On Polynomial Methods in Combinatorics

Conrad Crowley

118316041

Supervisor: Dr. Marco Vitturi

Second Reader: Dr. Andrei Mustata

University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Table of Contents

List of Figures

Chapter 1

Introduction

The following is a short exposition of the polynomial method in combinatorics. It is perhaps already misleading to call this the polynomial method as there are in fact a collection of polynomial methods that have applications in combinatorics, the first example of this being known since the 1990s where Alon's proved a combinatorial version of Hibert's Nullstellensatz.[Alo99] We examine this result in detail in Chapter 3. In 2008 Dvir produced a remarkably short resolution to the finite field analogue of the Kakeya Conjecture which provided a new framework and enthusiasm for the polynomial method in combinatorial problems.[Dvi08] We will explore this proof in the next chapter.

The most striking feature of the following proofs is that they leverage polynomials in problems which on the surface appear not to have anything to do with polynomials. Generally, extremal configurations of these problems tend to have a lot of algebraic structure and this is exactly what these methods exploit using polynomials.

In Chapter 2 we will use a low degree polynomial to interpolate a certain set of objects. We will then show that the zero set of the polynomial can not contain too many objects of this type due to the inherent structure of these objects. In Chapter 4 we will ... . Chapter 5 introduces the idea of using a polynomial to partition the plane into a degree-controlled number of cells each containing at most some uniform amount of points. Chapter 6 will discuss a proof that first uses a similar strategy to Chapter 2, however in this proof we will be interpolating objects of one type and then proving that the polynomial's zero set cannot contain too many objects of some second related type. We then provide a new proof of the same theorem which uses an extension of the polynomial partitioning seen in 5, the key difference being that instead of controlling the number of points in each cell we will control the number of varieties that intersect any given cell. Finally, in Chapter 3 we will provide an example of the polynomial method being used outside the context of incidence geometry.

do something indeed

weak

1.1 Why polynomials?

this section

Points to possibly mention here:

1

1. choosing a polynomial has D^n degrees of freedom $[\mathrm{Poly}_D(\mathbb{F}^n) \sim D^n]$

2. polynomials behave rigidly on lines, having only D degrees of freedom.

3. "parameter counting - vanishing lemma" method.

4. Non constructive method of finding a polynomial is reminiscent of probabilistic method.[Gow20] [Gut16]

5. ill-formed thoughts that polynomials extract information about finite series analogous to generating functions and infinite series.

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.

The indicator function $\mathbb{1}$ is defined on logical statements X as follows:

$$\mathbb{1}[X] = \begin{cases} 1 & \text{if X is true,} \\ 0 & \text{if X is false.} \end{cases}$$

For any function $f : \mathbb{R}^n \to \mathbb{R}$ let us denote the zero set of f by $Z(f) = \{x \in \mathbb{R}^n \mid f(x) = 0\}$. We borrow from Computer Science the big O notation. For functions $f, g : \mathbb{N}^+ \to \mathbb{R}$ we write:

$$f(N) = O(g(N)) \iff \exists N_0, M \in \mathbb{N} \text{ such that } f(n) \leq Mg(n) \forall n > N_0$$
$$f(N) = \Omega(g(n)) \iff g(N) = O(f(N)).$$

These can be thought of as asymtopic upper and lower bounds respectively.

Chapter 2

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 was led to consider 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.[Pal20] The more interesting problem obtained by dropping 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 2.0.1 (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 process allows to extend the construction of these measure-zero sets to the case of arbitrary dimension.

Given that kakeya sets can have measure zero, the natural question then arises, are Kakeya sets fractal in Nature? This leads one to consider the dimension of Kakeya sets as a quantification of their fractal nature. There are many notions of dimensions that can

be investigated, but we restrict ourselves to the Minkowski and Hausdorff dimensions.

Definition 2.0.2 (Minkowski Dimension). Given a set $S \subset \mathbb{R}^n$, define $N(\varepsilon)$ to be the number of cubes 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 2.0.3 (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 published [Dav71] showing that although the measure of a Kakeya set in $\mathbb{R}^2$ can be arbitrarily small, it must have Hausdorff and Minkowski dimension of 2. 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 $\dim_H(A) = n$.

In a survey on the problem, (see [Wol99]) Wolff proposed a finite analogue to the Kakeya Conjecture.

Definition 2.0.4 (Finite Field). A **finite field** $\mathbb{F}$ is a field of finite cardinality. The cardinality $|\mathbb{F}|$ of a finite field is called the **order** of the finite field.

It is known that finite field of order q exists if and only if $q = p^k$ for some prime p and integer k.

Lemma 2.0.1. *Each element X in a finite field $\mathbb{F}$ satisfies the identity:*

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

identically in $\mathbb{F}$.

Proof. This lemma follows immediately from Fermat's Little Theorem. $\qquad\square$

A Kakeya set in $\mathbb{F}_q^n$ is a set that contains a line in every direction. In analogy to the Euclidean case, we formally define lines in $\mathbb{F}_q^n$ as the sets of the form

$$\ell_{x,y} = \{x + ty : t \in \mathbb{F}_q\}$$

for some fixed $x, y \in \mathbb{F}_q^n$ with $y \neq 0$. It should be noted that a line in a finite field $\mathbb{F}_q^n$ contains exactly $|\mathbb{F}_q|$ points. Formally, directions in $\mathbb{F}_q^n$ can be identified using the projective space $\mathbb{PF}_q^n = \mathbb{F}_q^n / \mathbb{F}_q^\times$. In this projective space, two lines y and y' are equivalent if y' is a translation of y. The finite analogue to Conjectures 1 and 2 is:

Conjecture 3 (Kakeya Conjecture in Finite Fields). If $A \subset \mathbb{F}_q^n$ contains a line in every direction, then $|A| \geq \frac{1}{n!}|\mathbb{F}_q|^n$.

This conjecture had a significant influence on the subject, inspiring work on the sum-product phenomenon in finite fields. From its postulation in 1999, little progress was made in the following years and it was assumed that the problem was roughly as difficult as the Euclidean case.

In 2008, Dvir published a remarkably simple proof of Conjecture 3 using basic facts about polynomials. This proof revitalised interest in the polynomial method, and we shall explore its details later in this chapter.
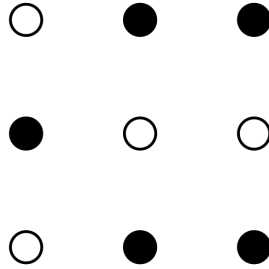
Figure 2.1: An example of a Kakeya set (shaded) in $\mathbb{F}_3^2$.

2.1 Combinatorial Attempts

To truly show the power of the polynomial method, we shall first explore purely combinatorial attempts at estimating the sizes of Kakeya sets. All of the following estimates are much weaker than the bound in Theorem 3. We fix a finite field $\mathbb{F} = \mathbb{F}_{p^k}$ where p is a prime.

Our first estimate shows that Conjecture 3 is true for the $n = 2$ case.

Lemma 2.1.1. *Suppose $s \leq |\mathbb{F}|$. If $l_1, \ldots, l_s$ are distinct lines in $\mathbb{F}^n$, then their union has cardinality at least $(1/2)|\mathbb{F}|s$.*

In particular, if $A \subset \mathbb{F}^n$ is a Kakeya set, then we have

$$|A| \gtrsim |\mathbb{F}|^2$$

Proof. We add the lines together one at a time and track the cardinality of their union. The first line contains $|\mathbb{F}|$ points. The second line must contain at least $|\mathbb{F}| - 1$ points not in the first line. Similarly the third line must contain at least $|\mathbb{F}| - 2$ points not in the first two lines, and so on. Thus the number of distinct points in the union of all s lines is given by

$$\sum_{i=1}^{s} |\mathbb{F}| - i + 1 > (1/2)|\mathbb{F}|s.$$

A Kakeya set always contains at least $|\mathbb{F}|$ lines, so setting $s = |\mathbb{F}|$ above yields

$$|A| > (1/2)|\mathbb{F}|^2.$$

$\square$

2.1.1   Bush Argument

Bourgain produced one of the first non-trivial estimates of the dimension in 1991.[Bou91] We present the finite field analogue of his argument here.[Gut16] This argument is known as the "bush" argument as we consider a high-multiplicity point through which pass many lines, forming a "bush" around that point.

Theorem 2.1.2 (Bush Argument)**.** *If A is a Kakeya set, then we have*

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

Proof. Let μ be a fixed multiplicity parameter to be chosen later. Either there exists a point $p \in A$ such that there are μ lines passing through p, or else every point in A has less than μ lines passing through it.

In the first case, since the lines have distinct directions they must become disjoint when p is removed. Hence,

$$|A| \gtrsim \mu|\mathbb{F}|.$$

In the latter case, by double counting we have

$$\sum_{\ell \subset A} \sum_{p \in A} \mathbb{1}[p \in \ell] = \sum_{\ell \subset A} |\mathbb{F}| = |\mathbb{F}|^{n-1}|\mathbb{F}|$$

$$\sum_{p \in A} \sum_{\ell \subset A} \mathbb{1}[p \in \ell] \leq \sum_{p \in A} \mu = |A|\mu$$

$$\implies \frac{|\mathbb{F}|^n}{\mu} \leq |A|.$$

Now we optimise the two lower bounds by choosing $\mu \sim |\mathbb{F}|^{\frac{n-1}{2}}$, so that in either of the above cases we obtain

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

$\square$

2.1.2 Hairbrush Argument

In [Wol95], Wolff presented the "hairbrush" argument we made an incremental improvement over the argument of Bourgain. It is similar in spirit to the "bush" argument above, however instead of using just one point of high-multiplicity we instead consider a line (or "stem") containing many points of high-multiplicity.

Theorem 2.1.3 (Hair Brush Argument). *If A is a Kakeya set, then we have*

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

Proof. Let μ be a fixed multiplicity parameter to be chosen later. We say a line ℓ is μ-rich if for at least $|\mathbb{F}|/2$ points $p \in \ell$ there are μ lines distinct from ℓ in A passing through p. Then either there exists a μ-rich line or there does not.

Suppose a μ-rich line exists, and denote this line by ℓ_μ. Consider the family Π of 2-dimensional planes passing through ℓ_μ. If a line ℓ intersects ℓ_μ then there exists a unique plane $\pi \in \Pi$ such that $\ell, \ell_\mu \in \pi$. Let $\mathcal{L}_\pi := \{\ell \subset \pi \mid \ell \cap \ell_\mu \neq \emptyset\}$. The set $A \cap \pi$ is a set in (an isomorphic copy of) $\mathbb{F}^2$ that contains at least $|\mathcal{L}_\pi|$ lines, and hence by Lemma 2.1.1 we have

$$|A \cap \pi| \gtrsim |\mathcal{L}_\pi||\mathbb{F}|.$$

Thus,

$$|A| \geq \sum_{\pi \in \Pi} |(A \cap \pi)\backslash \ell_\mu| \gtrsim |\mathbb{F}| \sum_{\pi \in \Pi} |\mathcal{L}_\pi| \gtrsim \mu|\mathbb{F}|^2,$$

where the last inequality comes from the fact ℓ_μ intersects at least $\mu|\mathbb{F}|/2$ lines, so since the planes Π foliate $\mathbb{F}^n$, the union $\cup_\Pi \mathcal{L}_\pi$ contains at least all of these lines.

Suppose there does not exist a μ-rich line. Let

$$A' = \{p \in A \mid p \text{ belongs to strictly less than } \mu \text{ lines in } A\}.$$

Since we assume there does not exist a μ-rich line in A, for any line $\ell \subset A$ we have $|A' \cap \ell| > |F|/2$. Proceeding by double counting,

$$|A| \geq |A'| \geq \frac{1}{\mu} \sum_{p \in A'} \sum_{\ell \subset A} \mathbb{1}[p \in \ell]$$

$$= \frac{1}{\mu} \sum_{\ell \subset A} |A' \cap \ell| \gtrsim \frac{1}{\mu} |\mathbb{F}|^{n-1} |\mathbb{F}|$$

$$\implies |A| \gtrsim \frac{|\mathbb{F}|^n}{\mu}.$$

Now optimising the two lower bounds by choosing $\mu \sim |\mathbb{F}|^{\frac{n-2}{2}}$, so that in either of the above cases we obtain the bound

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

$\square$

2.2   Dvir's Proof

Theorem 2.2.1 (Kakeya Conjecture in Finite Fields)**.** *If $A \subset \mathbb{F}_q^n$ contains a line in every direction, then $|A| \geq \frac{1}{n!}|\mathbb{F}_q|^n$.*

We shall prove this theorem via three surprisingly elementary lemmas. The general strategy of the proof is to assume the size of a Kakeya set A is small and find a low-degree non-zero polynomial that interpolates (contains in its zero set) the points in A. We then show that due to the structure of the Kakeya set the polynomial's zero set must contain many more points. This contradicts the fact our polynomial is non-zero and of low-degree which establishes the Kakeya Conjecture over finite fields.

The first lemma is a fundamental one to the polynomial method, exploiting the flexible interpolation properties of polynomials. Consider the problem of finding a non-zero polynomial in $\mathbb{R}[X, Y, Z]$ of the minimal possible degree that vanishes at the points $(j, k, 2^{j^k})$ for $1 \leq i \leq 10^6$. If we try to find an explicit polynomial we may produce

$$P(X, Y, Z) = \prod_{j,k=1}^{10^6} (X - j)(Y - k)$$

or perhaps

$$Q(X, Y, Z) = \prod_{j,k=1}^{10^6} (Z - 2^{j^k}).$$

Both P and Q vanish on our points and it is difficult to explicitly produce a polynomial of much lower degree that also satisfies this property. Q has a degree of 10^12, and naively

one might conjecture that the degree of any polynomial with this property is of the order of 10^12. Remarkably, the following lemma shows that we can find such a polynomial with a degree of about ~ 18000. This polynomial has roughly 18000^3 coefficients and as such the polynomial is quite difficult to explicitly write, but we can establish the existence of such a polynomial non-constructively.

come back to this

Lemma 2.2.2 (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 at most* 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 nth $|$. 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 assemble such a string we distribute the n $|$'s over $n + D$ spaces, and then fill the remainder with $\star$'s. Hence we get the binomial coefficient:

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

Now let $p_1, \ldots, p_{|A|}$ 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 at most $|\mathbb{F}| - 1$ that vanishes on A. Since $\frac{|\mathbb{F}|^n}{n!} < \binom{|\mathbb{F}|+n-1}{n}$, we can definitely find such a polynomial when $|A| \leq \frac{|\mathbb{F}|^n}{n!}$. The restriction of $D = |\mathbb{F}| - 1$ is somewhat necessary due to the fact that polynomials with a factor of $X^{|\mathbb{F}|} - X$ vanish identically by Lemma 2.0.1.

Lemma 2.2.3. *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 $\ell = \{x + ty : t \in \mathbb{F}\}$ with $x, y \in \mathbb{F}^n$ and $y \neq 0$. 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:

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

We now wish to examine the degree D term of Q, which consist in the terms of the expansion of the expression above obtained by the product of the ty_i terms when $|\alpha| = D$.

This is related to the degree D component Q_D of Q by the identity

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

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. In particular, we must have $Q_{x,y,D} = 0$. This is clear from the factor theorem, as we could write the roots of $P_{|\ell}$ as $(t - k_1)(t - k_2) \ldots (t - k_{|\mathbb{F}|})$; but this contradicts the fact P is of degree $D < |\mathbb{F}|$.

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

Lemma 2.2.4. *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 proceed by contradiction, assuming that P vanishes everywhere. We let $X_1, \ldots, X_n$ be coordinates on $\mathbb{F}^n$, and we write P in the form

$$P(X_1, \ldots, X_n) = \sum_{j=n}^{|\mathbb{F}|-1} P_j(X_1, \ldots X_{n-1}) X_n^j.$$

Each P_j are polynomials in $X_1, \ldots X_{n-1}$ of degree less than $|\mathbb{F}|$. Fix $X_1, \ldots X_{n-1}$, 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 $P_j(x_1, \ldots, x_{n-1}) = 0$ for all j and for all $(x_1, \ldots x_{n-1}) \in \mathbb{F}^{n-1}$. Now by induction on n, each P_j is the zero polynomial. Then P is the zero polynomial as well. $\qquad \square$

We now combine these lemmas to establish the Kakeya conjecture over finite fields.

Proof of Theorem 2.2.1. Assume $A \subset \mathbb{F}^n$ is a Kakeya set, and that $|A| \leq \frac{|\mathbb{F}|^n}{n!}$. Then by Lemma 2.2.2 we can find a non-zero polynomial of degree at most $|\mathbb{F}| - 1$, say P, that vanishes on A. Now by Lemma 2.2.3 there exists a non-zero polynomial $\bar{P}$ that vanishes everywhere on $\mathbb{F}^n$, and has degree less than $|\mathbb{F}|$. Finally, Lemma 2.2.4 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:

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

$\square$

Remark. *Theorem 2.2.1 lends a good degree of support for Conjectures 1 and 2 as it essentially rules out purely algebraic counter-examples.*

Chapter 3

Cauchy-Davenport Theorem

In this chapter we shall discuss applications to the exciting field of additive combinatorics, where in 1990 Alon provided perhaps the first example of a polynomial method in action (see [Alo99]). This chapter is distinct from the other chapters in this manuscript as it deals with applications outside a geometric setting. It showcases a different polynomial method to the previous chapter, employing instead a combinatorial version of Hilbert's Nullstellensatz. In [mic10], Michalek produced a short, elementary, and direct proof of the combinatorial Nullstellensatz which we present here.

3.1   Combinatorial Nullstellensatz

The German term *Nullstellensatz* means "theorem about zeros", so it should come as no surprise that the theorem is precisely a statement about the general size and shape of sets of zeros of a polynomial depending on its highest degree terms.

The main idea behind the Nullstellensatz comes from the fact that a polynomial in one variable of degree D cannot have more than D roots. As a consequence of this if we have a set of $D+1$ elements they cannot all be roots of the same degree D polynomial. In the univariate case this is somewhat elementary, but it has a very non-trivial extension to grids of points in arbitrary dimensions.

Theorem 3.1.1 (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 the coefficient of $X_1^{k_1} X_2^{k_2} \ldots X_n^{k_n}$ is non-zero and further suppose $\deg P = \sum_{i=1}^{n} k_i$, where each k_i is a non-negative integer.*

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

Proof. We proceed by induction on $\deg P = D$. When $D = 1$, P is simply a linear combination of n variables say $P(X_1, \ldots X_m) = c_1 X_1 + \ldots c_n X_n$. Without loss of generality assume X_1 has a non-zero coefficient and consider the sets $A_i = \{a_i, b_i\}$. Suppose P at

the point $(a_1, a_2, \ldots, a_n)$ is zero. We can then determine

$$c_1 = -\frac{c_2 a_2 + c_3 a_3 + \cdots + c_n a_n}{a_1}.$$

Now evaluating at $(b_1, a_2, \ldots, a_n)$ we see that this is zero only when $a_1 = b_1$, so our theorem holds.

Now let us assume the theorem holds for $\deg P = D - 1$, and prove it 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

$$P = (x_1 - a)Q + R \tag{3.1}$$

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 is independent of X_1. 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 (3.1). Since $P(x) = 0$ it follows that $R(x) = 0$. Hence R vanishes identically on the slice $\{a\} \times A_2 \times \cdots \times A_n$. Since R is independent of X_1 it must also vanish identically on $A_1 \times A_2 \times \cdots \times A_n$. Now take any $x \in A_1 \backslash \{a\} \times A_2 \times \cdots \times A_n$ and evaluate (3.1). Since the $(X_1 - a)$ term 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. $\qquad\square$

3.2 Proof of Cauchy-Davenport Theorem

To showcase the usefulness of the Combinatorial Nullstellensatz, we shall prove a classical result in Additive Combinatorics.

Theorem 3.2.1 (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:
$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

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 by the pigeonhole principle. For any $g \in \mathbb{Z}_p$ 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:

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

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 binomial coefficient is not divisible by p if all its factors are less than p. Applying Theorem 3.1.1 we see that there must exist some $(a, b) \in A \times B$ such that $f(a, b) \neq 0$, a contradiction. $\qquad\square$

The Cauchy-Davenport Theorem (Theorem 3.2.1) is indeed tight as illustrated by the following example.

Example 3.1. *Fix $b \in \mathbb{Z}_p$ and consider the subsets of $\mathbb{Z}_p$ given by*

$$A = \{tb \mid 1 \leq t \leq m\},$$
$$B = \{t'b \mid 1 \leq t' \leq n\}.$$

Notice that $|A| = m$ and $|B| = n$. Their sumset is given by

$$A + B = \{(t + t')b \mid 1 \leq t \leq m, \ 1 \leq t' \leq m\}.$$

The $(t + t')$ term takes on every value between 2 and $m + n$ at least once. Hence

$$|A + B| = m + n - 1 = |A| + |B| - 1.$$

Chapter 4

The Joints Problem

Definition 4.0.1. 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 in obtaining 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 $J(L)$. In other words $J(L)$ is the supremum over all configurations of lines in $\mathbb{R}^n$ of the number of joints.

The joints problem was first posed in 1990 by Chazelle et al in [CEG$^+$90]. They focused on the 3-dimensional case of the problem, establishing a lower bound of $\Omega(N^{3/2})$ and an upper bound estimate of $O(N^{7/4})$. This upper bound exponent has fallen gradually throughout the years, the best result prior to the application of the polynomial method being due to Sharir and Feldman in [FS05] where they established an upper bound of $O(N^{112/69})$. Their proof uses an array of tools from combinatorial geometry, including forbidden subgraphs in extremal graph theory, space decomposition techniques, and some results from the geometry of lines in space.

4.1   Examples

We shall begin by examining an example based on a grid, in order to gain better intuition about the problem and formulating a conjecture.

Example 4.1. *Consider an $N \times N \times N$ regular grid of integer coordinates in $\mathbb{R}^3$. 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 a point in this grid. For each horizontal $N \times N$ layer, there are $N + N = 2N$ such 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 horizontal $N \times N$ layers. This leaves us with $|\mathcal{L}| = 3N^2$ lines forming N^3 joints. The number of joints is thus $\sim |\mathcal{L}|^{3/2}$.*

We can extend this example to higher dimensional grids easily.
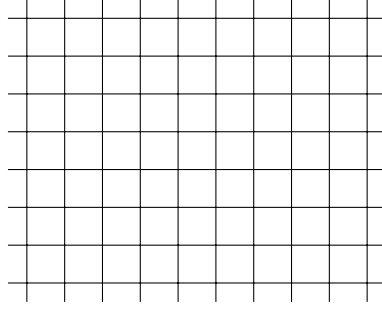
Figure 4.1: A $N \times N$ layer of our grid.

Example 4.2. *If we have an* $\underbrace{N \times \cdots \times N}_{n \ Dimensions}$ *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 $J(L) \leq CL^{\frac{n}{n-1}}$.

4.2 Solution of the Joints Problem

This solution was first produced by Guth-Katz for the three-dimensional case in[GK08] and later extended to the general case by Quilodrán in [Qui09] and independently at the same time by Kaplan-Sharir-Shustin in [KSS09].

Theorem 4.2.1. *In* $\mathbb{R}^n$ *we have*

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

We begin with the fundamental lemma to this proof.

Lemma 4.2.2. *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.*

poly method strat

Proof. Let P be a non-zero polynomial that vanishes at every joint of $\mathcal{L}$ and assume that the degree of P is minimal. By parameter counting (Lemma 2.2.2) the degree of P is at most $nJ^{\frac{1}{n}}$. (To see this, set $D = \lfloor nJ^{\frac{1}{n}} \rfloor$ and then notice that $J < \binom{D+n}{n}$.)

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 contained in the line, which are points of intersection between the line and $Z(P)$.

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

Lemma 4.2.3. *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 $l_1, \ldots, l_n$ with directions $v_1, \ldots, v_n$ respectively. Now consider the directional derivative for a particular v_i:

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

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 $\nabla F(x) = 0$. $\qquad \square$

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 a non-zero polynomial of minimal degree that vanishes at each joint, each derivative of P must be identically zero. This implies P must be constant, which is a contradiction. $\qquad \square$

Finally we can prove the main result.

Proof. Lemma 4.2.2 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

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

Rearranging we have

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

$\qquad \square$

Chapter 5

Szemerédi-Trotter Theorem

Incidence geometry is the quantitive study of incidence relations between simple geometric objects, such as lines or low degree curves. In this chapter we will study the application of the polynomial method to incidence geometry by proving a fundamental theorem in the field. 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 $\mathbb{R}^n$ can play in such problems.

The Szemerédi-Trotter theorem is a fundamental result in the field of incidence geometry, originally proved by an involved cell decomposition argument of Szemerédi and Trotter in [ST83] and later given a shorter proof using the crossing-number inequality by Székely in [Szé97].

Theorem 5.0.1 (Szemerédi-Trotter)**.** *Let $\mathcal{S} \subset \mathbb{R}^2$ be a finite set of points and let $\mathcal{L}$ be a finite set of lines in $\mathbb{R}^2$. 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

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

5.1 The Trivial Bounds

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

Lemma 5.1.1 (Trivial Bounds)**.** *For a set of points $\mathcal{S}$ and lines $\mathcal{L}$ we have*

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

and

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

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 by the pigeonhole principle there would exist a $p \in \mathcal{S}$ that lies in 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 as two lines intersect in at most one point. □

By double counting we can achieve a slightly less trivial bound, which as we will see in the next section turns out to be tight in finite fields.

Lemma 5.1.2 (Double Counting Bounds). *For a set of points $\mathcal{S}$ and lines $\mathcal{L}$ we have*

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

and

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

Proof. We bound the number of incidences using the Cauchy-Schwarz inequality followed by double counting.

$$|I(\mathcal{S}, \mathcal{L})|^2 = \left(\sum_{\ell \in \mathcal{L}} \sum_{p \in \mathcal{S}} \mathbb{1}[p \in \ell] \right)^2$$

Applying the Cauchy-Schwarz on $\mathcal{L}$ we attain

$$\leq |\mathcal{L}| \cdot \sum_{\ell \in \mathcal{L}} \left(\sum_{p \in \mathcal{S}} \mathbb{1}[p \in \ell] \right)^2$$
$$= |\mathcal{L}| \cdot \sum_{p_1, p_2 \in \mathcal{S}} \sum_{\ell \in \mathcal{L}} \mathbb{1}[p_1 \in \ell] \mathbb{1}[p_2 \in \ell]$$
$$\leq |\mathcal{L}| \cdot (|I(\mathcal{S}, \mathcal{L})| + |\mathcal{S}|^2)$$
$$\leq |\mathcal{L}|^2 + 2|\mathcal{L}| \cdot |\mathcal{S}|^2 \qquad \text{(Using Lemma 5.1.1)}$$

This implies

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

extra step needed here - split up sum and do triple

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

5.2   Examples

We can not improve beyond the double counting bounds shown in Lemma 5.1.2 in a finite field $\mathbb{F}^2$.

Example 5.1 (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 double counting bounds (Lemma 5.1.2) 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 turn out to be the best possible over $\mathbb{R}$. We will later prove that these are optimal for the Szemerédi–Trotter Theorem. We denote a line in $\mathbb{R}^2$ as follows

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

First we examine two trivial examples that explain the necessity of the $|\mathcal{S}| + |\mathcal{L}|$ terms in Theorem 5.0.1.

Example 5.2. *Let $|\mathcal{S}| = 1$ and suppose all $|\mathcal{L}|$ lines in $\mathcal{L}$ pass through this point. Then both sides of the Szemerédi-Trotter (Theorem 5.0.1) inequality are comparable as*

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

Consider the dual case where $|\mathcal{L}| = 1$ and suppose all $|\mathcal{S}|$ points in $\mathcal{S}$ lie on $\mathcal{L}$. Again we have

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

The next two examples deal with the more general case, where the $(|\mathcal{S}||\mathcal{L}|)^{2/3}$ term dominates Theorem 5.0.1.

Example 5.3. *Let N be a large integer and consider the following collections in $\mathbb{R}^2$*

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

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 (Theorem 5.0.1) inequality are comparable as

$$|I(\mathcal{S}, \mathcal{L})| = N^4 \sim (N^3)^{\frac{2}{3}}(N^3)^{\frac{2}{3}} \sim |\mathcal{S}|^{2/3}|\mathcal{L}|^{2/3} + |\mathcal{S}| + |\mathcal{L}|.$$
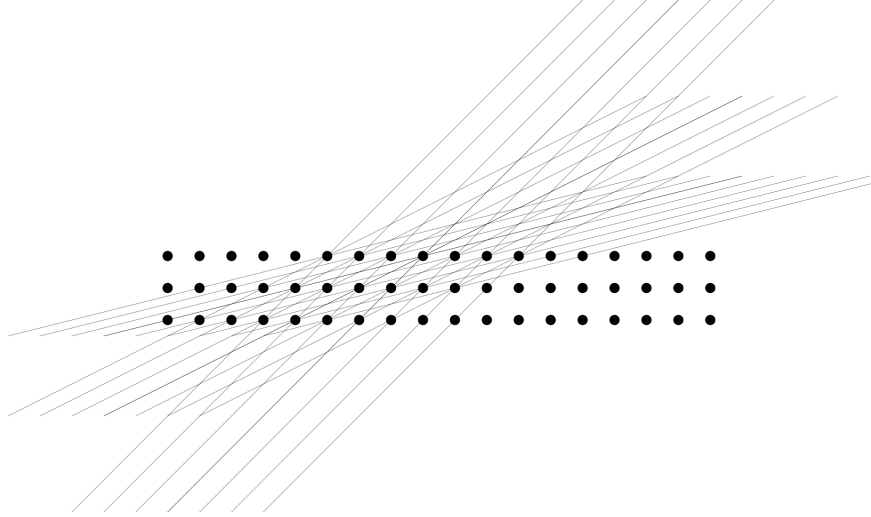
Figure 5.1: Example 5.3 in the case $N = 3$. (with the x, y axis reversed)

Example 5.4. *Let $N \gg 1$ be a large even integer and let $1 < R \ll N$ be another integer. Consider the collections in $\mathbb{R}^2$:*

$$\mathcal{S} = \{(a, b) \in \mathbb{Z}^2 \mid (a, b) \in [-N/2, N/2] \times [-N/2, N/2]\}$$

$$\mathcal{L} = \{\ell \mid \ell \text{ contains between } R \text{ and } 2R \text{ points of } \mathcal{S}\}$$

We begin by estimating how many lines of $\mathcal{L}$ 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 $\sim R$ 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 $\lesssim N^2/R^2$ lines in $\mathcal{L}$ through a given point p.

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 $\mathcal{S}$ it is enough that $m = \frac{l}{k} \in \mathbb{Q}$ with $\gcd(l, k) = 1$ and $l, k \in \left[\frac{N}{2R}, \frac{N}{R}\right]$. There are $\gtrsim N^2/R^2$ such pairs (l, k), 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

$$|\mathcal{S}| \sim N^2,$$

$$|\mathcal{L}| \sim |\mathcal{S}|\frac{N^2}{R^2}\frac{1}{R} \sim \frac{N^4}{R^3},$$

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

we can see that both sides of the Szemerédi-Trotter inequality (Theorem 5.0.1) are comparable:

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

add diagram (!)

5.3   Ham Sandwich Theorems

The above examples suggest that the topology of $\mathbb{R}^2$ plays a key role in this incidence problem. We shall now introduce the method of polynomial partitioning, which can be seen as the topological analogue to the vanishing lemma (Lemma 2.2.3) we used in the previous chapters.

The topological input in the proof will be provided by the following well-known result of Borsuk-Ulam. Let $\mathbb{S}^n$ denote the unit n-sphere in $\mathbb{R}^{n+1}$.

Theorem 5.3.1 (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.*

In the appendix to this manuscript, we present a beautiful combinatorial proof from Matousek's book *Using the Borsuk-Ulam theorem* (see [MBZ$^+$03]). The proof proceeds by constructively proving the Tucker Lemma, and then using this to imply the Borsuk-Ulam theorem.

Let us now define some useful definitions going forward.

Definition 5.3.1 (Bisection of a Set). A function $f : \mathbb{R}^n \to \mathbb{R}$ is said to bisect an open set U with volume[1] $\mathrm{Vol}(U) < \infty$ 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

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

We now show that as a consequence of Theorem 5.3.1, it is always possible to find a non-zero continuous function that bisects every open set in a collection.

Theorem 5.3.2 (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.

---

[1]This is just the Lebesgue measure.

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 ϕ_i 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 $U \backslash E$ with $m(E) < \varepsilon$. 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

$$\begin{aligned}
|m\left(\{x \in U \mid f_n(x) > 0\}\right) &- m\left(\{x \in U \mid f(x) > 0\}\right)| \\
&\leq |m\left(\{x \in U \mid f_n(x) > 0\}\right)| + |m\left(\{x \in U \mid f(x) > 0\}\right)| \\
&= |m\left(\{x \in U \mid f_n(x) > 0, f > 0\}\right)| + |m\left(\{x \in U \mid f_n(x) > 0, f < 0\}\right)| \\
&\quad - |m\left(\{x \in U \mid f > 0, f_n(x) > 0\}\right)| - |m\left(\{x \in U \mid f > 0, f_n(x) < 0\}\right)| \\
&= |m\left(\{x \in U \mid f_n(x) > 0, f < 0\}\right)| - |m\left(\{x \in U \mid f(x) > 0, f_n < 0\}\right)|
\end{aligned}$$

These two remaining terms are symmetrical, so we only need bound one of them. We continue to bound

$$< 2\varepsilon.$$

Since ε was arbitrary each ϕ_i is continuous.

We now combine each ϕ_i into the map $\phi : V \backslash \{0\} \to \mathbb{R}^N$ by $\phi = (\phi_1, \ldots, \phi_N)$. Since $\dim V > N$, select a subspace $W < V$ such that $\dim W = N + 1$. Now choose an isomorphism of W with $\mathbb{R}^{N+1}$, and think of $\mathbb{S}^N$ as a subset of W . 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 $\phi(f) = 0$. $\qquad \square$

> Explain that ϕ is actually a function on the unit sphere of V
>
> check

We are now going to use the Ham Sandwich Theorem to extend the conclusion to the bijection of finite sets also. The main idea will be to construct sets of arbitrarily small measure around each of our points in the finite set and apply the previous theorem.

Corollary 5.3.1 (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 $P \in \mathrm{Poly}_D(\mathbb{R}^n)$ that bisects each S_i.*

> V or poly Rn?

Proof. Let us equip the space with the L^1 norm. For each $\delta > 0$, define $U_{i,\delta}$ to be the union of δ-balls centred at the points of S_i. By Theorem 5.3.2, we can find a non-zero

P_δ with degree at most D that bisects each $U_{i,\delta}$. By rescaling we can assume $P_\delta \in \mathbb{S}^M \subset \mathrm{Poly}_D(\mathbb{R}^n)\backslash\{0\}$. Since $\mathbb{S}^M$ compact, we can find a sequence $\delta_m \to 0$ so that P_{δ_m} converges to P in $\mathbb{S}^M$. Since the coefficients of P_{δ_m} converge t1o those of P, P_{δ_m} converges to P uniformly on compact sets.

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 volume of the set U_{i,δ_m}, a contradiction. $\qquad \square$ **[check]**

We now utilise the above results to prove a powerful cell decomposition technique known as polynomial partitioning.

Theorem 5.3.3 (Polynomial Partitioning). *If S is a finite subset of $\mathbb{R}^n$ and D any degree, there exists a polynomial P of degree D such that $\mathbb{R}\backslash Z(P)$ is a disjoint union of $\sim D^n$* **[$\sim$ or $\lesssim$]** *open sets O_i each containing $\lesssim_n |S|D^{-n}$ points.*

Proof. The main idea of the 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,

$$P_1^+ = \{x \in S \mid P_1(x) > 0\}$$

and

$$P_1^- = \{x \in S \mid P_1(x) < 0\}$$

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 simultaneously bisects 2^{j-1} finite sets. By the Finite Ham Sandwich Theorem, we can find a polynomial of degree $\lesssim 2^{j/n}$ that simultaneously bisects 2^{j-1} finite sets.

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 $\leq |S|2^{-J} \leq c(n)|S|D^{-n}$ $\qquad \square$ **[unsure how to rephrase this]**

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 complement.

This is made most clear looking at the following two extremes. If all points line in the complement of $Z(P)$ then we have an optimal equidistribution of points, and can often use trivial bounds in a divide-and-conquer style argument. On the other hand, 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 complement which we need to deal with separately.

5.4   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 $|\mathcal{L}| = L$.

Considering the regime where $L > S^2$ and applying the trivial bounds (Lemma 5.1.1) yields
$$|I(\mathcal{S}, \mathcal{L})| \leq S^2 + L \sim L \sim (SL)^{2/3} + S + L.$$

Similarly in the case $L < S^{\frac{1}{2}}$ we have

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

Hence we need only consider the case $S^{\frac{1}{2}} \leq L \leq S^2$.

Let D be a fixed degree to be chosen later. By Theorem 5.3.3, there exists a polynomial P of degree D such that $\mathbb{R}^2 \backslash Z(P)$ splits into $\sim D^2$ disjoint open sets each containing $\lesssim SD^{-2}$ points of $\mathcal{S}$. Let $\{O_i \mid i \in \Pi\}$ denote the family of these components and let $\mathcal{S}_i = \mathcal{S} \cap O_i$ and $\mathcal{L}_i$ denote the lines that intersect the interior of each O_i respectively. We define the following pairs of complementary sets

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

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

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

We begin by examining the $I(\mathcal{S}_c, \mathcal{L})$ term

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

Using our trivial bound in each cell we attain

$$\leq \sum_{i\in\Pi} \mathcal{S}_i^2 + \sum_{i\in\Pi} \mathcal{L}_i.$$

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 $\sum_{i\in\Pi} L_i \leq (D+1)L$. So we have

$$\lesssim LD + SD^{-2} \sum_{i\in\Pi} S_i$$

$$\leq LD + S^2 D^{-2}.$$

The number of lines in $\mathcal{L}_z$ is at most D as $Z(P)$ can contain at most D degree 1 factors. **check** So we have by our trivial bounds (Lemma 5.1.1)

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

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:

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

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 to each other and hence $D \sim S^{\frac{2}{3}} L^{-\frac{1}{3}}$. From our restriction $S^{\frac{1}{2}} \leq L \leq S^2$ we have $S^{\frac{2}{3}} L^{-\frac{1}{3}} \geq 1$ and $D^2 \sim S^{\frac{4}{3}} L^{-\frac{2}{3}} \leq S$, so we achieve

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

Finally combining this with our result for the regime where $L > S^2$ we achieve 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 $\mathbb{R}^2$ plays. We use topology twice in the above proof. Firstly by using polynomial partitioning, which itself is a consequence of the Borsuk-Ulam theorem from topology. We also appeal to topology in our claim that each line intersects at most $\deg P + 1$ components of $\mathbb{R}^2 \backslash Z(P)$. It is a worthwhile heuristic to develop that polynomial **check** 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 were able to use very trivial bounds in each cell to achieve an asymptotically tight overall bound.

Chapter 6

Counting Circle Tangencies

Here we shall discuss the problem of counting the number of tangencies in a suitably non-degenerate collection of circles. We say two circles are tangent if their intersection contains a single point. The set of pairs of circles in a collection $\mathcal{C}$ which are mutually tangent are called the tangencies and the collection of all tangencies is denoted $\tau(\mathcal{C})$.

6.1 Trivial Bounds

Lemma 6.1.1 (Trivial Bound). *Let $\mathcal{C}$ be an arbitrary finite collection of circles. Then the number of tangencies $|\tau(\mathcal{C})|$ is bounded as follows:*

$$|\tau(\mathcal{C})| \leq |\mathcal{C}|^2.$$

Stated for arbitrary collections of circles the problem is not particularly interesting as the above bound turns out to be asymptotically tight, as the following example shows.

Example 6.1. *Denote a circle centred at (x, y) with radius r as $\gamma(x, y, r)$. Consider the following collection of $N + 1$ circles:*

$$C_0 = \gamma\,(0, 0, 1)$$
$$C_1 = \gamma\left(\frac{1}{2}, 0, \frac{1}{2}\right)$$
$$C_2 = \gamma\left(\frac{3}{4}, 0, \frac{1}{4}\right)$$
$$\vdots$$
$$C_N = \gamma\left(1 - \frac{1}{2^N}, 0, \frac{1}{2^N}\right)$$

Each circle in our collection $\mathcal{C} = \{C_i \mid 0 \leq i \leq N\}$ is tangent to N other circles at the point (1,0). Hence $|\tau(\mathcal{C})| \sim N^2 \sim |\mathcal{C}|^2$.

In light of this example, in order to obtain a non-trivial example we shall look at collections of circles that satisfy a non-degeneracy condition. We consider collections of
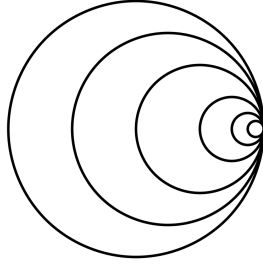
Figure 6.1: A collection of circles in $\mathbb{R}^2$ with N^2 tangencies.

circles such that no three circles are mutually tangent at a common point. The best known examples for collections that satisfy this non-degeneracy condition leverage our asymptotically tight Szemerédi-Trotter Theorem (Theorem 5.0.1) examples:

Example 6.2. *Let $\mathcal{S}$, $\mathcal{L}$ be collections of N points and N lines respectively such that the Szemerédi-Trotter Theorem's bound is asymptotically tight. In particular, they determine $\sim N^{4/3}$ point-line incidences. Let C_1 denote the collection of unit circles centred at the points of $\mathcal{S}$. Let C_2 denote the collection of lines obtained by translating each line $\ell \in \mathcal{L}$ one unit in the $\ell^\perp$ direction. If $(p, \ell) \in \mathcal{S} \times \mathcal{L}$ is a point-line incidence from our original collection, then the corresponding circle-line pair will be tangent. Performing an inversion transform about a point that does not lie in any of the circles or lines, our collection $\mathcal{C} = C_1 \cup C_2$ becomes a collection of $2N$ circles that determine at least $N^{4/3}$ tangencies.*

We shall now present a bound from a recent paper of Ellenberg-Solymosi-Zahl which uses the polynomial method.[ESZ16]

Theorem 6.1.2 ([ESZ16])**.** *Given a finite collection $\mathcal{C}$ of N circles in the plane such that no three are mutually tangent at a common point, then the number of tangencies $|\tau(\mathcal{C})|$ obeys:*

$$|\tau(\mathcal{C})| \lesssim N^{3/2}.$$

It is not obvious how to apply the polynomial method in the current formulation. We will perform a lifting of our circles into algebraic curves in $\mathbb{R}^3$, transforming tangencies between circles in the plane to intersections between their lifted curves in $\mathbb{R}^3$. This transforms the problem from a tangency problem to an incidence problem which can therefore be attacked with the tools available to incidence geometry. As an additional benefit to this lifting, it reduces the required degree of polynomial needed to interpolate the incidences. In general Lemma 2.2.2 tells us that if we are to interpolate a set of M points in $\mathbb{R}^d$

by a polynomial P, then the degree of P is $O(M^{1/d})$, so increasing the dimension of the problem yields a lower degree of the polynomial required.

6.2 Lifting of circles to $\mathbb{R}^3$

We shall now discuss this lifting in detail. Let $\gamma \subset \mathbb{R}^2$ be a circle in the plane of radius r_γ centred at (x_γ, y_γ). We define the lifting transform of the circle as:

$$\beta(\gamma) = \left\{ (x, y, z) \in \mathbb{R}^3 \mid (x - x_\gamma)^2 + (y - y_\gamma)^2 = r_\gamma^2, \ z = -\frac{x - x_\gamma}{y - y_\gamma} \right\}.$$

Clearly $\beta(\gamma)$ is an algebraic curve, so now we shall examine what happens to pairs of tangent circles under this transformation. Notice that z is defined as the slope of the tangent line at the point $(x, y) \in \gamma$.

Lemma 6.2.1. *Let β be the transform defined as above. Then two circles $\gamma, \gamma' \subset \mathbb{R}^2$ are tangent if and only if $\beta(\gamma) \cap \beta(\gamma') \neq \emptyset$.*

Proof. If γ and γ' are tangent then there exists a point $(x, y) \in \gamma \cap \gamma'$ and at a point of tangency we have that the slopes of the tangent lines coincide for γ and γ'. Explicitly $-\frac{x - x'_\gamma}{y - y'_\gamma} = -\frac{x - x_\gamma}{y - y_\gamma} = z$. Hence $(x, y, z) \in \beta(\gamma) \cap \beta(\gamma')$ and thus $\beta(\gamma) \cap \beta(\gamma') \neq \emptyset$.

In the other direction, assume there exists some $(x, y, z) \in \beta(\gamma) \cap \beta(\gamma')$. Clearly $(x, y) \in \gamma \cap \gamma'$ and the slopes of the tangent lines at this point are equal, hence we conclude γ is tangent to γ'. $\qquad\square$

This one-to-one correspondence between tangencies in $\mathbb{R}^2$ and incidences in $\mathbb{R}^3$ is the key idea behind the proof. For those more algebraically inclined, what we are doing here is equivalent to looking at the tangent bundles of our circle in the projective space, hence we are preserving intersections.

In the course of the proof we will need a Bezout-type result which bounds the number of intersections between a curve and a surface with no common components.

Lemma 6.2.2 (Bezout Lemma in $\mathbb{R}^3$)**.** *Let $Z(P)$ and $Z(Q_1, Q_2)$ be the zero sets of polynomials over $\mathbb{R}[X, Y, Z]$ and suppose that P, Q_1, Q_2 have no pairwise common factors. Then we can bound the cardinality of the intersection of the zero sets by*

$$|Z(P) \cap Z(Q_1, Q_2)| \lesssim \deg P \deg Q_1 \deg Q_2.$$

To preserve the flow of this chapter, the proof of this result will be given in the appendix.

6.3 Ellenberg-Solymosi-Zahl's Proof of Theorem 6.1.2

In this proof, we will need to ensure our tangencies are sufficiently uniformly distributed among our circles. We can refine our collection such that this is the case by the following

lemma.

Lemma 6.3.1 (Uniform Refinement)**.** *Let $\mathcal{C}$ be a collection of N circles and suppose that $|\tau(\mathcal{C})| \gtrsim N^\alpha$. Then we can refine our collection to a collection $\mathcal{C}' \subset \mathcal{C}$ such that every circle in $\mathcal{C}'$ is tangent to $\gtrsim N^{\alpha-1}$ other circles in $\mathcal{C}'$, $|\tau(\mathcal{C}')| \gtrsim N^\alpha$, and $|\mathcal{C}'| \gtrsim N^{\alpha/2}$.*

Proof. We proceed by a stopping-time argument. Let $\tau(\mathcal{C})$ be the set of tangencies of the circles in $\mathcal{C}$ and let c_0 be a constant such that $|\tau(\mathcal{C})| \geq c_0 N^\alpha$. Let $\mathcal{C}_0 = \mathcal{C}$ and let c_1 be a fixed constant to be chosen later. If there exists a circle $\gamma \in \mathcal{C}_0$ such that $|\{\gamma' \mid (\gamma, \gamma') \in \tau(\mathcal{C}_0)\}| < c_1 N^{1/2}$ remove it from the collection and label the new refined collection as $\mathcal{C}_1$. From this refined collection, if there exists a circle γ such that $|\{\gamma' \mid (\gamma, \gamma') \in \tau(\mathcal{C}_1)\}| < c_1 N^{1/2}$ we remove it and label the remaining collection as $\mathcal{C}_2$. After repeating this process M times until there are no more circles γ that satisfy $|\{\gamma' \mid (\gamma, \gamma') \in \tau(\mathcal{C}_M)\}| < c_1 N^{1/2}$, at each step removing a circle that contributes only a small number of tangencies, we attain a collection $\mathcal{C}_M$. We claim that $|\tau(\mathcal{C}_M)| \gtrsim N^\alpha$, and that $|\mathcal{C}_M| \gtrsim N^{\alpha/2}$.

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,

$$\begin{aligned} |\tau(\mathcal{C}_M)| &\geq |\tau(\mathcal{C}_0)| - M c_1 N^{\alpha-1} \\ &> c_0 N^\alpha - M c_1 N^{\alpha-1} \\ &> c_0 N^\alpha - c_1 N^\alpha \\ |\tau(\mathcal{C}_M)| &> \frac{c_0}{2} N^\alpha. \qquad \text{(by choosing } c_1 = c_0/2) \end{aligned}$$

We now provide a lower bound on the cardinality of our refined set $\mathcal{C}_M$. We have the trivial inequality $|\tau(\mathcal{C}_M)| \leq |\mathcal{C}_M|^2$. Combining this with the result above, we attain $|\mathcal{C}_M| \gtrsim |N|^{\alpha/2}$. $\qquad \square$

In a similar fashion to our arguments in the Kakeya problem we will be arguing by contradiction, however here we will be arguing that if the zero set of a polynomial contains too many of a certain first type of object, it must contain many more of a second kind of object.

We can now prove the main theorem.

Proof of Theorem 6.1.2. Given an arbitrary collection of circles $\mathcal{C}$ with $\gtrsim N^{3/2}$ tangencies, Lemma 6.3.1 with $\alpha = \frac{3}{2}$ allows us to reduce to a collection Γ where each circle is tangent to $\gtrsim N^{1/2}$ other circles. 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. Let $\beta(\Gamma) = \{\beta(\gamma) : \gamma \in \Gamma\}$, where β is the lifting transform defined earlier. Recall from Lemma 6.2.1 that two circles γ_1 and γ_2 are tangent if and only if $\beta(\gamma_1) \cap \beta(\gamma_2) \neq \emptyset$.

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

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

In other words, at the intersection of $\beta(\gamma_1)$ and $\beta(\gamma_2)$ their tangent vectors span a vertical subspace of $\mathbb{R}^3$. We can establish this by examining a parameterisation of γ_1 and γ_2 in the neighbourhood of (x,y). Define $f_i(t)$, $i \in \{1,2\}$ such that $(x+t, f_i(t))$ is a parameterisation of γ_i in the neighbourhood of (x,y) for all t in a small neighbourhood of 0. In particular $f_i(0) = y$. Since $(x+t, f_i(t))$ satisfies the equation of a circle γ_i we have the relation

$$(x + t - x_{\gamma_i})^2 + (f_i(t) - y_{\gamma_i})^2 = r_{\gamma_i}^2.$$

Taking the first derivative and evaluating at $t = 0$

$$\frac{df_i}{dt}(0) = -\frac{x - x_{\gamma_i}}{y - y_{\gamma_i}}.$$

Since γ_1 is tangent to γ_2 at (x,y) the slopes of their tangent lines coincide at that point so $\frac{df_1}{dt}(0) = \frac{df_2}{dt}(0)$. Now taking the second derivative and evaluating at $t = 0$:

$$\frac{d^2 f_i}{dt^2}(0) = -\frac{(y - y_{\gamma_i})^2 + (x - x_{\gamma_i})^2}{(y - y_{\gamma_i})^3} = -\frac{r_{\gamma_i}^2}{(y - y_{\gamma_i})^3}.$$

Since γ_1 and γ_2 are distinct circles, $\frac{d^2 f_1}{dt^2}(0) \neq \frac{d^2 f_2}{dt^2}(0)$. (In the case $r_{\gamma_1} = r_{\gamma_2}$, notice that the tangency must be external and hence $\mathrm{sgn}(y - y_{\gamma_1})^3 \neq \mathrm{sgn}(y - y_{\gamma_2})^3$)

In the neighbourhood of (x,y,z), $\beta(\gamma_i)$ is parametrised by $\left(t, f_i(t), \frac{df_1}{dt}(t)\right)$ as the slope of the tangent to the circle is given by $\frac{df_1}{dt}(t)$. It follows that the tangent vector $\left(1, \frac{df_i}{dt}(0), \frac{d^2 f_i}{dt^2}(0)\right)$ generates the vertical space $T_{(x,y,z)}\beta(\gamma_i)$. Thus

$$(0,0,1) \in \mathrm{span}\left(\left(1, \frac{df_1}{dt}(0), \frac{d^2 f_1}{dt^2}(0)\right) - \left(1, \frac{df_2}{dt}(0), \frac{d^2 f_2}{dt^2}(0)\right)\right)$$
$$\subset \mathrm{span}\left(T_{(x,y,z)}\beta(\gamma_1), T_{(x,y,z)}\beta(\gamma_2)\right). \tag{6.1}$$

We will now interpolate $\sim N^{3/2}$ incidence points with a minimal polynomial whose degree we can control, and show that if this contains too many intersections it must also contain the curves. Then due to the tangent vectors spanning the z-axis at the incidence points we will be able to achieve a contradiction.

For each $\beta(\gamma_i) \in \beta(\Gamma)$ define a collection K_i as a set of $\sim N^{1/2}$ incidence points of $\beta(\gamma_i)$. Then $|\cup K_i| \lesssim N^{3/2}$. Let $P \in \mathbb{R}[x,y,z]$ be a non-zero polynomial of minimal degree that vanishes on all the incidence points in $\cup K_i$. This polynomial interpolates $\lesssim N^{3/2}$ points in $\mathbb{R}^3$, so by Lemma 2.2.2 the degree of P is $\lesssim \left(N^{3/2}\right)^{\frac{1}{3}} = N^{1/2}$.

Due to our refinement each $\gamma \in \Gamma$ is tangent to $\gtrsim N^{1/2}$ circles and each of these tangencies occurs at a distinct point by the non-degeneracy condition. Hence we have that P vanishes at $\gtrsim N^{1/2}$ points of each curve in $\beta(\Gamma)$. By Bézout's Lemma (Lemma 6.2.2) we have that P vanishes on all curves in $\beta(\Gamma)$ as

$$\deg(P)\deg(\beta(\gamma)) \lesssim \#\{P \cap \beta(\gamma)\}$$

for suitable choice of implicit constants.

By Equation 6.1, if (x, y, z) is a point where two curves from $\beta(\Gamma)$ intersect, then $\partial_z P(x, y, z) = 0$. Thus by the same Bezout argument $\partial_z P$ is also a polynomial which vanishes on all curves in $\beta(\Gamma)$.

Since P was a non-zero polynomial of minimal degree that vanishes on all points of incidence in $\beta(\Gamma)$, we must conclude $\partial_z P \equiv 0$ and hence we must have that $P(x, y, z) = Q(x, y)$ for some $Q \in \mathbb{R}[x, y]$ with $\deg Q = \deg P \lesssim N^{1/2}$. But this implies that there must be at least of the $N^{3/4}$ circles in our original collection which are contained in $Z(Q)$. This is a contradiction, as Q has degree $\sim N^{1/2}$ whereas $\cup \gamma$ has degree $\gtrsim N^{3/4}$. Thus $\beta(\Gamma)$ has $\lesssim N^{3/2}$ curve-curve incidences, so we can conclude that Γ has $\lesssim N^{3/2}$ tangencies. $\qquad \square$

6.4   A New Proof via Polynomial Partitioning for Varieties

In this section we shall present a new proof of Theorem 6.1.2. There are a few key differences between the two methods of proof. In the following proof, it is no longer required to ensure the uniform distribution of tangent points among each circle in our collection, so we will not have to use Lemma 6.3.1. Secondly, in a similar fashion to the proof of the Szemerédi-Trotter Theorem (Theorem 5.0.1) in the previous chapter we will partition $\mathbb{R}^3$ using a polynomial of controlled degree and leverage our trivial bound (Lemma 6.1.1) in each cell. Slight care will be needed to deal with intersections of curves in the zero set, which we do via a recursive argument.

We begin by introducing the main tool for this proof, an extension of the polynomial partitioning theorem (Theorem 5.3.3) to algebraic varieties instead of just points (which are 0-dimensional varieties).

Lemma 6.4.1 (Polynomial Partitioning for Algebraic Varieties)**.** *Suppose Γ is a set of k-dimensional varieties in $\mathbb{R}^n$. For any positive integer D there exists a non-zero polynomial P of degree at most D such that each connected component of $\mathbb{R}^n \backslash Z(P)$ intersects $\lesssim D^{k-n}|\Gamma|$ varieties of Γ.*

We shall not prove this here. A proof of this result can be found as Theorem 0.3 in [Gut15], the original paper of Guth presenting the result. The proof is in the same spirit as the proof Theorem 5.3.3 given in Chapter 5, however some additional difficulties present themselves and a correct proof requires some care. One should notice that the $k = 0$ case above recovers Theorem 5.3.3.

Proof of Theorem 6.1.2 by Polynomial Partitioning. Relabel $\mathcal{C}$ as Γ for convenience. Again, we perform the lifting transform β on each $\gamma \in \Gamma$. We have a collection of N 1-dimensional varieties in $\mathbb{R}^3$ upon which we use our polynomial partitioning lemma (Lemma 6.4.1) to find a polynomial P such that each cell of $\mathbb{R}^3 \backslash Z(P)$ intersects $\lesssim ND^{-2}$ varieties. $\mathbb{R}^3 \backslash Z(P)$ partitions the space into $\sim D^3$ cells. Let us label the interior of each of these cells as $\{\Omega_i \mid 0 \leq i \lesssim D^3\}$, and further label the set of varieties in Γ that intersect a given cell Ω_i as Γ_i.

(margin note: add def of variety)

(margin note: rephrase closer to 5.3.3)

We can now define the following complementary sets based on whether the variety is contained entirely in $Z(P)$:

$$C_1 = \{\beta(\gamma) \mid \beta(\gamma) \not\subset Z(P)\}$$
$$C_2 = \{\beta(\gamma) \mid \beta(\gamma) \subset Z(P)\}.$$

Notice here that $\beta(\Gamma) = C_1 \cup C_2$. Recalling the correspondence between curve-incidences and circle-tangencies, we define the following incidence sets for any subcollections C and C' of $\beta(\Gamma)$

$$I(C,C') = \{(\beta(\gamma), \beta(\gamma')) \mid \beta(\gamma) \in C', \ \beta(\gamma') \in C, \ \beta(\gamma) \cap \beta(\gamma') \neq \emptyset\}.$$

Hence we can express $|\tau(\Gamma)|$ as the sum

$$|\tau(\Gamma)| = |I(C_1, C_1)| + 2|I(C_1, C_2)| + |I(C_2, C_2)|.$$

We now proceed to bound the cardinality for each of these sets. For $I(C_1, C_1)$ will use our trivial bound (Lemma 6.1.1) and Bézout's lemma (Lemma 6.2.2). Bounding the cardinality for $I(C_1, C_2)$ is again straightforward by Bézout. The interesting case here is $I(C_2, C_2)$, where we will be forced to argue via a recursive argument.

We begin with $I(C_1, C_1)$, that is, the intersections that occur between varieties not entirely contained in the zero set. We proceed by partitioning $I(C_1, C_1)$ according to whether the incidence occurs within a cell or on $Z(P)$, explicitly

$$I(C_1, C_1) = \{(\beta(\gamma), \beta(\gamma')) \mid \beta(\gamma), \beta(\gamma') \in C_1, \ \beta(\gamma) \cap \beta(\gamma') \in \mathbb{R}^3 \backslash Z(P)\}$$
$$\cup \{(\beta(\gamma), \beta(\gamma')) \mid \beta(\gamma), \beta(\gamma') \in C_1, \ \beta(\gamma) \cap \beta(\gamma') \in Z(P)\}.$$

Hence we have

$$|I(C_1, C_1)| = \sum_{\beta(\gamma), \beta(\gamma') \in C_1} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in \mathbb{R}^3 \backslash Z(P)] + \sum_{\beta(\gamma), \beta(\gamma') \in C_1} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in Z(P)]$$
$$= \sum_{\beta(\gamma), \beta(\gamma') \in C_1} \sum_i \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in \Omega_i] + \sum_{\beta(\gamma), \beta(\gamma') \in C_1} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in Z(P)]$$
$$= \sum_i \sum_{\beta(\gamma), \beta(\gamma') \in \Gamma_i} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in \Omega_i] + \sum_{\beta(\gamma), \beta(\gamma') \in C_1} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in Z(P)].$$

Using our trivial bound (Lemma 6.1.1) and the fact that there are $\lesssim ND^{-2}$ varieties intersecting a given cell we attain

$$\lesssim \sum_i \left(\frac{N}{D^2}\right)^2 + \sum_{\beta(\gamma), \beta(\gamma') \in C_1} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in Z(P)]$$
$$\sim D^3 N^2 D^{-4} + \sum_{\beta(\gamma) \in C_1} \sum_{\beta(\gamma') \in C_1} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in Z(P)].$$

For each fixed $\beta(\gamma) \in C_1$ we see by Bezout's Lemma (Lemma 6.2.2) that $\beta(\gamma)$ can intersect $Z(P)$ in at most $\lesssim D$ points. Since all the intersections in the latter sum are of this type, we have that each $\beta(\gamma)$ contributes at most $\lesssim D$ to the sum, and summing over all possible $\beta(\gamma)'s \in C_1$ we obtain

$$\lesssim N^2 D^{-1} + \sum_{\beta(\gamma) \in C_1} D$$
$$\sim N^2 D^{-1} + ND.$$

The argument for $I(C_1, C_2)$ is similar to the one above, however there are now no intersections happening inside the cells by the definition of C_2.

$$|I(C_1, C_2)| = \sum_{\beta(\gamma) \in C_1} \sum_{\beta(\gamma') \in C_2} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \in Z(P)]$$

Again thanks to Bezout's Lemma (Lemma 6.2.2) we have that the latter sum is $\lesssim D$. Hence

$$|I(C_1, C_2)| \lesssim \sum_{\beta(\gamma) \in C_1} D \leq ND.$$

Finally we need to handle the incidences between curves contained entirely in the zero-set, $I(C_2, C_2)$.

$$|I(C_2, C_2)| = \sum_{\beta(\gamma), \beta(\gamma') \in C_2} \mathbb{1}[\beta(\gamma) \cap \beta(\gamma') \neq \emptyset].$$

Suppose P was the minimal degree polynomial that partitioned the space as per Lemma 6.4.1. Then we can write C_2 as the union of disjoint sets:

$$C_2 = \{\beta(\gamma) \subset Z(\partial_z P)\} \cup \{\beta(\gamma) \subset \mathbb{R}^3 \backslash Z(\partial_z P)\}$$

If all the curves are in $\{\beta(\gamma) \subset Z(\partial_z P)\}$, then we use the exact same technique as in Ellenberg-Solymosi-Zahl's Proof. Since P was a minimal degree polynomial that partitioned the space, and $\partial_z P$ also partitioned space, then we must have that P does not depend on z, or in other words $P(X, Y, Z) = Q(X, Y)$. Since $Z(Q)$ is of degree D, it can contain up to D circles in the plane. Using trivial bound we can control the size of this contribution by $\lesssim D^2$.

In the other case, say there are some number K_1 curves in $\{\beta(\gamma) \subset \mathbb{R}^3 \backslash Z(\partial_z P)\}$, each of which can intersect $Z(\partial_z P)$ at most D times. We recursively iterate this process now, examining now the set:

$$\{\beta(\gamma) \subset Z(\partial_z P)\} = \{\beta(\gamma) \subset Z(\partial_z^2 P)\} \cup \{\beta(\gamma) \subset \mathbb{R}^3 \backslash Z(\partial_z^2 P)\}$$

Again, if all the curves are in $Z(\partial_z^2 P)$ the process stops and we proceed by the argument above. In the other case, $\mathbb{R}^3 \backslash Z(\partial_z^2 P)$ contains k_2 curves which intersect $Z(\partial_z^2 P)$ at most D times each. We can iterate this process at most D times, as after the D-th derivative we are in the first case. The contributions from the second case become:

$$\lesssim \sum_{i=0}^{D} k_i D = D \sum_{i=0}^{D} k_i = DN$$

$$|I(C_2, C_2)| \lesssim D^2 + ND$$

Adding together our bounds we achieve:

$$|I(C_1, C_1)| + 2|I(C_1, C_2)| + |I(C_2, C_2)| \lesssim N^2 D^{-1} + ND + ND + ND + D^2$$
$$\sim N^2 D^{-1} + ND + D^2.$$

We now optimise D by setting $N^2 D^{-1} \sim ND$ which gives $D \sim N^{1/2}$ and hence our bounds become:

$$|I(C_1, C_1)| + |I(C_1, C_2)| + |I(C_2, C_2)| \lesssim N^2 N^{-1/2} + NN^{1/2} + (N^{1/2})^2 \sim N^{3/2}.$$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \square$

Remark. *Since polynomial partitioning exploits the topology of $\mathbb{R}^n$ in an essential manner, it would have been reasonable to expect an improvement over the exponent 3/2 via the argument above. Alas, this was not the case.*

6.5   Considerations for the case of Sphere Tangencies in $\mathbb{R}^3$

[The Case of Sphere Tangencies in $\mathbb{R}^3$] Considering the analogous problem in $\mathbb{R}^3$, two new difficulties emerge. Firstly, our current non-degeneracy condition is not sufficient as we have new degenerate cases to consider where the trivial bound of $O(N^2)$ is achieved.

capitalisation?

Example 6.3 (Degenerate case in $\mathbb{R}^3$).

halo example

Due to cases like these, a new condition is required. A natural choice given this example would seem to be restricting our collections to those which do not contain too many tangencies along any one low-degree algebraic curve on the surface of a sphere.

Secondly, our simple Bézout lemma is no longer enough. An analogous lifting of a sphere $\gamma \subset \mathbb{R}^3$ is given by:

$$\beta(\gamma) = \left\{ (x, y, z, v, w) \in \mathbb{R}^5 \;\middle|\; \begin{array}{l} (x - x_\gamma)^2 + (y - y_\gamma)^2 + (z - z_\gamma)^2 = r_\gamma^2, \\ v = -\frac{x - x_\gamma}{z - z_\gamma}, \; w = -\frac{y - y_\gamma}{z - z_\gamma} \end{array} \right\}.$$

$\beta(\gamma)$ is a two-dimensional algebraic surface in $\mathbb{R}^5$. An interpolating polynomial's zero set $Z(P)$ such as the one used in Ellenberg-Solymosi-Zahl's proof would be a 4-dimensional surface in $\mathbb{R}^5$. These two surfaces could intersect along a 1-dimensional variety (i.e. at infinitely many points), hence we can no longer argue that $\beta(\gamma) \subset Z(P)$ due to $Z(P)$ containing too many points of $\beta(\gamma)$.

The best example of a lower bound for such tangencies is produced in a similar fashion to the circles case (Example 6.2). In place of the Szemerédi-Trotter theorem we appeal to a corollary of a theorem of Rudnev which bounds the number of point-plane incidences in $\mathbb{R}^3$:[Rud14]

Theorem 6.5.1. *Let $\mathcal{S}$ be a finite set of points in $\mathbb{R}^3$ and Π a finite set of non-collinear planes in $\mathbb{R}^3$. Assume further that $|\mathcal{S}| > |\Pi|$. Then the incidence set $I(\mathcal{S}, \Pi)$ obeys*

$$|I(\mathcal{S}, \Pi)| \lesssim |\mathcal{S}||\Pi|^{1/2}.$$

We now construct our lower bound utilising geometric inversion in $\mathbb{R}^3$ analogously to Example 6.2.

Example 6.4. *Let $\mathcal{S}$, Π be collections of N points and N non-collinear planes respectively such that the Theorem 6.5.1 is asymptotically tight. In particular, they determine $\sim N^{7/5}$ point-plane incidences. Let C_1 denote the collection of unit spheres centred at the points of $\mathcal{S}$. Let C_2 denote the collection of planes obtained by translating each plane $\pi \in \Pi$ one unit in the $\pi^\perp$ direction. If $(p, \pi) \in \mathcal{S} \times \Pi$ is a point-plane incidence from our original collection, then the corresponding sphere-plane pair will be tangent. Performing an inversion transform about a point that does not lie in any of the circles or planes, our collection $\mathcal{C} = C_1 \cup C_2$ becomes a collection of $2N$ spheres that determine $N^{3/2}$ tangencies.*

In [ESZ16], the authors conjectured a bound for higher dimensional spheres:

Conjecture 4. Let $\mathcal{C}$ be a collection of $(d-1)$-spheres in $\mathbb{R}^d$. Then the number of distinct points of tangencies is $\lesssim |\mathcal{C}|^{\frac{2d-1}{d}}$.

This is a somewhat weak conjecture, as the evidence to form it is simply the natural extension of the β-lifting technique into higher dimensions. As such, there is no evidence to suggest that it should be tight.

[margin note: change this to be correct]

[margin note: is this tight? EQ 2 Rudnev suggests N^7/5 is tight in R3]

[margin note: colon here?]

[margin note: rewrite sentence]

References

[Alo99] Noga Alon. Combinatorial nullstellensatz. *Combinatorics, Probability and Computing*, 8(1-2):7–29, 1999.

[Bou91] Jean Bourga'in. Besicovitch type maximal operators and applications to fourier analysis. *Geometric & Functional Analysis GAFA*, 1(2):147–187, 1991.

[CEG+90] Bernard Chazelle, Herbert Edelsbrunner, Leonidas J Guibas, Richard Pollack, Raimund Seidel, Micha Sharir, and Jack Snoeyink. Counting and cutting cycles of lines and rods in space. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 242–251. IEEE, 1990.

[Dav71] 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.

[Dvi08] Zeev Dvir. On the size of kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22(4):1093–1097, Jun 2008.

[ESZ16] Jordan S. Ellenberg, Jozsef Solymosi, and Joshua Zahl. New bounds on curve tangencies and orthogonalities, 2016.

[FS05] Sharona Feldman and Micha Sharir. An improved bound for joints in arrangements of lines in space. *Discrete & Computational Geometry*, 33(2):307–320, 2005.

[FT81] Robert M Freund and Michael J Todd. A constructive proof of tucker's combinatorial lemma. *Journal of Combinatorial Theory, Series A*, 30(3):321–325, 1981.

[GK08] Larry Guth and Nets Hawk Katz. Algebraic methods in discrete analogs of the kakeya problem, 2008.

[Gow20] Timothy Gowers. Topics in combinatorics - cambridge tripos lecture notes, 2020.

[Gut15] Larry Guth. Polynomial partitioning for a set of varieties. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 159, pages 459–469. Cambridge University Press, 2015.

[Gut16] L. Guth. *Polynomial Methods in Combinatorics.* University Lecture Series. American Mathematical Society, 2016.

[KSS09] Haim Kaplan, Micha Sharir, and Eugenii Shustin. On lines and joints, 2009.

[MBZ⁺03] Jiří Matoušek, Anders Björner, Günter M Ziegler, et al. *Using the Borsuk-Ulam theorem: lectures on topological methods in combinatorics and geometry.* Springer, 2003.

[mic10] *The American Mathematical Monthly*, 117(9):821–823, Nov 2010.

[Pal20] J Pal. über ein elementares variationsproblem danske videnskab. selskab. *Math. Fys. Meddel*, 3(2):10–35, 1920.

[Qui09] René Quilodrán. The joints problem in rn, 2009.

[Rud14] Misha Rudnev. On the number of incidences between points and planes in three dimensions, 2014.

[ST83] Endre Szemerédi and William T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3(3):381–392, 1983.

[Szé97] László A Székely. Crossing numbers and hard erdős problems in discrete geometry. *Combinatorics, Probability and Computing*, 6(3):353–358, 1997.

[Wol95] Thomas Wolff. An improved bound for kakeya type maximal functions. *Revista Matemática Iberoamericana*, 11(3):651–674, 1995.

[Wol99] Thomas Wolff. Recent work connected with the kakeya problem. *Prospects in mathematics (Princeton, NJ, 1996)*, 2:129–162, 1999.

Appendix A

Proof of Bézout's Lemma

Lemma A.0.1 (Bezout Lemma for Curves in $\mathbb{R}^3$)**.** *Let $Z(P)$ and $Z(Q_1, Q_2)$ be the zero sets of polynomials over $\mathbb{R}[X, Y, Z]$ and that P, Q_1, Q_2 have no common factors. Then we can bound their intersection:*

$$|Z(P) \cap Z(Q_1, Q_2)| \lesssim \deg P \deg Q_1 \deg Q_2.$$

Proof.

$$
\begin{array}{ccccccc}
 & & \frac{F_{D-\deg Q_2}[X,Y,Z]}{\langle Q_1 \rangle_{D-\deg Q_2}} & & \frac{F_{D-\deg P}[X,Y,Z]}{\langle Q_1,Q_2 \rangle_{D-\deg P}} & & \\
 & & \downarrow{\scriptstyle \beta'} & & \downarrow{\scriptstyle \gamma'} & & \\
F_D[X,Y,Z] & \xrightarrow{\ \alpha\ } & \frac{F_D[X,Y,Z]}{\langle Q_1 \rangle_D} & \xrightarrow{\ \beta\ } & \frac{F_D[X,Y,Z]}{\langle Q_1,Q_2 \rangle_D} & \xrightarrow{\ \gamma\ } & \frac{F_D[X,Y,Z]}{\langle Q_1,Q_2,P \rangle_D}
\end{array}
$$

$\square$

Appendix B

Proof of Borsuk-Ulam Theorem

Theorem B.0.1 (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.*

We present here a combinational proof due to Matousek.[MBZ$^+$03]

Let $\|x\|_1$ be the L_1 norm of x. Define B^n as the unit ball with respect to the L_1 norm, that is: $B^n = \{x \in \mathbb{R}^n \mid \|x\|_1 \leq 1\}$.

A simplex is the convex hull of an affinely independent set in $\mathbb{R}^n$. A family of simplexes $\Delta = \{\sigma_1, \sigma_2, \ldots, \sigma_m\}$ is called a **simplicial complex** if the following conditions hold:

1. Each non-empty face of any simplex $\sigma \in \Delta$ is also a simplex of Δ.

2. $\sigma_1, \sigma_2 \in \Delta \implies \sigma_1 \cap \sigma_2$ is a face of both σ_1 and σ_2.

A simplicial complex T is a **special triangulation** of B^n if all the following hold:

1. $\|T\| = B^n$

2. T is a refinement of the triangulation of B^n given by cutting the coordinate hyperplanes. (In other words, no simplex of T spans over a boundary of an orthant)

3. T is symmetrical around the origin.

To prove the Borsuk-Ulam theorem, we first prove the Tucker Lemma. This lemma can be thought of as the combinational analogue to the Borsuk-Ulam Theorem. We present here a constructive proof first published by Freund.[FT81]

Lemma B.0.2 (Tucker Lemma). *Let the vertices of an arbitrary special triangulation T be denoted by labels $lab(u) \in \{\pm 1, \pm 2, \ldots, \pm n\}$ in such a way that the vertices $u \in \partial B^n$ on the boundary satisfies $lab(-u) = -lab(u)$. Then there exists a 1-simplex (an edge) in T which is complimentary, that is its two vertices x, x' satisfy $lab(-x) = -lab(x')$.*

Proof. Let T be a special triangulation of B^n. For a simplex $\sigma \in T$ we set $\text{sgn}\,\sigma = (\text{sgn}\,x_1, \text{sgn}\,x_2, \ldots, \text{sgn}\,x_n)$, where x is an arbitrary point of the interior of σ. This definition is well-defined, as special triangulations refines the orthants of $\mathbb{R}^n$ and thus the signs

41

of each coordinate do not change in the interior of σ. We say σ is **completely labelled** if the following holds for each $0 \le i \le n$: if $\mathrm{sgn}\,(\sigma)_i = 1$, then at least one of the vertices of σ is labelled by the number i, and if if $\mathrm{sgn}\,(\sigma)_i = -1$, then at least one of the vertices of σ is labelled by the number $-i$.

We now define a graph G whose vertices are all completely labelled simplexes, and in which two vertices $\sigma, \sigma' \in T$ are connected by an edge if:

(a) $\sigma, \sigma' \in \partial B^n = S^{n-1}$ and $\sigma = -\sigma'$, or

(b) σ is a k-simplex and σ' is its $(k-1)$-face whose vertices are already labelled by all numbers required for a complete labelling of σ.

The degree of a completely labelled simplex is the number of completely labelled simplexes adjacent to it in G.

The simplex $\{0\}$ has degree 1 in G, since it is connected to exactly the edge of the triangulation which is completely labelled by $\mathrm{lab}(0)$. We now prove that any other vertex σ of G has degree 2 except when σ contains a complimentary edge. Since a graph cannot contain only one vertex of odd degree, the lemma will be established.

Let $\mathrm{sgn}\,\sigma$ have k non-zero components, then the dimension of σ is either k or $k-1$.

Suppose first that σ is a $(k-1)$-simplex. If σ does not lie in S^{n-1}, it is the face of precisely two k-simplices, both completely labelled since σ is. If σ lies in S^{n-1}, it is the face of one completely labelled k-simplex, and it has the other neighbour $-\sigma$ according to condition (a).

If σ is a k-simplex, it has k obligatory labels and one extra label. This label either:

- repeats one of the k obligatory labels in which case σ is adjacent to two of its faces, or

- it is opposite to one of the obligatory labels in which case we have a complimentary edge, or

- it is yet another number not in the k obligatory labels, in which case the neighbours of σ are its completely labelled face and one adjacent simplex of larger dimension determined by the extra label.

In both cases without a complimentary edge we have two neighbours. $\qquad\square$

Proof of Borsuk-Ulam from Tucker Lemma. Let $f : \mathbb{S}^n \to \mathbb{R}^n$ be a continuous mapping, and let B^n be the unit ball in the "equator" hyperplane of $\mathbb{S}^n$. We define $g : B^n \to \mathbb{R}^n$ by setting $g(x) = f(y) - f(-y)$, where y is the point of the upper hemisphere of $\mathbb{S}^n$ whose vertical projection on B^n is x. The map g is obviously antipodal on $\partial B^n = \mathbb{S}^{n-1}$. For contradiction let us assume that $g(x) \ne 0$ everywhere. From the compactness of the ball we have the existence of an $\varepsilon > 0$ such that $\|g(x)\|_1 \ge \varepsilon$ for all x. Further, a continuous fraction on a compact set is uniformly continuous, and thus there exists a $\delta > 0$ such that if $\|x - x'\|_1 \le \delta$ then $\|g(x) - g(x')\|_1 < \varepsilon/n$.

Let us choose a special triangulation T such that the diameter of each of its simplexes is at most δ. We define a labelling of the vertices of T as follows: $|\text{lab}(x)| = i$ if $|g_i(x)| = \max\{|g_1(x)|, \ldots, |g_n(x)|\}$ and $\text{sgn} \, \text{lab}(x) = \text{sgn} \, g_i(x)$ (if the maximum is attained for more than one index, we take the first such index). From the Tucker Lemma we know there exists a complimentary edge xx'. Let $\text{lab}(x) = -\text{lab}(x') = i$, then $g(x)_i \geq \varepsilon/n$ and $g(x')_i \leq -\varepsilon/n$. Hence $\|g(x) - g(x')\|_1 \geq 2\varepsilon/n$, a contradiction. Therefore there exists a zero x of the function g. $\qquad \square$