\deg_1(g) \le d$ $\quad \not\Rightarrow$

$|g_1| \le d+1$ $\mathbb{Z}_p$ elements

- checks that

$\to K_1 = g_1(0) + g_1(1)$

reject if not equal

$\alpha_1$

- Sample

$\alpha_1 \xleftarrow{\$} \mathbb{Z}_p$

- $K_2 = g_1(\alpha_1)$

Round 2

$$g_2(X_2) = \sum_{b \in \{0,1\}^{k-2}} g(\alpha_1, X_2, b)$$

$K_2 = g_2(0) + g_2(1)$ ?

$\alpha_2$

$\alpha_2 \xleftarrow{\$} \mathbb{Z}_p$

$K_3 = g_2(\alpha_2)$

⋮

$$g_i(X_i) = \sum_{b} g(\alpha_1, \dots, \alpha_{i-1}, X_i, b)$$

$$\longrightarrow$$

$$K_i = g_i(0) + g_i(1)$$

$$\xleftarrow{\alpha_i}$$

$$\alpha_i \xleftarrow{\$} \mathbb{Z}_p$$

$$K_{i+1} = g_i(\alpha_i)$$

Round $n-1$

$$g_n(X_n) = g(\alpha_1, \dots \alpha_{n-1}, X_n)$$

$$\longrightarrow$$

$$K_n = g_n(0) + g_n(1)$$

$$\alpha_n \xleftarrow{\$} \mathbb{Z}_p$$

$$g_n(\alpha_n) \stackrel{?}{=} \underline{g(\alpha_1, \dots, \alpha_n)}$$

poly-time

poly computable

Sum-check over $\mathbb{Z}_p$ for individual degree $\leq d$ polynomials has

① public-coins
② perfect completeness
③ soundness error $\leq \frac{dn}{p}$

<u>TQBF</u> $x_i \in \{0,1\}$

$$\varphi = \forall x_1 \exists x_2 \forall x_3 \cdots \exists x_n \, \phi(x_1, \ldots, x_n)$$

arithmitize these things

- $Q_\phi(x_1, \ldots, x_n)$ is arithmitization of $\phi$ from before

$\leftarrow Q_{\phi,n}$

$\varphi \in TQBF \longleftrightarrow$

$$\exists x_n\, \phi(x_1, \ldots, x_n)$$

$$\rightarrow \sum_{b_n} Q_{\phi,n}(x_1, \ldots, x_{n-1}, b)$$

$$Q_{\phi,n}(x_1, \ldots, x_{n-1}, 0) +$$
$$Q_{\phi,n}(\text{———}, 1)$$
$$\Uparrow$$
$$Q_{\phi,n-1}(x_1, \ldots, x_{n-1})$$

$$\forall x_{n-1} \rightarrow$$

$$\prod_{b_{n-1}} Q_{\phi,n-1}(x_1, \ldots, x_{n-2}, b_{n-1})$$

$$= Q_{\phi,n-1}(\text{———}, b_{n-1}) \cdot Q_{\phi,n-1}(\text{—}, b_{n-1})$$

$$=: Q_{\phi,n-2}(x_1, \ldots, x_{n-2})$$

$\vdots \ \forall x_1$

$$Q_{\phi,0} = Q_{\phi,1}(0) \cdot Q_{\phi,1}(1)$$

$\varphi \in TQBF \longleftrightarrow$

$$Q_{\phi,0} \neq 0$$

$\longleftrightarrow$

$$\prod_{b_1} \sum_{b_2} \prod_{b_3} \cdots \sum_{b_n} Q_\phi(b_1, \ldots, b_n)$$

why can't we do "Sum-check" on this?

Issue:

$\deg(Q_{\phi,1}) \leq 2^n$

$\uparrow \implies$ V is not poly-time

Observation: Over $\{0,1\}$,

$x^k = x \quad \forall x \in \{0,1\}$

$\downarrow$

$x$

$x_1^2 x_2^3 x_3 + x_1 \longleftrightarrow 2x_1 x_2 x_3 + x_1$

or something

## Linearization

$$Q_\phi(X_1, \dots, X_n)$$

$$Q_\phi(\bar{b}) = \phi(\bar{b}) \quad \forall\, \bar{b} \in \{0,1\}^n$$

$$L_i(Q_\phi)(X_1, \dots, X_n) =$$

$$= \underbrace{(1 - X_i)}_{X_i = 0} \cdot Q_\phi(\overbrace{X_1, \dots, X_{i-1}}^{\bar{b}}, 0, \overbrace{X_{i+1}, \dots, X_n}^{\bar{b}})$$

$$+ \underbrace{X_i}_{X_i = 1} \cdot Q_\phi(\overbrace{\quad}^{\bar{b}}, 1, \overbrace{\quad}^{\bar{b}})$$

Notice

$$① \; L_i(Q_\phi)(\bar{b}) = Q_\phi(\bar{b}) = \phi(\bar{b})$$

$$\forall\, \bar{b} \in \{0,1\}^n$$

② $\deg_i(L_i(Q_\phi)) = 1$

$$L_1(L_2(L_3(\cdots(L_n(Q_\phi))\cdots)$$

$$\shortparallel$$

$$f(x_1, \ldots, x_n)$$

$$f(\bar{b}) = Q_\phi(\bar{b}) = \phi(\bar{b})$$

$$\forall\ \bar{b} \in \{0,1\}^n$$

and

$$\deg(f) \leq n$$

$$\deg_i(f) = 1 \quad \forall\ i$$

$n$

Instead of proving

$$\prod_{b_1} \sum_{b_2} \cdots \sum_{b_n} Q_\phi(\bar{b})$$

$$\sum_{b_n} \boxed{\underline{L_1 L_2 \cdots L_n (Q_{\phi,n})} (\bar{b})}$$

$$\uparrow$$

$$f_{n-1}(x_1, \ldots, x_{n-1})$$

$$\prod_{b_{n-1}} f_{n-1}(x_1, \ldots, x_{n-1})$$

$$\downarrow$$

$$\prod_{b_{n-1}} L_1 L_2 \cdots L_{n-1}\left(f_{n-1}(x_1, \ldots, x_{n-1})\right)$$

$$\sum_{b_n} \frac{L_1 L_2 \cdots L_n (Q_{\phi,n})(\bar{b})}{f_n(x_1, \dots, x_n)}$$

$$\sum_{b_n} f_n(x_1, \dots, x_{n-1}, b_n)$$

$$f_{n-1}(x_1, \dots, x_{n-1}) = f_n(x_1, \dots, x_{n-1}, 0) + f_n(\text{---}, 1)$$

$$\prod_{b_{n-1}} \underbrace{L_1 L_2 \cdots L_{n-1}(f_{n-1})}_{f'_{n-1}}$$

$$f_{n-2}(x_1, \dots, x_{n-2}) =$$

$$f'_{n-1}(\cdots x_{n-2}, 0) \cdot$$

$$f'_{n-1}(\cdots, x_{n-2}, 1)$$

$$\sum_{b_{n-2}} f_{n-2}(\text{---}, b_{n-2})$$

$$\downarrow$$

$$\sum_{b_{n-2}} f'_{n-2}(\text{---}, b_{n-2})$$

$$f'_{n-2} = L_1 L_2 \cdots L_{n-2}(f_{n-2})$$

$$f_{n-3} = f'_{n-2}(\text{---}, 0) + f'_{n-2}(\text{---}, 1)$$

$L_1$

$$\psi = \forall x_1 \exists x_2 \ldots \exists x_n \, \phi(x)$$

$$f_0 = f_1'(0) \cdot f_1'(1)$$

$f_0 \neq 0 \iff \psi \in TQBF$

| $\underline{P}$ | | $V$ |
|---|---|---|
| | $\xrightarrow{f_0 \neq 0}$ | |
| | | $c_0 = f_0$ |
| | deg 1 | |
| | $\xrightarrow{f_1'(X_1)}$ | $\forall x_1$ |
| | | $c_0 = f_1'(0) \cdot f_1'(1)$ |
| | $\xleftarrow{\alpha_1 \xleftarrow{\$} \mathbb{Z}_p}$ | |
| | | $c_1 = f_1'(\alpha_1)$ |
| $\underline{\text{Round 2}}$ | const. deg | |
| | $\xrightarrow{f_1(X_1)}$ | |
| | | $c_1 = L_1(f_1)(\alpha_1)$ |
| | $\xleftarrow{r_1 \xleftarrow{\$} \mathbb{Z}_p}$ | |

$C_1 = f_1(\beta_1)$

**Round 3**

$g_2(X_2) = f_2'(\beta_1, X_2) \longrightarrow$

$g_2(0) + g_2(1) = C_1$

$\psi = \forall x_1 \exists x_2 \dots \exists x_n \, \phi(\bar{x})$

$\Downarrow$

$\psi' = \forall x_1 L_1 \exists x_2 L_1 L_2 \forall x_3 L_1 L_2 L_3 \dots \exists x_n L_1 \dots L_n \, \phi(\bar{x})$

$O(n^2)$

$\prod_{x_1} f_1'(x_1)$

$f_1(x_1)$ check that

$f_1'(x_1)$ is a correct linarization of $f_1(x_1)$

$\exists x_2 \; L_1 L_2 \; \forall x_3 \; L_1 L_2 L_3$

$$\hat{f}_2' = L_1\left[L_2(f_2)(x_1, x_2)\right]$$

$\sum f_2'$

$$L_2(f_2) = \hat{f}_2$$

$$L_1(L_2(f_2)) = L_1(\hat{f}_2)$$

- $O(n^2)$ rounds/messages
- Soundness error: $O\left(\frac{n^3}{p}\right)$
- Perfectly complete

$\Rightarrow$ TQBF $\in$ IP $\square$

$(\alpha_1, \dots, \alpha_n)$

$$L_1 L_2 \dots L_n \left( \boxed{Q_\phi} \right)$$

$$= \sum_{\bar{b} \in \{0,1\}^n} Q_\phi(\bar{b}) \, \chi(\bar{X}, \bar{b})$$

$$\chi(\bar{X}, \bar{b}) = \prod_{i=1}^{n} (1-X_i)(1-b_i) + X_i b_i$$

Lecture 22