Today

- Low Degree Testing II
  - * Polishchuk-Spielman
  - * Friedl-Sudan

CSS. 330.1 : PCPs

Limits of Approximation Algorithms

Lecture 04 (2023-2-17)

Instructor: Prahladh Harsha

Recall the setup from last lecture

$\mathbb{F}$ - finite field.

$U, V \subseteq \mathbb{F}$; $|U| = m$; $|V| = n$

$R(X,Y)$ - row polynomial . degree (d,n)-poly

$C(X,Y)$ - col polynomial degree (m,e)-poly

$$\Pr_{(u,v) \leftarrow U \times V} [R(u,v) \neq C(u,v)] \leq \eta$$

$\Downarrow$????

$\exists$ deg (d,e)-polynomial Q

$$\Pr_{(u,v)} [R(u,v) \neq Q(u,v) \text{ or } C(u,v) \neq Q(u,v)] \leq O(\eta)$$

Step 1: Error locator polynomial.

$\eta = \mu^2$. $\exists$ poly E $(\mu m, \mu n)$-deg.

s.t $\forall (u,v)$, $R(u,v)E(u,v) = C(u,v)E(u,v)$
$=: P(u,v)$

P $\quad$ deg $(d+\mu m, e+\mu n)$ $\left(\begin{array}{l} m > d+\mu m \\ n > e+\mu n \end{array}\right)$

Step 2: (*) For each $u \in U$

$$\frac{P(u,Y)}{E(u,Y)} = \underbrace{C(u,Y)}_{\le \text{ deg } e \text{ poly.}}$$

(*) For each $v \in V$

$$\frac{P(X,v)}{E(X,v)} = \underbrace{R(X,v)}_{\le \text{ deg } d \text{ poly.}}$$

Polishchuk-Spielman Lemma:

$U, V \subseteq \mathbb{F}$, $|U| = m$; $|V| = n$.

P, E are 2 bivariate poly of deg $(\alpha m + \delta m, \beta n + \varepsilon n)$ & $(\alpha m, \beta n)$ respectively

- For all $u \in U$, $\frac{P(u,Y)}{E(u,Y)}$ – deg $\le \varepsilon n$ poly

- For all $v \in V$, $\frac{P(X,v)}{E(X,v)}$ – deg $\le \delta m$ poly.

$\alpha + \beta + \delta + \varepsilon < 1$

$\Downarrow$

$\exists$ Q of deg $(\delta m, \varepsilon n)$. $\quad P(X,Y) \equiv Q(X,Y)E(X,Y)$

Pf: Wlog assumptions

(from last time)
$$\begin{cases} - \ \deg_x(P) = (\alpha+\delta)m \ \ \& \ \ \deg_x(E) = \alpha m \\ - \ \deg_Y(P) = (\beta+\varepsilon)n \ \ \& \ \ \deg_Y(E) = \beta n \\ - \ \gcd(P,E) = 1 \end{cases}$$

Need to show E is constant (subsequent to these simplifying assumptions).

Let $\beta \geq \alpha$

$$P(x,Y) = P_0(x) + P_1(x)\cdot Y + \ \ldots \ + P_{(\beta+\varepsilon)n}(x)\, Y^{(\beta+\varepsilon)n}$$

$$E(x,Y) = E_0(x) + E_1(x)\cdot Y + \ \ldots \ + E_{\beta n}(x)\cdot Y^{\beta n}$$

$$\& \ E_{\beta n}(x) \not\equiv 0.$$

$$M_x(P,E)(x) \triangleq \left[\begin{matrix} P_{(\beta+\varepsilon)n}(x) & P_{(\beta+\varepsilon)n-1}(x) & \ldots & P_0(x) & & & \\ & \ddots & \ddots & & \ddots & & \\ & & & & & & \\ E_{\beta n}(x) & E_{\beta n-1}(x) & \ldots & E_0(x) & & & \\ & \ddots & \ddots & \ddots & \ddots & \ddots & \end{matrix}\right] \begin{matrix} \}\ \beta n \\ \\ \}\ (\beta+\varepsilon)n \end{matrix}$$

$$\deg_x(R_Y) \leq \alpha m(\beta+\varepsilon)n + (\alpha+\delta)m\cdot\beta n$$
$$\leq mn(\alpha\beta + \alpha\varepsilon + \alpha\beta + \beta\delta)$$

$R_y(x) \stackrel{\Delta}{=} \det M_y(P,E)(x)$

$R_y(x) = Res_y(P,E)$

Since $\gcd(P,E)=1 \Rightarrow R_y(x) \not\equiv 0$

For each $u \in U$, $x = u$

$\frac{P(u,Y)}{E(u,Y)}$ — deg e

ie, top (βn) rows are spanned by the bottom $(\beta+\varepsilon)n$ rows.

Hence,

$R_y(u) = 0$; $R_y'(u) = 0$, $R_y^{(\beta n-1)}(u) = 0$

ie, u is a root with multiplicity $\cdot \beta n$.

Assume $\beta > 0$

Recall $\deg_x(R_y) \leq mn(2\alpha\beta + \alpha\varepsilon + \beta\delta)$

Counting Roots w/ multiplicity

$= m \cdot \beta n$

$> mn\,\beta(\alpha+\beta+\delta+\varepsilon)$ (by hypothesis & $\beta>0$

$= mn(\alpha\beta + \beta^2 + \beta\delta + \beta\varepsilon)$

$\geq mn(\alpha\beta + \alpha\beta + \beta\delta + \alpha\varepsilon)$ (since $\beta \geq \alpha$)

$= \deg_x(R_y)$

Contradiction

Hence $\beta = \alpha = 0$

Hence, E – $\deg(\alpha,\beta)$ – is a constant. $\boxtimes$

Returning to Axis Parallel Test

$$\Pr[R(u,v) = Q(u,v) = C(u,v)]$$
$$\geq \Pr[E(u,v) \neq 0]$$
$$\geq 1 - 2\mu = 1 - 2\sqrt{\eta}$$

(since E is $(\mu m, \mu n)$-deg poly)

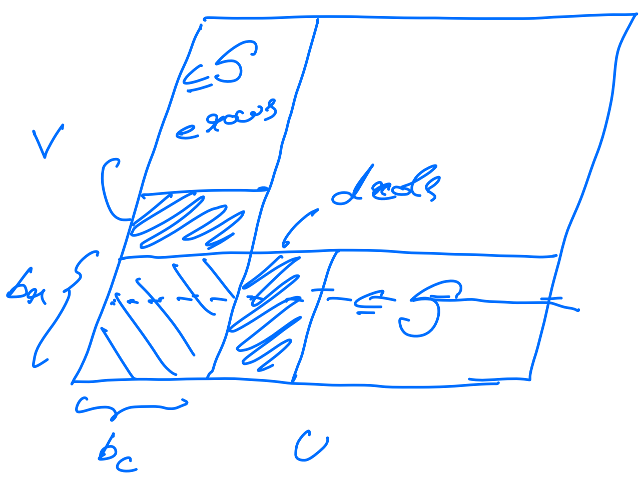
We will show something stronger

$$\Pr[R(u,v) = Q(u,v) = C(u,v)] \geq 1 - 2\eta$$

$$S = \{(u,v) \mid R(u,v) \neq C(u,v)\} \qquad |S| \leq \eta m n$$

$$T = \{(u,v) \mid R(u,v) = C(u,v) \neq Q(u,v)\}.$$

Suffice for us to show $|T| \leq |S|$.



r - row-bad

$$Q(x,v) \not\equiv R(x,v)$$

b_r - fraction of bad rows

u - col bad

$$Q(u,Y) \not\equiv C(u,Y)$$

b_c - fraction of bad col.

For any bad row v,
at most $d + \delta_c m$ pts of T.
(since otherwise this is a good row)

T lies in the shaded region above.

$1 > 2\eta + \frac{d}{m} \rightarrow$ every bad row $\geq \frac{m}{2}$ pts
S in the intersection
w/ good columns.

Concluding

Thm: Suppose R, C 2 poly of deg (d,n) & (m,e) respectively such that

$$2\left(\frac{d}{m} + \frac{e}{n} + \mu\right) < 1$$

$$\Pr_{(u,v)}\left[R(u,v) \neq C(u,v)\right] \leq \mu^2$$

then $\exists$ Q of deg (d,e) s.t

$$\Pr\left[R(u,v) \neq Q(u,v) \text{ or } Q(u,v) \neq C(u,v)\right] \leq 2\mu^2$$

$$\Pr_u\left[Q(u,Y) \neq C(u,Y)\right] \leq 2\mu^2$$

$$\Pr_v\left[Q(X,v) \neq R(X,v)\right] \leq 2\mu^2$$

Axis-Parallel Test to Random Line Test.

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

Want to check if $\deg(f) \leq d$.
(total degree, not individual degree).

Reed-Muller Codewords
$f \in RM_{\mathbb{F}}(m,d)$.

Question: ① Is there a local characterization?

② Is this char. robust?

"Candidate Characterization:"

$$f \in RM_{\mathbb{F}}(m,d) \iff \forall \text{ lines } \ell,\ f|_\ell \in RS_{\mathbb{F}}(d).$$

Counterexample: $\mathbb{F} = \mathbb{F}_{p^k}$ $\quad q = p^k \ (k \geq 1)$

$$Q(X,Y) = (X^{p-1}Y)^{q/p} \quad ; \deg Q = q$$

$\ell : a + Tb$ $\qquad Q|_\ell (T) = \left[(a_1T+b_1)^{p-1}(a_2T+b_2)\right]^{q/p}$

$a = (a_1, a_2)$

$b = (b_1, b_2)$

Every monomial in $Q_\ell(T)$ is of degree $\leq q$

& is a multiple of q/p.

$$\mathrm{Eval}(Q|_\ell) = \mathrm{Eval}(Q|_\ell(T) \bmod T^q - T)$$

$$\deg(Q|_\ell(T) \bmod (T^q - T)) \leq q - \frac{q}{p}$$

This fn on every line has degree $\leq q - q/p$

yet globally it has degree q.

Lemma: $q = p^k$, $d < q - q/p$, $f : \mathbb{F}^m \to \mathbb{F}$; $m \geq 2$

Suppose $\forall$ lines ℓ, $f|_\ell \in RS_{\mathbb{F}}(d)$

$\Downarrow$

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

Pf: Prove the contrapositive.

Let $d < q - q/p$, & $f \notin RM_{\mathbb{F}}(m,d)$.

Hence, $f(x_1 \ldots x_m) = \sum_e \alpha_e x_1^{e_1} \ldots x_m^{e_m}$

Suppose $\exists e$, s.t $\alpha_e \neq 0$; $\sum e_i > d$
$(0 \leq e_i < q)$

Suffices to show there is a line ℓ.
s.t $f|_\ell \in RS_{\mathbb{F}}(d')$ for some $d' > d$.

$$f(\quad) = \alpha_e x^e + \sum_{e' \neq e} \alpha_{e'} \cdot x^{e'}$$

$X = U + TV$

$U = (U_1 \ldots U_m)$

$V = (V_1 \ldots V_m)$

$T = T$

$$\alpha_e x^e \longrightarrow \alpha_e \prod_{i=1}^{m} (U_i + TV_i)^{e_i}$$

$$= \alpha_e \sum_{0 \leq f_i \leq e_i} \prod_i U_i^{e_i - f_i} V_i^{f_i} \binom{e_i}{f_i} \cdot T^{|f|}$$

$$= \alpha_e \sum_{0 \leq f_i \leq e_i} \left(\prod_{i=1}^{m} \binom{e_i}{f_i} U_i^{e_i - f_i} V_i^{f_i} \right) T^{|f|} \pmod{T^q - T}$$

$$f|_{U+TV} \pmod{T^q - T} = \sum_{j=0}^{D} T^j P_j(U, V)$$

If $P_j(U, V) \neq 0$, then there exist a (u, v)
s.t $f_{U+TV} \pmod{T^q - T}$ has degree $\geq j$.

Suffices to show that there is one
$P_j(U, V)$ that survives for $j > d$.

Need to choose $(f_1 \dots f_m)$ s.t (1) $\prod \binom{e_i}{f_i} \neq 0$

(2). $q > \deg\left(T^{|f|}\right)$

$\geq q - q/p$

<u>Lucas Thm:</u> $m = m_0 + m_1 p + \dots + m_r p^r$

$n = n_0 + n_1 p + \dots + n_r p^r$

$$\binom{m}{n} \pmod p = \prod \left(\binom{m_i}{n_i} \bmod p\right)$$

$$\binom{m}{n} \quad \begin{pmatrix} m_r & m_{r-1} & & m_0 \\ n_r & n_{r-1} & & n_0 \end{pmatrix}$$

<u>Claim:</u> $0 \leq e_i < q$. $\sum e_i > q - q/p$

then $\exists f_i$ s.t (1) $0 \leq f_i \leq e_i$.

(2) $\prod \binom{e_i}{f_i} \neq 0$

(3) $q > \sum f_i \geq q - q/p$.

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

<u>Thm:</u> $d < q - q/p$, $\text{Lifted-}RS_{\mathbb{F}}(m,d) = RM_{\mathbb{F}}(m,d)$

Robust characterization:

Thm [Friedl-Sudan].

$\forall \varepsilon > 0, \ \exists c < \infty$, s.t. $cd < |\mathbb{F}|$, the following holds:

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

$$\Pr_{\substack{x,\ell \\ x \in \ell}} \left[f(x) \neq F(\ell)(x) \right] \leq \delta \leq \frac{1}{8} - \varepsilon$$

$$\Downarrow$$

$$\exists \ P \in \text{Lifted-}RS_{\mathbb{F}}(m,d) \ , \ \delta(f,P) \leq 4\delta.$$

Proof:

$P^{(f,d)} : \{\text{lines}\} \to RS_{\mathbb{F}}(d)$

be the best fit lines-function that maximizes for each line ℓ

$$\Pr_{x \in \ell} \left[f(x) = F(\ell)(x) \right]$$

$$\delta_f = \Pr_{\substack{x,\ell \\ x \sim \ell}} \left[f(x) \neq P^{(f,d)}(\ell)(x) \right]$$

Obs: For any $F : \{\text{lines}\} \to RS_{\mathbb{F}}(d)$

$$\Pr_{\substack{x,\ell \\ x \sim \ell}} \left[f(x) \neq F(\ell)(x) \right] \geq \delta_f$$

$$g(x) =: f_{corr}(x) = \underset{l:\, l \ni x}{\text{Plurality}} \left\{ P^{(f,d)}(l)(x) \right\}$$

Claim: $\delta(f, f_{corr}) \leq 2\delta_f$

Lemma 1: $\delta_{f_{corr}} \leq \delta_f / 2$ (under the FS thm assumptions)

$$\underbrace{f^{(0)} = f}_{2\delta_f} \quad \underbrace{f^{(1)} = f^{(0)}_{corr}}_{\delta_f} \quad - \quad \underbrace{\quad}_{} \quad f_i = f^{(i-1)}_{corr} \quad \underbrace{\quad}_{} \quad f^{(k)} \quad \delta_{f^{(k)}} = 0$$

Claim 2: $\Pr_{\substack{x, l_1, l_2 \\ x \in l_1 \cap l_2}} \left[P^{(f,d)}(l_1)(x) \neq P^{(f,d)}(l_2)(x) \right] \leq \delta_f / 2.$

(Obs: Claim 2 $\Rightarrow$ Lemma 1)

$$\mathbb{E}_x \left[\Pr_{l;\, l \ni x} \left[f_{corr}(x) \neq P^{(f,d)}(l)(x) \right] \right]$$

$$\leq \mathbb{E}_x \left[\Pr_{l_1, l_2} \left[P^{(f,d)}(l_1)(x) \neq P^{(f,d)}(l_2)(x) \right] \right]$$

$$\leq \delta_f / 2.$$