Polynomial Method Notes

Jacob Denson

February 13th, 2024

1 Finite Field Kakeya Without Polynomials

In order to see why the polynomial method might be necessary in order to understand the finite field conjecture, let us begin by discussing some techniques that were used to analyze the finite field conjecture without the polynomial method. We start with an elementary bound, which shows that a union of a small number of lines intersect in a negligible way.

Lemma 1. *If $X \subset \mathbb{F}_q^n$ contains $s \leq q+1$ distinct lines, then $\#(X) \geq sq/2$.*

Proof. Order the lines $l_1, \ldots, l_n$. Any two lines intersect in a single place. Thus

$$\# \left(l_i - \bigcup_{j<i} l_j \right) \geq \#(l_i) - (i-1) \geq q - (i-1).$$

Thus

$$\#(X) \geq \sum_{i=1}^{s} \# \left(l_i - \bigcup_{j<i} l_j \right) \geq \sum_{i=1}^{s} q - (i-1) \geq sq/2 \qquad \square.$$

The bound is tight when we consider $s \leq q$, and proves Kakeya for $n = 2$, since Kakeya sets X in $\mathbb{F}_q^2$ contain $q+1$ lines, and so we can apply the result above with $s = q$ to conclude that $\#(X) \geq q^2/2$. For s between q and q^2, there is in general no possible improvement to apply the bound above with $s = q$, since a plane X in $\mathbb{F}_q^n$ contains $q(q+1)$ lines and q^2 points. However, for $s > q^2$, we can apply the *bush method* to get a betweenter bound.

Lemma 2. *If $X \subset \mathbb{F}_q^n$ contains s distinct lines, then $\#(X) \gtrsim qs^{1/2}$.*

Proof. Here's the idea. If X is small, then by pidgeonholing X contains a point x_0 lying on the intersection of many of the lines contained in X. Once we remove x_0 from these lines, each of these lines are disjoint, and so we obtain a contradiction.

Let's be more precise. For each point $x \in X$, let B_x be the *bush* corresponding to x, the union of the set $\mathcal{B}_x$ of lines passing through x. Now

$$\mathbb{E}_{x \in X}[\mathcal{B}_x] = \frac{1}{\#X} \sum_{p \in X} \#\mathcal{B}_p = \frac{sq}{\#(X)}.$$

Thus there is $x_0 \in X$ with $\#\mathcal{B}_{x_0} \geq qs/\#(X)$. Let $\mathcal{B}_{x_0} = \{l_1, \ldots, l_r\}$. Since each pair of lines intersects uniquely at x_0, the sets $l_j - \{x_0\}$ are disjoint from one another. Thus

$$\#(X) \geq \sum_{j=1}^{r} \#(l_j - \{x_0\}) = (\#X)(q-1) \geq q(q-1)s\#(X)^{-1}.$$

Rearranging and taking square roots gives that $\#(X) \gtrsim qs^{1/2}$. $\qquad\square$

Since a Kakeya set X in $\mathbb{F}_q^n$ contains $\gtrsim q^{n-1}$ distinct lines, we conclude that

$$\#(X) \gtrsim q^{\frac{n+1}{2}}.$$

We aren't exploiting the hypothesis enough, because X not only contains q^{n-1} distinct lines, but these lines are also *pointing in different directions*. In particular, at most $q+1$ of these lines lie in a two dimensional plane, so we can apply the *hairbrush method*.

Lemma 3. *If $X \subset \mathbb{F}_q^d$ contains s distinct lines $l_1, \ldots, l_s$, such that at most $q+1$ of these lines lie in any two dimensional plane, then $\#(X) \gtrsim q^{3/2}s^{1/2}$.*

Proof. For each j, define the *hairbrush* H_j to be the union of the set $\mathcal{H}_j$ of lines l_k with $k \neq j$ which intersect l_j. Now the average point intersects $qs/\#(X)$ of the lines $\{l_j\}$, and since a line contains q points, the average line intersects at least $\gtrsim q^2s/\#(X)$ other lines. Thus we can fix j_0 such that $\#\mathcal{H}_{j_0} \gtrsim q^2s/\#(X)$. Let $\Pi_1, \ldots, \Pi_r$ be the set all planes generated from l and some line in $\mathcal{H}_j$. If Π_n contains s_n lines in $\mathcal{H}_j$, then, since $s_n \leq q$, the union of the functions in Π_n essentially behave as if they were disjoint, i.e. $\#(X \cap (\Pi_n - l)) \geq q(s_n/2 - 1)$. The sets $\Pi_n - l$ are disjoint, so

$$\begin{aligned}
\#(X \cap H_j) &\geq \sum_n \#(X \cap (\Pi_n - l)) \\
&= \sum_n q(s_n/2 - 1) \\
&\geq (q/2)(\#\mathcal{H}_{j_0}) - r \\
&\geq (q/2 - 1)\#\mathcal{H}_{j_0} \\
&\gtrsim q^3s/\#(X).
\end{aligned}$$

Thus $\#(X) \gtrsim q^{3/2}s^{1/2}$.

More precisely,

$$\mathbb{E}_j[\#\mathcal{H}_j] = \frac{1}{s}\sum_j \#\mathcal{H}_j = \frac{1}{s}\sum_j \sum_{p \in l_j}[\#\mathcal{B}_p - 1]$$

$$= \frac{1}{s}\left[\sum_p \#(\mathcal{B}_p)^2\right] - q = \frac{\#(X)}{s}\mathbb{E}_{p \in X}[\#\mathcal{B}_p^2] - q$$

$$\geq \frac{\#(X)}{s}\mathbb{E}_{p \in X}[\#\mathcal{B}_p]^2 - q$$

$$= \frac{\#(X)}{s}\left[\frac{qs}{\#(X)}\right]^2 - q$$

$$= q^2 s \#(X)^{-1} - q.$$

If $\#(X) \leq q^{3/2}s^{1/2}$ and $s \geq q$, this quantity is $\gtrsim q^2 s/\#(X)$. $\qquad\square$

To show why the hypothesis above cannot be used to push past this bound over finite fields, we consider the *Hermitian variety*. Let $q = p^2$, and consider the variety H in $\mathbb{F}_q^3$ given by

$$H = \{(x,y,z) \in \mathbb{F}_q^3 : x^{p+1} + y^{p+1} + z^{p+1} = 1\}.$$

The map $x \mapsto x^p$ is a field isomorphism of $\mathbb{F}_q$, and we let $\overline{x} = x^p$. Then

$$H = \{(x,y,z) \in \mathbb{F}_q^3 : x\overline{x} + y\overline{y} + z\overline{z} = 1\}.$$

We note the following facts:

- The function $x \mapsto x^{p+1}$ is a group homomorphism of $\mathbb{F}_q^*$ onto $\mathbb{F}_p^*$ with a kernel of order $p + 1$.

- $\#(H) \sim q^{5/2}$ since, for each $x, y \in \mathbb{F}_q$, there are $p+1 \sim q^{1/2}$ points $z \in \mathbb{F}_q$ with $z^{p+1} = x^{p+1} + y^{p+1}$.

- Define $(v,w) = \sum v_j \overline{w_j}$. If we let $U(\mathbb{F}_q^n)$ be the group of all invertible matrices $M \in GL(\mathbb{F}_q^3)$ such that

$$(Mv, Mw) = (v, w)$$

  for all $v, w \in \mathbb{F}_q^3$, then $U(\mathbb{F}_q^3)$ acts transitively on H. Indeed, any element v of $\mathbb{F}_q^3$ is the element of some 'orthogonal' basis v, w, u, by applying a variant of Gram-Schmidt, and then the matrix M with columns v, w, and u is in $U(\mathbb{F}_q^3)$, and maps e_1 to v.

- The last point implies that if s is the number of lines in H passing through e_1, then H contains $s\#(H)/q \sim sq^{3/2}$ lines. For $v = (m, n) \in \mathbb{F}_q^2$, consider the line

$$l_v = \{(1 + t, tm, tn) : t \in \mathbb{F}_q\},$$

which counts all but $O(q)$ lines passing through e_1. Then this line is contained in H if and only if the polynomial

$$(1+t)^{p+1} + (tb)^{p+1} + (tc)^{p+1} - 1$$

vanishes for all t. We can write this polynomial as

$$(1+t)(1+t^p) + t^{p+1}b^{p+1} + t^{p+1}c^{p+1} - 1$$

expanded as
$$(1 + b^{p+1} + c^{p+1})t^{p+1}.$$

Since $p+1 < q$, This polynomial vanishes if and only if $1+b^{p+1}+c^{p+1} = 0$, an equation with $\sim q^{3/2}$ solutions. Thus H contains $\sim q^3$ lines.

- The variety H does not contain a 2-plane. If $V \subset \mathbb{F}_q^3$ is a 2-dimensional subspace, then there is $v \in V$ with $v \cdot \bar{v} = 0$.

- Now we show lines contained in H do not concentrate in planes.

- Consider some plane intersecting H. We claim this plane contains at most $q + 1$ points. By symmetry, we may assume this plane passes through e_1. We can thus write the plane as the solution set to the equation

$$a'x + b'y + c'z = a.$$

A line in H generated by some a, b, and c is contained in this plane if and only if
$$a^{p+1} + b^{p+1} + c^{p+1} = 0 \quad \text{and} \quad a'a + b'b + c'c = 0$$

Ellenberg Hablicsek proved if q is prime, then any set of lines in $\mathbb{F}_q^3$ with at most q lines in any 2-planemust have side $\gtrsim q^3$.

2 Why Polynomials?

What helps with finite field Kakeya.

- $\dim(\text{Poly}_D) \sim D^n$ is large.

- But for any line l, the vector space

$$\{f|_l : f \in \text{Poly}_D\}$$

is $D + 1$ dimensional.

Most function spaces do not have this property, e.g. the space of trigonometric polynomials of degree at most D has dimension $\sim D^n$, but for a generic line l, the set
$$\{f|_l : f \in \text{Poly}_D\}$$

has dimension $\sim D^n$. Indeed, a generic line l is equal to $\{x_0 + tv : t \in \mathbb{R}\}$, for $v \in \mathbb{R}^n$ such that $\xi \cdot v \neq 0$ for all $\xi \in \mathbb{Z}^n$. If

$$f(t) = \sum_{|\xi| \leq D} a_\xi e^{2\pi i \xi \cdot (x_0 + tv)},$$

is equal to zero for all $t \in \mathbb{R}$, then in particular, for all $k \geq 0$,

$$0 = \partial^k f(0) = \sum_{|\xi| \leq D} a_\xi (\xi \cdot v)^k.$$

The matrix with entries $\{(\xi \cdot v)^k : |\xi| \leq D, k \leq D^n\}$ is then an invertible Van Der Monde matrix (the quantities $\{\xi \cdot v : \xi \in \mathbb{Z}^d, |\xi| \leq D\}$ are distinct) and so we conclude that $a_\xi = 0$ for all ξ.

Theorem 4. *If $\#\mathbb{F} \geq D + 1$ and $V \subset Func(\mathbb{F}^n, \mathbb{F})$ has the property that for any line l and any $f \in V$, if f vanishes on $D + 1$ points on l, then f vanishes for all points on l. Then $\dim(W) \lesssim D^n$.*

Proof. For each line l, the function

$$\prod_{p_1, \ldots, p_d} (f(p_1) -)$$

$\square$

3   s

Encode Combinatorial Information in terms of 'low complexity' polynomials, and then use the size of the set in combination with some robust properties of low complexity polynomials to derive some properties of the set. You have to be a little clever, or 'change your perspective' to make these arguments work (e.g. Mockenhaupt, Tao, 2004 showed that Kakeya sets in k^n cannot be contained in low degree polynomials, but were unable to see why this implied Kakeya sets must contain k^n points - The paper even ironically says 'this Theorem is far from a proof of the finite field Kakeya conjecture'). We will be able to obtain deeper results using polynomial methods by exploiting deeper properties about algebraic surfaces.

JACOB DENSON, UW MADISON
email: jcdenson@wisc.edu