APPLICATIONS OF POLYNOMIAL METHODS

SIMON PARK

Abstract. Throughout the semester, we have seen the polynomial method being applied to various problems. Here, we review its application on the Kakeya Problem with a more thorough discussion about why polynomials were effective at solving the problem. Then using the same method, we approach other problems in combinatorial geometry: Joints Problem and Nikodym Problem. We also draw a connection between the results in these problems with the Reed-Muller code, another application of the polynomial method.

I pledge my honor that this paper represents my own work in accordance with University regulations. /s Juhyun 'Simon' Park

Contents

1. Review of Polynomial Methods

1.1. **Finite Field Kakeya Conjecture.** We briefly review some of the definitions and terminologies related to the Finite Field Kakeya Conjecture.

Definition 1. Let $\mathbb{F}$ be a field. A set $L \subset \mathbb{F}^n$ is called a *line* if L can be expressed as $L = \{at + b : t \in \mathbb{F}\}$ for some $a, b \in \mathbb{F}^n$ and $a \neq 0$.

Definition 2. Let $\mathbb{F}_q$ be a finite field. A set $K \subset \mathbb{F}_q^n$ is called a *Kakeya set* if for any $a \in \mathbb{F}_q^n \setminus \{0\}$, there is a line $L_a \ni a$ such that $L_a \subset K$; that is, there is a $b \in \mathbb{F}_q^n$ such that $\{at + b : t \in \mathbb{F}_q\} \subset K$.

Date: January 14, 2022.

Conjecture 3 (Finite Field Kakeya Conjecture)**.** *If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq c_n q^n$ where c_n is a constant that only depends on n.*

1.2. **Attempts Without Polynomials.** In class, we have seen two methods that approached the Finite Field Kakeya Conjecture using incidence geometry: the Bush Method and the Hairbrush Method. Here, we reproduce Bourgain's Bush Method to compare with the polynomial method.

Theorem 4 ([2], [4])**.** *If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq \frac{1}{2} q^{\frac{n+1}{2}}$.*

Proof. Let $L_1, \cdots, L_k$ be distinct, non-parallel lines contained in K and let L be the union of these lines. By direct calculation, $k \geq q^{n-1}$. By the Pigeonhole Principle, there is a point $p \in L$ that is on at least $kq\,|L|^{-1}$ of these lines. These lines are disjoint except at p. Therefore,

$$(q-1) \cdot kq\,|L|^{-1} \leq |L|$$

By rearranging the terms, we get

$$|K| \geq |L| \geq (kq(q-1))^{1/2} \geq (q^{n-1}(q-1)^2)^{1/2} \geq q^{\frac{n-1}{2}} \cdot (q-1) \geq \frac{1}{2} q^{\frac{n+1}{2}}$$

□

1.3. **Polynomial Methods.** Here, we reproduce Dvir's Polynomial Method, first presented in [1] and simplified in [2]. The following lemmas were proven in class and will be presented here without proof.

Definition 5. When $\mathbb{F}$ is a field, $\text{Poly}_D(\mathbb{F}^n)$ is the set of polynomials in n variables, with coefficients in $\mathbb{F}$ and with total degree at most D.

Lemma 6. *Let $\mathbb{F}$ be a field. For any $n \geq 2$, for any finite set $S \subset \mathbb{F}^n$, there is a non-zero polynomial that vanishes on S with degree $\leq n\,|S|^{1/n}$.*

Lemma 7. *Let $\mathbb{F}$ be a field. If $P \in Poly_D(\mathbb{F})$ and if P vanishes at $D+1$ points, then P is the zero polynomial.*

Lemma 8. *Let $\mathbb{F}$ be a field. If $P \in Poly_D(\mathbb{F}^n)$ and if P vanishes at $D+1$ points on a line $L \subset \mathbb{F}^n$, then P vanishes at every point of L.*

Lemma 9. *If $P \in Poly_D(\mathbb{F}_q^n)$, P vanishes everywhere, and $D < q$, then P is the zero polynomial.*

The following theorem proves the Finite Field Kakeya Conjecture 3.

Theorem 10. *If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq (2n)^{-n} q^n$.*

Proof. Assume to the contrary that $K \subset \mathbb{F}_q^n$ is a Kakeya set with $|K| < (2n)^{-n} q^n$. By Lemma 6, there is a non-zero polynomial P that vanishes on K with degree $\leq n\,|K|^{1/n} < q$. Let D be the degree of P and decompose P into $P = P_D + Q$ where P_D is the sum of all monomials of degree D and where Q has degree $< D$. Fix some non-zero $a \in \mathbb{F}_q^n$. Choose b so that the line $\{at + b : t \in \mathbb{F}_q\}$ is contained in K. Then the polynomial $R(t) := P(at+b)$ in one variable has degree $\leq D$ and vanishes on every $t \in \mathbb{F}_q$. By Lemma 7, R is the zero polynomial. Notice that the coefficient of t^D in R is exactly $P_D(a)$ and must be zero. This holds for any $a \neq 0$. Notice that $P_D(0)$ is also zero because it only contains monomials of degree $D \geq 1$. Lemma 9 gives the desired contradiction. □

1.4. **Discussion.** In section 1.2, we saw an example of a method using ideas from incidence geometry. Other similar proofs also rely on the Pigeonhole Principle. Using the principle, they first find a lower bound on the number of lines contained in an arbitrary Kakeya set. The lower bound is proportional to the size of the space (q^n) and inversely proportional to the size of the Kakeya set ($|K|$). The size of the Kakeya set is then proportional to the number of these lines. Combining the two results means that the square of the size of the Kakeya set ($|K|^2$) is proportional to the size of the space (q^n). Even with slight modifications or improvements to the method, the lower bound of the dimension of a Kakeya set is approximately half of the dimension of the space.

Then what is so special about polynomials? [2] notes that the dimension of $\text{Poly}_D(\mathbb{F}_q^n)$ is on the same order of growth as D^n, which is surprisingly large. This means that there is a lot of polynomials to choose from. This extent of freedom allows us to choose a polynomial that vanishes on a finite set in Lemma 6 with a very small degree. On the other hand, once fixed to a line, a polynomial operates very rigidly: a non-zero polynomial of degree D can vanish at up to D points on a given line. This means that the the polynomial we chose in Lemma 6 cannot have too small of a degree, without forcing it to be a zero polynomial. This discrepancy is where the Polynomial Method draws the desired conclusion.

[6] also gives a geometric interpretation to the polynomial method. The zero set of a polynomial can be interpreted as a hypersurface in the finite field. With this model, we can reinterpret the lemmas above. Lemma 6 says that 'small' sets in the finite field can be captured by hypersurfaces of low-degree polynomials. Lemma 7 says that the hypersurface of a polynomial is either very small if the degree of the polynomial is non-zero (at most equal to the degree) or very large if the degree is zero (the entire space). Lemma 8 describes how rigid a line is: as soon as more than d points of a line is contained in the hypersurface defined by a degree d polynomial, the entire line "snaps into place" and is completely contained in the surface.

In the following sections, we will discuss two other problems in combinatorial geometry and how polynomial methods can be applied to solve them.

2. Joints Problem and Polynomial Methods

2.1. **Joints Problem.**

Definition 11. Let $\mathcal{L}$ be a set of lines in $\mathbb{R}^3$. A point in $\mathbb{R}^3$ is called a *joint* of $\mathcal{L}$ if it lies in three non-coplanar lines of $\mathcal{L}$.

The Joints Problem asks for the maximal number of joints defined by L lines. Let us first consider a very simple example. Consider $S = [1, N] \times [1, N] \times [1, N]$ and all the integer grid lines passing through S that are parallel to one of the three axes. That is, consider all lines of the form

$$x_{i_1} = j_1, x_{i_2} = j_2 \quad \text{where} \quad i_1, i_2 \in \{1, 2, 3\}, \quad j_1, j_2 \in \{1, 2, \cdots, N\}$$

There are in total $3N^2$ lines. But notice that every integer point in S is a joint. Therefore, there are in total N^3 joints. If we let $L = 3N^2$ be the number of lines, we have approximately $L^{3/2}$ joints. People have been trying to find an example of a set of lines that contain more

joints (exponent greater than 3/2), but to little success. This led to the following conjecture.

Conjecture 12. *If $\mathcal{L}$ is a set of lines in $\mathbb{R}^3$, then the number of joints of $\mathcal{L}$ is at most $c\,|\mathcal{L}|^{3/2}$ where c is a constant.*

If the conjecture above is true, then the example of the lattice lines would be proven to be the most optimal layout.

2.2. **Polynomial Methods.** Polynomials were first applied to the Joints Problem in [3], and the method was later refined and simplified in [1], [2], and [5]

Lemma 13. *If p is a joint of $\mathcal{L}$, and if a smooth function $g : \mathbb{R}^3 \to \mathbb{R}$ vanishes on all lines of $\mathcal{L}$, then ∇g vanishes at p.*

Proof. Since p is a joint of $\mathcal{L}$, it lies in three non-coplanar lines $\ell_1, \ell_2, \ell_3 \in \mathcal{L}$. Let u_1, u_2, u_3 be the directional vectors for these lines. That is, for $i = 1, 2, 3$, let $u_i \in \mathbb{R}^3$ be a vector such that $\ell_i = \{p + tu_i : t \in \mathbb{R}\}$. Since g vanishes on the three lines, the polynomial $h_i(t) := g(p + tu_i)$ is identically zero. In particular, the coefficient of t in this polynomial is exactly $\langle \nabla g(p), u_i \rangle$ and is zero. Since the three lines ℓ_1, ℓ_2, ℓ_3 are not coplanar, the directional vectors u_1, u_2, u_3 are linearly independent, and therefore, $\nabla g(p) = 0$ □

Lemma 14. *If there are $J > 0$ joints of a set $\mathcal{L}$ of lines in $\mathbb{R}^3$, then at least one of the lines contains no more than $3J^{1/3}$ joints.*

Proof. Assume to the contrary that each of the lines contains at least $3J^{1/3}$ joints. Let g be a lowest degree non-zero polynomial that vanishes at every joint of $\mathcal{L}$. Since g has at least one zero, it is trivial that the degree of g is non-zero. Also, by Lemma 6, the degree of g is at most $3J^{1/3}$. Then by Lemma 8, g vanishes on all points of every line of $\mathcal{L}$.

By Lemma 13, ∇g vanishes on all joints. This means that each of the three partial derivatives of g is a polynomial that vanishes on all joints. But it is easy to check that if g is a non-zero polynomial with non-zero degree, g has at least one non-zero partial derivative of degree strictly less than the degree of g. This goes against the assumption that g was chosen to have the minimal degree out of all polynomials that vanish on the joints. □

We are now ready to solve the Joints Problem.

Theorem 15. *If $\mathcal{L}$ is a set of lines in $\mathbb{R}^3$, then the number of joints of $\mathcal{L}$ is at most $(3\,|\mathcal{L}|)^{3/2}$.*

Proof. Let J_L be the maximum number of joints that can be formed by L lines. It is clear that J_L is an increasing function of L. Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$. By Lemma 14, we know that one of the lines contains at most $3J_L^{1/3}$ of the joints. The number of joints not on this line is at most J_{L-1}. We can then use recursion to upper bound J_L:

$$J_L \leq J_{L-1} + 3J_L^{1/3} \leq J_{L-2} + 3J_{L-1}^{1/3} + 3J_L^{1/3} \leq J_{L-2} + 2 \cdot 3J_L^{1/3} \leq \cdots \leq L \cdot 3J_L^{1/3}$$

Rearranging the inequality above gives $J_L^{2/3} \leq 3L$ which is the desired result. □

3. Nikodym Problem and Polynomial Methods

3.1. Finite Field Nikodym Problem.

Definition 16. Let $\mathbb{F}_q$ be a finite field. A set $N \subset \mathbb{F}_q^n$ is called a *Nikodym set* if for any $p \in \mathbb{F}_q^n$, there is a line $L_p \ni p$ such that $L_p \setminus \{p\} \subset N$.

Just like the Finite Field Kakeya Problem, the Finite Field Nikodym Problem asks for the lower bound of the dimension of an arbitrary Nikodym set.

3.2. Polynomial Methods.

By applying a method very similar to the one we used in 1.3, we can easily solve the Finite Field Nikodym Problem.

Theorem 17 ([1], simplified in [2])**.** *If $N \subset \mathbb{F}_q^n$ is a Nikodym set, then $|N| \geq (3n)^{-n} q^n$.*

Proof. Proof by contradiction. Assume $|N| < (3n)^{-n} q^n$. By Lemma 6, we can find a non-zero polynomial P that vanishes on N with degree $\leq n\,|N|^{1/n} \leq \frac{1}{3}q < q - 1$ for any $q \geq 2$. Fix a point $p \in \mathbb{F}_q^n$. By the definition of a Nikodym set, there is a line L_p passing through p such that $L_p \setminus \{p\} \subset N$. Then the polynomial P vanishes on $q-1$ points on L_p. By Lemma 8, P vanishes on the entire line. In particular, P vanishes on p. Since this holds for any $p \in \mathbb{F}_q^n$, P vanishes everywhere. Then Lemma 9 gives the desired contradiction. □

3.3. Connection to the Error-Correcting Codes.

In class, we discussed how polynomials are used in error-correcting codes, a method to encrypt information such that the original message can be reconstructed even with certain percentage of data corruption. One example was the Reed-Muller code. The message we are trying to send is a list of $(D+1)^n$ elements of $\mathbb{F}_q$ where $D < q$ and $n \leq 1$. We think of the message as a function $g : \{0, \cdots, D\}^n \to \mathbb{F}_q$. We present the following lemma from [2] without proof.

Lemma 18. *If $D < q$, then for any function $g : \{0, \cdots, D\}^n \to \mathbb{F}_q$, there is a unique polynomial $P : \mathbb{F}_q^n \to \mathbb{F}_q$ such that $P = g$ on $\{0, \cdots, D\}^n$ and $Deg_{x_i} P \leq D$ for each $i = 1, \cdots, n$.*

The proof of the lemma describes how to construct P from a given g within polynomial time. The essence of the Reed-Muller code is to send the values of P, not just the values of g. When we send the values of this polynomial extension, it is known that we can recover the original message efficiently even when approximately half of the message is corrupted.

In this section, we discuss how the ideas from error-correcting codes are related to the proofs of the Nikodym Problem and the Kakeya Problem. Assume we are working with a Nikodym set $N \subset \mathbb{F}_q^n$. Also assume that D is an integer such that $nD < q - 1$. The Reed-Muller code in Lemma 18 takes as input a function $g : \{0, \cdots, D\}^n \to \mathbb{F}_q$ and constructs a polynomial $P : \mathbb{F}_q^n \to \mathbb{F}_q$ with degree at most D in each coordinate. The key observation is that the target polynomial is uniquely determined by the values on N. Indeed, fix a point $p \in \mathbb{F}_q^n$. Then by the definition of a Nikodym set, there is a line $L_p \ni p$ such that $L_p \setminus \{p\} \subset N$. The polynoimal P has degree at most $nD < q - 1$, so when we fix the values of P on $L_p \setminus \{p\}$, Lemma 8 guarantees that there is a unique polynomial with the given values. In particular, we can recover P on the point p. Since this holds for any given $p \in \mathbb{F}_q^n$, we see that the Reed-Muller code gives an injection:

$$Fcn(\{0, \cdots, D\}^n, \mathbb{F}_q) \to Fcn(N, \mathbb{F}_q)$$

This gives us a lower bound on the size of N: $|N| \geq (D+1)^n$. Notice that we are allowed to choose any D as long as $nD < q-1$. This shows that the lower bound can be improved to roughly $n^{-n}q^n$, which is precisely the result of Theorem 17. Therefore, in some sense, the Reed-Muller code solves the Finite Field Nikodym Problem.

References

[1] Z. Dvir. On the size of kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22(4):1093–1097, 2009.

[2] L. Guth. *Polynomial Methods in Combinatorics*. American Mathematical Society, Providence, 1977. reprinted in 2016.

[3] L. Guth and N. H. Katz. Algebraic methods in discrete analogs of the kakeya problem. *Advances in Mathematics*, 225(5):2828–2839, 2010.

[4] A. Iosevich. *A view from the top*. American Mathematical Society, Providence, 2007.

[5] H. Kaplan, M. Sharir, and E. Shustin. On lines and joints. *Discrete & Computational Geometry*, 44:838–843, 2010.

[6] T. Tao. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *EMS surveys in mathematical sciences*, 1(1):1–46, 2014.