Advanced Cryptography (Lecture 1 part 2)

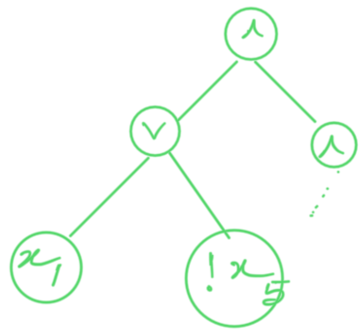
The sum check protocol is a type of public coin protocol. In a public coin protocol, the verifier doesn't keep any state and sends truly random messages (public coins) to the prover.

Suppose the false prover P^* knows t_1 ahead of time. It needs to find another polynomial which agrees with the true polynomial only at $h_1 = t_1$.

#SAT $\in$ IP

Proof: In #SAT, we are given a boolean formula $\phi(x_1, \ldots, x_n)$ and we want to find out the number of assignments make ϕ accept

$$\boxed{(\phi, K) \in \#SAT \text{ if } \left|\left\{x \in \{0,1\}^n : \phi(x) = 1\right\}\right| = K}$$



We will use arithmetization to solve this using the sum check protocol.

Fix any finite field $\mathbb{F}$. We will convert any AND gate into a multiplication gate.

$MULT(x, y) = xy$.

Any OR gate will get converted into $x + y - x.y$.

$NOT(x) \equiv 1 - x$.

$\tilde{\phi}$ be the arithmetized version. So we need to prove that

$$\sum_{b_1, \ldots, b_n \in \{0,1\}} \tilde{\phi}(b_1, \ldots, b_n) = K.$$

Since the soundness of the sum check protocol is $\frac{nd}{|\mathbb{F}|}$, we need to

show that $nd \ll |\mathbb{F}|$. We claim that $\sum_{i=1}^{n} \text{degree}_i \tilde{\phi} \leq s$ where

s = number of leaves in the binary tree representing the formula ϕ.

We will prove the claim by induction.

When # gates = 1, the claim holds true. Now, suppose,

$$\phi = \phi_1 \wedge \phi_2$$

$$\Rightarrow \tilde{\phi} = \tilde{\phi}_1 \cdot \tilde{\phi}_2$$

ϕ_1 and ϕ_2 be of sizes s_1 and s_2. Since a formula is a binary tree, size of $\phi = (s_1 + s_2)$.

$$\sum_i \deg_i \tilde{\phi} = \sum_i \left(\deg_i \tilde{\phi}_1 + \deg_i \tilde{\phi}_2\right)$$

$$\sum_i \delta'' \quad \sum_i \left(\delta_i' \quad \deg_i /2\right)$$

$$\le (s_1 + s_2) \text{ by induction.}$$

Soundness of the protocol $= \boxed{\dfrac{n s}{|\mathbb{F}|}}$

Doubly efficient interactive proof (DEIP)

Previously we assummed that the prover is all powerful. Now, we want the honest prover's runtime to be poly$(T(n))$ and V's runtime to be much less $\tilde{O}(n)$.

Consider the proof for counting the number of triangles in a graph $G(V, E)$.

Suppose there are β triangles in G.

$|V| = n$

The adjacency matrix can be represented by $f : V \times V \to \{0, 1\}$ where 1

represents the presence of an edge between the vertices.

We will represent a vertex by $\{0,1\}^{\log n}$. n vertices can be labelled from 0 to $(n-1)$. And $(n-1)$ can be represented by a binary string of size $\log n$.

$$\Rightarrow f : \{0,1\}^{\log n} \times \{0,1\}^{\log n} \longrightarrow \{0,1\}.$$

Any 3 vertices i, j and k form a triangle if $f(i,j) \cdot f(j,k) \cdot f(k,i) = 1$.

And we need to prove that

$$\frac{1}{6} \sum_{i,j,k \in V} f(i,j) \cdot f(j,k) \cdot f(k,i) = \beta$$

used to remove duplicate arrangement.

Any function can be converted into a polynomial using Low Degree Extension

For any function $f : \mathbb{F}^m \rightarrow \{0,1\}$ and

For any function $f: H^m \to \{0,1\}$ and a finite field $\mathbb{F}$ containing H $(H \subseteq \mathbb{F})$, there exists a unique low degree extension (a function $\tilde{f}: \mathbb{F}^m \to \mathbb{F}$.)

$\boxed{\tilde{f}\big|_{H^m} = f}$ and $\tilde{f}$ is of degree $(|H|-1)$ in each variable.

$$\boxed{\deg_i \tilde{f} \leq (|H|-1)}$$