POLYNOMIAL METHODS IN SOLVING COMBINATORICS PROBLEMS

YUDHISTER KUMAR

Abstract. This expository paper introduces the polynomial method in combinatorics and uses it to prove the Finite Field Kakeya Conjecture as well as the Joints problem in Euclidean space.

1. Introduction

The polynomial method in combinatorics is a method of solving combinatorics problems which uses polynomials to capture some underlying structure in the combinatorics problem and then reasons about the problem via the polynomial's algebraic properties. Roughly, the process is something along the lines of: embed the combinatorical problem into a vector space, construct a low-degree polynomial that is zero on a certain set, and show that because of this the original set must satisfy some properties.

The method was first used to great effect to solve the finite field Kakeya conjecture by Dvir in 2008, and has since been used to solve other related problems (such as the joints problem in this paper). This paper is meant to give an overview of the solutions to the finite field Kakeya conjecture and joints problem with the polynomial method, and hopefully to give you a better understanding of how it is used.

2. Finite Field Kakeya Conjecture

The finite field Kakeya problem is a toy problem of the more general *Kakeya* problem: *how small can you make sets in $\mathbb{R}$ such that they still contain a line segment in every direction?* Instead of operating over $\mathbb{R}^n$, it operates over $\mathbb{F}_q^n$.

We first formalize the definition of a Kakeya set.

Definition 2.1 (Kakeya Set)**.** A set $K \subset \mathbb{F}_q^n$ is a Kakeya set if for all $a \in \mathbb{F}_q^n$ there exists $b \in \mathbb{F}_q^n$ such that $\{at + b : t \in \mathbb{F}_q\} \subseteq K$. That is, for all a, K contains a line in that direction.

With this, we can now state the formal Finite Field Kakeya Theorem.

Theorem 2.2 (Finite Field Kakeya Theorem)**.** *If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then*

$$|K| \geq c_n q^n,$$

where $c_n = (10n)^{-n}$.

The proof of this consists of proving some basic properties about a polynomial which vanishes on K, and it is much shorter than most suspected when tackling the problem (as the Kakeya problem is still unsolved and has not yielded to such basic methods yet). We will need two key pieces of machinery to prove 2.2: parameter counting arguments and the vanishing lemma.

Date: February 2023.

Proposition 2.3. *Let $S \in \mathbb{F}^n$ be some finite set. Then, if $DimPoly_D(\mathbb{F}^n) > |S|$, there is a nonzero polynomial $P \in Poly_D(\mathbb{F}^n)$ that vanishes on S.*

Proof. Let $p_1, \ldots, p_{|S|}$ be the points of S. We let E be the evaluation map $E : \mathrm{Poly}_D(\mathbb{F}^n) \to \mathbb{F}^{|S|}$ defined by

$$E(Q) = (Q(p_1), \ldots, Q(p_{|S|}).$$

The map E is a linear map, and the kernel of E is exactly the set of polynomials that vanish on S. If $\dim \mathrm{Poly}_D(\mathbb{F}^n) > |S|$, by the Rank-Nullity Theorem, this map must have a non-trivial kernel, therefore there exists some polynomial in this set that vanishes on S. ■

This raises the obvious question, what is the dimension of $\mathrm{Poly}_D(\mathbb{F}^n)$?

Lemma 2.4. *We have an exact formula for the dimension, mainly that*

$$\dim Poly_D(\mathbb{F}^n) = \binom{D+n}{n}.$$

Proof. To find the dimension, we can count the number of monomials in $\mathrm{Poly}_D(\mathbb{F}^n)$, as these form the basis of the polynomial space. Fix D, n, and let the monomial $x_1^{D_1} \ldots x_n^{D_n}$ be represented by a string of D $*$ and n $|$ (stars and bars) such that each unique monomial corresponds to the stars and bars configuration of D_1 $*$, a $|$, etc. with $D - \sum D_i$ stars at the end. The total number of such configurations is $\binom{D+n}{n}$. ■

It is also useful to keep in mind the heuristic $\dim \mathrm{Poly}_D(\mathbb{F}^n) \geq D^n/n!$, which follows from 2.5.

Therefore, we get the following.

Lemma 2.5 (Parameter Counting)**.** *If $S \subset \mathbb{F}^n$ and $|S| < \binom{D+n}{n}$, then there is a nonzero polynomial $P \in Poly_D(\mathbb{F}^n)$ that vanishes on S.*

This follows from 2.3 and 2.5. Now, we will prove the vanishing lemma, starting with an elementary lemma.

Lemma 2.6. *If $P \in Poly_D(\mathbb{F}^n)$, and if P vanishes at $D+1$ points, then P is the zero polynomial.*

To show 2.6, we need two other lemmas.

Lemma 2.7. *If $P(x) \in Poly_D(\mathbb{F})$ is a polynomial in one variable and $x_1 \in \mathbb{F}$, then we can write P in the form*

$$P(x) = (x - x_1)P_1(x) + r.,$$

where $P_1(x) \in Poly_{D-1}(\mathbb{F})$ and $r \in \mathbb{F}$.

Proof. We will show this by induction on D. Our base case, when $D = 0$, P is a constant polynomial and this is obviously true.

Let $P(x) = \sum_{i=0}^{D} a_i x^i$. Let $Q(x) = P(x) - (x - x_1)(a_D x^{D-1})$. As the x^D term of $Q(x)$ vanishes, $Q(x) \in \mathrm{Poly}_{D-1}(\mathbb{F})$. By induction, we have that

$$P(x) - (x - x_1)(a_D x^{D-1}) = Q(x) = (x - x_1)Q_1(x) + r,$$

where $Q_1(x) \in \mathrm{Poly}_{D-2}(\mathbb{F})$ and $r \in \mathbb{F}$. Therefore, we see that

$$P(x) = (x - x_1)(a_D x^{D-1} + Q_1(x)) + r,$$

which completes the proof by induction. ■

Lemma 2.8. *If $P(x) \in Poly_D(\mathbb{F})$ is a polynomial over a field $\mathbb{F}$ and $P(x_1) = 0$ for some $x_1 \in \mathbb{F}$, then $P(x) = (x - x_1)P_1(x)$ for some polynomial $P_1(x) \in Poly_{D-1}(\mathbb{F})$.*

Proof. We can write P as $P(x) = (x - x_1)P_1(x) + r$ by 2.8. Substituting in $P(x_1) = 0$, we see that $r = 0$. ■

Proposition 2.9. *If $P \in Poly_D(\mathbb{F})$ and P vanishes at $D + 1$ points on a line l, then P vanishes at every point of l.*

Proof. We prove 2.9 by induction on D. Our base case is when $D = 0$, where P is constant. If P goes to 0 at any point, it is then the zero polynomial.

For the inductive step, let $P \in \text{Poly}_D(\mathbb{F})$, and assume P vanishes at $D + 1$ distinct points $x_1, \ldots, x_{D+1}$. By 2.8, there exists some polynomial $P_1 \in \text{Poly}_{D-1}(\mathbb{F})$ such that

$$P(x) = (x - x_{D+1})P_1(x).$$

However, P_1 must vanish on $x_1, \ldots, x_D$, and by the inductive hypothesis therefore P_1 is the zero polynomial. Therefore, P is the zero polynomial, and we have completed the proof. ■

Let a line $l \subset \mathbb{F}^n$ be a one-dimensional affine subspace.

Corollary 2.10 (Vanishing Lemma). *If $P \in Poly_D(\mathbb{F}^n)$ and P vanishes at $D + 1$ points on a line l, then P vanishes at every point in l.*

Proof. We can parametrize an arbitrary line l with a map $x : \mathbb{F} \to \mathbb{F}^n$, such that $x(t) = at+b$, for vectors $a, b \in \mathbb{F}^n$ with $a \neq 0$. Let $Q(t) = P(x(t)) = P(at + b)$, which is a polynomial in one variable of degree $\leq D$. As P vanishes at $D + 1$ points of l, Q vanishes on $D + 1$ points of t. By 2.9, Q is the zero polynomial, so P vanishes on l. ■

We can now prove the Finite Field Kakeya Theorem!

Proof. We will use a proof by contradiction. Suppose there exists a Kakeya set $K \subset \mathbb{F}_q^n$ such that $|K| < (10n)^{-n}q^n$. By 2.5, there is a nonzero polynomial P that vanishes on K with Deg $P \leq n|K|^{1/n} < q$.

Let $D =$ Deg P. We can write P as the sum of two polynomials: P_D, the polynomial consisting of the terms in P of degree D, and Q, containing the rest. Observe that P_D is nonzero, and that Deg $Q < D$.

Let $a \in \mathbb{F}_q^n$, with $a \neq 0$. Pick b such that the line $\{at + b : t \in \mathbb{F}\} \subset K$. Let there be a polynomial in one variable $R(t) = P(at + b)$. Observe that R vanishes for all $t \in \mathbb{F}$, and Deg $R \leq D < q$. By 2.10, R is the zero polynomial, so every coefficient of R is 0. However, the coefficient of t^D in R is exactly $P_D(a)$. So, we see that $P_D(a)$ vanishes for all $a \in \mathbb{F}_q^n/\{0\}$. As P_D is homogenous of degree $D \geq 1$, P_D also vanishes at 0, and also vanishes at all points in $\mathbb{F}_q^n$. Therefore, it is the zero polynomial, which is a contradiction.

This proves 2.2. ■

2.1. **Connection to Projective Spaces.**

The process of splitting P into its part of highest degree P_D and the rest in Q has an interesting geometric interpretation.

Definition 2.11 (Projective Spaces). The projective space $\mathbb{PF}^n$ is the set of equivalence classes of $\mathbb{F}^{n+1}/\{0\}$ where elements $x, y \in \mathbb{F}^{n+1}/\{0\}$ are equivalent if they are equivalent modulo some scalar factor: that is, $x \sim y \iff x = \lambda y$ for some $\lambda \in \mathbb{F}$.

We can write $\mathbb{PF}^n$ as a disjoint union of $\mathbb{F}^n$ and $\mathbb{PF}^{n-1}$. The natural way to do this is to identify some point $(x_1, \ldots, x_n) \in \mathbb{F}^n$ with the equivalence class of $(x_1, \ldots, x_n, 1) \in \mathbb{PF}^n$. Then, the equivalence classes of $(x_1, \ldots, x_n, 0) \in \mathbb{PF}^n$ naturally identify themselves to points in $\mathbb{PF}^{n-1}$.

Definition 2.12. The points in $\mathbb{PF}^{n-1} \subset \mathbb{PF}^n$ are called the points at infinity.

Observe that every line in $\mathbb{F}^n$ can be extended to a projective line in $\mathbb{PF}^n$ by adding a point at infinity. Take the line $\{at + b : t \in \mathbb{F}\}$ for $a, b \in \mathbb{F}^n$ where $a \neq 0$. Then, in projective space, this line extends to include the point $(a, 0) \in \mathbb{PF}^n$.

For polynomials, the process is similar (for extending the zero set). Let $P \in \text{Poly}_D(\mathbb{F}^n)$, and let $Z(P) \subset \mathbb{F}^n$. Then, if $a \in \mathbb{F}_q^n$ and $a \neq 0$, the point at infinity $(a, 0)$ only lies in the extended $Z(P)$ iff $P_D(a) = 0$.

This proof of the Finite Field Kakeya Theorem 2.2 essentially shows that if a line $l \subset \mathbb{F}^n$ lies in the zero set of a polynomial P of degree $< q$, then the point of l at infinity also lies in $Z(P)$. This can be thought of as a version of the vanishing lemma in projective space.

Therefore, we can summarize the proof of 2.2 as thus: if $K \subset \mathbb{F}_q^n$ is a small Kakeya set, then by parameter counting 2.5 there exists a polynomial that vanishes on K with degree less than q. Because K is Kakeya, the polynomial vanishes on one line in every direction, and by the version of the vanishing lemma for projective space it therefore vanishes at all the points of infinity of $\mathbb{PF}_q^n$. However, then it vanishes at too many points, leading to a contradiction. For more information see [Gut10, Chapter 2].

3. Joints Problem

Let $\mathcal{L}$ be a set of lines in $\mathbb{R}^3$. A *joint* of $\mathcal{L}$ is a point which lies in three non coplanar lines of $\mathcal{L}$ (is an intersection of three lines such that they are not coplanar). What is the maximal number of joints that can be formed from L lines?

Theorem 3.1. *Any L lines in $\mathbb{R}^3$ determine $\leq 10L^{3/2}$ joints.*

Lemma 3.2. *If $\mathcal{L}$ is a set of lines in $\mathbb{R}^3$ that determines J joints, then one of the lines contains at least $3J^{1/3}$ joints.*

Proof. Let P be the lowest degree non-zero polynomial that vanishes at every joint of $\mathcal{L}$. By 2.5, the degree of P is less than or equal to $3J^{1/3}$.

We will prove the lemma by contradiction, so assume that every line of $\mathcal{L}$ has $> 3J^{1/3}$ joints. By the vanishing lemma, 2.10, P must vanish on every line of $\mathcal{L}$.

Now we can look at the gradient of P at each joint of $\mathcal{L}$.

Lemma 3.3. *If x is a joint of $\mathcal{L}$, and if a smooth function $F : \mathbb{R}^3 \to \mathbb{R}$ vanishes on the lines of $\mathcal{L}$, then ∇F vanishes at x.*

Proof. As x lies in three non coplanar lines of $\mathcal{L}$, the tangent vectors for the three lines intersecting x form a basis for $\mathbb{R}^3$. For the tangent vectors v_i, $i = 1, 2, 3$, as $\nabla F(x) \cdot v_i = 0$, we have that $\nabla F(x) = 0$, because v_1, v_2, v_3 are a basis for $\mathbb{R}^3$. ■

Therefore, the derivatives of P vanish at each joint. As the derivatives of P have smaller degree than P, and P was the minimal degree non-zero polynomial that vanishes at each joint, then each derivative of P is zero, so P must be constant. As P is non-zero, then there must be no joints at all, and this is a contradiction. ■

To prove 3.1, we do some algebra.

Proof. Let $J(L)$ be the maximum number of joints that can be formed by L lines. If $\mathcal{L}$ is a set of L lines, then by 3.2 one of the lines contains at most $3J(L)^{1/3}$ of the joints. The numberr of joints not on this line is at most $J(L-1)$. Therefore, we can bound $J(L)$ as

$$J(L) \leq J(L-1) + 3J(L)^{1/3}.$$

Repeating this, we see that

$$J(L) \leq J(L-1) + 3J(L)^{1/3} \leq \cdots \leq L \cdot 3J(L)^{1/3}.$$

Rearranging gives us that $J(L)^{2/3} \leq 3L$, which implies 3.1. ■

References

[Gut10] Larry Guth. *Polynomial Methods in Combinatorics*. American Mathematical Society, first edition, 2010.