Table of Contents

List of Figures

Chapter 1

The Kakeya Problem in Finite Fields

Before we can discuss the Kakeya problem in finite fields, and its rather surprising resolution, we ought to first discuss the origin and history of the problem. Work on the Kakeya problem can be traced back to the Russian mathematician Abram Besicovitch in 1917. While working on a problem in Riemann integration, Besicovitch reduced it to the question of the existence of planar sets of measure zero which contain a line segment in every direction. In 1920, Besicovitch constructed such a set and published in a Russian Journal.

However, 1917 was a turbulent year as it marked the end of the Russian Empire and the start of the Russian civil war. Due to this and the ensuing blockade of Russian ports there was scarce communication with the outside world. Thus Besicovitch could not have known of a Japanese mathematician Kakeya who asked also in 1917 a related question: What is the smallest area of a convex set within which one can rotate a needle by 180 degrees in the plane? Julius Pal answered this question in 1921 with the equilateral triangle. The more interesting problem without the convexity condition remained open. In 1924, after leaving the newly formed Soviet Union for Copenhagen, Besicovitch discovered this problem and by modifying his previous construction produced a solution in 1925. This lead to the more general questions being asked about Kakeya sets in higher dimensions.

Definition 1.0.1 (Kakeya Set in $\mathbb{R}^n$)**.** A Kakeya set is a set $A \subset \mathbb{R}^n$ that contains a unit segment in every direction.

Besicovitch's construction showed that these sets can have arbitrarily small measures, even attaining zero, in $\mathbb{R}^2$. Further, a straightforward construction produces these measure zero sets in dimensions > 2.

The natural question then arises, what is the dimension of such sets? There are many notions of dimensions that can be investigated, but we restrict ourselves to the Minkowski and Hausdorff dimensions.

Definition 1.0.2 (Minkowski Dimension)**.** Given a set $S \subset \mathbb{R}^n$, define $N(\varepsilon)$ to be the number of boxes of side length ε required to cover the set. The Minkowski Dimension of the set S is then defined as:

$$\dim_M(S) = \lim_{\varepsilon \to 0} \frac{\log(N(\varepsilon))}{\log(1/\varepsilon)}.$$

If this limit does not exist, one can still define the upper and lower Minkowski dimensions, $\dim_{M_{\text{upper}}}$ and $\dim_{M_{\text{lower}}}$, by taking the limit superior and limit inferior respectively.

Definition 1.0.3 (Hausdorff Dimension)**.** We define the d-dimensional Hausdorff measure of a set $S \subset \mathbb{R}^n$ as:

$$\mathcal{H}^d(S) = \lim_{r \to 0} \inf \left\{ \sum_i r_i^d : \text{ there is a countable cover of } S \text{ by balls with radii } 0 < r_i < r \right\}$$

Then we can define the Hausdorff dimension of the set S to be:

$$\dim_H(S) = \inf\{d \geq 0 : \mathcal{H}^d(S) = 0\}.$$

These dimensions are related by the following inequality when they are all defined:

$$\dim_H \leq \dim_{M_{\text{lower}}} \leq \dim_{M_{\text{upper}}}.$$

In 1971, Davies produced a solution for the 2 dimensional case, proving that although the measure of a Kakeya set can be arbitrarily small, it must have Hausdorff (and hence Minkowski) dimension of 2.[1] This resulted in the following conjectures:

Conjecture 1 (Kakeya Conjecture for the Minkowski Dimension)**.** Let A be a Kakeya set in $\mathbb{R}^n$. Then $\dim_M(A) = n$.

Conjecture 2 (Kakeya Conjecture for the Hausdorff Dimension)**.** Let A be a Kakeya set in $\mathbb{R}^n$. Then $\dim_H(A) = n$.

Notation

We introduce some convenient notation here. We write that $A \lesssim_n B$ to mean that there exists some constant C_n which depends on n such that $A \leq C_n B$. Further, we write that $A \sim_n B$ if $A \lesssim_n B$ and $B \lesssim_n A$.

We write $\mathrm{Poly}_D(\mathbb{K}^n)$ to represent the space of polynomials in n variables with coefficients in $\mathbb{K}$ and degree at most D.

1.1 Background

Analogous to the Euclidean case, we define lines in $\mathbb{F}_p^n$ as the set:

$$\mathcal{L} = \{x + ty : x, y \in \mathbb{F}_p^n, t \in \mathbb{F}_p\}$$

A Kakeya set in $\mathbb{F}_p^n$ is a set that contains a line in every direction.

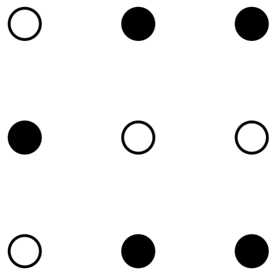

Figure 1.1: An example of a Kakeya set (shaded) in $\mathbb{F}_3^2$.

1.2 Introduction to Finite Fields

Definition 1.2.1 (Finite Field)**.** A finite field, $\mathbb{F}$, is a finite set that forms a field. That is, it is closed under addition, subtraction, multiplication, and non-zero division. The number of elements of a finite field, $|\mathbb{F}|$, is called the order of the finite field.

A finite field of order q exists if and only if $q = p^k$ for some prime p and integer k.

Lemma 1.2.1. *Each element X in a finite field $\mathbb{F}$ satisfies the identity:*

$$X^{|\mathbb{F}|} - X = 0$$

identically in $\mathbb{F}$.

This lemma follows immediately from Fermat's Little Theorem. more needed here

1.3 Combinatorial attempts at the proof

this section sucks, rewrite!

We fix a finite field $\mathbb{F} = \mathbb{F}_{p^k}$.

1.3.1 Bush Argument

Bourgain produced one of the first non-trivial estimates of the dimension in 1991.[2] We present the finite field analogue of his argument here.[3]

Theorem 1.3.1 (Bush Argument)**.** *If $l_1, \ldots, l_M$ are lines in $\mathbb{F}^n$, then the number of points in their union is at least*

$$\frac{1}{2}M^{1/2}|\mathbb{F}|$$

In particular, if A is a Kakeya set, then we have:

$$|A| \gtrsim |\mathbb{F}|^{\frac{n+1}{2}}$$

Proof. Let X be the union of the lines $l_1, \dots, l_M$. Each of these lines contains $|\mathbb{F}|$ points of X, so we have $|\mathbb{F}|M$ points to distribute over X. By the pigeonhole principle, there is a point $x \in X$ which lies in at least $|\mathbb{F}|M|X|^{-1}$ of the lines l_i.

Im not sure what to expand on here - we could contradict by saying if this wasn't the case but that seems verbose

These set of lines l_i through x is called the bush of x. These lines are disjoint except at x, and their union lies in X. So we have:

$$(|\mathbb{F}| - 1)|\mathbb{F}|M|X|^{-1} \leq |X|.$$

Rearranging we get:

$$\frac{1}{2}|\mathbb{F}|M^{1/2} \leq |X|$$

A Kakeya set $A \subset \mathbb{F}^n$ contains at least $|\mathbb{F}|^{n-1}$ lines. Setting $M = |\mathbb{F}|^{n-1}$ yields:

$$\frac{1}{2}|\mathbb{F}||\mathbb{F}|^{\frac{n-1}{2}} \sim |\mathbb{F}|^{\frac{n-1+2}{2}} = |\mathbb{F}|^{\frac{n+1}{2}} \lesssim |A|.$$

□

1.3.2 Hair Brush Argument

Due to Wolff. [4]

Theorem 1.3.2 (Hair Brush Argument). *Suppose $l_1, \dots, l_M$ are lines in $\mathbb{F}^n$, and that at most $|\mathbb{F}| + 1$ of the lines lie in any plane. Then their union has cardinality at least*

$$\frac{1}{3}|\mathbb{F}|^{3/2}M^{1/2}.$$

In particular, if A is a Kakeya set, then we have:

$$|A| \gtrsim |\mathbb{F}|^{\frac{n+2}{2}}$$

Proof. Let $X = \cup_i l_i$. If l_i is a line in A, then the hairbrush with stem l_i is defined to be the set of lines l_j which intersect l_i. An average point of X lies in $|\mathbb{F}|M|X|^{-1}$ lines l_i. If each point of X was about average, then each hairbrush would contain $\gtrsim |\mathbb{F}|^2M|X|^{-1}$ lines. We claim that there is always at least one hairbrush with $\geq (1/2)|\mathbb{F}|^2M|X|^{-1}$ lines.

Finish this proof

□

1.4 Dvir's Proof

In finite fields Kakeya's conjecture is as follows:

Theorem 1.4.1 (Kakeya Conjecture in Finite Fields). *If $A \subset \mathbb{F}_p^n$ contains a translate of every line, then $|A| \gtrsim_n p^n$.*

We shall prove this theorem via 3 surprisingly simple lemmas. This formulation of Dvir's proof is due to Gowers.[5]

Lemma 1.4.2 (Parameter Counting)**.** *Let $\mathbb{K}$ be a (not necessarily finite) field. If $A \subset \mathbb{K}^n$ and $|A| < \binom{n+D}{n}$, there exists a non-zero polynomial $P(x_1, \ldots, x_n)$ of degree D that vanishes on A.*

Proof. We first show the dimension of $\mathrm{Poly}_D(\mathbb{K}^n)$ is $\binom{D+n}{n}$. A basis for $\mathrm{Poly}_D(\mathbb{K}^n)$ is given by monomials of the form $x_1^{D_1} \ldots x_n^{D_n}$, where $\sum_i D_i \leq D$, hence we just need to count the number of monomials.

We can map a monomial $x_1^{D_1} \ldots x_n^{D_n}$ to a string of D $\star$'s and n $|$'s as follows. Begin with D_1 $\star$'s, then place one $|$. We put now D_2 $\star$'s, and place a second $|$. We continue until we have placed D_n $\star$'s followed by an n^{th} $|$. Finally we place $D - \sum_i D_i \star$'s. This is a bijective map between the monomials in $\mathrm{Poly}_D(\mathbb{K}^n)$ and all the strings of D $\star$'s and n $|$'s. To count the strings, fix the n $|$'s. Now we have $n+1$ bins to distribute our D $\star$'s. Therefore we have by the stars and bars theorem:

$$\mathrm{Poly}_D(\mathbb{K}^n) = \binom{n+1+D-1}{n+1-1} = \binom{n+D}{n}.$$

Let now $p_1, \ldots, p_{|A|}$ be the points of A. We consider the evaluation map $E : \mathrm{Poly}_D(\mathbb{K}^n) \to \mathbb{K}^{|A|}$ defined by:

$$E(Q) = \left(Q(p_1), \ldots, Q(p_{|A|})\right).$$

This map is clearly linear. Its kernel $\ker E$ is exactly the set of polynomials in $\mathrm{Poly}_D(\mathbb{K}^n)$ that vanish on A. By assumption, the dimension of $\mathrm{Poly}_D(\mathbb{K}^n)$ is greater than A, so the dimension of the domain of E is greater than the codomain of E. By the rank-nullity theorem, we conclude E must have a non-trivial kernel. Thus there exists a non-zero polynomial $P \in \mathrm{Poly}_D(\mathbb{K}^n)$ that vanishes on A. $\square$

Note that if $D = |\mathbb{F}| - 1$, and $|A| \leq \binom{|\mathbb{F}|+n-1}{|\mathbb{F}|-1} = \binom{|\mathbb{F}|+n-1}{n}$ we have a polynomial of degree $|\mathbb{F}| - 1$ that vanishes on A. Since $\frac{|\mathbb{F}|^n}{n!} < \binom{|\mathbb{F}|+n-1}{n}$,we can definitely find such a polynomial when $|A| \leq \frac{|\mathbb{F}|^n}{n!}$.

Lemma 1.4.3. *Suppose $A \subset \mathbb{F}^n$ contains a line in every direction, and suppose that there exists a non-zero polynomial P with degree $D < |\mathbb{F}|$ that vanishes on A. Then there exists a non-zero degree D polynomial $\bar{P}$ that vanishes everywhere on $\mathbb{F}^n$.*

Proof. Choose a line in A, say $\ell = \{x + tz : t \in \mathbb{F}\}$ with $x \in \mathbb{F}^n$ and $z \in \mathbb{F}^n/\mathbb{F}^\times$. Now we consider the restriction of our polynomial P to the line ℓ, $P_{|\ell}$. Recall P is a sum of monomials, and we use multi-index notation here with $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha_i \in \mathbb{N} \cup \{0\}$ and $|\alpha| = \sum \alpha_i$. P can be written as:

$$P(x_1, x_2, \ldots, x_n) = \sum_{|\alpha| \leq D} c_\alpha x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

Now $P_{|\ell}$ can be written:

$$P_{|\ell} = P(x+tz) = Q_{x,z}(t) = \sum_{|\alpha|\leq D} c_\alpha \prod_i (x_i + tz_i)^{\alpha_i}.$$

We now wish to examine the degree D term of Q, which is achieved by picking the tz_i terms from each bracket in the product above. This gives the degree D component of Q, $Q_{x,z,D}$, which has the form:

$$Q_{x,z,D} = t^D Q_D(z) = t^D \sum_{|\alpha|=D} c_\alpha \prod_i z_i.$$

Now if $P_{|\ell}$ vanishes everywhere on ℓ, since its dependence on t is given by a polynomial of degree less than $|\mathbb{F}|$, all its coefficients must be zero. This is clear from the factor theorem, as we could write the roots of $P_{|\ell}$ as $(t-k_1)(t-k_2)\dots(t-k_{|\mathbb{F}|})$, but this contradicts the fact P is of degree $D < |\mathbb{F}|$.

Notice that $Q_{x,z,D}$ no longer depends on x, but on z alone. In particular $Q_D(z) = 0$, but z was an arbitrary element of $\mathbb{F}^n/\mathbb{F}^\times$, and $Q_D(z)$ also vanishes at zero, so it vanishes everywhere. Thus we can pick $\bar{P} = Q_D$, and we are done. □

Lemma 1.4.4. *Let P be a non-zero polynomial on $\mathbb{F}^n$ with degree less than $|\mathbb{F}|$. Then P does not vanish everywhere.*

Proof. We proceed by induction on n. For $n = 1$, a non-zero polynomial that vanishes everywhere has $|\mathbb{F}|$ roots, so must be at least of degree $|\mathbb{F}|$. Let us assume that the statement holds in $\mathbb{F}^{n-1}$, we now prove it must also hold for $\mathbb{F}^N$.

We let $x_1, \dots, x_n$ be coordinates on $\mathbb{F}^n$, and we write P in the form:

$$P(x_1, \dots, x_n) = \sum_{j=n}^{|\mathbb{F}|-1} P_j(x_1, \dots x_{n-1}) x_n^j.$$

Each P_j are polynomials in $x_1, \dots x_{n-1}$ of degree less than $|\mathbb{F}|$. Fix $x_1, \dots x_{n-1}$, and let x_n vary. Now we have a polynomial in x_n of degree less than $|\mathbb{F}|$ that vanishes for all $x_n \in \mathbb{F}$. By the base case this must be the zero polynomial. So each $P_j(x_1, \dots, x_{n-1}) = 0$ for all j and for all $(x_1, \dots x_{n-1}) \in \mathbb{F}^{n-1}$. Now by induction on n, each P_j is the zero polynomial. Then P is the zero polynomial as well.

□

Proof of Theorem 1.4.1. Assume $A \subset \mathbb{F}^n$ is a Kakeya set, and that $|A| \leq \frac{|\mathbb{F}|^n}{n!}$. Then by 1.4.2 we can find a non-zero polynomial, say P, that vanishes on A. Now by 1.4.3 there exists a non-zero polynomial $\bar{P}$ that vanishes everywhere on $\mathbb{F}^n$, and has degree less than $|\mathbb{F}|$. Finally 1.4.4 says that such a $\bar{P}$ is necessarily the zero polynomial, a contradiction. We conclude that $|A| > \frac{|\mathbb{F}|^n}{n!}$, or in other words:

$$|A| \gtrsim_n |\mathbb{F}|^n.$$

□

Chapter 2

The Joints Problem

2.1 Background

Let $\mathcal{L}$ be a set of distinct lines in $\mathbb{R}^n$. A joint of $\mathcal{L}$ is a point which lies in three non-coplanar lines of $\mathcal{L}$. The joints problem consists of setting a sharp upper bound on the maximal number of joints that can be formed from a configuration of L distinct lines. We denote this quantity $J(L)$.

We shall begin by examining an example based on a grid, with the hopes of gaining better intuition about the problem and formulating a conjecture.

Example 2.1. *Consider an $N \times N \times N$ regular grid of integer coordinates. We shall give a collection of lines such that each point of this grid is a joint for the collection. Let $\mathcal{L}$ be the collection of all lines parallel to any of the Cartesian axes that intersect this a point in this grid. For each horizontal $N \times N$ layer, there are $N + N = 2N$ lines that intersect our grid. There are N layers, so we obtain $2N^2$ distinct lines in this manner. Finally we need to account for the N^2 lines perpendicular to the $N \times N$ layers. This leaves us with $|\mathcal{L}| = 3N^2$ lines forming N^3 joints. The number of joints is thus $\sim |\mathcal{L}|^{3/2}$.*

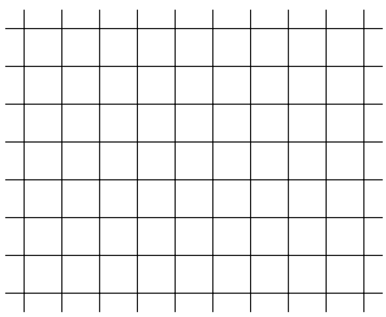

Figure 2.1: A $N \times N$ layer of our grid.

We can extend this example to higher dimensional grids easily.

Example 2.2. *If we have an $\underbrace{N \times \cdots \times N}_{n \text{ Dimensions}}$ regular grid of integer coordinates in $\mathbb{R}^n$, we can construct an example by a straightforward extension of the above example. Each additional* *dimension increases the number of lines by a factor of N, this can be seen by considering each new dimension as a layering of the previous set along the new axis. Thus we can see that $\sim N^{n-1}$ lines form N^n joints in this manner. So the number of joints is $\sim |\mathcal{L}|^{\frac{n}{n-1}}$.*

It turns out that the examples illustrated above provide asymptotically maximal configurations, that is, disregarding the best constant C such that $J(L) \leq CL^{\frac{n}{n-1}}$.

2.2 Solution of the Joints Problem

This solution was first produced by Guth-Katz for the three-dimensional case,[6] and later extended to the general case by Quilodrán,[7] and independently at the same time by Kaplan-Sharir-Shustin.[8]

Theorem 2.2.1. *Any L lines in $\mathbb{R}^n$ determine $\lesssim_n L^{\frac{n}{n-1}}$ joints.*

We begin with the fundamental lemma to this proof.

Lemma 2.2.2. *If $\mathcal{L}$ is a set of lines in $\mathbb{R}^n$ that determines J joints, then one of the lines contains at most $nJ^{\frac{1}{n}}$ joints.*

Proof. Let P denote the lowest degree non-zero polynomial that vanishes at every joint of $\mathcal{L}$. By parameter counting, Lemma 1.4.2, the degree of P is at most $nJ^{\frac{1}{n}}$. (To see this, set $D = \lfloor nJ^{\frac{1}{n}} \rfloor$ and then $J < \binom{D+n}{n}$.)

We proceed by contradiction. Assume every line contains more than $nJ^{\frac{1}{n}}$ joints. Now P must vanish on every line in $\mathcal{L}$ as the degree of P is less than the number of joints it must interpolate.

We now examine the gradient of P at each joint in $\mathcal{L}$. We will need a fact about gradients for this, which we will encapsulate in the following lemma for clarity.

Lemma 2.2.3. *If x is a joint of $\mathcal{L}$, and if a smooth function $F : \mathbb{R}^n \to \mathbb{R}$ vanishes on the lines of $\mathcal{L}$, then ∇F vanishes at x.*

Proof. The joint x is contained in n non-coplanar lines $l_1, \ldots, l_n$, in directions $v_1, v_2, \ldots, v_n$ respectively. Now consider the directional derivative for a particular v_i:

$$\frac{\partial F}{\partial v_i} = \lim_{t \to 0} \frac{\overbrace{F(x + tv_i)}^{F \equiv 0 \text{ on a line in } \mathcal{L}} \quad - \quad \overbrace{F(x)}^{F \equiv 0 \text{ on joints}}}{t} = \frac{0}{t} = 0.$$

Notice that $\frac{\partial F}{\partial v_i} = \langle \nabla F, v_i \rangle$, so since we have this for each v_i, and the set of v_i's form a basis of $\mathbb{R}^n$, we have that $\nabla F(x) = 0$. □

So we see that the partial derivatives of P vanish at each joint. The derivatives are polynomials of smaller degree than P and since P was assumed to be the minimal degree non-zero polynomial that vanishes at each joint, each derivative of P is identically zero. This implies P must be constant, which implies that there does not exist such a minimal degree polynomial, a contradiction. □

Finally we can prove the main result.

Proof. Lemma 2.2.2 tells us that if we remove a line from our collection, we are removing at most $nJ(L)^{\frac{1}{n}}$ joints. By repeating this process, we get the chain of inequalities:

$$\begin{aligned}
J(L) &\leq J(L-1) + n(J(L))^{\frac{1}{n}} \\
&\leq J(L-2) + 2\left[n(J(L))^{\frac{1}{n}}\right] \\
&\leq J(L-3) + 3\left[n(J(L))^{\frac{1}{n}}\right] \\
&\vdots \\
&\leq L\left[n(J(L))^{\frac{1}{n}}\right].
\end{aligned}$$

Now we have:

$$J(L) \leq L\left[n(J(L))^{\frac{1}{n}}\right]$$

$$J(L)^{\frac{n-1}{n}} \lesssim_n L$$

$$J(L) \lesssim_n L^{\frac{n}{n-1}}$$

□

Chapter 3

Szemerédi-Trotter Theorem

In this chapter we will study the application of the polynomial method to incidence geometry by proving a fundamental theorem in the field. Incidence geometry is the study of possible intersection patterns of simple geometric objects, such as lines or low degree curves. We have already seen an incidence problem in the previous chapter on the Joints problem. By developing the powerful tool of polynomial partitioning we shall see the key role that the topology of $\mathbb{R}$ can play in such problems, in contrast to the trivial topology of finite fields.

3.1 Background

The Szemerédi-Trotter theorem is a fundamental theorem to the field of incidence geometry, originally proved by an involved cell decomposition argument of Szemerédi and Trotter and later given a shorter proof using crossing numbers by Székely.

Theorem 3.1.1 (Szemerédi-Trotter). *Let $\mathcal{S} \subset \mathbb{R}^2$ be a finite set of points and let $\mathcal{L} \subset \mathbb{R}^2$ be a finite set of lines. We define*

$$I(\mathcal{S}, \mathcal{L}) = \{(p, \ell) \in \mathcal{S} \times \mathcal{L} \mid p \in \ell\}$$

to be the set of incidences between $\mathcal{S}$ and $\mathcal{L}$.

Then:

$$|I(\mathcal{S}, \mathcal{L})| \lesssim (|\mathcal{S}||\mathcal{L}|)^{2/3} + |\mathcal{S}| + |\mathcal{L}|$$

3.2 The Trivial Bound

In planar geometry, we have the following dual statements: two points determine a line and every pair of lines intersect in at most one point. Using this we can prove the following bounds on $I(\mathcal{S}, \mathcal{L})$:

Theorem 3.2.1 (Trivial Bounds)**.** *For a set of points $\mathcal{S}$ and lines $\mathcal{L}$ we have*

$$I(\mathcal{S},\mathcal{L})| \leq |\mathcal{S}|^2 + |\mathcal{L}|.$$

$$I(\mathcal{S},\mathcal{L})| \leq |\mathcal{L}|^2 + |\mathcal{S}|.$$

Proof. To see this, count the lines that have at most one point in P on them. These contribute at most $|\mathcal{L}|$ incidences. Every other line has at least two points in $\mathcal{S}$. The total number of incidences on these lines is at most $|\mathcal{S}|^2$ as otherwise there would exist a $p \in \mathcal{S}$ that lies on over $|\mathcal{S}|$ lines, and each of these lines would have an additional point on it. This would imply there are more that $|\mathcal{S}|$ points, a contradiction.

Interchanging the roles of $\mathcal{L}$ and $\mathcal{S}$ achieves the other bound. □ does it?

Theorem 3.2.2 (Second Trivial Incidence Bound)**.**

$$I(\mathcal{S},\mathcal{L}) \lesssim |\mathcal{S}| \cdot |\mathcal{L}|^{\frac{1}{2}} + |\mathcal{L}|$$

and

$$I(\mathcal{S},\mathcal{L}) \lesssim |\mathcal{L}| \cdot |\mathcal{S}|^{\frac{1}{2}} + |\mathcal{S}|.$$

Proof. We now bound the number of incidences.

$$\begin{aligned}
|I(\mathcal{S},\mathcal{L})|^2 &= \left(\sum_{\ell\in\mathcal{L}}\sum_{p\in\mathcal{S}} 1_{p\in\ell}\right)^2 \\
&\leq |\mathcal{L}| \cdot \sum_{\ell\in\mathcal{L}}\left(\sum_{p\in\mathcal{S}} 1_{p\in\ell}\right)^2 \qquad \text{(Cauchy-Schwarz on } \ell) \\
&= |\mathcal{L}| \cdot \sum_{p_1,p_2\in\mathcal{S}}\sum_{\ell\in\mathcal{L}} 1_{p_1\in\ell}1_{p_2\in\ell} \\
&\leq |\mathcal{L}| \cdot (|I(\mathcal{S},\mathcal{L})| + |\mathcal{S}|^2) \\
&\leq |\mathcal{L}|^2 + 2|\mathcal{L}| \cdot |\mathcal{S}|^2 \qquad \text{(Using Theorem 3.2.1)}
\end{aligned}$$

This implies

$$I(\mathcal{S},\mathcal{L}) \lesssim |\mathcal{S}| \cdot |\mathcal{L}|^{\frac{1}{2}} + |L|.$$

Repeating the above proof interchanging the roles $\mathcal{S}$ and $\mathcal{L}$ achieves the other bound. □

extra step needed here - split up sum and do triple thing

3.3 Examples

We can not improve beyond our second trivial bounds in a finite field $\mathbb{F}^2$.

Example 3.1 (Finite Fields)**.** *Consider the set of points $\mathcal{S} = \mathbb{F}^2$ and let $\mathcal{L}$ be the set of all lines in $\mathbb{F}^2$. Every line contains exactly $|\mathbb{F}|$ many points of $\mathcal{S}$, so we have $|\mathbb{F}|^3$ incidences. So both sides of the second trivial bound are comparable:*

$$I(\mathcal{S}, \mathcal{L}) = |\mathbb{F}|^3 \sim (|\mathbb{F}|^2)(|\mathbb{F}|^2)^{1/2} + |\mathbb{F}|^2.$$

In contrast, the following examples seem to be the best possible over $\mathbb{R}$. We will later prove that these are the tight case of the Szemerédi–Trotter Theorem. We define a line in $\mathbb{R}^2$ as follows:

$$\ell_{m,c} = \{(x, y) \in \mathbb{R}^2 \mid y = mx + c\}.$$

Example 3.2. *Consider the following collections in $\mathbb{R}^2$:*

$$\begin{aligned} \mathcal{S} &= \{(a, b) \in \mathbb{Z}^2 \mid a \in [1, N], b \in [1, 2N^2]\} \\ \mathcal{L} &= \{\ell_{m,c} \in \mathbb{R}^2 \mid m, c \in \mathbb{Z}, m \in [1, N], c \in [1, N^2]\} \end{aligned}$$

The collection $\mathcal{S}$ contains $2N^3$ points and $\mathcal{L}$ contains N^3 lines. Every line in $\mathcal{L}$ contains N points in $\mathcal{S}$ as for each $x \in [1, N]$ the y-coordinate of $\ell_{m,c}$, $mx + c$, gives a different integer in $[1, 2N^2]$. Hence there are N^4 incidences. Both sides of the Szemerédi-Trotter inequality are comparable as

$$I(\mathcal{S}, \mathcal{L}) = N^4 \sim (N^3)^{\frac{2}{3}}(N^3)^{\frac{2}{3}} \sim |\mathcal{S}|^{2/3}|\mathcal{L}|^{2/3}$$

diagram?

Example 3.3. *Let $N \gg 1$ be a large even integer and let $1 < R \ll N$ be another integer. Consider the collections in $\mathbb{R}^2$:*

$$\begin{aligned} \mathcal{S} &= \{(a, b) \in \mathbb{Z}^2 \mid (a, b) \in [-N/2, N/2] \times [-N/2, N/2]\} \\ \mathcal{L} &= \{\ell \mid \ell \text{ contains between } R \text{ and } 2R \text{ points of } \mathcal{S}\} \end{aligned}$$

We begin by estimating how many lines pass through a given point of the regular grid $\mathcal{S}$. Let $\ell \in \mathcal{L}$ and $p \in \mathcal{S}$. The closest point $p' \in \mathcal{S}$ such that $p \neq p'$ and $p' \in \ell$ must lie in a square centred at p of side length $\sim N/R$. This follows from the fact that there are at least R points of $\mathcal{S}$ in ℓ and hence the projections of these points to the axes can be separated by at most $\sim N/R$. Taking each possible combination of these we can conclude that there are $\lesssim N^2/R^2$ in $\mathcal{L}$ through a given point p. check here

We now claim that there are $\gtrsim N^2/R^2$ distinct such lines. We need only consider the points in the upper right quadrant of $\mathcal{S}$ as the problem is symmetrical. Further, we restrict ourselves to considering lines with slopes m satisfying $\frac{1}{2} < m < 2$. For such a line to contain R points of $\mathcal{S}$ we require $m = \frac{l}{k} \in \mathbb{Q}$ with $\gcd(l, k) = 1$ and $l, k \in \left[\frac{N}{2R}, \frac{N}{R}\right]$.

There are $\gtrsim N^2/R^2$ pairs, as the proportion of pairs that share a factor of 2 is $\frac{1}{2}^2$ and the proportion of pairs that share a factor of 3 is $\frac{1}{3}^2$, and in general the proportion that shares a factor of k is $\frac{1}{k}^2$. We have that $\sum_{k>1} \frac{1}{k}^2 < \frac{2}{3} < 1$ and hence there are $\gtrsim N^2/R^2$ distinct lines in $\mathcal{L}$ through each point. Taking account of what we have shown:

$$\begin{aligned} |\mathcal{S}| &\sim N^2 \\ |\mathcal{L}| &\sim |\mathcal{S}| \frac{N^2}{R^2} \frac{1}{R} \sim \frac{N^4}{R^3} \\ |I(\mathcal{S}, \mathcal{L})| &\sim |\mathcal{S}| \frac{N^2}{R^2} \sim \frac{N^4}{R^2} \end{aligned}$$

we can see that both sides of the Szemerédi-Trotter inequality are comparable:

$$|I(\mathcal{S}, \mathcal{L})| \sim \frac{N^4}{R^2} \sim (N^2)^{\frac{2}{3}} \left(\frac{N^4}{R^3}\right)^{\frac{2}{3}} \sim |\mathcal{S}|^{\frac{2}{3}} |\mathcal{L}|^{\frac{2}{3}}$$

Is the spacing messed up?

add diagram (!)

3.4 Ham Sandwich Theorems

The above examples suggest that the topology of $\mathbb{R}$ plays a key role in this incidence problem. We shall now introduce the method of polynomial partitioning, which can be seen as the topological analogy to the vanishing lemma we used in the previous chapters.

Let $\mathbb{S}^n$ denote the unit n-sphere in $\mathbb{R}^{n+1}$.

Theorem 3.4.1 (Borsuk-Ulam). *A map ϕ is said to be antipodal if it obeys $\phi(-x) = -\phi(x)$ for all x in its domain. Suppose $\phi : \mathbb{S}^N \to \mathbb{R}^N$ is a continuous antipodal mapping. Then the image of ϕ contains 0.*

The proof of this result is long and beyond the scope of this paper. We refer interested readers to a beautiful geometric proof in chapter 2 of Matousek's book *Using the Borsuk-Ulam theorem.*[9]

Let us now define some useful notation going forward. For any function $f : \mathbb{R}^n \to \mathbb{R}$ let us denote the zero set of f by $Z(f) = \{x \in \mathbb{R}^n \mid f(x) = 0\}$.

Definition 3.4.1 (Bisection of a Set). A function $f : \mathbb{R}^n \to \mathbb{R}$ is said to bisect an open set U with volume $\mathrm{Vol}(U) < \infty$ if:

$$\mathrm{Vol}\{x \in U \mid f(x) > 0\} = \mathrm{Vol}\{x \in U \mid f(x) < 0\} = \frac{1}{2}\mathrm{Vol}(U).$$

Analogously, a function f is said to bisect a finite set S if both:

$$|\{x \in S \mid f(x) > 0\}| \leq \frac{|S|}{2}$$

and
$$|\{x \in S \mid f(x) < 0\}| \leq \frac{|S|}{2}.$$

Theorem 3.4.2 (General Ham Sandwich Theorem)**.** *Let V be a finite dimensional vector space of continuous functions $f : \mathbb{R}^n \to \mathbb{R}$ such that for any non-zero function f, $Z(f)$ has zero Lebesgue measure. Let $U_1, U_2, \ldots, U_N \subset \mathbb{R}^n$ be finite volume open sets with $N < \dim V$.*

Then there exists a non-zero function $f \in V$ that bisects each U_i.

Proof. Define the functions $\{\phi_i\}_{i=1}^N$, $\phi_i : V \backslash \{0\} \to \mathbb{R}$ by

$$\phi_i(f) = \mathrm{Vol}(\{x \in U_i \mid f(x) > 0\}) - \mathrm{Vol}(\{x \in U_i \mid f(x) > 0\})$$

Since $Z(f)$ has measure zero, it is easy to see that $\phi_i(f) = 0$ if and only if f bisects U_i. Notice also that $\phi_i(-f) = -\phi_i(f)$, hence ϕ_i is antipodal.

We now show each $\phi_i(F)$ is continuous. It is enough to show that if U is a finite volume open set, then the measure of $\{x \in U \mid f(x) > 0\}$ depends continuously on $f \in V \backslash \{0\}$.

Suppose $f_n \to f$ in V for some $f, f_n \in V \backslash \{0\}$. f_n converges to f in the topology of V, so it follows it must converge pointwise. Pick any $\varepsilon > 0$. By Egorov's theorem, we can find a subset $E \subset U$ so that $f_n \to f$ uniformly pointwise on $U \backslash E$, and $m(E) < \varepsilon$. By hypothesis, $m(Z(f)) = 0$ and $m(U) < \infty$. Since the Lebesgue measure is continuous we can choose δ such that $m\left(\{x \in U \mid |f(x)| < \delta\}\right) < \varepsilon$.

Now we choose n sufficiently large that $|f_n(x) - f(x)| < \delta$ on $U \backslash E$. Then we have

$$|m\left(\{x \in U \mid f_n(x) > 0\}\right) - m\left(\{x \in U \mid f(x) > 0\}\right)| < 2\varepsilon.$$

Since ε was arbitrary each ϕ_i is continuous.

is this just cnty of everything? - ask marco

We now combine each ϕ_i into the map $\phi : V \backslash \{0\} \to \mathbb{R}^N$. Since $\dim V > N$, select a subspace $U < V$ such that $\dim U = N + 1$. Now choose an isomorphism of U with $\mathbb{R}^{N+1}$, and think of $\mathbb{S}^N$ as a subset of U. Now the map $\phi : \mathbb{S}^N \to \mathbb{R}^N$ is antipodal and continuous. By the Borsuk-Ulam theorem, there exists an $f \in \mathbb{S}^N \subset V \backslash \{0\}$ such that $\phi(f) = 0$. $\square$

Corollary 3.4.2.1 (Finite Ham Sandwich Theorem)**.** *Let $S_1, \ldots, S_N$ be finite sets in $\mathbb{R}^n$ and let D be such that $N < \binom{D+n}{n}$. Then there exists a non-zero $P \in Poly_D(\mathbb{R}^n)$ that bisects each S_i.*

Proof. For each $\delta > 0$, define $U_{i,\delta}$ to be the union of $\delta - balls$ centred at the points of S_i. By Theorem 3.4.2, we can find a non-zero P_δ with degree less than D that bisects each $U_{i,\delta}$. By rescaling we can assume $P_\delta \in \mathbb{S}^N \subset \mathrm{Poly}_D(\mathbb{R}^n) \backslash \{0\}$. Since $\mathbb{S}^N$ compact, we can find a sequence $\delta_m \to 0$ so that P_{δ_m} converges to P in $\mathbb{S}^N$. Since the coefficients of P_{δ_m} converge to P, P_{δ_m} converges to P uniformly on compact sets.

abusing notation, also the norm is l1?

We claim P bisects each S_i. By contradiction, suppose $P > 0$ on more than half the points of S_i, say on the points of S_i^+. Choosing ε sufficiently small, we can assume $P > 0$ on the ε-ball around each point of S_i^+. Further, we can choose ε such that each

ε-ball is disjoint. Since P_{δ_m} converges uniformly, we can find m sufficiently large such that $P_{\delta_m} > 0$ on the ε-ball around each point of S_i^+. By making m large, we can also arrange that $\delta_m < \varepsilon$. Thus $P_{\delta_m} > 0$ on more than half the points of U_{i,δ_m}. $\square$

Theorem 3.4.3 (Polynomial Partitioning)**.** *For any n there exists a constant $c(n)$ such that if S is a finite subset of $\mathbb{R}^n$ and D is any degree, then there exists a polynomial P of degree D such that $\mathbb{R}\backslash Z(P)$ is a disjoint union of $\lesssim D^n$ open sets O_i each containing $\lesssim_n |S|D^{-n}$ points.*

Proof. The main idea of this proof is the repeated application of the Finite Ham Sandwich Theorem. We begin by finding a polynomial P_1 of degree 1 that bisects S. This partitions $\mathbb{R}\backslash Z(P_1)$ into two disjoint open sets according to the sign of P_1, P_1^+ and P_1^-, each containing at most $|S|/2$ points. We then bisect both of these sets using another polynomial P_2. There are four sign conditions on P_1 and P_2, these being the four possible intersections of the sets $P_1^{\pm}$ and $P_2^{\pm}$, and the subset for each sign condition contains at most $|S|/4$ points of S. Continuing this process to define polynomials $P_3, P_4, \ldots$, where the polynomial P_j bisects 2^{j-1} finite sets. By the Finite Ham Sandwich Theorem, each P_j can have a degree $\lesssim 2^{j/n}$. Repeating this procedure J times, and defining $P = \prod_{i=1}^J P_i$, $\mathbb{R}^n\backslash Z(P)$ is the disjoint union of 2^J open sets each containing $\leq |S|2^{-J}$ points of S. Now we choose D such that $\deg(P) < D$ which is equivalent to $\sum_{j=0}^J c(n)2^{j/n} \leq D$. But $\sum_{j=0}^J 2^{j/n}$ is a geometric series so we can find $\deg(P) < D$ for $D \leq c(n)2^{J/n}$. The number of points in each O_i is $\leq |S|2^{-J} \leq c(n)|S|D^{-n}$ $\square$

There is a crucial point to note about polynomial partitioning. The above theorem does not guarantee anything about the distribution of points between $Z(P)$ and its compliment. This is made most clear looking at the extremal examples. If all points line in the compliment of $Z(P)$ then we have an optimal eqidistribution of points, and can often use trivial bounds in a divide-and-conquer style argument. On the otherhand, in the case all points are contained in $Z(P)$ we have many points in an algebraic surface of controlled degree, so we can try and use tools from algebraic geometry. Generally, there will be some points in both $Z(P)$ and its compliment, which we need to deal with seperately.

3.5 Proof of the Szemerédi-Trotter Theorem

We now can prove the Szemerédi-Trotter theorem using polynomial partitioning.

Proof of the Szemerédi-Trotter Theorem. Let $|\mathcal{S}| = S$ and $|\mathcal{L}| = L$. We need only consider the case $S^{\frac{1}{2}} \leq L \leq S^2$, as otherwise the proof follows immediately from the lemma above. Let D be a degree to be chosen later. By Theorem 3.4.3, there exists a polynomial P of degree D such that $\mathbb{R}^2\backslash Z(P)$ splits into D^2 components each having $\lesssim SD^{-2}$ points. Let $O_{i\in\Pi}$ denote these components and let $\mathcal{S}_i = \mathcal{S} \cap O_i$, $\mathcal{L}_i$ denote the lines that intersect the interior of each O_i respectively. We define the following complimentary sets:

$$\begin{aligned}\mathcal{S}_c &= \{x \in \mathcal{S} \mid x \notin Z(p)\}\\ \mathcal{S}_z &= \{x \in \mathcal{S} \mid x \in Z(p)\}\\ \mathcal{L}_c &= \{\ell \in \mathcal{L} \mid \ell \not\subset Z(p)\}\\ \mathcal{L}_z &= \{\ell \in \mathcal{L} \mid x \subset Z(p)\}\end{aligned}$$

Note that $\mathcal{S} = \mathcal{S}_c \cup \mathcal{S}_z$, $\mathcal{L} = \mathcal{L}_c \cup \mathcal{L}_z$. We can now write our total line-point incidences as the following sum

$$I(\mathcal{S}, \mathcal{L}) = I(\mathcal{S}_c, \mathcal{L}) + I(\mathcal{S}_z, \mathcal{L}_z) + I(\mathcal{S}_z, \mathcal{L}_c).$$

If a line ℓ is not contained entirely in $Z(P)$ then it can intersect P at most D times, so each line intersects at most $D+1$ cells. Hence $\sum_{i\in\Pi} L_i \le (D+1)L$. We begin by examining the $I(\mathcal{S}_c, \mathcal{L})$ term:

check equality?

$$I(\mathcal{S}_c, \mathcal{L}) = \sum_{i\in\Pi} I(\mathcal{S}_i, \mathcal{L}_i)$$

Using our trivial bound in each cell:

$$\begin{aligned}&\le \sum_{i\in\Pi} \mathcal{S}_i^2 + \sum_{i\in\Pi} \mathcal{L}_i\\ &\lesssim LD + SD^{-2} \sum_{i\in\Pi} S_i\\ &\le LD + S^2 D^{-2}\end{aligned}$$

The number of lines in $\mathcal{L}_z$ is at most D. So we have by our trivial bounds:

$$I(\mathcal{S}_z, \mathcal{L}_z) \le S + D^2.$$

Each line in $\mathcal{L}_c$ has at most D intersection points with $Z(P)$ so it has at most D incidences with $\mathcal{S}_z$. Hence:

$$I(\mathcal{S}_z, \mathcal{L}_c) \le LD.$$

Together we have now

$$I(\mathcal{S}, \mathcal{L}) \lesssim LD + S^2 D^{-2} + S + D^2.$$

We optimise $LD + S^2 D^{-2}$ by choosing D such that both terms comparable and hence $D \sim S^{\frac{2}{3}} L^{-\frac{1}{3}}$. From our restriction $S^{\frac{1}{2}} \le L \le S^2$ we have $S^{\frac{2}{3}} L^{-\frac{1}{3}} \ge 1$ and $D^2 \sim S^{\frac{4}{3}} L^{-\frac{2}{3}} \le S$, so we achieve

$$I(\mathcal{S}, \mathcal{L}) \lesssim (SL)^{2/3} + S.$$

Considering the regime where $L > S^2$ and applying the trivial bound yields the full

Szemerédi-Trotter inequality:

$$I(\mathcal{S},\mathcal{L}) \lesssim (SL)^{2/3} + S + L.$$

$\square$

There are two key things to note about the above proof. First, the key role that the topology of $\mathbb{R}$ plays. Topology is used in the proof of polynomial partitioning as it relies on the Borsuk Ulam theorem. It is a worthwhile heuristic to develop that polynomial partitioning may be useful for incidence problems where the best examples in a finite field (which is only equipped with the trivial topology) do not coincide with the best known examples over the reals. Secondly, the above proof illustrates the surprising power of polynomial partitioning. We are able to use very trivial bounds in each cell to achieve a tight overall bound.

consider adding a digression on ST

Chapter 4

The Circle Tangency Counting Problem

4.1 Include trivial 5/3 bound?

We discuss now a special case of the curve tangency problem from a recent paper of Zahl. [10]

Theorem 4.1.1. *Given a collection of circles $\mathcal{C}$ in the plane such that no three are tangent at a common point, then there are at most $\sim N^{3/2}$ tangencies.*

Lemma 4.1.2. *Given $\mathcal{C}$ as above and suppose that there are $\gtrsim N^{\alpha}$ tangencies. Then we can refine our set such that every circle in $\mathcal{C}' \subset \mathcal{C}$ is tangent to $\gtrsim N^{\alpha-1}$ circles.*

Proof. Let $\tau(\mathcal{C})$ be the set of tangencies of the circles in $\mathcal{C}$. Take a circle $\gamma \in \mathcal{C}$ such that $|\{\gamma \cap \tau(\mathcal{C})\}| < c_1 N^{1/2}$ and discard it. We label our new refined collection as $\mathcal{C}_1$. After repeating this process M times until there are no more circles that satisfy our criteria, at each step removing a circle that does not have sufficient tangencies, we attain a collection $\mathcal{C}_M$. We claim that $\tau(\mathcal{C}_M) \gtrsim N^{\alpha}$, and that $\mathcal{C}_M \neq \emptyset$.

For the first claim, observe that at each step i we are reducing $\tau(\mathcal{C}_i)$ by at most $c_1 N^{\alpha-1}$. Thus,

$$
\begin{aligned}
|\tau(\mathcal{C}_M)| &\geq |\tau(\mathcal{C})| - M c_1 N^{\alpha-1} \\
&> c_0 N^{\alpha} - M c_1 N^{\alpha-1} \\
&> c_0 N^{\alpha} - \underbrace{c_1}_{\text{Set } = c_0/2} N^{\alpha} \\
|\tau(\mathcal{C}_M)| &> \frac{c_0}{2} N^{\alpha}.
\end{aligned}
$$

We must now check that we have not removed every circle from our collection. We have the trivial inequality $|\tau(\mathcal{C}_M)| \leq c_2 N^2$. Combining this with the result above, we attain $|\mathcal{C}_M| \geq \frac{c_1}{2c_2} N^{3/4}$. $\square$

We can now prove the main theorem.

Last line is incorrect

Proof. Given an arbitrary collection of circles $\mathcal{C}$ with $\gtrsim N^{3/2}$ tangencies, we can reduce to a collection Γ where each circle is tangent to at least $\sim N^{1/2}$ other circles using the previous lemma. After applying a small rotation, we can assume that the tangent line at each point of tangency does not point vertically in the y-direction. Now for each $\gamma \in \Gamma$, we define:

$$\beta(\gamma) = \left\{ (x, y, z) \in \mathbb{R}^3 : (x, y) \in \gamma, z = -\frac{x - x_\gamma}{y - y_\gamma} \right\},$$

where (x_γ, y_γ) is the centre of the circle γ. Given a point (x, y), and a non-vertical line l containing (x, y) of slope z, γ is tangent to l at (x, y) if and only if $(x, y, z) \in \beta(\gamma)$.

Let $\beta(\Gamma) = \{\beta(\gamma) : \gamma \in \Gamma\}$. Two circles γ_1 and γ_2 are tangent if and only if $\beta(\gamma_1) \cap \beta(\gamma_2) \neq \emptyset$. [TODO: expand on this? diagram?]

Suppose $(x, y, z) \in \beta(\gamma_1) \cap \beta(\gamma_2)$ for some $\gamma_1 \neq \gamma_2$. Then

$$(0, 0, 1) \in \operatorname{span}\left(T_{(x,y,z)}\beta(\gamma_1), T_{(x,y,z)}\beta(\gamma_2)\right).$$

We can establish this by examining a parameterisation of γ_1 and γ_2 in the neighbourhood of (x, y). Define $f_i(t)$ such that $(t + x, f_i(t))$ is a parameterisation of γ_i in the neighbourhood of (x, y) for all t in a small neighbourhood of 0. Since γ_1 is tangent to γ_2 at (x, y), $\frac{df_1}{dt}(0) = \frac{df_2}{dt}(0)$. Since γ_1 and γ_2 are distinct, $\frac{d^2 f_1}{dt^2}(0) \neq \frac{d^2 f_2}{dt^2}(0)$. In the neighbourhood of (x, y, z), $\beta(\gamma_i)$ is parameterised by $\left(t, f_i(t), \frac{df_1}{dt}(t)\right)$. It follows that the vector $\left(1, \frac{df_i}{dt}(0), \frac{d^2 f_i}{dt^2}(0)\right)$ is in the space $T_{(x,y,z)}\beta(\gamma_i)$. Thus

$$\begin{aligned}(0, 0, 1) &\in \operatorname{span}\left(\left(1, \frac{df_1}{dt}(0), \frac{d^2 f_1}{dt^2}(0)\right) - \left(1, \frac{df_2}{dt}(0), \frac{d^2 f_2}{dt^2}(0)\right)\right) \\ &\subset \operatorname{span}\left(T_{(x,y,z)}\beta(\gamma_1), T_{(x,y,z)}\beta(\gamma_2)\right).\end{aligned}$$

Let $P \in \mathbb{R}[x, y, z]$ be the non-zero polynomial of minimal degree that vanishes on all the curves in $\beta(\Gamma)$. The degree of P is $\sim N^{1/2}$. By our result above, if (x, y, z) is a point where two curves from $\beta(\Gamma)$ intersect, then $\partial_z P(x, y, z) = 0$. Thus since each $\gamma \in \Gamma$ is tangent to $\gtrsim N^{1/2}$, and each of these tangencies occur at a distinct point, we have that $\partial_z P$ vanishes at $\gtrsim N^{1/2}$ points on each curve in $\beta(\Gamma)$. By Bézout's theorem we have that $\partial_z P$ vanishes on all curves in $\mathscr{C}$ as:

clean up here!

$$\deg(\partial_z P)\deg(\gamma) \sim (N^{1/2}) \gtrsim \#\{\partial_z P \cap \gamma\} \sim (N^{1/2}).$$

Since P was the non-zero polynomial of minimal degree that vanishes on all the curves in $\beta(\Gamma)$, we must conclude $\partial_z P = 0$. We have then that $P(x, y, z) = Q(x, y)$ for some $Q \in \mathbb{R}[x, y]$ with degree $\sim N^{1/2}$. But this implies that each of the N circles in Γ must be in $Z(Q)$. This is a contradiction, as Q has degree $\sim N^{1/2}$ whereas $\cup\gamma$ has degree $2N$. We conclude that Γ has fewer than $N^{3/2}$ tangencies. $\square$

Chapter 5

The Polynomial Method in Additive Combinatorics

Theorem 5.0.1 (Combinatorial Nullstellensatz)**.** *Let $\mathbb{K}$ be a (not necessarily finite) field, and let $P(x_1, \ldots, x_n) \in \mathbb{K}[X_1, \ldots, X_n]$ be a polynomial in n variables with coefficients in $\mathbb{K}$. Suppose $\deg P = \sum_{i=1}^{n} k_i$, where each k_i is a non-negative integer, and further suppose* Tautology? *the coefficient of $x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ is non-zero.*

Then for any subsets $A_1, \ldots A_n$ of $\mathbb{K}$ satisfying $|A_i| > k_i$ for each $1 \leq i \leq n$ there exist $a_1 \in A_1, \ldots, a_n \in A_n$ such that $P(a_1, \ldots, a_n) \neq 0$.

Proof. We proceed by induction on $\deg P = D$. When $D = 1$, P is simply a linear combination of n variables so the theorem holds.

Now let us assume the theorem holds for $\deg P = D - 1$, and prove for $\deg P = D$. Suppose that P satisfies the assumptions of the theorem but $P(x) = 0$ for every $x \in A_1 \times \cdots \times A_n$. Without loss of generality $k_1 > 0$. Fixing $a \in A_1$ we can write

$$P = (x_1 - a)Q + R \tag{†}$$

by the usual long division of polynomials. The degree of R in x_1 must be strictly less than $\deg(x_1 - a)$, so R does not contain any x_1 terms. Thus it follows that Q must have a monomial with non-zero coefficient of the form $x_1^{k_1-1} x_2^{k_2} \ldots x_n^{k_n}$ and $\deg(Q) = D - 1$.

Take any $x \in \{a\} \times A_2 \times \cdots \times A_n$ and evaluate (†). Since $P(x) = 0$ it follows that $R(x) = 0$, but R is independent of x_1 so R must also vanish on $A_1 \backslash \{a\} \times A_2 \times \cdots \times A_n$. Now take any $x \in A_1 \backslash \{a\} \times A_2 \times \cdots \times A_n$ and evaluate (†). Since $(x_1 - a)$ is non-zero, $Q(x) = 0$. So Q vanishes on all $x \in A_1 \backslash \{a\} \times A_2 \times \cdots \times A_n$, which contradicts the inductive hypothesis. $\square$

Theorem 5.0.2 (Cauchy-Davenport Theorem)**.** *Let A, B be non-empty subsets of $\mathbb{Z}_p$ for some p prime. Define their sumset $A + B$ as follows:*

$$A + B = \{x \in \mathbb{Z}_p \mid x = a + b \text{ for some } a \in A,\ b \in B\}.$$

Then we have:

$$|A+B| \geq \min\{p, |A|+|B|-1\}.$$

Generalise this!

Proof. Let us tackle the two cases separately. First, assume that $\min\{p, |A|+|B|-1\} = p$. Then if $|A|+|B| > p$, A and B must intersect. For some $g \in \mathbb{Z}_p$ denote the set $\{g - x \mid x \in B, \} \subset \mathbb{Z}_p$ as $g - B$. Since $|g - B| = |B|$, we have that $g - B$ and A must intersect as well. Thus there exists some $a \in A$, $b \in B$ such that:

More explanation on $\cap$ needed? PHP?

$$g - b = a$$
$$g = a + b.$$

Our choice of g was arbitrary, so it follows that $A + B = \mathbb{Z}_p$ and hence $|A+B| = p$.

Now assume that $\min\{p, |A|+|B|-1\} = |A|+|B|-1$. Then if the theorem is false we have $|A+B| \leq |A|+|B|-2$, so there exists some $C \subset \mathbb{Z}_p$ such that $A+B \subset C$ and $|C| = |A|+|B|-2$. Now let us define a polynomial $f(x,y) \in \mathbb{Z}_p[x,y]$ as:

$$f(x,y) = \prod_{c \in C}(x+y-c).$$

Since $A+B \subset C$, $f(a,b) = 0$ for all $(a,b) \in A \times B$. Further, the degree of f is $\deg f = |C| = |A|+|B|-2$. We can now appeal to the combinatorial nullstellensatz to yield a contradiction. Let $k_1 = |A|-1$, and $k_2 = |B|-1$. Now $\deg f = k_1 + k_2$, and the coefficient of $x^{k_1}y^{k_2}$ is $\binom{|A|+|B|-2}{|A|-1}$ which is non-zero in $\mathbb{Z}_p$ as the numerator cannot contain a factor of p by assumption. Applying Theorem 5.0.1 we see that there must exist some $(a,b) \in A \times B$ such that $f(a,b) \neq 0$, a contradiction. □

References

[1] Roy O Davies. Some remarks on the kakeya problem. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 69-3, pages 417–421. Cambridge University Press, 1971.

[2] Jean Bourga'in. Besicovitch type maximal operators and applications to fourier analysis. *Geometric & Functional Analysis GAFA*, 1(2):147–187, 1991.

[3] L. Guth. *Polynomial Methods in Combinatorics*. University Lecture Series. American Mathematical Society, 2016.

[4] Thomas Wolff. An improved bound for kakeya type maximal functions. *Revista Matemática Iberoamericana*, 11(3):651–674, 1995.

[5] Timothy Gowers. Topics in combinatorics - cambridge tripos lecture notes, 2020.

[6] Larry Guth and Nets Hawk Katz. Algebraic methods in discrete analogs of the kakeya problem, 2008.

[7] René Quilodrán. The joints problem in rn, 2009.

[8] Haim Kaplan, Micha Sharir, and Eugenii Shustin. On lines and joints, 2009.

[9] Jiří Matoušek, Anders Björner, Günter M Ziegler, et al. *Using the Borsuk-Ulam theorem: lectures on topological methods in combinatorics and geometry*. Springer, 2003.

[10] Jordan S. Ellenberg, Jozsef Solymosi, and Joshua Zahl. New bounds on curve tangencies and orthogonalities, 2016.