Polynomial Method & Variations

Note Title 4/14/2014

Madhu Sudan

(Microsoft)

Based on an old joint work with Dvir, Kopparty, Saraf.

Polynomial Method?

(Actual method later)

- method to analyze combinatorial aspects of geometrically nice set.
- Early seeds in coding theory / "list-decoding"
- recent generalization due to Dvir 2008
- many implications due to Guth, Katz, others.
- this talk: method + strengthening.

Central Examples: Kakeya Sets & Nikodym Sets

Notation: $\mathbb{F}_q$ - finite field with q elements.

Defn: $K \subseteq \mathbb{F}_q^n$ is Kakeya if it "contains a line in every direction"

i.e. $\forall b \in \mathbb{F}_q^n \ \exists a \in \mathbb{F}_q^n$ s.t.

$$\{a + t \cdot b \mid t \in \mathbb{F}_q\} \subseteq K$$

Defn: $S \subseteq \mathbb{F}_q^n$ Nikodym if it almost contains line through every point

$$\forall a, \exists b \text{ s.t. } \{a + t \cdot b \mid t \in \mathbb{F}_q\} \subseteq S \cup \{a\}$$

Central Question: How small can a Kakeya (or Nikodym) Set be?

- Clearly at most q^n
- # lines through m points $\leq \binom{m}{2} \approx m^2$

  But need q^n lines $\Rightarrow$

  $m \geq q^{n/2}$

- State of art pre-Dvir

  $\sim \geq q^{.51n}$

- Dvir? wait .....

Two CS motivations

- Both indirect "in spirit".

  if small Kakeya sets exist then ∃ small sets of points with many lines.

- By extension, maybe ∃ small sets with many low-degree polynomials passing through them.

- Ruling this out ⇒ nice results in pseudorandomness, error-correction.

The Polynomial Method (for Kakeya Sets)

① $|K|$ small $\Rightarrow$

$\exists$ polynomial $Q(x_1 \dots x_n)$ of deg $\leq D$ s.t.

① $Q(a) = 0 \quad \forall a \in K$

② $Q \not\equiv 0$

② $D < q \Rightarrow$ Contradiction

Proof of (2):

- let $Q = R + S$ $\quad R$ homogenous

$$\deg(S) < \deg(Q) \; (= D)$$

↑ for simplicity

- $R \neq 0$!
- let $\{a + t \cdot b\} \subseteq K$ &

$$Q_{a,b}(t) = Q(a + t \cdot b)$$

thus $Q_{a,b}(t) = R(b) \cdot t^D + \dots + Q(a) \cdot t^0$

- But $Q_{a,b}(t) = 0 \quad \forall t$

$$\Rightarrow R(b) = 0$$

- But this is true for every b ☒

$|K|$ vs. D ?

- Claim: if $|K| < \binom{q+n-1}{n}$ then $\exists$ Q of degree $D \leq q-1$
- Proof: $Q = \sum q_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$
  - $\{q_{i_1 \ldots i_n}\}$ unknown; # unknowns $= \binom{q+n-1}{n}$
  - Each $a \in K$ gives a constraint
    - linear
    - homogeneous.
  - # unknowns > # constraints $\Rightarrow$ non-zero solution ⊠

Consequently

Theorem [Dvir]: K is a Kakeya set in $\mathbb{F}_q^n$

$$\Rightarrow |K| \geq \binom{q+n-1}{n} \approx \frac{q^n}{n!}.$$

- Improves from $q^{0.51n} \rightsquigarrow q^n$ ...

- How small can K be? Non-trivial constructions?

Best known $\sim \frac{q^n}{2^{n-1}}$

Improvement?

- Can we prove $|K| \geq \frac{q^n}{c^n}$ for constant c?

- Can we get $c = 2$?

- YES! MULTIPLICITIES!

Multiplicity Method

① Find Q of $\deg \leq D$ s.t.

$\forall\, a \in K$, Q vanishes with multiplicity m at a

② $D < m \cdot q \Rightarrow$ highest degree part of Q is zero at every point in $\mathbb{F}_q^n$.

But when is this a contradiction?

Implementation ①: [Saraf + S. 2009]

① Q has degree $< q$ in each variable

(so $D = n \cdot (q-1)$)

② # unknowns $= q^n$

③ # constraints $= ?$

Multiplicity = ?

- Multiplicity 1: $Q(a) = 0$
- Multiplicity 2: $Q(a) = 0$; $\frac{\partial Q}{\partial x_i}(a) = 0 \quad \forall i$
- Multiplicity m: $\frac{\partial Q}{\partial x_1^{i_1} \partial x_2^{i_2} \cdots \partial x_n^{i_n}}(a) = 0$

$$\forall \; i_1 + i_2 + \cdots i_n \leq m$$

Key Point : # constraints $= \binom{m+n}{n}$

Implementation ① : [Saraf + S. 2009]

① Q has degree $< q$ in each variable

(so $D = n \cdot (q-1)$)

② # unknowns $= q^n$

③ # constraints $= ? = \binom{m+n}{n} \cdot |K|$

④ $m = n \Rightarrow$ # constraints $\leq 4^n \cdot |K|$

$4^n \cdot |K| < q^n \Rightarrow$ contradiction !

Extended Method of Multiplicities

(1) Find $Q \not\equiv 0$ s.t. Q vanishes with multiplicity m at every $a \in K$

(2) Conclude (highest degree part of) Q vanishes with multiplicity $m/2$ at every $b \in \mathbb{F}^n$

[provided $D < \left(\frac{m}{2}\right) \cdot q$]

(3) Somehow derive contradiction.

Why is (2) true? [mult. of Q on $K \geq m$ $\Rightarrow$ mult. of Q on $\mathbb{F}_q^n \geq \frac{m}{2}$]

(i) $\left(\frac{m}{2}\right) \cdot q > D \Rightarrow$ any poly P of deg $< D$ that vanishes with mult. $\frac{m}{2}$ on K is identically 0 on $\mathbb{F}_q^n$

(ii) Every derivative of Q of order $\leq \frac{m}{2}$ is such a poly.

(iii) $\Rightarrow$ Q vanishes with mult. $\frac{m}{2}$ on $\mathbb{F}_q^n$

Final Contradiction: Multiplicity of Zero Lemma

Lemma: $\deg Q \leq D$; $Q \not\equiv 0$;

$$\Rightarrow \mathop{\mathbb{E}}_{a \in \mathbb{F}_q^n} \left[\text{mult}(Q, a) \right] \leq \frac{D}{q} \qquad \boxtimes$$

Proof: Omitted.

Final Calculations:

$D = \underbrace{\frac{m}{2} \cdot q}$; $\frac{m^n}{n!} \cdot |K| < \frac{D^n}{n!} \Rightarrow Q$ exists

needed twice

$\Rightarrow |K| \geq (q/2)^n$ $\boxtimes$

Nikodym Sets?

- Similar analysis $\Rightarrow |N| \geq \left(\frac{q}{2}\right)^n$
- But no matching upper bound
- Recent work with Guo:

$$q = 2^t \; ; \; n = O(1) \; ; \; q \to \infty$$

$$\Rightarrow |N| \geq (1 - o(1)) \cdot q^n$$

Key Idea: Set of functions $\{Q \mid \deg(Q|_\ell) < D \; \forall \text{ line } \ell\}$ has much higher dim. than set of deg D poly

Conclusions

- Polynomial Method
  - Simple, Elegant, Widely used
- Multiplicity Method
  - Almost as Simple
  - Very Powerful
  - Not as widely used

THANK YOU !!