Today

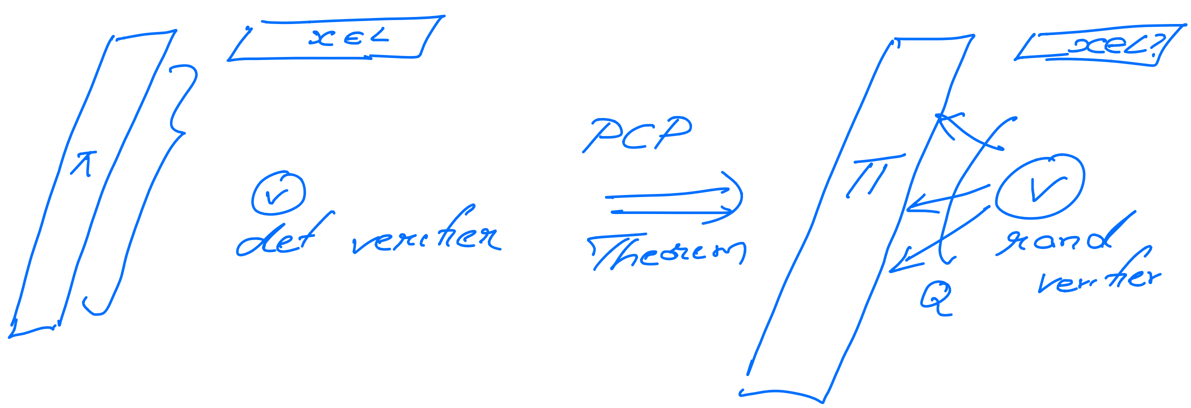
- Proof of the PCP Theorem (a bird's eyeview)

Lecture 27
Computational Complexity (12 May'20)
Instructor: Prahladh Harsha

High level overview of the proof of PCP Theorem

PCP Theorem: $NP \subseteq PCP_{1,\frac{1}{2}}[O(\log n), O(1)]$

(Lecture outline - similar to Bootcamp lecture at Simons).



Key difference: (1) PCP verifier - randomized

(2) PCP verifier - localized.

Locality of Errors.

Abundance of local erro

↳ Smear/spread errors everywhere (use (1) codes).

Warmup Version:

- Membership in Linear Space.

$$\left[A \in \{0,1\}^{m \times n} \right] \left[\quad \right] = \bar{0}$$

$x \; [\quad] \in \{0,1\}^n \rightarrow$ Does x satisfy $Ax = 0$

- Write x in a slightly longer format
exponentially long.

such that it can be easily checked
probing a constant # locations

that $Ax = 0$.

- Main tool: Hadamard Code

$$\text{Had}: \{0,1\}^n \longrightarrow \{0,1\}^{2^n}$$

(locations are indexed by $y \in \{0,1\}^n$)

$$x \longmapsto \{\langle x, y \rangle\}_{y \in \{0,1\}^n}$$

$$\langle x, y \rangle = \sum x_i y_i \pmod 2$$

$y \mapsto \langle x, y \rangle$ (linear fn in $GF(2)$).

2 $\ell_x : y \mapsto \langle x, y \rangle$

Rate: $n \longmapsto 2^n$ $R = \frac{n}{2^n}$

Distance: $x_1 \neq x_2$; $\Pr_y[\mathrm{Had}(x_1)|_y = \mathrm{Had}(x_2)|_y]$

$$= \Pr_y[\langle x_1, y\rangle = \langle x_2, y\rangle]$$

$$= \Pr_y[\langle x_1 - x_2, y\rangle = 0]$$

$$= \tfrac{1}{2}.$$

$f : \{0,1\}^n \to \{0,1\}$. function as a table of values

Claim: $f \equiv \ell_x$ for some (unknown) x.
(ie, it is a Hadamard codeword).

Qn: How does one check this claim?

$f(y_1)$, $f(y_2)$ .. $f(y_n)$
— linearly independent y's.

$\langle x, y_1\rangle$, $\langle x, y_2\rangle$, .. $\langle x, y_n\rangle$
↪ Recover x. & then check for random y
$\langle x, y\rangle = f(y)$.

→ # queries into fn → $n+1$.

$f: \{0,1\}^n \to \{0,1\}$ is linear

$\Updownarrow$

$f(x)+f(y) = f(x+y), \quad \forall x,y \in \{0,1\}^n$

Above characterization is a robust characterization

Local Linearity Test

Input: $f:\{0,1\}^n \to \{0,1\}$ (oracle access)

Test: ① Pick $y, z \in_R \{0,1\}^n$

② Query f at $y, z, y+z$

③ Accept if $f(y)+f(z) = f(y+z)$.

[Extremely local - 3 queries

Completeness: If $f = \ell_x$ for some x.

$$\Pr_{y,z}[\text{Test accepts}] = 1$$

Soundness: [Blum Luby Rubinfeld, BCHKS]

$\forall \delta < 1/2$

$$\Pr[\text{Test accepts}] \geq 1-\delta$$

$$\Downarrow$$

$\exists$ a lin fn ℓ_x for some $x \in \{0,1\}^n$

s.t. $\Pr_y[\ell_x(y) = f(y)] \geq 1-\delta$

(ie, f mostly agrees w/ ℓ_x)

Self-Correction

Suppose f is δ-close to some l_x for some $x \in \{0,1\}^n$ & $\delta < 1/4$.

$$\forall y, \quad \Pr_{z}[l_x(y) = f(y+z) - f(z)] \geq 1 - 2\delta$$

Original Problem:

Give a proof that "$\exists x$ satisfies '$Ax = 0$'".

$x \in \{0,1\}^n$ satisfies

$$\langle a_1, x\rangle = 0$$
$$\langle a_2, x\rangle = 0$$
$$\vdots$$
$$\langle a_m, x\rangle = 0$$
$$a_i \in \{0,1\}^n.$$

Proof: Hadamard Encoding of x.

$f : \{0,1\}^n \to \{0,1\}$

(Honest Case: $f \equiv l_x$)

Verifier: $f : \{0,1\}^n \to \{0,1\}$

(1) (Syntactic Tests)

f is close to linear (linearity test) — 3 query

(2) (Semantic Test)

Pick $b_1 \ldots b_m \in_R \{0,1\}$.

Constr $a = \sum b_i a_i \in \{0,1\}^n$

5 queries

5

Pick $\bar{a}' \in_R \{0,1\}^n$
Query f at $a+a'$, a'
Accept if $f(a+a') - f(a') = 0$.

Completeness: $f \equiv \ell_x$ for some x that satisfies all $\langle a_i, x\rangle = 0$.

- $f \equiv \ell_x$ - linear ✓ syntactic test
- $f(a+a') - f(a') = \ell_x(a+a') - \ell_x(a') =$

$$= \langle a+a', x\rangle - \langle a', x\rangle$$
$$= \langle a, x\rangle$$
$$= \langle \sum b_i a_i, x\rangle$$
$$= \sum b_i \langle a_i, x\rangle = 0$$

✓ Prob w/ 1.

Soundness: Suppose f satisfies.

$$\Pr[\mathrm{Ver}^f \text{ acc}] \geq \frac{99}{100}$$
$$\Downarrow$$

$\exists\, x$ st f $\frac{1}{100}$-close to ℓ_x & furthermore x satisfies all the equations.

Pf: f is not close to linear
- then syntactic test captures this.

f is close to linear (say some ℓ_x)
but x does not satisfy all the linear eqns $\langle a_i, x\rangle = 0$.

Then, w/ prob $\frac{1}{2}$ x does not satisfy $\langle a, x\rangle = 0$.

$$\ell_x(a) \neq 0$$

$$\Pr_{a'}\left[\ell_x(a) = f(a+a') - f(a')\right] \geq 1 - 2\cdot\frac{1}{100}$$

Warmup $\longrightarrow$ General:

"Vector space has a non-zero member"

$\exists\, x,$ st
$$\left.\begin{aligned}\langle a_1, x\rangle &= 0\\ \langle a_2, x\rangle &= 0\\ &\vdots\\ \langle a_m, x\rangle &= 0\end{aligned}\right\} \text{linear eqns}$$

Gen: $\exists\, x$ st $\underbrace{\sum_{i,j} a_{ij}^{(k)} x_i x_j = 0}_{\text{quadratic eqns.}}$; $k = 1 \ldots m$

Hadamard: $\ell_x : y \mapsto \langle x, y\rangle$.
- evaluation of the linear fn ℓ_x.
- for every lin fn ℓ_y eval of ℓ_y at the pt x.

Quad Code: Evaluation of every quad fn at the point x.
(there are $2^{O(n^2)}$ quad fns)

PCP Verifier: $f: \{0,1\}^{n^2+n+1} \to \{0,1\}$ } Exponential long.

(1) Syntactic Test
Check that f is close to codeword of ~~some~~ quad code

(2) Semantic Test

- 15 queries.

$NP \subseteq PCP_{1, \frac{99}{100}}[n^2, 15]$.

- # queries $= O(1)$
- randomness $= O(n^2)$
(for a PCP - $O(\log n)$).

Exponentially long proof $\to$ Poly sized proof

$O(n^2)$ - randomness $\to O(\log n)$ randomness

Exponential sized proof - Hadamard Code.
$\to$ If they were a code w/ better rate, locally testable

Reed-Muller Code: Eval of multivariate low deg poly

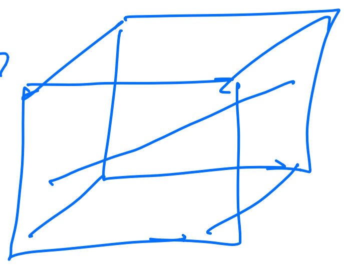
finite field $\mathbb{F} = GF(q)$ $\quad q = p^r$.

d - degree parameter $\quad p^r$ - large number

m = # variables.

$$RM_{\mathbb{F}}[m, d] = \{ Eval(p) \,/\, p : \mathbb{F}^m \to \mathbb{F},\ deg(p) \le d \}$$

$\mathbb{F}^m$



$f : \mathbb{F}^m \to \mathbb{F}$

f - evaluations of low degree polynomials

Properties:

① Distance:

(Univariate). $p \not\equiv 0$ (p is a non-zero deg d poly)

$$\Pr_{x \in \mathbb{F}} [p(x) = 0] \le \frac{d}{|\mathbb{F}|}$$

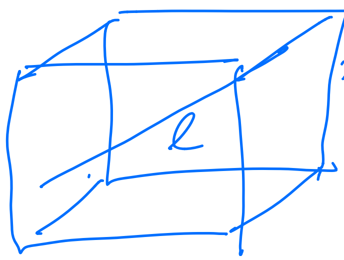
(Multivariate) SZ Lemma.

$p \not\equiv 0$ is a non-zero m-variate deg d polynomial

$$\Pr_{(x_1 \ldots x_m) \in \mathbb{F}^m} [p(x_1 \ldots x_m) = 0] \le \frac{d}{|\mathbb{F}|}$$

② Testability

Restriction of a low-degree fn to a line is also low-degree.



$f : \mathbb{F}^m \to \mathbb{F}$

Low-Degree Test

Input: $f : \mathbb{F}^m \to \mathbb{F}$ (oracle)

$m, d, \mathbb{F}$ (explicit inputs)

1. Pick a random ℓ in $\mathbb{F}^m$
2. Query f on all pts on ℓ
3. Accept if $f|_\ell$ is a univariate deg d polynomial.

<u>Comp</u>: $p : \mathbb{F}^m \to \mathbb{F}$ is of deg $\leq d$

$$\Downarrow$$

$$\Pr_{\ell}[LDT^{p} \text{ acc}] = 1$$

Soundness: $\exists\, \delta_0 = \delta_0(m, d, \mathbb{F})$ s.t. $\forall\, \delta \leq \delta_0$

$$\Pr[LDT^{f} \text{ acc}] \geq 1 - \delta$$

$$\Downarrow$$

$\exists$ a poly $p : \mathbb{F}^m \to \mathbb{F}$ of deg d, s.t.

$$\Pr_{x}[p(x) = f(x)] \geq 1 - O(\delta).$$