Today

- Low Degree Testing III (Friedl-Sudan)
- PCPs from LDT.

CSS.330.1 : PCPs
Limits of Approximation Algorithms

Lecture 05 (2023-2-24)

Instructor: Prahladh Harsha

Recall from last time.

Input: $\mathbb{F}$ - field, m - dimension, d - degree $\Big\}$ explicit

$f : \mathbb{F}^m \to \mathbb{F}$, $F : \{\text{lines}\} \to RS_{\mathbb{F}}(d)$ $\Big\}$ oracle access

Low-Degree Test:

(1) Pick $x \in_R \mathbb{F}^m$; $h \in_R \mathbb{F}^m$; $\ell = \{x + th \mid t \in \mathbb{F}\}$

(2) Query f on x & F on ℓ

(3) Accept if $F(\ell)(x) = f(x)$.

Thm [Friedl-Sudan].

$\forall \varepsilon \in (0,1)$, $\exists\, c > 0$ s.t. $|\mathbb{F}| > cd$, if f & F

$\Pr_{x,h}[f(x) \neq F(\ell)(x)] \leq \delta < 1/8 - \varepsilon$

Then $\exists\, P \in \text{Lifted-}RS_{\mathbb{F}}(m,d)$ s.t. $\delta(f, P) \leq 2\delta$.

Reed Muller(d): Evaluation of multivariate poly of deg $\leq d$ over $\mathbb{F}^m$

$RM_{\mathbb{F}}(m, d)$

Lifted-$RS_{\mathbb{F}}(m, d)$: $\{ f : \mathbb{F}^m \to \mathbb{F} \mid \forall$ lines in $\mathbb{F}^m$ $f|_\ell \in RS_{\mathbb{F}}(d) \}$.

Lemma [Friedl-Sudan] $\mathbb{F}$ - finite field of size $q = p^k$ (p-prime)
If $d < q - q/p$ then
$$\text{Lifted-}RS_{\mathbb{F}}(m, d) = RM_{\mathbb{F}}(m, d).$$

FS Thm is true for any F given f

So, one might as well work w/ the best fit F

$$P^{(f,d)}(\ell) = \underset{g \in RS_{\mathbb{F}}(d)}{\operatorname{argmin}} \; \delta(f|_\ell, g).$$

Hypothesis of FS: $\Pr_{x,h}[f(x) \neq P^{(f,d)}(\ell)(x)] \leq \delta.$

$$\delta_f(\ell) \triangleq \Pr_{x \sim \ell}[f(x) \neq P^{(f,d)}(\ell)(x)]$$
$$\delta_f \triangleq \Pr_{x,h}[f(x) \neq P^{(f,d)}(\ell)(x)]$$

$$\delta_f = \mathbb{E}_{\ell}[\delta_f(\ell)].$$

FS Hypothesis: $\delta_f \leq \delta$.

Self-Correction of f:

$$f_{corr} : \mathbb{F}^m \to \mathbb{F}$$

$$\forall x \in \mathbb{F}^m \; ; \; f_{corr}(x) = \underset{h \in \mathbb{F}^m}{\text{plurality}} \left\{ P^{(f,d)}(x+th)(x) \right\}$$

Claim 1: $\delta(f, f_{corr}) \leq 2\delta_f$ [Similar to BLR setting].

Claim 2: $\forall \varepsilon \in (0,1)$, $\exists c$, $|\mathbb{F}| > cd$. & $\delta_f < 1/8 - \varepsilon$.

then $\delta_{f_{corr}} < \delta_f / 2$.

(Claim 1 & 2 $\Rightarrow$ FS Theorem).

Lemma [Friedl-Sudan]

If $\delta_f < 1/8 - \varepsilon$

$$\Pr_{x, h_1, h_2} \left[P^{(f,d)}(x+th_1)(x) \neq P^{(f,d)}(x+th_2)(x) \right] \leq 4\alpha\delta_f$$

where $\alpha = 4/\varepsilon^2|\mathbb{F}|$.

(Lemma $\Rightarrow$ Claim 2) if $4\alpha < 1/2$.

$$\delta_{f_{corr}} = \Pr_{x,h}\left[f_{corr}(x) \neq P^{(f_{corr},d)}(x+th)(x)\right]$$

$$\leq \Pr_{x,h}\left[f_{corr}(x) \neq P^{(f,d)}(x+th)(x)\right]$$

$$\leq \Pr_{x,h,h'}\left[P^{(f,d)}(x+th)(x) \neq P^{(f,d)}(x+th')(x)\right]$$

Lemma: States if

Rej (lines-point) $< 1/8 - \varepsilon$

then

Rej (lines-lines) $< 4\alpha \cdot \mathrm{Rej}$ (lines-point)

Workhorse for the proof of lemma:

Polishchuk-Spielman Axis Parallel Low Degree Test

$\forall \varepsilon \in (0,1)$, $\exists c > 0$; $|\mathbb{F}| > cd$. &

$\mathcal{R}_i$ & $\mathcal{G}_j$ are 2 families of degree d poly as $i \in \mathbb{F}$, & $j \in \mathbb{F}$

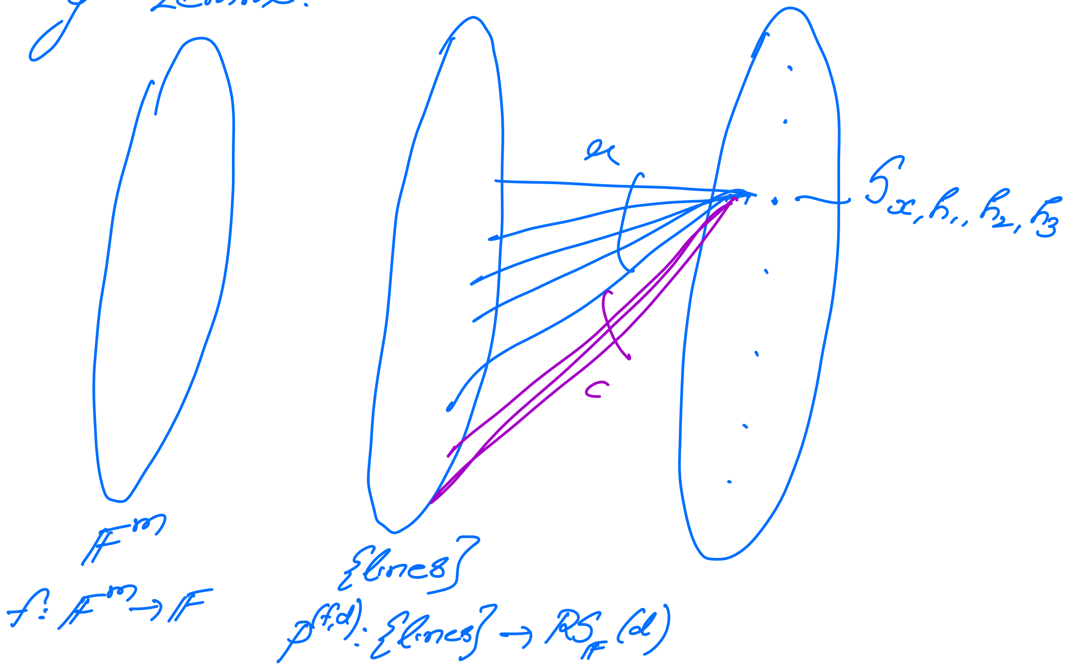
$$\Pr_{ij \in \mathbb{F}\times\mathbb{F}}\left[\mathcal{R}_i(j) \neq \mathcal{G}_j(i)\right] \leq 1/4 - \varepsilon$$

$$\Downarrow$$

$\exists$ bivariate poly $Q(X,Y)$ of ind deg d (in either var)

$\Pr_i\left[\mathcal{R}_i(\cdot) \neq Q(i,\cdot)\right] \leq 1/4$ & $\Pr_j\left[\mathcal{G}_j(\cdot) \neq Q(\cdot,j)\right] \leq 1/4$

Proof of Lemma:



$$S_{x,h_1,h_2,h_3} = \{x + ih_1 + jh_2 + ijh_3 \mid i,j \in \mathbb{F}\}$$

Given S_{x,h_1,h_2,h_3}, $\quad i, j \in \mathbb{F}$

$$row_i = \{x + ih_1 + j(h_2 + ih_3) \mid j \in \mathbb{F}\}$$

$$col_j = \{x + jh_2 + i(h_1 + jh_3) \mid i \in \mathbb{F}\}$$

$$r_i(\cdot) = P^{(f,d)}(row_i) \qquad \Big| \quad m(i,j) = f(x + ih_1 + jh_2 + ijh_3)$$

$$c_j(\cdot) = P^{(f,d)}(col_j)$$

Recall we want to prove

$$\Pr_{x,h_1,h_2,h_3}\left[c_0(0) \neq r_0(0)\right] \leq 4\alpha\delta_f$$

Consider the following 4 (bad) events for a random x, h_1, h_2, h_3

E1: "$\mathbb{E}_{c \in \mathbb{F}}\left[\delta(\text{row}_c)\right] \geq \frac{1}{8} - \frac{\varepsilon}{2}$"

E2: $\mathbb{E}_{j \in \mathbb{F}}\left[\delta(\text{col}_j)\right] \geq \frac{1}{8} - \varepsilon/2$

E3: $\Pr_{c \in \mathbb{F}}\left[x_i(0) \neq m(i,0)\right] \geq \frac{1}{8} - \frac{\varepsilon}{2}$

E4: $\Pr_{j \in \mathbb{F}}\left[g_j(0) \neq m(0,j)\right] \geq \frac{1}{8} - \varepsilon/2.$

Suffices to show the following

(a) $\forall k \quad \Pr[E_k] \leq \alpha \delta_f$

(b) $\neg E_1 \wedge \neg E_2 \wedge \neg E_3 \wedge \neg E_4 \Rightarrow x_0(0) = c_0(0).$

Proof of (b):

$$\neg E_1 \wedge \neg E_2 \Rightarrow \Pr_{i,j}\left[x_i(j) \neq g_j(i)\right] \leq \frac{1}{8} - \frac{\varepsilon}{2} + \frac{1}{8} - \frac{\varepsilon}{2} = \frac{1}{4} - \varepsilon.$$

Hence, PS hypothesis is true

$\exists\ Q(i,j)$ of ind deg $\leq d$ s.t.

$$\Pr_i\left[Q(i,\cdot) \not\equiv x_i(\cdot)\right] \leq 1/4$$

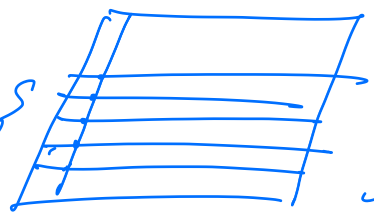
& similarly for columns.

$\neg E_3$: $\Pr_{i \in \mathbb{F}}\left[m(i,0) = r_i(0) = Q_i(i,0)\right]$

$$\geq \frac{3}{4} - \left(\frac{1}{8} - \frac{\varepsilon}{2}\right)$$

Hence $c_0(\cdot) \equiv Q(\cdot, 0)$.

$\# j \geq \left(\frac{3}{4} - \left(\frac{1}{8} - \frac{\varepsilon}{2}\right)\right)|\mathbb{F}|$ i



0

$m(i,0) = Q(i,0)$

Hence, $c_0(\cdot) \equiv Q(\cdot, 0)$

(since $c_0(\cdot)$ is the best fit poly for col_0.

Similarly $\neg E_4$ (w/ $\neg E_1 \wedge \neg E_2$) $\Rightarrow$ $r_0(\cdot) \equiv Q(0, \cdot)$

Hence, $\neg E_1 \wedge \neg E_2 \wedge \neg E_3 \wedge \neg E_4$

$$\Rightarrow r_0(0) = Q(0,0) = c_0(0)$$

(Proof of (b).) $\boxtimes$

Proof of (a).

$$\mathbb{E}_{x, h_1, h_2, h_3}\left[\mathbb{E}_i\left[\delta(row_i)\right]\right] = \delta_f$$

<u>Observation</u>: Fix $i_1 \neq i_2$

random x, h_1, h_2, h_3

$$row_{i_1} = \{x + i_1 h_1 + j(h_2 + i_1 h_3) \mid j \in \mathbb{F}\}$$

$$row_{i_2} = \{x + i_2 h_1 + j(h_2 + i_2 h_3) \mid j \in \mathbb{F}\}$$

row_{c_1} & row_{c_2} are independent random lines (for random x, h_1, h_2, h_3)

$$(x + c_1 h_1,\ x + c_2 h_1,\ (h_2 + c_1 h_3),\ (h_2 + c_2 h_3))$$

$$= (x, h_1, h_2, h_3) \begin{bmatrix} 1 & 1 & 0 & 0 \\ c_1 & c_2 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & c_1 & c_2 \end{bmatrix}$$

Hence $\{\delta(row_c) \mid c \in \mathbb{F}\}$ are pairwise indep

$$\mathbb{E}_{x, h_1, h_2, h_3, c}[\delta(row_c)] = \delta_f < \frac{1}{8} - \varepsilon$$

$$\Pr_{x, h_1, h_2, h_3}\left[\frac{\sum_{c \in \mathbb{F}} \delta(row_c)}{|\mathbb{F}|} \geq \frac{1}{8} - \frac{\varepsilon}{2}\right] \leq \alpha \delta_f (1 - \delta_f)$$

where $\alpha = \frac{4}{\varepsilon^2 |\mathbb{F}|}$

Hence $\Pr[E1] \leq \alpha \delta_f$.

Similarly $E2$.

$E3$: $\Pr_i[r_i(0) \neq m(i, 0)] \geq \frac{1}{8} - \frac{\varepsilon}{2}$

Argument is similar as above as for $c_1 \neq c_2$ $(row_{c_1}, row_{c}(0))$ & $(row_{c_2}, row_{c_2}(0))$

are independent line-point pairs.

Part II: PCPs from LDT

Recap:

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

If there exists a $F: \{\text{lines}\} \to RS_{\mathbb{F}}(d)$

$$\Pr_{x,h}[f(x) \neq F(x+th)(x)] < \delta$$

$$\Downarrow$$

$\exists \; P \in RM_{\mathbb{F}}(m,d)$ s.t. $\delta(f,P) < 4\delta$.

(assuming $|\mathbb{F}| > cd$ & $\delta < 1/10$)

Alternate LDT^f (no lines oracle).

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

Test: (1) Pick a random line ℓ

(2) Query f on all points of ℓ

(3) Accept if $f|_\ell \in RS_{\mathbb{F}}(d)$.

Completeness: Trivial

Soundness: $\delta(f, RM_{\mathbb{F}}(m,d)) \geq \delta \overset{??}{\Rightarrow} \Pr[LDT^f \text{ rejects}] \geq \Omega(\delta)$.

$\mathbb{E}[\mathbb{1}[\text{Test rej}]]$

The lines-point analysis of LDT yields the following stronger stmt

Robust Soundness

$$\delta(f, RM_{\mathbb{F}}(m,d)) \geq \delta \Rightarrow \mathbb{E}_{x,h}\left[\delta(f|_{x+th}, RS_{\mathbb{F}}(d))\right] \geq \delta/4.$$

$\mathbb{E}[\delta(\text{local}, \text{ACCEPTING})]$

Zero-on-Subcube Test

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

LDT: Distinguish
- $f \in RM_{\mathbb{F}}(m,d)$
- $\delta(f, RM_{\mathbb{F}}(m,d)) \geq \delta$

$H \subseteq \mathbb{F}$

$$ZRM_{\mathbb{F}}(m,d,H) = \{f \in RM_{\mathbb{F}}(m,d) \mid f|_{H^m} = 0\}$$

$f: \mathbb{F}^m \to \mathbb{F}$
- $\to f \in ZRM_{\mathbb{F}}(m,d,H)$
- $\to \delta(f, ZRM_{\mathbb{F}}(m,d,H)) \geq \delta$.

<u>Observation:</u> $P \in RM_{\mathbb{F}}(m,d)$; $H \subseteq \mathbb{F}$

$P|_{H^m} \equiv 0 \iff \exists\, Q_1, \ldots Q_m \in RM(m,d)$ s.t

$$P(X) \equiv \sum_{i=1}^{m} Q_i(X)\, Z_H(X_i)$$

where $Z_H(Y) = \prod_{h \in H} (Y-h)$

The following is a PCP for the Zero-on-SubCube Problem

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

Proof: $q_1, \ldots, q_m : \mathbb{F}^m \to \mathbb{F}$

Zero-on-Subcube Test

(1) Pick a random ℓ

Checks $f|_\ell, q_1|_\ell, \ldots, q_m|_\ell \in RS_{\mathbb{F}}(d)$.

(2) For all pts x in ℓ

check

$$f(x) = \sum_{i=1}^{m} q_i(x)\, Z_H(x_i)$$

Soundness: $|\mathbb{F}| > O(d, |H|)$

$$\delta(f, ZRM_{\mathbb{F}}(m,d,H)) > \delta \implies \Pr[\text{Zero-on-Subcube Test rejects}] \geq \Omega(\delta) - \frac{d+|H|}{|\mathbb{F}|}$$

PCPs for 3COLOR (using LDT)

3COLOR:

Instance: $G = (V, E)$

YES: $\exists\, c : V \to \{0,1,2\}$ st

$\forall \{u,v\} \in E,\ c(u) \neq c(v)$

NO: Such a 3-coloring does not exist.

"Encode the coloring using a PCP"

Arithmetization:

Choose a field $\mathbb{F}$, m, $S \subseteq \mathbb{F}$

- $S^m = V$

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

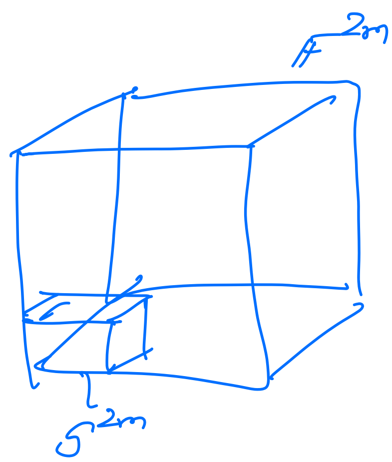
Low-degree extension

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

$\deg_i(\hat{E}) \leq |S|$

- $\hat{E}|_{S^m \times S^m} = E$

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



(2) $C: S^m \to \{0,1,2\}$

$\hat{C}: \mathbb{F}^m \to \mathbb{F}$ (Low-degree extension of C)

Expect as proof : $C: \mathbb{F}^m \to \mathbb{F}$

(purportedly the low-degree extension of a valid 3-coloring).

Need to check

(1) $\forall x \in S^m$, $c(x) \in \{0, 1, 2\}$

$f = (C-0)(C-1)(C-2)$

$f|_{S^m} \equiv 0$

} it is a 3-coloring

(2) $\forall (u,v) \in S^m \times S^m$

$g: \mathbb{F}^m \times \mathbb{F}^m \to \mathbb{F}$

$$g(x,y) = E(x,y)(c(x)-c(y)-1)(c(x)-c(y)+1)(c(x)-c(y)-2)(c(x)-c(y)+2).$$

$g|_{S^m \times S^m} \equiv 0.$

PCP Proof: $C : \mathbb{F}^m \to \mathbb{F}$ (purported LDE of a valid 3-coloring)

$Q_1 \dots Q_m : \mathbb{F}^m \to \mathbb{F}$ (additional poly to check that $f|_{S^m} \equiv 0$)

$P_1 \dots P_{2m} : \mathbb{F}^{2m} \to \mathbb{F}$ (poly reqd to check $g|_{S^{2m}} \equiv 0$)

Verifier:

(1) Pick ℓ in $\mathbb{F}^m$, ℓ' in $\mathbb{F}^{2m}$

(2) Query $C, Q_1, \dots Q_m$ on ℓ
  & reject if any restriction is not low-degree

(3) Query $P_1 \dots P_{2m}$ on ℓ'
  & reject if any restriction is not low-degree

(4) For each $z \in \ell$, reject if

$$(C(z)-1)(C(z)-2)(C(z)-3)) \neq \sum_{i=1}^{m} Q_i(z) Z_S(z_i)$$

(5) For each $\underset{(x', y')}{z'} \in \ell'$, reject if

$$E(z') \cdot (\quad) (\quad) (\quad) (\quad) \neq \sum_{i=1}^{2m} P_i(z') Z_S(z_i')$$

Next lecture: 1. Quantitave Analysis of above PCP

2. PCP Composition.

3. Proof of PCP Theorem.