Today
- Proof of the PCP Theorem

Lecture 28
Computational Complexity
(14 May 2020)
Instructor: Prahladh Harsha

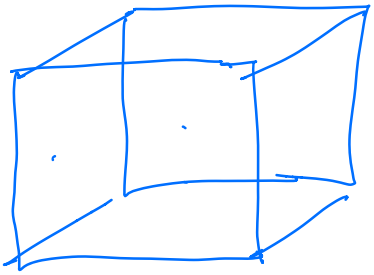
Today: $NP \subseteq PCP_{1, 0.99}[O(\log n), \log^2 n]$

gap ✓ randomness ✓ #queries (not constant)

Main Technical Ingredient:

Reed-Muller & its local testability.

RM code: $\mathbb{F}$ - finite field
d - degree
m - #variables



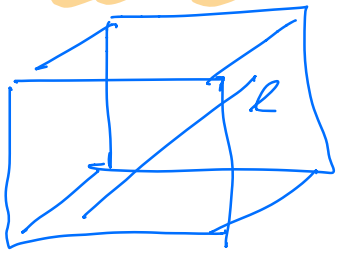
$RM_{\mathbb{F}}[m,d] = \{Eval(p) \mid p$ is a m-variate deg d poly$\}$.

$Eval(p)$: $\underbrace{p: \mathbb{F}^m \to \mathbb{F}}_{\text{table of evaluations of } p}$

Properties

① Distance: $p \neq 0$ $\quad \Pr_{x \in \mathbb{F}^m}[p(x)=0] \leq \frac{d}{|\mathbb{F}|}$

(2) Testability



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

Test:

1. Pick a random line ℓ in $\mathbb{F}^m$
2. Query f on ℓ
3. Accept if f_ℓ is a univariate poly

Soundness

$\exists\ \delta_0 = \delta_0(m, d, |\mathbb{F}|)$ s.t.

$\forall\ \delta < \delta_0$, $\forall\ f: \mathbb{F}^m \to \mathbb{F}$

$\Pr_\ell[\text{LDT}^f \text{ acc}] \geq 1 - \delta \Rightarrow \exists$ a $p \in \text{RM}[m,d]$ s.t. $\delta(f,p) \leq \alpha(\delta)$

3. Interpolation

(Univariate): $S \subseteq \mathbb{F}$; $f: S \to \mathbb{F}$

$\exists$ a unique poly $p: \mathbb{F} \to \mathbb{F}$ of deg $< |S|$ s.t.

$p(\alpha) = f(\alpha) \quad \forall \alpha \in S$.

(Multivariate). $S \subseteq \mathbb{F}$; $f: S^m \to \mathbb{F}$

$\exists$ a (unique) $p: \mathbb{F}^m \to \mathbb{F}$ of individual degree less than $|S|$ in each var

s.t. $p(\alpha) = f(\alpha) \quad \forall \alpha \in S^m$

(Hence p is of total degree $< m|S|$) (not unique).

Equipped w these properties of RM

$NP \subseteq PCP_{1,0.99}[O(\log n), \log^2 n]$.

In particular, 3COL has such a PCP.

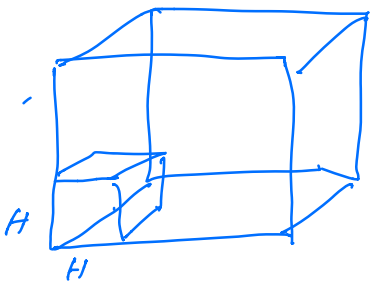
3COL: Instance: $G = (V, E)$ undirected.

YES: $\exists$ a 3-coloring of vertices s.t. no edge is monochromatic.

NO: $\nexists$ a 3-coloring ...

NP proof: $A: V \to \{0,1,2\}$ a candidate 3-coloring.

Arithmetize the 3col problem



Let $H \subseteq \mathbb{F}$ s.t. $|H|^m = n$ (#vertices in the graph)

Identify $V \cong H^m$

$E: V \times V \to \{0,1\}$ (symmetric $\exists$)

((($E: H^m \times H^m \to \{0,1\}$ (symmetric $\exists$)

Interpolation / (low-degree) extension

$\hat{E}: \mathbb{F}^m \times \mathbb{F}^m \to \mathbb{F}$ s.t. $\forall (i,j) \in H^{2m}$ $\hat{E}(i,j) = E(i,j)$

s.t $\deg(\hat{E}) \leq 2m|H|$

- Arithmetized the edge $\hat{E}$ (above)
- Arithmetize the "proof".

NP-proof: $A: V \to \{0,1,2\}$

$A: H^m \to \{0,1,2\}$

↓ Interpolation / LDE

$\hat{A}: \mathbb{F}^m \to \mathbb{F}$ (s.t $\hat{A}(i) = A(i)$ $\forall i \in H^m$).

$\deg(\hat{A}) \leq m|H|$.

New PCP proof. $\hat{A}: \mathbb{F}^m \to \mathbb{F}$

(Verifier needs to check that $\hat{A}$ in fact encodes a valid 3-coloring A).

- For all edges $(i,j) \in E$

$A(i) - A(j) \neq 0$ (or in other words $\in \{1, 2, -1, -2\}$)

or equivalently

$E(i,j)(A(i)-A(j)-1)(A(i)-A(j)-2)(A(i)-A(j)+1)(A(i)-A(j)+2) = 0$

In the arithmetized world $\forall (i,j) \in V \times V$

(A)... $\hat{E}(i,j)(\hat{A}(i)-\hat{A}(j)-1)(\hat{A}(i)-\hat{A}(j)-2)\ldots = 0$ $\forall (i,j) \in H^m \times H^m$

Proof: $\hat{A}: \mathbb{F}^m \to \mathbb{F}$ instead of $A: H^m \to \{0,1,2\}$

(**) $\hat{A}(i) \in \{0,1,2\}$, $\forall i \in H^m$

$\hat{A}(i)(\hat{A}(i)-1)(\hat{A}(i)-2) = 0 \quad \forall i \in H^m$

NP

Instance $G = (V, E)$

$E: V \times V \to \{0,1\}$

Proof: $A: V \to \{0,1,2\}$

Verification: $\forall (i,j) \in E$

$A(i) - A(j) \neq 0$

PCP

$\hat{E}: \mathbb{F}^m \times \mathbb{F}^m \to \mathbb{F}$

$\deg(\hat{E}) \leq 2m|H|$

$\hat{A}: \mathbb{F}^m \to \mathbb{F}$

$\deg(\hat{A}) \leq m|H|$

(*) $\hat{E}(i,j) \prod_{b \in \{\pm 1, \pm 2\}} (\hat{A}(i) - \hat{A}(j) - b) = 0 \quad \forall (i,j) \in H^{2m}$

(**) $\hat{A}(i)(\hat{A}(i)-1)(\hat{A}(i)-2) = 0 \quad \forall i \in H^m$

PCP proof: $\hat{A}: \mathbb{F}^m \to \mathbb{F}$

$\tilde{A} \triangleq \hat{A}(z)(\hat{A}(z)-1)(\hat{A}(z)-2)$

$\tilde{A}: \mathbb{F}^m \to \mathbb{F}$

$C(x,y) \triangleq \hat{E}(x,y) \prod_{b \in \{\pm 1, \pm 2\}} (\hat{A}(x) - \hat{A}(y) - b)$

$C: \mathbb{F}^{2m} \to \mathbb{F}$

Verifier Checks: (Instance: $\hat{E}: \mathbb{F}^{2m} \to \mathbb{F}$)

Proof: $\hat{A}: \mathbb{F}^m \to \mathbb{F}$
$\tilde{A}: \mathbb{F}^m \to \mathbb{F}$
$C: \mathbb{F}^{2m} \to \mathbb{F}$
} provided by prover as table of values.

(1) [Syntactic Tests]
LDT for each of $\hat{A}, \tilde{A}, C$ of deg $O(m|H|)$.

(2) [Semantic Tests]

(a) $\tilde{A}$ & C are consistently defined from $\hat{A}$.

Pick a random $z \in_R \mathbb{F}^m$ & $(x,y) \in_R \mathbb{F}^{2m}$

$$\tilde{A}(z) = \hat{A}(z)\left(\hat{A}(z)-1\right)\left(\hat{A}(z)-2\right).$$

$$C(x,y) = \hat{E}(x,y)\prod\left(\hat{A}(x)-\hat{A}(y)-b\right)$$

(b). Zero Testing.
[i.e. the true polynomials $\tilde{A}$ & C are close to vanishing on H^m & H^{2m} respectively.]

Zero-Testing

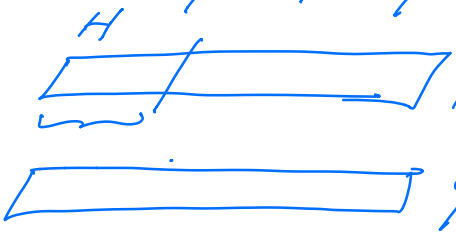
Univariate: $p: \mathbb{F} \to \mathbb{F}$ – deg d.

$p|_H \equiv 0$. $\quad |H| \le d$.

Claim: $p|_H \equiv 0 \iff p(x)$ is a multiple of $\prod_{h \in H}(x-h)$

i.e. $p(x) = q(x) \underbrace{\prod_{h \in H}(x-h)}_{Z_H(x)}$

$$p(x) = q(x) \cdot Z_H(x).$$



} proof

$p(x) = q(x) \cdot Z_H(x)$ for random $x \in F$

Multivariate Version:

$p : F^m \to F$ of deg $\le d$ vanishes on H^m

$\Updownarrow$

$\exists$ polynomials $Q_1, \dots, Q_m : F^m \to F$ of deg $\le d - |H|$

s.t.

$$p(x_1, \dots, x_m) = Q_1(x_1, \dots, x_m) Z_H(x_1) + Q_2(x_1, \dots, x_m) Z_H(x_2) + \vdots + Q_m(x_1, \dots, x_m) \cdot Z_H(x_m)$$

Proof that $p|_{H^m} \equiv 0$.

$Q_1 \ldots Q_m : \mathbb{F}^m \to \mathbb{F}$

- LDT of $Q_1 \ldots Q_m$
- Pick a random pt $z \in \mathbb{F}^m$

$$p(z) = \sum z_H(z_i) \cdot Q_i(z).$$

Recap Entire Proof

Proof: $\hat{A} : \mathbb{F}^m \to \mathbb{F}$

$\tilde{A} : \mathbb{F}^m \to \mathbb{F}$ $(Q_1 \ldots Q_m : \mathbb{F}^m \to \mathbb{F})$

$C : \mathbb{F}^{2m} \to \mathbb{F}$ $(Q_1' \ldots Q_{2m}' : \mathbb{F}^{2m} \to \mathbb{F})$

Verifier Check

(1) Syntactic Test:
Check all tables are low-degree (LDT)

(2) Semantic Test

(a) Consistency of $\tilde{A}$ & C:

$z \in_R \mathbb{F}^m$; $(x, y) \in_R \mathbb{F}^{2m}$

$$\tilde{A}(z) = (\hat{A}(z))(\hat{A}(z)-1)(\hat{A}(z)-2).$$

$$C(x,y) = E(x,y) \prod (\hat{A}(x) - \hat{A}(y) - b)$$

⑥ Zero Testing

$\forall z \in \mathbb{F}^m$, $(x, y) \in \mathbb{F}^{2m}$

$$\tilde{A}(z) = \sum Q_i(z) Z_H(z_i)$$

$$C(x, y) = \sum Q_i'(x, y) Z_H((xy)_i).$$

Randomness: $O(m \log |\mathbb{F}|)$

#Queries: $O(m) \cdot O(|\mathbb{F}|) = O(m|\mathbb{F}|)$.

Completeness: $c = 1$ (honest prover).

Soundness: $s \le 0.99$. (soundness of LDT + 52 extra)

$$\frac{d}{|\mathbb{F}|} = \frac{O(m|H|)}{|\mathbb{F}|}$$

Parameter Setting: $|H|^m = n$

$$m = \frac{\log n}{\log \log n}, \quad |H| = \text{poly} \log n \Rightarrow |H|^m = n.$$

$$d = O(m|H|) = O(\text{poly} \log n)$$

$$|\mathbb{F}| = 100d = O(\text{poly} \log n).$$

Randomness: $O(m \log |\mathbb{F}|) = \frac{\log n}{\log \log n} \log(\log n) = O(\log n)$

#Queries: $O(m|\mathbb{F}|) = \text{poly} \log n$.

Thus $3COL \in PCP_{1,0.99}[O(\log n), \text{polylog}]$

PCP Theorem is obtained by "composing" above PCP w/ itself twice. & then w/ the constant-query PCP (from lecture).

Randomness:

$O(\log n)$	$O(\log n)$
$+$	
$\log(\text{polylog}(n))$	$O(\log\log n)$
$+$	
$O((\text{polylog}\log n)^2)$	$o(\log n)$
	$O(\log n)$