Advanced Cryptography (Lecture 2, part 1)

When $(|H|-1) = 1$ as in case of $H = \{0, 1\}$, $\tilde{f}$ is also called the multi-linear extension, since $\deg_i \tilde{f} = 1$.

For $m = 1$, the low degree extension theorem becomes Lagrange Interpolation theorem. which states that there exists a unique way of extending $f : H \to \{0, 1\}$ to $\tilde{f} : \mathbb{F} \to \mathbb{F}$ of degree $(|H|-1)$ such that

$$\boxed{\tilde{f}(x) = \sum_{h \in H} f(h) \cdot \chi_h(x)}$$

where

$$\forall h' \in H, \quad \chi_h(h') = \begin{cases} 1 & \text{when } h = h' \\ 0 & \text{otherwise} \end{cases}$$

$$\Rightarrow \boxed{\chi_h(x) = \prod_{h' \in H \setminus \{h\}} \frac{h' - x}{h' - h}}$$

$$\boxed{f(z \in \mathbb{F}^m) = \sum_{h_1, \ldots, h_m} f(h_1, \ldots, h_m) \cdot \chi_{h_1, \ldots, h_m}} \quad (3)$$

where $\boxed{\chi_{h_1, \ldots, h_m} = \prod_{i=1}^{m} \chi_{h_i}(x_i)}$

Proof $\forall (h_1^*, \ldots, h_m^*) \in H$,

$$\tilde{f}(h_1^*, \ldots, h_m^*) = \sum_{h_1, \ldots, h_m} f(h_1, \ldots, h_m) \, \chi_{h_1, \ldots, h_m}(h_1^*, \ldots, h_m^*)$$

$$\Rightarrow \tilde{f}(h_1^*, \ldots, h_m^*) = f(h_1^*, \ldots, h_m^*)$$

Thus $\tilde{f}$ extends f. Now

$$\deg_i(\tilde{f}) = \deg_i\left(\chi_{h_1, \ldots, h_m}(x_1, \ldots, x_m)\right)$$

$$= \deg_i(\chi_{h_i}(x_i))$$

$$= (|H| - 1).$$

Suppose $\tilde{f}$ is not unique.

m

$\Rightarrow \exists\, g : \mathbb{F} \to \mathbb{F}$ such that g is non zero but $g\big|_{H^m} = 0$ and $\deg_i g = (|H|-1)$.

g here is the difference of the 2 extensions of f.

$\Rightarrow \exists\, (t_1, \dots, t_m) \in \mathbb{F}^m$ such that $g(t_1, \dots, t_m) \neq 0$.

We need to find a point in H^m for which $g \neq 0$.

Consider $g(h_1, t_2, \dots, t_m) \neq 0$ and of degree $(|H|-1)$ in h_1. By the uniqueness property enforced by the Lagrange Interpolation theorem, $\exists\, h_1 \in H$ such that $g(h_1, t_2, \dots, t_m) \neq 0$.

$\Rightarrow g(h_1, t_2, \dots, t_m)\big|_{H} \neq 0$

We can do the same in other dimensions.

Thus $g(h_1, \dots, h_m)\big|_{H^m} \neq 0$

$\Rightarrow \tilde{f}$ is thus unique.

Lets now go back to the proof for number of triangles in $G(V, E) = \beta$.

$f : \{0,1\}^{2\log n} \rightarrow \{0,1\}$ where

$$f(i,j) = \begin{cases} 1 & \text{if } (i,j) \in E \\ 0 & \text{otherwise} \end{cases}$$

f has a multilinear extension $\tilde{f} : \mathbb{F}^{2\log n} \rightarrow \mathbb{F}$. The proof statement can be written as

$$\boxed{\frac{1}{6} \sum_{i,j,k \in \{0,1\}^{\log n}} \tilde{f}(i,j) \cdot \tilde{f}(j,k) \cdot \tilde{f}(k,i) = \beta.}$$

and we can use the sum check protocol.

Runtime of $P = \tilde{O}\left(3\log n \cdot |H|^{3\log n} \cdot T_f\right)$

$$= \tilde{O}\left(3\log n \cdot |H|^{3\log n} \cdot T_f\right)$$

GKR protocol

Until now, we have seen application of the sum check protocol in proving statements involving counting. Now we will see how to do DEIPs for any circuit C with size S and depth d.

We will assume that C is layered. A gate in layer i is connected to a gate in $(i-1)$th layer. If C is unlayered we can use dummy gates to make it layered.

First, the prover P arithmetizes C. Then it computes values of all the gates in C.

Add some dummy gates if required to have s gates per level. For layer i, the s values in that layer can be written as $V_i : H^m \to \{0,1\}$ where $|H|^m = s$. We can choose s and

H^m such that $\boxed{|H| = \log s}$ and

$$\boxed{m = \frac{\log s}{\log(\log s)}}$$

$$|H|^m = (\log s)^{\frac{\log s}{\log(\log s)}}$$

$$= u^{\frac{u}{\log u}} \quad \text{where } u = \log s$$

$$= \exp\left(\log\left(u^{u/\log u}\right)\right)$$

$$= \exp(u)$$

$$= s.$$

$\forall$ layer i, P computes $V_i : H^m \longrightarrow \{0,1\}$. The low degree extension of V_i be $\tilde{V}_i : \mathbb{F}^m \longrightarrow \mathbb{F}$.

P $\quad V_0(z_0 \in H^m) = v_0$ is the statement. Or more generally $\tilde{V}_i(z_i) = v_i$.

$\longrightarrow V$

The verifier V will try to reduce

the claim to layer $(i-1)$.

$$v_i = \tilde{V}_i(z_i \in \mathbb{F}^m)$$

$$= \sum_{\text{point } p \in H^m} V_i(p) \cdot \chi_p(z_i)$$

V_i is either an addition or multiplication gate.

$$\text{addition}_i : H^{3m} \longrightarrow \{0, 1\}.$$

$$\text{add}_i(p, \omega_1, \omega_2) \longmapsto \begin{cases} 1 & \text{if } p = (\omega_1 + \omega_2) \\ 0 & \text{otherwise} \end{cases}$$

where ω_1 and $\omega_2 \in V_{i+1}$.

We can similarly define multiplication_i.

$\Rightarrow \quad v_i =$

$$\sum_{p \in H^m} \sum_{\omega_1, \omega_2 \in H^m} \Big[\tilde{\text{add}}_i(p, \omega_1, \omega_2) \cdot \{\tilde{V}_{i+1}(\omega_1) + \tilde{V}_{i+1}(\omega_2)\}$$

$$+ \tilde{\text{mult}}_i(p, \omega_1, \omega_2) \cdot \{\tilde{V}_{i+1}(\omega_1) \cdot \tilde{V}_{i+1}(\omega_2)\} \Big] \chi_p(z_i).$$

The sum check protocol can now be used to prove the above statement

The verifier needs to compute

$$\left[\widetilde{add}\big(\underset{\overset{\uparrow}{\mathbb{F}^m}}{z_0}, \underset{\overset{\uparrow}{\mathbb{F}^m}}{z_1}, \underset{\overset{\uparrow}{\mathbb{F}^m}}{z_2}\big) \left\{ \tilde{V}_{i+1}(z_1) + \tilde{V}_{i+1}(z_2) \right\} + \cdots \right] \chi_{z_0}(z_i^*)$$

Here z_0, z_1 and $z_2 \in \mathbb{F}^m$ are chosen by the verifier.

Note that $\chi_h(x)$ is a bivariate polynomial $\chi_h(x) : \mathbb{F}^2 \rightarrow \mathbb{F}$. $\boxed{\chi_h(x) = \chi(h, x)}$

There are a couple of problems

① V doesn't know how to do the $\widetilde{add}_i$ and $\widetilde{mult}_i$ operations. For now we will assume that there is a trusted oracle which helps V with evaluating these operations.

② V needs to now check that $\tilde{V}_{i+1}(z_1)$ and $\tilde{V}_{i+1}(z_2)$ sent by P, are true.