Today

- Low Degree Testing
  - * Rubinfeld-Sudan
  - * Polishchuk-Spielman

CSS.330.1 : PCPs

Limits of Approximation Algorithms

Lecture 03 (2023-2-10)

Instructor: Prahladh Harsha

Last time

Linearity Testing : Constant-query PCP (based).

+ : Constant-query

− : Rate / Blowup - Exponential

Qn: Are there properties which are locally testable but w/ inverse-polynomial rate?

Low-Degree Testing:

$\mathbb{F}$ - field (finite field).

$m$ - dimension.

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

Want to check $f$ is "low-degree" w/o querying all of $f$.

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

$f(x_1, \ldots, x_m)$ – polynomial of degree at most $|\mathbb{F}|-1$ in each variable

$$\sum_{i_j \le |\mathbb{F}|} a_{i_1 i_2 \ldots i_m} \underbrace{x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}}_{\text{monomial}}$$

Low-degree:

Individual Degree: $\forall i \in [m]$, $\deg_{x_i}(f) \le d$

Total Degree: For every monomial (s.t. $a_{i_1 i_2 \ldots i_m} \ne 0$)

$i_1 + i_2 + \ldots + i_m \le d$.

---

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

Test$^f$:
1. Random coins $R$
2. $Q \leftarrow Q(R, \mathbb{F}, m, d)$
3. Read $f$ on $Q$
4. Accept if "$f|_Q$ is a valid view"

Completeness: $f$ - low-degree $\Rightarrow \Pr_R[\text{Test}^f \text{ acc}] = 1$

Remark: All tests studied, the above is a characterization of 'low-degree-ness'

Soundness: $\exists\, \delta_0$, $\forall\, \delta \le \delta_0$

$\Pr[\text{Test}^f \text{ acc}] \ge 1-\delta \Rightarrow f$ is $O(\delta)$-close to some low-degree

Qn: How large is $\delta_0$?

(a). Multilinear polynomials

Babai-Fortnow

Babai-Fortnow-Lund (MIP = NEXP)

Feige-Lovasz-Goldwasser-Safra-Szegedy

(b) Individual Degree:

Arora-Safra '92 : $\delta_0 = O(\frac{1}{m})$

Polishchuk-Spielman 94 : Clean Analysis.

(c) Total Degree:

Rubinfeld-Sudan '91 : $\delta_0 = O(\frac{1}{d^2})$

Arora-Lund-Motwani-Sudan-Szegedy '92 : $\underbrace{\delta_0 = O(1)}_{\text{key ingredient in PCP Theorem}}$

Friedl-Sudan '95 : $\delta_0 = 1/8$.

Arora-Sudan '96 : $\delta_0 = 1 - \mathrm{poly}(m, d, \frac{1}{|F|})$

Raz-Safra '96

$\left( \Pr[\mathrm{Test}^f] \geq \varepsilon \Rightarrow \mathrm{agr}(f, P(m,d)) \geq \varepsilon - \mathrm{poly}(m,d,\frac{1}{|\mathbb{F}|}) \right)$

In lecture: Rubinfeld-Sudan
Polishchuk-Spielman
Friedl-Sudan
Arora-Sudan / Raz-Safra

Today: Rubinfeld-Sudan Total-degree test

Characterization for low degreeness

Univariate: $f : \mathbb{F} \to \mathbb{F}$

$f$ is of degree $\leq d$. $\qquad$ $\mathrm{char}(\mathbb{F}) \geq d+2$

$$\Updownarrow$$

$\forall x, h \in \mathbb{F}$, $\sum_{i=0}^{d+1} \alpha_i f(x+ih) = 0$

where $\alpha_i = \binom{d+1}{i}(-1)^{i+1}$

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

$f$ is of degree $\leq d$ $\qquad$ $(\mathrm{char}(\mathbb{F}) > d+2)$

$$\Updownarrow$$

$\forall x, h \in \mathbb{F}^m$, $\sum_{i=0}^{d+1} \alpha_i f(x+ih) = 0$.

RS: The above is a <u>robust</u> characterization

Theorem [Rubinfeld-Sudan] $(\text{char}(\mathbb{F}) > d+2)$

$\exists\, \delta_0 = \frac{1}{(d+1)(2d+5)}$, $\forall \delta < \delta_0$

$$\Pr_{x,h \in \mathbb{F}^m}\left[\sum_{i=0}^{d+1} \alpha_i f(x+ih) = 0\right] \geq 1-\delta$$

$$\Downarrow$$

$f$ is $2\delta$-close to a deg $d$ polynomial

**Proof:**

Self-correction of $f$

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

$$g(x) = \underset{h \in \mathbb{F}^m}{\text{plurality}} \left\{ -\sum_{i=1}^{d+1} \alpha_i f(x+ih) \right\}$$

Claim I: $\delta(f,g) \leq 2\delta$

Claim II: [Overwhelming majority]

$$\forall x \quad \Pr_h\left[g(x) = -\sum_{i=1}^{d+1} \alpha_i f(x+ih)\right] \geq 1 - 2(d+1)\delta$$

Claim III: If $\delta < \frac{1}{(d+1)(2d+5)}$, $g(x)$ is of degree $\leq d$.

Proof of Claim I: $BAD = \left\{ x \in \mathbb{F}^m \,/\, \Pr_h\left[\sum_{i=0}^{d+1} \alpha_i f(x+ih) = 0\right] < 1/2 \right\}$

$x \notin BAD \Rightarrow g(x) = f(x)$

$(\delta(f,g) \leq \Pr_x [x \in BAD]$

$$\delta \geq \Pr_{x,h}\left[\sum_{i=0}^{d+1} \alpha_i f(x+ih) \neq 0\right]$$

$$\geq \Pr_x [x \in BAD] \Pr_{x,h}\left[\sum_{i=0}^{d+1} \alpha_i f(x+ih) \neq 0 \,/\, x \in BAD\right]$$

$$\geq \delta(f,g) \cdot 1/2$$

$\boxtimes$

---

Proof of Claim II:

Suffices to prove for every $x \in \mathbb{F}^m$

$$\Pr_{h_1, h_2}\left[\sum_{i=1}^{d+1} \alpha_i f(x+ih_1) = \sum_{i=1}^{d+1} \alpha_i f(x+ih_2)\right] \geq 1 - 2(d+1)\delta.$$

$Z \in \mathbb{F}^{(d+2)\times(d+2)}$

$$\begin{array}{c|c} {}_i \diagdown {}^j & 0 \quad 1 \quad \cdot \quad \cdot \quad\quad d+1 \\ \hline \begin{array}{c} 0 \\ \\ \\ d+1 \end{array} & \begin{bmatrix} & & \\ & Z_{ij} & \\ & & \end{bmatrix} \end{array}$$

$Z_{ij} = \alpha_i \alpha_j f(x + ih_1 + jh_2)$

$R_i$ : " $\sum_{j=0}^{d+1} \alpha_i \alpha_j f(x+ih_1+jh_2) = 0$ "

$$\alpha_i \sum_{j=0}^{d+1} \alpha_j \; f(x' + j h_2) = 0$$

$i \neq 0$; $x' = x + i h_1$ - random elt if $h_1$ is random

$$\forall\, i \neq 0; \quad \Pr_{h_1, h_2}[\neg R_i] \leq \delta$$

$$G: \quad \sum_{i=0}^{d+1} \alpha_i \alpha_j \; f(x + i h_1 + j h_2) = 0$$

$$\alpha_j \sum \alpha_i \; f(x' + i h_1) = 0$$

$j \neq 0$, $x' = x + j h_2$ - random elt

$$\forall_j \neq 0 \quad \Pr_{h_1, h_2} [\neg G] \leq \delta.$$

Hence,

$$\Pr\left[\left(\bigvee_{i=1}^{d+1} \neg R_i\right) \vee \left(\bigvee_{j=1}^{d+1} \neg G\right)\right] \leq 2(d+1)\delta$$

$$\Pr\left[\left(\bigwedge_{i=1}^{d+1} R_i\right) \wedge \left(\bigwedge_{j=1}^{d+1} G\right)\right] \geq 1 - 2(d+1)\delta.$$

However $\bigwedge_{i=1}^{d+1} R_i \wedge \left(\bigwedge_{j=1}^{d+1} G\right)$

$$\Downarrow$$

$$\sum_{i=1}^{d+1} \alpha_0 \alpha_i \cdot f(x + i h_1) = \sum_{j=1}^{d+1} \alpha_0 \alpha_j \; f(x + j h_2)$$

$\boxtimes$.

Proof of Claim III:

To show $g$ is of degree $d$ suffices to show:

$\forall x, h \in \mathbb{F}^m.$ $\quad \sum_{i=0}^{d+1} \alpha_i \, g(x+ih) = 0$

Fix $x, h$ $\qquad h_1, h_2 \in_R \mathbb{F}^m$

$$\begin{array}{cc} & \begin{array}{ccc} j \; 0 & & d+2 \end{array} \\ \begin{array}{c} i \\ 0 \\ \vdots \\ d+2 \end{array} & \begin{bmatrix} & & \\ & Y & \\ & & \end{bmatrix} \end{array}$$

$Y(h_1, h_2) \in \mathbb{F}^{(d+2)\times(d+2)}$

$$Y_{i,j} = \begin{cases} \alpha_i \alpha_j f(x+ih + j(h_1+ih_2)) & \text{if } j \neq 0 \\ \alpha_i \alpha_0 \, g(y+ih) & j = 0 \end{cases}$$

$R_i : C_j$ - refer to events that the corresponding row/col sum to 0.

Suffices to show $\Pr_{h_1,h_2}[C_0] > 0$

which is true $\Pr_{h_1,h_2}\left[\bigwedge_{i=0}^{d+2} R_i \wedge \bigwedge_{j=1}^{d+1} C_j\right] > 0.$

$$C_j : \sum_{i=0}^{d+1} \alpha_i \alpha_j f(x+ih+j(h_1+ih_2)) = 0 \qquad (j \neq 0)$$

$$\alpha_j \sum_{i=0}^{d+1} \alpha_i f(\underbrace{x+jh_1}_{x'} + i\underbrace{(h+jh_2)}_{h'}) = 0$$

$$\Pr_{h_1,h_2}[\neg C_j] \leq \delta$$

$$R_i: \quad \alpha_i \alpha_0\, g(\underbrace{x+ih}_{x'}) + \sum_{j=1}^{d+1} \alpha_i \alpha_j\, f(\underbrace{x+ih}_{x'} + j(\underbrace{h_1+ih_2}_{h'})) = 0$$

$$\Pr_{h_1,h_2}[\neg R_i] \leq 2(d+1)\delta.$$

Hence,
$$\Pr\left[\bigvee_{i=0}^{d+1}(\neg R_i) \vee \left(\bigvee_{j=1}^{d+1} \neg C_j\right)\right]$$
$$\leq 2(d+1)(d+2)\delta + (d+1)\delta$$
$$= (d+1)(2d+5)\delta$$
$$< 0 \quad \text{if } \delta < \frac{1}{(d+1)(2d+5)}.$$

$\boxtimes$

---

Part 2: Low Individual Degree Test.

$f: X \times Y \to \mathbb{F}$ ; $|X| = m$; $|Y| = n$, $X, Y \subseteq \mathbb{F}$.

Check : $\deg_X(f) \leq d$ & $\deg_Y(f) \leq d$.

<u>Notation</u>: $f: X \times Y \to \mathbb{F}$
$$f(x,y) = \sum_{j=0}^{|Y|-1} \sum_{i=0}^{|X|-1} a_{ij}\, x^i y^j \quad \text{(unique)}$$

$f$ is of deg $(d,e)$ if $a_{ij} = 0 \;\forall\, i > d$ & $j > e$.
(for $d < |X|$, $e < |Y|$)

Characterization: $U, V \subseteq \mathbb{F}$, $d < |U|$, $e < |V|$
$|U| = m$; $|V| = n$

$f : U \times V \to \mathbb{F}$

$f$ is of deg $(d, e)$

$\Updownarrow$

$\forall u \in U$, $f(u, Y)$ - deg $\leq e$ in var $Y$

$\forall v \in V$, $f(X, v)$ - deg $\leq d$ in var $X$.

$R(X, Y)$ - row polynomial of degree $d$
(i.e., $\forall v \in V$, $R(X, v)$ - deg $d$)

$C(X, Y)$ - column poly of deg $e$
(i.e., $\forall u \in U$, $C(u, Y)$ - deg $e$)

$R$ — deg $(d, n)$ polynomial
$C$ - deg $(m, e)$ polynomial.

Suppose $\Pr_{(x,y) \in U \times V}[R(x,y) = C(x,y)] \geq 1 - \eta$

$\Downarrow$ ??? (is this true)

$\exists$ $Q$ of deg $(d, e)$

$\Pr_{x,y}[R(x,y) = Q(x,y) = C(x,y)] \geq 1 - O(\eta)$.

Analysis due to Polishchuk & Spielman.

Analysis (via Polynomial Method).

$S = \{(x,y) \in C \times V \mid R(x,y) \neq C(x,y)\}$

$|S| \leq \eta mn \qquad \eta = \mu^2$

There exists a nonzero poly $E(X,Y)$ of deg $(\mu m, \mu n)$ s.t

$\forall (x,y) \in S \implies E(x,y) = 0.$

(since #vars > # constraints).

$\forall (x,y) \in (C \times V) \setminus S, \quad R(x,y) = C(x,y)$

$\forall (x,y) \in C \times V, \quad R(x,y) E(x,y) = C(x,y) \cdot E(x,y)$

$$P(x,y) := R(x,y) E(x,y) = C(x,y) E(x,y).$$

Obs: (1) For every $u \in C$, $P(u,Y) = C(u,Y) \cdot E(u,Y)$

$\deg_Y P(u,Y) \leq c + \mu n$

(2) For every $v \in V$, $P(X,v) = R(X,v) E(X,v)$

$\deg_X P(X,v) \leq d + \mu m$

Hence, $P$ is of deg $(d+\mu m, e+\mu n)$.

(provided $d+\mu m < m$
$e+\mu n < n$ )

$$P(x,y) = R(x,y) \cdot E(x,y) = C(x,y) \cdot E(x,y).$$

$(d+\mu m, e+\mu n)$ $(\mu m, \mu n)$

Want to show that $E$ divides $P$ formally.

What can we say.

(1) For each $u \in U$

$$P(u,y) = C(u,y) \cdot E(u,y) \quad \forall y \in V$$

Since, $|V| > e+\mu n$

$$P(u,Y) \equiv C(u,Y) \cdot E(u,Y)$$

ie, for each fixing $u \in U$
$P(u,Y)$ is divisible by $E(u,Y)$
& the quotient $C(u,Y)$ is of deg $\leq e$

(2) Similarly, for each fixing $v \in V$
$P(X,v)$ is divisible by $E(X,v)$

& the quotient $R(X,v)$ is of deg $\leq d$.

Polishchuk-Spielman Lemma:

Suppose $P$, $E$ are two deg $(\alpha m+\delta m, \beta n+\varepsilon n)$ & $(\alpha m, \beta n)$ polynomials.

s.t. $\begin{cases} \forall\, u \in U,\ |U|=m: & \dfrac{P(u,Y)}{E(u,Y)} \text{ is of deg } \varepsilon n \\ \forall\, v \in V,\ |V|=n, & \dfrac{P(X,v)}{E(X,v)} \text{ is of deg } \delta m \end{cases}$

then $\exists$ poly $Q$ of deg $(\delta m, \varepsilon n)$ s.t.

$$P(X,Y) \equiv Q(X,Y)\,E(X,Y)$$

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

— Want to show $E$ divides $P$.

ie, $\gcd(P,E) = E$

— Simpler Qn $\gcd(P,E) \neq 1$

( in the bivariate setting).

- What about the univariate setting.

$$P(x) = P_0 + P_1 X + \dots + P_r X^r \qquad r = \deg(P)$$
$$E(x) = E_0 + E_1 X + \dots + E_s X^s \qquad s = \deg(E)$$

**Claim:** $\gcd(P,E) \neq 1 \iff \exists$ non-zero poly $A$, $B$
$\deg(A) \le s-1$, $\deg(B) \le r-1$ s.t.
$$P(x)\cdot A(x) = E(x)\cdot B(x).$$

Pf: $F = \gcd(P,E)$

$P = \hat{P}\cdot F$ ; $E = \hat{E}\cdot F$

$A = \hat{E}$ ; $B = \hat{P}$ $\boxtimes$

Existence of such non-zero $A$ & $B$.

$$\begin{array}{c} s\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. \\ r\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. \end{array}
\underbrace{\begin{bmatrix} P_r & P_{r-1} & \dots & P_0 & 0 & \dots & 0 \\ & P_r & & & P_0 & & \\ & & & P_r & \dots & & P_0 \\ E_s & E_{s-1} & \dots & E_0 & 0 & \dots & 0 \\ & E_s & E_{s-1} & & E_0 & \dots & \\ & & & E_s & \dots & & E_s \end{bmatrix}}_{}
\left.\begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array}\right\} r+s$$

$M(P,E)$

$\mathrm{Res}(P,E) = \det(M(P,E))$

**Prop:** $\gcd(P,E) \neq 1 \iff \mathrm{Res}(P,E) \neq 0.$

$$P(X,Y) = P_0(X) + P_1(X)Y + \dots \qquad + P_r(X)Y^r$$
$$E(X,Y) = E_0(X) \qquad\qquad + E_s(X)Y^s$$

where $P_r(X) \not\equiv 0$
$E_s(X) \not\equiv 0$.

Prop: [Gauss' Lemma]
$\gcd_Y(P, E) \neq 1 \iff \mathrm{Res}(P, E) \equiv 0$
(In this case, $\mathrm{Res}(P, E) \in \mathbb{F}[X]$).

Proof of PS Lemma:

$P$ — $(\alpha m + \delta m, \beta n + \varepsilon n)$ deg
$E$ — $(\alpha m, \beta n)$ deg.

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

Wlog, we can assume $\deg_X(P) = \alpha m + \delta m$ (exactly)
or $\deg_X(E) = \alpha m$
(otherwise replace $\alpha$ by $\alpha - \frac{1}{m}$)

Similarly, we can assume $\deg_Y(P) = \beta n + \varepsilon n$ (exactly)
or
$\deg_Y(E) = \beta n$. (exactly).

$\gcd(P,E) = F$ (Want to show $F = E$)

$P = \hat{P} \cdot F$ $\qquad F$ - deg $(a,b)$

$E = \hat{E} \cdot F$

Hypothesis is true for $\hat{P}$, $\hat{E}$ as well

$P(x,Y) = E(x,Y) \cdot c(x,Y)$

$\hat{P}(x,Y) \cdot F(x,Y) = \hat{E}(x,Y) \cdot F(x,Y) \cdot C(x,Y)$

on $U' \times V'$ where $|U'| \geq |U| - a$

$|V'| \geq |V| - b$.

$$\alpha' + \beta' + \delta' + \varepsilon' = \frac{\delta m - a}{m-a} + \frac{\varepsilon n - b}{n-b} + \frac{\alpha m}{m-a} + \frac{\beta n}{n-b}$$

$$= \frac{(\alpha+\delta) m - a}{m-a} + \frac{(\beta+\varepsilon) n - b}{n-b}$$

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

$\gcd(P,E) \neq 1 \Rightarrow$ Replace $(P,E)$ by $(\hat{P}, \hat{E})$

Assume PS Lemma hypothesis

$\gcd^{2}(P,E) = 1$ $\Rightarrow$ $E$ has constant polynomial.

Next lecture.