Polynomial Method & Variations - IITB

Thursday, December 22, 2016 10:50 PM

Polynomial Method

Problem

- $S \subseteq \mathbb{F}^n$ ($\mathbb{F}$ = field)
- S has nice algebraic / geometric property P
- $\mu(S)$ - combinatorial parameter

Paradigm

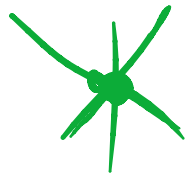
- Assume $\mu(S) < k$

- Assume $\mu(S) < k$
- Prove $\overset{\text{poly}}{\exists} Q$ s.t. $Q(S) = 0$
- Use low-deg of Q & property P to prove Q is zero in "unexpected" ways
- Get contradiction ☒

Remarkably Effective!

- Bounds of # polynomials through small set of points (RS decoding)

- Bounds on # lines through small set of points (Kakeya / Nikodym)

- Bounds on joints  in 3-d through small # lines

- Distinct distances ...

- Capset Problem

- Property testing ....

I. Reed-Solomon Decoding

Context: Message ≡ Polynomial

Encoding ≡ Sequence of Evaluations

Decoding ≡ "find poly consistent with many points"

Question: How many polynomials?

Concrete Problem:

Given: $(x_1, y_1), (x_2, y_2) \dots (x_n, y_n)$ $x_i, y_i \in \mathbb{F}$

+ parameters d, t

Question:

- $p \in \mathbb{F}^{\leq d}[x]$ is <u>t-agreeing</u> if

$$|\{i \mid p(x_i) = y_i\}| \geq t$$

- $\exists$ bound : $|\{p \mid p \text{ t-agreeing}\}| \leq ?$

<u>Solution</u>:

[illegible] Λ in x, y s.t.

- Let $Q(x,y) \neq 0$ be of deg Δ in x, y s.t.

$$Q(x_i, y_i) = 0 \quad \forall i \in [n]$$

- Claim ①: $y - p(x) \mid Q(x,y)$ if

p is $(\Delta(d+1))$-agreeing

- Claim ②: Such Q exists with $\Delta = \sqrt{n}$

- Conclude ③:

$$\#\{(\sqrt{n}(d+1))\text{-agreeing poly}\} \leq \sqrt{n}.$$

$\times$

① ② ③

Proofs of ①, ②, ③

① : . $R(x) \equiv Q(x, p(x))$ has deg. $\leq \Delta(d+1)$

. $R(x_i) = 0$ if $p(x_i) = y_i$

. $\Rightarrow R \equiv 0 \Rightarrow y - p(x) \mid Q(x, y)$

② Counting: # coefficients of $Q = (\Delta+1)^2 > n$

$=$ # constraints

"Homogeneous linear system of small rank has many solutions"

③ $Q(x,y)$ of deg Δ has at most Δ factors of the form $y - p(x)$.

State of art: know bounds for $t > \sqrt{dn}$;

But open for $t \leq \sqrt{dn}$.

- Proof 1: Jaikumar Radhakrishnan "Zarankiewicz" method
- Proof 2: Guruswami + S. "multiplicity"

II. Nikodym Sets

- $S \subseteq \mathbb{F}_q^n$
- $\overline{S} = S \cup \left(\bigcup_{\ell} \{ \text{line } \ell \mid |\ell \cap S| \geq q-1 \} \right)$

(close S under lines almost entirely in S)

- S = Nikodym if $\overline{S} = \mathbb{F}_q^n$
- $|S| \geq ?$

Solution [Dvir]:

- Find $Q \in \mathbb{F}^{\leq q-2}[x_1 \dots x_n] \not\equiv 0$ s.t.

  $Q(\alpha) = 0 \quad \forall \alpha \in S$

$Q(\alpha) = 0 \quad \forall \alpha \in S$

- Claim: such Q exists if $|S| < \binom{n+q-2}{n}$ [counting]

- Claim: if $\ell \in \bar{S} \Rightarrow Q|_\ell \equiv 0$

  (since $Q|_\ell$ is of deg $\leq q-2$

  & $|\ell \cap S| > q-2$)

- $\bar{S} = \mathbb{F}_q^n \Rightarrow Q \equiv 0$

- Contradiction $\Rightarrow |S| \geq \binom{n+q-2}{n} \approx \frac{q^n}{n!}$

State-of-art

General q: $|S| \geq \frac{q^n}{2^n}$ [multiplicities]

Dvir - Kopparty - Saraf - S

q of small char: $|S| \geq q^n(1 - o_q(1))$

[Lifted Codes]

[Guo-Kopparty-S]

III. Joints Problem [Guth-Katz]

J = finite set of lines in $\mathbb{R}^3$

- $\mathcal{L}$ = finite set of lines in $\mathbb{R}^3$
- $N \triangleq |\mathcal{L}|$
- $p \in \mathbb{R}^3 \triangleq$ "joint" if

  $\exists\ l_1, l_2, l_3 \in \mathcal{L}$ lin. ind. s.t.

  $p \in l_1, l_2, l_3$
- Bound: $J \triangleq \#\{p \mid p \text{ joint in } \mathcal{L}\} \leq ?$

- Trivial Bound: $J \leq \binom{N}{2}$

- Best Example = $K \times K \times K$ grid

$$N = 3K^2 \; ; \; J = K^3 = \Omega(N^{3/2}).$$

Guth-Katz Theorem

$$J = O(N^{3/2})$$

Proof: fix $D = 10 \cdot N^{1/2}$

will prove $J \leq (D+1)L$

① Pruning: - Throw away lines with $\leq D$ joints iteratively

joints iteratively

- At end every line has $> D$ joints.
- Notational Simplicity: L = this set.

(2) Fix $S \subseteq J$ s.t. every line in L has at least D points of S, but $|S| \leq (D)N$

(3) Let Q be lowest deg. poly s.t.

$Q(p) = 0 \quad \forall p \in S.$

(4) Deg $Q = (3(D)N)^{1/3} \approx (30)^{1/3} N^{1/2} < D$

④ $\deg Q = (3(D-1)N)$ ~ (illegible)

⑤ $Q|_\ell \equiv 0 \quad \forall \ell \in L$ [$\deg Q|_\ell < D$;
Δ $Q|_\ell(p) = 0$
$\forall p \in \ell \cap S$]

⑥ Let $Q_x = \frac{\partial Q}{\partial x}$, $Q_y = \frac{\partial Q}{\partial y}$, $Q_z = \frac{\partial Q}{\partial z}$

$$Q_\ell = \frac{\partial Q}{\partial \ell}$$

⑦ $Q|_\ell \equiv 0 \Rightarrow Q_\ell(p) = 0 \quad \forall p \in \ell \cap S$

$\exists 3$ l.i. lines s.t. $Q_{\ell_1} = Q_{\ell_2} = Q_{\ell_3} = 0$

$\exists 3$ l.i. lines s.t. ℓ_1 ℓ_2 ... at p

$\Rightarrow Q_x(p) = Q_y(p) = Q_z(p) = 0 \quad \forall p \in S$

But at least one is zero contradicting minimality of Q

⑧ Conclude: Pruning leaves us with empty set.

$$J \leq (D+1) \cdot N$$

IV. "Capset" in $\mathbb{F}_3^n$

- $A \subseteq \mathbb{F}_3^n$ has a 3-AP if $\exists\, x, y, z \in A$ (distinct) s.t.

  $y - x = z - y \iff x + y + z = 0$

  $\iff$ "$\{x, y, z\}$ form a line in $\mathbb{F}_3^n$"

- Question: if A has no 3-AP. then $|A| \leq$??

... Bound: $|A| \leq 3^n$

Trivial Bound: $|A| \leq 3^n$

Roth ... : $|A| \leq 3^{n - \Theta(\sqrt{n})}$

Theorem: [Ellenberg-Gijswijt]

$$|A| < (2.99)^n$$

(Based on Croot-Lev-Pach analysis in $\mathbb{Z}_4^n$)

Proof:

⊛ Find Q s.t. $Q(b) = 0 \quad \forall b \in \overline{A}$

Q non-zero as often as possible

& Q non-zero as often as possible in A.

① Say $T = \{a \mid Q(a) \neq 0\}$

consider $T \times T$ matrix M

with $M(a,b) = Q(-(a+b))$

② A is 3-AP free

$\Rightarrow T$ is 3-AP free

$\Rightarrow M$ is diagonal

$\Rightarrow$ $\text{rank}(M) \geq |T|$

③ On the other hand if $\deg Q \leq d$

then $M(x,y) = Q(-(x+y))$

$= A(x,y) + B(x,y)$

$\uparrow$ $\deg_y \leq \frac{d}{2}$ $\quad$ $\uparrow$ $\deg_x \leq \frac{d}{2}$

$\Rightarrow \text{rank}(M) \leq 2\,\Delta\left(n,3,\frac{d}{2}\right)$

Proves $|T| \leq 2\,\Delta\left(n,3,\frac{d}{2}\right)$

Proves $|H| \leq 2\Delta(n, 3, \frac{d}{2})$

But want $|A| \leq \ldots$

$\Rightarrow$ need bound on d!

Strategy:

Will set it up such that

$$\dim(\{Q \mid Q(\bar{A}) \equiv 0\}) > \frac{|A|}{2}$$

$$\Rightarrow \exists Q \text{ s.t. } |\{t \mid Q(t) \neq 0\}| > \frac{|A|}{4}$$

($|A|/4$ easy ; $\frac{|A|}{2}$ also..)

$\Rightarrow |\Pi| > \frac{|A|}{4}$

$\dim(\{Q \mid Q(A) = 0\})$

$= \Delta(n,3,d) - |\bar{A}|$

$= \Delta(n,3,d) + |A| - 3^n > \frac{|A|}{4}$

$\Rightarrow$ Want d s.t.

$\Delta(n,3,d) > 3^n - \frac{3}{4}|A|$

Δ get

$$|A| < 4|T| < 8\,\Delta\left(n,3,\frac{d}{2}\right)$$

$$\Rightarrow |A| \geq \max_d \left\{ \min \left\{ \frac{4}{3}\left(3^n - \Delta(n,3,d)\right),\ 8\,\Delta\left(n,3,\frac{d}{2}\right) \right\} \right\}$$

Turns out $d \approx 1.98n$ works

$$\text{Prob}_{e:\{0,1,2\}^n}\left[e_1 + e_2 \cdots e_n > (1.98)n \right] \leq \alpha^n \qquad \alpha < 1$$

$$\Rightarrow \Delta(n,3,1.98n) \geq 3^n(1-\alpha^n)$$

$$\Rightarrow 1^{st}\ \text{term} \leq \frac{4}{2}(3\alpha)^n \,.$$

$$\text{Prob}_{e_1 \ldots e_n \in \{0,1,2\}} \left[\sum e_i \leq .99n \right] \leq \beta^n \qquad \beta < 1$$

$$\Rightarrow \text{2nd term} \leq 8(3\beta)^n$$

⊠

Many Open Questions

ORS Decoding: Is $\sqrt{dn}$ right?

$\exists$ fields s.t. this bound can be

increased?

② Nikodym Set:

Resolve prime vs. non-prime gap

③ Joints

if # 3-way intersection is large

then this is because of co-planarity?

④ Capsets

4-term AP bound?

4-term AP bound?

in general bound size of sets that have no solution to linear systems!