Recap Sum-Check Protocol

Given a func. $\Phi: \mathbb{F}^m \to \mathbb{F}$ of $\deg \le d$

$H \subset \mathbb{F}$, Verify that

$$\sum_{\vec{x} \in H^m} \Phi(\vec{x}) = c \qquad \text{where } c \in \mathbb{F}$$

Define $g_i[\Phi]: \mathbb{F}^i \to \mathbb{F}$

$$g_i[\Phi](x_1, \ldots, x_i) := \sum_{a_{i+1} \ldots a_m \in H} \Phi(x_1, \ldots, x_i, a_{i+1}, \ldots, a_m)$$

Observe:

* $\deg g_i[\Phi] \le \deg \Phi$
* $g_i[\Phi](x_1 \ldots x_i) \equiv \sum_{a \in H} g_{i+1}[\Phi](x_1, \ldots, x_i, a)$

Sum-Check Lemma

Given a $\deg \le d$ poly $\Phi: \mathbb{F}^m \to \mathbb{F}$, a set $H \subset \mathbb{F}$, $c \in \mathbb{F}$,
(denote $G_0 = c$, $G_m = \Phi$)

I. If $\sum_{\vec{x} \in H^m} \Phi(\vec{x}) = c \Rightarrow \exists G_1, \ldots, G_{m-1}$ $\quad G_i: \mathbb{F}^i \to \mathbb{F}$

s.t. $\forall i, r_1 \ldots r_i \in \mathbb{F}$ $\quad G_i(r_1, \ldots, r_i) = \sum_{a \in H} G_{i+1}(r_1 \ldots, r_i, a)$

II If $\sum_{\vec{x} \in H^m} \Phi(\vec{x}) \ne c \Rightarrow \forall G_1, \ldots, G_{m-1}$ $\deg \le d$

$$P_{r_1 \ldots r_m \in \mathbb{F}}\left(\forall i \; G_i(r_1, \ldots, r_i) = \sum_{a \in H} G_{i+1}(r_1, \ldots, r_i, a) \right) \le \frac{d}{|\mathbb{F}|}$$

Proof I - Obvious

II - there must be i for which $G_i \not\equiv g_i[\Phi]$.

Let i be the maximal such i. So,

$G_{i+1} \equiv g_{i+1}[\Phi]$, i.e., $\sum_{a \in H} G_{i+1}(x_1, \ldots, x_i, a) \equiv g_i(x_1, \ldots, x_i)$,

so we're testing whether $G_i(\vec{r}) \stackrel{?}{=} g_i(\vec{r})$,

and the lemma follows from Schwartz-Zippel. □

Observe that the number of queries into $\Phi, G_1, \ldots, G_{m-1}$ is $\leq m \cdot (|H|+1)$ (rather than $|H|^m$!)

—

Low Degree Extension

Given $H \subset \mathbb{F}$, $f: H^m \to \mathbb{F}$

There exists a unique $\deg < |H|$ in each var extension $\hat{f}: \mathbb{F}^m \to \mathbb{F}$.

Thm $NP \subseteq PCP[O(\log n), \text{polylog}\, n]$

Proof We start with the NP-hard gap-ZT. →

gap-ZT Given $p_1, \dots, p_m \in \mathbb{F}[x_1, \dots, x_n]$, $\deg p_i \le 3$. Decide between:

1) $\exists a_1 \dots a_n \in \mathbb{F}$ s.t. $P_t(p_t(a_1, \dots, a_n) = 0) = 1$

2) $\forall a_1 \dots a_n \in \mathbb{F}$ $P_t(p_t(a_1 \dots a_n) = 0) \le \frac{1}{2}$

$|\mathbb{F}| = \Theta((\log n)^{10})$

Assume an instance $p_1, \dots, p_s \in \mathbb{F}[x_1, \dots, x_n]$ (defined by coefficients)

Step 1 Recast problem into more dimensions.

Denote p^t_{ijk} - coeff. of $x_i x_j x_k$ in p_t.
(some of i,j,k may be equal. $x_0 \equiv 1$)
Can view (p^t_{ijk}) as a func. from $\{0, \dots, n\}^3$ to $\mathbb{F}$,
or as a func. from $(H^m)^3$ to $\mathbb{F}$.

Verifier

Input $p_1, \dots, p_s \in \mathbb{F}[x_1, \dots, x_n]$

1) Choose random $t \in [s]$

2) Compute new rep. $H \subseteq \mathbb{F}$ $|H| = \log(n+1)$ $m = \frac{\log(n+1)}{\log\log(n+1)}$

Fix mapping $\{0, \dots, n\}$ to H^m.

P_t is now viewed as a fun. $(H^m)^3 \to \mathbb{F}$

Compute $Q_t : (\mathbb{F}^m)^3 \to \mathbb{F}$ $\deg < H$ in each var extension of P_t

Honest Prover

Let $\vec{a} = (1, a_1, \ldots, a_n)$ denote the common zero of $p_1, \ldots, p_m$.

Can view $\vec{a}$ as $A : \{0, \ldots, n\} \to \mathbb{F}$

also as $A : H^m \to \mathbb{F}$. Let $\hat{A}$ be its LDE

$$\sum_{\bar{u},\bar{v},\bar{w} \in H^m} Q(\bar{u},\bar{v},\bar{w})\, \hat{A}(\bar{u})\hat{A}(\bar{v})\hat{A}(\bar{w}) = p^{+}(a_1, \ldots, a_n)$$

Denote $\Phi(\bar{u},\bar{v},\bar{w}) = Q(\bar{u},\bar{v},\bar{w})\,\hat{A}(\bar{u})\hat{A}(\bar{v})\hat{A}(\bar{w})$

Verifier

3) ⓐ Select at random $\bar{u},\bar{v},\bar{w} \in \mathbb{F}^n$

Check if $\Phi(\bar{u},\bar{v},\bar{w}) \stackrel{?}{=} Q(\bar{u},\bar{v},\bar{w})\,\hat{A}(\bar{u}) \cdot \hat{A}(\bar{v}) \cdot \hat{A}(\bar{w})$

$\hat{A}(\vec{0}) = 1$

ⓑ Select at random $r_1, \ldots, r_{3m} \in \mathbb{F}$,

Check if $\forall i \in \{0, \ldots, 3m-1\}$

$$G_i(r_1, \ldots, r_i) \stackrel{?}{=} \sum_{a \in H} G_{i+1}(r_1, \ldots, r_i, a)$$ (Denote $G_0 \equiv 0$, $G_m \equiv \Phi$)

4) Test that $\hat{A}, \Phi^{+}, G_1^{+}, \ldots, G_{3m-1}^{+}$ are of low degree.

(not counting ldt)

#random bits $\log S + 3m \log|\mathbb{F}| + 3m \log|\mathbb{F}| = O(\log n)$

#quries to proof $4\log|\mathbb{F}| + 3m \cdot (|H|+1)\log|\mathbb{F}| = O(\log^2 n)$

Completeness If there are $a_1, \ldots, a_n$ s.t. $\underset{t}{P}(p_t(a_1 \ldots a_n)=0)=1$,
then there are $\{\Phi^t\}, \{\sigma_1^t\} \ldots \{\sigma_{3m-1}^t\}, \hat{A}$ s.t. $\underset{t}{P}(\text{Ver accepts})=1$.

Soundness Lemma Assume that for all $a_1 \ldots a_n \in \mathbb{F}$, $\underset{t}{P}(p_t(a_1 \ldots a_n)=0) < \frac{1}{2}$

Then: for all low degree functions $\hat{A}$ (↖ $\le m(|H|-1)$), Φ^t, σ_i^t (↖ ↗ $\le 3m(|H|-1)$)

$$P(\text{Ver accepts}) < \text{soundness}$$

↖ some constant

Proof With prob. $> \frac{1}{2}$ over the choice of t,

$$p_t(\hat{A}(\vec{1}), \ldots, \hat{A}(\vec{n})) \neq 0 \qquad (*)$$

↑ the point that 1 was mapped to

Assume that $(*)$ is the case.

Let Q be the LDE of p_t.

Observe that $\deg Q(\bar{u},\bar{v},\bar{w})\hat{A}(\bar{u})\hat{A}(\bar{v})\hat{A}(\bar{w}) \le \deg Q + 3\deg\hat{A}$

$$< 3m|H| + 3m|H|$$
$$= 6m|H|$$

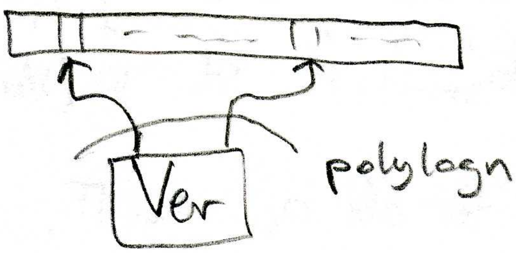
Since $\deg\Phi < 6m|H|$, if $\Phi(\bar{x},\bar{y},\bar{z}) \not\equiv Q(\bar{x},\bar{y},\bar{z})\hat{A}(\bar{x})\hat{A}(\bar{y})\hat{A}(\bar{z})$,
step 3ⓐ passes w.p $< \frac{6m|H|}{|\mathbb{F}|}$

Assume "$\Phi \equiv Q\hat{A}\hat{A}\hat{A}$". We know that $0 \neq p_t(\hat{A}(1) \ldots \hat{A}(n)) = \sum_{\bar{u},\bar{v},\bar{w} \in H^m} \Phi(\bar{u},\bar{v},\bar{w})$
assuming $\hat{A}(\vec{0})=1$, by the Sum Check Lemma,

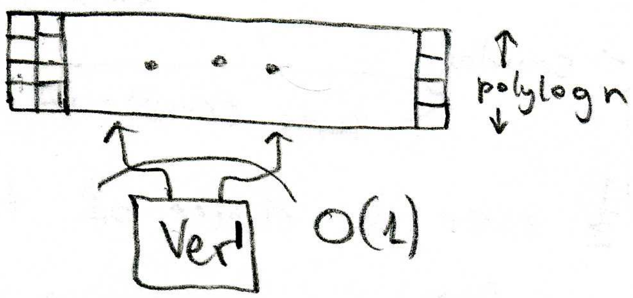
$$P(\text{Ver accepts}) < \frac{6m|H|}{|\mathbb{F}|}$$

Total acceptance prob. $\le \frac{1}{2} + O\left(\frac{m|H|}{|\mathbb{F}|}\right) < \frac{2}{3}$ for large enough $\mathbb{F}$.

So far



We will next show



Note this direction is trivial

Thm $NP \subseteq PCP[O(\log n), \text{polylog } n]_{\{0,1\}} \Longrightarrow$

$NP \subseteq PCP[O(\log n), O(1)]_{\{0,1\}^{\text{polylog} n}}$

How to prove $NP \subseteq PCP[O(\log n), O(1)]_{\{0,1\}}$?
By composition. — Motivation

Def A degree-d polynomial **curve** is a function $\gamma : \mathbb{F} \to \mathbb{F}^m$, $\gamma = (\gamma_1, \dots, \gamma_m)$, $\gamma_i : \mathbb{F} \to \mathbb{F}$, s.t. $\deg \gamma_i \leq d$.

Example $t \overset{\gamma}{\longmapsto} (t^3, 3t-1, 2t^2+4t-1, 7)$

γ can be written as $\gamma(t) = \bar{a}_0 + \bar{a}_1 t + \bar{a}_2 t^2 + \dots + \bar{a}_d t^d$

* If $f : \mathbb{F}^m \to \mathbb{F}$ is a degree $\leq r$ function, then $g : \mathbb{F} \to \mathbb{F}$ defined by $g(t) := f(\gamma(t))$ is of $\deg \leq r \cdot d$.

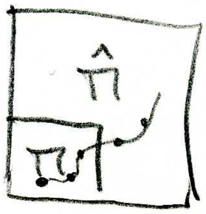
* Given points $\bar{x}^1, \dots, \bar{x}^l \in \mathbb{F}^m$, there is a unique $\deg < l$ curve $\gamma : \mathbb{F} \to \mathbb{F}^m$ s.t. $\gamma(i) = \bar{x}_i$. (assuming $\{1, \dots, l\} \subset \mathbb{F}$)

Ver'

Let r' = random bits

① Simulate Ver on the input and compute indices $i_1, \dots, i_q$ ($q = \text{polylog} n$) to read from Π.

compute $\vec{x}_1, \dots, \vec{x}_q \in H^m$ corr. points.



② compute γ - the deg $< q$ curve s.t. $\gamma(i) = \vec{x}^i$

Ask the prover for $g: \mathbb{F} \to \mathbb{F}$, supposedly $g(t) \equiv \hat{\Pi}(\gamma(t))$

$|H| = \log|pf|$

$m = \frac{\log|pf|}{\log\log|pf|}$

$|\mathbb{F}| = |H|^{\text{constant}}$

Tests:

① Select random $r \in \mathbb{F}$ and check $g(r) = \hat{\Pi}(\gamma(r))$

② Eval. $g(1), g(2), \dots$ and accept iff Ver would have accepted.

③ Test $\hat{\Pi}$ for low degree.

$\deg g = \deg(\hat{\Pi}) \cdot \deg(\gamma) \leq m \cdot |H| \cdot q$

to describe g, we need $m|H| q \log|\mathbb{F}| = \text{polylog} n$ bits.

Completeness Clearly $\hat{\Pi}$ can be computed from Π. Set $g := \hat{\Pi} \circ \gamma$ for all γ.

Soundness Suppose that $\forall \Pi$ $P(\text{Ver acc}) < \frac{1}{2}$.

Lemma Then for any deg $m \cdot |H|$ $\hat{\Pi}: \mathbb{F}^m \to \mathbb{F}$ and any poly $\{g_\gamma\}_\gamma$

$$\underset{r, r'}{P}(\text{Ver' acc}) < \frac{1}{2} + \frac{m|H|q}{|\mathbb{F}|}$$

Proof If r' is s.t. Ver rejects, then $\hat{\Pi}(\gamma_{r'}(1), \dots, \gamma_{r'}(q))$ cause Ver to reject. So Ver' only acc. if $g \not\equiv \hat{\Pi} \circ \gamma_{r'}$, but then it acc in Test ① w. prob $\leq \frac{m|H|q}{|\mathbb{F}|}$. □