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

Def (Zero Testing) $\mathbb{F}$ - finite field. d natural number (here $d=3$)

Denote $\mathbb{F}_{\leq d}[x_1, \ldots, x_n]$ - all poly of deg $\leq d$ in $x_1 \ldots x_n$ over $\mathbb{F}$.

Instance = $p_1, \ldots, p_m \in \mathbb{F}_{\leq d}[x_1, \ldots, x_n]$

Decision problem: Decide if $\exists a_1 \ldots a_n \in \mathbb{F}$ s.t. $\forall j \quad P_j(a_1, \ldots, a_n) = 0$

Gap problem: Decide whether:

Yes $\exists a_1 \ldots a_n = \bar{a} \quad \forall j \quad p_j(a_1 \ldots a_n) = 0$

No $\forall \bar{a} \quad \Pr_{j \in [m]}(p_j(\bar{a}) = 0) \leq \frac{1}{2}$

Claim 1 Decision version is NPC.

Pf By reduction from 3SAT

$$\bar{x}_i \vee x_j \vee x_k \longmapsto x_i \cdot (1-x_j) \cdot (1-x_k)$$

$\square$

Claim 2 The gap version is NP-hard.

Pf In exercise

$\square$

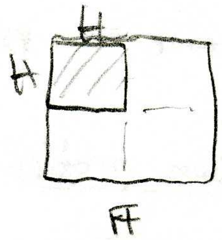
Remark Claim 2 doesn't prove the PCP Thm, since each poly may depend on all variables.

Restricted Problem:

Given a deg 3 poly $P(x_1 \ldots x_n)$ (given via coeff.)
Locally verify there is a zero for P.

Def Let $\mathbb{F}$ be a finite field, $H \subset \mathbb{F}$, $|H| = h$
Given a func. $f : H^m \to \mathbb{F}$, its degree-h extension

$$\hat{f} = LDE_h(f) \text{ is a unique poly } \hat{f} : \mathbb{F}^m \to \mathbb{F} \text{ s.t.}$$



1. The degree of $\hat{f}$ in each var. is $< h$.
2. $\forall \bar{v} \in H^m$, $f(v) = \hat{f}(v)$

Lemma For any $f : H^m \to \mathbb{F}$, $LDE_h(f)$ is well-defined. (Interpolation)

Proof For $\bar{a} = (a_1, \ldots, a_n) \in H^m$

$$L_{\bar{a}}(x_1, \ldots, x_m) = \prod_{i=1}^{m} \prod_{\substack{b \in H \\ b \neq a_i}} \frac{x_i - b}{a_i - b}$$

- $L_{\bar{a}}(\bar{a}) = 1$
- $L_{\bar{a}}(\bar{x}) = 0 \quad \forall \bar{x} \neq \bar{a} \in H^m$

Take $\hat{f}(x_1, \ldots, x_m) = \sum_{\bar{a} \in H^m} f(\bar{a}) \cdot L_{\bar{a}}(x_1, \ldots, x_m)$

Clearly, the deg of $\hat{f}$ is $< h$ in each var.

Uniqueness Let $g_1, g_2 : \mathbb{F}^m \to \mathbb{F}$ of deg$<h$ in each var.
Then either $g_1 \equiv g_2$ or $\exists \bar{a} \in H^m$ $g_1(\bar{a}) \neq g_2(\bar{a})$.

Proof By induction on m

$m=1$: Two distinct univariate poly of deg$<h$ cannot agree on h pts.

$(m-1) \to m$: Assume $g_1(\bar{a}) = g_2(\bar{a})$ $\forall \bar{a} \in H^m$

For $a \in \mathbb{F}$, denote $g_{1,a}(x_2, \ldots, x_m) := g_1(a, x_2, \ldots, x_m)$
$g_{2,a}(x_2, \ldots, x_m) := g_2(a, x_2, \ldots, x_m)$

If $a \in H$ then $g_{1,a}$ agrees with $g_{2,a}$ on H^{m-1}, so by induction $g_{1,a} \equiv g_{2,a}$.
Now let $(b_2, \ldots, b_m) \in \mathbb{F}^{m-1}$

$g_{1,\bar{b}}(y) := g_1(y, b_2, \ldots, b_m)$
$g_{2,\bar{b}}(y) := g_2(y, b_2, \ldots, b_m)$

These are univariate deg$<h$ poly and $\forall y \in H$, $\bar{b} \in \mathbb{F}^{m-1}$ $g_{1,\bar{b}}(y) = g_{2,\bar{b}}(y)$

$g_{1,\bar{b}} \equiv g_{2,\bar{b}} \Rightarrow g_1 \equiv g_2$. $\square$

Lemma Given $f \neq g : \mathbb{F}^m \to \mathbb{F}$ of deg$<h$ in each var. (Schwartz-Zippel)

$$P_{x \in \mathbb{F}^m}\left(f(x) = g(x)\right) \leq \frac{(h-1)m}{|\mathbb{F}|}$$

Proof By induction on m.

$m=1$: known.

$(m-1) \to m$: Consider $f_a(x_2, \ldots, x_m)$, $g_a(x_2, \ldots, x_m)$ restrictions of f, g for $a \in \mathbb{F}$.
Let $A = \{a \mid f_a \equiv g_a\}$. Need to prove $|A| < h$ ...

Let us return to the restricted problem.

We are given a poly. $\sum_{ijk} p_{ijk} x_i x_j x_k$

Fix $h = \lg(n+1)$. Let $\mathbb{F}$ be a finite field of size $h^{\Theta(1)}$

Let $H \subset \mathbb{F}$ be an arbitrary set $|H| = h$

$m = \frac{\log(n+1)}{\log\log(n+1)}$

$(1+n) = h^m$

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

The coeff. of P can be described by $p: H^{3m} \to \mathbb{F}$

s.t. $a_1 \ldots a_n$ is a zero for P.

Similarly the prover can write $1, a_1, \ldots, a_n$ as $A: H^m \to \mathbb{F}$

The verifier needs to check $\sum p_{ijk} a_i a_j a_k = 0$, or in other words

$$\sum_{\bar{u}, \bar{v}, \bar{w} \in H^m} p(\bar{u}, \bar{v}, \bar{w}) \cdot A(\bar{u}) \cdot A(\bar{v}) \cdot A(\bar{w}) = 0 \qquad (*)$$

Consider

$\hat{A} = LDE(A)$

$\hat{P} = LDE(P) \Leftarrow$ The verifier can compute

Clearly, $(*)$ and $(**)$ are equivalent

$$\sum_{\bar{u}, \bar{v}, \bar{w} \in H^m} \hat{P}(\bar{u}, \bar{v}, \bar{w}) \cdot \hat{A}(\bar{u}) \hat{A}(\bar{v}) \cdot \hat{A}(\bar{w}) = 0 \qquad (**)$$

Define $\Phi : \mathbb{F}^{3m} \to \mathbb{F}$

$$\Phi(\bar{x}, \bar{y}, \bar{z}) := \hat{P}(\bar{x}, \bar{y}, \bar{z})\, \hat{A}(\bar{x})\, \hat{A}(\bar{y})\, \hat{A}(\bar{z})$$

Verifier expects as proof $\hat{A}$ and Φ (given as truth-tables)

Check:

I $\hat{A}$ is a truth-table of a low deg func. $\leq mh$

Φ is a truth-table of a low deg func. $\leq 6mh$ } low deg test

II ⓐ $\displaystyle\sum_{\bar{u}, \bar{v}, \bar{w} \in H^m} \Phi(\bar{u}, \bar{v}, \bar{w}) = 0$

ⓑ $\forall\, \bar{x}, \bar{y}, \bar{z} \in \mathbb{F}^m \quad \Phi(\bar{x}, \bar{y}, \bar{z}) = \hat{P}(\bar{x}, \bar{y}, \bar{z})\, A(\bar{x})\, A(\bar{y})\, A(\bar{z})$

Note that ⓑ is "robust":

Claim If $\Phi(\bar{x}, \bar{y}, \bar{z}) \equiv \hat{P}(\bar{x}, \bar{y}, \bar{z})\, \hat{A}(\bar{x})\, \hat{A}(\bar{y})\, \hat{A}(\bar{z})$, then ⓑ always holds.

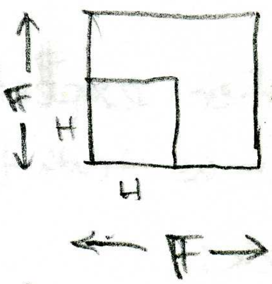
If $-//- \;\not\equiv\; -//-$, then

$$\Pr_{\bar{x}, \bar{y}, \bar{z} \in \mathbb{F}^m}\left(\Phi(\bar{x}, \bar{y}, \bar{z}) = \hat{P}(\bar{x}, \bar{y}, \bar{z})\, \hat{A}(\bar{x})\, \hat{A}(\bar{y})\, \hat{A}(\bar{z}) \right) \leq \frac{6mh}{|\mathbb{F}|}$$

<u>Sum Check</u> Given a degree $\leq d$ function $\Phi : \mathbb{F}^{\ell} \to \mathbb{F}$, $c \in \mathbb{F}$

Check that

$$\sum_{\bar{a} \in H^{\ell}} \Phi(\bar{a}) = c$$



Let $g_i(x_1, \dots, x_i) := \sum_{a_{i+1}, \dots, a_\ell \in H} \Phi(x_1, \dots, x_i, a_{i+1}, \dots, a_\ell)$

$g_0 :\equiv c$

$g_\ell \equiv \Phi$

Assume we get truth tables $\overset{c}{\overset{\shortparallel}{G_0}}, \dots, \overset{\Phi}{\overset{\shortparallel}{G_\ell}}$

Select at random $(r_1, \dots, r_\ell) \in \mathbb{F}^{\ell}$

$$\forall i \qquad G_i(r_1, \dots, r_i) = \sum_{a \in H} G_{i+1}(r_1, \dots, r_i, a)$$

<u>Lemma</u> If $\sum_{\bar{a} \in H^{\ell}} \Phi(\bar{a}) = c$, then $\exists\, G_1, \dots, G_{\ell-1}$ s.t. test passes w.p. 1.

<u>Lemma</u> If $\sum_{\bar{a} \in H^{\ell}} \Phi(\bar{a}) \neq c$, then $\forall\, G_1, \dots, G_{\ell-1}$ <u>low degree functions</u>

$$P(\text{test passes}) \leq \frac{d}{|\mathbb{F}|}$$

Proof Let i be maximal s.t. $G_i \neq g_i$.

i'th test : $G_i(r_1 \ldots r_i) \overset{?}{=} \sum_{a \in H} G_{i+1}(r_1, \ldots, r_i, a) \underset{\substack{\text{maximality} \\ \text{of } i}}{=} \sum_{a \in H} g_{i+1}(r_1, \ldots, r_i, a) \overset{\text{def}}{=} g_i(r_1, \ldots, r_i)$

Since $r_1, \ldots, r_i$ chosen randomly, this accepts w.p $\leq \frac{d}{|\mathbb{F}|}$