Boston College

Senior Thesis

The Polynomial Method in Combinatorics

Author:
Robert Laudone

Supervisor:
Dr. Joshua Greene

April 28, 2015

Acknowledgments:

I would first like to thank my parents Gina and Bob Laudone, without their constant support and love I am not sure where I would be. Thanks to my sisters Rachel and Kate who always provide an important outside perspective and keep me grounded.

I am deeply indebted to my advisor Joshua Greene, whose advice and encouragement have guided me for the past three years. I count myself extremely lucky to have taken his introduction to abstract mathematics course as a sophomore. He continues to be a massive source of motivation as I pursue a career in mathematics.

Finally, a big thanks to my roommate Cameron Givens who in the past year, and really the past four years, has sat through hours of my mathematical babbling and worked with me through some long nights in the conference room.

Contents

1 Introduction

The polynomial method is an emerging field in extremal combinatorics. It borrows much of its ideology from algebraic geometry, but also touches upon topology, number theory and algebra. In combinatorics, we often want to study a certain set of points P or lines L over a field F. We can inquire about the minimal number of distinct distances among a point set P, whether or not a subset of the points of P can form an N-gon, the number of incidences between the points and lines, and more. Recently, mathematicians realized that they could extract important combinatorial properties about specific sets P or L by examining the set of polynomials that vanish on these sets.

In this paper we explore the reach of this new method. Up to this point, only Terence Tao [22] has created an expository paper exploring parts of the Polynomial Method. Our goal is to take this a step further: introducing the Polynomial Method through reconstructing and explaining proofs with very little assumed mathematical knowledge. In so doing, we provide greater detail concerning the historical development of the polynomial method and hopefully allow the general reader to glean the essential tools this method offers. Throughout the process of the proofs, we introduce and explain all material as it becomes pertinent and provide many examples as an attempt to make the material more understandable. We ultimately desire to unite the heretofore disparate pieces of the polynomial method for a more general audience.

We begin our exploration of the Polynomial Method by exploring Dvir's proof of the finite field Kakeya Conjecture [3]. We choose this proof as a starting point for two reasons. Our first reason is chronological as Dvir essentially pioneered the polynomial method and his methods of proof in the finite field Kakeya conjecture formed the foundation for all future proofs. Secondly, finite fields provide an easier introduction to the material. As we will see, much of the proofs in the finite field case can be reduced to simple linear algebra. This allows us to delve more deeply into the ideology behind the polynomial method rather than getting immediately bogged down in complex proofs.

We then jump into one of the first applications of Dvir's new ideology outside of the Kakeya Conjecture: a new proof of the Szemerédi and Trotter Theorem, bounding the number of incidences between points and lines in the plane. Within this context we take our first steps into an infinite field, $\mathbb{R}^2$. Along the way we discuss projective geometry, topology and the fundamental theorem of algebra. With this in hand, we explore the implications of generalizing the Szemerédi and Trotter theorem to algebraic curves instead of lines. We explore this idea through a proof of a weaker version of Pach and Sharir's Theorem [17]. We notice that as we transition from lines to algebraic curves we have to replace the fundamental theorem of algebra with Bézout's Theorem. To better understand the role Bézout's Theorem plays in the polynomial method we explore a proof of Welzl's Theorem [24] concerning spanning trees. We will see Bézout's Theorem play a critical role in almost all of the remaining proofs.

With an understanding of the polynomial method over finite fields, the projective plane and $\mathbb{R}^2$, we make the transition to $\mathbb{R}^3$ by exploring the Joints Problem. This is another problem concerned with bounding incidences, but in this case we want to bound the number of possible points where a given set of lines could meet in three or more places. Guth and Katz provide the first proof using a degree reduction argument [6]. We walk through this proof and the ideology behind degree reduction: finding a smaller degree polynomial that vanishes over a given point set where many of the points are collinear. We then examine a simpler proof provided by Quilodrán [18] that involves finding a line without many points on it, removing this line and continuing inductively. We provide both proofs to show the different techniques and their relative merits within the polynomial method and to introduce the idea of degree reduction which will play an important role in the proof of the Distinct Distances Problem.

At this point we have explored the majority of the polynomial method, and are ready to tackle the Distinct Distances Problem. This simple question–"What is the minimum number of distinct distances determined by N points in the plane?"–baffled mathematicians since Erdős posed it in 1946 [5]. In 2013 Guth and Katz [7] finally provided an almost optimal answer. In the exploration of their proof we provide explanation, missing detail and trace the methods back to earlier sections in the paper, revealing their roots.

2 The Finite Field Nikodym Conjecture

In this section we will explore a simple example of using the Polynomial method to provide a lower bound on the size of certain point sets. We follow Dvir's method [3]. To derive a lower bound, we prove that a set of too small a size cannot possibly have a polynomial we find with small degree that vanishes on all of its points. We know that given a set of points, we can find a polynomial that vanishes on all of those points with small degree in relation to the size of the point set. We can thus use this relation to find a lower bound on the size of the point set.

We will make this more explicit below, but first we must state the Nikodym Conjecture. The original Nikodym conjecture is still an open problem, and the finite field version we are about to discuss provides some important insights into the general case. Considering the polynomial method over finite fields also provides an easier introduction to some of the basic techniques. We will first present some important definitions that are necessary for the statement of our theorem.

Definition 2.1. Let F be a field with q elements. A *Nikodym Set* is a set $N \subset F^n$ such that $\forall x \in F^n$, there exists a line $L(x)$ containing x so that $|L(x) \cap N| \geq q/2$.

Example 2.1. Trivially we can see that F^n is a Nikodym set. As for any point in F^n we can take any line. The motivating question is, how small can we possible make our Nikodym set? The following theorem provides an answer to that question in the finite field case.

Theorem 2.1 (Nikodym Problem)**.** *Any (generalized) Nikodym set in F^n contains at least $c_n(q^n)$ elements. Where q is the order of the finite field F.*

In other words, the Nikodym set must contain a definite fraction of the points in F^n.

2.1 Polynomial Method Adaptations for Finite Fields

The following lemmas are finite field adaptations of lemmas we will see and prove for general fields in the following sections. Restricting our field to only finitely many elements allows us to prove slightly more powerful results which ultimately makes the finite field versions of problems much easier to prove. In the case of finite fields we can often reduce what would be a complicated proof to a fairly simple linear algebra problem, as we will see. The first result concerns the vector space of polynomials of bounded degree.

Lemma 2.1. *The vector space $V(d)$ of polynomials of degree $\leq d$ with n variables defined over F^n has dimension $\binom{d+n}{n} \geq d^n/n!$.*

Proof: It is easily verified that this is in fact a vector space. We can see that $x_1^{d_1} \cdots x_n^{d_n}$ where $d_1 + \cdots + d_n \leq d$ is a basis for this vector space. We now need to count how the number of such monomials. By a stars and bars argument we are really looking to partition the number d into $n+1$ subsets in every possible way. Where the first n partitions designate the degrees of each x_i and the last is not included which accounts for the possibility that the degree is less than d. This is the same as choosing n spots from $d+n$ spaces uniquely. Thus the number of such monomials is exactly $\binom{d+n}{n} \geq d^n/n!$. $\square$

Example 2.2. For example, say we want all bivariate polynomials of degree ≤ 5. One basis element is x^5 which corresponds to $*****--$, another is $x^3y = ***-*-*$.

Now we will use this and some basic linear algebra to show that we can find a polynomial of small degree that vanishes over a finite point set $S \subset F^n$.

Lemma 2.2. *If $S \subset F^n$ is finite, there exists a nonzero polynomial that vanishes on S with degree $\leq n|S|^{1/n}$.*

Proof: Let $\{p_1, \ldots, p_s\} = S$ and let $V(d)$ be the vector space of polynomials in n variables with degree $\leq d$ defined over F^n. We know that $V(d)$ has dimension $\binom{d+n}{n}$ by Lemma 2.1. Consider the evaluation map $E : V(d) \to F^s$ given by

$$E(f) = (f(p_1), \ldots, f(p_s))$$

It is easy to verify that this is a linear map. We can thus see that there exists a nonzero polynomial $f \in V(d)$ that vanishes on all of S if and only if E has a nontrivial kernel. By a basic fact from linear algebra we know that this must occur if $\dim(V(d)) > s$ where s is the dimension of the range of E. This follows from the fact that a trivial kernel of a linear map implies injectivity. Thus if $\dim(V(d))$ is larger than s we cannot possibly have injectivity and so there must be a nontrivial polynomial that vanishes on all of S. So we need $\binom{d+n}{n} > |S|$. This will occur if $\binom{d+n}{n} \geq D^n/n > |S|$. Thus we have $d \geq n|S|^{1/n}$ and so we can choose $d = n|S|^{1/n}$. As a result of our approximations we could possibly find d lower than this, but this proves the result. $\square$

Now that we can create a polynomial of relatively small degree that vanishes on our finite point set, we want to investigate some limitations on the zero set of polynomials. We thus present the vanishing lemma for finite fields. This lemma and its general field analogue will be an essential tool in almost every proof we investigate throughout this paper.

Lemma 2.3 (Vanishing Lemma). *If ℓ is a line in F^n and $f \in F[x_1, \ldots, x_n]$ of degree at most d. Then either f vanishes on ℓ, or $|\ell \cap Z(f)| \leq D$. In other words, the polynomial f vanishes on less than or equal to d points of a line ℓ, or it vanishes on the entire line.*

Proof: We can write ℓ in parametric form as $\ell = \{(u_1 t + v_1, \ldots, u_n t + v_n) \mid t \in F\}$. Now we will define a single variable polynomial in t using our bivariate polynomial f. Let $g(t) = f(u_1 t + v_1, \ldots, u_n t + v_n)$. As f has degree less than or equal to d, so does g. Thus by the Fundamental Theorem of Algebra, g has at most d zeroes if it is not uniformly zero. So $g = 0$ uniformly, or it vanishes on $\leq D$ values of t. In terms of our original polynomial f, this implies that $f = 0$ uniformly on the line ℓ, or that it vanishes on $\leq D$ points of the line. $\square$

We now prove another important result concerning how large the degree of our polynomial must be in order for it to vanish on the entire space F^n. This is a result without a true analogue in the case of general fields. It allows us to derive the lower bound we seek as it forces a polynomial to have a minimum degree to vanish on all the points in the vector space F^n.

Lemma 2.4. *A polynomial $f \in F[x_1, \ldots, x_n]$ of degree $d < q$ where q is the cardinality of F cannot vanish at every point of F^n unless each coefficient of f is zero.*

Proof: We will proceed by induction on n the dimension of the vector space F^n. In the case that $n = 1$ this is trivially true as a polynomial with degree less than q cannot vanish on q points. Now assume the result is true for f defined over F^{n-1}, and consider any polynomial $f \in F[x_1, \ldots, x_n]$. We can write $f = \sum_{i=1}^{d} f_i(x_1, \ldots, x_{n-1}) x_n^d$. We are grouping all of the x_n terms based on degree and considering f as a single variable polynomial over x_n, with coefficients in $x_1, \ldots, x_{n-1}$. We know that for each choice of $x_1, \ldots, x_{n-1}$ that $f(x_1, \ldots, x_n) = 0$ for all $x_n \in F$. Since $d < q$, we are now back in the case where $n = 1$, and thus f when defined this way must have zero coefficients. This tells us that $f_i(x_1, \ldots, x_{n-1}) = 0$ for each choice of i, but not necessarily that the coefficients of these polynomials are all zero. By our induction hypothesis however each f_i is a polynomial defined over F^{n-1} and therefore must have zero coefficients. But then all of the coefficients of f vanish. Thus f is the zero polynomial. $\square$

2.2 Proof of the Nikodym Conjecture

We now have a polynomial of degree $\leq n|S|^{1/n}$ that vanishes over any finite point set $S \subset F^n$. This in conjunction with the other lemmas will allow us to prove the finite field Nikodym conjecture.

Proof: Let $V(d)$ be as we have defined it above. We know we can find a polynomial f that vanishes on $N \subset F^n$ with degree $\leq n|N|^{1/n}$ by Lemma 2.4. If this degree is $< q/2$ where q is the cardinality of F we can see that f must vanish at every point $x \in F^n$. As we know that f vanishes on N, this implies that for every point $x \in F^n$ f vanishes on $q/2$ points of a line passing through x, by Lemma 2.3 f vanishes on that line and therefore on x. However, by Lemma 2.4 a polynomial of degree $\leq q/2$ cannot vanish at every point of

F^n unless it vanishes identically. Thus the degree of f is at least $q/2$. As we know the degree of our polynomial is bounded above by $c_n|N|^{1/n}$ we have that $n|N|^{1/n} \geq q/2$, which implies that $|N| \geq (\frac{1}{2n})^n q^n$. Choosing a suitable constant $C_n = (\frac{1}{2n})^n$ we have $|N| \geq C_n q^n$ as desired. □

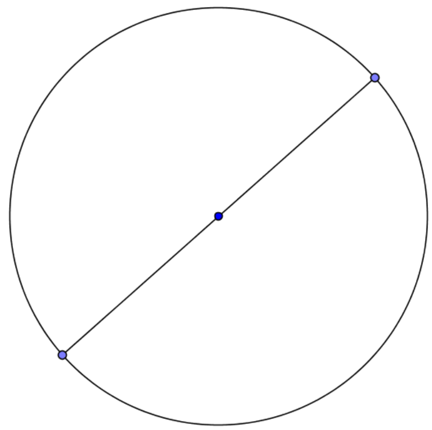
3 The Kakeya Conjecture

In this section we will explore the open Kakeya Conjecture and its finite field analog, proved recently by Zeev Dvir utilizing the polynomial method. The tension between the finite field analog and the actual conjecture reveals the possible limitations of the Polynomial Method in general Euclidean Geometry. This results from the polynomial method's general dependence on the algebraic nature of the finite field in which we work. We will explain this in more detail soon, but the general idea is that the polynomial method struggles to generalize to results concerning infinite sets and fields as it often explores the algebraic properties of finite fields and sets. Exploring the polynomial method's general reliance on the topology and algebraic structure of the field in which we work is an important consideration and will be a theme throughout this paper. However, as we will see, the finite field analog can lend significant support to understanding and possibly proving the general Kakeya conjecture. We will first present the origin of the Kakeya conjecture, known as the Kakeya needle problem posed in 1917.

Problem 3.1 (Kakeya Needle Problem)**.** *What is the least area in the plane required to continuously rotate a needle of unit length and zero thickness three hundred and sixty degrees?*

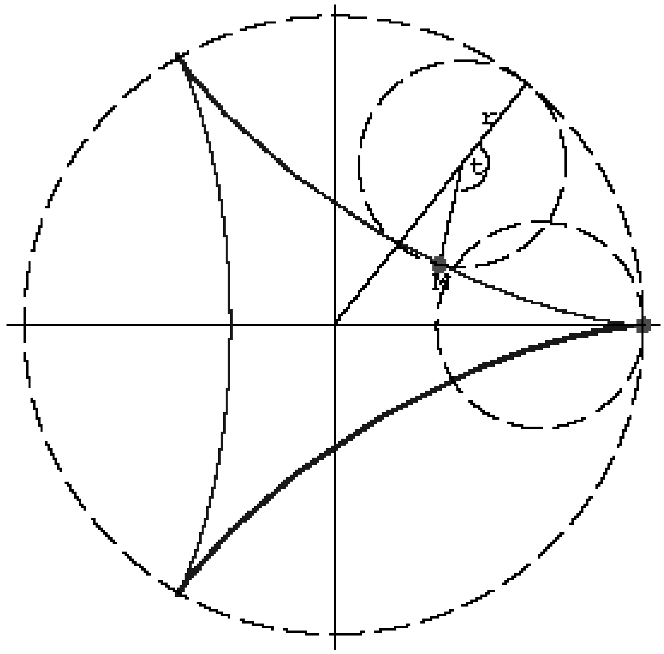
To illustrate this idea and gain some intuition, we present a couple of examples.

Example 3.1. Obvious examples of regions that would work are the unit circle, with area $\pi/4$. Given any unit line segment, we know it must have endpoints on opposite sides of the circle. We can perform an obvious rotation by spinning the line around the center of the circle. This can be seen below



We take this unit line and rotate it 360 degrees about the center of the circle. This, however, is not even close to the least amount of area required.

Example 3.2. A less obvious example is a deltoid, or Steiner Curve. Given any unit line segment, it must have endpoints on opposite edges of the deltoid. An intuitive way to picture the rotation is to return to how a deltoid is defined. We can define the deltoid by the rotation of the line. We create a circle with diameter equal to half the length of the needle. So in this case we create a circle of diameter 1/2. We then start with a tangent segment of unit length whose midpoint is the tangent point of the circle. We begin to continuously move this segment along the circle at its midpoint, continuously rotating the segment so that when the midpoint has traced out the circle the line is in its starting position. The deltoid is defined by the shape traced out by the two ends of the line segment. We can see this illustrated below



This illustrates how a deltoid is constructed, the deltoid is the solid, slightly bent triangle.

Soichi Kakeya posed this problem in 1917. Eleven years later, Besicovitch shows that one could in fact rotate a unit needle using an arbitrarily small amount of positive area. In other words an ϵ of area where $\epsilon > 0$ is arbitrarily small. This is not remotely intuitive, and he proved it utilizing the two facts below which ultimately gave birth to the Kakeya Conjecture. The first fairly intuitive fact is that we can translate a given needle using an arbitrarily small amount of area. The idea being that we move the needle an arbitrary distance away and slowly rotate it. We then move the needle in a straight line back so that it has been moved over, and we shift it back. The second fact required the definition of a Kakeya Set:

Definition 3.1. A *Kakeya set* in $\mathbb{R}^2$ is any set that contains a unit line segment in each direction.

A circle would be another example of a Kakeya set, as would the deltoid. Any set that satisfies the Kakeya needle problem will necessarily be a Kakeya set as we can rotate the unit line segment 360 degrees. So we can find a unit line segment in each direction. Besicovitch's shocking theorem states:

Theorem 3.1 (Besicovitch, 1919)**.** *There exists Kakeya sets in $\mathbb{R}^2$ of arbitrarily small lebesgue measure.*

We will not go through the proof of this theorem, as it requires a deep level of analysis beyond the scope of our current investigations. It is true that we can construct such sets in $\mathbb{R}^2$ with Lebesgue measure 0. These Kakeya sets with Lebesgue measure 0 are called *Besicovitch sets*. Utilizing Besicovitch sets and the intuitive fact 1, Besicovitch was able to prove that we could find sets that satisfy the Kakeya Needle Problem with arbitrarily small area. He found Kakeya sets that contained the small rotations described above. Thus the answer to the Kakeya Needle Problem is 0.

We discussed that every set satisfying the Kakeya needle problem is a Kakeya set, but the converse is not the case. This is illustrated by an important question: Can we take $\epsilon = 0$? In other words, is there a set that satisfies that Kakeya Needle Problem with area equal to 0. Intuitively, we can posit no by the construction above, as the translations required extremely small amounts of area. We will rigorously prove this below. We first note that every Besicovitch set is a Kakeya set with zero area, so if the converse were true and every Kakeya set satisfied the Kakeya needle problem, we would be done. However, we note that this cannot be the case, thus although there are sets with arbitrarily small Lebesgue measure (area in $\mathbb{R}^2$) that satisfy the Kakeya Needle Problem, there is no such set with area equal to 0. This proof is instructive, but requires some knowledge of real analysis. We encourage the reader to work through it, but as long as the reader understands the difference between a Kakeya set and a set satisfying the Kakeya Needle Problem nothing will be lost by skipping this proof.

Proposition 3.1. *There does not exist a Lebesgue measure* 0 *set that satisfies the Kakeya Needle Problem, i.e. we cannot continually rotate a unit line segment* 360 *degrees within it.*

Proof: Let $E \subset \mathbb{R}^2$ be a set within which a unit line segment can be continuously rotated. This means that there exists a continuous map $\ell : t \to \ell(t)$ for $t \in [0,1]$ to unit line segments $\ell(t) \subset E$. We can parameterize each such line segment

$$\ell(t) = \{(x(t) + s\cos(w(t)), y(t) + s\sin(w(t))) \mid -.5 \leq s \leq 0.5\}$$

where $x, y, w : [0,1] \to \mathbb{R}$ are continuous functions. We can see that the function $w(t)$ defines the rotation as time changes and the functions x and y determine the midpoint of the line segment. We recall that on a compact set such as $[0,1]$, all continuous functions are uniformly continuous. This means by definition that for each $\epsilon > 0$, there exists some $\delta > 0$ such that if $t, t' \in [0,1]$ such that $|t - t'| < \delta$ we have

$$|x(t) - x(t')|, |y(t) - y(t')|, |w(t) - w(t')| \leq \epsilon$$

Fix $\epsilon = .001$ and the corresponding δ. We observe that $w(t)$ cannot be a constant function of t as otherwise the needle would never rotate. Therefore, there must exist some $t_0, t_1 \in [0,1]$ with $|t_0 - t_1| \leq \delta$ and $w(t_0) \neq w(t_1)$. As if such a pair did not exist it would imply that w is constant. Without loss of generality assume that $t_0 < t_1$ and $x(t_0) = y(t_0) = w(t_0) = 0$, as we can just translate if this is not the case. So we can picture a line whose midpoint is at the origin on the x-axis of unit length.

Let $a \in [-.4, .4]$ be a real number. From our choice of $\epsilon = .001$, as we know that $|t_0 - t_1| \leq \delta$, we can see that for any $t_0 \leq t \leq t_1$, the line $\ell(t)$ must intersect the line $x = a$ in some point $(a, y_a(t))$ as for t in that interval, we know that x, y, w can at most change by .001. Thus given the starting position of our line, as $-.4 \leq a \leq .4$ there must be a point on the line that intersects the line $x = a$. By the definition of our line we know that $(a, y_a(t))$ must lie in E. Also, we notice that as we are continuously rotating our line that $y_a(t)$ varies continuously with t. By the intermediate value theorem, we conclude that the interval between $(a, y_a(t_0))$

and $(a, y_a(t_1))$ lies in E. This by itself will have an area of zero as it is going to trace the rotation of our original curve along one point. However, If we then take unions over all $a \in [-.4, .4]$ each of these segments must lie in E. This then traces the rotation of the entire line between $x = -.4$ to $x = .4$ as t varies from t_0 to t_1, and we know the line must at the least rotate by the above observation. Thus this constructed sector contained in E must have nontrivial area. This proves the claim. $\square$

This result does make intuitive sense, and we will now examine how the investigation of the Kakeya Needle Problem led to the Kakeya conjecture. We discussed how the answer to the needle problem is 0, as we can make the sets arbitrarily small. However, although these sets have essentially zero area, Davies [2] noticed that they were still necessarily two-dimensional. When we discuss dimension, we mean Hausdorff or Minkowski dimension for a rigorous definition we refer the reader to [16], as we will not be dealing with the Hausdorff or Minkowski dimension in the finite case. Trivially all Besicovitch sets in $\mathbb{R}$ have dimension 1, and Davies noticed that in $\mathbb{R}^2$ they must have dimension 2, thus the Kakeya conjecture asks:

Conjecture 3.1. *A Bescovitch set in $\mathbb{R}^n$ has Hausdorff and Minkowski dimension n.*

This conjecture remains open for dimensions $n \geq 3$, and it becomes more and more difficult as n increases. There have been many partial results bounding the Hausdorff and Minkowski dimension, but no exact results thus far. In an attempt to better understand this conjecture, in 1999 Woolf utilized a common mathematical technique and proposed a simpler analogue known as the Finite Field Kakeya conjecture avoiding all the technical issues involved in dealing with the Hausdorff and Minkowski dimension. We will generalize the definition of a Kakeya set:

Definition 3.2. If F^n is a vector space over a finite field F, we define a *Kakeya set* to be a subset of F^n which contains a line in each direction.

With this definition in mind, we can now pose the Finite Field Kakeya Conjecture as stated by Wolff in 1999 [25].

Conjecture 3.2. *Let $E \subset F^n$ be a Kakeya set. Then E has cardinality at least $c_n|F|^n$, where $c_n > 0$ depends only on n.*

The idea being that in the finite case we want to show that in order for a subset of a vector space over a finite field to be a Kakeya set, it must contain a large enough number of points that is related to the cardinality of the field and the dimension of the vector space. This is analogous to the set necessarily having a high dimension. Very recently Zeev Dvir was able to prove the above conjecture using the Polynomial Method. The proof follows from an adaptation of the Polynomial Ham Sandwich Theorem below, and an ingenious observation. For some intuition, we realize that we can produce a lower bound on the size of a finite set E that is one dimensional by showing that the only low degree polynomial that vanishes on E is the zero polynomial. This would imply that this set E with certain qualities must be trivial, as otherwise we could find a nontrivial polynomial that vanishes on E. We will use this intuition to prove the result. We will first discuss the lemma that is a simple corollary of the Polynomial Ham Sandwich Theorem.

Lemma 3.1. *Let $E \subset F^n$ be a set of cardinality less than $\binom{n+d}{n}$ for some $d \geq 0$. Then there exists a non-zero polynomial $P \in F[x_1, \ldots, x_n]$ on n variables of degree at most d which vanishes on E.*

Remark 3.1. This is a basic restatement for clarity of Lemma 2.2 above. The same proof applies.

So we know that there exists a suitable polynomial that vanishes on our entire set as long as the cardinality of E is less than $\binom{n+d}{n}$ for some $d \geq 0$. Now we will prove something unique and incredible about Kakeya sets that forces there to be a certain number of elements in E:

Theorem 3.2. *Let $P \in F[x_1, \ldots, x_n]$ be a polynomial of degree $\leq |F| - 1$ which vanishes on a Kakeya set E. Then P must be identically zero.*

Proof: Suppose for sake of contradiction that P is not identically zero. Then we can write $P = \sum_{i=0}^{d} P_i$ where $0 \leq d \leq |F| - 1$ is the degree of P and P_i is the i^{th} homogeneous component of P. So we are partitioning P into its homogeneous components, thus P_d is nonzero as P is of degree d. Since we know that P vanishes on E and E is nonempty this implies that d cannot be zero.

Let $v \in F^n \setminus \{0\}$ be an arbitrary direction. We note that we subtract zero as the result would be trivial if we chose the zero direction. As E is a Kakeya set, we know that E contains a line $\{x + tv \mid t \in F\}$ for some $x = x_v \in F^n$. Thus as we know that P vanishes on E this implies that $P(x + tv) = 0 \ \forall t \in F$. The left hand side is a polynomial in t of degree at most $|F| - 1$ as P is of degree at most $|F| - 1$ and it vanishes on all of F. Thus this polynomial must be identically zero. As if it is nontrivial, it can vanish on at most $|F| - 1$ points, but F clearly contains $|F|$ points.

In particular, the t^d coefficient of the polynomial, $P_d(v)$ vanishes for any nonzero v as we chose v arbitrarily since E is a Kakeya set. We can see that the coefficient of this polynomial is $P_d(v)$ if we examine all the coefficients of t^d, each t^d coefficient will be generated by a term in our polynomial of degree d. Thus when we factor out the t^d and consider the multivariable polynomial as a single variable polynomial defined over t, the coefficient is the polynomial P_d. Since P_d is a homogeneous polynomial of degree $d > 0$, P_d must vanish on all of F^n. This is because we know that $P_d(v) = 0 \ \forall v \in F^n \setminus \{0\}$, and trivially equals zero for the zero vector. As F is finite, however, this does not imply that P_d is identically zero. We do now have that $P_d(x) = 0 \ \forall x \in F^n$. Since $d \leq |F| - 1 < |F|$, we can apply the above analysis to P_d. As we now know that it must vanish on the entire Kakeya set as it vanishes on F^n. However, this implies that when we consider P_d as a polynomial defined over each variable, $x_1, \ldots, x_n$ independently with coefficients in the remaining variables that P_d must vanish identically as it vanishes on all of F, since it vanishes on all of F_n, but has degree $< |F|$. If we do this for each variable we reach get the same result, and thus we conclude that $P_d = 0$ identically. However we stated in the beginning of the proof that P_d cannot be zero as P is of degree d. This is a contradiction and proves the theorem. □

Essentially we have now proved that given a polynomial that vanishes on a Kakeya set, it must have degree at least $|F|$ where the Kakeya set is defined over F^n. We will now combine this with the above lemma to prove the result which we will just state as a corollary.

Corollary 3.1. *Every Kakeya set in F^n has cardinality at least $\binom{|F|+n-1}{n}$*

Proof: If this is not the case that it implies that there exists a nontrivial polynomial of degree $|F|-1$ that vanishes on E by Lemma 3.1. This is a direct contradiction to Theorem 3.2. $\square$

The method employed in this proof is to show that any polynomial of a small enough degree m that vanishes over the Kakeya set E must be the trivial polynomial. We know, however, by Lemma 3.1 that we can find nontrivial polynomials that vanish over any given set as long as the cardinality of that set is less than $\binom{n+d}{n}$ where n is the degree of the vector space that E is defined over and d is the degree of the polynomial. Combining these two results forces the cardinality of E to be a certain size, as otherwise the results contradict each other. In other words, we must have $\binom{n+m}{n} \leq |E|$, as otherwise we can take $d = m$ and Lemma 3.1 applies and leads to a contradiction.

We said that this analogue would lend significant support to the original conjecture. This is the case as this result essentially rules out highly algebraic counterexamples to the original conjecture. By highly algebraic we mean sets with a strong algebraic structure. This is because these sets could likely be adapted to a finite field example. This result differs greatly from the other results we have proved thus far, as we utilized the polynomial method to supply a lower bound on the cardinality of a set. The following joints problem actually evolved from the above proof of the Finite Field Kakeya conjecture.

4 The Szemerédi and Trotter Theorem

We now transition to working over an infinite field by investigating one of the most seminal results in incidence geometry and combinatorics that is deeply intertwined with the polynomial method: The Szemerédi and Trotter Theorem. This theorem deals with a given set P of m points and L of n lines. Given these two sets, one may wonder how many possible incidences they generate and how this is related to the number of elements in each set. The Szemerédi and Trotter Theorem provides a bound on this number of incidences, and we will actually prove that this bound is optimal.

4.1 Statement of Theorem

Before the statement of the theorem, we must first provide the definition for some notation.

Definition 4.1. Given a set points P and lines L in the plane, let $I(P, L)$ denote the number of incidences between that occur between the points in P and lines in L. i.e, the number of pairs (p, ℓ) such that $p \in P$ and $\ell \in P$, and $p \in \ell$.

Theorem 4.1 (Szemerédi and Trotter Theorem)**.** *$I(P, L) = O(m^{2/3}n^{2/3} + m + n)$ for every set P of m distinct points and every set L of n distinct lines in the plane.*

4.2 Introduction to Projective Geometry

Many important techniques throughout this paper will involve basic ideas from Projective Geometry. We will thus introduce the ideology behind Projective Space, and the idea of Planar Duality. For further reading, we refer the reader to [14, 10].

Definition 4.2. The *Complex Projective Space* P_n of dimension n is the set of complex one-dimensional subspaces of the complex vector space $\mathbb{C}^{n+1}$. An analogous definition can be supplied for the *Real Projective Space.*

Definition 4.3. Alternatively, we can define an equivalence relation $\sim$, where given vectors $a, b \in V$ in some vector space V, $a \sim b$ if $a = \lambda b$, where λ is a constant in U, the field over which the vector space is defined. The projective space of V can then be defined as $(V \setminus \{0\})/\sim$. Where P_n is thus the set of equivalences classes of $V \setminus \{0\}$ under our defined equivalence relation. We can see that this is an analogous definition as each unique line passing through the origin will by definition represent a unique equivalence class.

Remark 4.1. We can utilize this definition to define the Real and Complex Projective spaces as above. In these cases we let $V = U = \mathbb{R}$ or $\mathbb{C}$. The Complex Projective Space then becomes $(\mathbb{C} \setminus \{0\}/\sim)$.

Definition 4.4. When working in Projective Space, we utilize *projective coordinates.* For sake of ease we will make this definition for $P_2(\mathbb{R})$, and explain how it can be generalized. The coordinate $[a, b, c] \in P_2(\mathbb{R})$ is representative of the equivalence class of all scalar multiples of $[a, b, c]$ as a vector in $\mathbb{R}^3 \setminus \{0\}$. In other words, the projective coordinates $[a, b, c]$ and $[c, d, f]$ are equal if $[a, b, c] = [\lambda c, \lambda d, \lambda f]$ for some nonzero constant λ. We can easily generalize this to greater dimensions by taking vectors with more elements.

Utilizing this definition, we can see that any point $[a, b, c] \in P_3$ can be represented by $[a/c, b/c, 1]$. This leads to the following natural and interesting fact:

Proposition 4.1. *The mapping $(x, y) \to [x, y, 1]$ defines an inclusion from the Euclidean Plane to the projective plane. Once again we note that this mapping can be generalized.*

Proof: This is fairly clear as given any (x, y) we know that $x = a/c$ and $y = b/c$ for some a, b, c in the original vector space. Thus, this defines an injective mapping. $\square$

One may wonder, however, what occurs when $z = 0$ in our projective coordinates. This is exactly the complement of the above image, and it elicits the following definition.

Definition 4.5. The set of points $z = 0$ in the projective plane defines a line. We call this the *line at infinity.*

This definition makes intuitive sense, as if $z = 0$ in any point in the projective plane, if we were to attempt to divide by 0 we would have the point $[\infty, \infty, 1]$ (in a loose sense). The above map also illustrates why the dimension of P_n is n, as we can define an embedding of $\overline{\mathbb{R}}$, the *extended real numbers*, i.e. $\mathbb{R} \cup \{\infty, -\infty\}$ into P_n. This is defined by the above mapping coupled with sending $\{-\infty, \infty\} \to \infty$. In this sense we can now multiple and divide by 0 and infinity.

Definition 4.6. We define an *affine space* as a point set A together with a vector space V over a field F and a transitive group action of V on A. Explicitly, an affine space is a point set A with a map $f : V \times A \to A$ where

$$f(\mathbf{v}, a) = \mathbf{v} + a$$

with the following properties

(a) $\forall a \in A$, $\mathbf{0} + a = a$

(b) $\forall \mathbf{v}, \mathbf{w} \in V$, $\forall a \in A$, $\mathbf{v} + (\mathbf{w} + a) = (\mathbf{v} + \mathbf{w}) + a$

(c) $\forall a \in A$, $f(\mathbf{v}, a) = \mathbf{v} + a$ is unique.

Remark 4.2. Under these operations we note that by choosing an origin point for A, one can identify it with V. Each point can then become a vector and A will become a vector space under the operations of V. Similarly, any vector space V is an affine space over itself if we take each vector as a point set. Obviously all of the axioms hold. Affine spaces generalize properties of parallel lines in Euclidean Space. There is no way to add vectors as there is no origin to serve as reference. It does make sense to subtract two points of the space to create a vector. Affine spaces will become extremely useful when we discuss hyperplanes. We will now connect Affine Spaces, Projective Spaces and Vector Spaces.

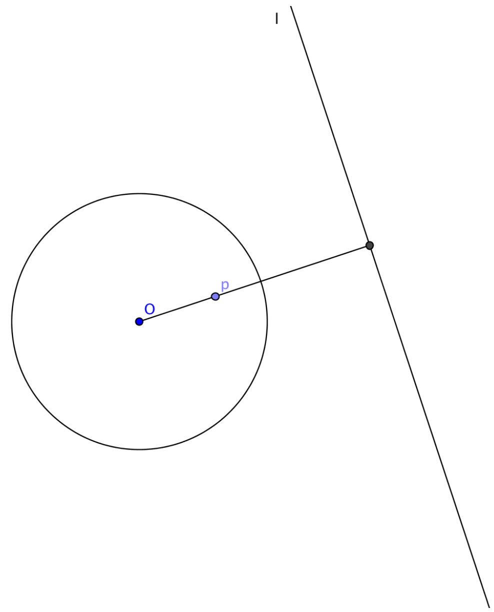
Proposition 4.2. *Affine Spaces are open subspaces of Projective Spaces which are quotient spaces of Vector Spaces.*

We now introduce the procedure to create the planar dual of a set points P and lines L.

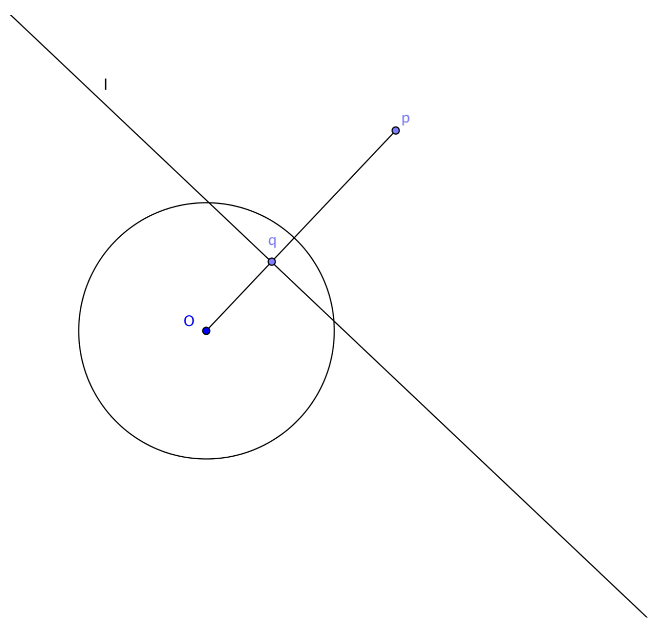
Proposition 4.3. *Given a set of m points P and n lines L in the plane. We can construct a set of n points J and m lines K that are the original arrangement's* standard planar dual.

Proof: Given our original arrangement, we let $I(P, L) = k$. Thus we need $I(J, K) = k$. We can achieve this planar duality utilizing a trick from projective geometry. We select a point O in the plant that does not lie on any line in L and is not any point in P. We create a circle of arbitrary radius r around that point (preferably small radius). We then exchange points and lines in the following manner. For any given line ℓ, we draw a line segment q perpendicular to ℓ that passes through O. We then place a point p on this perpendicular such that the product of the length of q and the length of the line segment Op equals r^2.

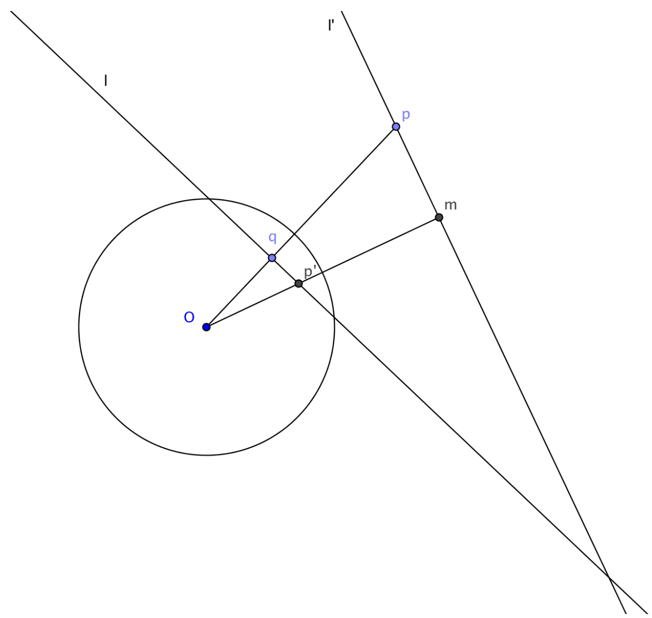
This points p is the dual of the line ℓ. We can see this explicitly below.



Then, for any given point p, examine the line segment Op. Find the point q on the segment Op such that $Op \cdot Oq = r^2$. Draw a line ℓ perpendicular to Op, that passes through q. This is the planar dual of the point p. We can explicitly see this process below.



If we proceed in this fashion for all points and lines, I claim that we preserve incidences. It is clear that we interchange the number of points and lines. We will examine the specific case where a point and a line are incident in the original graph and prove this incidence is preserved in the dual. This then generalizes easily for all incidences. We will first show an example where a point p and a line l' are incident in the original graph. Utilizing the above process we create the line l, the planar dual of p. We also create the point p', the planar dual of l'. It stands to show that l and p' are incident.



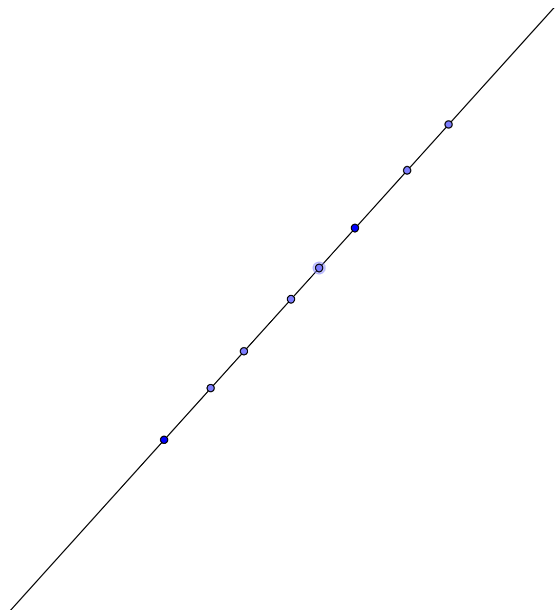
From the construction we know that $Oq \cdot Op = r^2$ and that $Op' \cdot Om = r^2$. Let v be the point where l intersects Om. We want to show that $v = p'$. We can achieve this by proving that $Ov \cdot Om = r^2$. As these two right triangles share a common angle, they are similar. Thus we can see that $\frac{Oq}{Om} = \frac{Ov}{Op}$, cross multiplying we have that $Oq \cdot Op = Ov \cdot Om$, but $Oq \cdot Op = r^2$. This implies that $Ov \cdot Om = r^2$. Thus $p' = v$ and incidence is preserved.

$\square$

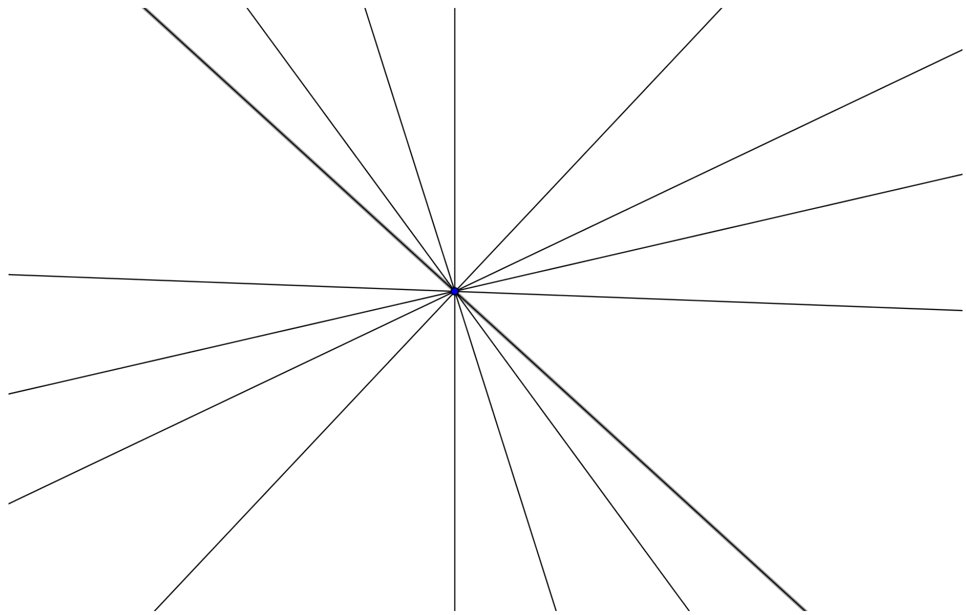
4.3 Extremal Examples

Before proving the Szemerédi and Trotter Theorem, we wish to explore the extremal cases that make the theorem tight and thus optimal. One must notice the three terms that can contribute to the number of incidences. Asymptotically, we fall into two cases: (1) One of the terms m or n dominates the other, (2) They are within a close enough range that $n^{2/3}m^{2/3}$ dominates m and n. We want to explore explicit examples of each of these cases and discuss the implications.

Example 4.1. If we examine the extremal example where we have m points and $n = 1$ line, we can see that the Szemerédi and Trotter Theorem is tight. The maximal number of incidences that could occur is if all of the points could be intersected by the one line, in which case the number of points m completely determines the number of incidences. In other words $I(P, L) = O(m)$. Which is what the Theorem predicts, as if $n = 1$, $m^{2/3} < m$ and $n < m$, assuming there is more than one point, thus we have $I(P, L) = O(m)$. This is easily illustrated where $m = 8$, the maximal number of incidences is exactly 8. This can be seen in the figure below.

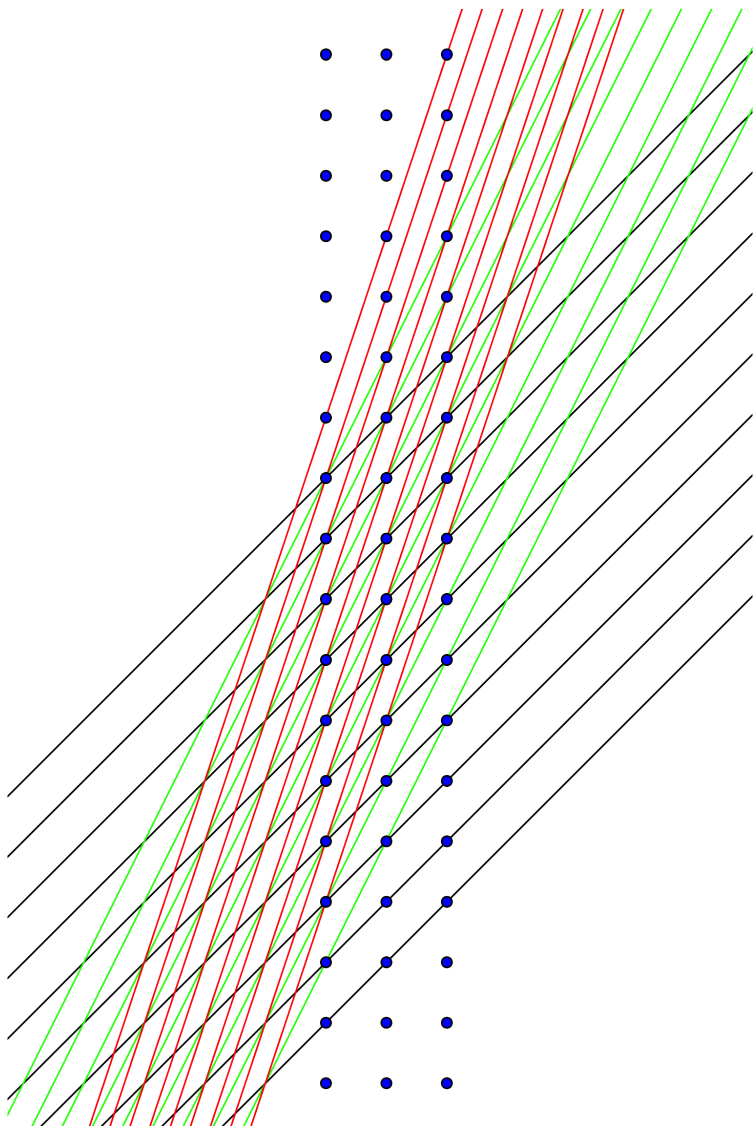


Example 4.2. The exact same idea can be applied for the case where we have $n > 1$ lines and $m = 1$ point. We can see that by standard planar duality, the maximal number of incidences occurs when every line intersects the point, and it can only intersect it once. Thus $I(P, L) = O(n)$ where the implied constant is 1. This is exactly what the Szemerédi and Trotter Theorem tells us. We can see an illustration of this extremal example below:



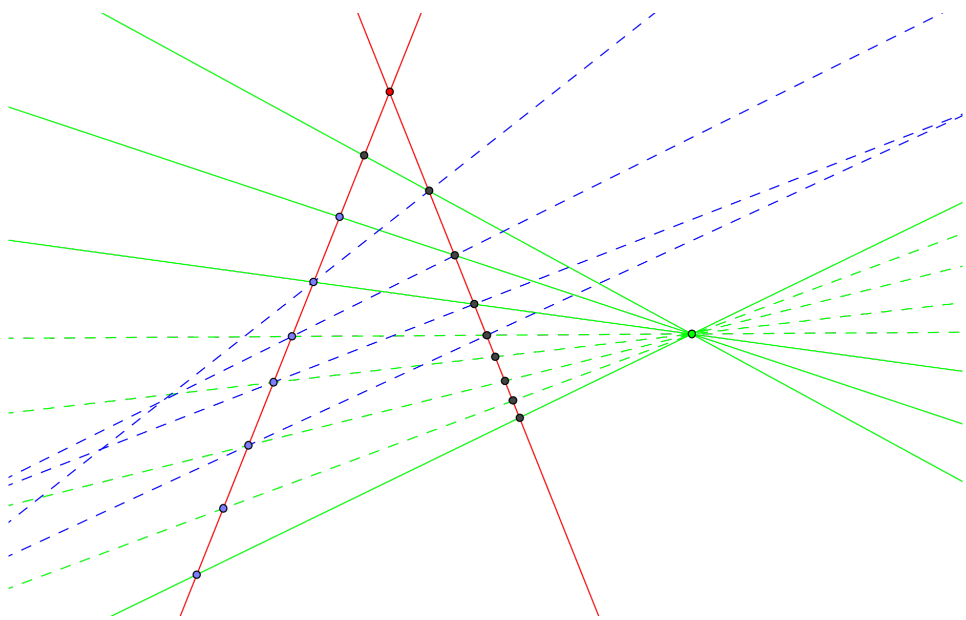
The above image is actually the planar dual of the first image. There are exactly eight lines and one point. The line becomes the point, and every point it intersects becomes a line that intersects the point in the dual.

Example 4.3. We will now look at a more interesting example that provides a sharp bound for the case when m and n are close enough that neither term can dominate the other. Take the set of points $P = \{1, \ldots, N\} \times \{1, \ldots, 2N^2\}$ and the set of lines $L = \{(x, y) \mid y = mx + b\}$ where $m \in \{1, \ldots, N\}$ and $b \in \{1, \ldots, N^2\}$. We can see that $|P| = m = 2N^3$ and $|L| = n = N^3$. The Szemerédi and Trotter Theorem would tell us that $I(P, L) = O(N^4)$. We can see that the number of incidences is exactly N^4. This is because each line intersects exactly N points. We can see this because a line intersects a point for every value of x as x ranges between 1 and N. This is because in this interval, $x \leq N$, $m \leq N$ and $b \leq N^2$, thus $y \leq 2N^2$, for each point x, and y is an integer. This tells us that a given line ℓ with slope m and y-intercept b intersects exactly N points, mainly $(1, m+b), (2, 2m+b), \ldots, (N, Nm+b)$. We can see an illustration of this below where we let $N = 3$:

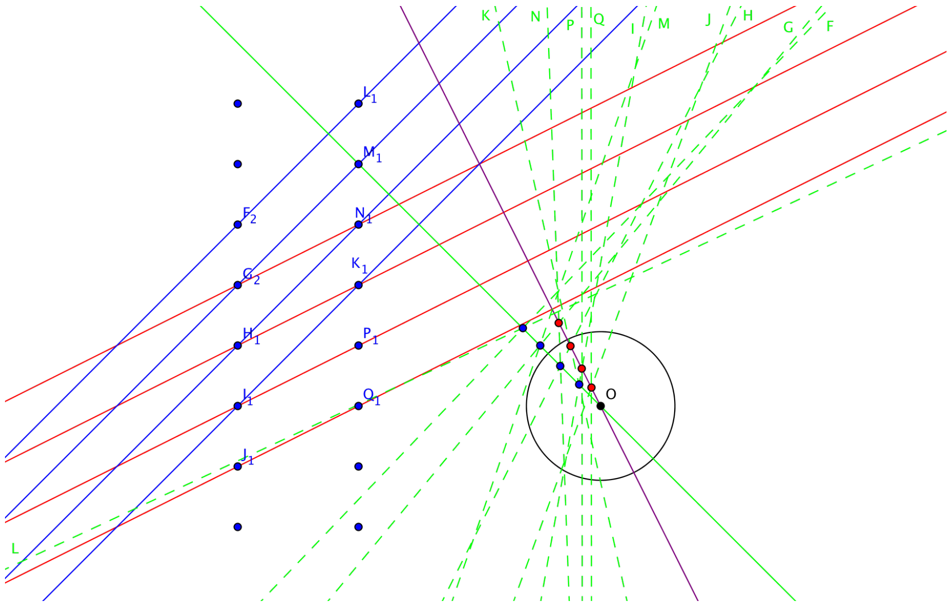


The black lines are when $m = 1$ and b ranges from 1 to 9. The green lines are when $m = 2$, and the red are when $m = 3$. We can see that each line contributes exactly three incidences, and as there are a total of 27 lines, this means that there are $3^4 = 81$ incidences. Looking at the Szemerédi and Trotter Theorem, it would tell us that we should expect at most this many incidences.

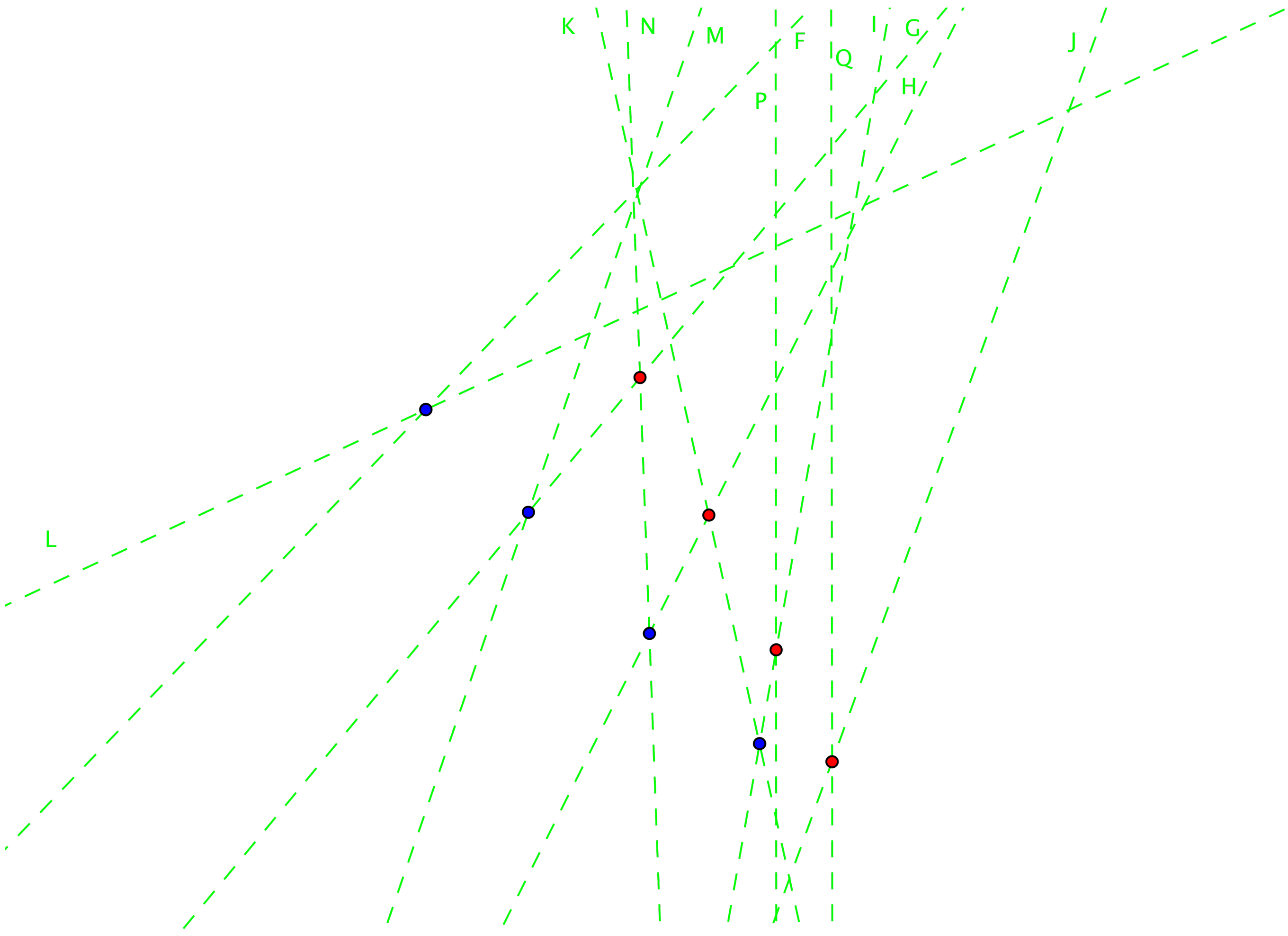
Example 4.4. We notice the iterating fact that utilizing a linear transformation of the above lattice, we can generate infinitely many extremal examples. These extremal examples in general can be visualized in the projective plane. If we have N lines going through the point at infinity and we select another point in the plane and draw $2N^2$ lines passing through that point, the incidences generated by these lines create an extremal example. This extremal example is merely a linear transformation of our original integer lattice. An example of this can be seen below.



We can see that this is exactly the same as our lattice example. The dashed green and blue lines represent the N^3 lines, here where $N = 2$, and we can see that we have $2N^3$ points. We also notice that this very closely resembles the standard planar dual of the lattice. The dual graph will also represent an extremal example, as it presences incidences. The dual graph for $N = 2$ is pictured below.



This picture has many parts. We have the original graph pictured with blue points, four blue lines and four red lines. We then selected our point O, and drew a circle to begin constructing our dual graph. The purple line is perpendicular to each of the red lines, and the corresponding red points on that line represent the planar dual of each red line in the original graph. Similarly, the light blue line is perpendicular to each of the blue lines. Each blue point on this line represents the planar dual of each of the blue lines. We then labeled each point that is important to the dual. Each of the dashed green lines represents one of those points and is labeled accordingly. We will now only show a picture of the completed dual graph, excluding points from the original graph that are not incident to any lines, as these can really be placed anywhere in the dual graph as long as they are not incident to any of the dual points. We can see the dual graph below.



We notice that there are 8 points and 16 lines, i.e. N^3 points and $2N^3$ lines. We once again note that some lines are not included as they do not generate any incidences, just as in the original graph there were points that were not incident with any lines. There are also exactly 16 incidences, i.e. $O(N^4)$ incidences. Thus, this is another extremal example. The partitioning polynomial in this case is of degree 2 as before and is created by placing a line through each of the blue points and a line through each of the red points. We will investigate the possibility of creating duals for algebraic curves and r-partitioning polynomials in a later section.

4.4 Discussion of Optimality

Between these three examples, we illustrate how the bound cannot be improved (i.e. there is no lower bound), as in any case there exists a point line arrangement that makes the Szemerédi and Trotter Theorem sharp. The only issue that could arise is if there exists a point-line arrangement such that $I(P, L) > O(m^{2/3}n^{2/3} + m + n)$. Thus, we will combine these examples with the proof below that any set of lines and points is in fact bounded by $O(n^{2/3}m^{2/3} + m + n)$ to show that the bound is optimal.

4.5 A Soft Bound and Its Implications

We will now introduce an important Lemma which illustrates how one can quickly derive a soft bound on $I(P, L)$. This will ultimately play an important role in the proof of the Szemerédi and Trotter Theorem.

Lemma 4.1. *$I(P, L) \leq n + m^2$, where P contains m points and L contains n lines.*

Proof: We will divide the lines of L into two subsets: the lines in L' that are incident to at most one point of P, while the lines in L'' pass through at least two points.

It is clear that $I(P, L') \leq |L'| \leq n$, as each line can only have one incidence with a point by definition. Now we must bound $I(P, L'')$. This can be done by noticing that a point $p \in P$ can have at most $m-1$ incidences with the lines of L'', since there are at most $m-1$ lines passing through p, as each line in L'' that passes through a point p, must also pass through at least one other point in P. As there are only $m-1$ other possible points the line could pass through, this means there are at most $m-1$ lines from L'' incident with any point p. As there are a total of m points, this means that, $I(P, L'') \leq m(m-1) \leq m^2$. Thus $I(P, L) = I(P, L') + I(P, L'') \leq n + m^2$. □

For these first few propositions, we will explore the implications of the above lemma that will prove extremely useful in the proof of the theorem. Our motivation here is to explore the separation between m and n necessary so that one term individually begins to asymptotically dominate $I(P, L)$.

Proposition 4.4. *If $m^2 \leq n$, then $I(P, L) = O(n)$.*

Proof: If $m^2 \leq n$, then by Lemma 1.1 above, we have that $I(P, L) \leq n + m^2 \leq 2n = O(n)$. We can see that in this case the Szemerédi and Trotter Theorem is tight. If $m^2 \leq n$, then $O(m^{2/3}n^{2/3} + m + n) = O(n)$. □

Corollary 4.1. *If $n^2 \leq m$, then $I(P, L) = O(m)$.*

Proof: This follows from standard planar duality. Interchanging the roles of the lines and the points. The above proposition implies the corollary immediately. In this case we see that the Szemerédi and Trotter Theorem is tight again, as if $n^2 \leq m$, $O(m^{2/3}n^{2/3}+m+n) = O(m)$. □

It is important to notice that within the interval $\sqrt{n} \leq m \leq n^2$, the Szemerédi and Trotter Theorem predicts that $m^{2/3}n^{2/3}$ will dominate. As within this interval $O(n^{2/3}m^{2/3}+m+n) = O(n^{2/3}m^{2/3})$ Thus, the above corollaries need to be the exact points at which m and n begin to dominate in order for the theorem to be true. We will prove that this is actually the case. It turns out to be extremely useful that we only have to consider the interval $\sqrt{n} \leq m \leq n^2$, as we will see.

4.6 Background and Preliminary Results

Here we present and establish all of the results necessary to prove Szemerédi and Trotter Theorem using the polynomial method. In the following subsection, we highlight the effectiveness of the polynomial method by presenting some of the restrictive qualities of $Z(f)$ for a given polynomial f. We begin by introducing the Fundamental Theorem of Algebra. It will come into play repeatedly, and eventually be subsumed by Bézout's Theorem when we begin our study of incidences with algebraic curves in place of lines.

Definition 4.7. If a function f has a derivative on a set G, we say that f is *analytic* on G. If f is analytic on the entire complex plane, we say that f is *entire*.

Theorem 4.2 (Fundamental Theorem of Algebra)**.** *Every nonconstant, single variable polynomial $f \in \mathbb{C}[x]$, has at least one complex root.*

Proof: Suppose that $P(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$, with $a_n \neq 0$, has no roots. It follows immediately that $f(z) = \frac{1}{P(z)}$ is entire. This is clear as rational polynomials (i.e. functions of the form $f(z)/g(z)$ where $f(z)$ and $g(z)$ are polynomials) are analytic whenever the denominator is nonzero [19]. Thus if $P(z) \neq 0$ for any z, then the rational function $f(z)$ is entire. We will prove that it is bounded over the whole plane. There are two cases to consider.

(a) We know that $|P(z)/z^n| \geq |a_n|/2$ for $|z|$ sufficiently large, as $|P(z)/z^n| \to a_n$ as $|z| \to \infty$. Say $|z| \geq \alpha$. Thus we see

$$|f(z)| = \frac{1}{|P(z)|} \leq \frac{2}{|z^n||a_n|} \leq \frac{2}{\alpha^n |a_n|}$$

Where $|z| \geq \alpha$. So in this case $|f(z)|$ is bounded by a constant.

(b) When $|z| \leq \alpha$, we have the case of a continuous function, $|f(z)|$, on a closed disk. Under such circumstances, by the extreme value theorem it is know that the function must be bounded, as it achieves its maximum and minimum within this disk.

Thus in either case $f(z)$ is bounded, and we know that it is entire. However, the only bounded entire functions are constant [19]. If $f(z)$ is constant, this implies that $P(z)$ is as well. This proves that the only polynomials that have no roots are constant. □

Corollary 4.2. *We can inductively apply the above theorem to factor any given $f \in \mathbb{C}[x]$ into exactly n linear factors, where $n = \deg(f)$. This tells us that a given nonconstant, single variable polynomial $f \in \mathbb{C}[x]$ has exactly n roots in $\mathbb{C}$.*

4.6.1 Essential Qualities of Polynomials

Definition 4.8. For a given polynomial $f \in \mathbb{R}[x, y]$ we will define the *zero set* of f as the set of all points in $\mathbb{R}^2$ on which f vanishes. We will denote the zero set as $Z(f)$.

Lemma 4.2 (Vanishing Lemma)**.** *If ℓ is a line in $\mathbb{R}^2$ and $f \in \mathbb{R}[x, y]$ is of degree at most D, then either $\ell \subseteq Z(f)$, or $|\ell \cap Z(f)| \leq D$. i.e. The polynomial f vanishes on less than or equal to D points of a line ℓ, or it vanishes on the entire line.*

Proof: We must write ℓ in parametric form: $\ell = \{(u_1 t + v_1, u_2 t + v_2) \mid t \in \mathbb{R}\}$. Now we will define a single variable polynomial in t utilizing our bivariate polynomial f. Let $g(t) = f(u_1 t + v_1, u_2 t + v_2)$. As f is of degree D, this means that g is of degree at most D.

Thus by the Fundamental Theorem of Algebra, g has at most D zeroes if it is not uniformly zero. So it is either uniformly zero on the line, or it only equals zero at $\leq D$ values of t. In terms of our original function f and our line ℓ this means that if f vanishes on $> D$ points of the line ℓ, that f must vanish on the entire line. $\square$

Proposition 4.5. *A nonzero bivariate polynomial $f \in \mathbb{R}[x, y]$ does not vanish on all of $\mathbb{R}^2$.*

Proof: Assume we have such a nonzero bivariate polynomial $f \in \mathbb{R}[x, y]$ that vanishes on all of $\mathbb{R}^2$. This means that every point $(x, y) \in \mathbb{R}^2$ satisfies $f(x, y) = 0$. Let $f(x, y) = \sum_{ij} a_{ij}x^i y^j$, and define $g(x) := \sum_{ij} a_{ij}x^{i+j}$. We know that $f(x, y)$ vanishes on all the points where $x = y$. At these points $f(x, x) = \sum_{ij} a_{ij}x^i x^j = \sum_{ij} a_{ij}x^{i+j} = g(x)$. However, $f(x, x) = 0$ for all x by assumption. This implies that $g(x) = 0 \ \forall x \in \mathbb{R}$. Also, as f was a nonzero polynomial, this implies that g is as well because f and g share coefficients. This implies that we have found a nonzero single variable polynomial with real coefficients and bounded degree ($\deg(g) = \max i + \max j$) that vanishes on infinitely many points $x \in \mathbb{R}$. This is a contradiction by the Fundamental Theorem of Algebra. Thus, f cannot vanish on all of $\mathbb{R}^2$. $\square$

Lemma 4.3. *If $f \in \mathbb{R}[x, y]$ is nonzero and of degree at most D, then $Z(f)$ contains at most D distinct lines.*

Proof: We know that a nonzero bivariate polynomial does not vanish on all of $\mathbb{R}^2$. Now we fix some point $p \in \mathbb{R}^2$ such that $p \notin Z(f)$. Assume that $Z(f)$ contains the distinct lines $\ell_1, \ldots, \ell_k$. We can select another line ℓ incident to p that is not parallel to any of the ℓ_i, and does not pass through any of the points of intersection $\ell_i \cap \ell_j$. This is true because we must only avoid finitely many points as the lines $\ell_1, \ldots, \ell_k$ are distinct. By assumption ℓ is not completely contained in $Z(f)$ as it is incident to p, and it has at most k possible intersections with $\bigcup_{i=1}^{k} \ell_i$ as a distinct line can only intersect a line in one point. Thus Lemma 2.1 tells us that $k \leq D$. $\square$

4.6.2 The Borsuk Ulam Theorem

We introduce the following theorem as a tool to prove the Ham-Sandwich Theorem.

Theorem 4.3 (Borsuk-Ulam Theorem)**.** *Let $f : S^n \to \mathbb{R}^n$ be a continuous map from the n-dimensional sphere $S^n \subset \mathbb{R}^{n+1}$ to the Euclidean Space $\mathbb{R}^n$ which is antipodal. Then $f(x) = 0$ for at least one $x \in S^n$.*

We will prove this theorem in the case the n=2 and for a proof of the n-dimensional case and applications we refer to reader to [1, 15]. To prove this theorem we will take a quick detour into Topology. Skipping the following section will not detract from the rest of the paper, but we include the proof for completeness and for the curious reader as an example of how many disciplines the polynomial method spans. We must first introduce some terminology. In the following we assume a basic knowledge of topology.

Definition 4.9. For our purposes, we will assume that we are working in $\mathbb{R}^d$. A *hyperplane* h in $\mathbb{R}^d$ is an affine linear subspace of dimension $d - 1$.

Definition 4.10. We say that a function f is *antipode-preserving* on its domain X if $\forall x \in X$, $f(-x) = -f(x)$.

Definition 4.11. If f and g are continuous maps of the space X into the space Y, we say that f is *homotopic* to g if there is a continuous map $F : X \times [0,1] \to Y$ such that $F(x,0) = f(x)$ and $F(x,1) = g(x)$ for each $x \in X$. F is called a *homotopy* between f and g. We say that a function h is *nul-homotopic* if it is homotopic to a constant map.

We are now ready to state and prove some important lemmas and theorems that will ultimately make the proof of the Borsuk-Ulam Theorem relatively simple.

Theorem 4.4. *If $h : S^1 \to S^1$ is continuous and antipode-preserving, then h is not nulhomotopic.*

Lemma 4.4. *Let $h : S^1 \to X$ be continuous. Then the following conditions are equivalent:*

(a) h is nulhomotopic.

(b) h extends to a continuous map $k : B^2 \to X$.

(c) h_* is the trivial homomorphism of fundamental groups.

We will not prove this theorem or lemma, but for rigorous proofs we refer the readers to Munkres [16]. The theorem number is 57.1 and the lemma number 55.3. We will now use this theorem to prove an important lemma.

Lemma 4.5. *There is no continuous antipode-preserving map $g : S^2 \to S^1$.*

Proof: Assume for sake of contradiction that such a map exists. Let S^1 be the equator of S^2. Then consider the restriction of g to its equator. This is a continuous antipode-preserving map h from S^1 to itself. By Theorem 4.4 we know then that h is not nulhomotopic. However we can see that h easily extends to a map from the upper half-sphere of S^2 to S^1 as g is a map of all of S^2 to S^1 so we can easily restrict it to the upper half-sphere and h is a restriction of g. However we notice that the upper half-sphere is homeomorphic to B^2. Lemma 4.4 then tells us that h is nulhomotopic, contradicting the claim of Theorem 4.4. Thus such a function g cannot exist. □

We are now ready to prove the Borsuk-Ulam Theorem in the case that $n = 2$.

Proof: Suppose that $f(x) \neq f(-x)$ $\forall x \in S^2$. Then the map

$$g(x) = \frac{f(x) - f(-x)}{||f(x) - f(-x)||}$$

Is a well-defined, continuous map from $S^2 \to S^1$. We also notice that g is antipode preserving as $g(-x) = -g(x)$ for all x. Thus g is a continuous, antipode preserving map from $S^2 \to S^1$, which we just proved cannot exist. So there must exist a point $x \in S^2$ such that $f(x) = f(-x)$. □

4.6.3 Partitioning Polynomials and the Ham Sandwich Theorem

In this subsection, we present the core tools utilized to prove the Szemerédi and Trotter Theorem. We ultimately desire a way to efficiently partition a set of given points in the plane utilizing the zero set of a bivariate polynomial. When we accomplish this, we will utilize the above results concerning the restrictive nature of the zero sets of such polynomials to establish the desired bound on $I(P, L)$. We first present the Ham Sandwich Theorem in its discrete version.

Theorem 4.5 (The Ham Sandwich Theorem). *Every d Lebesgue-measurable sets $A_1, \ldots, A_d \subset \mathbb{R}^d$ can be simultaneously bisected by a hyperplane.*

Now we are ready to prove the Ham-Sandwich Theorem. The techniques in this proof are closely related to and helped spawn the ideas behind the polynomial ham sandwich theorem.

Proof: We can recognize $\mathbb{R}^{n+1}$ as the space of affine-linear transformations $(x_1, \ldots, x_n) \to a_1x_1 + \cdots + a_nx_n + a_0$ on $\mathbb{R}^n$. Each non-trivial affine linear form $E \in \mathbb{R}^{n+1} \setminus \{0\}$ determines a hyperplane in $\mathbb{R}^{n+1}$, mainly the set of vectors such that $\{E = 0\}$. This divides $\mathbb{R}^n$ into two spaces $(E > 0)$ and $(E < 0)$. We can thus define $f : \mathbb{R}^{n+1} \setminus \{0\} \to \mathbb{R}^n$ whose i^{th} coordinate $f_i(E)$ at E is the volume of $A_i \cap \{E > 0\}$ minus the volume of $A_i \cap \{E < 0\}$. Essentially, f measures the extent to which the given hyperplane $\{E = 0\}$ bisects the given sets $A_1, \ldots, A_n$. It is intuitively clear that f is continuous, but very subtle to prove. For an intensive proof we refer the reader to [15].

The function f is also homogenous of degree zero, as it has no variables. Most importantly it is odd, as if we take $f(-P)$, the i^{th} coordinate will by definition be $A_i \cap \{-P > 0\}$ minus $A_i \cap \{-P < 0\}$. This equals $A_i \cap \{P < 0\}$ minus $A_i \cap \{P > 0\}$ which we can easily recognize as $-f(P)$. This means that if we restrict f to S^n, it is an antipodal map. By Theorem 1.3 above, this means that there exists some P such that $f(P) = 0$. Thus, the hyperplane described by $\{P = 0\}$ exactly bisects the given sets $A_1, \ldots, A_n$. □

Corollary 4.3. *[15] Every collection of d finite sets $A_1, \ldots, A_d \subset \mathbb{R}^d$ can be simultaneously bisected by a hyperplane.*

Definition 4.12. For a given bivariate polynomial $f \in \mathbb{R}[x, y]$ and $A_1, \ldots, A_s \subseteq \mathbb{R}^2$, we say that f *bisects* A_i if $f > 0$ on at most $\lfloor |A_i|/2 \rfloor$ points of A_i and $f < 0$ on at most $\lfloor |A_i|/2 \rfloor$ points of A_i.

Lemma 4.6. *Bivariate Polynomials of degree D form a real vector space V of dimension $\binom{D+2}{2}$ with basis given by the monomials x^iy^j where $i, j \in \mathbb{Z}_{\geq 0}$ and $i + j \leq D$.*

Proof: It is clear that given any two polynomials $f, g \in V$ that $f + g \in V$ and $k \cdot f \in V$ where $k \in \mathbb{R}$ is a constant. We also have an identity element $f(x, y) = 0$. The other axioms of a vector space follow easily. Now, we must prove that $\dim(V) = \binom{D+2}{2}$.

We can easily see that the proposed basis elements are linearly independent, as they each contain distinct powers of x and y. We can also see that they do in fact span the entire space V, as any polynomial of degree D is by definition a sum of monomials $\sum_{0\le i+j\le D} a_{ij}x^iy^j$ where $a_{ij} \in \mathbb{R}$. Thus any element of V is a $\mathbb{R}$-linear combination of monomials. Thus, by definition the proposed set is a basis for V. It remains to found the number of basis elements to determine the dimension of V.

We can see that counting the number of described monomials is equivalent to counting the number of pairs (i, j) of nonnegative integers with $i + j \le D$. We can see that $\binom{D+2}{2} = \sum_{i=1}^{D+1} i$. We will count these pairs utilizing a "stars and bars" argument. If we want the sum of (i, j) to equal D we have $D + 1$ options for i and then we only have 1 for j. In general, the choice of i determines the choice of j if we fix our desired sum. Thus, if we want to sum to equal $n \le D$, we have $n + 1$ options. To count the total number of possible pairs, we must sum from $n = 0, \dots, D$. This sum is exactly,

$$\sum_{i=0}^{D} i + 1 = \sum_{i=1}^{D+1} i = \binom{D+2}{2}$$

This tells us that $\dim(V) = \binom{D+2}{2}$, as desired. □

Theorem 4.6 (The Polynomial Ham Sandwich Theorem). *[7] Let $A_1, \dots, A_s \subseteq \mathbb{R}^2$ be finite sets, and let D be an integer such that $\binom{D+2}{2} - 1 \ge s$. Then there exists a nonzero polynomial $f \in \mathbb{R}[x, y]$ of degree at most D that simultaneously bisects all the sets of A_i,*

Proof: By Lemma 4.6, $\binom{D+2}{2}$ is the dimension of the vector space of all bivariate real polynomials of degree D. Now, set $k := \binom{D+2}{2} - 1$, and we let $\Phi : \mathbb{R}^2 \to \mathbb{R}^k$ denote the *Veronese map*, given by:

$$\Phi(x, y) := (x^iy^j)_{(i,j)|1\le i+j\le D} \in \mathbb{R}^k$$

We regard the right side as a k-tuple, where each element of the tuple is determined by raising a given x and y to all the possible powers (i, j) where their sum is greater than 1 and less than D. This will give us k pairs as we have just removed the one pairing where $i = j = 0$. We may assume that $s = k$ as $k \le \binom{D+2}{2} - 1$, set $A'_i := \Phi(A_i)$ for $i = 1, 2, \dots, k$, and we let h be a hyperplane simultaneously bisecting $A'_1, \dots, A'_k$. This is guaranteed to exist by the Ham Sandwich Theorem (Theorem 4.5). We know that h is defined as the set of vectors z satisfying, $a_{00} + \sum_{i,j} a_{ij}z_{ij} = 0$, where $(z_{ij})_{(i,j)|1\le i+j\le d}$ are the coordinates in $\mathbb{R}^k$ of a given vector z. We do this to easily think of our embedded vectors, as z_{ij} will correspond to the coordinate in our vectors that equals x^iy^j.

Now let $f(x, y) := \sum_{i,j} a_{ij}x^iy^j$. The zero set of this polynomial splits each subset in the desired fashion. This is because if $f(x, y) = 0$ for some (x, y) this implies that the embedded vector $\Phi(x, y)$ lies on the hyperplane. This results from the definition of the embedding, where each coordinate is a possible monomial of our bivariate polynomial. Thus if (x, y) satisfies our polynomial, and our polynomial has the same coefficients as the hyperplane description, the embedding of (x, y) must be contained in the hyperplane. Similarly, if a vector contained in the hyperplane has a Veronese pre image, the corresponding vector in $\mathbb{R}^2$ will satisfy f. This means that the zero set of our polynomial corresponds directly to the given hyperplane. We can see that in the case where a point in $\mathbb{R}^k$ has a Veronese preimage, the hyperplane and bivariate polynomial are in a sense equivalent. Thus, if we are given a point $x \in A_i'$ "above" our hyperplane, this means that $a_{00} + \sum_{i,j} a_{ij} z_{ij} > 0$, where z_{ij} represents the components of our vector x. We can see that given the corresponding pre image $\Phi(z, y) = x \in A_i'$, which we know exists by our definition of A_i', where $(z, y) \in A_i$, by definition $f(z, y) > 0$. Similarly, if we are given any points $(x, y) \in A_i$ where $f(x, y) > 0$, we can embed it with the Veronese mapping and see that it lies "above" the hyperplane. Equivalent arguments establish the case for points in which $f(x, y) < 0$. Thus as the hyperplane bisects each A_i', the zero set of f must bisect each corresponding A_i. □

Remark 4.3. It is important to note that this the Polynomial Ham Sandwich Theorem could be generalized to Lebesgue-measurable sets by applying the same argument. However, in this case one must carefully account for the relationship between the measure of a set and the corresponding measure of its Veronese Mapping.

Definition 4.13. Let P be a set of m points in the plane, and let r be a parameter, $1 < r \leq n$. We say that $f \in \mathbb{R}[x, y]$ is an *r-partitioning polynomial* for P if no connected component of $\mathbb{R}^2 \setminus Z(f)$ contains more than m/r points of P.

Definition 4.14. We will define the connected components of $\mathbb{R}^2 \setminus Z(f)$ as *cells.*

Theorem 4.7 (Polynomial Partitioning Theorem)**.** *[7] For every $r > 1$, every finite point set $P \subset \mathbb{R}^2$ admits an r-partitioning polynomial f of degree at most $O(\sqrt{r})$.*

Proof: The motivating idea is that we want to inductively utilize the polynomial ham sandwich theorem to find our desired polynomial. We want to construct collections $\mathcal{P}_0, \mathcal{P}_1, \ldots,$ each consisting of disjoint subsets of P, such that $|\mathcal{P}_j| \leq 2^j$ for each j. This means that each collection $\mathcal{P}_j$ contains at most 2^j subsets of P. We start with $\mathcal{P}_0 := \{P\}$. Having constructed $\mathcal{P}_j$, with at most 2^j sets, we use the polynomial ham-sandwich theorem to construct a polynomial f_j of degree $\deg(f_j) \leq \sqrt{2 \cdot 2^j}$, as we have at most 2^j sets and we need D so that $\binom{D+2}{2} - 1 \leq s \leq 2^j$ where s is the number of sets in $\mathcal{P}_j$. By the polynomial ham sandwich theorem this f_j bisects each of the sets of $\mathcal{P}_j$. Now examine all the subsets $Q \in \mathcal{P}_j$, we will let Q^+ and Q^- consist of the points at which $f_j > 0$ and $f_j < 0$ respectively. We will set $\mathcal{P}_{j+1} := \bigcup_{Q \in P_j} \{Q^+, Q^-\}$. In this way, we are essentially evenly splitting each of the sets of $\mathcal{P}_j$ utilizing Theorem 1.4, to construct $\mathcal{P}_{j+1}$ which will result in $|P_{j+1}| \leq 2^{j+1}$ sets.

We can also see that each of the sets in $\mathcal{P}_j$ has size at most $|P|/2^j$, as each of the collections of sets is constructed by starting from the original set P and splitting that set in half with the polynomial ham sandwich theorem. So after j iterations, each set in the collection can have size at most $|P|/2^j$. Now for sake of ease, let $t = \lceil \log_2(r) \rceil$; this means that each of the sets $\mathcal{P}_t$, has size at most $|P|/r$, as $2^t \geq r$. Now set $f := f_1 f_2 \cdots f_t$.

By our construction, no component of $\mathbb{R}^2 \setminus Z(f)$ can contain points of two different sets in $\mathcal{P}_t$, as any arc connecting a point in one subset to a point in another subset must contain a point at which one of the polynomials f_j vanishes, so the arc must cross $Z(f)$. Using the iteration above, we have divided P in each iteration i with the zero set of the polynomial f_i, once we reach the t^{th} iteration, if we multiply all of the polynomials in the preceding steps, we create a polynomial whose zero set is the union of all of the other zero sets. Thus we can see that f is an r-partitioning polynomial for P.

Now we only have to bound the degree to complete the proof:

$$\deg(f) = \sum_{i=1}^{j} \deg(f_j) \leq \sqrt{2}\sum_{j=1}^{t} 2^{j/2} \leq \frac{2}{\sqrt{2}-1}2^{t/2} \leq c\sqrt{r}$$

We get the second inequality because we know that the degree of each $f_i \leq \sqrt{2}2^{j/2}$ by construction. The second inequality is just summing a geometric series:

$$\begin{aligned} \sqrt{2}\cdot\sum_{j=1}^{t}(\sqrt{2})^j &= \sqrt{2}^2\frac{\sqrt{2}^{t+1}-1}{\sqrt{2}-1} \\ &= \frac{2}{\sqrt{2}-1}\cdot(2^{\frac{t+1}{2}}-1) \\ &\leq \frac{2}{\sqrt{2}-1}2^{t/2} \end{aligned}$$

From above, we can let $c = 2\sqrt{2}/(\sqrt{2}-1) < 7$, as we know that $t = \lceil \log_2(r) \rceil$. This completes the proof. $\square$

4.7 Proof of the Szemerédi and Trotter Theorem

We are now ready to prove the Szemerédi and Trotter Theorem. It took a lot of preliminary work, but each lemma and theorem we proved thus far is a tool we will utilize while implementing the polynomial method throughout the remainder of the paper. The myriad number of tools makes the following proof simple and concise. We now present the proof of the Szemerédi and Trotter Theorem, first presented by [13].

Proof: We will first do the proof for $m = n$, and show in this case that $I(P, L) = O(n^{2/3}m^{2/3})$. It is easy from there to indicate the changes necessary to handle an arbitrary m.

We set $r := \lfloor n^{2/3} \rfloor$, and let f be an r-partitioning polynomial for P. By the polynomial partitioning theorem (Theorem 4.7), we know that $D = \deg(f) = O(\sqrt{r}) = O(n^{1/3})$. This is where the choice of r becomes more clear. It will be important soon that the degree of our partitioning polynomial be asymptotically bounded by $n^{1/3}$.

Now let $Z := Z(f)$ the zero set of f; let $C_1, \ldots, C_s$ be the connected components of $\mathbb{R}^2 \setminus Z(f)$; let $P_i := P \cap C_i$, and let $P_0 := P \cap Z$. So now we have partitioned the plane utilizing our polynomial's zero set, and we have created a collection of sets that consists of all of the points of P that are contained in each cell of $\mathbb{R}^2$ we created in our partitioning. Since f is an r-partitioning polynomial, we have that $|P_i| \leq n/r = n^{1/3}$, $i = 1, 2, \ldots, s$. Once again we see the importance of the r we selected. Now the degree of our partitioning polynomial and the number of points in each partition are bounded by the same number. Also, let $L_0 \subset L$ consist of the lines of L contained in Z; we have that $|L_0| \leq D$ by Lemma 4.3 above. Now we can break up $I(P, L)$ and bound each component:

$$I(P, L) = I(P_0, L_0) + I(P_0, L \setminus L_0) + \sum_{i=1}^{s} I(P_i, L)$$

The first piece can be easily bounded:

$$I(P_0, L_0) \leq |L_0| \cdot |P_0| \leq |L_0|n \leq Dn = O(n^{4/3})$$

It is clear that the number of total incidences can be at most the number of points times the number of lines, and we have adequate bounds on both sets. We can also bound the second piece:

$$I(P_0, L \setminus L_0) \leq |L \setminus L_0|D = O(n^{4/3})$$

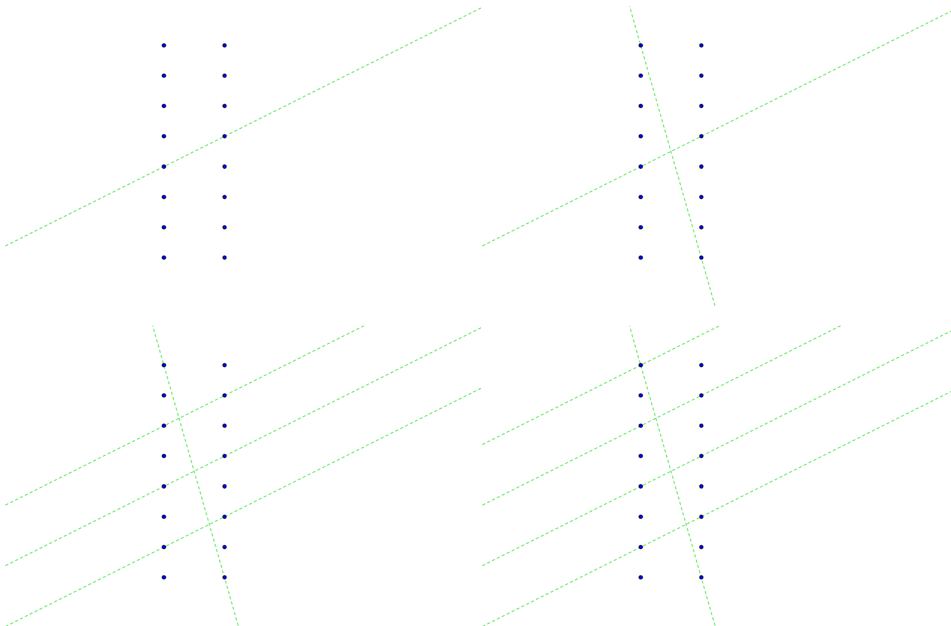
The first inequality follows from the fact that we know each line in $L \setminus L_0$ can only intersect $Z(f)$, and thus the points of P_0 in at most $D = \deg(f)$ points. Otherwise, by the vanishing lemma (Lemma 4.2) above, this would imply that the line was in L_0, which by definition is impossible. So now we are close, it just remains to bound $\sum_{i=1}^{s} I(P_i, L)$. Let $L_i \subset L$ be the set of lines containing at least one point of P_i, it is important to note that the L_i are typically not disjoint as multiple lines can contain points from multiple P_i. By repeatedly applying Lemma 4.1, and summing we know that:

$$\sum_{i=1}^{s} I(P_i, L) \leq \sum_{i=1}^{s} (|L_i| + |P_i|^2)$$

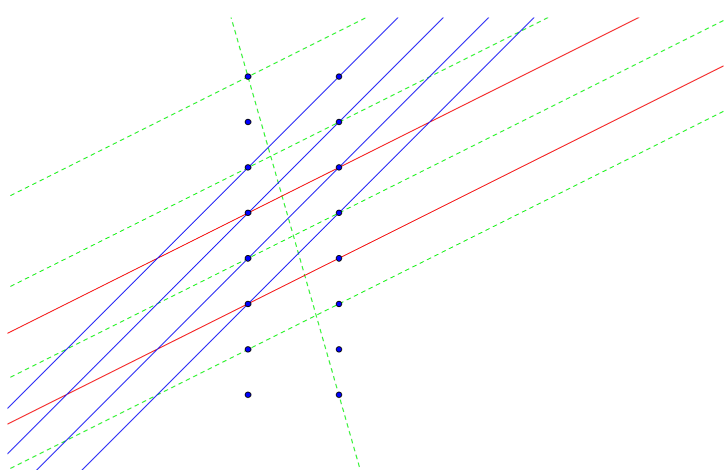
We know that $\sum_{i=1}^{s} |L_i| = O((D+1)n) = O(n^{4/3})$, since by Lemma 4.2, no line in $L \setminus L_0$ intersects more than $D+1$ of the sets P_i, as this would imply that it crossed through Z in more than D places, which would imply that f vanished on L_i, a contradiction. Finally, we can see that $\sum_{i=1}^{s} |P_i|^2 \leq (\max_i |P_i|) \cdot \sum_{i=1}^{s} |P_i| \leq \frac{n}{r} \cdot n = O(n^{4/3})$. The first inequality is clear. We know, however, that the largest a set P_i can be is $\frac{n}{r}$ by Theorem 4.7, and we know that the sum of all of the sets is exactly n. Once again, though, we see the importance of having $r := \lfloor n^{2/3} \rfloor$, as this means that each set contains at most $n^{1/3}$ points, and we are able to extract the same bound on the third component as all the rest. Thus if look at the sum, we see that $I(P, L) = O(n^{4/3}) = O(m^{2/3}n^{2/3} + m + n)$, as desired.

We can generalize the above proof for an arbitrary m as follows. We may assume, without loss of generality, that $m \leq n$; the complementary case is handled by interchanging the roles of P and L by a standard planar duality. In other words, once we know how the points and lines are arranged and where the intersect, we can imagine each point as a line, and each line as a point. Where a line intersects a point in the dual graph if the point was intersected by the line in the original. We may also assume that $\sqrt{n} \leq m$, as otherwise the theorem follows from Lemma 4.1 above. As in this case $n \leq m^2$, so $I(P, L) \leq 2n = O(n^{2/3}m^{2/3} + m + n)$ very easily. So we set $r := \lfloor \frac{m^{4/3}}{n^{2/3}} \rfloor$ (which we quickly note is consistent with the proof above where $m = n$). We also note that $1 \leq r \leq m$ for the assumed range of m because $m \geq \sqrt{n}$. We can then proceed as above where $m = n$. We will have $D = \deg(f) = O(m^{2/3}/n^{1/3})$, and it follows that each of the partial bounds in the proof are at most $O(m^{2/3}n^{2/3})$. $\square$

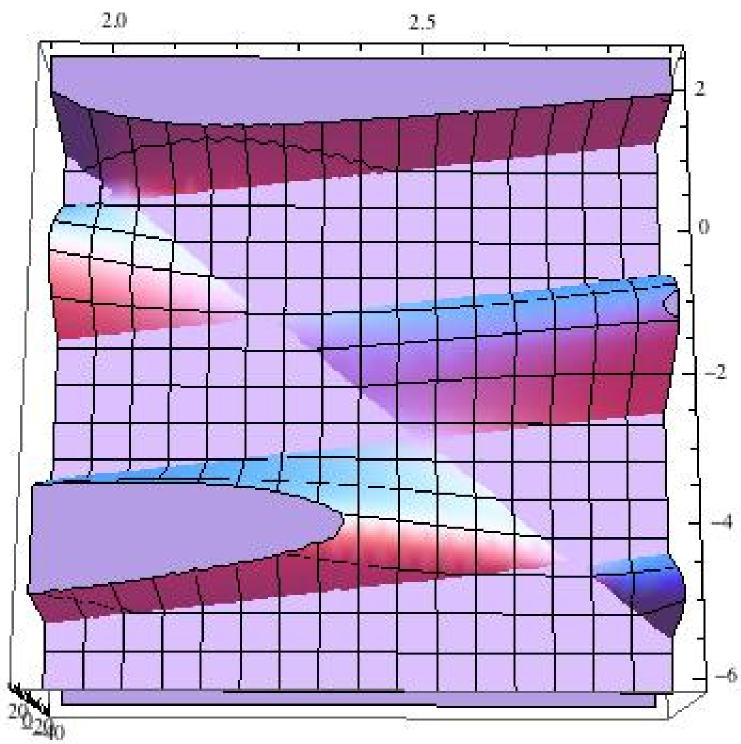
Example 4.5. We will explore how this partitioning technique in the above proof works in practice with the third extremal example described above in the case where $N = 2$. We will have 16 points and 8 lines creating 16 incidences. As $m \neq n$, we will let $r = \lfloor \frac{m^{4/3}}{n^{2/3}} \rfloor = \lfloor \frac{16^{(4/3)}}{8^{2/3}} \rfloor = 10$. We also know, then, that each cell can contain at most $\lfloor \frac{16}{10} \rfloor = 1$ point. So we will create a 10 partitioning in which each cell contains at most one point utilizing the process described in the proof of the polynomial partitioning theorem. The green dashed line will represent the zero set of our constructed polynomial.



We omit $\mathcal{P}_0$ as it is just the set of lines without any partitions. We begin in the top left image with $\mathcal{P}_1$. We can see it has exactly two partitions, each containing less than 9 points. We continue to partition the sets. In the last image, we have added an additional line to get exactly 10 cells, but we can achieve the desired partitioning with one point in each cell with only 8 cells. As we followed the exact process described above, we know that our polynomial will have degree $O(\lfloor \sqrt{10} \rfloor) = O(3)$ as desired. Utilizing this polynomial, we now want to make sure that each section that we separated the incidences into above is actually bounded by $O(16^{2/3}8^{2/3}) = O(25.39)$. We now include all of the lines to directly examine the incidences.

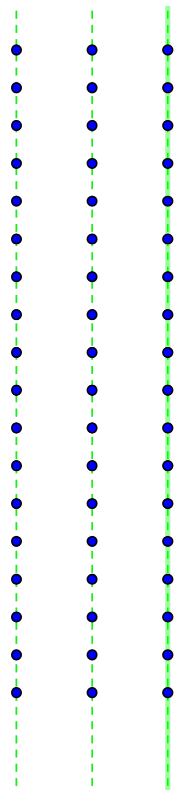


We can see that exactly two of the lines are completely contained within the zero set of our polynomial f. This is allowed, as f is of degree $O(3)$. We also quickly note that f must be of degree ≥ 5, as otherwise more than two lines would vanish, and this would too drastically increase the size of the zero set. We can actually explicitly calculate f, as we have described all of its zero sets as lines. We have $f(x,y) = (y-x+3)(y+7x-15)(y-x+1)(y-x+5)(y-x+7)$, which expands to $f(x,y) = 7x^5 - 27x^4y - 127x^4 + 38x^3y^2 + 380x^3y + 842x^3 - 22x^2y^3 - 378x^2y^2 - 1838x^2y - 2522x^2 + 3xy^4 + 124xy^3 + 1150xy^2 + 3636xy + 3375x + y^5 + y^4 - 154y^3 - 1114y^2 - 2535y - 1575$. As predicted, this polynomial has degree exactly 5. We can see that $I(P_0, L_0) = 4$, $I(P_0, L \setminus L_0) = 4$ and $\sum_{i=1}^{s} I(P_i, L) = 8$, giving us a total of 16 incidences. We notice that each piece is bounded by $O(2^{14/3})$ as desired. If we picture this point line arrangement in the plane, we can plot our polynomial to visualize exactly what we mean by a polynomial bisecting a set of points.



This is the graph of our polynomial $f(x,y)$ with the plane $z = 0$. The intersection shows the lines we had described as the zero set of f. We can see that there are exactly 10 cells. Also note that the picture is consistent with our definition of bisection. i.e. f is positive in 5 cells and negative in 5 cells.

Example 4.6. We will now introduce a general technique for manufacturing an r-partitioning polynomial for the extremal lattice example with $2N^3$ points and N^3 lines. We notice that according to the proof of the Szeméredi and Trotter Theorem, we want $r := \lfloor \frac{2^{4/3}N^4}{N^2} \rfloor = \lfloor 2^{4/3}N^2 \rfloor$. This means that we want a polynomial with degree $O(\sqrt{2^{4/3}N^2}) = O(2^{2/3}N) = O(N)$. We also want each cell to contain $\leq \lfloor \frac{2N^3}{2^{4/3}N^3} \rfloor = \lfloor \frac{N}{2^{1/3}} \rfloor$ points. To achieve this, we can construct the zero set of the polynomial by placing a line through each column of the points in our lattice. This will give us exactly a degree N polynomial as there are N columns in total. We also notice that each cell will contain 0 points, which is clearly less than $\lfloor \frac{N}{2^{1/3}} \rfloor$. We also notice that in this case $I(P_0, L \setminus L_0) = N^4 = O(N^4)$ as desired. We can see an example of this below.



In this case, we do not even need more cells to achieve the result in the proof of the Szeméredi and Trotter Theorem.

5 Incidences of Points with Algebraic Curves

We have just established an asymptotic bound on the number of possible incidence between a given set of points and lines. The next reasonable step is to investigate the possible number of incidences between a set of points and a set of algebraic curves. We will first provide some necessary definitions, which will lead into a discussion of the main result, followed by a presentation of lemmas and proof.

5.1 Definitions and Terminology

Definition 5.1. An *algebraic curve* is a subset of $\mathbb{R}^2$ of the form $\{(x, y) \in \mathbb{R}^2 \mid P(x, y) = 0\}$, where $P(x, y) \in \mathbb{R}[x, y]$ is a bivariate polynomial. In other words, an algebraic curve is the zero set of a real bivariate polynomial.

Definition 5.2. The *degree* of an algebraic curve is the degree of its determining bivariate polynomial.

Definition 5.3. A *simple curve* is any curve described in the plane that does not intersect itself.

5.2 Pach and Sharir's Theorem

We begin this section by presenting the main theorem. This theorem by Pach and Sharir generalizes the Szemerédi and Trotter Theorem to deal with simple curves. The number of incidences in the former case was limited by the fact that no more that one line could pass through any two given points. This is not the case with simple curves.

Theorem 5.1 (Pach and Sharir)**.** *[17] Let P be a set of m points and let Γ be a set of n simple curves, all lying in the plane. If no more that C_1 curves of Γ pass through any k given points, and every pair of curves of Γ intersect in at most C_2 points, then:*

$$I(P, \Gamma) = O(m^{k/(2k-1)} n^{(2k-2)/(2k-1)} + m + n)$$

with an appropriate constant of proportionality that depends on k, C_1, C_2.

This is really an incredible result. We can see that it does agree with the Szemerédi and Trotter Theorem in the case that we only consider lines, which are simple curves. Here, no more than 1 line of Γ can pass through any 2 given points, and every pair of lines intersect in at most 1 point. Thus Pach and Sharir's Theorem tells us that $I(P, \Gamma) = O(m^{2/3}n^{2/3}+m+n)$, the exact bound given by the Szemerédi and Trotter Theorem. We will now investigate some preliminary lemmas and theorems before stating and proving a slightly weaker version of this result.

5.3 Bézout's Theorem

This section acts as an introduction to basic algebraic geometry. We will follow Kirwan's [14] framework and elaborate slightly. Bézout's Theorem is a seminal result concerning the interaction between zero sets of two bivariate polynomials. It is interesting to note that once we substitute algebraic curves for lines, the Fundamental Theorem of Algebra no longer provides the necessary bounds on the zero sets of bivariate polynomials. We were able to use this simpler result by exploiting the line $y = x$ to examine our bivariate polynomials $f(x, y)$ as a single variable polynomial $f(x, x)$. Due to the complexity of Algebraic Curves, this is no longer possible. Thus we must introduce a stronger result: Bézout's Theorem. We will prove that Bézout's Theorem is actually a generalization of the Fundamental Theorem of Algebra which allows us to bridge the gap between lines and algebraic curves. We also note that we can working in P_2 is equivalent to working in $\mathbb{C}^2$ by the section above on projective geometry. This is because any point $(a, b) \in \mathbb{C}^2$ maps to a unique equivalence class $[a, b, 1]$ in P_2. This ability to interchange and exploit qualities of projective spaces will be extremely useful in the following proofs. We will only present a weaker version of the theorem, as it is sufficient for our needs in the following proofs.

Theorem 5.2 (Bézout's Theorem Weaker Version)**.** *Let $f, g \in \mathbb{C}[x, y]$ be two bivariate polynomials of degree D_f and D_g respectively that do not share a common component. Then the system $f = g = 0$ has at most $D_f D_g$ solutions.*

Before we can prove Bézout's Theorem, we must first present some important theory concerning resultants.

5.3.1 Resultants

Definition 5.4. Let

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n$$

where $a_0, \ldots, a_n \in \mathbb{C}$, $a_n \neq 0$, and

$$Q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

where $b_0, \ldots, b_m \in C$, $b_m \neq 0$, be polynomials of degrees n and m in x. The *resultant* $\mathcal{R}_{P,Q}$ of P and Q is the determinant of the $m+n$ by $m+n$ matrix

$$\begin{pmatrix}
a_0 & a_1 & \ldots & a_n & 0 & 0 & & & \ldots & 0 \\
0 & a_0 & a_1 & \ldots & a_n & 0 & & & \ldots & 0 \\
. & & & \ldots & & & & & & . \\
. & & & \ldots & & & & & & . \\
0 & 0 & \ldots & 0 & a_0 & a_1 & & & \ldots & a_n \\
b_0 & b_1 & & \ldots & & b_m & 0 & & \ldots & 0 \\
0 & b_0 & b_1 & & \ldots & & b_m & 0 & \ldots & 0 \\
. & & & \ldots & & & & & & . \\
0 & \ldots & 0 & b_0 & b_1 & & & & \ldots & b_m
\end{pmatrix}$$

If

$$P(x, y, z) = a_0(y, z) + a_1(y, z)x + \cdots + a_n(y, z)x^n$$

and

$$Q(x, y, z) = b_0(y, z) + b_1(y, z)x + \cdots + a_m(y, z)x^m$$

are polynomials in three variables x, y, z then the resultant $\mathcal{R}_{P,Q}(y, z)$ of P and Q with respect to x is defined as a determinant in exactly the same way as $\mathcal{R}_{P,Q}$ was defined above but with $a_i(y, z)$ and $b_j(y, z)$ replacing a_i and b_j for $0 \leq i \leq n$ and $0 \leq j \leq m$.

Remark 5.1. We note that $\mathcal{R}_{P,Q}(y, z)$ is a polynomial in y and z whose value when $y = b$ and $z = c$ is the resultant of the polynomials $P(x, b, c)$ and $Q(x, b, c)$ in x, provided that $a_n(b, c)$ and $b_m(b, c)$ are nonzero.

We will soon provide an equivalent definition of the resultant of two polynomials that is much easier to understand intuitively. We first begin by presenting some important lemmas about resultants.

Lemma 5.1. *If $P(x, y)$ is a nonzero homogeneous polynomial of degree d in two variables with complex coefficients then it factors as a product of linear polynomials.*

$$P(x, y) = \prod_{i=1}^{d} (\alpha_i x + \beta_i y)$$

for some $\alpha_i, \beta_i \in \mathbb{C}$.

Proof: As $P(x, y)$ is homogeneous, we can write

$$P(x,y) = \sum_{r=0}^{d} a_r x^r y^{d-r} = y^d \sum_{r=0}^{d} a_r (\frac{x}{y})^r$$

where $a_0, \dots, a_d \in \mathbb{C}$ are not all zero by assumption. Let e be the largest element of $\{0, \dots, d\}$ such that $a_e \neq 0$. Then

$$\sum_{r=0}^{d} a_r (\frac{x}{r})^r$$

is a polynomial with complex coefficients of degree e in one variable $\frac{x}{y}$. By the Fundamental Theorem of Algebra, we can factorize the above single variable polynomial as

$$\sum_{r=0}^{d} (\frac{x}{y})^r = a_e \prod_{i=1}^{e} \left(\frac{x}{y} - \gamma_i \right)$$

for some $\gamma_1, \dots, \gamma_e \in \mathbb{C}$. Then

$$\begin{aligned} P(x,y) &= a_e y^d \prod_{i=1}^{e} \left(\frac{x}{y} - \gamma_i \right) \\ &= a_e y^{d-e} \prod_{i=1}^{e} (x - \gamma_i y) \end{aligned}$$

This is $P(x, y)$ expressed as a product of linear polynomials. $\square$

Remark 5.2. We were able to utilize the homogeneity of our polynomial to simplify our problem, allowing us to utilize the Fundamental Theorem of Algebra. This trick of proving properties of bivariate polynomials by exploiting a reduction to single variable equivalences will be a recurring practice.

Lemma 5.2. *Let $P(x)$ and $Q(x)$ be polynomials in x. Then $P(x)$ and $Q(x)$ have a non constant common factor if and only if $\mathcal{R}_{P,Q} = 0$. i.e. the above matrix is singular.*

Proof: Let

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n$$

and

$$Q(x) = b_0 + b_1 x + \cdots + a_n x^n$$

be polynomials of degrees n and m in x. Then $P(x)$ and $Q(x)$ have a nonconstant common factor $R(x)$ if and only if there exist polynomials $\phi(x)$ and $\psi(x)$ such that

$$P(x) = R(x)\phi(x), Q(x) = R(x)\psi(x)$$

Where

$$\phi(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}$$

and

$$\psi(x) = \beta_0 + \beta_1 x + \cdots + \beta_{m-1} x^{m-1}$$

We can see that $\deg(\phi(x)) < n$ and $\deg(\psi(x)) < m$ as $P(x)$ and $G(x)$ must have a non-constant common factor. Thus $\deg(R(x)) \geq 1$. We know that $\deg(R(x)) + \deg(\phi(x)) = \deg(P(x)) = n$ and similarly for $G(x)$. Thus $\deg(\phi(x)) < n$ and $\deg(\psi(x)) < m$. The above factorization happens if and only if there exist the same $\psi(x)$ and $\phi(x)$ such that

$$P(x)\psi(x) = R(x)\phi(x)\psi(x) = Q(x)\phi(x)$$

If we equate the coefficients of x^j in the equation $P(x)\psi(x) = Q(x)\phi(x)$, which is equivalent to $\phi(x)\psi(x) = \psi(x)\phi(x)$ for $0 \leq j \leq mn - 1$, we find

$$\begin{aligned}
\alpha_0\beta_0 &= \beta_0\alpha_0 \\
\alpha_0\beta_1 + \alpha_1\beta_0 &= \beta_1\alpha_0 + \beta_0\alpha_1 \\
&\vdots \\
\alpha_n\beta_{m-1} &= \beta_m\alpha_{n-1}
\end{aligned}$$

The existence of a nonzero solution

$$(\alpha_0, \ldots, \alpha_{n-1}, \beta_0, \ldots, \beta_{m-1})$$

to these equations is equivalent to the vanishing of the determinant which defines $\mathcal{R}_{P,Q}$. $\square$

The following lemma is a generalization of the previous to polynomials in three variables. It is important to note that we can assume our polynomials in three variables are homogeneous as we add the third variable for homogenization.

Lemma 5.3. *Let $P(x, y, z)$ and $Q(x, y, z)$ be nonconstant homogeneous polynomials in x, y, z such that*

$$P(1, 0, 0) \neq 0 \neq Q(1, 0, 0)$$

Then $P(x, y, z)$ and $Q(x, y, z)$ have a non constant homogeneous common factor if and only if the polynomial $\mathcal{R}_{P,Q}(y, z)$ in y and z is identically zero.

As we make the shift to polynomials in three variables, we must utilize Gauss' Lemma concerning primitive polynomials. We ultimately want to redefine our three variable polynomials as single variable polynomials, and prove the following results in $\mathbb{C}[x, y]$ (the field of polynomials with complex coefficients). Considering our polynomials over x in this ring is equivalent to considering them in x, y, z with coefficients in $\mathbb{C}$. However, $\mathbb{C}[x, y]$ is a ring and not a field, which restricts our ability to interact with the polynomial. Thus, utilizing Gauss' Lemma, we can relate $\mathbb{C}[x, y]$ to the ring $\mathbb{C}(x, y)$ (the field of rational polynomials with complex coefficients). Gauss' Lemma tells us that if our polynomials share a common factor in $\mathbb{C}(x, y)$, they must also share a common factor in $\mathbb{C}[x, y]$. We will now make this rigorous.

Lemma 5.4 (Gauss' Lemma)**.** *If R is a unique factorization domain and $g(x), h(x) \in R[x]$ are primitive then so is their product $g(x)h(x)$.*

Proof: Let $g(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$ and $h(x) = \beta_0 + \beta_1 x + \cdots + \beta_m x^m$. Suppose for sake of contradiction that $g(x)h(x)$ are nor primitive. This means that the coefficients of $g(x)h(x)$ are divisible by some element $p \in R$ that is greater than the unit element. We can assume as R is a unique factorization domain that this element is irreducible. Since $g(x)$ is primitive, this implies that p does not divide some α_i. Let α_j be the first coefficient of $g(x)$ that p does not divide. Similarly, let β_k be the first coefficient of $h(x)$ that p does not divide. In $f(x)g(x)$, the coefficient of x^{j+k}, c_{j+k} is

$$c_{j+k} = \alpha_j \beta_k + \sum_{i=1}^{k} \alpha_{j+i}\beta_{k-i} + \sum_{i=1}^{j} \alpha_{j-i}\beta_{k+i}$$

We represented c_{j+k} in this way for a reason. By our choice of β_k, $p|\beta_{k-1}, \beta_{k-2}, \ldots, \beta_0$. This implies that $p| \sum_{i=1}^{k} a_{j+i}b_{k-i}$. Similarly, by our choice of α_j, $p|\alpha_{j-1}, \alpha_{j-2}, \ldots, \alpha_0$. This implies that $p| \sum_{i=1}^{j} a_{j-i}b_{k+i}$. We assumed, though, that $p|c_{j+k}$. This means that $p|\alpha_j\alpha_k$. As p is an irreducible element of R a unique factorization domain, this implies that $p|\alpha_j$ or $p|\beta_k$. This is impossible though, as we assumed that p does not divide either. Thus $g(x)h(x)$ is primitive. $\square$

Definition 5.5. Given a polynomial $g(x)$ defined over a unique factorization domain R, we call the greatest common divisor of the coefficients of $g(x)$ the *content* of $g(x)$.

Corollary 5.1. *Let R be a unique factorization domain and K a field containing R such that every element of K can be written as ab^{-1} where $a, b \in \mathbb{R}$ and $b \neq 0$. K is the* field of quotients *of R. If $f(x) \in R[x]$ is primitive then $f(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$.*

Proof: First, suppose that we have some $f(x) \in R[x]$ that is primitive and irreducible in $R[x]$ but reducible in $K[x]$. Thus $f(x) = g(x)h(x)$, where $g(x), h(x) \in K[x]$ of positive degree. As K is the field of quotients of R, we know that $g(x) = (g_0(x)/a)$ and $h(x) = (h_0(x)/b)$ such that $a, b \in R$, and where $g_0(x), h_0(x) \in R[x]$. We also know that $g_0(x) = \alpha g_1(x)$ and $h_0(x) = \beta h_1(x)$ where $\alpha, \beta \in R$ and are the content of $g_0(x)$ and $h_0(x)$ respectively. Thus $g_1(x)$ and $h_1(x)$ are primitive polynomials in $R[x]$. Combining the above we can see that $f(x) = \frac{\alpha\beta}{ab} g_1(x)h_1(x)$. Whence, $abf(x) = \alpha\beta g_1(x)h_1(x)$. By Gauss' Lemma we know that $g_1(x)h_1(x)$ is primitive in $R[x]$ and $K[x]$ as $g_1(x)$ and $g_2(x)$ are. Thus, the content of $\alpha\beta g_1(x)h_1(x)$ is $\alpha\beta$. Since $f(x)$ is primitive, the content of $abf(x)$ is ab. But then $ab = \alpha\beta$. This implies that $f(x) = g_1(x)h_1(x)$ and we have obtained a nontrivial factorization of $f(x)$ in $R[x]$. This contradicts our assumption that $f(x)$ is irreducible in $R[x]$. We note that this factorization is nontrivial is $g_1(x)$ and $h_1(x)$ are of the same degrees as $g(x)$ and $h(x)$ in $R[x]$, as we are only factoring out constants, so they cannot be units.

Now, suppose that we have some $f(x) \in R[x]$ that is primitive and irreducible in $K[x]$. This immediately implies that $f(x)$ is irreducible in $R[x]$ as $R \subset K$. $\square$

Corollary 5.2. *Let R be a unique factorization domain and K its field of quotients. Then two polynomials $f(x)$ and $g(x)$ in $R[x]$ have a nonconstant common factor as elements of $R[x]$ if and only if they have a nonconstant common factor as elements of $K[x]$.*

Proof: Corollary 5.1 immediately implies this result. Assume that $f(x)$ and $g(x)$ in $K[x]$ have a nonconstant common factor $h(x)$. This means that $f(x) = h(x)\phi(x)$ and $g(x) = h(x)\psi(x)$. We can assume without loss of generality that both of these polynomials are primitive (we could just factor our the content). Following the same proof as above, we can prove that $f(x) = \frac{\alpha\beta}{ab}h(x)\phi(x)$ and $g(x) = \frac{\alpha\gamma}{ac}h(x)\psi(x)$ where $h(x), \phi(x), \psi(x) \in R[x]$. This implies that $f(x)$ and $g(x)$ have a nonconstant common factor in $R[x]$. The other direction is trivial as $R \subset K$. □

Now we are ready to prove Lemma 5.3.

Proof: Let $P(x, y, z)$ and $Q(x, y, z)$ be nonconstant homogeneous polynomials in x, y, z of degrees n and m such that

$$P(1, 0, 0) \neq 0 \neq Q(1, 0, 0)$$

We may assume that $P(1, 0, 0) = 1 = Q(1, 0, 0)$ by a simple transformation. Then we can regard P and Q as monic polynomials of degrees n and m in x with coefficients in the ring $\mathbb{C}[y, z]$ of polynomials in y and z with complex coefficients. This ring $\mathbb{C}[y, z]$ is contained in the field $\mathbb{C}(y, z)$ of rational functions of y and z. That is, functions of the form

$$\frac{f(y, z)}{g(y, z)}$$

where $f(y, z)$ and $g(y, z)$ are polynomials in $\mathbb{C}[x, y]$ and $g(y, z)$ is not identically zero. We can see the containment by making g identically one. We must also notice that $\mathbb{C}(x, y)$ is the field of quotients of $\mathbb{C}[x, y]$. Since $\mathbb{C}(y, z)$ is a field the proof of Lemma 2.2 shows that the resultant $\mathcal{R}_{P,Q}(y, z)$ vanishes identically if and only if $P(x, y, z)$ and $Q(x, y, z)$ have a nonconstant common factor when regarded as polynomials in x with coefficients in the field $\mathbb{C}(y, z)$. It follows from Corollary 2.2 to Gauss' Lemma that this happens if and only if $P(x, y, z)$ and $Q(x, y, z)$ have a nonconstant common factor when regarded as polynomials in x with coefficients in $\mathbb{C}[x, y]$, or equivalently as polynomials in x, y, z with coefficients in $\mathbb{C}$. Since any polynomial factor of a homogeneous polynomial is homogeneous [14], the result follows. □

Remark 5.3. We also want to point out that we require

$$P(1, 0, 0) \neq 0 \neq Q(1, 0, 0)$$

So that $P(x, y, z)$ and $Q(x, y, z)$ have the same degree when regarded as polynomials in x with coefficients in $\mathbb{C}[y, z]$ as they do when regarded as polynomials in x, y, z together. This will be important in the coming proof.

Lemma 5.5. *If*

$$P(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

and

$$Q(x) = (x - \beta_1) \cdots (x - \beta_m)$$

where $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m \in \mathbb{C}$*, then*

$$\mathcal{R}_{P,Q} = \prod_{1 \leq i \leq n, 1 \leq j \leq m} (\beta_j - \alpha_i)$$

In particular

$$\mathcal{R}_{P,QR} = \mathcal{R}_{P,Q}\mathcal{R}_{P,R}$$

Where P, Q and R are polynomials in x. The corresponding result is also true when P, Q and R are polynomials in x, y, z.

Proof: In the algebraic closure of $P(x)$ and $Q(x)$, which is necessarily contained in $\mathbb{C}$ we can regard

$$P(x) = (x - \alpha_1)\cdots(x - \alpha_n)$$

and

$$Q(x) = (x - \beta_1)\cdots(x - \beta_m)$$

as homogeneous polynomials in x, $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ then the proof below of Lemma 5.6 shows that the resultant $\mathcal{R}_{P,Q}$ is a homogeneous polynomials of degree nm in the variables $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$. Moreover, by Lemma 2.2, this polynomial vanishes if $\alpha_i = \beta_j$ for any $1 \le i \le n$ and $1 \le j \le m$. As this would imply that $P(x)$ and $Q(x)$ have a nonconstant common factor $(x - \alpha_i) = (x - \beta_j)$. We note that this is a nonconstant factor as we are assuming that α_i and β_j are variables. Thus, $\mathbb{R}_{P,Q}$ is divisible by

$$\prod_{1\le i\le n, 1\le j\le m} (\alpha_i - \beta_j)$$

As it vanishes on each of these sets. Since this is also a homogeneous polynomial of degree nm in $\alpha_1, \ldots, \alpha_n$ and $\beta_1, \ldots, \beta_m$ it must be a scalar multiple of $\mathcal{R}_{P,Q}$. If we let

$$\beta_1 = \beta_2 = \cdots = \beta_m = 0$$

So that $Q(x) = x^m$ then

$$\mathcal{R}_{P,Q} = \prod_{i=1}^{n}(-\alpha_i)^m$$

and

$$\prod_{1\le i\le n, 1\le j\le m} (\alpha_i - \beta_j) = \prod_{i=1}^{n}(-\alpha_i)^m$$

This is because all of the coefficients of $Q(x)$ are 0 except for the first which is one. Thus the determinant of the above matrix yields the above product. This tells us that we must have $\mathcal{R}_{P,Q} = \prod_{1\le i\le n, 1\le j\le m}(\alpha_i - \beta_j)$. We can also see that $\mathcal{R}_{P,QR} = \mathcal{R}_{P,Q}\mathcal{R}_{P,R}$. This is because we now know that $\mathcal{R}_{P,QR} = \prod_{1\le i\le n, 1\le j\le m}(\alpha_i - \beta_j)$ where β_j is all of the roots of the polynomial product QR. However, we can see that this is the same as $\prod_{1\le i\le n, 1\le j\le r}(\alpha_i - \gamma_j) \cdot \prod_{1\le i\le n, 1\le j\le \ell}(\alpha_i - \nu_j)$ where $r + \ell = m = \deg RQ$. Where γ_j are the roots of Q and ν_j are the roots of R. Thus $\mathcal{R}_{P,QR} = \mathcal{R}_{P,Q}\mathcal{R}_{P,R}$. Therefore, if P, Q, R are polynomials in x, y, z we have

$$\mathcal{R}_{P,QR}(b, c) = \mathcal{R}_{P,Q}(b, c)\mathcal{R}_{P,R}(b, c)$$

for all $b, c \in \mathbb{C}$, and so

$$\mathcal{R}_{P,QR}(y, z) = \mathcal{R}_{P,Q}(y, z)\mathcal{R}_{P,R}(y, z)$$

as desired. $\square$

Lemma 5.6. *Let $P(x, y, z)$ and $Q(x, y, z)$ be homogeneous polynomials of degrees n and m respectively in x, y, z. Then the resultant $\mathcal{R}_{P,Q}(y, z)$ is a homogeneous polynomial of degree nm in y and z.*

Proof: By definition, the resultant $\mathcal{R}_{P,Q}(y, z)$ of homogeneous polynomials $P(x, y, z)$ and $Q(x, y, z)$ of degrees n and m is the determinant of an $n + m$ by $n + m$ matrix whose ij^{th} entry $r_{ij}(y, z)$ (where it makes sense to have an entry) is a homogeneous polynomial in y and z of degree d_{ij} given by

$$d_{ij} = \begin{cases} n + i - j & \text{if } 1 \leq i \leq m \\ i - j & \text{if } m + 1 \leq i \leq n + m \end{cases}$$

In other words, the row we are in determines which polynomial we are looking at. That is, if we are in rows 1 through m, we are looking at the homogeneous degree n polynomial $P(x, y, z)$. When we are in rows $m + 1$ through $n + m$ we are examining the coefficients of the homogeneous degree m polynomial $Q(x, y, z)$. So in the first m rows, the sum of x and the homogeneous polynomial $r(y, z)$ must be n. In any given row i, the degree of the x term in the j^{th} row is exactly $j - i$ where it is defined. This is equivalent to our statement in the definition that we place the constant term of the polynomial in the i, j position. Thus we can see that for the first m rows the degree of $r(y, z)$ must be $n+i-j$, as $(n+i-j)+(j-i) = n$ as desired. For the remaining n rows, we can see that the degree of x in a fixed row i and column j is exactly $m + j - i$, as we must account for the fact that we are starting m rows lower. Thus we can see that d_{ij} in this case equals exactly $i - j$ as $(m + j - i) + (i - j) = m$ as desired. This tells us that $\mathcal{R}_{P,Q}(y, z)$ is a sum of terms of the form

$$\pm \prod_{i=1}^{n+m} r_{i\sigma(i)}(y, z)$$

where σ is a permutation of $\{1, \ldots, n+m\}$. This can be seen by utilizing Laplace Expansions. The determinant just a sum of products of the homogeneous polynomials that make up its entries. The permutation allows us to account for ambiguity. We do not need to know the exact form of the resultant to prove this result. We do note that we must have one coefficient from each column by the nature of the Laplace Expansion. We know that each term is a homogeneous polynomial of degree

$$\begin{aligned} \sum_{i=1}^{n+m} d_{i\sigma(i)} &= \sum_{i=1}^{m} (n + i - \sigma(i)) + \sum_{i=m+1}^{m+n} (i - \sigma(i)) \\ &= nm + \sum_{i=1}^{m+n} i - \sum_{i=1}^{m+n} \sigma(i) \\ &= nm \end{aligned}$$

The first equality is easily derived from our above discussion of the degrees of each entry of the matrix. The second equality is a redistribution of the sums. We can just collect all m of the n terms to get nm. We then collect all of the positive i terms, which gives us $\sum_{i=1}^{m+n} i$.

Similarly we collect all of the negative $\sigma(i)$ terms, which gives us $\sum_{i=1}^{m+n} \sigma(i)$. However, if we sum from 1 to $n+m$ a permutation is bijective so we will have each term in our sum. Thus $\sum_{i=1}^{m+n} i - \sigma(i) = 0$. Therefore $\mathcal{R}_{P,Q}$ is a homogeneous polynomial of degree nm in y and z. As the sum of homogeneous polynomials is homogeneous and we just calculated the degree of each term in the sum. □

5.4 Proof of Bézout's Theorem

With the above lemmas, we are ready to prove the weaker form of Bézout's Theorem. The above theorem is equivalent to finding a bound of $D_f D_g$ on the intersections of the algebraic curves described by the zero sets of the polynomials f and g.

Proof: Let C and D be the algebraic curves described by the zero sets of $f(x, y, z)$ and $g(x, y, z)$ respectively. We first suppose that C and D have at least $nm + 1$ points of intersection. We will prove that in this case C and D must have a common component, which contradicts our assumption that they do not. Choose any set S of $nm + 1$ distinct points in $C \cap D$. Then we choose a point p in P_2, the projective real plane, which does not lie on C or on D or on any of the finitely many lines in P_2 passing through two distinct points of S. For sake of ease and application we apply a projective transformation to assume that $p = [1, 0, 0]$. Then the curves C and D are defined by homogeneous polynomials $f(x, y, z)$ and $g(x, y, z)$ of degrees n and m such that

$$f(1, 0, 0) \neq 0 \neq g(1, 0, 0)$$

because $[1, 0, 0]$ does not belong to $C \cup D$. By Lemma 5.5 the resultant $\mathcal{R}_{f,g}(y, z)$ of f and g with respect to x is a homogeneous polynomial of degree nm in y and z. We also know $\mathcal{R}_{f,g}(y, z)$ is not identically zero by Lemma 5.3 as we are assuming that f and g do not share any common component. By Lemma 5.1 then the resultant is the product of nm linear factors of the form $bz - cy$ where $(b, c) \in \mathbb{C}^2 \setminus \{0\}$. Furthermore, if $(b, c) \in \mathbb{C}^2 \setminus \{0\}$, then $bz - cy$ is a factor of $\mathcal{R}_{f,g}(y, z)$ if ant only if the resultant of the polynomials $f(x, b, c)$ and $g(x, b, c)$ in x vanishes. This is because we know the resultant can be written as a product of linear factors of the form $(bz - cy)$. If $bz - cy$ is a factor and we let $z = c$ and $y = b$ the resultant must vanish. However, we can regard $f(x, b, c)$ and $g(x, b, c)$ as polynomials in x, and Lemma 5.3 tells us that they vanish if and only if $f(x, b, c)$ and $g(x, b, c)$ share a common factor. This means that $\exists a \in \mathbb{C}$ such that $f(a, b, c) = 0 = g(a, b, c)$. This string of implications ultimately tells us that $f(a, b, c) = 0 = g(a, b, c)$ if and only if $bz - cy$ is a linear factor of $\mathcal{R}_{f,g}(y, z)$.

Now if $[a, b, c] \in S$ for any possible point $[a, b, c]$, then by definition $f(a, b, c) = 0 = g(a, b, c)$. We also know that b and c are not both zero because $[1, 0, 0]$ does not belong to S, and if b and c were 0, as we were working in projective space $[a, 0, 0] = [1, 0, 0]$. Thus by the above, we have that $bz - cy$ is a linear factor of $\mathcal{R}_{f,g}(y, z)$. Furthermore, if $[\alpha, \beta, \gamma] \in S$ is distinct from $[a, b, c] \in S$ then $\beta z - \gamma y$ is not a scalar multiple of $bz - cy$, because otherwise $[a, b, c]$, $[\alpha, \beta, \gamma]$ and $[1, 0, 0]$ would all lie on the line in P_2 defined by $bz = cy$. This contradicts our assumption that we selected $[1, 0, 0]$ such that it did not lie on any of the finitely many lines passing through two points in S. This shows that for each point in S, there is a distinct linear factor of $\mathcal{R}_{f,g}(y, z)$. As we know that $|S| = nm + 1$, this means that $\mathcal{R}_{f,g}(y, z)$ has $nm + 1$ distinct linear factors. However, we know that $\mathcal{R}_{f,g}(y, z)$ is homogeneous of degree nm. So it can only have $nm + 1$ distinct linear factors if it is identically zero. This, however, implies by Lemma 5.2 that $f(x, y, z)$ and $g(x, y, z)$ have a nonconstant homogeneous common factor. This, as we discussed, is a contradiction. □

Remark 5.4. As mentioned in the beginning, Bézout's Theorem implies the Fundamental Theorem of Algebra. Given any single variable polynomial $f(x)$ of degree n, we can also regard it as a bivariate polynomial $f(x, y)$ of degree n over x and y. If we let $g(x, y) = x - y$. Bézout's Theorem tells us that $f = g = 0$ has at most n solutions. However, $g(x, y) = 0$ when $x = y$. Thus we are looking for the solutions to $f(x, y)$ when $x = y$. This is equivalent to examining the zero set of $f(x)$. This tells us that $f(x)$ vanishes on at most n points. The stronger version of Bézout's Theorem tells us that $f(x)$ vanishes at exactly n points. This is the exact statement of the Fundamental Theorem of Algebra. Incredibly, the stronger version of Bézout's Theorem also tells us that two lines intersect in exactly one point. We recall our discussion of the projective plane above and recognize that given two parallel lines, they will in fact intersect at the point at infinity.

5.5 A Weaker Version of Pach and Sharir's Theorem

We have now made the transition from lines to algebraic curves with Bézout's Theorem. Thus, we are ready to prove a weaker version of Pach and Sharir's Theorem. We note that this version still generalizes the Szeméredi and Trotter theorem, but restricts Pach and Sharir's result to algebraic curves rather than simple curves.

Theorem 5.3. *Let b, k, C be constants, let P be a set of m points in the plane, and let Γ be a family of n planar curves such that*

(a) every $\gamma \in \Gamma$ is an algebraic curve of degree at most b, and

(b) for every k distinct points in the plane, there exist at most C distinct curves in Γ passing through all of them.

Then $I(P, \Gamma) = O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)} + m + n)$, with the constant of proportionality depending on b, k, C.

Before we commence, we must again restrict the range of m and n that we have to consider. We thus introduce a lemma analogous to Lemma 4.1.

Lemma 5.7. *Under the conditions of Theorem 5.3, we have $I(P, \Gamma) = O(n + m^k)$, and also $I(P, \Gamma) = O(m + n^2)$; the constants of proportionality depend on b, k, C.*

Proof: Just as in Lemma 1.1, for the first estimate we divide the planar curves of Γ into two subsets: Γ' consisting of curves with fewer than k incidences, and Γ'' curves with at least k incidences. The first group altogether generates $O(n)$ incidences, as each can generate at most k incidences and there can be at most n curves in Γ'. We also note that there are at most $C\binom{m-1}{k-1}$ curves in Γ'' that intersect each point of P. This is because given any point in P, we know by (b) that there exist at most C distinct curves in Γ passing through k distinct points. However, each curve in Γ'' must pass through at least k distinct points. Thus given any point $p \in P$, we can count the number of possible curves in Γ'' passing through that point by counting all of the possible sets of k distinct points that include p. This is exactly $\binom{m-1}{k-1}$. For each of these sets, we know that there are at most C distinct curves in Γ'' passing through them. Minimally, each curve of Γ'' passes through exactly k points. Thus the number of curves in Γ'' is at most $C\binom{m-1}{k-1}$. Thus the curves of Γ'' generate at most $m \cdot C\binom{m-1}{k-1}$ incidences. We note that $m \cdot C\binom{m-1}{k-1} = O(m) \cdot O(m^{k-1}) = O(m^k)$. This tells us that between our two sets Γ' and Γ'' we have at most $O(n)+O(m^k) = O(n+m^k)$ incidences.

For the second estimate, we first note that we can assume the curves of Γ are irreducible. As if they are not, we can reduce them and apply the following analysis to each irreducible part. As each of the curves are irreducible, by Bézout's Theorem, every pair of curves of Γ intersects in at most b^2 points. This draws upon assumption (a), that each curve has degree at most b. We then divide the points of P into P' consisting of points lying on at most one curve each, and P'' consisting of points lying on at least two curves. We note that P' generates at most $O(m)$ incidences. As there are m points, each generating one incidence. Now if we examine the points in P'', we know they lie at intersections of our algebraic curves. However, by Bézout's Theorem, we know that any $\gamma \in \Gamma$ has at most $b^2(n-1)$ intersections with the other curves. This is because it can intersect every other curve in at most b^2 points. Thus P'' contribute at most $b^2(n-1)$ incidences. As at worst, there could be a point of P'' at each of those points of intersection. However, as b is a constant, we note that $b^2(n-1) = O(n^2)$. Combining, we have that $I(P,\Gamma) = O(m) + O(n^2) = O(m+n^2)$. $\square$

As before, this allows us to prove the following proposition. Notice how similar this is to our previous proposition. The sole change being that we take the k^{th} root of n. We note that this is consistent with our previous bounding of m, where for any 2 distinct points, there exist at most 1 line passing through them, which makes $k = 2$.

Proposition 5.1. *If $m^k \leq n$, then $I(P,\Gamma) = O(n)$*

Proof: If $m^k \leq n$, then Lemma 5.7 implies $I(P,\Gamma) = O(m^k + n) = O(2n) = O(n)$. We can see that in this case Theorem 5.3 is tight, as $O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)} + m + n) = O(n^{1/(2k-1)}n^{(2k-2)/(2k-1)} + n + n) = O(n)$. $\square$

Proposition 5.2. *If $n^2 \leq m$, then $I(P,\Gamma) = O(m)$.*

Proof: If $n^2 \leq m$, then Lemma 5.7 implies $I(P,\Gamma) = O(m+n^2) = O(2m) = O(m)$. We can once again see that Theorem 5.3 is tight in this case, as $O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)} + m + n) = O(m^{k/(2k-1)}m^{(2k-2)/(4k-2)} + m + m) = O(m)$. $\square$

Remark 5.5. Similarly, this means that in order for our Theorem to be correct, these need to be the exact points as which m and n begin to dominate. As within these bounds, the Theorem predicts that $m^{k/(2k-1)}n^{(2k-2)/(2k-1)}$, will begin to dominate. We will once again prove that this is the case. Utilizing this soft bound allows us to restrict our gaze to the interval $\sqrt[k]{n} \leq m \leq n^2$, which will be extremely useful in the following proof.

We are now ready to prove Theorem 5.3. We make a preliminary note that this proof will be extremely similar to the proof of the Szeméredi and Trotter Theorem. This makes sense, as we have made the transition from lines to algebraic curves utilizing Bézout's Theorem, which will allow us to apply the same proof techniques. This ingenious idea highlights the power of mathematical progression.

Proof: As discussed, we may assume that $m \leq n^2$ and that $n \leq m^k$. We then set $r := m^{2k/(2k-1)}/n^{2/(2k-1)}$, and we observe that our assumptions on m, n yield $1 \leq r \leq m$. Let f be an r-partitioning polynomial for P of degree

$$\deg(f) = O(\sqrt{r}) = O(m^{k/(2k-1)}/n^{1/(2k-1)})$$

We now proceed similarly to the proof of the Szemerédi and Trotter Theorem. We let $Z := Z(f)$, $P_0 := P \cap Z$, and let $\Gamma_0 \subset \Gamma$ consist of the curves fully contained in Z. As discussed we may assume that each $\gamma \in \Gamma$ is irreducible, as otherwise we can reduce it and apply the proof to the irreducible components. Thus each $\gamma \in \Gamma_0$ is irreducible. This implies that $\gamma \in \Gamma_0$ must be a zero set of a factor of f. This follows form Bézout's Theorem, as if we let g_γ be the irreducible bivariate polynomial whose zero set describes γ, then we know that g_γ has finite degree. Bézout's Theorem tells us that if g_γ and f do not share a common factor that they intersect in at most $\deg(f)\deg(g)$ places. However, we know that they intersect in infinitely many points, mainly every points in γ. This implies that f and g_γ must share a common component. However, as g_γ is irreducible, this implies that g_γ must be a factor of f. Thus γ is the zero set of the factor g_γ of f. This implies that $|\Gamma_0| \leq \deg(f) = O(\sqrt{r})$, as each curve determines a factor of f and f has at most $\deg(f)$ factors. Thus we have $I(P_0, \Gamma_0) = O(m + |\Gamma_0|^2) = O(m + r) = O(m) = O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)})$ by Lemma 2.7 and the definition of r, as $r \leq m$, and because $m \leq n^2$ and $n \leq m^k$. We quickly note here that we had to utilize a slightly harder technique to bound $I(P_0, \Gamma_0)$, as the trivial bound of $|P_0||\Gamma_0|$ that sufficed in the proof of the Szemerédi and Trotter Theorem would not provide the desired result here.

We next consider $\gamma \in \Gamma \setminus \Gamma_0$. If we apply Bézout's Theorem to γ and every irreducible component of Z in turn, we see that $|\gamma \cap Z| \leq b \cdot \deg(f) = O(\sqrt{r})$. As we know that f cannot vanish on all of γ, and thus they must not share a common component as the bivariate polynomial describing γ is irreducible. This tells us that for any given γ that $|\gamma \cap Z| \leq b \cdot \deg(f)$, as Z is the algebraic curve described by f and by definition each γ is an algebraic curve of degree at most b. This tells us that $I(P_0, \Gamma \setminus \Gamma_0) = O(n\sqrt{r})$ as there are at most n curves in $\Gamma \setminus \Gamma_0$. We notice that $O(n\sqrt{r}) = O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)})$.

Now if we let $C_1, \ldots, C_s$ be the connected components of $\mathbb{R}^2 \setminus Z$, we just have to bound $\sum_{i=1}^{s} I(P_i, \Gamma_i)$, where $P_i = P \cap C_i$ and Γ_i is the set of curves that meet C_i. By Bézout's Theorem, we have $\sum_{i=1}^{s} |\Gamma_i| = O(n \cdot \deg(f)) = O(n\sqrt{r})$. To get a bound on this sum, we know that we are working with n curves at most. So we must ask, how many Γ_i can a single curve be in. We know that if a curve γ appears in two Γ_i that it must intersect Z in at least one place. Thus we see that each γ can be in at most $b \cdot \deg(f) + 1 = O(\deg(f))$ Γ_i by Bézout's Theorem. This tells us that as there are n total curves that if we sum the number of curves in all of the Γ_i that there are at most $O(n) \cdot O(\deg(f)) = O(n \cdot \deg(f))$ curves. Thus by Lemma 2.7, we have

$$\sum_{i=1}^{s} I(P_i, \Gamma_i) = O\left(\sum_{i=1}^{s}(|\Gamma_i| + |P_i|^k)\right) \leq O(n\sqrt{r}) + (\max_i |P_i|)^{k-1} O\left(\sum_{i=1}^{s} |P_i|\right)$$
$$= O(n\sqrt{r} + (m/r)^{k-1}m) = O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)}).$$

If we combine all of the above results, it tells us that $I(P, \Gamma) = O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)})$. $\square$

Remark 5.6. It is incredible that we do not need a stronger version of Bézout's Theorem to prove this result. The mere bound on the number of incidences provides the necessary information. This proves that within our unknown interval where m and n are no longer greater than $m^{k/(2k-1)}n^{(2k-2)/(2k-1)}$ the number of incidences is bounded by $O(m^{k/(2k-1)}n^{(2k-2)/(2k-1)})$. Thus this weaker form of Pach and Sharir's Theorem is sharp in all cases.

6 Spanning Trees and Welzl's Theorem

This section deals with a Theorem originally proved by Chazelle and Welzl. We will first provide a few definitions

Definition 6.1. We say that a topological space X is *arcwise connected* if for any points $a, b \in X$, there exists a homeomorphism $f : [0, 1] \to X$ such that $f(0) = a$ and $f(1) = b$.

Remark 6.1. We note that this is a stronger connection than the usual path-connectedness discussed in Topology. In order for a topological space to be *path-connected*, there has to exist a continuous function from $[0, 1]$ to X whose initial point is a and final point is b. Arcwise connected requires the existence of a homeomorphism, i.e. there must also exist a continuous inverse and f must be bijective. To see an example illustrating the difference take the set $X = \{a, b\}$, with the trivial topology. It is path connected but not arc wise connected. As the function $f : [0, 1] \to X$ defined by $f(t) = a$ for $t \neq 1$ and $f(t) = b$ for $t = 1$ is a path from a to b that is continuous (as the pre image of any open set is open). However, we note that there cannot exist a homeomorphism from $[0, 1]$ to X since injectivity is impossible.

Definition 6.2. Let P be a finite set of points in $\mathbb{R}^2$. A *geometric graph* of P is a graph G with vertex set P whose edges are realized as straight segments connecting the respective end-vertices. A *geometric spanning tree* on P is an acyclic connected geometric graph on P.

Definition 6.3. Let X be an arc wise connected set made of segments and algebraic arcs that contains the point set P. We say that a set $X \subset \mathbb{R}^d$ has *crossing number* at most k if each line, possibly with finitely many exceptions, intersects X in at most k points. An equivalent definition is that the crossing number of a geometric graph G whose vertices are represented by a point set P is the maximum number of edges that can be intersected simultaneously by a line not passing through any point of P.

With these definitions in mind, we are now ready to present Welzl's Theorem:

Theorem 6.1 (Welzl [24]). *Every set of n points in the plane has a geometric spanning tree with crossing number $O(\sqrt{n})$*

In this section, we begin to explore the breadth of applications for the Polynomial Method. The weaker form of Pach and Sharir's Theorem was a generalization of the Szemerédi and Trotter Theorem, and thus we could say it makes sense for the polynomial method to apply to both with the added tool of Bézout's Theorem. However, this problem utilizes the Polynomial Method to construct geometric spanning trees with reasonable crossing number. The only common theme being a limit on crossing. Our knowledge of the zero set of bivariate polynomials should lead us to think we can control a crossing number by lowering the number of points in each cell of our decomposition. Before we can prove this Theorem, we will need to provide some terminology. We also must prove another important Theorem concerning the number of possible (arc wise) connected components of $Z(f)$ for a given bivariate polynomial f.

6.1 Harnack's Curve Theorem

As mentioned above, this theorem allows us to bound the number of components of the zero set of an r-partitioning polynomial f. We already have all of the tools necessary to prove this fairly easily. The general idea is to fix a variable in the bivariate polynomials to consider them as a single variable polynomial so we can apply basic theorems from Calculus.

Theorem 6.2 (Harnack's Curve Theorem [8, 13]). *Let $f \in \mathbb{R}[x, y]$ be a bivariate polynomial of degree D. Then the number of (arc wise) connected components of $Z(f)$ is at most $1 + \binom{D-1}{2}$. The bound is tight in the worst case.*

Proof: We will begin by bounding the number of bounded components of $Z(f)$. We choose an arbitrary direction, assuming without loss of generality that it is the x-direction. We may assume that f is square-free, because eliminating repeated factors of f does not change its zero set. We notice that every bounded component of $Z(f)$ has at least two extreme points in the x-direction as we are working with an arc wise connected bounded component. We also know that such an extreme point has to satisfy $f = f_y = 0$, as we know the boundary points are dictated by the zero set of f. We can see that $f_y = 0$ as we know the directional derivative on our curve in the x direction is maximal. This tells us that

$$\nabla f \cdot < 1, 0 >= \frac{df}{dx}$$

Is the maximal rate of change at those extremal values. However, we also know that the magnitude of the gradient is the maximal rate of change at a given point this tells us that

$$\sqrt{(\frac{df}{dx})^2 + (\frac{df}{dy})^2} = ||\nabla f|| = \frac{df}{dx}$$

This implies that $\frac{df}{dy} = 0$ as desired. Here f_y is the partial derivative of f with respect to y. Since f is square free, f and f_y have no common factor [12], and so by Bézout's Theorem, the system $f = f_y = 0$ has at most $D(D-1)$ solutions. As f_y will have degree at most $D-1$

assuming f has degree D. We know that every bounded component consumes at least two of these critical points, as each bounded component has at least two extreme values and that is where $f = f_y = 0$. Thus we can see that the number of bounded components of $Z(f)$ is at most $\frac{1}{2}D(D-1) = O(D^2)$.

If B is a sufficiently large number, then if we are assuming generic directions of the coordinate axes every unbounded component of $Z(f)$ meets at least one of the two lines $x = \pm B$. Thus, there are at most $2D$ unbounded components, and in total we get a bound of $\frac{1}{2}D(D+1)$ on all components. $\square$

6.2 Preliminary Lemmas

With a simplified form of Harnack's Curve Theorem allowing us to bound the number of cells created by our r-partitioning polynomial, we will now begin to approach the Lemma. The original proof of this Lemma involved the iterative construction of the Geometric Spanning tree [24]. In order to create this spanning tree, however, we want to convert the zero set of our r-partitioning polynomial with a fairly low crossing number for the point set P into a geometric spanning tree. The following Lemmas allow us to do this. We will first introduce the Steiner Tree, as it will be essential in the proof of the following Lemma.

Definition 6.4. Given a point set P, we say that S is a *Steiner Tree* for P if S connects all of the points in P by lines of minimal length in such a way that any two points may be interconnected by line segments either directly or by the addition of other points and line segments. These other points are called *Steiner Vertices.*

Remark 6.2. We note that this is extremely similar to creating a minimal spanning tree for a set of vertices P, and in some cases the minimal spanning tree and the Steiner Tree are the same, but in most they are not.

Lemma 6.1 (Euler's Theorem)**.** *In a connected graph where every vertex has even degree, there exists an Eulerian Circuit.*

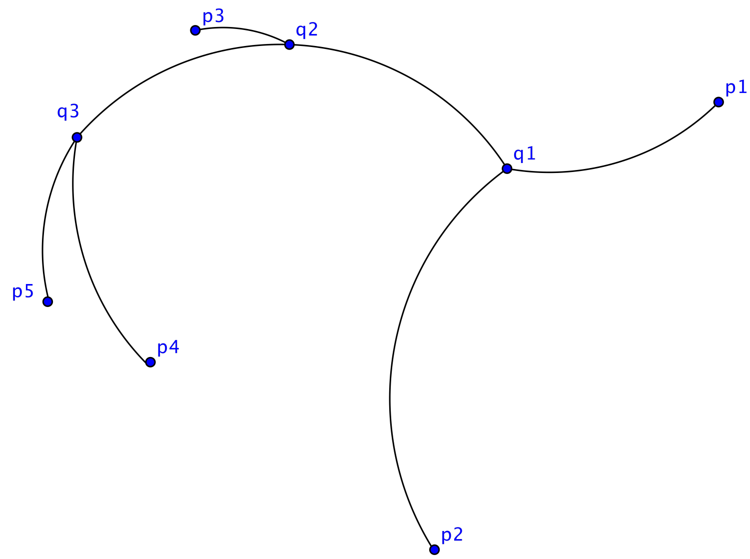
Proof: Suppose that we have a graph G with even degree vertices. We will prove this by induction on the number of edges in the graph. In order for every vertex to have even degree we know that there have to be at least two edges that form a two-cycle. This is the base case, clearly if there are two vertices with a duplicated edge between them there is an Eulerian Circuit. Now suppose we have a graph G on $n > 2$ edges. We designate an arbitrary root vertex v in G and follow edges, arbitrarily selecting one edge after another until we return to v. Call this trail W. We know that we can return to v eventually as every time we encounter a vertex that is not v, we are listing one edge adjacent to it. As there are an even number of edges adjacent to each vertex there will always be a suitable edge to list next. In other words, we will never get stuck at a vertex that is not v, as if we could reach the vertex by construction there must be an edge to leave on. We note that if W includes every edge in G we are done as this is our Eulerian Circuit.

Otherwise, let E be the edges of W. The graph $G \setminus E$ has components $C_1, \ldots, C_k$. We note that each component satisfies the induction hypothesis. It must be connected, as otherwise we would have designated it as two or more different components, it has less than m edges as it is a subset of G and by definition our walk W contains at least two edges. We also note that every vertex in each component has even degree. We know that every vertex has even degree because every vertex in our walk W has even degree by construction. Thus when we removed these edges from G, we are removing an even amount of edges from vertices of even degree. This means that the vertices will still all have even degree.

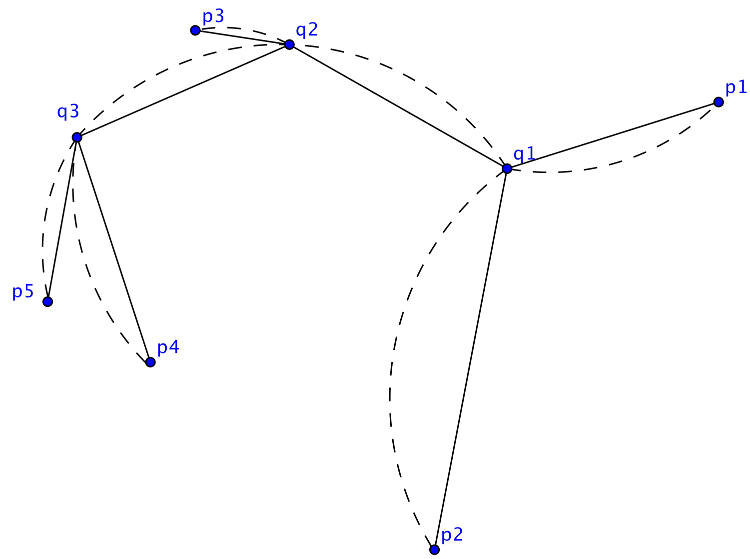
By induction, each component has an Eulerian Circuit $E_1, \ldots, E_k$. As G is connected, there is a vertex a_i in each component C_i on both our walk W and the circuit E_i (as otherwise we could separate the graph). Without loss of generality, assume that as we follow W, the vertices $a_1, \ldots, a_k$ are encountered in that order. If this is not the case we can just relabel. We now create an Eulerian Circuit in G by starting at v, following W until we reach a_1, following the entire circuit E_1 ending back at a_1, and then continuing to follow W until reaching a_2, where we then follow the entire circuit E_2. We continue this process until we have reached a_k, follow E_k, end up at a_k again and follow W back to v. We note that in this way we use every edge exactly once. This shows that there exists an Eulerian Circuit in G. This completes our induction step, and the result follows for any connected graph G with even degree vertices on any number of edges by induction. □

Lemma 6.2. *Let P be a set of n points in the plane, and let X be an arc wise connected set containing P, with crossing number at most k. Then there exists a geometric spanning tree of P whose edges are straight segments and whose crossing number is at most $2k$.*

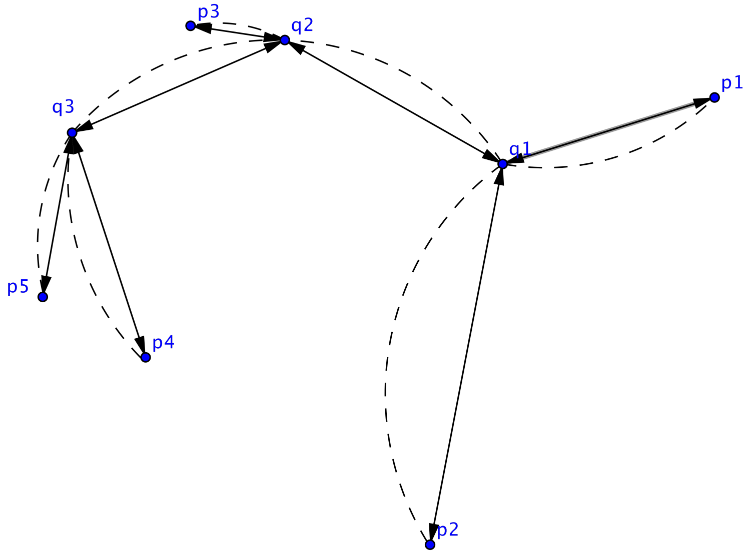
Proof: We will algorithmically construct this spanning tree. In the first stage of the proof, we will construct a Steiner tree S for P, whose edges are arcs contained in X. For sake of ease, we will order the points of P arbitrarily to create a sequence $p_1, \ldots, p_n$. We will set $S_1 = \{p_1\}$, and, having iteratively built a Steiner tree $S_i \subset X$ for $\{p_1, \ldots, p_i\}$, we choose an arc $\alpha_i \subset X$ connecting p_{i+1} to some point q_i of S_i, in such a way that $\alpha_i \cap S_i = \{q_i\}$. We know such an α_i exists as $S_i \subset X$, and $P \subset X$. Thus there is some arc α_i in X that connects the existing S_i to p_{i+1}. We can choose this arc to only intersect S_i at q_i almost trivially. Then we set $S_{i+1} := S_i \cap \alpha_i$. Having reached $i = n$, we set $S := S_n$. This is demonstrated in the figure below



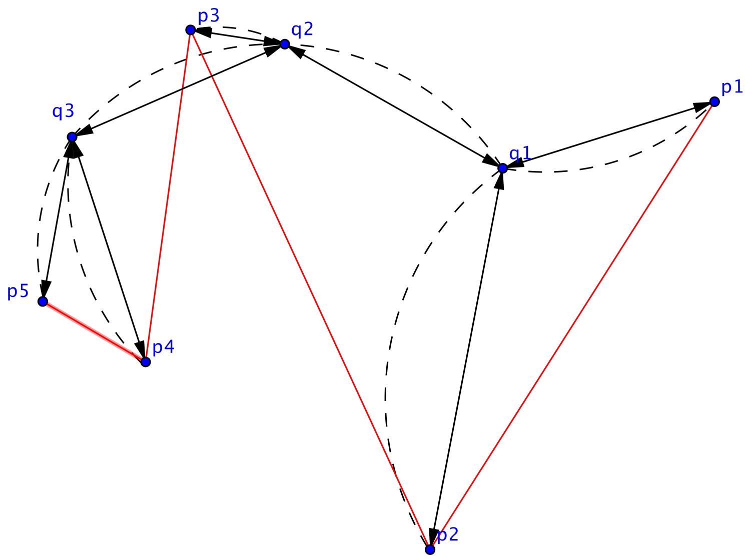
We also note that the crossing number of S is at most k since $S \subseteq X$ and X has crossing number at most k. Now in the second stage of our construction, we replace arcs by straight segments. We do this by noticing that the points q_j divide S into finitely many sub arcs, and we replace each of them by a straight segments connecting its endpoints. It is easily seen that the crossing number does not increase [13]. This yields a Steiner tree for P whose edges are straight segments. We note that we cannot necessarily construct a normal spanning tree in this way as we need the potential Steiner vertices to allow $S_i \subseteq X$ in our first stage. As a continuation of our example, we can see this process below.



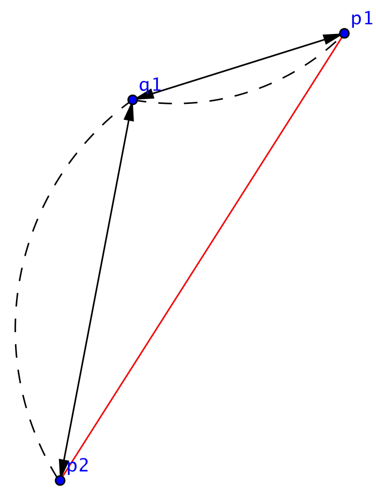
In the third and final stage, we will eliminate the Steiner vertices and obtain a normal spanning tree, at the price of at most doubling the crossing number. This is done by performing an in order traversal of the tree. We designate an arbitrary root vertex of the tree and arbitrarily order the vertices of the constructed Steiner tree. Starting from our arbitrary root vertex, we trace each edge in both directions, skipping over the Steiner points, and connect each pair of consecutively visited points of P by a straight segment. The image below illustrates exactly what we mean by tracing each edge in both directions. The idea is we start at a root, want to reach each other vertex from this root and return to the root. This is equivalent to doubling all of the edges in our graph and finding an Eulerian Circuit in the resulting graph. We know we can do this by Lemma 3.1 as all of the vertices in our graph would have even degree. This Eulerian Circuit in the newly created graph is equivalent to a closed walk where we use each edge exactly twice as desired. We are following this path in our tree and connecting the points from P that we visit. After we have completed our walk and created all of the segments between P, we eliminate any cycles that we may have created in our walk. In this way, we at most double the crossing number. We can see the traversal process below



We have chosen the root vertex to be p_1. We can see the tree that this traversal creates below.



The constructed tree is in red. Now we notice that depending on the choice of root vertex we could end up constructing a different spanning tree. We note, however, that each of these trees can at most double the crossing number that our Steiner tree had. This is the case because if we look at every edge in our new graph, we can follow the train between edges in our steiner tree that led between the two vertices we ultimately connected in our final tree. The idea behind this is seen below:



This is the component that is associated to our first edge. It consists of two edges of our original graph. Minimally the component can consist of one edge if the edge in our new tree is already an edge in the old tree. If we add in all of the components of our Steiner Tree that we picked up in order to connect edges in our new tree during our walk, we will at most have two copies of each edge from our Steiner tree. This is because we used each edge exactly twice. We also notice that we must always have at least one copy of each edge. Now, we see that in order for a line to intersect an edge in our new graph, it must intersect the component associated to that graph. However, as these components are part of the original tree, we know that the line can only cross k unique edges of the components. As each edge can appear in at most two unique components, this implies that any line can intersect at most $2k$ components which correspond to new edges in our spanning tree. Thus the crossing number of our spanning tree at most doubles. $\square$

Now we have the ability to create a Spanning tree for a point set contained within an arc wise connected set X that has crossing number at most twice that of X. Now we will utilize the Polynomial Method to construct such a point set with a low crossing number.

Lemma 6.3. *Let P be a set of n points in the plane. Then there exists a set $X \subset \mathbb{R}^2$ that contains P, has at most $n/2$ arc wise connected components, and crossing number $O(\sqrt{n})$.*

Proof: If n is below a suitable constant, we can interconnect the points of P by an arbitrary geometric spanning tree that will satisfy our requirements for the Theorem. Thus we may assume that n is large. We now apply the polynomial partitioning theorem to obtain an r-partitioning polynomial f for P. We want r as large as possible, while also requiring that $Z := Z(f)$ is guaranteed to have at most $n/2$ connected components. We know we can do this because we have $\deg(f) = O(\sqrt{r})$, and so by Harnack's theorem, we can take $r = n/c$ for a suitable constant c. The idea is that we want each cell to contain as few points of P as possible, while also controlling the number of cells that are created. Harnack's Curve Theorem relates the degree of f to the number of connected components of Z, telling us that the number of connected components is $O(\deg(f)^2) = O(r)$. Thus if we make $r = n/c$ for a correct constant c, this allows us to maximize r while making sure there are less than $n/2$ components.

Then, for every $p \in P$ not lying in Z, we pick a straight segment α_p connecting p to a point of Z. Just as above we also require that α_p intersects Z in only one point. We let $X := Z \cup \bigcup_{p \in P \setminus Z} \alpha_p$. Clearly, X has at most $n/2$ components by construction as adding these α_p does not increase the number of connected components. It remains to bound the crossing number of X.

Let ℓ be a line that is not contained in Z and that does not contain any of the segments α_p. We notice that these conditions exclude only finite many lines as above we bounded the number of lines that can be contained in Z, and we know there are only finitely many segments α_p as there are only finitely many points in P. We notice that ℓ intersects Z in at most $\deg(f) = O(\sqrt{n})$ points, as $r = n/c$. We know that if ℓ is not contained in Z by the vanishing lemma it must only intersect Z in at most $\deg(f)$ points. So it remains to bound the number of segments α_p intersected by ℓ.

Since f is an r-partitioning polynomial for P, no component of $\mathbb{R}^2 \setminus Z$ contains more than c points of P as $r = n/c$. The line ℓ meets at most $1 + \deg(f)$ components as discussed, so it intersects at most $c(1 + \deg(f)) = O(\sqrt{n})$ of the segments of α_p. Adding, this tells that any arbitrary line crosses X in at most $O(\sqrt{n})$ places. $\square$

Remark 6.3. This is really incredible. By maximizing r, we maximized the number of cells and minimized the number of points in each cell. In this way we were able to utilize the vanishing lemma and this small bound on the number of points in each cell to see that any line could intersect our constructed set X in at most $O(\sqrt{n})$ points.

6.3 Proof of Welzl's Theorem

With these two lemmas, we can now easily prove Welzl's Theorem.

Proof: Given Lemma 6.1, we notice that it suffices to construct an arc wise connected set X containing P, with crossing number $O(\sqrt{n})$. We notice the set X constructed in Lemma 6.2 has at most $n/2$ arc wise connected components. We want to iteratively apply this Lemma to construct an arc wise connected set.

Thus we construct a sequence $A_0, A_1, \ldots$ of sets such that each A_i contains P and has a t most $n/2^i$ arc wise connected components. We begin with $A_0 := P$, and having constructed A_i we choose a point in each of its components. This yields a set R_i of at most $n/2_i$ points. Lemma 3.2 then provides us with a set X_i such that $R_i \subset X_i$ with at most $n/2^{i+1}$ components and crossing number $O(\sqrt{n/2^i})$. We set $A_{i+1} := A_i \cup X_i$ and continue with the next iteration. Eventually for some j we reach an arc wise connected A_j, which we use as X. We notice that this must happen as there are $n/2^i$ connected components in A_i, thus if we reach j such that $2^j \geq n$ this implies that A_j will have 1 connected component. The crossing numbers of the X_i are bounded by a geometrically decreasing sequence, and we see that X has crossing number bounded by its sum. This sum is exactly $O(\sqrt{n})$ as desired. $\square$

Remark 6.4. The key here was to start with our point set and repeatedly apply the polynomial partitioning theorem to construct these sets X_i that will eventually yield a completely connected set that contains P. The polynomial partitioning theorem allows us to control the crossing number as mentioned above. We can then use Lemma 6.1 to create the desired spanning tree.

7 The Joints Problem

We will now transition into a discussion of the Joints Problem. In the Szemerédi and Trotter Theorem section, we were calculating the number of possible incidences between sets of points and lines. In the Joints Problem, we now consider the issue of bounding the number of intersections between a set of N lines when we restrict our view to only considering intersections of three of more linearly independent lines. These points of intersection will be referred to as joints:

Definition 7.1. Given a set of lines L, we define a *joint* as a point where three lines with linearly independent directions intersect.

We can see that given a $\sqrt{\frac{N}{3}} \times \sqrt{\frac{N}{3}} \times \sqrt{\frac{N}{3}}$ cube in the integer lattice, we get N lines with $\frac{N^{3/2}}{3\sqrt{3}}$ joints by simply taking all lines in coordinate directions which intersect the cube and the lattice. Each point of the integer lattice that intersects with our cube will generate a joint, and there are exactly $\left(\sqrt{\frac{N}{3}}\right)^3 = \frac{N^{3/2}}{3\sqrt{3}}$ points. This acts as our extremal example for the joints problem, just as the integer lattice acted as our extremal example for the Szemerédi and Trotter Theorem. We notice that this makes sense, as before we were looking for intersections of two lines, so we examined the integer lattice in $\mathbb{R}^2$. Now if we want to maximize the number of times intersections of three lines occur the natural step is to look at the integer lattice cube in $\mathbb{R}^3$. The joints conjecture emerged form this line of thinking, and posited that the integer cube is in fact the worst possible case. In 2008, Larry Guth and Nets Katz proved the Joints conjecture stated below more rigorously as a Theorem:

Theorem 7.1. *[6] Any set of N lines in $\mathbb{R}^3$ form at most $O(N^{3/2})$ joints.*

7.1 Generalization of our Techniques to $\mathbb{R}^3$

We already have most of the algebraic techniques necessary to complete the proof of the Joints Problem. However, our current weakened form of Bézout's Theorem only works in $\mathbb{C}^2$ where we have two polynomials in $\mathbb{C}[x_1, x_2]$ the vanish on many similar points. We need to generalize Bézout's Theorem one step further so that it works in $\mathbb{C}^3$ when two polynomials in $\mathbb{C}[x_1, x_2, x_3]$ vanish simultaneously on many lines. Before we proved that if two bivariate polynomials vanish on many similar points, they must share a line on which they both vanish. Now we will prove that if two trivariate polynomials vanish on many lines, they must share a plane on which they both vanish. The proof of this is similar to the above, as it utilizes the technique of considering these multivariable polynomials as single variable polynomials with coefficients in the other variables and applying the techniques with resultants to obtain the desired result. We first need a quick definition.

Definition 7.2. We say that a plane and a line *intersect transversally* if at every point of intersection, their separate tangent spaces at the point together generate the tangent space of the ambient manifold at that point.

Lemma 7.1. *Let f and g be elements of $\mathbb{C}[x_1, x_2, x_3]$ and suppose that f and g have positive degrees l and m respectively. Suppose there are more than lm lines on which f and g simultaneously vanish identically. Then f and g have a common factor.*

Proof: Without loss of generality, we may choose x_1 so that f and g have positive degree in x_1. As they must have positive degree in one of the variables, so we will call this variable x_1. We can also choose x_3 so that the plane $x_3 = 0$ is transverse to at least $lm + 1$ of the lines of vanishing. We can see that at least one variable must have this property as we assumed that f and g vanish simultaneously on more than lm lines, and thus if we look at a plane, up to a simple change of variables for the polynomials we can find a transverse plane. Fixing x_3 and applying Bézout's Theorem, we have that the polynomials f and g with x_3 fixed now considered as polynomials in $\mathbb{C}[x_1, x_2]$ intersect in at least $lm + 1$ points. Thus they share a common component. Thus if we consider f and g as polynomials in x_1 with coefficients in x_2 and x_3, by definition 2.4 above we see that the $R_{f,g}(x_2, x_3)$ is a bivariate polynomial in x_2 and x_3. We also see that if we we fix $x_3 = c$ for some $c \in \mathbb{C}$, that f and g as polynomials in x_1 now have coefficients in x_2 alone, and thus as we know that they share a common component for any fixed x_3, by Lemma 5.2, $R_{f,g}(x_2) = 0$. However, as this is true for any $x_3 = c$ that we chose, this implies that $R_{f,g}(x_2, x_3) = 0$ identically. Thus by Lemma 2.3, we have that $f(x_1, x_2, x_3)$ and $g(x_1, x_2, x_3)$ have a nonconstant homogeneous common factor as desired. $\square$

Now we will prove the real analog of this lemma. We will only use the result below, but we needed the complex version to prove the real version.

Corollary 7.1. *Let f and g be elements of $\mathbb{R}[x_1, x_2, x_3]$, and suppose that f and g have positive degrees l and m respectively. Suppose that there are more than lm lines on which f and g simultaneous vanish identically. Then f and g have a common factor.*

Proof: We can think of f and g as elements of $\mathbb{C}[x_1, x_2, x_3]$, and they must vanish on more than lm complex lines of $\mathbb{C}^3$ as any real line is a complex line. By Lemma 5.3, f and g

must have a common factor h in $\mathbb{C}[x_1, x_2, x_3]$. We can assume h is irreducible. We cannot, however, assume that h is real. If it is real we are done If h is non-real, then the irreducible factorization of f must contain both h and $\overline{h}$. As it is a well known fact that if a polynomial has a common complex factor, it must also contain the complex conjugate of h, $\overline{h}$. Thus, f is divisible by the real polynomial $h\overline{h}$, and similarly so is g. Thus they share a common real nontrivial factor. $\square$

We will now prove a result similar to Lemma 4.3 above dealing with polynomials in $\mathbb{R}[x, y, z]$. We first provide a few definitions

Definition 7.3. Let f be a nontrivial irreducible polynomial in $\mathbb{R}[x, y, z]$ of degree $D > 0$. We say that a point $a \in Z(f)$ is *critical* if $\nabla f(a) = 0$, where this is the gradient of f. Otherwise, we say that a is *regular*.

Definition 7.4. Similarly, we say that a line ℓ is *critical* if $\ell \subset S$ and every point of ℓ is critical.

Proposition 7.1 (Joint's Property). *If $f \in \mathbb{R}[x, y, z]$ is a trivariate polynomial that vanishes on three non coplanar lines that define a joint j, ∇f also vanishes at j. Up to a simple shift of variable we may assume without loss of generality that these non coplanar lines point in the x, y and z directions respectively. Say our three lines are ℓ_1, ℓ_2, ℓ_3. If f vanishes when restricted to ℓ_1, we obtain the fact that $\nabla f \cdot v|_{\ell_1} = 0$ where v is the direction of ℓ_1, which we have assumed is the x-direction. Thus $f_x = 0$. Similarly, when we restrict to ℓ_2 and ℓ_3 we get that $f_y = f_z = 0$. Thus at each joint $\nabla f = 0$.*

Proof: If f vanishes on three non-coplanar lines, this means that it must have a critical point at their intersection. Up to a simple change of variable we may assume without loss of generality that these three different directions are the x, y and z directions. As f vanishes $\square$

We can now prove the extension of Lemma 4.3

Lemma 7.2. *Given an irreducible polynomial $f \in \mathbb{R}[x, y, z]$ of degree D, the set $Z(f)$ contains no more than $D(D-1)$ critical lines.*

Proof: Suppose this is not the case. We examine f and a nontrivial component of ∇f which will have degree at most $D-1$. We know that $Z(f)$ contains more that $D(D-1)$ lines, thus f and ∇f vanish on more than $D(D-1)$ lines, as every point on those lines is critical and by definition this means that $\nabla f = 0$. By Bézout's Theorem, we see that f and ∇f must have a common factor. However if f and its gradient share a common factor, this implies that f contains a square [12], which is a contradiction to the irreducibility of f. Thus $Z(f)$ cannot contain more than $D(D-1)$ critical lines. $\square$

7.2 Combinatorial Background

Next, we must introduce some combinatorial lemmas essential for the upcoming proof. First we will provide some basic definitions. For further reading we refer the reader to [9].

Definition 7.5. We define a *graph* G as a *vertex set* $V(G)$ paired with an *edge set* $E(G)$, we say $G = (V, E)$. Where the vertex set is some collection of points, and the edge set consists of pairs of points in the vertex set. Each pair in the edge set represents an edge in the graph.

Definition 7.6. We say that a graph is *bipartite* if its vertex set V can be partitioned into two subsets X and Y such that every edge in $E(G)$ consists of a pairing (x, y) where $x \in X$ and $y \in Y$.

Definition 7.7. The *degree* of a vertex $v \in V(G)$ is equal to the number of pairs in $E(G)$ in which v is present. In other words, the number of edges that are incident to v.

Lemma 7.3. *Let (X, Y, E) be a bipartite graph with E the edges and X and Y the two sets of vertices. Suppose that $|E| > \rho|Y|$. Let Y' be the set of vertices of Y having degree at least μ and let E' be the set of edges in E between Y' and X. Then*

$$|E'| > (\rho - \mu)|Y|$$

Proof: We notice that the vertices in $Y \setminus Y'$ are incident to at most $\mu|Y|$ edges in total as otherwise they would be included in Y'. Since the total number of edges $|E| > \rho|Y|$ we can see that

$$|E'| > |E| - \mu|Y| > \rho|Y| - \mu|Y| = (\rho - \mu)|Y|$$

As desired. □

Lemma 7.4. *Let $x_1, \ldots, x_m$ be positive quantities and $y_1, \ldots, y_m$ positive quantities, then there is an integer $1 \leq k \leq m$ so that*

$$\frac{x_k}{y_k} \geq \frac{\sum_{j=1}^m x_j}{\sum_{j=1}^m y_j}$$

Proof: Suppose that this is not the case. Let $\rho = \frac{\sum_{j=1}^m x_j}{\sum_{j=1}^m y_j}$. Then $x_k < \rho y_k$ for all k. Thus we have that

$$\sum_{j=1}^m x_j < \rho \sum_{j=1}^m y_j$$

This is clearly impossible as we know that ρ equals this implies that

$$\rho > \frac{\sum_{j=1}^m x_j}{\sum_{j=1}^m y_j} = \rho$$

□

7.3 Proof of the Joints Problem

We now have the tools necessary to attack the Joints Problem. We will first present the original proof of Guth and Katz [6] as published in 2008. We will then discuss a recent development that utilized the same ideas and massively simplified the proof. First we will state an important fact

Fact 7.1. $\binom{n}{k} \leq \frac{n^k}{k!}$

Proof: Suppose that we are given a set of lines L of cardinality N. Let J be the set of joints determined by L. We suppose that $|J| \geq KN^{3/2}$ with K a large, but universal, constant. We ultimately hope to arrive at a contradiction.

We create a bipartite, three-colored graph (L, J, R, G, B). Where our first vertex set X consists of the set of joints and our second vertex set Y consists of a vertex for each line. We draw an edge between a vertex in X and a vertex in Y if a line in Y is incident to a joint in X. In this way we see that each joint vertex in X has degree at least three, as it is formed by three non coplanar lines by definition. For each joint, we arbitrarily color one of its incident edges red, one green, and one blue. We know we can do this as we just said that each of these vertices has degree at least three. The sets R, G, and B consist of, respectively, the red, green, and blue edges.

We will now refine these sets slightly. We let L_R be the set of lines which have at least $\frac{K}{1000}N^{1/2}$ indecencies in R. In other words, a line can only be in L_R if its corresponding vertex in Y has at least $\frac{K}{1000}N^{1/2}$ red edges incident to it. We let J_R be the set of joints having a red incidence with aline of L_R. In this way we restrict some of the joints, as not every red edge connects a joint to line that has many red edges incident to it. By Lemma 4.3,

$$|J_R| \geq \frac{999}{1000}|J|$$

This is the case because we know that there are at least $3|J|$ edges, so we can let $\rho = 3|J|$, and there each edge in L_R has degree at least $\frac{K}{1000}N^{1/2}$ by construction, so $\mu = \frac{K}{1000}N^{1/2}$ and once again we know that $|Y| \geq 3|J|$, we also note that each edge between L_R and X must correspond to a unique joint as each joint only has one red edge by construction, thus if we can find a lower bound on the number of edges we find a lower bound on the number of joints in J_R

$$|J_R| \geq (|Y| - \frac{K}{1000}N^{1/2})|Y| \geq (3|J| - \frac{1}{1000}|J|)(3|J|) \geq \frac{999}{1000}|J|$$

As desired using Lemma 4.3. Now let L_G and L_B be those lines having respectively at least $\frac{K}{1000}N^{1/2}$ green or blue incidences with joints in J_R. In this way we know that each of these lines intersects a joint that also intersects a line in L_R. We could have easily selected green or blue as our base color and the same results would follow. We let J' denote the set of joints which has red, green, and blue incidences with lines in L_G and L_B. Once again by Lemma 4.3, we can see that

$$|J'| \geq \frac{99}{100}|J|$$

This is the case for a similar reason as above. This time we restrict our bipartite graph to be the set of joints in J_R and the vertices of the sets of lines in L_R, L_G and L_B. We have a lower bound on J_R in terms of J, and we know how many incidences the vertices in J_R must have with each of the vertices in L_R, L_G and L_B. A fairly simple lower bound can then be obtained. We now want to produce a polynomial of relatively low degree vanishing on all the points of J'. We say a line ℓ of L_G and L_B meets a line ℓ' of L_R if $\ell \cap \ell'$ is a joint of J_R. Each line of L_G and each line of L_B meets at least $\frac{K}{1000}N^{1/2}$ lines of L_R by construction. We now take a random subset L'_R of the lines of L_R, picking each line with probability $\frac{1}{K}$.

By the law of large numbers, with positive probability, the following events occur. Each line of L_G and L_B must meet at least $\frac{1}{2000}N^{1/2}$ lies of L'_R and

$$|L'_R| \leq \frac{2N}{K}$$

The Law of Large Numbers essentially states that if we perform an experiment enough times the average of the results will be close to the expected value. Thus if we take enough random subsets of L_R we can find one with the above qualities. We now make a set of points S by selection $\frac{1}{2}N^{1/2}$ points of each line L'_R. Then

$$|S| \leq \frac{N^{3/2}}{K}$$

This is clear as there are at most $\frac{2N}{K}$ lines and we are selection $\frac{1}{2}N^{1/2}$ points from each. We now find a polynomial p which vanishes on all poitns of S. By the estimate on the size of S, we may select p with degree $O(\frac{N^{1/2}}{k^{1/3}})$. This is the case as we need $\binom{D+3}{3} - 1 > \frac{N^{3/2}}{K}$, this implies we can take $D = O(\frac{N^{1/2}}{k^{1/3}})$ by the above fact. With K sufficiently large, this means that p must vanish on each line of L'_R by the vanishing lemma as each line contains $\frac{1}{2}N^{1/2}$. We also notice that because of the number of lines of L'_R that each line of L_G and L_B meet, it means that p must vanish identically on each line of L_G and L_B by the vanishing lemma again. Therefore, the polynomial p must vanish on the entire set J'.

Now, it is not necessarily the case that p is irreducible. Thus we factor p into irreducibles

$$p = \prod_{j=1}^{m} p_j$$

We denote the degree of the polynomial p_j by d_j and observe that

$$\sum_{j=1}^{m} d_j = O(\frac{N^{1/2}}{K^{1/3}})$$

This is clear as we know that the sum of these degrees equals the degree of the original polynomial p. We let J_j be the set of J' on which p_j vanishes, and we have that

$$\sum_{j=1}^{m} |J_j| = \Omega(KN^{3/2})$$

Thus we have that

$$\frac{\sum_{j=1}^{m} |J_j|}{\sum_{j=1}^{m} d_j} = \Omega(K^{4/3}N)$$

By Lemma 7.4 this implies that we can find a j for which $|J_j| = \Omega(K^{4/3}Nd_j)$. From now one we will restrict our attention to J_j. We denote by $L_{R,j}$, $L_{G,j}$, and $L_{B,j}$ those lines in L_R, L_B and L_G which are incident to at least $d_j + 1$ elements of J_j, and we let J'_j be those elements of J_j incident to a line each from $L_{R,j}$, $L_{G,j}$, and $L_{B,j}$. With K sufficiently large by the same logic as above we have

$$|J'_j| \geq \frac{999}{1000}|J_j|$$

We now define $L'_{R,j}$, $L'_{G,j}$, and $L'_{B,j}$ as the set of lines which are incident to more than $d_j + 1$ points of J'_j. We define J''_j to be the set of joints defined by these lines. We have

$$|J''_j| \geq \frac{99}{100}|J_j|$$

We now consider two cases. First, if there are fewer than d_j^2 lines in each of $L'_{R,j}$, $L'_{G,j}$, and $L'_{B,j}$. In this case, we start over again, having a joints problem with fewer liens and more favorable exponents than the original. We can see that the above process is easily utterable and we just continue to restrict our sets until we reach our contradiction.

In the second case, we may assume without loss of generality that $L'_{R,j}$ contains at least d_j^2 lines. By the definition of $L_{R,j}$, $L_{G,j}$, and $L_{B,j}$, the polynomial p_j vanishes identically on each one in these sets. However, this implies that each point of J'_j is a critical point of p_j because otherwise it would be impossible for p_j to vanish on three, intersection, non-coplanar lines. As is proved in the Joints Property above. This, however, implies that each component of the gradient of p_j vanishes at each point of J'_j. let q be one of the components of the gradient which does not vanish identically. We know that this must exist as p_j is not constant. Then q has degree at most $d_j - 1$. Thus, it must vanish on every line of $L'_{R,j}$. But this contradicts Proposition 7.2, as this implies that p_j is reducible. $\square$

7.4 The New Proof

The Polynomial Method is evolving so quickly that often when one proof is produced, mathematicians quickly refine the techniques to produce a more succinct proof. As evidenced by the new proof below presented by René Quilodrán in 2009 [18]. The motivating idea is that we want to find a *soft line* that is incident to less than $2j^{1/3}$ joints where j is the number of joints. If we can always find such a line, we will then be able to bound the total number of joints based off of the number of lines. This is the essence of the above proof, and the proof of the following lemma follows almost directly from the end of the above proof.

Lemma 7.5. *Given a set of N lines $\ell_1, \ldots, \ell_N$, L that form j joints, we can find a line ℓ_i that is incident to less than or equal to $2j^{1/3}$ joints.*

Proof: Suppose for sake of contradiction that this is not the case. In other words assume that every line is incident to $> 2j^{1/3}$ joints. We will now find a polynomial p that vanishes on all of the joints with minimal degree. As there are j joints and we are now working in $\mathbb{R}^3$ we want to find a degree D such that $\binom{D+3}{3} - 1 > j$. However by our above fact we know that

$\binom{D+3}{3} - 1 \le \frac{(D+3)^3}{6} - 1$. Thus we want $D > \sqrt[3]{6} j^{1/3} + 6^{1/3} - 3$, so we can choose $D = 2j^{1/3}$. By the polynomial ham sandwich theorem, we can find a polynomial that vanishes on all of the joints with degree $D = 2j^{1/3}$. As we want to choose the degree of our polynomial minimally this implies that $D < 2j^{1/3}$. However, by the vanishing lemma, as each line contains more than $2j^{1/3}$ joints this means that f must vanish completely on each line. By the *Joints Property*, we know that each joint is incident to at least three non-coplanar lines. This implies that f vanishes on three non-coplanar lines, i.e. in three non coplanar directions at each joint. Just as in the above proof that the gradient of f, ∇f must vanish on each joint, as f can only vanish in three non coplanar directions at a point if that point is an extremal value of f by the Joints Property above. We also know that as f is not a constant function by construction that one of the elements of ∇f must be nontrivial. Let's say that it is f_x without loss of generality. We can see that f_x is a polynomial of degree $D - 1$ that vanishes on every joint. However, we chose f so that it has minimal degree. This is a contradiction. So there must exist a line that is incident to at most $2j^{1/3}$ joints. □

With this lemma, we can now easily prove the Joints Theorem. The new proof is given below.

Proof: Given our N lines we can write them $\ell_1, \ldots, \ell_N$. Say they form j joints. We know that amongst these lines by the above lemma there exists a line ℓ_i such that ℓ_i is incident to at most $2j^{1/3}$ joints. If we say without loss of generality that this is line 1, we can now examine the set of lines $\ell_2, \ldots, \ell_N$, and reapply the lemma. If we do this inductively, we know that for each set there exists a line that is incident to less than or equal to $j^{1/3}$ joints. As there will be a total of N iterations we have

$$2Nj^{1/3} > j$$

This implies that $j < 2^{3/2} N^{3/2}$. As desired. □

We notice that neither of the above proofs actually prove that the grid graph is the worst possible scenario. As this would imply that $j < \frac{N^{3/2}}{\sqrt{27}}$. We will investigate a sharper bound to prove that the grid graph is the worst case example.

8 The Distinct Distances Problem

We are now ready to approach arguably the greatest problem solved by the polynomial method: The Distinct Distances Problem. Posed by Paul Erdős in 1946 [5], and finally solved in 2013 by Guth and Katz [7], the polynomial method did not provide an alternative proof, but rather the first and only answer to the distinct distances problem. In order for it to become applicable a massive process of contextual shifts had to occur in order to reframe the question in terms of incidences between lines and points in $\mathbb{R}^3$. We will first state the theorem. We will then work through the proofs in Guth and Katz's paper [7] explaining and piecing them together in a slightly different fashion.

8.1 Statement of the Theorem

In his 1946 paper [5], Erdős conjectures that the number of distinct distances determined by m points in the plane is $\gtrsim \frac{m}{\sqrt{\log m}}$. However in 2013 Guth and Katz were able to prove the following:

Theorem 8.1 (Guth and Katz [7])**.** *A set of m points in the plane determines $\gtrsim \frac{m}{\log m}$ distinct distances.*

The rest of this chapter will be dedicated to carefully examining the proof of this theorem. We notice that Guth and Katz's lower bound is slightly different from Erdős's conjecture. We will later go over how Guth and Katz's argument works on the square grid that Erdős founded his conjecture upon, and show that their estimate is actually sharp up to constant factors. We will now provide some definitions to begin the process of the aforementioned contextual shift.

8.2 A Contextual Shift

Elekes and Sharir are really the pioneers of the contextual shift we are about to discuss. We follow a string of relations to simplify the problem. Before we do so we will quickly introduce some notation for sake of ease.

Definition 8.1. Let P be a set of points. We denote by $d(P)$ the set of distinct distances determined by the points in P.

We are now ready to make our first reduction by defining a quadruple.

Definition 8.2. Given a set of points P, we say that a subset of points $(p_1, p_2, p_3, p_4) \in P^4$ is a *quadruple* if $d(p_1, p_2) = d(p_3, p_4) \neq 0$. The collection of all quadruples for a given set of points P is denoted $Q(P)$.

We notice that given two pairs of points who are equal distance from each other, say $(p_1, p_2) = d(p_3, p_4)$, they define eight different quadruples at least. That is (p_1, p_2, p_3, p_4), (p_3, p_4, p_1, p_2), and all other permutations where pairs must be adjacent in the first two or last two spots are valid and distinct quadruples. We also notice that given one pair of points at any distance we can define a quadruple using that pair. We define such a group because the number of quadruples is intimately related to the number of distinct distances. Intuitively we can see that if the number of distinct distances is large, the number of quadruples should be relatively small as there would not be many pairs of points at equal distance. We can make this exact with the following Lemma.

Lemma 8.1. *For any set $P \subset \mathbb{R}^2$ with m points,*

$$|d(P)| \geq \frac{m^4 - 2m^3}{|Q(P)|}$$

Proof: Consider the distances in $d(P)$. We will denote them by $d_1, \ldots, d_n$, assuming here that $|d(P)| = n$. There are exactly $m^2 - m$ ordered pairs $(p_i, p_j) \in P^2$ with $p_i \neq p_j$. This is easily seen as we have m choices for the first point and then $m-1$ choices for the second point. Let k_i be the number of these pairs that are at a distance d_i from one another. We can see then that

$$\sum_{i=1}^{n} k_i = m^2 - m$$

If we sum over all of the possible distances we will by necessity get every pair of points and we know there are exactly $m^2 - m$ points.

Now we notice that the cardinality of $|Q(p)|$ is equal to $\sum_{i=1}^{n} k_i^2$. This is because for each element of k_i we want all pairs such that the distance between the first two points equals the distance between the second two. If we limit our view to each subcategory k_i we want to select two pairs of points, one for the first slot in the quadruple and one for the second. There are exactly k_i^2 ways to choose these two pairs of points as we discussed above that we can choose the same pair of points twice. Thus these points determine exactly k_i^2 quadruples. If we sum over all possible distinct distance we can count all quadruples. Now we notice that by the Cauchy-Schwartz inequality

$$(m^2 - m)^2 = (\sum_{i=1}^{n} k_i)^2 \leq (\sum_{i=1}^{n} k_i^2)n = |Q(P)||d(P)|$$

If we divide through and rearrange we have

$$|d(P)| \geq \frac{m^4 - 2m^3 + m^2}{|Q(P)|} \geq \frac{m^4 - 2m^3}{|Q(P)|}$$

As desired. □

With this relationship, we can now provide a lower bound on $|d(P)$ by establishing an upper bound on $|Q(P)|$. Using this lemma we can now prove Theorem 8.1 by establishing the following upper bound on $|Q(P)|$.

Proposition 8.1. *For any $P \subset \mathbb{R}^2$ of m points, the number of quadruples in $Q(P)$ is bounded by $|Q(P)| \lesssim m^3 \log(m)$.*

We notice that if this is the case applying Lemma 7.1 we have

$$|d(P)| \geq \frac{m^4 - 2m^3}{|Q(P)|} \gtrsim \frac{m^4 - 2m^3}{m^3 \log(m)} = \frac{m-2}{\log(m)}$$

Which is the exact inequality we desire. We will now make our next reduction by relating this set of quadruples to a group of positively oriented rigid motions of the plane. We will define exactly what this is now.

Definition 8.3. A *rigid motion* is the action of taking an object and moving it to a different location without altering its shape and size. Examples of a rigid motion are reflection, rotation, translation and glide reflections. Actually, all rigid motions can be created by some combination of those four movements.

Definition 8.4. We say that a rigid motion is *positively oriented* if the plane after we alter it defined by v_1, v_2 satisfies $(v_1 \times v_2) \cdot e_3 > 0$.

We will now define an extremely important group that is surprisingly closely related to our set of quadruples that allows us to study the set of quadruples in relation to symmetries of the plane in $\mathbb{R}^3$.

Definition 8.5. Let G denote the group of positively oriented rigid motions of the plane in $\mathbb{R}^3$.

This reduction and connection is made possible by the following proposition.

Proposition 8.2. *Let (p_1, p_2, p_3, p_4) be a distance quadruple in $Q(P)$. Then there exists a unique positively oriented rigid motion $g \in G$ such that $g(p_1) = p_3$ and $g(p_2) = p_4$.*

Proof: The existence of such a rigid motion is fairly obvious and easy to prove, its uniqueness is what will be extremely useful. We notice that all positively oriented rigid motions taking p_1 to p_3 can be obtained from the translation from p_1 to p_3 and then rotating the resulting plane about p_3. We want to show that the rigid motion that sends p_1 to p_3 and the resulting rotation that sends the translated p_2 to p_4 is unique. Since $d(p_3, p_4) = d(p_1, p_2) > 0$ we know that there exists a unique rotation sending the point $p_2 + p_3 - p_1$ to p_4. As we shift p_2 up by $p_3 - p_1$ since we are shifting the entire plane on which p_1 and p_2 are defined up by $p_3 - p_1$ in order to translate p_1 to p_3. We can then rotate the plane about p_3 to move this point $p_2 + p_3 - p_1$ to p_4 because the distance from p_1 to p_2 is equal to $d(p_3, p_2 + p_3 - p_1)$ as the distances between corresponding points were not changed in translation. This tells us that $d(p_3, p_2 + p_3 - p_1) = d(p_1, p_2) = d(p_3, p_4)$, so there exists a unique rotation about p_3 that sends our translated p_2 to p_4. Thus we have constructively shown that there is a unique rigid motion g such that $g(p_1) = p_3$ and $g(p_2) = p_4$. □

Now using Proposition 8.2 we can define a map $E : Q(P) \to G$ in the following way.

Definition 8.6. Given a set of quadruples $Q(P)$ we define a map $E : Q(P) \to G$ the group of positively oriented rigid motions of the plane by $E((p_1, p_2, p_3, p_4)) = g$ where $g(p_1) = p_3$ and $g(p_2) = p_4$.

We know that this map is well defined by the uniqueness proved in Proposition 8.2. We want to use E to estimate $|Q(P)|$ by counting appropriate rigid motions of the plane. It is important to note that E is not necessarily injective. We could easily have the same rigid motion for different quadruples. We notice that the number of quadruples in $E^{-1}(g)$ depends on the size of $P \cap g(P)$. This makes sense as we would expect that more quadruples would map to a rigid motion if that rigid motion 'preserves' more points in our point set P. We will make this explicit now.

Lemma 8.2. *Suppose $g \in G$ is a rigid motion of the plane and that $|P \cap g(P)| = k$. Then the number of quadruples in $E^{-1}(g) = 2\binom{k}{2}$.*

Proof: Suppose that $P \cap g(P) = \{q_1, \ldots, q_k\}$. Let $p_i = g^{-1}(q_i)$. Since $q_i \in g(P)$, each point p_i lies in P. For any ordered pair (q_i, q_j) with $q_i \neq q_j$, the set (p_i, p_j, q_i, q_j) is a distance quadruple. This is theca ace because we know that $p_i, p_j, q_i, q_j \in P$ by definition. We also know that

g preserves distances, thus as $q_i = g(p_i)$ and $q_j = g(p_j)$ we know that $d(p_i, p_j) = d(q_i, q_j)$. Since $q_i \neq q_j$ we know that $d(q_i, q_j) \neq 0$ and so this is a well defined distance quadruple.

Now we need to check that every distance quadruple in $E^{-1}(g)$ is of this form. Once we do this, we can easily count the number of quadruples in the pre image of g under E. Let (p_1, p_2, p_3, p_4) be a distance quadruple in $E^{-1}(g)$. We know that $g(p_1) = p_3$ and that $g(p_2) = p_4$ by definition of E. So $p_3, p_4 \in P \cap g(P)$. Say $p_3 = q_i$ and $p_4 = q_j$. Now we can see that $p_1 = g^{-1}(q_i) = p_i$ and $p_2 = g^{-1}(p_4) = p_j$. This implies that our quadruple is actually of the form (p_i, p_j, q_i, q_j) as desired.

Now that we know every possible quadruple in the pre image of g under E is of the above form we will count all such quadruples. We can do this by selecting q_i, q_j from $P \cap g(P)$ in $\binom{k}{2}$ possible ways. For each one we get two possible quadruples as we can order q_i, q_j in 2 ways. Alternatively we could count the number of quadruples by selecting q_i, for which we have k options, and q_j for which we have $(k-1)$ options as we cannot have $q_i = q_j$. Either way this gives us a total of $k(k-1) = 2\binom{k}{2}$ options. Each selection will define a quadruple as p_i and p_j are uniquely determined by q_i and q_j. □

We now have a relationship between quadruples and rigid motions defined by our mapping. We will use this to count the number of quadruples in an alternative way. However, we notice that in order to use Lemma 8.2 we need to divide our rigid motions based on how many points of P they preserve. We accomplish this with the following definition.

Definition 8.7. Let $G_{=k}(P) \subset G$ be the set of $g \in G$ with $|P \cap g(P)| = k$.

Notice that $G_{=m}(P)$ is a subgroup of G as it is the set of all $g \in G$ such that all points overlap. It is the group of orientation-preserving symmetries of P. We also notice that for other k, $G_{=k}(P)$ is not a group, but these sets can still be regarded as *partial symmetries* of P. Since P has m elements, $G_{=k}(P)$ is empty if we take $k > m$. With this definition and Lemma 7.2 we can now could $Q(P)$ in terms of $G_{=k}(P)$.

Proposition 8.3. $|Q(P)| = \sum_{k=2}^{m} 2\binom{k}{2}|G_{=k}(P)|$

Proof: This is the case as for each $g \in G_{=k}(P)$ we know that there are exactly $2\binom{k}{2}$ quadruples in its pre image by Lemma 8.2. We also know that if $k > m$ that $G_{=k}(P) = 0$. Thus to count all possible quadruples it suffices to count all of the possible rigid motions in each $G_{=k}(P)$ where $2 \leq k \leq m$ and multiply each by $2\binom{k}{2}$. We notice that $k \geq 2$ as otherwise we could not have a quadruple as at least two points must overlap. □

Now we would like to rewrite this in a slightly easier way. Rather than considering all partial symmetries that preserve exactly k points of P, we would like to consider the sets of partial symmetries that preserve $\geq k$ points of P. This motivates the following definition.

Definition 8.8. Let $G_k(P) \subset G$ be the set of $g \in G$ such that $|P \cap g(P)| \geq k$.

We can see that $G_{=k}(P) = |G_k(P)| - |G_{k+1}(P)|$. Substituting this in to Proposition 8.3 we can count our quadruples in terms of $G_k(P)$.

Proposition 8.4. $|Q(P)| = \sum_{k=2}^{m}(2k-2)|G_k(P)|$

Proof: From Proposition 8.3 we know that $|Q(P)| = \sum_{k=2}^{m} 2\binom{k}{2}|G_{=k}(P)|$. As noted above we can see that $G_{=k}(P) = |G_k(P)| - |G_{k+1}(P)|$. Substituting this in we have

$$|Q(P)| = \sum_{k=2}^{m} 2\binom{k}{2}(|G_k(P)| - |G_{k+1}(P)|) = \sum_{k=2}^{m}(2k-2)|G_k(P)|$$

We get the last equality by examining the two coefficients of each $G_k(P)$, with the exception of $G_2(P)$ which only occurs once, with coefficient 2 which is exactly $2 * 2 - 2$. For every other k $G_k(P)$ appears exactly once as when $k = m$ $G_{m+1} = 0$ as we have noted. Thus the coefficient of each term $G_k(P)$ is exactly $(k)(k-1) - (k-1)(k-2) = 2k+2$ where here $k \geq 2$ by our previous observation. □

We will now work on bounding the number of partial symmetries to bound the number of quadruples which will in turn provide a lower bound on the number of distinct distances.

Proposition 8.5. *For any $P \subset \mathbb{R}^2$ of m points, and any $2 \leq k \leq m$, the size of $G_k(P)$ is bounded as follows*

$$|G_k(P)| \lesssim m^3 k^{-2}$$

We notice that if we can prove this inequality we have

$$|Q(P)| \lesssim \sum_{k=2}^{m} \frac{2k-2}{k} m^3 \lesssim m^3 \log(m)$$

Which proves Proposition 8.1 and thus the desired result. In order to prove this result need to reduce the problem once more to bounding the number of incidences between points and lines in $\mathbb{R}^3$, a problem similar to the Szemerédi and Trotter Theorem we addressed at the beginning of this paper. Elekes and Sharir [4] were the first to relate $G_k(P)$ to an incidence problem involving certain curves in G. Their choice of coordinate system ultimately reduced the distinct distances problem to bounding the number of incidences between a certain class of helices. As these helices were difficult to deal with Elekes and Sharir were not able to complete the proof. However, Guth and Katz [7] adapted Elekes and Sharir's framework, providing a better coordinate system, to reduce the distinct distances problem to bounding the number of incidences between lines and points determined by a certain subset of rigid motions. These lines were far easier to deal with and lent themselves well to the polynomial method. This motivates the following definition.

Definition 8.9. For any points $p, q \in \mathbb{R}^2$ define the set $S_{pq} \subset G$ by

$$S_{pq} = \{g \in G \mid g(p) = q\}$$

This is the set of positively oriented rigid motions moving p to q.

We notice that each S_{pq} is a smooth one-dimensional curve in the 3-dimensional Lie group G. The sets $G_k(P)$ are closely related to the curves S_{pq} as we can see in the following Lemma.

Lemma 8.3. *A rigid motion G lies in $G_k(P)$ if and only if it lies in at least k of the curves $\{S_{pq}\}_{p,q\in P}$.*

Proof: First suppose that $g \in G_k(P)$. Then we can see that $|P \cap g(P)| \geq k$ by definition. Let $q_1, \ldots, q_k$ be the distance points in $P \cap g(P)$. As before let $p_i = g^{-1}(q_i)$. For any $q_i \in g(P)$, we see that p_i lies in P by the definition of p_i. Since $g(p_i) = q_i$ we can see that g lies in $S_{p_i q_i}$ for $i = 1, \ldots, k$. Since that q_i are all distinct, these are k distinct curves.

To address the converse, suppose that g lies in the curves $S_{p_1q_1}, \ldots, S_{p_kq_k}$. Where we assume that $(p_1, q_1), \ldots, (p_k, q_k)$ are all distinct. We claim that $q_1, \ldots, q_k$ are distinct points. If this is the case we can see that g lies in $G_k(P)$. Suppose not, then $\exists i, j$ such that $q_i = q_j$. Since g is a bijection over these points, we see that $p_i = g^{-1}(q_i) = g^{-1}(q_j) = p_j$. This tells us that $(p_i, q_i) = (p_j, q_j)$ which contradicts our assumption that all of the pairs are distinct. This tells us that $q_1, \ldots, q_k$ are distinct points, and thus that g lies in $G_k(P)$. □

Thus bounding $G_k(P)$ is a problem of incidence geometry about the curves $\{S_{pq}\}_{p,q\in P}$ in the group G. By maing a careful change of coordinates, Guth and Katz were able to reduce this problem to an incidence problem for lines in $\mathbb{R}^3$. First we must make a slight distinction between rigid motions in our set G.

Definition 8.10. Let G' denote the open subset of the orientable rigid motion group G given by the rigid motions which are not translations.

We can write $G = G' \sqcup G^{trans}$, where G^{trans} denotes the translations. We then divide $G_k(P) = G'_k \sqcup G_k^{trans}$. Translations are a very special class of rigid motions and it is fairly easy to obtain the bound $|G_k^{trans}| \lesssim m^3 k^{-2}$, as we can see

Proposition 8.6. *Let P be any set of m points in $\mathbb{R}^2$. The number of quadruples in $E^{-1}(G^{trans})$ is $\leq m^3$. Moreover, $|G_k^{trans}| \lesssim m^3 k^{-2}$ for all $2 \leq k \leq m$.*

Proof: Suppose that (p_1, p_2, p_3, p_4) is a distance quadruple in $E^{-1}(G^{trans})$. By definition, there is a translation g so that $g(p_1) = p_3$ and $g(p_2) = p_4$. Therefore we know that $p_3 - p_1 = p_4 - p_2$ as the translation will preserve distances and these points are in a distance quadruple. This equation allows us to determine p_4 from p_1, p_2, p_3. Hence in order to get p_4 we only need to select the points p_1, p_2, p_3 for which there are at most m^3 options. Hence there are $\leq m^3$ quadruples in $E^{-1}(G^{trans})$.

By Proposition 8.3 we can see that

$$|E^{-1}(G^{trans})| = \sum_{k=2}^{m} 2\binom{k}{2} |G_{=k}^{trans}(P)|$$

By noting that $|G_k^{trans}(P)| = \sum_{l \geq k} |G_{=l}^{trans}(P)|$ we see that

$$m^3 \geq |E^{-1}(G^{trans})| \geq 2\binom{k}{2} |G_k^{trans}(P)|$$

This inequality shows that $|G_k^{trans}(P)| \lesssim m^3k^{-2}$ for all $2 \leq k \leq m$. $\square$

We can thus separate out all of the rigid motions that are translations. Unfortunately, bounding $G_k'(P)$ is far more difficult and studying how Guth and Katz [7] were able to accomplish this bound will be the focus of the rest of this section. Their first step was to pick a nice new set of coordinates $\rho : G' \to \mathbb{R}^3$. We know that each element of G' has a unique fixed point and an angle θ of rotation about this fixed point with $0 \leq \theta \leq 2\pi$, as this is how we can define these rigid motions. We thus define the following map.

Definition 8.11. We define the map $\rho : G' \to \mathbb{R}^3$ by

$$\rho(x, y, \theta) = (x, y, \cot(\frac{\theta}{2}))$$

Where (x, y) is the unique fixed point of the rigid motion $g \in G'$ and θ is the angle of rotation as discussed above.

With this change in coordinate system Guth and Katz were able to prove the following.

Proposition 8.7. *Let $p = (p_x, p_y)$ and $q = (q_x, q_y)$ be points in $\mathbb{R}^2$. With ρ as above, the set $\rho(S_{pq} \cap G')$ is a line in $\mathbb{R}^3$.*

Proof: We notice that the fixed point of any transformation taking p to q must lie on the perpendicular bisector of p and q. We can verify that the set $\rho(S_{pq} \cap G')$ can be parameterized as

$$\left(\frac{p_x + q_x}{2}, \frac{p_y + q_y}{2}, 0\right) + t\left(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1\right)$$

This set is all rigid motions that take p to q and are not translations. The idea being that as we move along the perpendicular bisector to find the fixed point of our rigid motion we are moving in a linear fashion and using our map ρ as we find a point on the perpendicular bisector that is the fixed point of a rigid motion sending p to q the angles θ change linearly in $\mathbb{R}^3$ under the cotangent function. $\square$

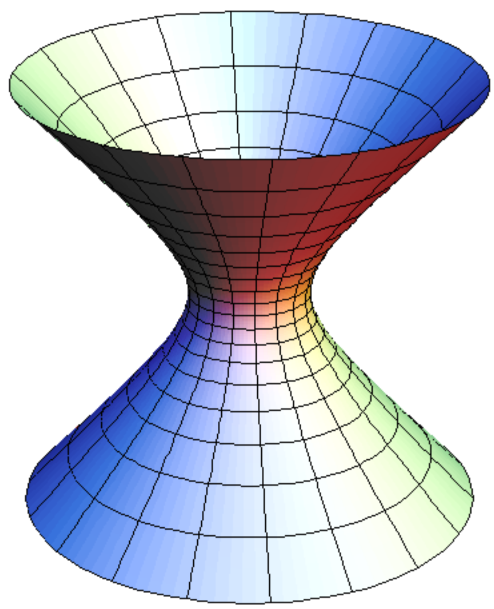
Definition 8.12. For any $p, q \in \mathbb{R}^2$, let L_{pq} denote the line $\rho(S_{pq} \cap G')$. L_{pq} is parameterized by the above line in Proposition 8.7.

If we let $\mathcal{L}$ be the set of lines $\{L_{pq}\}_{p,q \in P}$, by examining the parameterization it is easy to check that there are exactly m^2 distinct lines in this set where $|P| = m$, as two points determine a line in our parameterization and there are exactly m^2 distinct pairs of points. Incredibly now we notice that $g \in G_k'(P)$ if $\rho(g)$ lies in at least k lines of $\mathcal{L}$. This is the case by Lemma 8.3, as if $g \in G_k'(P)$ then it lies in at least k of the curves $\{S_{pq}\}_{p,q \in P}$, and as $g \in G'$ this implies that $\rho(g)$ will intersect $\{\rho(S_{pq} \cap G')\}_{p,q \in P}\} = \{L_{pq}\}_{p,q \in P} = \mathcal{L}$ in at least k places. We have now officially reduced the distinct distances problem to bounding incidences between points and lines in $\mathbb{R}^3$. For the remainder of this chapter we will study the set of lines $\mathcal{L}$ determined by the set G' and we will see how Guth and Katz bounded the number of points lying in k lines.

To prove the distinct distances problem, it would suffice to prove that there are $\lesssim m^3 k^{-2}$ points that lie in at least k lines of $\mathcal{L}$, as bounds the size of $G'_k(P)$ appropriately. Unfortunately, such an estimate does not hold for an arbitrary set of m^2 lines. For example, if all the lines of $\mathcal{L}$ lie in a plane, then one may expect $\sim m^4$ points that lie in at least two lines as we should be able to select two lines at random and find that they intersect as they lie in the same plane. This number of intersection points is far too high. There is another important example, which occurs when all the lines lie in a regulus. We will provide some definitions to make our discussion of reguli make sense.

Definition 8.13. We say that a surface S is *ruled* if for every point of S there is a line that intersects that point and lies completely in S. We say that a surface is *doubly-ruled* if for every point of S there are two lines that intersect that point and lie completely in S.

A common exactly of a doubly ruled surface is a hyperboloid of one sheet depicted below.



We can see that for each point on the Hyperboloid there are exactly two lines that intersect at that point and lie completely in the hyperboloid. Now for a more complicated example we can consider a regulus.

Definition 8.14. A *regulus* is a doubly-ruled surface where each line from one ruling intersects all the lines from the other ruling.

Now we notice that if $\mathcal{L}$ contains $m^2/2$ lines in each of the rulings, then we would have $\sim m^2$ points that lie in at least 2 lines. This once again creates a problem as there are far too many points of incidence. because of this example and the last, Guth and Katz had to show that not too many lines of $\mathcal{L}$ lie in a plane or a regulus. They accomplished this in the following proposition.

Proposition 8.8. *No more than n lines of $\mathcal{L}$ lie in a single plane*

Proof: For each $p \in P$, we consider the subset $\mathcal{L}_P \subset \mathcal{L}$ give by

$$\mathcal{L}_p = \{L_{pq}\}_{q \in P}$$

Notice that if $q \neq q'$ then L_{pq} and $L_{pq'}$ cannot intersect. We notice that with different q and q' but the same p under our map ρ there is only one point where the fixed point of our rotation could be the same (a possible intersection of perpendicular bisectors of (p,q) and (p,q')). However at this point as q and q' are not the same, the angle of rotation could not be the same so that p is sent to q in the first case and p is sent to q' in the second. Thus our two lines cannot intersect at this point either and therefore can never intersect.

So the lines of $\mathcal{L}_p$ are disjoint. From the parametrization of our line in Proposition 8.7, it follows that the lines of $\mathcal{L}_p$ all have different directions. So the lines of $\mathcal{L}_p$ are pairwise skew, and no two of them lie in the same plane. Therefore, any plane contains at most n lines of $\mathcal{L}$, as otherwise this would imply that there were two lines in one of our subsets $\mathcal{L}_p$ that lie in the same plane. $\square$

The situation for reguli is more complicated because all m lines of $\mathcal{L}_p$ lie in a single regulus. However, we will prove that this can only occur for at most two values of p.

Proposition 8.9. *No more than $O(n)$ lines of $\mathcal{L}$ lie in a single regulus.*

Proof: To prove this proposition we will first prove the following lemma

Lemma 8.4. *Suppose that a regulus R contains at least five lines of $\mathcal{L}'_p$. Then all the lines in one ruling of R lie in $\mathcal{L}'_p$.*

Proof: We fix the value of p. We'll check below that each point of $\mathbb{R}^3$ lies in exactly one line of $\mathcal{L}_p$, then all the lines in one ruling of R lie in $\mathcal{L}'_p$. We will construct a non-vanishing vector field $V = (V_1, V_2, V_3)$ on $\mathbb{R}^3$ tangent to the lines of $\mathcal{L}'_p$. Moreover, the coefficients V_1, V_2, V_3 are all polynomials in (x, y, z) of degree ≤ 2. We will do this construction explicitly at the end of the proof.

The regulus R is defined by an irreducible polynomial f of degree 2. Now suppose that a line L_{pq} lies in R. At each point $x \in L_{pq}$, the vector $V(x)$ points tangent to the line L_{pq}, and so the directional derivative of f in the direction $V(x)$ vanishes at the point x. In other words $V \cdot \nabla f$ vanishes on the line L_{pq}. Since f has degree 2, the dot product $V \cdot \nabla f$ is a degree 2 polynomial.

Now suppose that R contains five lines of $\mathcal{L}'_p$. We know that f vanishes on each line, and the previous paragraph shows that the dot product $V \cdot \nabla f$ vanishes on each line. By Bézout's theorem as discussed above, f and $V \cdot \nabla f$ must have a common factor as they are both degree 2 and they both share infinitely many points of vanishing. Since f is irreducible, we must have that f divides $V \cdot \nabla f$. Since f vanishes on R, this implies that $V \cdot \nabla f$ must vanish on the regulus R. As this is the dot product of V and ∇f, this implies that V is tangent to R at every point of R. If x denotes any point in R, and we let L be the line of $\mathcal{L}'_p$ containing x, then we see that this line lies in R. In this way, we get a ruling of R consisting of lines from $\mathcal{L}'_p$.

Essentially what we have done is show that given a line in $\mathcal{L}'_p$ contained in our regulus defined by f, we know that $V \cdot \nabla f$ also vanishes on that line. So by Bézout's Theorem we show that $V \cdot \nabla f$ and f must share a common factor. However, as f is irreducible this implies that f must divide $V \cdot \nabla f$. This implies that $V \cdot \nabla f$ vanishes on the entire regulus. Thus V is tangent to R at every point of R. We have used a common line to show that our vector space is tangent to the entire regulus. Once we show this, if we examine any point on the Regulus, we know that it is contained in exactly one line in $\mathcal{L}'_p$, as $V \cdot \nabla f$ vanishes on each line in $\mathcal{L}'_p$ we know that it vanishes on this line. However at this point x on the Regulus $V \cdot \nabla f$ is tangent to the Regulus, and thus so is the line.

It remains to define the vector field V. We begin by checking that each point (x, y, z) lies in exactly one line of $\mathcal{L}'_p$. By the equation in Proposition 8.7, (x, y, z) lies in L_{pq} if and only if the following equation holds for some t.

$$\left(\frac{p_x + q_x}{2}, \frac{p_y + q_y}{2}, 0\right) + t\left(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1\right) = (x, y, z)$$

Given p and (x, y, z), we can solve uniquely for t and (q_x, q_y). First, we see that $t = z$. This is easy. Next we get a matrix equation of the following form

$$\begin{pmatrix} 1 & z \\ -z & 1 \end{pmatrix} \begin{pmatrix} q_x \\ q_y \end{pmatrix} = a(x, y, z)$$

In this equation, $a(x, y, z)$ is a vector whose entries are polynomials in x, y, z of degree ≤ 1. We must notice that the polynomials also depend on p, but since p is fixed in this case, we suppress the dependence. Since the determinant of the matrix on the left-hand side is $1 + z^2 > 0$, we can solve this equation for q_x and q_y. The solution has the form

$$\begin{pmatrix} q_x \\ q_y \end{pmatrix} = (z^2 + 1)^{-1} b(x, y, z)$$

In this equation, $b(x, y, z)$ is a vector whose entries are polynomials in x, y, z of degree ≤ 2. The vector field $V(x, y, z)$ is $(z^2+1)(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1)$. Recall that p is fixed, and q_x and q_y can be expressed in terms of (x, y, z) by the equation above. By the equation in Proposition 8.7, this vector field is tangent to the line L_{pq}. After multiplying out, the third entry of V is z^2+1, so V is non vanishing. Plugging in the above equation for q_x and q_y and multiplying everything out, we see that the entries of $V(x, y, z)$ are polynomials of degree ≥ 2. As desired. $\square$

Given this lemma, the proof of Proposition 8.9 is fairly straightforward. If a regulus R contains at least five lines of $\mathcal{L}_p$, then all the lines in one ruling of R lie in $\mathcal{L}'_p$ by Lemma 7.4. But if $p_1 \neq p_2$, then $\mathcal{L}'_{p_1}$ and $\mathcal{L}'_{p_2}$ are disjoint, which we can check form the explicit formula in proposition 7.7. Heuristically, this is fairly easy to see as we have discussed above since these lines are the image of a set of rigid motions under our mapping ρ, and if p_1 and p_2 are different points, it is not possible for the lines to intersect. Explicitly, if we plug in p_1 and p_2 into our equation for the line we see that it is impossible for them to every be equal. Since a regulus has only two rulings, there are at most two values of p such that R contains ≥ 5 lines of $\mathcal{L}_p$. As if there were more than 2 it would imply that all of the lines in the two rulings of R were contained in three disjoint sets of lines which is impossible. There two values of p contribute $\leq 2n$ lines of $\mathcal{L}$ in the surface R, as p is fixed and there can be at most n values of q that could at best create n distinct lines in $\mathcal{L}_p$ for each of the two p. Thus these two values of p can contribute at most $2n$ lines. The other $n-2$ values of p contribute at most $4(n-2)$ lines of $\mathcal{L}$ in the surface R, as each one can contribute at most 4 lines by the above. Since if they contributed more than 4 it would imply that all the lines in a ruling were contained in a third disjoint $\mathcal{L}_p$ set. Therefore, the surface R constains at most $2n + 4(n-2) \lesssim n$ lines of $\mathcal{L}$. Which tells us that no more than $O(n)$ lines of $\mathcal{L}$ lie in a single regulus. □

The motivating idea behind the above proof is that when we restrict our gaze to the set of lines with a fixed p there are a limited number of lines form each set that can exist in the regulus. We use the Lemma to show that the regulus can contain at most 2 of the $\mathcal{L}_p$ sets completely. We have a bound on the number of lines from $\mathcal{L}$ that can exist in these sets, mainly m. Then we use the fact that the regulus can contain at most 4 lines from the remaining $\mathcal{L}_p$ sets, which accounts for all the possible lines in $\mathcal{L}$ as $\mathcal{L} = \bigcup_{p \in P} \mathcal{L}_p$. This forces the number of the lines in any given regulus from $\mathcal{L}$ to be relatively low. We are now ready to prove part of the distinct distances problem using Flecnodes.

8.3 Flecnodes

Unfortunately, when bounding the number of incidences we must consider the cases where $k = 2$ and $k > 2$ separately. In other words, we need to use different methods to bound the number of points of intersection of two or more lines in $\mathcal{L}$ and the number of points where at least $k > 3$ lines meet. We will first address the problem of bounding the number of points where at least two lines meet. To derive this bound Guth and Katz used Flecnodes and their relationship with ruled surfaces. We will first state the theorem and then work through its proof. We notice that many of these techniques are familiar as they are used throughout the proofs above.

Theorem 8.2. *Let $\mathcal{L}_1$ be any set of n^2 lines in $\mathbb{R}^3$ for which no more than n lie in a common plane and no more than $O(n)$ lie in a common regulus. Then the number of points of intersection of two lines in $\mathcal{L}_1$ is $O(n^3)$.*

We notice that this theorem implies that $|G_2'(P)| \lesssim n^3$, as we just proved above that in our set no more than n lines lie in a single plane and no more than $O(n)$ lines lie in a single regulus. To commence with the proof of this theorem we must first introduce Flecnodes.

Definition 8.15. Given an algebraic surface in $\mathbb{R}^3$, $p(x, y, z) = 0$ where p is a polynomial of degree $d \geq 3$. A *flecnode* is a point (x, y, z) where a line agrees with the surface to order three. That is, the directional derivative of the surface at (x, y, z) in the direction of our line up to the third derivative equals zero.

To find all such points it suffices to solve the system of equations:

$$\begin{cases} p(x,y,z) & = 0 \\ \nabla_v p(x,y,z) & = 0 \\ \nabla_v^2 p(x,y,z) & = 0 \\ \nabla_v^3 p(x,y,z) & = 0 \end{cases}$$

Where v is the direction of our line. These are four equations for six unknowns (x, y, z) and the components for the direction vector v. However, we notice that the last three equations are homogeneous in v and may be viewed as there equations in five unknowns. As we notice that given any two components of v, we can uniquely determine the third component. Thus, we can view the whole system as 4 equations in 5 unknowns. We may also reduce the last three equations to a single equation in three unknowns (x, y, z). We write the reduced equation

$$Fl(p)(x,y,z) = 0$$

The polynomial $Fl(p)$ is of degree $11d - 24$. It is called the flecnode polynomial of p and vanishes at any flecnode of any level set of p. For a greater discussion of how we reduce our original equation to just three unknowns and for more information on the Flecnode Polynomial, we refer the reader to Katz's paper concerning the flecnode polynomial [11]. This polynomial is extremely useful in determining when a surface is ruled or when a surface contains a ruled factor.

Proposition 8.10. *The surface $p = 0$ is ruled if and only if $Fl(p)$ is everywhere vanishing on it.*

Proof: If the surface $p = 0$ is ruled, by definition there is a line contained in the surface through any point you choose. Thus if you take this line it will obviously agree with the surface at this point up to order three, so $Fl(p)$ vanishes at that point.

Conversely, if $Fl(p)$ vanishes everywhere on $p = 0$ we must prove this in a more computational manor. Ultimately the argument involved seeing that setting $Fl(p) = 0$ is equivalent to rewriting a differently equation on p which implies rudeness. Once again we refer the reader to Katz [11] for a rigorous proof. □

An immediate and useful corollary of Proposition 8.10 stems from a technique we are familiar with. This corollary is essentially the reason we involve the flecnode polynomial.

Corollary 8.1. *Let $p = 0$ be a degree d hyper surface in $\mathbb{R}^d$. Suppose that the surface contains more than $11d^2 - 24d$ lines. Then p has a ruled factor.*

Proof: By Bézout's Theorem since both p and $Fl(p)$ vanish on the same set of more than $11d^2 - 24d$ lines, they must have a common factor q. We know that q is a factor of p and that $Fl(p)$ vanishes on the surface $q = 0$ as q is also a factor of $Fl(p)$ and so when $q = 0$ $Fl(p) = 0$. Thus, by the definition of the Flecnode polynomial, for every regular point on the surface $q = 0$, there must exist a line which agrees with the surface to the third order.

We can see that this is the case because q is a factor of p, as $Fl(p)$ is the flecnode polynomial corresponding to p, if it vanishes on any point in any level surface of p that point is a flecnode. We determined that $Fl(p)$ vanishes on all points of the surface $q = 0$ which is a subset of a level surface of p. This tells us that the flecnode polynomial corresponding to q, $Fl(q)$, vanishes identically. This implies by Proposition 7.10 that q is ruled. $\square$

Now Guth and Katz restricted their gaze to surfaces of degree less than n. The reason for this will become apparent in the proof of Theorem 8.2 below. Ultimately, we will prove some important results concerning ruled algebraic surfaces of degree less than n. These will become useful because when we utilize the polynomial method in the proof of Theorem 8.2, we will be working with a polynomial of degree $O(n)$. Thus they restrict their attention to surfaces modeled by

$$p(x, y, z) = 0$$

Where p is a square free polynomial (if there is a square we remove it and reduce the degree without affecting the zero set) of degree less than n. We can thus uniquely factorize the polynomial into irreducible polynomials,

$$p = p_1 \cdots p_k$$

Where $k \leq n$.

Definition 8.16. We say that p is *plane-free* and *regulus-free* if none of the zero sets of the factors is a plane or a regulus.

As we have already noticed, the only doubly-ruled algebraic surfaces in $\mathbb{R}^3$ are planes and reguli. Thus if p is plane-free and regulus-free this means that the zero-set of the factors of p are irreducible algebraic singly-ruled surfaces. These surfaces have some fairly rigid properties that we will exploit to prove the following lemma that will ultimately allow us to prove Theorem 8.2. We will first introduce an essential Lemma and then provide some important propositions that will allow us to prove it.

Lemma 8.5. *Let p be a polynomial of degree less than n so that $p = 0$ is ruled and so that p is plane-free and regulus-free. let $\mathcal{L}_1$ be a set of lines contained in the surface $p = 0$ with $|\mathcal{L}_1| \lesssim n^2$. Let Q_1 be the set of points of intersection of lines of $\mathcal{L}_1$. Then*

$$|Q_1| \lesssim n^3$$

Before we are able to prove Lemma 7.5, we need to address some potential problems. Specifically lines that intersect infinitely many other lines and points that have infinitely many lines passing through them. We will obtain a bound on the number of such lines and points that will allow us to exclude them and only consider well behaved lines and points. In the forthcoming analysis we let $p(x, y, z)$ be an irreducible polynomial so that $p(x, y, z) = 0$ is a ruled surface which is not a plane or a regulus. In other words, the surface $S = \{(x, y, z) \ : \ p(x, y, z) = 0\}$ is irreducible and singly-ruled. Our discussion in this paragraph motivates the following definition.

Definition 8.17. We say that a point $(x_0, y_0, z_0) \in S$, where S is described above, is an *exceptional point* of the surface if it lies on infinitely many lines contained in the surface. We say that a line ℓ contained entirely within S is an *exceptional line* of the surface if there are infinitely many lines in S which intersect ℓ at non-exceptional points.

Now we have to be careful here in understanding this definition. If a line ℓ contains an exceptional point, we know that there will be infinitely many lines in S which intersect ℓ by the definition of an exceptional point. However, this does not mean that ℓ is necessarily exceptional. In order for ℓ to be exceptional, it must intersect infinitely many lines in S at points that have only finitely many lines through them. In other words, it must contain infinitely many points of intersection. This is the reason for our definition. Exceptional points have infinitely many intersections with lines and exceptional lines must contain infinitely many points of intersection. Intuitively, there should not be many of these lines in our surface. We will now make this idea explicit.

Proposition 8.11. *Let $p(x, y, z)$ be an irreducible polynomial. Let $S = \{(x, y, z) : p(x, y, z) = 0\}$ be an irreducible surface which is neither a plane nor a regulus.*

(a) Let (x_0, y_0, z_0) be an exceptional point of S. Then every other points (x, y, z) of S is on a line ℓ which is contained in S and which contains the points (x_0, y_0, z_0).

(b) Let ℓ be and exceptional line of S. Then there is an algebraic curve C so that every point of S not lying on C is continued in a line contained in S and intersecting ℓ.

Proof: The idea here is to prove that because exceptional points lie on so may lines, given any point in S we can find a line completely contained in S that is incident to both that point and our exceptional point. We will ultimately use this fact to show that there can only be so many exceptional points on an irreducible algebraic surface that is neither a plane or a regulus. To prove part (a), we observer hat by a change of coordinates we can move (x_0, y_0, z_0) to the origin. We let Q be the set of points q different from the origin so that the lines q to the origin is contained in S. We want to show that Q contains all points of S besides the origin. We observe that Q is the intersection of an algebraic set with the complement of the origin. We know this is the case because the surface S is described by a polynomial of finite degree, say d. By definition Q with the origin is a ruled surface that is a subset of our singly-ruled surface S. Thus Q itself is the intersection of this ruled surface which is an algebraic set with the origin removed. In other words, there is a finite set of polynomials E so that a point q different from the origin lies in Q if and only if each polynomial in E vanishes at q. This is because if d is the degree of p, to test whether $q \in Q$ we need only check that the line containing q and the origin is tangent to S to degree $d + 1$ at q. If this is the case then p must vanish identically on the line and therefore the line is contained in S and thus $q \in Q$.

By assumption the zero set of each polynomial in E contains the union of infinitely many lines contained in S since we are assuming that the origin is an exceptional point. Thus by Bézout's Lemma we know that each polynomial in E must share a common factor with p. As p is irreducible this implies that each polynomial in E has p as a factor. As Q is described by the union of the zero sets of these polynomials intersected with the complement of the origin, this implies that Q is all of S except the origin as $Z(p) \subseteq \bigcup_{e \in E} Z(e)$ but obviously $\bigcup_{e \in E} Z(e) \subseteq Z(p) = S$. We have thus proved part (a).

To prove part (b) we observe that by a change of coordinates, we may choose ℓ to be the coordinate lin$y = 0$;$z = 0$. We let Q be the set of points q not on ℓ so that there is a line from q to a non-exceptional point of ℓ which is contained in S. We would like to prove that Q is the intersection of an algebraic set with the complement of an algebraic curve which we will call C. This implies that except for a set of points defined by an algebraic curve, for every other point in S, we can find a line that contains that point and intersects our line ℓ in a non-exceptional point. To prove this claim, for points (x, y, z) on S outside of an algebraic curve, we will identify the point at which the line containing (x, y, z) intersects ℓ.

Consider a point (x, y, z) on S for which $\frac{\delta p}{\delta x}(x, y, z) \neq 0$. In particular, the point (x, y, z) is a regular point of S, as if (x, y, z) were a singular point all of the partial derivatives must vanish. Since $\frac{\delta p}{\delta x}(x, y, z) \neq 0$ we know there is a well-defined tangent plane to the surface S at (x, y, z). Thus, there is a unique point $(x', 0, 0)$ of ℓ which lies in the tangent plane to S at the point (x, y, z). In fact, we can solve for x' as a rational function of (x, y, z) with only the polynomial $\frac{\delta p}{\delta x}(x, y, z)$ in the denominator. We can do this by explicitly creating the tangent plane at that point (x, y, z) and solving for x when $y = z = 0$ in our plane. We know that the plane must intersect the x-axis because it's partial derivative with respect to x is non-zero, thus it cannot be tangent to the x-axis. Thus we can find a set E of rational functions having only powers of $\frac{\delta p}{\delta x}(x, y, z)$ in their denominators ,so that for any (x, y, z) at which $\frac{\delta p}{\delta x}(x, y, z)$ does not vanish, we have that $(x, y, z) \in Q$ if and only if every function in E vanishes on (x, y, z).

In order for the previous paragraph to be useful, we need to know that $\frac{\delta p}{\delta x}(x, y, z)$ does not vanish identically on S, as otherwise we will not be considering any points. Suppose for sake of contradiction that $\frac{\delta p}{\delta x}(x, y, z)$ does vanish identically on S. Since $\frac{\delta p}{\delta x}(x, y, z)$ is definitionally of lower degree than p and p is irreducible, it must be that $\frac{\delta p}{\delta x}(x, y, z)$ vanishes identically as a polynomial so that p depends only on y and z. In this case, since S contains ℓ and it contains a line ℓ' intersecting ℓ by the definition of ℓ, it must contain all translations of ℓ' in the x-direction, as we could shift it along ℓ in the x-direction since p does not depend on x. Thus it contains a plane which is a contradiction. This is where we see the importance of our assumption that $Z(p)$ is plane free.

Thus, we let C be the algebraic curve where both p and $\frac{\delta p}{\delta x}(x, y, z)$ vanish. Away from C, there is a finite set of polynomials F which we can obtain from E by multiplying through by a large enough power of $\frac{\delta p}{\delta x}(x, y, z)$ so that a point (x, y, z) of S outside of C is in Q if and only if each polynomial in F vanishes at (x, y, z). This makes sense based on our previous observation that $(x, y, z) \in Q$ if and only if the set E of rational functions vanishes at (x, y, z) where $\frac{\delta p}{\delta x}(x, y, z)$ does not vanish. We are restricting our view to only points where $\frac{\delta p}{\delta x}(x, y, z)$ does not vanish. So if we clear the powers of $\frac{\delta p}{\delta x}(x, y, z)$ out of the denominator and examine where these new polynomials F vanish outside of C we will find all of the points that are in Q. Since we know that p is irreducible and Q contains an infinite number of lines by the definition of an exceptional line, it must be that each polynomial in F has p as a factor. This is extremely similar to the previous argument. Thus every point of S which is outside of C lies in Q, as desired. $\square$

With this structural result, we can now control the number of exceptional points and lines contained in our surface. WIth this quantitative bound we can then proceed to prove Lemma 8.5.

Corollary 8.2. *Let $p(x, y, z)$ be an irreducible polynomial. Let $S = \{(x, y, z) : p(x, y, z) = 0\}$ be an irreducible surface which is neither a plane nor a regulus. Then S has at most one exceptional point and at most two exceptional lines.*

Proof: Let (x_0, y_0, z_0) and (x_1, y_1, z_1) be distinct exceptional points of S. Since S is singly-ruled, a generic point of S is contained in only a single line ℓ contained in S. Thus by Proposition 7.11 if the point is different from (x_0, y_0, z_0) and (x_1, y_1, z_1) this line ℓ must contain both (x_0, y_0, z_0) and (x_1, y_1, z_1). However, there is only one such line (i.e. the line between (x_0, y_0, z_0) and (x_1, y_1, z_1)), and this would imply that S is a single line. However, this implies that (x_0, y_0, z_0) and (x_1, y_1, z_1) are not exceptional points which is a contradiction. Thus there can only be one exceptional point.

Now let ℓ_1, ℓ_2, ℓ_3 be exceptional lines of S. There are curves C_1, C_2 and C_3 so that the generic point in the complement of C_1, C_2 and C_3 lies on only one line contained in S (since S is singly-ruled) and this line must intersect each of ℓ_1, ℓ_2 and ℓ_3 by Proposition 8.11. Thus as there are infinitely many points not contained in C_1, C_2 and C_3, this means that there are infinitely many lines contained in S which intersect ℓ_1, ℓ_2 and ℓ_3. Moreover, we notice that since the lines are exceptional, there must be an innate set of lines which intersect the three away from the possible three points of intersection of any two of ℓ_1, ℓ_2, ℓ_3. This stems from our previous discussion about the importance of the definition of an exceptional line. If any two of the three lines are coplanar, this means there is an infinite set of lines contained in S which lie in one plane. This contradicts the irreducibility and non planarity of S, as we could factor out the plane. If, on the other hand, ℓ_1, ℓ_2 and ℓ_3 are pairwise skew, then the set of all lines which intersect all three are one ruling of a regulus. We recall that a regulus is a doubly-ruled surface where each line from one ruling intersects all the lines from the other ruling. We can define the first ruling by the set of all lines that intersect ℓ_1, ℓ_2 and ℓ_3 and since they are pairwise skew we could define the second ruling by the set of lines defined by drawing lines through all the lines in our first ruling. This second ruling will not necessarily be contained in our surface S, but between the two rulings we have created a regulus. Thus we can see that as our first ruling is by construction contained in S, that S contains infinitely many lines of a regulus which contradicts the fact that S is irreducible and not a regulus. Here is where our assumption that $Z(p)$ does not contain a regulus is important. $\square$

We are now ready to prove Lemma 8.5, which will ultimately allow us to prove Theorem 8.2.

Proof: We will say that a point (x, y, z) or a line ℓ is exceptional for the surface $p = 0$, if it is exceptional for $p_j = 0$ where p_j is one of the irreducible factors of p. Thus, Corollary 8.2 tells us that there are no more than n exceptional points and $2n$ exceptional lines for

$p = 0$. As p has at most n factors, since p has degree less than or equal to n. Each factor can have at most two exceptional lines and one exceptional point–thus the n exceptional points and $2n$ exceptional lines. Thus there are $\lesssim n^3$ intersections between exceptional lines and lines of $\mathcal{L}_1$ as there are n^2 lines in $\mathcal{L}_1$ and at most $2n$ exceptional lines. Thus to prove the lemma, we need only consider intersections between non exceptional lines of $\mathcal{L}_1$ at nonexceptional points. As there are also at most n points of intersection generated by exceptional points. Thus if we can bound the number of points of intersection generated by non exceptional lines of $\mathcal{L}_1$ and non exceptional points and find that this number is $\lesssim n^3$ this would prove the lemma as we would account for all possible types of intersections.

We note that any line contained in a ruled surface which is not a generator (i.e. part of the ruling. As we know that in a ruled surface every point has at least one line contained in the surface that contains that point, a set of lines such that this is true for all points is a generator for the ruled surface) must be an exceptional line since each point of the line ail lave a generator going through it. Since there are only finitely many non-generators, almost every point must lie in a generator. It is actually possible to prove by a limiting argument that every point lies in a generator. Let q be a point in the ruled surface and let q_i be a sequence of points that converge to q with q_i lying in a generator ℓ_i. It is clear that such a sequence exists as if this were not the case it would imply that there was an infinite sequence of points that all were not contained in generators, which is impossible. By taking a subsequence, we can arrange it so that the directions of ℓ_i converge, and so the lines ℓ_i converge to a limit line ℓ which contains q and lies in the surface. This is the case because as we approach q on the surface, the lines will begin to approach a common direction. If we are farther away we can disregard stray lines that do not begin to converge. This line ℓ is a limit of generators and so it is a generator.

Let ℓ be a non-exceptional line in the ruled surface. In particular ℓ is a generator, as we know that not being a generator implies that it must be an exceptional line, so the contrapositive tells us that a non-exceptional line must be a generator. We claim that there are at most $n-1$ non-exceptional points in ℓ where ℓ intersects another non-exceptional line in the ruled surface. This claim implies that there are at most $(n-1)n^2$ non-exceptional points where two non-exceptional lines intersect, as at each of these $n-1$ points ℓ can at most intersect n^2 other lines. This would prove the bound we desire.

To prove the claim, choose a plane π through the generator ℓ. The plane intersects the surface in a curve of degree at most n, as we know that the surface does not contain the plane and the surface is of degree n. One component is the generator itself by construction. The other component is an algebraic curve c of degree at most $n-1$. There are at most $n-1$ points of intersection between ℓ and c as otherwise c contains ℓ by Bézout's Theorem and we know this is not the case. Suppose that ℓ' is another non-exceptional line and that ℓ' intersects ℓ at a non-exceptional point q. It suffices to prove that q lies in the curve c. As if this is the case we just discussed that there are at most $n-1$ points of intersection between ℓ and c. Thus if q lies in c there can be at most $n-1$ non-exceptional points in ℓ where ℓ intersects another non-exceptional line in the ruled surface.

Since ℓ' is a generator, as it is non-exceptional, it lies in a continuous 1-parameter family of other generators. This is true because we know that ℓ' is a generator for our surface and that our surface is singly-ruled. Now, consider a small open set of generators around ℓ'. These generators intersect the lane π as we know that ℓ' intersects ℓ which is part of the plane and thus generators in this small open set must intersect π by a similar limiting argument as above. So each of the generators in this small open neighborhood intersects either ℓ or c. Since q is non-exceptional, only finitely many of the generators intersect q. Since there are only finitely many exceptional points, we can arrange it so that each generator in our small open set intersects π in a non-exceptional point by a simply transformation. Since ℓ is non-exceptional, only finitely many of our generators can intersect ℓ. Therefore, almost all of our generators must intersect c. As q is the points of intersection between ℓ and ℓ', in order for essentially all of our generators in the small open neighborhood about ℓ' to intersect c q must lie in c. This proves the result as discussed. □

The overall progression of thought in the above proof begins by exploiting our limits on extremal lines and points that could generate too many incidences. We can then narrow our view to intersections between non-exceptional lines at non-exceptional points. Guth and Katz first make the important observation that if a line in the ruled surface is not exceptional, then it must be a generator for the surface. We then examine any non-exceptional line in the surface and another non-exceptional line that intersects our original line at a non-exceptional point. We look at a small open family of generators around our second non-exceptional line. Guth and Katz exploit the fact that the original line is non-exceptional to show that most of the generators in this family must intersect c, as we know they intersect the plane that the original line and c define but can only intersect the original line in finitely many places. Now we know that this open set of lines is generated around our second line and thus q. We can make this open neighborhood arbitrarily small, thus in order for infinitely many of these lines to always intersect c q must be contained in c. With this Lemma we can now prove Theorem 8.2.

Proof: We assume that we have a set $\mathcal{L}$ of at most n^2 lines for which no more than n lie in a plane and no more than n lie in a regulus. We suppose for sake of contradiction that for Q a positive real number $Q >>> 1$ there are Qn^3 points of intersection of lines in $\mathcal{L}$ and we assume that this is an optimal example. In other words, there is no $m < n$ such that we have a set of m^2 lines so that no more than m lie in a plane and no more than m lie in a regulus where there are more than Qm^3 intersections.

We now apply a degree reduction argument similar to the original proof of the Joints Problem in chapter 6. For further discussion of this degree reduction technique we refer the reader to a paper by Katz [11] in which he discusses both the Flecnode polynomial and this idea of degree reduction we will soon use. We let $\mathcal{L}'$ be the subset of $\mathcal{L}$ consisting of lines which intersect other lines of $\mathcal{L}$ in at least $\frac{Qn}{10}$ different points. The lines not in $\mathcal{L}'$ participate in at most $\frac{Qn^3}{10}$ points of intersection. This is because there are at most n^2 points not in $\mathcal{L}'$ and each of them can participate in at most $\frac{Qn}{10}$ points of intersection by construction. Thus there are at least $\frac{9Qn^3}{10}$ points of intersection between lines of $\mathcal{L}'$ as we are assuming that there are Qn^3 points of intersection between all the lines of $\mathcal{L}$. We let α be a real number $0 < \alpha \leq 1$ so that $\mathcal{L}'$ has αn^2 lines.

Now the idea is we have many points on each line, and we want to find a low degree polynomial that vanishes on all the points. To reduce the degree of this polynomial, we reduce the density of our points or our lines while still maintaining enough to find a low degree polynomial that vanishes on all of our lines using the vanishing lemma. It will then vanish on all of our points. So we select a random subset $\mathcal{L}''$ of lines in $\mathcal{L}'$ choosing lines independently with probability $\frac{100}{Q}$. With positive probability, there will be no more than $\frac{200\alpha n^2}{Q}$ lines in $\mathcal{L}''$. We notice that we could state that there will be no more than $\frac{100\alpha n^2}{Q}$ lines in $\mathcal{L}''$ based off of our chosen density, but this statement is still correct as we can raise the upper bound, and it will only increase the probability. We can also see that each line of $\mathcal{L}'$ will intersect lines of $\mathcal{L}''$ in at least n different points. This is because each of these liens must intersect at least other lines of $\mathcal{L}$ in at least $\frac{Qn}{10}$ different points and we are selecting the lines with density $\frac{100}{Q}$, so we can say with positive probability that there will be approximately $\frac{Qn}{10}\frac{100}{Q} \sim 10n \sim n$ points of intersection between $\mathcal{L}''$ and $\mathcal{L}'$.

Now pick $\frac{R\sqrt{\alpha}n}{\sqrt{Q}}$ points on each line of $\mathcal{L}''$, where R is a constant that is sufficiently large, but universal. Call the set of all the points $\mathcal{G}$. There are $O(\frac{R\alpha^{3/2}n^3}{Q^{3/2}})$ points in $\mathcal{G}$, as we know there are approximately $\frac{200\alpha n^2}{Q}$ lines in $\mathcal{L}''$ and we are selecting $\frac{R\sqrt{\alpha}n}{\sqrt{Q}}$ points from each of these lines. The bound even holds if we consider the fact that there are at most n^2 lines in $\mathcal{L}''$. So we may find a polynomial p of degree $O(\frac{R^{1/3}\alpha^{1/3}n}{Q})$ that vanishes on every point of $\mathcal{G}$ using the polynomial ham-sandwich theorem in $\mathbb{R}^3$. With R sufficiently large, p must vanish identically on every line of $\mathcal{L}''$ by the vanishing lemma as we know there are at least $\frac{R\sqrt{\alpha}n}{\sqrt{Q}}$ points on each line of $\mathcal{L}''$. Since each line of $\mathcal{L}'$ meets $\mathcal{L}''$ at n different points, it must be that p vanishes identically on each line of $\mathcal{L}'$ once again by the vanishing lemma. We have thus found a polynomial of reduced degree that vanishes on all of our lines and most importantly all the points of intersection. We will now study the zero set of p to bound the total number of incidences between lines in the zero set.

We may factor $p = p_1 p_2$ where p_1 is the product of the ruled irreducible factors of p and p_2 is the product of the unruled irreducible factors of p. Each of p_1 and p_2 is of degree $O(\frac{\alpha^{1/2}n}{Q^{1/2}})$. Guth and Katz purposefully suppress the R dependence here since R is universal. This is an assumed worse case scenario where the original polynomial p could be the product of ruled irreducible factors in which case $p = p_1$, or that p is the product of unruled irreducible factors in which case $p = p_2$. Either way we know that the degree is $O(\frac{\alpha^{1/2}n}{Q^{1/2}})$ as this is the degree of p. We now break up the set of lines of $\mathcal{L}'$ into the disjoint subsets $\mathcal{L}_1$ consisting of those lines in the zee set of p_1 and $\mathcal{L}_2$ consisting of all the other lines in $\mathcal{L}'$.

Here Guth and Katz are continuing to subdivide the entire set of lines we began with in order to bound each subdivision and reach a contradiction. An important aspect of creating this subdivisions is to make sure that there are not too many intersections between the points in each subdivision. Here, for example, we notice that there are no more than $O(n^3)$ points of intersection between lines of $\mathcal{L}_1$ and $\mathcal{L}_2$ since each line of $\mathcal{L}_2$ contains no more than $O(\frac{\alpha^{1/2}n}{Q^{1/2}})$ points where p_1 is zero by Bézout's Lemma. As otherwise this would imply that p_1 and p_2 have a common factor which we know is impossible. However, we know that $\mathcal{L}_2$ contains at most n^2 points, and thus there are no more than $O(n^3)$ possible points of intersection between $\mathcal{L}_1$ and $\mathcal{L}_2$. Thus we are left with two not mutually-exclusive cases which cover all possible points of intersection. This tells us that there are either $\frac{3Qn^3}{10}$ points of intersection between lines of $\mathcal{L}_1$ or there are $\frac{3Qn^3}{10}$ points of intersection between lines of $\mathcal{L}_2$. This follows from our assumption that there must be Qn^3 points of intersection of lines of $\mathcal{L}$. We will handle each of these cases separately and derive a contradiction in each case.

Suppose we are in the first case where there are $\frac{3Qn^3}{10}$ intersections between lines of $\mathcal{L}_1$. Guth and Katz now use the same technique to further partition our set of lines. We factor $p_1 = p_3p_4$ where p_3 is plane-free and regulus-free and p_4 is a product of planes and reguli. We break $\mathcal{L}_1$ into disjoint sets $\mathcal{L}_3$ and $\mathcal{L}_4$. Where $\mathcal{L}_3$ consists of lines in the zero set of p_3 and $\mathcal{L}_4$ consisting of all the other lines of $\mathcal{L}_1$. Just as before there are $O(n^3)$ intersections between lines of $\mathcal{L}_3$ and $\mathcal{L}_4$ since lines of $\mathcal{L}_4$ are not in the zero set of p_3 and we know that p_3 has degree $O(\frac{\alpha^{1/2}n}{Q^{1/2}})$ and so every line cannot intersect more than this many points, otherwise this implies that the line is in $\mathcal{L}_3$. As there are at most n^2 lines we get our desired bound on the number of incidences between lines in $\mathcal{L}_3$ and $\mathcal{L}_4$, so our partition is valid and useful.

Now we wish to prove that there are at most $O(n^3)$ points of intersection between the lines in each of our respective partitions which will force us into case two. Moreover, there are at most $O(n^3)$ points of intersection between lines of $\mathcal{L}_4$ because they lie in at most n planes and reguli each containing at most n lines. This is the case because there are at most n^2 lines in $\mathcal{L}_4$. We know that these lines must all lie in some set of planes and reguli by construction. However, by assumption no more than n lines lie in any single plane or reguli. Thus there are at most n reguli that contain at most n lines as this would account for all n^2 lines. This is a worst case scenario, we notice that there could be more reguli and planes that each contain less lines, but this will reduce the total number of points of intersection between lines as these reguli and planes must be distinct. We see that if we are in the worst case scenario each line has at most $O(n)$ intersections with planes and reguli it is not contained in and there are at most $O(n^2)$ points of intersection between lines internal to each plane and regulus as each of the n lines contained in the plane or the regulus could at most intersect all of the other n lines, leading to n^2 points of intersection. As there are at most n planes and reguli this means that there are at most $n \cdot O(n^2) = O(n^3)$ points of intersection in $\mathcal{L}_4$. We also notice that as p_3 is plane free and regulus free by Lemma 7.5 there are $O(n^3)$ points of intersection between lines in $\mathcal{L}_3$.

Thus we must be in the second case as otherwise we contradict our assumption that there are at least Qn^3 points of intersection. So this means that many of the points of intersection are between lines of $\mathcal{L}_2$, all of which lie in the zero set of p_2 which is totally unruled by construction. Recall that p_2 is of degree $O(\frac{\alpha^{1/2}n}{Q^{1/2}})$. Thus by Lemma 4.3, its zero set contains no more than $O(\frac{\alpha n^2}{Q})$lines, this is essentially $O(d^2)$ where d is the degree of p_2. This is because it must be unruled and we know that if its zero set contains more than that many lines it must have a ruled factor as it would share a factor with the Flecnode Polynomial. We would like to invoke the fact that the example we started with was optional to reach a contradiction. In other words, we would like to construct a smaller set of lines such that these lines with M elements satisfy the conditions that no more than M lie in a plane and no more than M lie in a regulus but that there are QM^3 points of intersection. Unfortunately, we cannot quite do this yet with our set $\mathcal{L}_2$, we need slightly more refinement. Our set $\mathcal{L}_2$ has βn^2 lines with $\beta = O(\frac{\alpha}{Q})$. This is because $\mathcal{L}'$ has αn^2 lines, so we can always find some large constant such that the number of lines in $\mathcal{L}_2$ is bounded by βn^2 for our defined β. We know that no more than n lines lie in any plane or regulus, whereas we need to know that there are no more than $\sqrt{\beta}n$ lines. As this would imply that we could take our new $M = \sqrt{\beta}N < N$, as at worst $\beta = \alpha < 1$. Then there are exactly M^2 lines, with no more than M in any plane or regulus.

Suppose that this is not the case. We will now further refine our set of lines. We construct a subset of $\mathcal{L}_2$ which we call $\mathcal{L}_5$ as follows. If there is a plane or regulus containing more than $\sqrt{\beta}n$ lines of $\mathcal{L}_2$ we put those lines in $\mathcal{L}_5$ and remove them from $\mathcal{L}_2$. We repeat as needed labeling the remaining lines $\mathcal{L}_6$. Since we removed $O(n)$ planes and reguli, there are $O(n^3)$ points of intersection between lines of $\mathcal{L}_5$. This is because as we have discussed there are at most n lines in any plane or regulus, and at most n^2 lines in $\mathcal{L}_2$. We want to remove planes or reguli if and only if they contain more than $\sqrt{\beta}n$ lines of $\mathcal{L}_2$, as they can contain at most n lines, there are at most $O(n)$ planes or reguli to remove. Thus $\mathcal{L}_5$ consists of at most $O(n)$ planes or reguli containing at most n^2 lines. We've seen this argument before a few paragraphs up. Each of these lines can at most intersect $O(n)$ lines from a plane or reguli they are not contained in, and there are at most $O(n^2)$ points of intersection between lines internal to each plane and regulus as each of the n lines contained in the plane or the regulus could at most intersect all of the other n lines, leading to n^2 points of intersection. As there are $O(n)$ planes and reguli this means that there are at most $O(n) \cdot O(n^2) = O(n^3)$ points of intersection between lines in $\mathcal{L}_5$. Now, since no line of $\mathcal{L}_6$ belongs to any plane or regulus of $\mathcal{L}_5$ there are fewer than $O(n^3)$ points of intersection between lines of $\mathcal{L}_5$ and $\mathcal{L}_6$. This is because there are at most n^2 lines in $\mathcal{L}_6$ and they can intersect at most $O(n)$ lines of planes and reguli they are not contained in. Thus as they are not contained in any planes of reguli of $\mathcal{L}_5$, they can intersect at most $O(n^3)$ lines. Thus this partitioning is acceptable. Now we apply optimality of our original example to rule out having more than $O(\frac{n^3}{Q^{1/2}})$ points of intersection between lines of $\mathcal{L}_6$, as otherwise as discussed out original choice of n would not be optimal. Thus we have reached a contradiction and there must be $O(n^3)$ points of intersection between our original set of lines $\mathcal{L}$. $\square$

This is an incredible proof. It utilizes degree reduction, the important results of the polynomial method concerning the zero set of a polynomial and algebraic properties of planes and reguli. We see elements of almost all of the previous theorems we have discussed. The degree reduction argument seems eerily similar to the original Joints Problem proof. This does beg the question of whether or not there is a simplified proof like the one Quilodran produced for the Joints Problem. The idea of exploiting a low degree polynomial is very familiar to us. Exploiting the properties of planes and reguli is really the hidden key to this argument. This concludes Guth and Katz's proof of the first part of the distinct distance problem where we want to bound the number of incidences between two of more lines. We will now begin to prove the final part in which we find a better bound on the number of three or more incidences. An interesting point to consider is that all of the following proofs work for $\mathbb{R}^3$, but not for the complex numbers. We know that the Szemerédi and Trotter Theorem holds for the complex version

8.4 Cell Decomposition in $\mathbb{R}^3$

We will now begin discussing how Guth and Katz prove the second and final part of the Distinct Distances Proof. As previously discussed they had to break the proof into two cases. We have now dealt with the case of bounding the number of points of incidence between two or more lines in our set, however this bound will not be good enough in general to prove the final result if we were to use it for all points of incidence. Thus we now want to bound the number of incidences between three or more lines in our set. Guth and Katz used this in conjunction with the previous section to prove the Distances Problem. This section will rely heavily upon work we have already discussed, specifically Theorem 4.7, the Polynomial Partitioning Theorem, above. We begin by stating the Theorem that we will prove throughout this section, the second piece to the proof of the Distinct Distances Problem:

Theorem 8.3. *Let $\mathcal{L}$ be any set of n^2 lines in $\mathbb{R}^3$ for which no more than n lie in a common plane, and let k be a number $3 \leq k \leq n$. Let P_k be the set of points where at least k lines meet. Then*

$$|P_k| \lesssim N^3 k^{-2}$$

Once we prove this Theorem we have shown that $|G_k'(P)| \lesssim n^3 k^{-1}$ for all $2 \leq k \leq n$. We will discuss how this directly proves Theorem 8.1 at the conclusion of this section. We begin proving Theorem 8.3 by introducing a generalized version of the Polynomial Ham Sandwich Theorem (Theorem 4.6) to $\mathbb{R}^n$ due to Stone-Tukey [20].

Theorem 8.4 (Stone-Tukey [20])**.** *For any degree $d \geq 1$, the following holds. Let $U_1, \ldots, U_M$ be any finite volume open sets in $\mathbb{R}^n$, with $M = \binom{d+n}{n} - 1$. Then there is a real algebraic hypersufrace of degree at most d that bisects each U_i.*

We will not provide a proof of this result, as it delves slightly too deep for the purposes of our paper, but we refer the curious reader to Stone and Tukey's paper. We will now present and prove a corollary to this theorem that Guth and Katz introduced concerning finite sets of points.

Theorem 8.5. *Let $A_1, \ldots, A_M$ be finite sets of points in $\mathbb{R}^n$ with $M = \binom{n+d}{n} - 1$. Then there is a real algebraic hyper surface of degree at most d that bisects each S_i.*

Proof: For each $\delta > 0$, define $U_{i,\delta}$ to be the union of δ-balls centered at the points of S_i. By the generalized polynomial ham sandwich theorem we can find a non-zero polynomial p_δ of degree $\leq d$ that bisects each set $U_{i,\delta}$.

We want to take a limit of polynomials p_δ as $\delta \to 0$. This will ultimately provide the result we desire. To help make this work, we define a norm $||||$ on the space of polynomials of degree $\leq d$. Any norm would work, but we will let $||p||$ denote the maximal absolute value of the coefficients of p. By scaling p_δ we can assume that $||p_\delta|| = 1$ for all δ. Now we can find a sequence $\delta_m \to 0$ so that p_{δ_m} converges in the space of degree $\leq d$ polynomials. We let p be the limit polynomial and observe that $||p|| = 1$. In particular, p is not 0. Since the coefficients of p_{δ_m} converge to the coefficients of p, it's easy to check that p_δ converges to p uniformly on compact sets.

We claim that p bisects each set S_i. Suppose this is not the case and that instead without loss of generality $p > 0$ on more than half the points of S_i. Let $S_i^+ \subset S_i$ denote the set of points of S_i where $p > 0$. By choosing ϵ sufficiently small, we can assume that $p > \epsilon$ on the ϵ-ball around each point of S_i^+. Also, we can choose ϵ small enough so that the ϵ-balls around the points of S_i are disjoint. Since p_{δ_m} converges to p uniformly on compact sets, we can find m large enough so that $p_{\delta_m} > 0$ on the ϵ-ball around each point of S_i^+ as these ϵ-balls are compact. By making m large, we can also arrange so that $\delta_m < \epsilon$. Therefore, $p_{\delta_m} > 0$ on the δ_m-ball around each point of S_i^+. But then $p_{\delta_m} > 0$ on more than half of the U_{i,δ_m}. As we constructed each p_δ so that is bisects each of these sets this is a contradiction which proves that p bisects S_i. □

The basic idea here is to create shrinking balls around each of the points in our finite point set. We know that for any set of any sized balls around some points we can find a polynomial that bisects the union of these balls by the Polynomial Ham Sandwich Theorem. We then continue to shrink the balls and look at the corresponding limit of the polynomials. These polynomials will converge to a polynomial that necessarily bisects the finite points that all of the ϵ-balls were centered at. Using this generalization of Theorem 4.6 it only makes sense that we can now prove a generalization of Theorem 4.7 (The Polynomial Partitioning Theorem) to n dimensions.

Theorem 8.6. *If P is a set of S points in $\mathbb{R}^n$ and $J \geq 1$ is an integer, then there is a polynomial surface Z of degree $d \lesssim 2^{J/n}$ with the following property. The complement $\mathbb{R}^n \setminus Z$ is the union of 2^J open cells O_i, and each cell contains $\leq 2^{-J}S$ points of P.*

Proof: We will do the construction as before in J steps. In the first step, we pick a linear polynomial p_1 that bisects P. We let P^+ and P^- be the sets where p_1 is positive and negative respectively. In the second step, we find a polynomial p_2 that bisects P^+ and P^-. We continue in this process, more finely dividing the points. At each new step we use our generalized polynomial ham sandwich theorem to bisect the sets from the previous step.

We will make this inductive process explicit. At the end of step j, we have defined j polynomials $p_1, \ldots, p_j$. We define 2^j subsets of P by looking at the points where the polynomials $p_1, \ldots, p_j$ have specified signs. There are j polynomials and 2 options for their signs (we also notice that the polynomials could vanish on some of the points, but these points could be placed in either subset). Now we use Theorem 8.4 to bisect each of these 2^j sets. It follows by induction that each subset contains $\leq 2^{-j}S$ points.

Now we let p be the product $p_1, \ldots, p_J$ and we let Z denote the zero set of p. We want to estimate the degree of p as before. By Theorem 8.4 the degree of p_j is $\lesssim 2^{j/n}$. Hence the degree of p is $d \lesssim \sum_{j=1}^{J} 2^{j/n} \lesssim 2^{J/n}$.

Now we define the 2^J open sets O_i as the sets where the polynomials $p_1, \ldots, p_J$ have specified signs. Can really be imagines as a 2^J-tuple containing entries that are either 0 or 1. If the i^{th} entry is 1, this means that p_i is positive on this set and if it is 0 it means that p_i is negative. The sets O_i are open as for any point in the set we can necessarily find a small enough ϵ so that each of the polynomials maintains its sign on that point as all of the polynomials are continuous. We can also see that these O_i are disjoint by construction. Their union is exactly the complement of Z as for any point not in Z our polynomials assume either or positive or negative value and thus the point is in one of the O_i. As we saw above, the number of points in $P \cap O_i$ is at most $2^{-J}S$. This completes the generalization. $\square$

It's interesting to see how easily some of these results can be generalized once the original result that they depend on is generalized. Now using this generalized cell decomposition we will prove an estimate for incidences of lines when too many lines lie in a plane. This Theorem will ultimately imply the second piece of the Distinct Distances Problem proof. We will spend the rest of this section proving this theorem.

Theorem 8.7. *Let $k \geq 3$. Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$ with at most B lines in any plane. Let P be the set of points in $\mathbb{R}^2$ intersecting at least k lines of $\mathcal{L}$. Then the following inequality holds:*

$$|P| \leq C[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$$

It is important to notice that if we set $L = N^2$ and $B = N$ we have that

$$|P| \leq C[N^3k^{-2} + N^3k^{-3} + N^2k^{-1}]$$

If we compare this to Theorem 8.3 we see that it is exactly what we seek to prove. It is extremely interesting to compare Theorem 8.7 to the Szemerédi and Trotter Theorem. It is actually rather easy to generalize the Szemerédi and Trotter Theorem to higher dimensions,

Theorem 8.8 (Szemerédi and Trotter)**.** *If $\mathcal{L}$ is a set of L lines in $\mathbb{R}^n$ and P denotes the set of points lying in at least k lines of $\mathcal{L}$, then*

$$|P| \lesssim L^2k^{-3} + Lk^{-1}$$

We will not explicitly go through the proof as we only mention this for a point of comparison and to illustrate the connection between the Distinct Distances problem and everything we have discussed thus far. The general idea it that we take any generic projection from $\mathbb{R}^n$ to $\mathbb{R}^2$. The set of lines $\mathcal{L}$ will project to L distinct lines in $\mathbb{R}^2$ and the points of P project to distinct points in $\mathbb{R}^2$. We can then apply the Szemerédi and Trotter theorem in $\mathbb{R}^2$ to get the result. We can actually see that Theorem 8.7 implies the Szemerédi and Trotter theorem when $B = L$. In other words, if we really don't have any restriction on how many of the lines can lie in a single plane. We notice that as B gets smaller we can bound the number of incidences far more efficiently. This interestingly illustrates that if we know not too many lines lie in a single plane the number of incidences decreases. Guth and Katz use both Theorem 8.7 and 8.8 in their proof of Theorem 8.3. Guth and Katz now prove Theorem 8.7 under some uniformity hypotheses and ultimately show that every possible case reduces to this special case by some inductive arguments.

Proposition 8.12. *Let $k \geq 3$. Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$ with at most B lines in any plane. Let P be a set of S points in $\mathbb{R}^3$ so that each point intersects between k and $2k$ lines of $\mathcal{L}$. Also, assume that there are $\geq \frac{1}{100}L$ lines in $\mathcal{L}$ which each contain $\geq \frac{1}{100}SkL^{-1}$ points of P. Then*

$$S \leq C[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$$

The second part of this proposition is our uniformity assumption about the lines. We notice that there are $\sim Sk$ total incidences between lines of $\mathcal{L}$ and points of P. This is because there are S points and each intersects at least k lines. This tells thus that the average line of $\mathcal{L}$ contains $\sim SkL^{-1}$ points of P. We essentially assume here that there are many lines that are about average. We handle extremal examples simply by reducing them to this case. We will first give a general outline for the proof of the Proposition and then commence with the proof.

We suppose that

$$S \geq AL^{3/2}k^{-2} + Lk^{-1} \tag{1}$$

Where A is a large constant that we will choose below. Assuming equation (1), we need to show that many lines of $\mathcal{L}$ lie in a plane. In particular, we will find a plane that contains $\gtrsim SL^{-1}k^3$ lines of $\mathcal{L}$. If this is the case, it forces $B \gtrsim SL^{-1}k^3$ as we assumed that no more than B lines lie in a single plane. This then tells us that $S \lesssim BLk^{-3}$, and we will be done. So really the problem has been reduced to finding a plane that contains many lines.

Now we will outline how Guth and Katz found this plane. First, we prove that a definite fraction of the lines of $\mathcal{L}$ lie in an algebraic surface Z of degree $\lesssim L^2S^{-1}k^{-3}$. Second, we prove that this variety Z contains some planes, and that a definite fraction of the lines of $\mathcal{L}$ lie in the planes. Since there are at most d planes in Z, one plane must contain $\gtrsim L/d$ lines by the Pigeon Hole Principle. As $d \lesssim L^2S^{-1}k^{-3}$, this plane contains $\gtrsim SL^{-1}k^3$ lines, which is what we wanted to prove. The essential aspect is really finding this algebraic surface with the proper degree.

We notice that the bound for the degree d is sharp up to a constant factor because of the example where we have L/B planes with B lines in each plane. We can arrange the B lines in each plane to create B^2k^{-3} k-fold incidences. This set of lines has a total of LBk^{-3} k-fold incidences as there are exactly L/B planes. In this specific case the lines $\mathcal{L}$ lie in $\sim L^2S^{-1}k^{-3}$ planes. Since the planes can be taken in general position, the lines $\mathcal{L}$ do not lie in an algebraic surface of lower degree.

A reasonable question to ask is why we don't use the same methods in the last section to prove the case where $k \geq 3$. Guth and Katz originally tried this to find Z but using their reduction arguments could only reduce Z to be an algebraic surface of degree $L^2S^{-1}k^{-2}$

which was not small enough for their purposes. Thus they had to rely on this cell decomposition method. First we will prove that almost all the points of P lie in a surface Z with properly controlled degree. Guth and Katz regard this lemma as the most important step.

Lemma 8.6. *If the constant A in inequality (1) is sufficiently large, then there is an algebraic surface Z of degree $\lesssim L^2S^{-1}k^{-3}$ that contains at least $(1-10^{-8})S$ points of P.*

Proof: asdf □

This lemma ultimately shows that most of the points of P are contained in our algebraic surface of the desired degree. We now let P_z denote the points of P that lie in Z. By Lemma 8.6 we know that $|P \setminus P_Z| \leq 10^{-8}S$. We now want to prove that many lines of $\mathcal{L}$ lie in the surface Z. This result depends on a quick calculation about the degree of d. Recall that an average line of $\mathcal{L}$ contains SkL^{-1} points of P. We prove that the degree of d is much smaller than SkL^{-1}, thus by the vanishing Lemma the average line is contained in Z and by our uniformity assumption almost all of our lines are average. Thus almost all of our lines are contained in Z.

Lemma 8.7. *If the constant A is sufficiently large, then*

$$d < 10^{-8}SkL^{-1}$$

Proof: Inequality (1) can be rewritten as

$$1 \leq A^{-1}SL^{-3/2}k^2$$

If we square both sides and multiplying by d, we see that

$$d \leq dA^{-2}S^2L^{-3}k^4 \lesssim A^{-2}SkL^{-1}$$

Choosing A sufficiently large completes the proof. □

As an immediate corollary using the vanishing lemma, we get the following lemma.

Lemma 8.8. *If l is a line of $\mathcal{L}$ that contains at least $10^{-8}SkL^{-1}$ points of P_Z, then l is contained in Z.*

Proof: The line l contains at least $10^{-8}SkL^{-1}$ points of Z. Since $d > 10^{-8}SkL^{-1}$, the line l must lie in the surface Z by the vanishing lemma. □

Now let $\mathcal{L}_Z$ denote the set of lines in $\mathcal{L}$ that are contained in Z. We will show that a definite fraction of the lines of $\mathcal{L}$ are in $\mathcal{L}_Z$.

Lemma 8.9. *The set $\mathcal{L}_Z$ contains at least $(1/200)L$ lines.*

Proof: We assumed that there are $\geq (1/100)L$ lines of $\mathcal{L}$ which each contain $\geq (1/100)SkL^{-1}$ points of P. Let $\mathcal{L}_0 \subset \mathcal{L}$ be the set of these lines. We claim that most of these lines lie in $\mathcal{L}_Z$. Suppose that a line l lies in $\mathcal{L}_0 \setminus \mathcal{L}_Z$. It must contain at least $(1/100)SkL^{-1}$ points of P. However, if our polynomial does not vanish on the line it must contain $< 10^{-8}SkL^{-1}$ points of P_Z. This tells us that it must contain at least $(1/200)SkL^{-1}$ points of $P \setminus P_Z$. Using this we derive the following inequality:

$$(1/200)SkL^{-1}|\mathcal{L}_0 \setminus \mathcal{L}_Z| \leq I(P \setminus P_Z, \mathcal{L}_0 \setminus \mathcal{L}_Z)$$

Where here as before the right hand side of the inequality represents the number of incidences between the point set and line set. However, we know that each points of P lies in at most $2k$ liens of $\mathcal{L}$, giving us an upper bound on the number of incidences:

$$I(P \setminus P_Z, \mathcal{L}_0 \setminus \mathcal{L}_Z) \leq 2k|P \setminus P_Z| \leq 2 \cdot 10^{-8}Sk$$

As we know from Lemma 8.6 that $|P \setminus P_Z| \leq 10^{-8}S$. Combining these two inequalities we have

$$(1/200)SkL^{-1}|\mathcal{L}_0 \setminus \mathcal{L}_Z| \leq 2 \cdot 10^{-8}Sk$$

This tells us that $|\mathcal{L}_0 \setminus \mathcal{L}_Z| \leq 4 \cdot 10^{-6}L$. We know that at the very least there are $(1/100)L$ lines in L_0. This tells us that $|\mathcal{L}_Z| \geq (1/200)L$ at the very least. □

We have no completed the first step of our outline. We have found a surface Z of degree $\lesssim L^2S^{-1}k^{-3}$ which contains a definite fraction of the lines from $\mathcal{L}$. We now prove that Z contains some planes, and that these planes contain many lines of $\mathcal{L}$. This step is closely based on the work in Elekes and Sharir's paper [4]. We know that each point of P_Z lies in at least k lines of $\mathcal{L}$ by construction. However, such a point does not necessarily lie in any lines of $\mathcal{L}_Z$. Therefore we make the following definition.

Definition 8.18. We define P'_Z to be the set of points in P_Z that lie in at least three lines of L_Z.

This subset is important because each point of P'_Z is a special point on the surface Z, it is either critical or flat. We will quickly define and recall exactly what this means

Definition 8.19. We say that a point $x \in Z$ an algebraic surface defined by a polynomial p is *critical* if the gradient ∇p vanishes at x. If x is not critical we say that x is *regular*.

We saw this before, but we have not yet discussed what a flat point is

Definition 8.20. We say that a regular point $x \in Z$ is flat if the second fundamental form of Z vanishes at x.

We will not deeply delve into exactly what the second fundamental form of Z is, but it is the symmetric bilinear form on the tangent space of the surface of a point p. Understanding exactly what this means is not essential to the proof, only understanding properties of flat points. These will be discussed as they come up. We now prove that each point of P'_Z must fall into one of these two categories.

Lemma 8.10. *Each point of P'_Z is either a critical point or a flat point of Z.*

Proof: Let $x \in P'_Z$. By definition, x lies in three lines which all lie in Z. If x is a critical point of Z, we are done. If x is a regular point of Z, then all three lines must lie in the tangent space of Z at x. In particular, the three lines are coplanar. Let v_1, v_2, v_3 be non-zero tangent vectors of the three lines at x. The second fundamental form of Z vanishes in each of these three directions. This is because the second fundamental form is a symmetric bilinear form on the two-dimensional tangent space, thus it must vanish. Thus, by definition x is a flat points of Z. $\square$

Lemma 8.10 shows that points of P'_Z are important or special points. Next we will show that almost every point of P lies in P'_Z. Heuristically this makes sense given our regularity assumption. We know that each point has at least three lines going through it, we also now know that there are many lines in Z. As there are many lines going through each point, and a large fraction of these lines are contained in Z, it stands to reason that many of the points will be incident to at least three lines in $\mathcal{L}_Z$.

Lemma 8.11. *The set $P \setminus P'_Z$ contains at most $10^{-7}S$ points.*

Proof: Lemma 8.6 tells us that $|P \setminus P_Z| \leq 10^{-8}S$. Suppose that x is a point if $P_Z \setminus P'_Z$. We know by assumption that x lies in at least k lines from $\mathcal{L}$, but that it lies in at most two lines from $\mathcal{L}_Z$ as otherwise it would be in P'_Z. So x lies in $\geq k-2$ lines of $\mathcal{L} \setminus \mathcal{L}_Z$. This tells us that

$$(k-2)|P_Z \setminus P'_Z| \leq I(P_Z \setminus P'_Z, \mathcal{L} \setminus \mathcal{L}_Z)$$

As minimally each of the points in the set $P_Z \setminus P'_Z$ lies in $k-2$ lines of $\mathcal{L} \setminus \mathcal{L}_Z$, thus the total number of incidences between that set of points and lines has the above lower bound. However, we showed in Lemma 8.8 that each lines of $\mathcal{L} \setminus \mathcal{L}_Z$ contains $\leq 10^{-8}SkL^{-1}$ points of P_Z. This allows us to obtain an upper bound on the number of incidences:

$$I(P_Z \setminus P'_Z, \mathcal{L} \setminus \mathcal{L}_Z) \leq I(P_Z, \mathcal{L} \setminus \mathcal{L}_Z) \leq (10^{-8}SkL^{-1})L$$

Combining these inequalities, and once again invoking our assumption that $k \geq 3$ we obtain:

$$|P_Z \setminus P'_Z| \leq 10^{-8}\frac{k}{k-2}S \leq 3 \cdot 10^{-8}S \leq 10^{-7}S$$

As desired. $\square$

We now let $P_{crit} \subset P'_Z$ denote the critical points of P'_Z and we let $P_{flat} \subset P'_Z$ denote the flat points of P'_Z. We will now attempt to separate our lines in the same way we just separated our points, to do so we have the following definitions

Definition 8.21. We say that a line $l \subset Z$ is a *critical line* if every points of l is a critical points of Z. Now if a line is not critical but $l \subset Z$ and every regular points of l is flat, we call l a *flat line.*

Our next goal is to show that Z contains many flat lines, which is a step towards showing that Z contains a plane. As each flat line is contained in the tangent surface to Z at the point, and so if Z contains many such lines it makes sense that it would contain a plane. In order to do this, we show that the flat points of Z are defined by the vanishing of certain polynomials.

Lemma 8.12. *Let x be a regular point of Z. Then x is flat if and only if the following three polynomial vectors vanish at x:*

$$\triangledown_{e_j \times \triangledown_p} \triangledown p \times \triangledown p$$

For $j = 1, 2, 3$.

here e_j are the coordinate vectors of $\mathbb{R}^3$, and $\times$ denotes the cross product of vectors. Each vector above has three components, so we have a total of nine polynomials. Each polynomial has degree $\leq 3d$. For further explanation we refer the reader to [4]. They actually use a more efficient set of polynomials–only three. Now, to find critical or flat lines, we use the following lemmas.

Lemma 8.13. *Suppose that a line l contains more than d critical points of Z. Then l is a critical line of Z.*

Proof: At each critical points of Z, the polynomial p and all the components of $\triangledown p$ vanish. Since p has degree d, we conclude that p vanishes on every points of l by the vanishing lemma. Similarly, since $\triangledown p$ has degree $d-1$ we conclude that $\triangledown p$ vanishes on every point of l. By definition this means that l is a critical line of Z. □

Now we will prove a similar lemma for determining when a line is flat based on how many flat points it contains.

Lemma 8.14. *Suppose that a line l contains more than $3d$ flat points of Z. Then l is a flat line of Z.*

Proof: Let $x_1, \dots, x_{3d+1}$ be flat points of Z contained in l. By Lemma 8.12 each polynomial $\triangledown_{e_j \times \triangledown_p} \triangledown p \times \triangledown p$ vanishes at x_i. Since the degree of these polynomials is $\leq 3d$, we once again use the vanishing lemma to conclude that each of these polynomials vanishes on l. Similarly, p vanishes on l as $3d + 1 > d$. Therefore, the line l lies in Z and every regular points of l is a flat points. However as x_i are all regular points of Z this means that l cannot be a critical line, and thus it must be a flat line. □

Using these basic lemmas we will now prove that a definite fraction of the lines of $\mathcal{L}$ are either critical or flat. As we did before the the set of points, we will define $\mathcal{L}'_Z$ to be the set of lines of $\mathcal{L}_Z$ that contain at least $(1/200)SkL^{-1}$ points of P'_Z. In other words, $\mathcal{L}'_Z$ is the set of lines that are contained in the zero set Z that contain at least $(1/200)SkL^{-1}$ points in Z that are either flat or critical. We will show that if each line contains this many points, they necessarily must be either critical or flat.

Lemma 8.15. *Each line of $\mathcal{L}'_Z$ is either critical or flat.*

Proof: Since every points of P'_Z is either critical or flat, each line in $\mathcal{L}'_Z$ contains either $(1/400)SkL^{-1}$ critical points or $(1/400)SkL^{-1}$ flat points. As at worst the points are exactly equally distributed, otherwise the line would contain more of one kind. However, by Lemma 8.7, $d \leq 10^{-8}SkL^{-1}$. Thus by Lemmas 8.13 and 8.14 each line of $\mathcal{L}'_Z$ must be either critical or flat. It's interesting to note that this actually forces the large majority of the points on our lines to be either critical or flat as a line cannot be both. Thus the line must contain less than $10^{-8}SkL^{-1}$ points of the other class (divided by 3 if the line is critical). $\square$

We have already shown that $\mathcal{L}_Z$ contains a definite fraction of the lines of $\mathcal{L}$, but we will now show that actually thanks to our regularity assumption and our new bounds on the number of critical and flat points a definite fraction of the lines of $\mathcal{L}$ lie in $\mathcal{L}'_Z$. Another way of thinking about this is that most of the lines in $\mathcal{L}$ contain a large enough portion of either critical or flat points.

Lemma 8.16. *The number of lines in $\mathcal{L}'_Z$ is $\geq (1/200)L$.*

Proof: Guth and Katz first bring attention to the regularity assumption in Proposition 8.12. That is, we know that there are at least $(1/100)L$ lines of $\mathcal{L}$ that each contain $\geq (1/100)SkL^{-1}$ points of P. We denote these lines by $\mathcal{L}_0 \subset \mathcal{L}$.

Suppose a line l lies in $\mathcal{L}_0 \setminus \mathcal{L}'_Z$. We know that l contains at least $(1/100)SKL^{-1}$ points of P by the above. However, it must contain less that $(1/200)SkL^{-1}$ points of P'_Z as otherwise it would be in $\mathcal{L}'_Z$. Therefore, it contains at least $(1/200)SkL^{-1}$ points of $P \setminus P'_Z$. This allows us to derive the following inequality:

$$(1/200)SkL^{-1}|\mathcal{L}_0 \setminus \mathcal{L}'_Z| \leq I(P \setminus P'_Z, \mathcal{L}_0 \setminus \mathcal{L}'_Z)$$

This is a similar argument to Lemma 8.9. The similar idea being: derive a lower bound on the number of points a line in a certain set must contain and use this to derive a lower bound on the number of incidence between a point set and that set of lines. We will then examine properties of this point and line set to derive another upper bound on the incidences which will ultimately give us a bound on the number of lines that are in $|\mathcal{L}_0 \setminus \mathcal{L}'_Z|$. This then gives us a bound on the number of lines that must lie in $\mathcal{L}'_Z$. We will now complete the second part of this line of argument.

Since each point of P lies in at most $2k$ lines of $\mathcal{L}$:

$$I(P \setminus P'_Z, \mathcal{L}_0 \setminus \mathcal{L}'_Z) \leq I(P \setminus P'_Z, \mathcal{L}) \leq 2k|P \setminus P'_Z|$$

We once again see the importance of creating an upper bound on the number of lines our points can lie on. Now Lemma 8.11 tells us that $P \setminus P'_Z$ contains at most $10^{-7}S$ points. Combining the above we have

$$(1/200)SkL^{-1}|\mathcal{L}_0 \setminus \mathcal{L}'_Z| \leq 2k \cdot 10^{-7}S$$

If we simplify this expression, we see that

$$|\mathcal{L}_0 \setminus \mathcal{L}'_Z| \leq 4 \cdot 10^{-5}L$$

Thus almost all the lines of $\mathcal{L}_0$ lie in $\mathcal{L}'_Z$. We know that there are at least $(1/100)L$ lines in $\mathcal{L}_0$, and that at most $4 \cdot 10^{-5}L$ of them are not in $\mathcal{L}'_Z$. Thus $\mathcal{L}'_Z \geq (1/100)L - 4 \cdot 10^{-5}L \geq (1/200)L$. $\square$

Now we know that a definite fraction of our lines are either critical or flat. We will now bound the number of critical lines in Z. Once we obtain this bound, we know that the number of critical or flat lines in Z is $\geq (1/200)L$, so we see how many of these lines must be flat. Once we have a lower bound on the number of flat lines in Z, we will prove that a large majority of these lines must lie in planes contained in Z. By the pigeon hole principle, this will allow us to find a plane with a suitably large number of lines in it to prove our theorem.

Lemma 8.17. *A surface Z of degree d contains $\leq d^2$ critical lines.*

Proof: This lemma follows easily from Bézout's theorem applied to p and ∇p. As p has degree d and ∇p has degree $d-1$, this implies that p and ∇p can at most share $d(d-1)$ lines. Each of these shared lines is critical by definition and thus there are at most d^2 critical lines in Z. $\square$

We notice now that if A from equation (1) is sufficiently large, then d^2 will be much less than L. We explicitly record this calculation in the next lemma.

Lemma 8.18. *If A is sufficiently large, then $d \leq 10^{-4}L^{1/2}$*

Proof: The inequality in equation (1) implies that $1 \leq A^{-1}SL^{-3/2}k^2$. Thus

$$d \leq dA^{-1}SL^{-3/2}k^2 \lesssim A^{-1}L^{1/2}k^{-1}$$

If we choose A sufficiently large this completes the proof. $\square$

We explicitly proved and stated this lemma because it illustrates, in conjunction with Lemma 8.17 proves that Z contains at most $d^2 < 10^{-8}L$ critical lines. Since $\mathcal{L}'_Z$ contains at least $(1/200)L$ lines, we see that most of these lines must be flat. In particular, $\mathcal{L}'_Z$ contains at least $(1/300)L$ flat lines of Z.

Guth and Katz now use this to prove that Z contains some planes. We let Z_{pl} denote the union of all the planes contained in Z. We let $\tilde{Z}$ denote the rest of Z so that $Z = Z_{pl} \cup \tilde{Z}$. In terms of polynomials, Z is the vanishing set of p. The polynomials p factors into irreducibles $p = p_1 p_2 \cdots$. We separate these factors into two groups: factors of degree 1 and factors of degree greater than 1. Each factor of degree 1 defines a plane, and Z_{pl} is the union of these planes. The product of the remaining factors is a polynomial $\tilde{p}$, and $\tilde{Z}$ is the zero set of $\tilde{p}$. The point of making this distinction is that any line that lies in both Z_{pl} and $\tilde{Z}$ must be a critical line of Z. So a flat line of Z lies either in Z_{pl} or in $\tilde{Z}$ but not in both. A flat line of Z that lies in $\tilde{Z}$ is a flat line of $\tilde{Z}$ fairly clearly because if the polynomials if Lemma 8.12 vanish for Z and $\tilde{Z} \subseteq Z$, then they vanish when we restrict to $\tilde{Z}$. Now we use a lemma proved by Elekes and Sharir to bound the number of flat lines in a surface of degree $\leq d$.

Lemma 8.19 (Proposition 8, [4])**.** *If Z is an algebraic surface of degree $\leq d$ with no planar component, then Z contains $\leq 3d^2$ flat lines.*

We know that $\mathcal{L}$ contains at least $(1/300)L$ flat lines of Z by the above arguments. But $\tilde{Z}$ contains only $3 \cdot 10^{-8}L$ flat lines by Lemma 8.19 as we know that $d \leq 10^{-4}L^{1/2}$ by Lemma 8.18 and by construction $\tilde{Z}$ has no planar component. This tells us that the rest of the flat lines lie in Z_{pl}. In particular, $\mathcal{L}$ contains at least $(1/400)L$ lines in Z_{pl}.

Now we know that there are a lot of lines in Z_{pl}, and we know that the number of planes in Z_{pl} is $\leq d \lesssim L^2S^{-1}k^{-3}$. As the number of planes contained in a surface can be at most the degree of the surface, because each plane is a factor of degree one. So one of these planes must contain $\gtrsim Sk^3L^{-1}$ lines of $\mathcal{L}$ as a result of the Pigeon Hole Principle as there are at least $(1/400)L$ lines to be divided amongst at most $L^2S^{-1}k^{-3}$ planes. Thus at least one plane contains at least $\frac{(1/400)L}{(L^2S^{-1}k^{-3})} \sim Sk^3L^{-1}$ lines. In other words $B \gtrsim Sk^3L^{-1}$, since by definition there are no more than B lines contained in any plane.

At several points throughout this argument we need A to be sufficiently large. We now choose A large enough for all of this steps, i.e. we take the maximum A necessary. We thus conclude that either $S \leq AL^{3/2}k^{-2} + Lk^{-1}$ or else $S \lesssim LBk^{-3}$. In general this tells us that $S \leq C[L^{3/2}k^{-2} + Lk^{-1} + LBk^{-3}]$ as desired. This completes the proof of Proposition 8.12.

Guth and Katz consider Proposition 8.12 to be the heart of the proof of Theorem 8.3. Now that we have proved it we only need to reduce the general case to Proposition 8.12. We do this by first removing the assumption that many liens have roughly the average number of points and proving that the result reduces properly.

Proposition 8.13. *Let $k \geq 3$. Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$ with $\leq B$ lines in any plane. Let P be a set of S points so that each points meets between k and $2k$ lines of $\mathcal{L}$. Then*

$$S \leq C[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$$

Proof: Let $\mathcal{L}_1$ be the subset of lines in $\mathcal{L}$ which contain $\geq (1/100)SkL^{-1}$ points of P. If $\mathcal{L}_1 \geq (1/100)L$, then we have all the hypotheses of Proposition 8.12 and we have

$$S \leq C[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$$

Guth and Katz now show that S actually obeys this same estimate, with the same constant, regardless of the size of $\mathcal{L}_1$. The proof proceeds by induction on the number of lines. From now on we will assume that $|\mathcal{L}_1| \leq (1/100)L$, as otherwise as discussed we are done. We now only have finitely many size of $\mathcal{L}_1$ to consider. We know that the lines in $\mathcal{L}_1$ contribute the majority of the incidences as they contain a majority of the points in P. In particular we have the following inequality,

$$I(P, \mathcal{L} \setminus \mathcal{L}_1) \leq (1/100)SkL^{-1} \cdot L = (1/100)Sk$$

As there are at most L lines in $\mathcal{L} \setminus \mathcal{L}_1$, each of which is incident to at most $(1/100)SkL^{-1}$ points of P. We now define $P' \subset P$ to be the set of points with $\geq (9/10)k$ incidences with lines of $\mathcal{L}_1$. If $x \in P \setminus P'$ then x lies in at least k lines of $\mathcal{L}$ by construction, but less than $(9/10)k$ lines of $\mathcal{L}_1$. In other words, we know that x lies in at least $(1/10)k$ lines of $\mathcal{L} \setminus \mathcal{L}_1$. This tells us

$$(1/10)k|P \setminus P'| \leq I(P \setminus P', \mathcal{L} \setminus \mathcal{L}_1) \leq I(P, \mathcal{L} \setminus \mathcal{L}_1) \leq (1/100)Sk$$

If we divide through by $(1/10)k$ we have

$$|P \setminus P'| \leq (1/10)S$$

In particular this tells us that $|P'| \geq (9/10)S$. Thus, most of the points in P are incident to $\geq (9/10)k$ lines of $\mathcal{L}_1$. We know that a point of P' has at least $(9/10)k$ incidences with $\mathcal{L}_1$ and at most $2k$ incidences with $\mathcal{L}_1$. Once again we see the importance of the upper bound. Unfortunately, this is just a slightly larger range than we have considered before. In order to do induction, we need to reduce the range. We observe that $P' = P'_+ \cup P'_-$, where P'_+ consists of paris with $\geq k$ incidences to $\mathcal{L}_1$ and P'_- consists of points with $\leq k$ incidences with $\mathcal{L}_1$. We define P_1 to be the larger of P'_+ and P'_-. It has $\geq (9/20)S$ points in it as P' has $\geq (9/10)S$ points and the larger of the two subdivisions will have at least half the points of P'.

If we picked $P_1 = P'_+$ then we define $k_1 = k$. If we picked $P_1 = P'_-$ then we define k_1 to be the smallest integer $\geq (9/10)k$. Each point in P_1 has at least k_1 and at most $2k_1$ incidences with lines of $\mathcal{L}_1$. If we fall in the first case we know that each point has $\geq k$ incidences and also $\leq 2k$ incidences with $\mathcal{L}_1$. If we fall into the second case we that that each point has $\leq k$ incidences with lines in $\mathcal{L}_1$ and $\geq (9/10)k$ incidences, where we note that $2(9/10)k \geq k$. We also importantly note that k_1 is an integer $\geq (9/10)k \geq (27/10)$ as $k \geq 3$ and thus $k_1 \geq 3$.

The set of liens $\mathcal{L}_1$ and the set of points P_1 obey all the hypotheses of Proposition 8.12 using k_1 in place of k and the same B. We also note that there are fewer lines in $\mathcal{L}_1$ than in $\mathcal{L}$. Doing induction on the number of lines and applying the same argument, we may assume that our result holds for these sets $\mathcal{L}_1$ as we increase the size of $\mathcal{L}$ arbitrarily. If we denote $|\mathcal{L}_1| = L_1$ and $|P_1| = S_1$, we have

$$S_1 \leq C[L_1^{3/2}k_1^{-2} + BL_1k_1^{-3} + L_1k_1^{-1}]$$

We know that $S_1 \geq (9/20)S$, this implies that $S \leq (20/9)S_1$. Also we know that $L_1 \leq (1/100)L$ and that $k_1 \geq (9/10)k$. Using these relationships we have

$$S \leq (20/9)S_1 \leq [(20/9)(1/100)(10/9)^3]C_0[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$$

The braced product of fractions is < 1, and so S obeys the desired bound with the same constant. $\square$

In this proof we should recognize a familiar technique. Guth and Katz are able to prove a larger theorem about a set of points and lines by limiting their gaze to favorable sets of points and lines and relating the results from these favorable sets to the overall sets. If we can obtain sufficient bounds on the favorable sets we consider such as $\mathcal{L}_1$ and P_1 above, this can often allow us to prove more general results about the remaining points and lines we are considering. Finally with this proposition we are ready to prove Theorem 8.3:

Proof: Let $k \geq 3$. Suppose that $\mathcal{L}$ is a set of L lines with $\leq B$ in any plane. Suppose that P is a set of points, each intersecting at least k lines of $\mathcal{L}$. We subdivide the points $P = \bigcup_{j=0}^{\infty} P_j$, where P_j consists of the points incident to at least $2^j k$ lines and at most $2^{j+1}k$

lines. We define k_j to be $2^j k$. Then Proposition 8.13 applies to $(\mathcal{L}, P_j, k_j, B)$ as we have partitioned the points so that each set P_j meets between k_j and $2k_j$ lines of $\mathcal{L}$. We can thus conclude that

$$|P_j| \leq C_0[L^{3/2}k_j^{-2} + LBk_j^{-3} + Lk_j^{-1}] \leq 2^{-j}C_0[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$$

Now $S \leq \sum_j |P_j| \leq 2C_0[L^{3/2}k^{-2} + LBk^{-3} + Lk^{-1}]$. This completes the proof. □

We can now backtrack through our reduction argument from the beginning of this section to show how we proved the distinct distances problem by proving these two theorems. With Theorems 8.3 and 8.2 we proved that in general $|G_k(P)| \lesssim n^3k^{-2}$ for all $2 \leq k \leq n$. This proves Proposition 8.5. Now the number of quadruples in $Q(P)$ is expressed in terms of $|G_k(P)|$ in Proposition 8.4. Plugging in our bound for $|G_k(P)|$, we get that $|Q(P)| \lesssim N^3 \log(N)$, proving Proposition 8.1. Finally, the number of distinct distances is related to $|Q(P)|$ by Proposition 8.1. Thus plugging in our bound for $|Q(P)|$ we see that $|d(P)| \gtrsim N(\log(N))^{-1}$, proving the distinct distances problem (Theorem 8.1).

9 Conclusion

We conclude this survey with the proof of the Distinct Distances Problem as it acts as a pseudo-survey for the polynomial method. In it Guth and Katz employ degree reduction, polynomial partitioning, and Bézout's Theorem. They also generalize the Szemerédi and Trotter Theorem and employ the common practice of partitioning a given set of points and lines into subsets with more favorable conditions. Through a series of reduction arguments Guth and Katz proved that the potential reach of the Polynomial Method is almost limitless. We have seen it appear in the basic context of point-line incidences, curve-line incidences, construction of spanning trees, dense line incidences and finally in bounding distances.

We now want to discuss some potential future applications and questions. Particularly, we wonder how these techniques could be applied to the unit distances problem, which involves bounding the number of unit distances that can exist amongst a set of N points. Erdős also posed this problem in 1946 [5], and conjectured that the answer is $O(N\sqrt{\log(N)})$. If this were the case it would imply the distinct distances problem by a simple Pigeon-Hole argument. We want to know the minimal number of distinct distances amongst N points, we know that there are at most $O(N\sqrt{\log(N)})$ pairs at the same distance, and there are approximately N^2 pairs of points. Thus there are at least $O(N/\sqrt{\log(N)})$ distinct distances which is exactly what Erdős conjectured.

We also wonder how many distinct r-partitioning polynomials there are for a given set of points up to equivalence based on which points are grouped in each cell. The polynomial partitioning theorem guarantees the existences of such a polynomial, but it would be interesting to investigate exactly how many exist. This could shed more light on the properties of the zero sets of polynomials, and could lead to an explicit algorithm constructing such a polynomial.

We leave the reader with a question concerning the dependence of the polynomial method on the topology of the field over which we work. Particularly we notice that recently Toth [23] proved that the Szemerédi and Trotter theorem holds in the complex plane. However, he needed to produce a completely different proof as the proof we present in Section 4 depends on the Topology of $\mathbb{R}^2$. In particular, the Szemerédi and Trotter theorem relies on convexity in $\mathbb{R}^2$, which has no analogue and thus fails over finite fields. For example, if we let F be our finite field and P be the entire plane F^2, and L be all of the lines in F^2. We can see that $|P|$ and $|L|$ are both of order $O(|F|^2)$, however $I(P, L) = O(|F|^3)$ which is far larger than the Szemerédi and Trotter bound. So it makes sense that the topology of our field plays an essential role. For a deeper exploration of this topic we refer the reader to Tao's blog [21]. On the contrary, we can see that the proof of the Joints Problem can easily be generalized to higher dimensions and can apply to finite fields. Thus an interesting question to consider is how these techniques could be stripped of their reliance on the topology of the underlying field.

These are merely a few potential future avenues to explore with the Polynomial Method. We hope that this paper revealed the importance and elegance of this emerging field in extremal combinatorics.

References

[1] Karol Borsuk. Drei stze ber die n-dimensionale euklidische sphre. *Fundamenta Mathematicae*, 20(1):177–190, 1933.

[2] Roy O. Davies. Some remarks on the Kakeya problem. *Proc. Cambridge Philos. Soc.*, 69:417–421, 1971.

[3] Zeev Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22(4):1093–1097, 2009.

[4] György Elekes and Micha Sharir. Incidences in three dimensions and distinct distances in the plane. *Combin. Probab. Comput.*, 20(4):571–608, 2011.

[5] P. Erdös. On sets of distances of n points. *Amer. Math. Monthly*, 53:248–250, 1946.

[6] Larry Guth and Nets Hawk Katz. Algebraic methods in discrete analogs of the Kakeya problem. *Adv. Math.*, 225(5):2828–2839, 2010.

[7] Larry Guth and Nets Hawk Katz. On the Erdős distinct distances problem in the plane. *Ann. of Math. (2)*, 181(1):155–190, 2015.

[8] Axel Harnack. Ueber die Vieltheiligkeit der ebenen algebraischen Curven. *Math. Ann.*, 10(2):189–198, 1876.

[9] John Harris, Jeffry Hirst, and Michael Mossinghoff. *Combinatorics and Graph Theory.* Springer Science and Business Media, 2008.

[10] Robin Hartshorne. *Algebraic geometry.* Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[11] Nets Hawk Katz. The flecnode polynomial: a central object in incidence geometry. *ArXiv e-prints*, April 2014.

[12] I. N. Herstein. *Abstract algebra.* Macmillan Publishing Company, New York, second edition, 1990. With a preface by David J. Winter.

[13] Haim Kaplan, Jiří Matoušek, and Micha Sharir. Simple proofs of classical theorems in discrete geometry via the Guth-Katz polynomial partitioning technique. *Discrete Comput. Geom.*, 48(3):499–517, 2012.

[14] Frances Kirwan. *Complex Algebraic Curves.* Cambridge University Press, first edition, 1992.

[15] Jirí Matousek. *Using the Borsuk-Ulam Theorem.* Springer, second edition, 2008.

[16] James R. Munkres. *Topology.* Prentice Hall, Incorporated, 2000.

[17] János Pach and Micha Sharir. On the number of incidences between points and curves. *Combin. Probab. Comput.*, 7(1):121–127, 1998.

[18] René Quilodrán. The joints problem in $\mathbb{R}^n$. *SIAM J. Discrete Math.*, 23(4):2211–2213, 2009/10.

[19] E.B. Saff and A.D. Snider. *Fundamentals of Complex Analysis.* Pearson Education, third edition, 2003.

[20] A. H. Stone and J. W. Tukey. Generalized "sandwich" theorems. *Duke Math. J.*, 9:356–359, 1942.

[21] Terence Tao. The szemerédi and trotter theorem and the cell decomposition. *Online Blog*, 2009.

[22] Terence Tao. Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory. *EMS Surv. Math. Sci.*, 1(1):1–46, 2014.

[23] Csaba Toth. The szemeredi-trotter theorem in the complex plane. *ArXiv e-prints*, May 2003.

[24] Emo Welzl. Partition trees for triangle counting and other range searching problems. In *Proceedings of the Fourth Annual Symposium on Computational Geometry (Urbana, IL, 1988)*, pages 23–33. ACM, New York, 1988.

[25] Thomas Wolff. Recent work connected with the Kakeya problem. In *Prospects in mathematics (Princeton, NJ, 1996)*, pages 129–162. Amer. Math. Soc., Providence, RI, 1999.