The University of Melbourne

Department of Mathematics and Statistics

Polynomial Methods in Combinatorial Geometry

Kevin Scott Fray

Supervised by David Wood

Submitted in partial fulfillment of the
requirements for the degree of
Master of Science

May, 2013

Contents

Abstract

Problems in combinatorial geometry (also called discrete geometry) concern the combinatorial structure of discrete geometric structures. This thesis revolves around two extremely classical problems, both concerning finite sets of points in the plane—Erdős' *distinct distance problem* and the *ordinary line conjecture* of Dirac and Motzkin. Recently, each of these problems has been *almost* resolved, the former by Guth and Katz [27] and the latter by Green and Tao [25]. Both proofs involve the study of *algebraic curves* related to the geometric object, a technique that has come to be known as the *polynomial method*. In this thesis we give a thorough exposition of the polynomial method in combinatorial geometry, motivated by the proofs of the results of Guth-Katz and Green-Tao. Along the way we will see the symbiotic relationship between combinatorial geometry and arithmetic combinatorics. Our original contribution is work on the topic of isosceles triangles. We present several conjectures and a related new incidence bound.

Chapter 1

The Erdős Distance Problem

Consider the following puzzle:

> How can a farmer arrange his four farm buildings such that the distance between any two buildings is exactly 100m?

Equivalently, we are required to find a configuration of four points such that every pair is unit distance apart. The key to solving the puzzle is to realise that such a configuration does not exist—at least *in the plane*—the configuration we need is the vertices of a regular tetrahedron. The farmer must place (at least) one of the buildings on a hill or in a valley!

This puzzle is the simplest special case of an open question in the field of discrete geometry: precisely when do point sets with given distance distributions occur in the plane? More precisely, let P be a finite set of points in the plane, then the **distance distribution** is the function $D_P : \mathbb{R}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ given by

$$D_P(x) = \left|\{(a, b) \in P \times P \mid |a - b| = x \text{ and } a \neq b\}\right|.$$

The distance distribution contains all the information about the number of pairwise distances between points. Some visualisations of distance distributions are given in Figure 1.1.

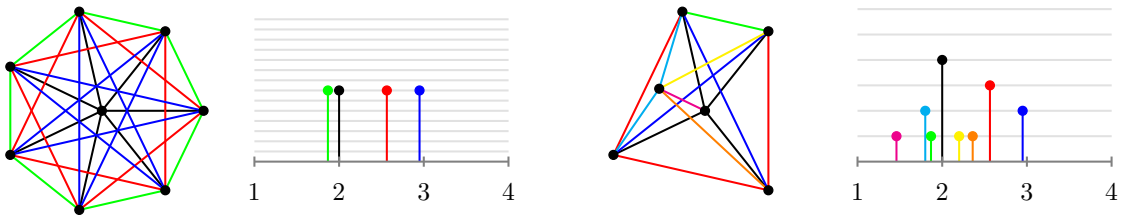


Figure 1.1: Distance distributions for some planar point sets

Our puzzle asks to find a point set with a specified distance distribution, so it is natural to consider this problem in general.

Problem 1.1. *Which functions $D : \mathbb{R}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ arise as distance distributions of finite sets of points in the plane?*

In general this problem is not well understood, and research has focused on special cases. Note that since we are only interested in finite point sets, the distance distribution has finite support. Hence it is natural to study the size of the support of D_P, the **number of distinct nonzero distances** determined by P:

$$d(P) = |\{|a-b| \mid (a,b) \in P \times P, a \neq b\}| = |\{x \in \mathbb{R} \mid D_P(x) \neq 0\} \setminus \{0\}|$$

In particular, we are interested in the relationship between $d(P)$ and $|P|$. Trivially, since P determines only $\binom{|P|}{2}$ pairs at nonzero distance, $d(P) \leq \binom{|P|}{2}$. Note that there are point sets that achieve this upper bound—in fact almost all point sets have no repeated nonzero distances, so determine exactly $\binom{|P|}{2}$ distances. Also, $d(P) \geq 1$ whenever $|P| \geq 2$ since there is at least one nonzero distance. We can restate the observation from the puzzle as the following

Proposition 1.2. *Let P be a finite set of points in the plane. If $d(P) = 1$ then $|P| \leq 3$.*

It is natural to wonder whether such a result always holds—given $d(P)$ can we bound $|P|$, or can we find arbitrarily large point sets that determine a bounded number of distances? To find a solution, consider again the puzzle. Suppose we have a set P of four points in the plane such that each pair are unit distance apart. Choose two of these points, a and b. Consider the circle of unit radius centred at a. Any other point of P is at unit distance from a and thus lies on this circle. The same holds for the circle of unit radius centred at b, so the remaining two points must lie at the two points of intersection of these circles. The puzzle is now solved because these two points are not at unit distance from each other, proving such a configuration does not exist in the plane.

Simply considering more than one distance in this argument, we obtain the following result first obtained by Erdős in 1944 (though his original proof was different, the proof we give can be found in [24]).

Proposition 1.3 (Erdős, [19])**.** *Let P be a finite set of points in the plane. Then*[1] $|P| \lesssim d(P)^2$.

Proof. Let a, b be distinct points in P. Let C_a (resp. C_b) be the collection of $d(P)$ circles centred at a (resp. b), with radii corresponding to the $d(P)$ distinct nonzero distances determined by P. Every point of $P \setminus \{a, b\}$ lies at an intersection point of a circle from C_a and a circle from C_b (Figure 1.2). Since two circles intersect in at most two points, the number of such intersections is at most $2|C_a||C_b| = 2d(P)^2$. Therefore $|P| - 2 = |P \setminus \{a, b\}| \leq 2d(P)^2$. □

[1]The notation $f(n) \lesssim g(n)$ has identical meaning to $f(n) \in O(g(n))$, and is common in the literature. We use this notation throughout.

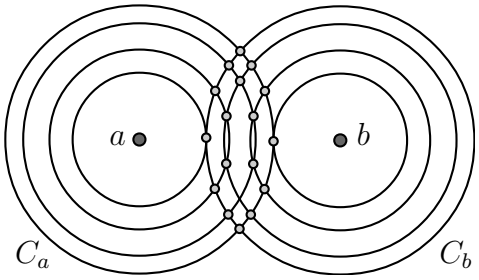
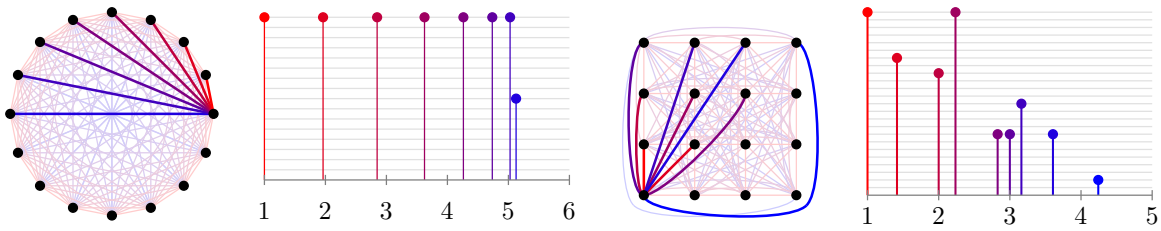


Figure 1.2: Points of P lie at the intersection of two sets C_a and C_b of circles.

Rearranging gives the bound $d(P) \gtrsim |P|^{\frac{1}{2}}$. That is, there do not exist arbitrarily large point sets that determine a bounded number of distances. Following on from this result, interest grew in trying to understand just how $d(P)$ grows with $|P|$. How small can $d(P)$ be when the size of $|P|$ is fixed? Looking back to Figure 1.1 we see that a point set determines few distances if it has a high degree of *symmetry*. In particular, consider the point set P given by the vertices of a regular n-gon. As shown for the case $n = 16$ in Figure 1.3, P determines $d(P) = \lfloor \frac{n}{2} \rfloor$ distances and one might conjecture that such examples minimise $d(P)$ due to the high degree of symmetry.



(a) Distances in a regular 16-gon.

(b) Distances in a 4-by-4 square grid.

Figure 1.3: Distance distributions for highly symmetric point sets.

However, the regular n-gons do not minimise $d(P)$—consider the regular square grids $\{(a, b) \mid a, b \in \mathbb{Z} \text{ and } 1 \leq a, b \leq \sqrt{n}\}$ for square $n \geq 1$. The case $n = 16$ (a 4×4 grid) is shown in Figure 1.3. Although it determines more distances than the 16-gon, for $\sqrt{n} \geq 12$ the $\sqrt{n}$-by-$\sqrt{n}$ grid determines *fewer* distances than the corresponding n-gon. As noted by Erdős, distances between points in the grid are of the form $\sqrt{x^2 + y^2}$ for integer x, y, and so the number of distinct distances is at most the number of different integers at most $2n$ that have a representation of the form $x^2 + y^2$ for integer x, y. This quantity was studied by Landau [34] and is known to be $\lesssim n/\sqrt{\log n}$, thus the grids asymptotically determine fewer distances than the regular n-gons. In Chapter 2 we will see that this is a consequence of the grids having more 'partial symmetries' in a way that will be made precise.

Erdős made the famous conjecture that the n-by-n grids *do* minimise $d(P)$, at least asymptotically:

Conjecture 1.4 (Erdős' Distinct Distances Conjecture, [19]). *Let P be a finite set of points in the plane. Then $d(P) \gtrsim |P|/\sqrt{\log |P|}$.*

We have already seen Erdős' 1946 result that $d(P) \gtrsim |P|^{\frac{1}{2}}$. Gradually improvements to this lower bound were discovered, including:

- $d(P) \gtrsim |P|^{\frac{2}{3}}$ in 1952 due to Moser [39];
- $d(P) \gtrsim |P|^{\frac{4}{5}}$ in 1992 due to Székely [54];
- $d(P) \gtrsim |P|^{\frac{6}{7}}$ in 2001 due to Solymosi and Toth [51];
- $d(P) \gtrsim |P|^{0.8641\ldots}$ in 2004 due to Katz and Tardos [32].

In November 2010, Larry Guth and Nets Katz posted to the arXiv '*On the Erdős distinct distance problem in the plane*' [27], in which they give the following almost optimal result.

Theorem 1.5 (Guth-Katz, [27]). *Let P be a finite set of points in the plane. Then $d(P) \gtrsim |P|/\log |P|$.*

Their proof introduces new ideas from algebraic geometry that have begun to be used to approach many other problems in discrete geometry from a new perspective. In Chapters 2–6, we give an account of the new methods used in their proof, and their relationship to other problems in the field.

For background material on topics in combinatorial geometry, see Pach and Agarwal [41] or Matoušek [36]. Similarly for background on basic algebraic geometry see Bix [3] or Silverman and Tate [50] and for topics in arithmetic combinatorics see Tao and Vu [57].

Chapter 2

Incidence Geometry

We begin by remarking that the proof of Proposition 1.3 in the previous chapter is a corollary of an elementary *incidence* theorem—a result about the number of points where a collection of geometric objects intersect.

Proposition 2.1. *Distinct circles in the plane intersect in at most two points.*

The proof is elementary, but for now we will not give it as we will find it is a consequence of a very general result (Theorem 4.3) in Chapter 4. In general, incidence problems about lines, circles, points and higher dimensional varieties are widely studied in combinatorial geometry. In this section we will give Elekes' reduction ([17]) of the Erdős distance problem to an incidence problem.

2.1 The distinct distances incidence problem

Recall the observation that point sets determining few distances possess a high degree of symmetry (c.f. Figure 1.3). To study this carefully, we will consider the *repeated* distances amongst the point sets. In particular, consider the collection of pairs of line segments of the same length determined by a point set P, or equivalently the set of *quadruples* formed by the endpoints of those segments:

$$Q(P) = \{(a,b,c,d) \in P^4 \mid |a-b| = |c-d| \neq 0\}.$$

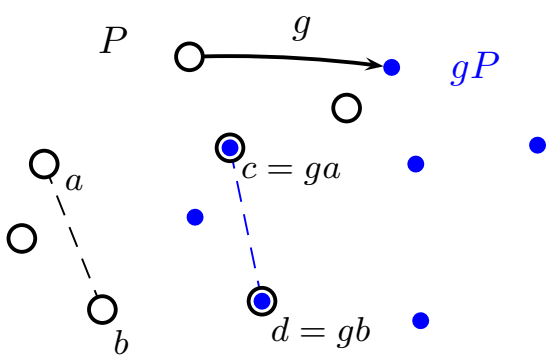
Note that $Q(P)$ contains the degenerate quadruples with $\{a,b\} = \{c,d\}$. If many segments share the same length, the number of distinct distances should be small. Indeed, let $d_1, d_2, \ldots, d_{d(P)}$ be the distinct nonzero distances determined by P, and let n_i be the number of ordered pairs $(a,b) \in P^2$ satisfying $|a-b| = d_i$. Then by the Cauchy-Schwarz inequality,

$$d(P)|Q(P)| = d(P)\sum_{i=1}^{d(P)} n_i^2 \geq \left(\sum_{i=1}^{d(P)} n_i\right)^2 = (|P|^2 - |P|)^2,$$

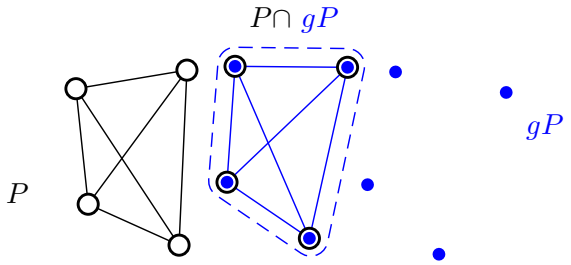
giving the bound

$$d(P) \geq \frac{|P|^4 - 2|P|^3}{|Q(P)|}. \tag{2.1}$$

Hence to estimate $d(P)$ it suffices to be able to estimate $|Q(P)|$.



(a) A quadruple (a, b, c, d) originates from an overlap of P and gP.



(b) The one-to-one correspondence between directed segments in $P \cap gP$ and directed segments in $g^{-1}(P \cap gP)$.

Figure 2.1: Studying the repeated distances in terms of partial symmetries g. The point set P is illustrated with white circles, and the transformed point set gP is illustrated with filled dark circles.

Elekes' idea was to transform the problem of estimating $|Q(P)|$ into an incidence problem by looking at the symmetries of the point set P, or more specifically the *partial symmetries*. That is, those rigid transformations g of the plane such that the image gP intersects the point set P. So, let G be the group of orientation-preserving rigid motions of the plane—the translations and rotations. Then for a given quadruple $(a, b, c, d) \in Q(P)$ there is a *unique* transformation $g \in G$ such that $g(a) = c$ and $g(b) = d$ — simply the composition of the translation sending a to c with a rotation about c. Therefore we can define a map $E : Q(P) \to G$ which takes each quadruple to the corresponding unique g.

Proposition 2.2. *Let P be a finite set of points in the plane. Then the function $E : Q(P) \to G$ given by*

$$(a, b, c, d) \mapsto \textit{the unique } g \in G \textit{ such that } ga = c \textit{ and } gb = d$$

is well-defined.

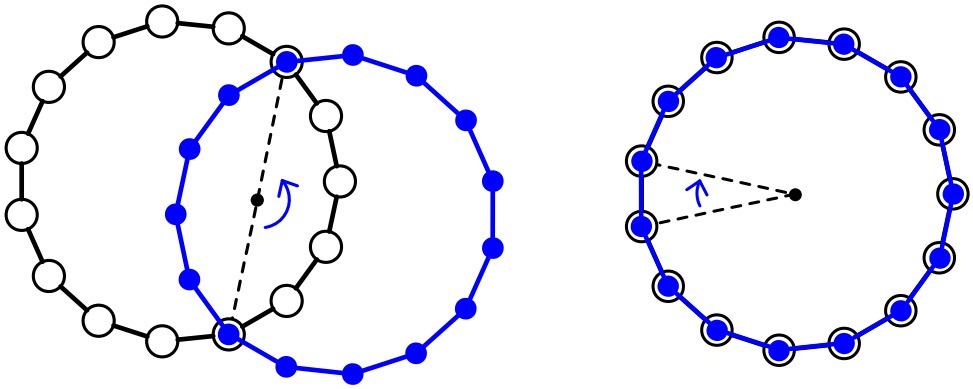
A transformation g is called a *partial symmetry* of P if $|P \cap gP| \geq 1$. The map E allows us to translate information about the partial symmetries of the point set P into information about the set of quadruples $Q(P)$.

Lemma 2.3. *Let P be a finite planar point set and let $g \in G$ be an orientation-preserving rigid motion. If $|gP \cap P| = k$ then $|E^{-1}(g)| = k(k-1)$.*

Proof. If $k = 0$ then there is no $a \in P$ with $ga \in P$ and hence $E^{-1}(G) = \emptyset$. Otherwise assume $k \geq 1$. Let $gP \cap P = \{p_1, \ldots, p_k\}$. For every $i = 1, \ldots, k$ we have $p_i = gq_i$ for some $q_i \in P$. For each pair $(p_i, p_j) \in (gP \cap P)^2$ with $p_i \neq p_j$ we have $(q_i, q_j, p_i, p_j) \in E^{-1}(g)$ (as in Figure 2.1b, each such segment (p_i, p_j) gives a quadruple when taken with its corresponding segment (q_i, q_j)). Since distinct pairs give distinct 4-tuples, $|E^{-1}(g)| \geq k(k-1)$. Conversely, if $(a, b, c, d) \in E^{-1}(g)$ then $c = ga$ and $d = gb$, so $c, d \in gP \cap P$ (see Figure 2.1a). Hence $|E^{-1}(g)| = k(k-1)$. □

Lemma 2.3 shows that $|Q(P)| = |E^{-1}(G)|$ can be computed from the number of partial symmetries of the point set P. To give some notation for the number of partial symmetries, let $G_{=k}(P) = \{g \in G \mid |gP \cap P| = k\}$ be those partial symmetries of size k. Notice that by Lemma 2.3 partial symmetries g with $k = 0$ or $k = 1$ satisfy $|E^{-1}(g)| = 0$. Hence by Lemma 2.3 we can count $|Q(P)|$ in terms of the partial symmetries of size 2 or greater,

$$|Q(P)| = \sum_{k=2}^{|P|} |G_{=k}(P)| k(k-1). \tag{2.2}$$



(a) A rotation about a chord gives a partial symmetry with $k = 2$.

(b) A rotation about the centre is a partial symmetry with $k = n$ (i.e. a full symmetry.)

Figure 2.2: Studying the repeated distances of Δ_n in terms of partial symmetries g. The point set Δ_n is illustrated with white circles, and the transformed point set $g\Delta_n$ is illustrated with filled dark circles.

Let us briefly return to look at the example of the regular n-gon Δ_n from the point of view of partial symmetries. Suppose g is a partial symmetry of Δ_n. Any three points in general position in the plane determine a unique circle. Hence if $|g\Delta_n \cap \Delta_n| \geq 3$, both Δ_n and $g\Delta_n$ lie on the same circle, so coincide. Thus every partial symmetry has $k = 2$ or $k = n$ (in which case it is a full symmetry.) One can check that the partial symmetries g with $k = 2$ are precisely rotations about the centre of a chord followed by a rotation about the centre of Δ_n (Figure 2.2a), and those with $k = n$ are precisely the rotations about the centre of Δ_n (Figure 2.2b). That is, $|G_{=2}(\Delta_n)| = \binom{n}{2} n$ and

$|G_{=n}(\Delta_n)| = n$. By (2.2),

$$|Q(P)| = 2\binom{n}{2}n + n(n-1)n = 2n^3 - 2n^2.$$

Hence, by (2.1), $d(P) \geq (n^4 - 2n^3)/(2n^3 - 2n^2) \approx n/2$. This is almost tight with the true value $\lfloor n/2 \rfloor$ because Δ_n has distances almost uniformly distributed (c.f. Figure 1.3), so our usage of Cauchy-Schwarz in the derivation of (2.1) is almost tight.

For technical reasons we will see in Chapter 6, it is easier to estimate the sizes of the sets $G_{\geq k}(P) = \{g \in G \mid |gP \cap P| \geq k\}$ than the sets $G_{=k}(P)$. Substituting $|G_{=k}(P)| = |G_{\geq k}(P)| - |G_{\geq k+1}(P)|$ into (2.2), we can estimate $|Q(P)|$ in terms of these sets,

$$|Q(P)| = \sum_{k=2}^{|P|} 2|G_{\geq k}(P)|(k-1). \tag{2.3}$$

Recall that we ultimately want to transform the distinct distances problem into an incidence problem. In particular, we want to relate the sets $G_{\geq k}(P) \subset G$ to the incidences of some family of structures inside G. Elekes' idea was to consider the family of sets $S_{p,q} = \{g \in G \mid gp = q\}$ of transformations taking p to q, for $p, q \in P$. Since transformations $g \in G_{\geq k}(P)$ take k' points in P to k' points in P for some $k' \geq k$, such g lie in at least k of the sets $S_{p,q}$.

Lemma 2.4. *Let P be a finite planar point set and $2 \leq k \leq n$. Then $|G_{\geq k}(P)|$ is exactly the number of elements $g \in G$ that are in at least k of the sets $S_{p,q}$ for $p, q \in P$.*

Proof. Let $g \in G_{\geq k}(P)$, and let $gP \cap P = \{p_1, p_2, \ldots, p_{k'}\}$ for some k' satisfying $k \leq k' \leq |P|$. Further, since $p_i \in gP \cap P$ let $p_i = gq_i$ for some $q_i \in P$. Then for each $i = 1, \ldots, k'$, $g \in S_{q_i,p_i}$. Hence g lies in at least $k' \geq k$ of the sets $S_{p,q}$. Conversely, if $g \in S_{q_i,p_i}$ for $i = 1, \ldots, k'$ where $k \leq k' \leq |P|$, then $p_i = gq_i$ and hence $p_i \in gP \cap P$. If $p_i = p_j$ then $q_i = q_j$ so $S_{q_i,p_i} = S_{q_j,p_j}$, hence $p_i \neq p_j$ whenever $i \neq j$. Thus $|gP \cap P| \geq k' \geq k$ so by definition $g \in G_{\geq k}(P)$. □

So, as desired, the quantities $|G_{\geq k}(P)|$ are the solutions to an incidence problem about the sets $L = \{S_{pq} \mid p, q \in P\}$. If the bound $|G_{\geq k}(P)| \lesssim |L|^{3/2}/k^2$ holds then by (2.3),

$$|Q(P)| \lesssim \sum_{k=2}^{|P|} 2|L|^{3/2}(k-1)/k^2 \sim |P|^3 \log |P|,$$

which by (2.1) gives the Guth-Katz result $d(P) \gtrsim |P|/\log |P|$.

Problem 2.5. *Let P be a finite planar point set, and let $L = \{S_{p,q} \subset G \mid p, q \in p\}$. If $G_{\geq k}(P)$ is the set of elements $g \in G$ contained in at least k of the sets $S_{p,q} \in L$, how big is $|G_{\geq k}(P)|$? In particular, is $|G_{\geq k}(P)| \lesssim |L|^{3/2}/k^2$?*

In Section 2.2 we will see that it makes sense to think of the sets $S_{p,q}$ as 'curves' in G, but for now we consider the incidence problem in Problem 2.5 as a purely combinatorial problem. If we study this incidence problem from the purely combinatorial viewpoint we arrive at a problem about *pseudolines.*

Definition 2.6. Let A be any set and L be a set of subsets of A. We call the elements of L **pseudolines** if they satisfy:

(i) If $l_1, l_2 \in L$ and $l_1 \neq l_2$ then $|l_1 \cap l_2| \leq 1$.

Pseudolines meet in at most one point[1].

(ii) If $p_1, p_2 \in A$ and $p_1 \neq p_2$ then $|\{l \in L \mid p_1 \in l, p_2 \in l\}| \leq 1$

There is at most one pseudoline through any two points.

Let us now verify that the 'curves' in our collection of sets $L = \{S_{p,q} \mid p, q \in P\}$ are pseudolines.

(i) If $g \in S_{a,b} \cap S_{c,d}$ for $S_{a,b} \neq S_{c,d}$ (so $(a, b) \neq (c, d)$) then $ga = b$ and $gc = d$ and there is at most one rigid transformation $g \in G$ that achieves this—the translation τ with $\tau a = b$ composed with a rotation θ about b such that $\theta\tau c = d$ (which only exists if $|a - c| = |b - d|$).

(ii) If $g_1, g_2 \in G$ both lie in $S_{p,q}$ and satisfy $g_1 \neq g_2$ then $g_1 p = q = g_2 p$ and p is a fixed point of the transformation $g_2^{-1} g_1$. Recall that all nontrivial orientation-preserving rigid motions have at most one fixed point. Hence since $g_1 \neq g_2$, $g_2^{-1} g_1$ is not the identity transformation, p (and hence q) is unique.

Finally we will show how far purely combinatorial results can get us. First we state the combinatorial incidence results we will prove.

Lemma 2.7. *Let S be a set, $P \subset S$ be a set of points, and L be a set of pseudolines in S. Then we can bound the number of incidences $I(P, L) = |\{(p, l) \mid p \in P, l \in L, p \in l\}|$ by*

(a) $I(P, L) \lesssim |L|^2 + |P|$ *and* $I(P, L) \lesssim |P|^2 + |L|$

(b) $I(P, L) \lesssim |L||P|^{1/2} + |P|$ *and* $I(P, L) \lesssim |P||L|^{1/2} + |L|$

Though the first of these is a weaker bound, we give it here as we will find use for it later. The bounds with $|P|$ and $|L|$ exchanged follow by duality (see Section 8.1). To see the relation to the incidence problem from Problem 2.5, we postpone the proof of Lemma 2.7 to first give the following corollary.

[1]Sometimes it is required that pseudolines meet in exactly one point, so we emphasise that we are using a weaker notion in this document.

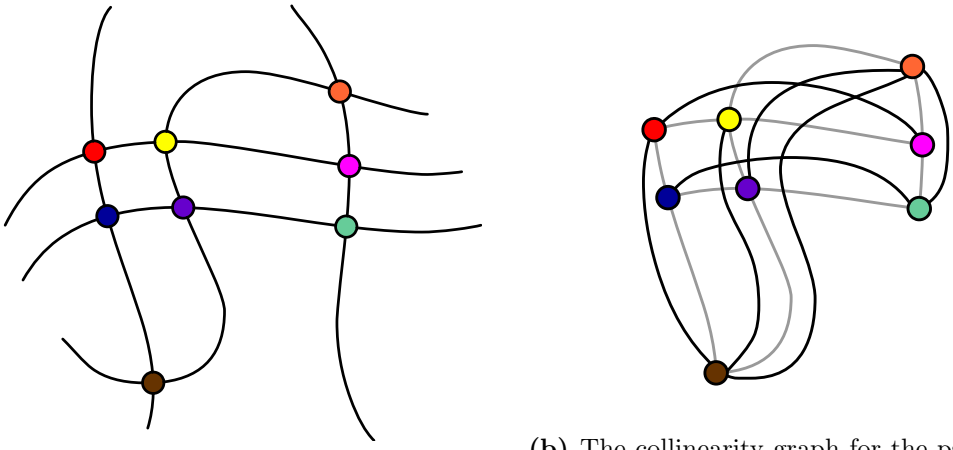
Corollary 2.8. *Let S be a set and L be a set of pseudolines in S. Then we can bound the size of the set of incidences $I_{\geq k}(L) = |\{p \in S \mid p \in l_1, l_2, \ldots, l_{k'} \text{ for some } k' > k\}|$ of at least k pseudolines in L by*

$$(a) \quad |I_{\geq k}(L)| \lesssim \frac{|L|^2}{k} \qquad \text{and} \qquad (b) \quad |I_{\geq k}(L)| \lesssim \frac{|L|^2}{k^2}$$

Proof. We only prove (a) as the deduction of (b) is the same, simply using Lemma 2.7(b) rather than Lemma 2.7(a). Set $P = I_{\geq k}(L)$. By Lemma 2.7(a) applied to P and L,

$$|P|k \leq I(P, L) \lesssim |L|^2 + |P|.$$

That is, $|P|(k-1) \lesssim |L|^2$ and hence $|I_{\geq k}(L)| = |P| \lesssim |L|^2/k$. □



(a) An arrangement of pseudolines, with intersection points illustrated.

(b) The collinearity graph for the pseudoline arrangement. Edges between adjacent vertices on the pseudolines are lightened for clarity.

Figure 2.3: The construction of the collinearity graph of an arrangement of pseudolines.

Proof of Lemma 2.7. Let $L = L_{\leq 1} \cup L_{\geq 2}$ where $L_{\leq 1}$ consists of the lines containing at most one point of P and $L_{\geq 2}$ those containing at least two points. Thus $I(P, L) = I(P, L_{\leq 1}) + I(P, L_{\geq 2})$. First note that $I(P, L_{\leq 1}) \leq |L_{\leq 1}| \leq |L|$.

To bound $I(P, L_{\geq 2})$, construct the *collinearity graph* of G with vertices $V = P$ and an edge $p_1 \sim p_2$ if there is a pseudoline $l \in L$ with $p_1 \in l$ and $p_2 \in l$. This construction is illustrated in Figure 2.3. Each edge $p_1 \sim p_2$ is associated to a unique $l \in L$ since two points determine at most one pseudoline, so this construction produces a graph rather than a multigraph.

Proof of (a). Since each edge corresponds to at most two incidences, $I(P, L_{\geq 2}) \leq 2|E(G)|$. Also $|E(G)| \leq \binom{|P|}{2} \leq |P|^2$ since $|V| = |P|$. Thus

$$I(P, L) \leq I(P, L_{\leq 1}) + I(P, L_{\geq 2}) \leq |L| + 2\binom{|P|}{2} \lesssim |L| + |P|^2.$$

Proof of (b). Let $l_1, \ldots, l_{|L|}$ be the pseudolines in L, and let n_i be the number of points of P on line l_i. Line l_i contributes $\binom{n_i}{2}$ edges to G, so

$$\sum_{i=1}^{|L|} \binom{n_i}{2} = |E(G)| \leq \binom{|P|}{2} \quad \text{and hence} \quad \sum_{i=1}^{|L|} (n_i - 1)^2 \leq |P|^2.$$

Applying Cauchy-Schwarz,

$$\begin{aligned} I(P, I_{\geq 2}(L)) = \sum_{n_i \geq 2} n_i \leq |L| + \sum_{i=1}^{|L|} (n_i - 1) &\leq |L| + |L|^{1/2} \left(\sum_{i=1}^{|L|} (n_i - 1)^2 \right)^{\frac{1}{2}} \\ &\leq |L| + |L|^{1/2} |P|. \end{aligned}$$

Therefore $I(P, L) \leq I(P, L_{\leq 1}) + I(P, L_{\geq 2}) \lesssim |L| + |L|^{1/2}|P|$. □

To see how far these purely combinatorial techniques have propelled us, we substitute the bound Corollary 2.8*(b)*, into (2.3) to get

$$|Q(P)| \lesssim \sum_{k=2}^{|P|} 2 \frac{|L|^2}{k^2} (k-1) \approx |P|^4 \log |P|,$$

recalling that our incidence problem involves $|L| = |P|^2$ pseudolines. This bound on the number of quadruples implies (by (2.1)) the (very underwhelming) bound $d(P) \gtrsim \frac{1}{\log |P|}$. As far as solving our incidence problem, this is as far as purely combinatorial techniques can take us, since the bound (b) is tight for pseudolines. For example take P to be an $n \times n$ grid in the plane and L to be the $2n$ horizontal and vertical lines through the grid — the number of incidences is $I(P, L) = 2n^2 \approx |L||P|^{1/2} + |L|$.

In the next section, we find that to resolve our incidence problem we need to exploit additional geometric structure—the structure of the group G of transformations and the structure of our collection of 'curves' $S_{p,q}$.

2.2 The geometry of Elekes' incidence problem

In the previous section we saw Elekes' transformation of the distinct distances problem to an incidence problem in the group G of rigid orientation-preserving transformations of the plane. To have a hope of solving this incidence problem, we need to understand the geometry of the 'curves' $S_{p,q}$ whose intersections we wish to understand. In this section we will give Guth and Katz' observation [27, Section 2] that we can further reduce to an incidence problem about *lines* in $\mathbb{R}^3$.

First, we note that almost all transformations $g \in G$ are rotations, so it is not unreasonable to expect that also most incidences occur at rotations. It turns out this is in some sense correct, since it is easy to bound the number of incidences occurring

at translations. To see this, let G^{rot} consist of the rotations $g \in G$, and G^{trans} consist of the translations. Then $G = G^{rot} \cup G^{trans}$ and in an analogous way we decompose $G_{\geq k}(P) = G^{rot}_{\geq k}(P) \cup G^{trans}_{\geq k}(P)$.

As hoped, the number of incidences at translations obeys the desired bound from Problem 2.5.

Lemma 2.9. $|G^{trans}_{\geq k}(P)| \lesssim |L|^{3/2}/k^2$.

Proof. Let $Q^{trans}(P)$ consist of those quadruples in $Q(P)$ arising from translations. If $(a, b, c, d) \in Q^{trans}(P)$ then $d = c + (b - a)$, so that d is determined from a, b, c. Hence $|Q^{trans}(P)| \leq |P|^3 = |L|^{3/2}$. By the derivation of (2.2), we can restrict (2.2) to just translations,

$$|L|^{3/2} \geq |Q^{trans}(P)| = \sum_{i=2}^{|P|} i(i-1)|G^{trans}_{=i}(P)| \geq k(k-1)|G^{trans}_{\geq k}(P)|,$$

that is, $|G^{trans}_{\geq k}(P)| \lesssim |L|^{3/2}/k^2$ as desired. □

Having dealt with translations, we can turn to understanding the incidences at rotations. The advantage of isolating the rotations is that the geometry is far easier to understand. Any planar rotation g is a rotation around some fixed point $f = (f_x, f_y)$ by an angle θ. Hence the space has a natural parameterisation[2] $\eta : G^{rot} \to \mathbb{R}^2 \times (0, 2\pi)$ taking $g \mapsto (f_x, f_y, \theta)$. To understand the incidences of the sets S_{pq} in G^{rot}, we can study the incidences of the images $\eta(S_{pq} \cap G^{rot})$ in the much more familiar space $\mathbb{R}^2 \times (0, 2\pi)$.

As first noticed by Guth and Katz [27], this parameterisation is especially simple if we 'stretch' it to fill $\mathbb{R}^3$ appropriately. Specifically, define $\rho : G^{rot} \to \mathbb{R}^3$ by

$$\rho(g) = (f_x, f_y, \cot \frac{\theta}{2}) \tag{2.4}$$

for f_x, f_y, θ as above. Amazingly, by stretching the parameterisation in this way the images $L_{p,q} = \rho(S_{pq} \cap G^{rot})$ becomes *lines*.

Proposition 2.10. *If $p = (p_x, p_y)$ and $q = (q_x, q_y)$ are points in $\mathbb{R}^2$ then the set $L_{p,q}$ is a line in $\mathbb{R}^3$.*

Proof. Consider any $g \in S_{pq} \cap G^{rot}$. As in Figure 2.4, let $m = (p + q)/2$ denote the midpoint of pq and let f be the fixed point of g on the perpendicular bisector of p and q. We will only give the proof in the general case $p \neq q$ and $f \neq m$—the degenerate cases are similar and simpler. We have $\cot \frac{\theta}{2} = \frac{||f-m||}{||p-m||}$. Let us write $f = m + \frac{f-m}{||f-m||}||f - m||$, and note that

$$||p - m|| \frac{f - m}{||f - m||} = \left(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2} \right).$$

[2]The original parameterisation proposed by Elekes considered g as a rotation by θ about the origin followed by a translation by (x, y), and parameterised g by $g \mapsto (x, y, \theta)$. Unfortunately the images of the $S_{p,q}$ under this parameterisation are *helices* in $\mathbb{R}^2 \times (0, 2\pi)$ and proved difficult to understand.

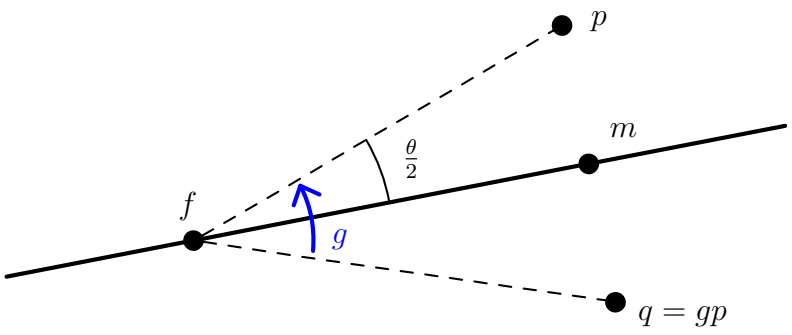


Figure 2.4: Computing the angle of rotation of the rotation taking p to q.

Hence

$$\rho(g) = \left(f_x, f_y, \frac{||f-m||}{||p-m||}\right) = \left(\frac{p_x+q_x}{2}, \frac{p_y+q_y}{2}, 0\right) + \frac{||f-m||}{||p-m||}\left(\frac{q_y-p_y}{2}, \frac{p_x-q_x}{2}, 1\right).$$

As g ranges over all rotations taking p to q, $\frac{||f-m||}{||p-m||}$ assumes all values in $\mathbb{R}$, so that

$$L_{pq} = \left\{\left(\frac{p_x+q_x}{2}, \frac{p_y+q_y}{2}, 0\right) + t\left(\frac{q_y-p_y}{2}, \frac{p_x-q_x}{2}, 1\right) : t \in \mathbb{R}\right\} \tag{2.5}$$

is indeed a line. □

Redefining our notation from before (pg. 8), we will now let $L = \{L_{pq} \mid p, q \in P\}$ be the set of lines in $\mathbb{R}^3$. Since we have removed a point (the translation) from each of our curves, we first verify that they are still distinct.

Proposition 2.11. $|L| = |P|^2$

Proof. Let $L_{a,b}$ and $L_{c,d}$ be two lines in L. Again we just give the argument in the general case $a \neq b$ and $a \neq c$, since similar arguments work in the degenerate cases. Let g be the rotation by 180° around the midpoint of a and b, so $g \in S_{ab}$. If $g \notin S_{cd}$ we are done, since the lines do not share the point $\rho(g)$, so are distinct. Otherwise c and d lie on the line $\overline{ab}$. For any other rotation $g' \in S_{ab}$, $g' \notin S_{cd}$ since a is the only point on $\overline{ab}$ for which $g'(a)$ is also on $\overline{ab}$, and we have assumed $c \neq a$. □

We have seen that our main problem can be transformed into an incidence problem about $|P|^2$ lines in $\mathbb{R}^3$. It makes sense, then, to wonder in what generality this incidence problem holds. Will the desired bound hold for an *arbitrary* set of lines in $\mathbb{R}^3$.

Problem 2.12. *Let L be a finite set of lines in $\mathbb{R}^3$. If $I_{\geq k}(L)$ is the set of points in $\mathbb{R}^3$ contained in at least k of the lines $l \in L$, how big is $I_{\geq k}(L)$? In particular, is $|I_{\geq k}(L)| \lesssim |L|^{3/2}/k^2$?*

Unfortunately, examples exceeding this bound are easy to construct. For instance, consider the case where all lines of L lie in a plane, with no two parallel. Since each pair intersects, there are $|I_{\geq 2}(L)| \gtrsim |L|^2$ intersections of $k = 2$ or more lines. Similarly for $k = 3$ one could take the lines L to form a finite section of a triangular lattice, so that $|I_{\geq 3}(L)| \gtrsim |L|^2$. Fortunately, the special properties of the lines L_{pq} rule these sorts of examples out for the lines we are looking at.

Proposition 2.13. *L_{pq} and $L_{pq'}$ are disjoint and have different directions if $q \neq q'$.*

Proof. If $g \in L_{pq} \cap L_{pq'}$ then $q' = g(p) = q$, so the lines are disjoint. By the parameterisation of L_{pq} in (2.5), if they have the same direction then $(\frac{q_y - p_y}{2}, \frac{p_x - q_x}{2}, 1) = \lambda(\frac{q'_y - p_y}{2}, \frac{p_x - q'_x}{2}, 1)$ so $\lambda = 1$. This implies $q_y - p_y = q'_y - p_y$ so $q_y = q'_y$. Similarly, $p_x - q_x = p_x - q'_x$ so $q_x = q'_x$. That is, $q = (q_x, q_y) = (q'_x, q'_y) = q'$. □

Corollary 2.14. *At most $|L|^{1/2} = |P|$ lines of L lie in a given plane π.*

Proof. By Proposition 2.13, if two lines $L_{p,q}$ and $L_{p,q'}$ were contained in π then they would intersect. However, these lines are disjoint as one cannot simultaneously have $p = gq$ and $p = gq'$. Hence for each $p \in P$ there is at most one $q \in P$ such that $L_{p,q} \subset \pi$, so π contains at most $|P|$ lines of L. □

Having ruled out this instance, one would again ask whether Problem 2.12 holds in the restricted case where at most $|L|^{1/2}$ lines lie in any one plane. Yet again it turns out that this is not the case—if our lines L all lie in a *doubly ruled surface*, with half of the lines in each ruling, then again $|I_{\geq k}(L)| \gtrsim |L|^2$. However since the only k-ruled surface for $k \geq 3$ is the plane, these types of exceptions don't exist for $k \geq 3$. In fact, Guth and Katz proved the following incidence theorem.

Theorem 2.15 (Guth-Katz, [27, Proposition 2.11])**.** *Let L be a finite set of lines in $\mathbb{R}^3$ for which no more than $|L|^{1/2}$ lie in a common plane, and let $3 \leq k \leq |L|^{1/2}$. Then $|I_{\geq k}(L)| \lesssim |L|^{3/2}/k^2$.*

In the next section we will investigate the exceptional examples lying in ruled surfaces that arise in the $k = 2$ case.

2.3 Ruled Surfaces

We now turn to the theory of ruled surfaces. We give the relevant results without proof, though the interested reader shall find an exposition in [27, Section 3]. A more through treatment of the theory of ruled surfaces is available in [47, Chapter XIII, Part 3]. The fundamental definition is:

Definition 2.16. Let $S \subset \mathbb{R}^3$ be an algebraic surface, and $k \geq 1$. We say S is **k-ruled** if through every point on S there are k *distinct* lines which are contained in the surface S. A 1-ruled surface is called **singly-ruled** and a 2-ruled surface is called **doubly-ruled**.

We give special names to the $k = 1, 2$ cases because the only surface which is 3-ruled, or k-ruled for any $k \geq 3$, is a plane (sometimes the plane is called ∞-ruled). Non-planar examples are given by a cylinder or a cone, both of which are singly ruled, or a hyperboloid of one sheet which is doubly-ruled (these examples are illustrated in Figure 2.5.) Other examples are given by *reguli*.

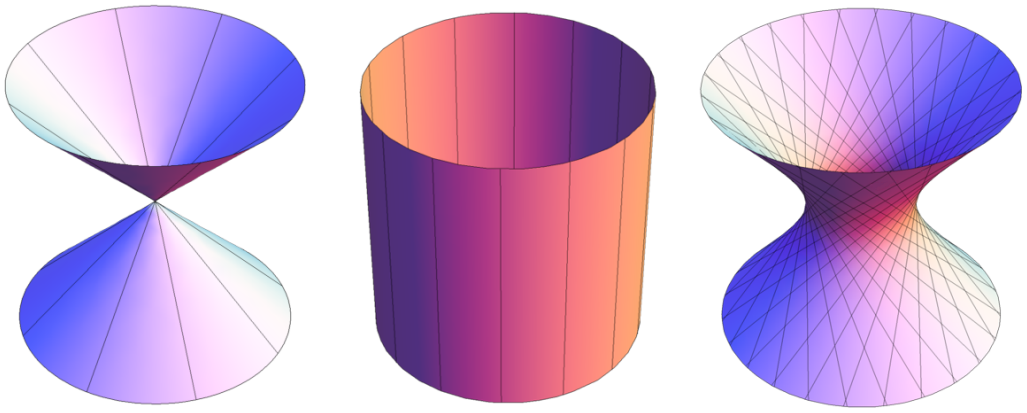


Figure 2.5: The singly-ruled cone and cylinder and a doubly-ruled hyperboloid. Some lines contained in each of the surfaces are shown.

Definition 2.17. An algebraic surface $S \subset \mathbb{R}^3$ is a **regulus** if there are three pairwise skew lines l_1, l_2, l_3 such that S is the union of the family of lines that intersect all three lines l_1, l_2, and l_3.

It is not obvious, but any choice of three pairwise skew lines gives a regulus by this construction (that is, the union S is an algebraic surface). For example, in Figure 2.6 a regulus has been constructed from the three lines

$$l_1 = \{(-1, t, 0) \mid t \in \mathbb{R}\}, \quad l_2 = \{(0, s, s) \mid s \in \mathbb{R}\}, \quad l_3 = \{(1, 0, r) \mid r \in \mathbb{R}\}.$$

The family of lines intersecting all three lines l_1, l_2, and l_3 is the family of lines connecting $(-1, t, 0), (0, t/2, t/2)$, and $(1, 0, t)$ for each $t \in \mathbb{R}$. The corresponding regulus S is doubly-ruled, for instance the point $(-1, t, 0) \in l_1$ is contained in the aforementioned line as well as the line l_1 itself. In fact, every regulus is doubly-ruled, and moreover we have now seen *all* doubly-ruled surfaces.

Proposition 2.18 (Classification of Ruled Surfaces, [47])**.** *Let $S \subset \mathbb{R}^3$ be an irreducible ruled surface. Then exactly one of the following holds*

(i) S is a plane and S is k-ruled for every $k \geq 3$;

(ii) S is a regulus and S is doubly-ruled;

(iii) S is singly-ruled.

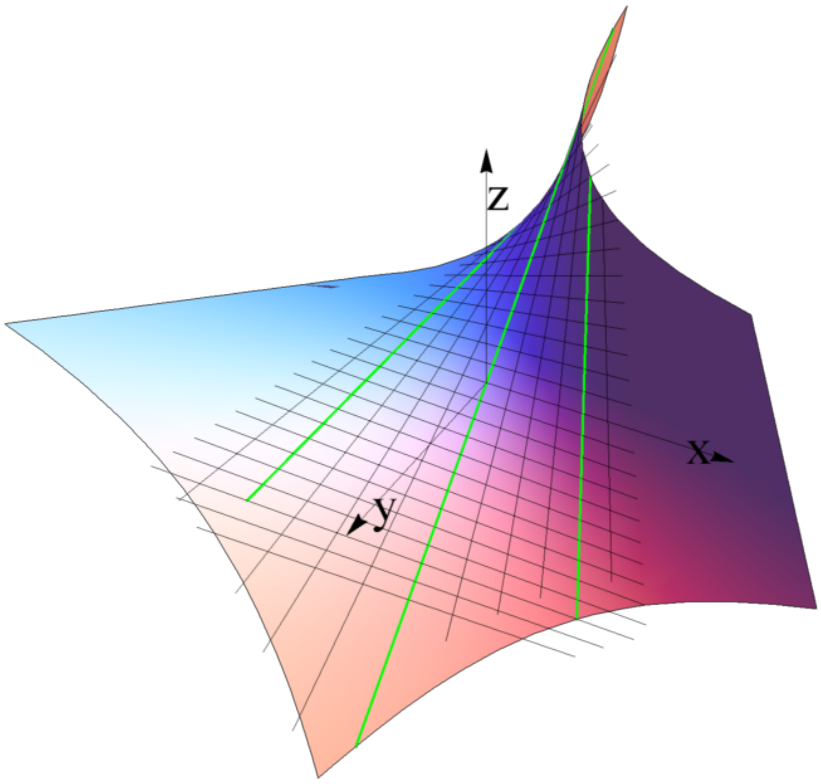


Figure 2.6: Example of a regulus determined by the three highlighted lines l_1, l_2, l_3. We show some of the lines in each direction of the ruling, and the surface formed by the union of lines intersecting all of l_1, l_2, and l_3.

Returning to our incidence problem, we have an analogous result to Corollary 2.14 for reguli.

Lemma 2.19 ([27, Proposition 2.8])**.** *The number of lines of L lying in a given regulus S is $\lesssim |L|^{1/2}$.*

In an analogous way to Theorem 2.15, it turns out that the plane and reguli examples are the only examples contradicting the incidence theorem for $k = 2$.

Theorem 2.20 (Guth-Katz, [27, Proposition 2.10])**.** *Let L be a finite set of lines in $\mathbb{R}^3$ for which at most $|L|^{1/2}$ lie in a common plane, and $\lesssim |L|^{1/2}$ lie in a common regulus. Then $|I_{\geq 2}(L)| \lesssim |L|^{3/2}$.*

So far, we have seen Elekes' reduction of the Erdős distinct distances problem to an incidence problem and how by studying the geometry of the resulting problem, Guth and Katz isolated the properties of the incidence problem that give the desired bounds in Theorem 2.15 and Theorem 2.20. In Chapters 3–6 we introduce the polynomial method and show how it has been used by Guth and Katz to prove these two bounds.

Chapter 3

Dvir's Polynomial Method

In 2008, Dvir solved the long outstanding finite field Kakeya problem with a remarkably simple argument exploiting the behaviour of polynomials. His proof introduced algebraic ideas that are the core of Guth and Katz' bound on the Erdos distinct distances problem. In this section we will present his use of what is now called the *polynomial method* to solve this problem. To begin with, we define the finite-field Kakeya problem.

Problem 3.1. *Let $\mathbb{F}$ be a finite field. Call a set $K \subset \mathbb{F}^n$ a* **Kakeya set** *if it contains a line in every direction—that is, for every direction $x \in \mathbb{F}^n$ there is a line $\{y+tx \mid t \in \mathbb{F}\}$* contained *in K. What is the minimum size of a Kakeya set?*

This problem was first considered by Wolff [58], as a simpler version of the (still open) problem for infinite fields, which instead considers sets containing line *segments* in every direction. Prior to Dvir's work, the lower bound was conjectured to be $\gtrsim |\mathbb{F}|^n$ but the strongest known bound was just $\gtrsim |\mathbb{F}|^{4n/7}$ due to Rogers [46]. In 2008, Dvir [13] proved this conjecture with a remarkably simple proof using the polynomial method, even obtaining a respectable estimate of the constant in the bound.

3.1 The Polynomial Method

We begin by defining the basic object of study in the polynomial method.

Definition 3.2. Let $p \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial. The **degree** of p is the largest value of $a_1 + \cdots + a_n$ for all monomials $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ in p. The **zero set** of p is $Z(p) = \{x \in \mathbb{F}^n \mid p(x) = 0\}$.

The zero set of p depends on the ring we consider p to be a member of. For instance, $Z(x) = \{0\}$ if we consider x to belong to the ring $\mathbb{F}[x]$, while $Z(x) = \{(0, y) \mid y \in \mathbb{F}\}$ if we consider x to belong to the ring $\mathbb{F}[x, y]$. Whenever we refer to $Z(p)$ the ring in question will be clear from context. We also remark that where we will use *degree* some authors prefer *total degree*; we use the former since it is the only concept of degree that we use. Similarly we use the term *zero set* where others may find *variety* or *algebraic curve/surface* more familiar.

The essence of the polynomial method is studying a combinatorial structure by relating it to the zero set $Z(p)$ of some polynomial p. In the applications we will see, the procedure is as follows.

(i) We have a finite set S in some field $\mathbb{F}^n$ and we want to bound its size.

(ii) Find a *nonzero* polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ with $S \subset Z(p)$ of 'small' degree.

(iii) Use the properties of the set S together with the low degree of the polynomial p to conclude that S cannot be contained in $Z(p)$, a contradiction.

Intuitively, the polynomial method works because the 'complexity' of $Z(p)$ is closely related to the degree of p. If one can use the properties of S to conclude it is more 'complex' than $Z(p)$, one can arrive at a contradiction. We will see how this outline is implemented in Dvir's resolution of the finite-field Kakeya conjecture, but first we must give some basic results about polynomials that allow us to achieve (ii) and (iii).

3.2 Properties of Polynomials

Remarkably, step (ii) is often achieved with a general polynomial existence result, rather than by using the structure of S to construct a polynomial. Thinking about this problem in dimension $n = 1$, the obvious construction is to take the product

$$p(x) = \prod_{s \in S} (x - s)$$

giving a polynomial with $S \subset Z(p)$ of degree $d = |S|$. The natural generalization to 2-dimensions is to again let p be the product of linear factors, so that the zero set of each factor is a line. One can choose these lines to vanish on at least 2 points of S, giving a polynomial of degree $d = \lceil \frac{|S|}{2} \rceil$. Similarly in n dimensions, the analogous construction gives a polynomial of degree $d = \lceil \frac{|S|}{n} \rceil$. For applications, this naïve approach is much too weak—using only linear factors is far too restrictive. A much more efficient approach is available, using simple linear algebra.

Lemma 3.3. *Let $\mathbb{F}$ be any field and $S \subset \mathbb{F}^n$ a finite set. Then there is a* nonzero *polynomial vanishing on S of degree $d \lesssim |S|^{1/n}$, where the hidden constant depends on n (or precisely, of any degree d such that $\binom{n+d}{d} > |S|$).*

Proof. Consider a general polynomial $p(x_1, \ldots, x_n)$ of degree d. It has $\binom{n+d}{d}$ coefficients. For each $s = (s_1, \ldots, s_n) \in S$, we have the linear equation $p(s_1, \ldots, s_n) = 0$ in the $\binom{n+d}{d}$ coefficients. Taking all of these $|S|$ equations, we see that there is a nonzero polynomial of degree d vanishing on S if and only if this system has a nonzero solution. Hence we have a solution whenever $\binom{n+d}{d} > |S|$. Rearranging, we will have a solution with $d \lesssim |S|^{1/n}$ where the hidden constant depends on n. □

This takes care of constructing vanishing polynomials. To carry out (*iii*), one technique is to show that our polynomial is in fact zero, contradicting that we constructed a nonzero polynomial. To show that the polynomial is zero, we have several standard results that can show if a polynomial vanishes in one place is must vanish in another. The first of these is the familiar result that a nonzero degree d polynomial has at most d zeros.

Proposition 3.4. *Let $\mathbb{F}$ be a field and $p \in \mathbb{F}[x]$ be a* nonzero *polynomial of degree d. Then $|Z(p)| \leq d$.*

Proof. Simply apply the fact that if $p(a) = 0$ then $(x - a)$ divides p (a consequence of division of polynomials, since if $p(x) = (x-a)q(x)+r(x)$ then $0 = p(a) = (a-a)q(a)+r(a) = r(a)$). □

This proposition is usually used in its contrapositive form, to conclude that a polynomial *is zero* because it vanishes in too many places. We also remark that for finite fields, we cannot use the proposition in this way for polynomials of degree $|\mathbb{F}|$ or more, since there are not $|\mathbb{F}| + 1$ points at which the polynomial vanishes.

From this, we can derive the following lemma that implements the concept that low-degree polynomials have 'simple' zero-sets.

Lemma 3.5. *Let $\mathbb{F}$ be a field and $p \in \mathbb{F}[x_1, \ldots, x_n]$ be a* nonzero *polynomial of degree d. Also, let $L = \{y + tx \mid t \in \mathbb{F}\} \subset \mathbb{F}^n$ be a line in $\mathbb{F}^n$. If $|Z(p) \cap L| > d$ then $L \subset Z(p)$. (That is, any line not contained in $Z(p)$ intersects $Z(p)$ in at most d points.)*

Proof. The *restriction of p to L* is $p_0(t) = p(y + tx)$, a single-variable polynomial in $\mathbb{F}[t]$ of degree at most d which has at most d zeros from Proposition 3.4. □

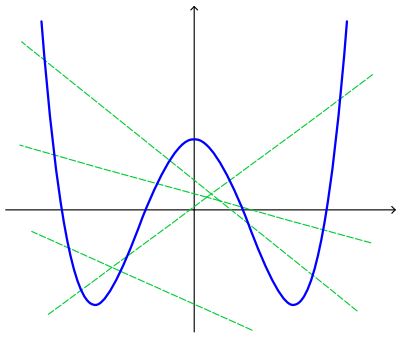


Figure 3.1: The curve $Z(y - (x - 3)(x - 1)(x + 1)(x + 3))$ meets each of the dashed lines in at most four points.

An example in the plane is shown in Figure 3.1, for the curve $y = (x-3)(x-1)(x+1)(x+3)$. In this planar case, Lemma 3.5 is a generalisation of Proposition 3.4 which simply counts intersections with the line $y = 0$.

In infinite fields analogous results to Proposition 3.4 do not hold for multivariate polynomials, since $Z(p)$ is always infinite. However, in finite fields the *Schwartz-Zippel lemma* extends Proposition 3.4.

Lemma 3.6 (Schwartz-Zippel lemma, [49, 59])**.** *Let $\mathbb{F}$ be a finite field and $p \in \mathbb{F}[x_1, \ldots, x_n]$ be a* nonzero *polynomial of degree d. Then $|Z(p)| \leq d|\mathbb{F}|^{n-1}$.*

Proof. We proceed by induction on n. The $n = 1$ case is Proposition 3.4. Otherwise $n > 1$. Considering p as an element of $(\mathbb{F}[x_2, \ldots, x_n])[x_1]$,

$$p(x_1, \ldots, x_n) = \sum_{i=1}^{r} g_i(x_2, \ldots, x_n) x_1^i,$$

where r is such that g_r is a nonzero polynomial of degree at most $d - r$. Then by induction, $|Z(g_r)| \leq (d-r)|\mathbb{F}|^{n-2}$. For any zero $(a_1, \ldots, a_n) \in Z(p)$, we must have that a_1 is a zero of the single variable polynomial $p_0(x_1) = p(x_1, a_2, \ldots, a_n)$. Hence we can count the zeros in two cases

Case 1: If $(a_2, \ldots, a_n) \in Z(g_r)$ then p_0 could be zero, so $|Z(p_0)| \leq |\mathbb{F}|$.

Case 2: If $(a_2, \ldots, a_n) \notin Z(g_r)$ then p_0 is nonzero of degree r, so $|Z(p_0)| \leq r$.

Combining,

$$\begin{aligned} |Z(p)| &\leq |\mathbb{F}||Z(g_r)| + r|\mathbb{F}^{n-1} \setminus Z(g_r)| \\ &\leq (d-r)|\mathbb{F}|^{n-1} + r|\mathbb{F}|^{n-1} \\ &\leq d|\mathbb{F}|^{n-1}. \end{aligned}$$

□

Clearly we cannot bound the number of points in the same way for an infinite field, but we do have the simple result that if $p \neq 0$ there is some point not in $Z(p)$.

Lemma 3.7. *Let $\mathbb{F}$ be an infinite field and $p \in \mathbb{F}[x_1, \ldots, x_n]$ be a* nonzero *polynomial of degree d. Then $|\mathbb{F}^n \setminus Z(p)| \geq 1$.*

Proof. We proceed by induction on n, noting that the case $n = 1$ follows immediately from Proposition 3.4. Suppose $p \in \mathbb{F}[x_1, \ldots, x_n]$. Cconsidering p as an element of $(\mathbb{F}[x_1, \ldots, x_{n-1}])[x_n]$, it has only finitely many roots, so there is some $a \in \mathbb{F}$ such that $0 \neq p(x_1, \ldots, x_{n-1}, a) \in \mathbb{F}[x_1, \ldots, x_{n-1}]$. Applying the induction hypothesis, this polynomial does not vanish everywhere so we are done. □

It turns out this is enough to prove another useful result which bounds the 'complexity' of zero sets in a certain sense.

Lemma 3.8. *Let $\mathbb{F}$ be a field and $p \in \mathbb{F}[x, y]$ be a nonzero polynomial of degree d.*

(a) If $\mathbb{F}$ is finite and $d < |\mathbb{F}|$ then $Z(p)$ contains at most d distinct lines.

(b) If $\mathbb{F}$ is infinite then $Z(p)$ contains at most d distinct lines.

Proof. Suppose for contradiction that $Z(p)$ contains $d + 1$ distinct lines. Now either

(a) $\mathbb{F}$ is finite, so apply Lemma 3.6 to conclude that p does not vanish identically and hence find $a \notin Z(p)$. Since there are $d+1 \leq |\mathbb{F}|$ lines in $Z(p)$, there is a line l through a not parallel to any of these lines (since lines in $\mathbb{F}^2$ can have $|\mathbb{F}|+1$ different directions.)

(b) $\mathbb{F}$ is infinite, so apply Lemma 3.7 to conclude that p does not vanish identically and hence find $a \notin Z(p)$. Choose a line l through a that is not parallel to any of the $d+1$ lines contained in $Z(p)$.

The line l intersects all $d+1$ of the lines in $Z(p)$ and hence is contained in $Z(p)$ by Lemma 3.5. This is a contradiction, since p does not vanish at a. □

Readers familiar with algebraic geometry may like to note that over an algebraically closed field Lemma 3.8 is a consequence of the Nullstellensatz (since if $Z(ax+by) \subset Z(p)$ then $ax+by$ divides p), and indeed over $\mathbb{R}$ the result follows from similarly general statements from real algebraic geometry (see [5, Section 4]).

3.3 Proof of the Finite Field Kakeya Conjecture

Before we give Dvir's full proof of the finite field Kakeya conjecture, we first give an intuitive proof for the planar case. To the author's knowledge this simple method of proof is original, although the planar case is of little independent interest since the planar result was known even in Wolff's original paper [58].

Proposition 3.9. *Let $\mathbb{F}$ be a finite field, and $K \subset \mathbb{F}^2$ a Kakeya set. Then $|K| \gtrsim |\mathbb{F}|^2$.*

Proof. Suppose K is a Kakeya set with $|K| \lesssim |\mathbb{F}|^2$. By Lemma 3.3 there is a nonzero polynomial p vanishing on K of degree $d \lesssim |\mathbb{F}|$. By choosing a small enough hidden constant in the statement of the theorem, we in fact have $d < |\mathbb{F}|$. Since K is a Kakeya set, it contains at least $|\mathbb{F}|+1$ distinct lines, one in each of the $|\mathbb{F}|+1$ directions (they are distinct since they are in different directions.) This is a contradiction, since $Z(p)$ should contain at most $d \leq |\mathbb{F}|-1$ distinct lines, by Lemma 3.8. □

We obtain an intuitive contradiction by 'complexity': a Kakeya set must contain a line in every direction, so cannot be placed inside a zero set of a 'low degree' polynomial, and hence the Kakeya set must be 'big'.

We are now ready to give Dvir's proof in full detail. Dvir's original proof uses a closely related concept to Kakeya sets, which we briefly define.

Definition 3.10. Let $\mathbb{F}$ be a finite field. A set $N \subset \mathbb{F}^n$ is a **Nikodym set** if through every $y \notin N$ there is a line through y which lies otherwise entirely in N, that is $\{y+tx \mid t \in \mathbb{F}^*\} \subset N$ for some $x \in \mathbb{F}^n$.

The first simpler version of Dvir's argument does not prove the full Kakeya conjecture, but was still groundbreaking.

Theorem 3.11 ([13, Theorem 1])**.** *Let $\mathbb{F}$ be a finite field, and $K \subset \mathbb{F}^n$ a Kakeya set. Then $|K| \gtrsim |\mathbb{F}|^{n-1}$ where the hidden constant depends on n.*

Proof. Suppose for contradiction that K is a Kakeya set with $|K| \lesssim |\mathbb{F}|^{n-1}$. Then the set $N = \mathbb{F}K$ is a Nikodym set, since given $y \notin N$ we can choose a line $\{x + ty \mid t \in \mathbb{F}\}$ in the direction y contained in K, and then $\{sx + sty \mid s \in \mathbb{F}, t \in \mathbb{F}\}$ is contained in N. In particular, $\{sx + y \mid s \in \mathbb{F}^*\}$ is contained in N. We have $|N| \lesssim |\mathbb{F}|^n$ so by Lemma 3.3 there is a nonzero polynomial p vanishing on N of degree $d \lesssim |\mathbb{F}|$. With a small enough hidden constant, $d \leq |\mathbb{F}| - 2$. Then for any point $y \notin N$, p vanishes on the $|\mathbb{F}| - 1 > d$ points $\{sx + y \mid s \in \mathbb{F}^*\}$. Hence p vanishes at the remaining point y on this line, by Lemma 3.5. That is, p vanishes everywhere and so must be the zero polynomial (by the Schwartz-Zippel Lemma) contradicting our choice of p. □

The proof of Theorem 3.11 arrives at a contradiction by exploiting the high 'complexity' of the Nikodym set—having a line through *every* external point that is otherwise contained in the set. Following the preprint of Dvir's work, Alon and Tao found an alternative approach that exploited the complexity of the Kakeya set itself, to give a tighter bound.

Theorem 3.12 ([13, Theorem 3])**.** *Let $\mathbb{F}$ be a finite field, and $K \subset \mathbb{F}^n$ a Kakeya set. Then $|K| \gtrsim |\mathbb{F}|^n$ where the hidden constant depends on n.*

Proof. The proof uses ideas from projective space, which we review in Section 8.1. Suppose for contradiction that K is a Kakeya set with $|K| \lesssim |\mathbb{F}|^n$. As in the previous proof, by Lemma 3.3 we can find a nonzero polynomial p vanishing on K of degree $d < |\mathbb{F}|$. Now *embed* K into projective space $\mathbb{PF}^n$ and consider the homogenisation of p given by $p^h(x_0, \ldots, x_n) = x_0^d p(x_1/x_0, \ldots, x_n/x_0)$. Since K is a Kakeya set, through every point $a = [0, a_1, \ldots, a_n]$ on the hyperplane at infinity there is a line $L \subset K$ in the direction a. This line contains $|\mathbb{F}|$ points of K so by Lemma 3.5, p^h vanishes at a. That is, p^h vanishes at every point on the hyperplane at infinity. However, p^h restricted to the line at infinity is just $p^h(0, x_1, \ldots, x_n)$ which is the highest degree homogeneous part of p. This is a contradiction since we assumed p was nonzero of degree $d < |\mathbb{F}|$, so it cannot vanish identically by the Schwartz-Zippel Lemma (Lemma 3.6). □

The proof of Theorem 3.12 exploits the complexity of the Kakeya set K to conclude that any polynomial vanishing on K must vanish on the hyperplane at infinity, which is a copy of $\mathbb{PF}^{n-1}$. Since we can not find a 'low' degree polynomial vanishing on this space, we can not find a 'low' degree polynomial vanishing on K, so K is big.

3.4 Extensions to the Method

Following the work of Dvir, refinements to the polynomial method have been used to improve Theorem 3.12. Saraf and Sudan [48] used the concept of the multiplicity of a zero to get a tighter bound on the size of Kakeya sets. Recall that in the single-variable case, the polynomial $p(x) = (x - a)^k$ has a zero of order k at a. In general, a

polynomial $p(x_1, \ldots, x_n)$ has a zero of multiplicity k at $(a_1, \ldots, a_n)$ if every monomial in $p(x_1 + a_1, \ldots, x_n + a_n)$ has degree at least k. By finding analogues of Lemma 3.3 and Lemma 3.5 for general multiplicities, Saraf and Sudan improved Theorem 3.12. This idea has come to be known as the *method of multiplicities.*

With some additional improvements, Dvir et al. [14] obtained the current best bound, tight to within a small constant factor.

Theorem 3.13 ([14, Theorem 11])**.** *Let $\mathbb{F}$ be a finite field, and $K \subset \mathbb{F}^n$ a Kakeya set. Then $|K| \geq \frac{1}{(2-1/|\mathbb{F}|)^n}|\mathbb{F}|^n$.*

The ideas were also extended by Ellenberg, Oberlin and Tao [18] to solve a related problem. If $\mathbb{F}$ is a finite field and $S \subset \mathbb{F}^n$ then S is a *k-plane* if S is a translation of a k-dimensional subspace of $\mathbb{F}^n$. A subset $K \subset \mathbb{F}^n$ is a *k-plane Kakeya* set if for every k-dimensional subspace V of $\mathbb{F}^n$, there is a k-plane contained in K which is a translation of V. We note that by an induction argument, Lemma 3.8 can be generalised to bound the number of $(n-1)$-planes contained in $Z(p) \subset \mathbb{F}^n$ when $p \in \mathbb{F}[x_1, \ldots, x_n]$. Using this, the same proof as Lemma 3.3 bounds the size of $(n-1)$-plane Kakeya sets. Ellenberg, Oberlin and Tao obtained a strong bound in the general k case.

Theorem 3.14 ([18, Proposition 4.16])**.** *Let $\mathbb{F}$ be a finite field and $K \subset \mathbb{F}^n$ a k-plane Kakeya set where $2 \leq k < n$. Then $|K| \geq (1 - |\mathbb{F}|^{1-k})^{\binom{n}{2}}|\mathbb{F}|^n$.*

So far we have seen the successful application of the polynomial method to problems over finite fields. As we will see, the method has much wider applicability, although it remains to be seen whether the method of multiplicities can be applied in other contexts. In the next section we will see how the polynomial method can be applied to problems over $\mathbb{R}^n$.

Chapter 4

The Joints Conjecture

After Dvir's work, Guth and Katz [26] successfully applied the polynomial method to the joints problem, an incidence problem in real space. The joints problem is a simpler version of the incidence problem in Theorem 2.15 for the case $k = 3$, and the proof of the joints conjecture introduced many elements that were eventually used in the full proof of Theorem 2.15. In this chapter we give the proof of the joints conjecture.

Definition 4.1. Let L be a set of lines in $\mathbb{R}^3$. A point p of $\mathbb{R}^3$ is called a **joint** of L if there are three lines in L which meet at p and do not all lie in a plane.

The work of Guth and Katz [26] resolved the joints conjecture of Chazelle et al. [6], obtaining the following tight bound.

Theorem 4.2. *Let L be a set of lines in $\mathbb{R}^3$ and let J be the set of joints of L. Then $|J| \lesssim |L|^{3/2}$.*

Prior to the application of the polynomial method to the problem by Guth and Katz, the best known bound was $|J| \lesssim |L|^{1.6232}$, obtained by Feldman and Sharir [21]. Guth and Katz' motivation for studying the joints problem was the connection with the real Kakeya problem. We will study this proof as a stepping stone to the resolution of the Erdős distinct distances problem, but the reader interested in the connections to the Kakeya problem should consult [43]. Several different simplifications to Guth and Katz original proof have appeared [42, 16, 31]. We follow the proof of [16], and in particular we give their generalisation of the proof to 'flat' points, a case which is crucial for the resolution of the Erdős distinct distances conjecture.

4.1 Algebraic Tools

Most of our algebraic results are corollaries of Bezout's famous theorem on the number of incidences between algebraic curves in the plane.

Theorem 4.3 (Bezout's Theorem)**.** *If $p, q \in \mathbb{R}[x, y]$ have degrees d_p and d_q respectively and have no common factors, then $|Z(p) \cap Z(q)| \leq d_p d_q$.*

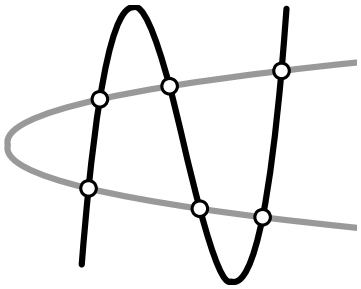


Figure 4.1: $Z(y^2 - x)$ and $Z(y - 100(x-1)(x-2)(x-3))$ meet in six points.

For example, if q is of degree 1 then $Z(q)$ is a line, and for any polynomial $p \in \mathbb{R}[x, y]$ this line intersects $Z(p)$ in at most d_p points. This is the planar case of our very first lemma on the complexity of zero sets, Lemma 3.5. Figure 4.1 illustrates an example where $p = y^2 - x$ and $q = y - 100(x-1)(x-2)(x-3)$ are of degree 2 and 3 respectively, and we see that the two curves $Z(p)$ and $Z(q)$ intersect in 6 points. As another application, we can quickly obtain the result of Proposition 2.1 (two circles intersect in at most two points) by applying a planar inversion[1] at a point on one of the circles, giving a line and a circle which by Bezout's theorem intersect in at most two points.

For application to the joints problem, we will use the following proposition which leverages Bezout's theorem up to dimension 3.

Proposition 4.4. *If $p, q \in \mathbb{R}[x, y, z]$ have degrees d_p and d_q and have no common factors then there are at most $d_p d_q$* lines *contained in $Z(p) \cap Z(q)$.*

For instance, if p and q are products of linear factors then $Z(p)$ and $Z(q)$ are unions of planes. In the general case where none of these planes are parallel and no 3 intersect along a line, we get $d_p d_q$ lines contained in $Z(p) \cap Z(q)$ from each choice of a plane in $Z(p)$ and a plane in $Z(q)$, so this proposition is tight. Both Bezout's theorem and Proposition 4.6 can be proven using the theory of resultants; we will not give these proofs but they can be found in [26, Corollary 2.3] and [16, Proposition 1].

The proof of the joints conjecture via the polynomial method involves finding a vanishing polynomial p on the set of lines L, and observing that the joints are 'special' points of $Z(p)$. To that end we introduce the following definitions.

Definition 4.5.

1. A point $a \in Z(p)$ is **critical** for p if $\nabla p(a) = 0$.

2. A point $a \in Z(p)$ is **regular** for p if $\nabla p(a) \neq 0$ (i.e. if it is not critical.)

[1] Viewing elements of $\mathbb{R}^2$ as elements of $\mathbb{C} \cup \{\infty\}$, inverting the plane at the point a means to apply the map $\frac{1}{z-a}$, sending the point ∞ to a and sending a to ∞. One can check that circles through a map to lines and other circles remain circles after applying inversion, and that inversion preserves the incidence structure.

3. A line $l \subset Z(p)$ is a **critical line** for p if every point in l is critical for p.

Intuitively, we can think of critical points as points where two irreducible components of $Z(p)$ meet. For instance, if $p = xy \in \mathbb{R}[x, y, z]$ then $Z(p)$ is the union of the planes $x = 0$ and $y = 0$, and $\nabla p = (y, x, 0) = 0$ exactly on the line $x = y = 0$ where the two planes meet. In general, ∇p is normal to the surface $Z(p)$, and where two distinct irreducible components of $Z(p)$ meet there is no nonzero normal vector, so $\nabla p = 0$.

Notice that the we define critical lines as lines contained in the zero set of the two polynomials p and the three polynomials ∇p. Looking at Proposition 4.4, the following result should not be surprising.

Proposition 4.6. *Let $p \in \mathbb{R}[x, y, z]$ be square-free of degree d. Then $Z(p)$ contains at most $d(d-1)$ critical lines for p.*

Proof. If p is irreducible then p and $\frac{\partial p}{\partial x}$ have no common factors, and the partial derivative has degree $d - 1$, so from Proposition 4.4, $Z(p)$ contains at most $d(d-1)$ critical lines for p. The case where p is reducible involves induction on the degree; details are given in [16, Proposition 3]. □

To see why square-free polynomials must be excluded, consider the example $p = x^2 \in \mathbb{R}[x, y, z]$, where $\nabla p = (2x, 0, 0)$. In this example, *any* line contained in the plane $x = 0$ is a critical line.

In addition to critical points where two components of the surface meet, we will have to deal with a second special type of point.

Definition 4.7.

1. A regular point $a \in Z(p)$ is **linearly flat** for p if there are three distinct lines $l_1, l_2, l_3 \subset Z(p)$, each containing a.

2. A regular point $a \in Z(p)$ is **flat** for p if the second fundamental form of $Z(p)$ vanishes at a.

3. A line $l \subset Z(p)$ is a **flat line** for p if all but finitely many points in l are flat points for p.

Readers not familiar with the second fundamental form can find details in [12], although Proposition 4.13 gives an equivalent definition of flat points without reference to the second fundamental form. If we let $p = xy \in \mathbb{R}[x, y, z]$ as before then any $a \in Z(p) \setminus (Z(x) \cap Z(y))$ is linearly flat, since there are three lines containing a in whichever of the planes $Z(x)$ or $Z(y)$ contains a. The line $l = \{(0, y, 1) \mid y \in \mathbb{R}\}$ is a flat line for p since $(0, 0, 1)$ is the only critical point in l.

We will need to understand the relationship between flat lines and the irreducible components of $Z(p)$. In particular we have the following result.

Proposition 4.8. *If $p = fg \in \mathbb{R}[x, y, z]$ and $l \subset Z(p)$ is a flat line for p, then l is a flat line for either f or g.*

Since the second fundamental form is defined locally, Proposition 4.8 is not surprising—whether a point is flat is determined only by the component $Z(f)$ or $Z(g)$ in which the point sits. At the intersection of $Z(f)$ and $Z(g)$ the points are critical, so are of no concern in determining whether a line is flat.

If the second fundamental form vanishes at a regular point $a \in Z(p)$ then locally at a, $Z(p)$ is part of a plane, so $Z(p)$ is indeed 'flat'. The following proposition justifies calling linearly flat points 'flat'.

Proposition 4.9. *Let $a \in Z(p)$ and suppose there are three distinct lines $l_1, l_2, l_3 \subset Z(p)$, which each contain a. If a is a regular point then the three lines are coplanar. If the three lines are noncoplanar, then a is a critical point.*

Proof. We only prove the latter statement as it is the contrapositive of the first. We use the argument from Kaplan, Sharir and Shustin [31]. Let u_1 be a unit vector in the direction of l_1, so that $l_1 = \{a + tu_1 \mid t \in \mathbb{R}\}$. Then taking a first order Taylor approximation,

$$p(a + tv) = p(a) + t\nabla p \cdot u_1 + O(t^2).$$

But $p(a + tv) = p(a) = 0$ for all $t \in \mathbb{R}$, so by taking t small enough we conclude $\nabla p \cdot u_1 = 0$. However, repeating for l_2 and l_3 we get

$$\nabla p \cdot u_1 = \nabla p \cdot u_2 = \nabla p \cdot u_3 = 0$$

where u_2, u_3 are unit vectors in the directions of l_2 and l_3 respectively. However, since the lines are noncoplanar, these three directions *span* $\mathbb{R}^3$, so $\nabla p = 0$ and a is critical. □

This justifies the use of the term linearly flat, as a linearly flat point must be the meeting point of three lines lying in a plane in $Z(p)$. Indeed, linearly flat points *are* flat in the sense of Definition 4.7.

Proposition 4.10 ([16])**.** *A linearly flat point is flat.*

We are especially interested in linearly flat points as they are the flat points that are easiest to work with. In Proposition 4.6, we were able to control the number of critical lines in $Z(p)$ by using the fact that ∇p characterises the critical points. It is not so obvious that there are polynomials that characterise flat points in this way. Guth and Katz' original construction ([26]) used nine polynomials, we instead use the construction of Elekes, Kaplan and Sharir [16] of three polynomials characterising linearly flat points.

Definition 4.11. Let $e_1, e_2, e_3 \in \mathbb{R}^3$ denote the standard unit vectors in the x, y, z directions. The **Hessian** of p is

$$H_p = \begin{pmatrix} p_{xx} & p_{xy} & p_{xz} \\ p_{xx} & p_{xy} & p_{xz} \\ p_{xx} & p_{xy} & p_{xz} \end{pmatrix}.$$

Define $\Pi_i(p) \in \mathbb{R}[x, y, z]$ for $i = 1, 2, 3$ by

$$\Pi_i(p) = (\nabla p \times e_i)^T H_p (\nabla p \times e_i)$$

and denote $\Pi(p) = (\Pi_1(p), \Pi_2(p), \Pi_3(p))$.

Since the degrees of the polynomials in ∇p are $d_p - 1$ and the degrees of the second derivatives in the Hessian are $d_p - 2$, the degrees of the polynomials $\Pi(p)$ are $3d_p - 4$. We will not prove the following, but these polynomials characterise flat points in the following sense.

Proposition 4.12. *Let $p \in \mathbb{R}[x, y, z]$, and $a \in Z(p)$. Then a is flat if and only if $\Pi(p)(a) = 0$.*

We note that we can use this to prove Proposition 4.10 by first checking that the second order Taylor approximation to $Z(p)$ vanishes on the three lines through a, and noticing that it also vanishes at a general line in the tangent plane at a since the Taylor approximation has degree 2 and already vanishes at the three points where the line meets l_1, l_2 and l_3. Thus we are in the same situation as for critical lines, where flat lines are lines contained in the intersection of two zero sets, of $Z(p)$ and of $Z(\Pi_i(p))$ for some $i = 1, 2, 3$.

Proposition 4.13 ([16])**.** *Let $p \in \mathbb{R}[x, y, z]$ be square-free of degree d with* no linear factors. *Then $Z(p)$ contains at most $d(3d - 4)$ flat lines for p.*

Again we defer to the proof in [16, Proposition 7]. Intuitively for an irreducible polynomial, if we have too many flat lines then p divides each Π_j, so that *every* regular point is a flat point—but that means that $Z(p)$ is a plane!

To find critical and flat lines in $Z(p)$, we will require the following statements relating them to critical and flat points.

Proposition 4.14.

1. *A line $l \subset Z(p)$ containing more than $d - 1$ critical points of $Z(p)$ is a critical line for p.*

2. *A line $l \subset Z(p)$ containing more than $3d - 4$ linearly flat points of $Z(p)$ is a flat line for p.*

Proof. Both statements follow from Lemma 3.5 since if p_x vanishes at more than $d-1 = \deg(p_x)$ points or $\Pi_1(p)$ vanishes at more than $3d - 4 = \deg(\Pi_1(p))$ flat points (we use that linearly flat points are flat) then p_x (or $\Pi_1(x)$ respectively) vanishes identically on l. Hence by definition l is a critical line or l is a flat line. □

We choose to state the second statement for *linearly flat points* as this is the version we will use, though one could as well state it for flat points. Finally, combining all of these results gives a statement about the complexity of collections of lines contained in $Z(p)$ which meet in a lot of places.

Proposition 4.15. *Let $p \in \mathbb{R}[x, y, z]$ be a* square-free *polynomial of degree d and let L be a collection of lines contained in $Z(p)$. Let J be the set of points where are least three lines of L meet, and suppose that*

(i) no plane contains more than B lines of L;

(ii) every line $l \in L$ contains more than $4d$ points of J.

Then $|L| \leq 4d^2 + Bd$.

Proof. Let $l \in L$. Any point where two other lines of L meet l is either a critical point or a linearly flat point, by Proposition 4.9. Since l contains more than $4d$ such points, it either contains more than d critical points or more than $3d$ linearly flat points, so is either a critical or flat line by Proposition 4.14. So every line in l is critical or flat for p.

Write $p = \pi_1 \cdots \pi_k \tilde{p}$ for some $k \leq d$ where each π_i is a linear factor and $\tilde{p}$ has no linear factors. Every line $l \in L$ is either critical or flat for p, and a flat line for p is a flat line for one of the factors $\pi_1, \cdots, \pi_k, \tilde{p}$ by Proposition 4.8. Now we can bound the number of lines in L by observing:

- $Z(p)$ contains at most d^2 critical lines by Proposition 4.6;
- $Z(\pi_i)$ contains at most B lines by assumption, so in particular contains at most B flat lines, for each $i = 1, \ldots, k$;
- $Z(\tilde{p})$ contains at most $3d^2$ flat lines by Proposition 4.13.

Since every line in L is of one of these types,

$$|L| \leq d^2 + Bk + 3d^2 \leq 4d^2 + Bd. \qquad \square$$

Proposition 4.14 controls the number of lines in terms of the degree of the surface, the number of lines in any given plane and crucially the line-line incidences amongst the collection of lines. We now have the tools to understand the collection of lines contained in the zero set of a polynomial. To apply these tools, it will be convenient to isolate some particular ways to apply Lemma 3.3 to place a given set of lines inside the zero set of a polynomial. The simplest method is the following.

Lemma 4.16. *Let $L \subset \mathbb{R}^n$ be a finite set of lines. Then there is a nonzero polynomial p of degree $d \lesssim |L|^{1/(n-1)}$ such that every line $l \in L$ is contained in $Z(p)$.*

Proof. For each line $l \in L$ choose $C|L|^{1/(n-1)}$ points in $\mathbb{R}^n$ which lie on l, where C is a constant to be fixed later. This gives a total of $C|L|^{n/(n-1)}$ points, so by Lemma 3.3 there is a nonzero polynomial p vanishing at these points of degree $d \lesssim C^{1/n}|L|^{1/(n-1)}$. By choosing C large enough we have $d < C|L|^{1/(n-1)}$, so by Lemma 3.5 every line $l \in L$ is contained in $Z(p)$, as desired. $\square$

For some applications, however, we will be concerned with a family L of lines which intersect often. It turns out that in this situation, a more powerful result is available. The following proof is implicit in [26, 16].

Lemma 4.17. *Let $C \gtrsim 1$ be a constant and let $L \subset \mathbb{R}^n$ be a finite set of lines with $|L| \gtrsim 1$ and satisfying:*

(i) every line $l \in L$ contains at least $C|L|^{1/(n-1)}$ points lying on other lines in L.

Then there is a nonzero polynomial p of degree $d \lesssim \frac{1}{C^{1/(n-1)}}|L|^{1/(n-1)}$ such that every line $l \in L$ is contained in $Z(p)$.

Proof. Take a random subset $L' \subset L$ by choosing each line independently with probability $\frac{1}{C}$.

Claim. With positive probability,

(1) $1 \leq \frac{1}{2C}|L| \leq |L'| \leq \frac{2}{C}|L|$ and

(2) every line $l \in L$ contains at least $\frac{1}{2}|L|^{1/(n-1)}$ points lying on *lines in* L'.

To see this, first recall Chernoff's bounds (see [2]) which we use in the form

$$P\left[\sum_{i=1}^{m} Y_i \geq mp + m\epsilon\right] \leq \exp(-2\epsilon^2 m), \quad P\left[\sum_{i=1}^{m} Y_i \leq mp - m\epsilon\right] \leq \exp(-2\epsilon^2 m)$$

whenever Y_i are independent Bernoulli random variables with $P[Y_i = 1] = p$. To apply Chernoff's bounds we set $L = \{l_1, \ldots, l_{|L|}\}$ and rephrase the claims (1) and (2) in terms of the indicator variables $\mathbb{1}_{l_i \in L'}$, giving:

- $P[A] = P[\sum_{i=1}^{|L|} \mathbb{1}_{l_i \in L'} \geq \frac{2}{C}|L|] \leq \exp(-2|L|/C^2)$;
- $P[B] = P[\sum_{i=1}^{|L|} \mathbb{1}_{l_i \in L'} \leq \frac{1}{2C}|L|] \leq \exp(-\frac{1}{2}|L|/C^2)$;
- For each $l \in L$, let $L_l = \{l_{n_1}, \ldots, l_{n_k}\} \subset L$ be a set of distinct lines each incident to a distinct point on L, with $k \geq C|L|^{1/(n-1)}$ by the assumption (i). Then $P[C_l] = P[\sum_{i=1}^{k} \mathbb{1}_{l_{n_i} \in L'} \leq \frac{1}{2}|L|^{1/(n-1)}] \leq \exp(-\frac{1}{2}|L|^{1/(n-1)}/C)$.

Putting them together, by the union bound

$$P[A \cup B \cup \bigcup_{l \in L} C_l] \leq \exp(-2|L|/C^2) + \exp(-\frac{1}{2}|L|/C^2) + \sum_{l \in L} \exp(-\frac{1}{2}|L|^{1/(n-1)}/C)$$

and since we have $|L| \gtrsim 1$ and $C \gtrsim 1$ by choosing these constants appropriately, we will have $P[A \cup B \cup \bigcup_{l \in L} C_l] < 1$, so with positive probability (1) and (2) hold.

Now by Lemma 4.16 we can find a polynomial p vanishing on L' of degree $d \lesssim \frac{1}{C^{1/(n-1)}}|L|^{1/(n-1)}$. Since each line of L contains at least $\frac{1}{2}|L|^{1/(n-1)}$ points lying on lines in L', and this can be made larger than d by ensuring C is large enough, we have by Lemma 3.5 that each line of L is in $Z(p)$. □

4.2 The Joints Conjecture

We can now give the slick proof of the joints conjecture. We give the proof by Kaplan et al. [31], which somewhat simplifies the original proof by Guth and Katz [26].

Theorem 4.2. *Let L be a set of lines in $\mathbb{R}^3$ and let J be the set of joints of L. Then $|J| \lesssim |L|^{3/2}$.*

Proof. We proceed by induction on $|L|$. For clarity, let the hidden constant in the statement be A so we wish to prove that $|J| \leq A|L|^{3/2}$. For $|L|$ less than some fixed large constant we obtain the result by taking a large enough implicit constant in the statement, since trivially $|J| \leq |L|^2$. For the induction step assume for the sake of contradiction that we have a set L of n lines and a set J as specified, and such that $|J| > A|L|^{3/2}$.

We first prune L by iteratively removing any line from L that contains fewer than $C|L|^{1/2}$ points and removing the corresponding points from J (here C is a constant which we will fix later, and this threshold $C|L|^{1/2}$ stays fixed as we remove lines from L). This gives us a subset $L' \subset L$ and its set of joints J' which satisfy:

(i) every line of L' is incident to at least $C|L|^{1/2}$ joints of L';

(ii) $|J'| \geq |J| - C|L|^{3/2}$ (since we removed at most $C|L|^{3/2}$ points in this process).

Case 1. If $|L'| < |L|/2$ then applying induction to L' we get

$$|J'| \leq A|L'|^{3/2} < A/2|L|^{3/2}.$$

Hence

$$A|L|^{3/2} < |J| \leq |J'| + C|L|^{3/2} < (A/2 + C)|L|^{3/2},$$

a contradiction since we can take A with $A/2 \geq C$.

Case 2. Otherwise, $|L'| \geq |L|/2$. By Lemma 4.17 we can find a square-free polynomial p which vanishes on every line in L' and by appropriate choice of C, has degree $d \leq \frac{1}{2}|L|^{1/2}$. By Proposition 4.9 (and that the three lines at any joint are noncoplanar) each joint is a critical point for p. Hence since each line contains at least $C|L|^{3/2}$ joints each line in L is critical by Proposition 4.14. However, by Proposition 4.6 the number of critical lines is at most $d^2 \leq |L|/4$, a contradiction.

In either case, we reach a contradiction. □

Amazingly, the results about critical lines do most of the work for us. The remaining work of the proof is just checking the easier case when there are lines not containing many joints!

Elekes, Kaplan and Sharir [16] observed that the proof of the Joints conjecture could be altered to bound the number of incidences with points that are 'flat' joints, where the three incident lines are coplanar. This was a crucial step towards the resolution

of the Erdős distinct distances conjecture as the incidence problem is of this form. To control the number of these flat points, an assumption about the number of points or lines lying in any given plane is required (recall that in the distinct distances incidence problem, we can bound the number of lines in any given plane or regulus.)

Theorem 4.18 ([16, Theorem 9])**.** *Let L be a set of at most n lines in $\mathbb{R}^3$ and let P be a set of m arbitrary points in $\mathbb{R}^3$ such that:*

(i) no plane contains more than Bn points of P, where B is an absolute constant;

(ii) each point of P is incident to at least three lines of L.

Then $m \leq An^{3/2}$ for some absolute constant A.

Proof. Set $\epsilon = 10^{-8}$ and $c = 10^{20}$. We can take A such that

$$A \geq \max\{100c, \sqrt{N_{\epsilon,c}}\} = \max\{10^{22}, \sqrt{N_{\epsilon,c}}\}.$$

We proceed by induction on n. If $n \leq N_{\epsilon,c}$ then $m \leq n^2 \leq \sqrt{N_{\epsilon,c}} n^{3/2} \leq An^{3/2}$. We suppose for contradiction that $|L'| = n$ and $|P'| = m$ satisfy the assumptions, but $m > An^{3/2}$.

While there is a line in L' incident to fewer than $cn^{1/2}$ points of P', remove that line and the incident points from L' and P', and call the resulting sets L and P. This removes at most $cn^{3/2}$ points of P', so $|P| \geq |P'| - cn^{3/2}$. These sets satisfy that

(i) no plane contains more than $|L|^{1/2} \leq n^{1/2}$ points of P

(ii) each point of P is incident to at least three lines of L

(iii) each line of L is incident to at least $cn^{1/2}$ points of P

Suppose $|L| < \frac{n}{100}$. Set $L_0 = L$ and $P_0 = P$. Iteratively, if there is a plane π containing more than $\sqrt{|L_i|}$ lines then remove the lines and points from that plane to form L_{i+1} and P_{i+1}. This process takes at most $2n^{1/2}$ steps. A point is in $P \setminus P_k$ comes either from the intersection of two lines in $L \setminus L_k$ or from a line in L_k with a line in $L \setminus L_k$. There can be at most $2n^{3/2}$ of the first kind since $L \setminus L_k$ consists of at most $2n^{1/2}$ planes each containing at most $n^{1/2}$ lines, so each plane has at most n internal intersections and each pair of planes has at most $2n$ points of incidence on their line of intersection. We also have at most $n^{3/2}$ of the second kind since a line of L_k does not lie in any plane and so intersects each of the $n^{1/2}$ planes at most once. Lastly by the induction hypothesis, $|P_k| \leq A|L_k|^{3/2} \leq \frac{A}{100} n^{3/2}$. Hence

$$(A - c)n^{3/2} \leq |P'| - cn^{3/2} \leq |P| \leq 2n^{3/2} + n^{3/2} + \frac{A}{100} n^{3/2}$$

which is a contradiction since $A > \frac{100}{99}(3 + c)$.

Otherwise $|L| \geq \frac{n}{100}$. Since $1 > \epsilon > 0$ and $c > 3000\epsilon^{-2}$, by a careful examination of the constants we can apply Lemma 4.17 to P and L to get a polynomial p of degree $d \leq \epsilon n^{1/2}$ which vanishes on the lines of L. Applying Proposition 4.15, since no plane contains more than $n^{1/2}$ lines of L, we have

$$|L| \leq 4d^2 + n^{1/2}d \leq (4\epsilon^2 + \epsilon)n$$

which is a contradiction since $4\epsilon^2 + \epsilon < \frac{1}{100}$. □

In this chapter, we have seen how the polynomial method can be used to prove an incidence problem with many of the features of Guth and Katz' Theorem 2.15. The proof of Theorem 2.15 combines the tools we have seen so far with another new idea: polynomial partitioning. In Chapter 5 we introduce the method of polynomial partitioning, the last tool needed to give the bound on the Erdős distinct distances problem.

Chapter 5

Polynomial Partitioning

We have already seen how the polynomial method can be used to solve incidence problems by placing a combinatorial structure inside a low degree algebraic surface and arguing that this surface is 'simple' in an appropriate sense. One of the breakthroughs of Guth and Katz was to realise that polynomials could be used to replace a classical tool in combinatorial geometry – space decompositions. In this section we will see both the classical tool of *cell decompositions* and Guth and Katz' *polynomial partitions*, and their relationship.

5.1 The Szemerédi-Trotter Theorem

We will use the famous Szemerédi-Trotter theorem to introduce the method of polynomial partitioning. The theorem improves upon the weak purely combinatorial bounds we have seen in Lemma 2.7 to give an optimal bound for incidences between points and lines in $\mathbb{R}^2$.

Theorem 5.1 (Szemerédi-Trotter, [55])**.** *Let $P \subset \mathbb{R}^2$ be a finite planar point set and L be a finite set of lines. Recall the definition of the number of point-lines incidences, $I(P,L) = |\{(p,l) \mid p \in P, l \in L, p \in l\}|$. Then*

$$I(P,L) \lesssim |P|^{2/3}|L|^{2/3} + |P| + |L|. \tag{5.1}$$

To see that the bound is optimal, consider the grid $P = \{1,2,\dots,n\} \times \{1,2,\dots,2n^2\}$ with the collection of lines L of the form $l_{m,c} = \{(t, mt+c) \mid t \in \mathbb{R}\}$ for $m \in \{1,\dots,n\}$ and $c \in \{1,\dots,n^2\}$. We have $|P| = 2n^3$, $|L| = n^3$ and $l_{m,c} \cap P = \{(t, mt+c) \mid t \in \{1,\dots,n\}\}$ has size n, so that $I(P,L) = n^4 \sim |P|^{2/3}|L|^{2/3}$. As we have seen when studying Lemma 2.7, the other terms in (5.1) can also be dominant for certain examples.

Theorem 5.1 was originally proved by Szemerédi and Trotter [55] by an argument using a decomposition of space into *squares*. Later we will see a simpler proof in this style, but first we will look at the beautiful modern proof given by Székely [54]. The main ingredient of this proof is the crossing number inequality.

Theorem 5.2 (Crossing Number Inequality, [1, 35])**.** *Suppose $G = (V, E)$ is a graph with a drawing in the plane. Denote by $cr(G)$ the number of* crossings *in the drawing (the number of points where a pair of edges intersect, excluding intersections at vertices). If $|E| \geq 4|V|$ then*

$$cr(G) \gtrsim \frac{|E|^3}{|V|^2}. \tag{5.2}$$

Proof. Recall that a planar graph has less than $3|V|$ edges (a corollary of Euler's formula for planar graphs). If at each crossing of G we remove one edge, we are left with a planar subgraph having at most $3|V|$ edges, so the total number of edges is

$$|E| < 3|V| + cr(G). \tag{5.3}$$

Randomly choose an induced subgraph of G by selecting each vertex independently with probability p. Then taking expectations in (5.3) we get $p^2|E| < 3p|V| + p^4 cr(G)$. Rearranging, $cr(G) > (p|E| - 3|V|)/p^3$. Taking $p = 4|V|/|E|$ (note that $p \leq 1$) we obtain $cr(G) \geq \frac{|E|^3}{64|V|^2}$ as desired. □

For instance, every drawing of K_n for n large enough has $\gtrsim n^4$ crossings. By the argument of Székely, Theorem 5.2 quickly gives the Szemerédi-Trotter theorem.

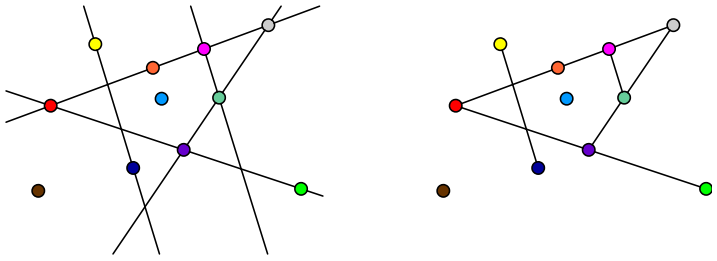


Figure 5.1: The sets P, L of points and lines determine a natural (drawing of a) graph

First proof of Szemerédi-Trotter. Define a graph $G = (P, E)$ by joining two points by an edge exactly when they are consecutive points on some line of L. Additionally, there is a natural drawing of this graph with $P \subset \mathbb{R}^2$ and edges drawn as segments of the lines of L (an example is given in Figure 5.1.) By the crossing number inequality (5.2), if $|E| \geq 4|P|$ then

$$\frac{|E|^3}{|P|^2} \lesssim cr(G) \leq |L|^2$$

where the upper bound comes from the fundamental fact that a pair of lines cross at most once. Since either $|E| < 4|P|$ or $|E| \geq 4|P|$, $|E| \lesssim (|L|^2|P|^2)^{1/3} + |P|$.

By the construction of G, and since a line with k incidences with P contains $k - 1$ edges in E, $I(P, L) = |E| + |L|$. Hence

$$I(P, L) \lesssim |L|^{2/3}|P|^{2/3} + |P| + |L|. \qquad \square$$

5.2 Decompositions of Space

We will now see how the Szemerédi-Trotter theorem can be proven by a *decomposition* argument. Indeed, the original proof by Szemerédi and Trotter [55] used a decomposition of the plane into squares. We will instead use a decomposition introduced by Clarkson et al. [7], which was given a relatively simple probabilistic proof by Tao [56].

Definition 5.3. A subset $S \subset \mathbb{R}^n$ **decomposes** $\mathbb{R}^n$ into k cells if

$$\mathbb{R}^n \setminus S = C_1 \cup C_2 \cup \cdots \cup C_k$$

where each C_i is an open subset of $\mathbb{R}^n$ and $C_i \cap C_j = \emptyset$ for $i \neq j$. We call S the **boundary** of the decomposition.

Note that the cells C_i are not required to be connected, so a boundary does not determine a unique decomposition into cells. If we do not explicitly specify the cells C_i then the cells shall be taken to be the connected components of $\mathbb{R}^n \setminus S$.

Lemma 5.4 (Cell Decomposition Lemma, [7, 56])**.** *Let $r \geq 1$, let P be a finite planar point set and let L be a finite set of lines. Then there is a set R of lines with $|R| \lesssim r$ and a set S of line segments and rays that are not incident to P, such that $R \cup S$ decomposes the plane into $\lesssim r^2$ cells, and each of these cells is incident to at most $\lesssim |L|/r$ lines of L.*

Remark 5.5. The set S of line segments and rays can be chosen such that any line in $R \cup S$ is contained in R. This is evident from the proof in [56] as one can perturb individual segments and rays in S while maintaining the decomposition.

An insight of Guth and Katz was to realise that polynomials offer an alternative to the partitioning set $R \cup S$ in the cell decomposition lemma. That is, instead of partitioning space with a relatively small set of lines and segments, one can partition space by an *algebraic curve of small degree.*

Lemma 5.6 (Polynomial Partitioning Lemma)**.** *Let $r \geq 1$ and let $P \subset \mathbb{R}^n$ be a finite point set. Then there is a polynomial $p \in \mathbb{R}[x_1, \ldots, x_n]$ of degree $d \lesssim r$ such that $Z(p)$ decomposes the plane into $\lesssim r^3$ cells each containing $\lesssim |P|/r^n$ points.*

This partitioning result is a consequence of the famous ham sandwich theorem of Stone and Tukey [52] which asserts that a single hyperplane can evenly divide a number of sets simultaneously. We only require the following discrete version, but we remark that in general the sets are not required to be finite, merely bounded, and the sets can be halved with respect to any measure.

Theorem 5.7 (Ham Sandwich Theorem, [52])**.** *Let $A_1, \ldots, A_n$ be finite sets in $\mathbb{R}^n$. Then there exists an $(n-1)$-dimensional hyperplane H that* bisects *the sets A_i (that is, each side of H contains at most half of the points in each A_i.)*

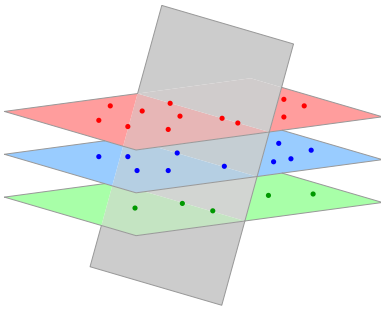


Figure 5.2: Three point sets lying on the three planes $Z(z-2), Z(z-1)$ and $Z(z)$ in $\mathbb{R}^3$ can each be bisected by a single plane.

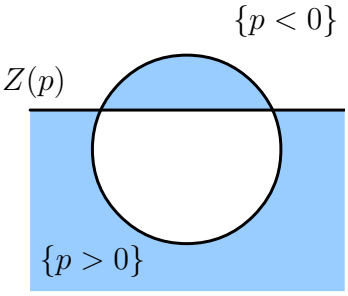


Figure 5.3: The curve $Z(p)$ where $p(x, y) = (x^2 + y^2 - 2)(y - 1)$. The shaded area is the region $\{(x, y) \mid p(x, y) > 0\}$.

For example, in Figure 5.2, if $A \subset Z(z-2), B \subset Z(z-1)$ and $C \subset Z(z)$, then there is always a single plane bisecting each of A, B and C (imagining A, C as the bread and B as the ham in a ham sandwich gives the motivation for the name of the theorem, that we can always cut our 'sandwich' evenly in half.) We cannot give a lower bound on the number of points on each side of the cut—indeed in the plane if A_1 and A_2 lie on opposite ends of a line, the only ham sandwich cut is that very line. In general, the sets A_i can all be *contained* in the cutting hyperplane. For our purposes we instead require a version replacing the hyperplane by the zero-set of a *polynomial*. The following discrete version first appeared in [27], but we give the proof appearing in [30].

Corollary 5.8 (Polynomial Ham Sandwich Theorem)**.** *Let $A_1, \ldots, A_m$ be finite sets in $\mathbb{R}^n$. Then there exists a polynomial p of degree $d \lesssim m^{1/n}$ such that $Z(p)$* bisects *the sets A_i (that is $Z(p)$ splits $\mathbb{R}^n$ into two pieces $C_1 = \{x \in \mathbb{R}^n \mid p(x) > 0\}$ and $C_2 = \{x \in \mathbb{R}^n \mid p(x) < 0\}$, each of which contains at most half of the points in each A_i.)*

Proof. Denote $M_d = \{(a_1, \ldots, a_n) \in \mathbb{Z}_{\geq 0} \mid a_1 + \ldots + a_n \leq r\}$ and note $|M_d| = \binom{n+d}{n}$. For any degree $d \geq 1$ we have the Veronese map $V_d : \mathbb{R}^n \to \mathbb{R}^{|M_d|}$ given by

$$(x_i)_{1 \leq i \leq n} \overset{V_d}{\longmapsto} (x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n})_{(a_1,\ldots,a_n) \in M_d}.$$

By the ham sandwich theorem, for any d with $\binom{n+d}{n} > m$, there exists a hyperplane bisecting the sets $V_d(A_i)$ for $i = 1, \ldots, m$. In particular such a d exists with $d \lesssim m^{1/n}$.

So we have a hyperplane defined by

$$\sum_{(a_1,\ldots,a_n) \in M_d} \alpha_{(a_1,\ldots,a_n)} x_{(a_1,\ldots,a_n)} = 0$$

in $\mathbb{R}^{|M_d|}$ which bisects each $V_d(A_i)$. Now we can simply take the polynomial

$$p = \sum_{(a_1,\ldots,a_n) \in M_d} \alpha_{(a_1,\ldots,a_n)} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

and observe that $Z(p)$ bisects each A_i as desired. $\square$

Note that using the polynomial ham sandwich theorem the boundary $Z(p)$ decomposes space into two not necessarily connected pieces, as seen in Figure 5.3. By iterating the polynomial ham sandwich theorem, Lemma 5.6 is obtained (we follow the proof in [30].)

Proof of the Polynomial Paritioning Lemma, 5.6. First apply Corollary 5.8 to the point set P to get a polynomial p_1 of degree $d_1 \lesssim 2^{1/n}$ which separates P into sets

$$P_0 = P \cap \{x \in \mathbb{R}^n \mid p_1(x) > 0\} \text{ and } P_1 = P \cap \{x \in \mathbb{R}^n \mid p_1(x) < 0\}$$

each containing at most $|P|/2$ points. Now by induction we can define for each $k \geq 1$ the sets $\{P_w \mid w \in \{0,1\}^k\}$ indexed by binary words by applying Corollary 5.8 to the sets $\{P_w \mid w \in \{0,1\}^{k-1}\}$, obtaining a polynomial p_k of degree $d_k \lesssim 2^{k/n}$ which separates each $P_w, w \in \{0,1\}^{k-1}$ into sets

$$P_{w0} = P_w \cap \{x \in \mathbb{R}^n \mid p_k(x) > 0\} \text{ and } P_{w1} = P_w \cap \{x \in \mathbb{R}^n \mid p_k(x) < 0\}$$

each containing at most $|P|/2^k$ points. Fix k with $2^k \geq r^n > 2^{k-1}$. Letting $p = p_1 p_2 \cdots p_k$, we have that $Z(p)$ decomposes the plane into the 2^k cells $\{P_w \mid w \in \{0,1\}^k\}$. By construction, each of these cells contains at most $|P|/2^k \leq |P|/r^n$ points. Finally the degree of p is

$$d = \sum_{i=1}^{k} d_i \lesssim \sum_{i=1}^{k} 2^{i/n} \leq 2^{(k+1)/n} < (4r^n)^{1/n} \lesssim r. \qquad \square$$

5.3 Proof of the Szemerédi-Trotter Theorem via Polynomial Partitioning

In this section we apply the method of cell decomposition via polynomial partitioning to give a proof of the Szemerédi-Trotter theorem. For contrast, we will also give the proof via the classical cell decomposition method, Lemma 5.4. We restate the theorem for convenience.

Theorem 5.1 (Szemerédi-Trotter theorem)**.** *Let P be a finite planar point set and L be a finite set of lines. Then*

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

We highlight the difference between the proof using the cell decomposition lemma and the proof using the polynomial partitioning lemma.

Proof. By planar duality we can assume $|P| \leq |L|$ and by the combinatorial incidence bounds in Lemma 2.7 we can assume $|L|^{1/2} \lesssim |P|$. Now apply either the cell-decomposition or polynomial-partitioning lemma for an r to be chosen later, and let $C_1, \ldots, C_N$ be the resulting cells. Let $Z = R \cup S$ in the cell-decomposition case and $Z = Z(p)$ in the polynomial-partitioning case, so that Z is the region of the plane used to define our cell partitions, and $Z \cup C_1 \cup \cdots \cup C_N = \mathbb{R}^2$.

Let $P_i = C_i \cap P$ be those points in cell C_i, and let $L_i = \{l \in L \mid l \cap C_i \neq \emptyset\}$ be those lines passing through the cell C_i. Also let $P_0 = P \cap Z$ and $L_0 = \{l \in L \mid l \subset Z\}$ be those points and those lines contained in Z, respectively.

Considering how incidences can arise from these sets of points and lines,

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

The quantities in the sum can be bounded as follows:

Cell Decomposition

Every point of P_0 lies on one of the lines R and $|R| \lesssim r$. Lines in $L \setminus L_0$ are not in R, so since distinct lines intersect at most once:

$$I(P_0, L \setminus L_0) \lesssim r|L \setminus L_0| \lesssim r|L|.$$

Note that $I(P_0, L_0) \leq |P_0||L_0|$ and any line in L_0 is in R (by Remark 5.5), so that $|L_0| \lesssim r$, hence

$$I(P_0, L_0) \lesssim r|P| \lesssim r|L|.$$

By the simple incidence bounds in Lemma 2.7,

$$\sum_{i=1}^{N} I(P_i, L_i) \lesssim \sum_{i=1}^{N} (|P_i||L_i|^{1/2} + |L_i|).$$

Each cell is incident to at most $|L|/r$ lines so $|L_i| \lesssim |L|/r$, and hence

$$\sum_{i=1}^{N} |L_i| \lesssim r|L|.$$

Polynomial Partitioning

Lines in $L \setminus L_0$ are not contained in $Z(p)$, so each can vanish on at most $d \lesssim r$ points of P_0 (otherwise p would vanish on the whole line, by Lemma 3.5).

$$I(P_0, L \setminus L_0) \lesssim r|L \setminus L_0| \lesssim r|L|.$$

Note that $I(P_0, L_0) \leq |P_0||L_0|$ and $Z(p)$ contains at most $d \lesssim r$ lines by Lemma 3.8, so $|L_0| \lesssim r$ and

$$I(I(P_0, L_0) \lesssim r|P| \lesssim r|L|.$$

By the simple incidence bounds in Lemma 2.7,

$$\sum_{i=1}^{N} I(P_i, L_i) \lesssim \sum_{i=1}^{N} (|P_i|^2 + |L_i|).$$

Again, a line not contained in $Z(p)$ can intersect it at most r times, so each such line meets at most $r + 1$ cells, and

$$\sum_{i=1}^{N} |L_i| \lesssim r|L|.$$

Again $|L_i| \lesssim |L|/r$and $\sum_{i=1}^N |P_i| \leq |P|$, thus

$$\sum_{i=1}^N |P_i||L_i|^{1/2} \lesssim |P||L|^{1/2}/r^{1/2}.$$

Substituting $r = |P|^{2/3}/|L|^{1/3}$ gives

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

Note that $|P_i| \lesssim |P|/r^2$ and $\sum_{i=1}^N |P_i| \leq |P|$, thus

$$\sum_{i=1}^N |P_i|^2 \lesssim |P|^2/r^2.$$

Substituting $r = |P|^{2/3}/|L|^{1/3}$ gives

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

In either case, we are done. Note that by the proof above, $I(P,L) \lesssim |P|^{2/3}|L|^{2/3}$ except in the case where $|P| \geq |L|$. □

As a quick check, we will see how far the Szemerédi-Trotter theorem can get us with regards to the distinct distances incidence problem, Theorem 2.15. We first state a version of the Szemerédi-Trotter theorem bounding the number of incidence-rich points, in the manner of Corollary 2.8.

Corollary 5.9. *Let L be a finite set of lines in $\mathbb{R}^2$. Then we can bound the number of incidences $|I_{\geq k}(L)|$ of at least k lines in L by*

$$|I_{\geq k}(L)| \lesssim \frac{|L|^2}{k^3} + \frac{|L|}{k} \tag{5.4}$$

Proof. Set $P = I_{\geq k}(L)$. By the Szemerédi-Trotter theorem applied to P and L,

$$|P|k \leq I(P,L) \lesssim |P|^{2/3}|L|^{2/3} + |P| + |L|.$$

Thus $|P|(k-1) \lesssim |P|^{2/3}|L|^{2/3} + |L|$. We are then in one of two cases:

Case 1. if $|P|k \lesssim |P|^{2/3}|L|^{2/3}$ then $|P| \lesssim \frac{|L|^2}{k^3}$;

Case 2. if $|P|k \lesssim |L|$ then $|P| \lesssim \frac{|L|}{k}$.

Finally combining the bounds in either case, $|I_{\geq k}(L)| = |P| \lesssim \frac{|L|^2}{k^3} + \frac{|L|}{k}$. □

Although Corollary 5.9 is stated for lines in $\mathbb{R}^2$, we get the same bound for lines in $\mathbb{R}^3$ by applying a random projection into a plane, which will almost certainly preserve the incidence structure. Hence we can plug bound (5.4) into equation (2.3) from the distinct distances incidence problem to get

$$|Q(P)| \lesssim \sum_{k=2}^{|P|} 2\frac{|L|^2}{k^3}(k-1) \approx |P|^4\frac{\pi^2}{6}$$

recalling that our incidence problem involves $|L| = |P|^2$ pseudolines. This bound on the number of quadruples implies (by (2.1)) the bound $d(P) \gtrsim 1$—an improvement on

the *decreasing* bound afforded by the purely combinatorial incidence results (pg. 11), but still a completely trivial statement. As we shall see, the much stronger incidence results of Theorem 2.15 and Theorem 2.20 are needed to obtain a meaningful result from Elekes' reduction. In Chapter 6, we will see how Guth and Katz prove this result by *combining* the power of the polynomial method and polynomial partitioning.

Chapter 6

The Guth-Katz Proof

So far we have seen how the polynomial method was used for problems over finite fields and adapted by Guth and Katz to solve a related incidence problem in $\mathbb{R}^3$. We now have all the machinery to present Guth and Katz' almost-optimal bound for the Erdos distance problem.

Theorem 1.5 (Guth-Katz, [27]). *Let P be a finite set of points in the plane. Then $d(P) \gtrsim |P|/\log|P|$.*

Recall (from Chapter 2) that using an idea of Elekes, Guth and Katz reduced this problem to the following two incidence problems.

Theorem 2.15 ([27, Proposition 2.11]). *Let L be a finite set of lines in $\mathbb{R}^3$ for which no more than $|L|^{1/2}$ lie in a common plane, and let $3 \leq k \leq |L|^{1/2}$. Then $|I_{\geq k}(L)| \lesssim |L|^{3/2}/k^2$.*

Theorem 2.20 ([27, Proposition 2.10]). *Let L be a finite set of lines in $\mathbb{R}^3$ for which no more than $|L|^{1/2}$ lie in a common plane, and no more than $\lesssim |L|^{1/2}$ lie in a common regulus. Then $|I_{\geq 2}(L)| \lesssim |L|^{3/2}$.*

We will refer to these as the $k \geq 3$ and $k = 2$ cases of the incidence problem, and give the proofs of each in turn.

6.1 Proof of the $k \geq 3$ case

To prove Theorem 2.15, we first prove a weaker version with some regularity assumptions. Note that if $|I_{\geq k}(L)| \sim |L|^{3/2}/k^2$ then we expect each line of L to contain about $|L|^{1/2}/k^2$ points of $I_{\geq k}(L)$ on average. We also will deal first with the more difficult case where the points are all incident to between k and $2k$ lines of L, so we will deal instead with the set $I = I_{\geq k}(L) \setminus I_{\geq 2k}(L)$ of points. Afterwards we will see how to recover Theorem 2.15 from this regular version.

Guth and Katz' proof elegantly combines the two approaches we have seen so far, by creating a decomposition of space by polynomial partitioning and arguing that either:

1. many of the points lie in cells, in which case we can use a divide and conquer technique like we saw in the proof of the Szemerédi-Trotter theorem; or

2. most of the points lie in the boundary $Z(p)$, in which case we can use the polynomial method like for the joints conjecture.

In the second case, the boundary $Z(p)$ on which most of the points lie is of much lower degree than we would get by constructing it directly, which is what enables the proof to be completed.

Theorem 6.1. *Let L be a finite set of lines in $\mathbb{R}^3$ and I a finite set of points satisfying*

(a) no plane contains more than $|L|^{1/2}$ lines of L,

(b) every point in I is incident to between k and $2k$ lines of L, and

(c) at least $\frac{1}{100}|L|$ lines in L contain at least $\frac{1}{100}k\frac{|I|}{|L|}$ points of I.

Then there is an absolute constant A such that for $3 \leq k \leq |L|^{1/2}$,

$$|I| \leq A\frac{|L|^{3/2}}{k^2}$$

Proof. If $k \leq 10^9$ then from the joints problem (Theorem 4.2) there is a constant A_1 such that

$$|I| \leq A_1 N^3 = 10^{18} A_1 \frac{N^3}{10^{18}} \leq A\frac{N^3}{k^2}$$

for large enough A. Hence in the following we assume $k \geq 10^9$.

For contradiction, suppose that we have sets L, I satisfying the hypothesis and such that

$$|I| > A\frac{N^3}{k^2}. \tag{6.1}$$

By the Polynomial Partitioning lemma 5.6, there is a polynomial $p \in \mathbb{R}[x, y, z]$ of degree $d_0 \lesssim d$ (where $d \geq 1$ is a parameter) such that $\mathbb{R}^3 \setminus Z(p)$ consists of d^3 open cells $O_1, \ldots, O_m$ satisfying $|P_i| = |I \cap O_i| \leq |I|/d^3$. Let

$$d = \lfloor 10^5 |L|^{1/2}/k \rfloor \leq 10^5 |L|^{1/2}/k. \tag{6.2}$$

Then d satisfies:

(i) $d \geq 1$ since $k < |L|^{1/2}$, so this choice of d is valid;

(ii) $d < 10^{-8} k\frac{|I|}{|L|}$ since using (6.1),

$$d \leq 10^5 |L|^{1/2} k^{-1} \leq \frac{10^5}{A}\frac{A|L|^{3/2}}{k^2}\frac{k}{|L|} < 10^{-8} k\frac{|I|}{|L|};$$

(iii) $d \leq 10^{-4}|L|^{1/2}$ since $k \geq 10^9$ so

$$d \leq 10^5|L|^{1/2}k^{-1} \leq 10^{-4}|L|^{1/2}.$$

Now we split into cases depending on whether most points lie on the boundary $Z(p)$ of the decomposition or most points lie in the cells O_i. In each case we arrive at a contradiction.

Case 1. $|Z(p) \cap I| < 1 - 10^{-8}$**:**

Then the cells O_i together contain at least $10^{-8}|I|$ points. Let P_i and L_i denote respectively the sets of points and lines intersecting O_i. Thus

$$\sum_{i=1}^{m} |P_i| > 10^{-8}|I|. \tag{6.3}$$

By the Szemerédi-Trotter theorem (Corollary 5.9),

$$\sum_{i=1}^{m} |P_i| \leq \sum_{i=1}^{m} \left(\frac{|L_i|^2}{k^3} + \frac{|L_i|}{k} \right). \tag{6.4}$$

Furthermore, by Lemma 3.5 and since a line intersecting a cell O_i is not contained in $Z(p)$, $\sum_{i=1}^{m} |L_i| \leq d|L|$. Since each point has at most $2k$ lines passing through it, $\max_{i=1}^{m} |L_i| \leq 2k|I|/d^3$. Thus

$$\sum_{i=1}^{m} |L_i|^2 \leq (\max_{i=1}^{m} |L_i|) \sum_{i=1}^{m} |L_i| \leq 2k|I||L|/d^2. \tag{6.5}$$

Now applying (6.3), (6.4), (6.5) and finally (6.2),

$$10^{-8}|I| \leq 2|I||L|/(d^2k^2) + d|L|/k \leq 2 \cdot 10^{-10}|I| + 10^5|L|^{3/2}/k^2,$$

which implies that

$$|I| \leq 10^{14}|L|^{3/2}/k^2,$$

a direct contradiction to (6.1) provided the constant A is large enough.

Case 2. $|Z(p) \cap I| \geq 1 - 10^{-8}$**:**

By constructing this surface via polynomial partitioning, we have managed to find a very low degree surface containing most of I. We now show that it contains a definite fraction of the lines L as well.

Let $L_Z = \{l \in L \mid l \subset Z(p)\}$ denote the lines of L contained in $Z(p)$, and $I_Z = I \cap Z(p)$ the points of I contained in $Z(p)$.

Claim. $|L_Z| \geq \frac{1}{200}|L|$.

By Lemma 3.5, each line in $L \setminus L_Z$ contains at most d points of I_Z. Let L_0 be the set of lines in L containing at least $10^6 d$ points of I. Then each line of $L_0 \setminus L_Z$ contains at least $(10^6 - 1)d \geq \frac{1}{2}10^6 d$ points of $I \setminus I_Z$. On the other hand, each point of $I \setminus I_Z$ is incident to at most $2k$ lines of L. Together this gives us

$$\frac{1}{2}10^6 d|L_0 \setminus L_Z| \leq I(I \setminus I_Z, L_0 \setminus L_Z) \leq |I \setminus I_Z|2k \leq 2 \cdot 10^{-8}|I|k$$

So that by (ii), $|L_0 \setminus L_Z| \leq 4 \cdot 10^{-6} N^2$. We have $10^6 d \leq \frac{1}{100}\frac{|I|}{|L|}$ by (ii). Thus $|L_0| \geq \frac{1}{100}|L|$ and hence $|L_Z| \geq \frac{1}{200}N^2$.

We know that the surface contains most of the points and lines of L and I. We already know that each point of I is incident to at least k lines of L, but we want to know that in fact most points of I are incident to at least 3 lines *in* L_Z. Let $I'_Z = I_Z \cap I_{\geq 3}(L_Z)$ denote those points of I_Z incident to at least three lines of L_Z.

Claim. $|I'_Z| \geq (1 - 10^{-7})|I|$.

Each point in $I_Z \setminus I'_Z$ is incident to at least k lines of L but at most 2 lines of L_Z. Each line of $L \setminus L_Z$ is incident to at most d points of I_Z. Hence

$$(k-2)|I_Z \setminus I'_Z| \leq I(I_Z \setminus I'_Z, L \setminus L_Z) \leq |L|d \leq 10^{-8}|I|k,$$

where the last inequality uses (ii). Then $|I_Z \setminus I'_Z| \leq 10^{-8}\frac{k}{k-2}|I| \leq 3 \cdot 10^{-8}|I|$, while $|I_Z| \geq (1 - 10^{-8})|I|$. Hence $|I'_Z| \geq (1 - 10^{-7})|I|$.

Finally, we can show that the surface $Z(p)$ contains many lines which are incident to a large number of points of I'_Z. Let L'_Z be the set of lines of L_Z that contain at least $\frac{1}{200}k\frac{|I|}{|L|}$ points of I'_Z.

Claim. $|L'_Z| \geq \frac{1}{200}|L|$.

By Lemma 3.5, each line in $L \setminus L'_Z$ contains at most d points of I'_Z. As before we take L_0 to be the lines in L containing at least $10^6 d$ points of I. Then each line of $L_0 \setminus L'_Z$ contains at least $(10^6 - 1)d \geq \frac{1}{2}10^6 d$ points of $I \setminus I'_Z$. On the other hand, each point of $I \setminus I'_Z$ is incident to at most $2k$ lines of L. Together this gives us

$$\frac{1}{2}10^6 d|L_0 \setminus L'_Z| \leq I(I \setminus I'_Z, L_0 \setminus L'_Z) \leq |I \setminus I'_Z|2k \leq 2 \cdot 10^{-7}|I|k$$

So that by (ii), $|L_0 \setminus L'_Z| \leq 4 \cdot 10^{-5}|L|$. So since $|L_0| \geq \frac{1}{100}|L|$ we have $|L'_Z| \geq \frac{1}{200}|L|$.

Let us recap: we have found a surface $Z(p)$ of low degree and we have found a set of lines L'_Z contained in $Z(p)$ with the property that each line in this set intersects many other lines in the set, and at these intersection points at least three lines meet. This is exactly the kind of structure we were dealing with in the joints conjecture and the 'flat' joints conjecture. Indeed we have already given Proposition 4.15 which bounds the number of lines in this situation.

To check we can apply Proposition 4.15 we first note that we can assume p is square-free, since if we form p' by removing repeated factors from p, then $Z(p') = Z(p)$ and the degree of p' is at most the degree of p. Furthermore we know that each line in L'_Z is incident to $\frac{1}{200}k\frac{|I|}{|L|}$ points of I'_Z and

$$\frac{1}{200}k\frac{|I|}{|L|} > \frac{1}{200}10^8 d > 4d$$

by (ii). Hence applying Proposition 4.15 to the set L'_Z of lines and the set I'_Z of points we have

$$|L'_Z| \leq 4d^2 + |L|^{1/2}d.$$

Finally, by (7.iii) note that $4d^2 + |L|^{1/2}d \leq 4 \cdot 10^{-8}|L| + 10^{-4} < \frac{1}{200}$, contradicting the previous claim.

So in either case we arrive at a contradiction. □

Having proved Theorem 6.1, we can remove the regularity assumptions to get the full Theorem 2.15. The first step is to remove the assumption that intersections are roughly evenly spread amongst the lines, using an inductive argument similar to that in the proof of the joints conjecture.

Theorem 6.2. *Let L be a finite set of lines in $\mathbb{R}^3$ and I a finite set of points satisfying*

(a) no plane contains more than $|L|^{1/2}$ lines of L, and

(b) every point in I is incident to between k and $2k$ lines of L.

Then there is an absolute constant A such that for $3 \leq k \leq |L|^{1/2}$ we have

$$|I| \leq A\frac{|L|^{3/2}}{k^2}$$

Proof. Let $L_1 \subset L$ be those lines containing at least $\frac{1}{100}k\frac{|I|}{|L|}$ points of I. If $|L_1| \geq \frac{1}{100}|L|$ then we can apply Theorem 6.1, and we are done. We will show by induction that this in fact holds for all $|L_1|$, by induction on $|L|$. From now on we assume $|L_1| < \frac{1}{100}|L|$.

We have

$$I(I, L \setminus L_1) \leq \frac{1}{100}|I|k|L|/|L| \leq \frac{1}{100}|I|k.$$

Let I_1 be those points with at least $\frac{9}{10}k$ incidences with lines of L_1. Any point in $I \setminus I_1$ lies in at least k lines of L, but at most $\frac{9}{10}k$ lines of L_1, so lies in at least $\frac{1}{10}k$ lines of $L \setminus L_1$. Hence

$$\frac{1}{10}k|I \setminus I_1| \leq I(I \setminus I_1, L \setminus L_1) \leq \frac{1}{100}|I|k.$$

Or rearranged, $|I \setminus I_1| \leq \frac{1}{10}|I|$ and so $|I_1| \geq \frac{9}{10}|I|$.

Let $I_1 = I_+ \cup I_-$ where I_+ consists of the points with at least k incidences to L_1 and I_- the points with less than k incidences to L_1. Let I' be the larger of these, so that $|I'| \geq \frac{9}{20}|I|$.

Case 1. $I' = I_+$.

Each point of I' is incident to between k and $2k$ lines of L_1, so we can apply induction to the sets L_1 and I', which satisfy the hypotheses. Hence

$$|I'| \leq A(|L_1|^{3/2}/k^2 + |L_1|/k) \leq \frac{1}{100} A(|L|^{3/2}/k^2 + |L|/k)$$

so that $|I| \leq \frac{20}{9}|I'| \leq \frac{20}{900} A(|L|^{3/2}/k^2 + |L|/k)$.

Case 2. $I' = I_-$.

Each point of I' is incident to between $\lceil \frac{9}{10}k \rceil$ and k lines of L_1, so we can apply induction to the sets L_1 and I' with $k_1 = \lceil \frac{9}{10}k \rceil \geq 3$, which satisfy the hypotheses. Hence

$$|I'| \leq A(|L_1|^{3/2}/k_1^2 + |L_1|/k_1) \leq \frac{1}{100} \left(\frac{10}{9}\right)^3 A(|L|^{3/2}/k^2 + |L|/k)$$

so that $|I| \leq \frac{20}{9}|I'| \leq \frac{200}{6561} A(|L|^{3/2}/k^2 + |L|/k)$.

Finally we have $k \leq |L|^{1/2}$ so that $|L|/k \leq |L|^{3/2}/k^2$ and hence in either case we have $|I| \leq A\frac{|L|^{3/2}}{k^2}$ as desired.

□

Finally, Theorem 2.15 follows quickly from Theorem 6.2 by applying it to a decomposition of the possible values for the number of lines meeting at a point, i.e. the discrete interval $[k, \infty)$.

Theorem 2.15 ([27, Proposition 2.11])**.** *Let L be a finite set of lines in $\mathbb{R}^3$ for which no more than $|L|^{1/2}$ lie in a common plane, and let $3 \leq k \leq |L|^{1/2}$. Then $|I_{\geq k}(L)| \lesssim |L|^{3/2}/k^2$.*

Proof. Notice that as discrete intervals,

$$[k, \infty) = [k, 2k) \cup [2k, 2^2k) \cup [2^2k, 2^3k) \cup \cdots .$$

The idea is to apply Theorem 6.2 for k values in these subintervals individually. Let $I = \cup_{j=0}^{\infty} I_j$ where I_j is the set of points in I incident to between $2^j k$ and $2^{j+1}k$ lines. Applying Theorem 6.2 to the lines L and the set I_j gives

$$|I_j| \leq 2^{-2j} A \frac{|L|^{3/2}}{k^2}.$$

Now since $I = \cup_{j=0}^{\infty} I_j$,

$$|I| \leq \sum_{j=0}^{\infty} |I_j| \leq 2A\frac{|L|^{3/2}}{k^2}.$$

□

6.2 Proof of the $k = 2$ case

Recall that in the $k = 2$ case, we have examples of sets of lines L contained in reguli which have more than $|L|^{3/2}$ incidences. We have already seen in Section 2.2 that these examples can be excluded from the distinct distances incidence problem. To prove Theorem 2.20, some other observations analogous to those in Chapter 4 are required, to understand the nature of lines contained in ruled surfaces.

Proposition 6.3. *Let $p \in \mathbb{R}[x, y, z]$ be a polynomial of degree d such that $Z(p)$ contains no ruled surface, and let L be a set of lines contained in $Z(p)$. Then*

$$|L| \lesssim d^2$$

This proposition says that ruled surfaces are the only examples of surfaces containing many lines.

Proposition 6.4 ([27, Lemma 3.6])**.** *Let $p \in \mathbb{R}[x, y, z]$ be an irreducible polynomial of degree d such that $Z(p)$ is singly-ruled, and let L be the set of lines contained in $Z(p)$. Then there are two lines $l_1, l_2 \in L$ such that every line in $L \setminus \{l_1, l_2\}$ intersects at most d other lines in L.*

Intuitively, singly-ruled surfaces do not allow for many intersections amongst lines on the surface, with the possible exception of two special lines. Indeed, it follows from Lemma 6.4 that the incidence result holds for singly-ruled surfaces.

Proposition 6.5 ([27, Lemma 3.4])**.** *Let $p \in \mathbb{R}[x, y, z]$ be an irreducible polynomial of degree d such that $Z(p)$ is singly-ruled, and let L be the set of lines contained in $Z(p)$. Then if $d \lesssim |L|^{1/2}$, we have*

$$|I_{\geq 2}(L)| \lesssim |L|^{3/2}.$$

With these three propositions, we can proceed to give the proof of Theorem 2.20.

Theorem 2.20 ([27, Proposition 2.10])**.** *Let L be a finite set of lines in $\mathbb{R}^3$ for which no more than $|L|^{1/2}$ lie in a common plane, and no more than $\lesssim |L|^{1/2}$ lie in a common regulus. Then $|I_{\geq 2}(L)| \lesssim |L|^{3/2}$.*

Proof. We assume for the sake of contradiction that we have a counterexample L which has minimal $|L|$ amongst all counterexamples. Let $I = I_{\geq 2}(L)$. Then

$$|I| \geq A|L|^{3/2}$$

where A is the hidden universal constant in the statement of the theorem.

Let $L' \subset L$ be the subset of lines containing at least $\frac{1}{10}C|L|^{1/2}$ points of intersection in I, where C is a constant to be fixed later. Also let $I' = I_{\geq 2}(L') \subset I$ be the subset of points of intersection of the lines L'. Then

$$|I'| \geq \frac{9}{10}C|L|^{3/2},$$

since lines in $L \setminus L'$ meet at most $\frac{1}{10}C|L|^{1/2}$ points of I, so at most $\frac{1}{10}C|L|^{3/2}$ points have been removed from I.

Define $\alpha \in (0,1]$ by $|L'| = \alpha^2|L|$. Applying Lemma 4.17 to the set L' with constant parameter $\frac{C}{100}$ we get a nonzero polynomial p of degree

$$d \lesssim \frac{1}{C^{1/2}}|L'|^{1/2} = \frac{1}{\sqrt{C}}\alpha|L|^{1/2}$$

such that every line $l \in L'$ is contained in $Z(p)$.

Next we factor $p = p_1 \cdots p_k$ as irreducible factors, for $k \leq d$. As in the proof of 6.1 we can assume that p is square-free so no factors are repeated. If we have two lines $l_1, l_2 \in Z(p)$ which intersect, then one of the following holds

(i) $l_1 \subset Z(p_i)$ and $l_2 \subset Z(p_j)$ with $l_1, l_2 \notin Z(p_i) \cap Z(p_j)$ (an incidence between two lines in different components, with neither line in the intersection);

(ii) $l_1, l_2 \subset Z(p_i)$ and $Z(p_i)$ is ruled; or

(iii) $l_1, l_2 \subset Z(p_i)$ and $Z(p_i)$ is not ruled.

We can bound incidences of each type as follows

(i) A given line $l_1 \in Z(p_i)$ intersects at most d of the sets $Z(p_j)$ with $i \neq j$, so there are at most $d|L'| \lesssim \frac{\alpha^3}{\sqrt{C}}|L|^{3/2}$ such incidences;

(ii) If $Z(p_i)$ is a plane or regulus it contains at most $\lesssim |L|^{1/2}$ lines, so contains at most $\lesssim |L|$ such incidences. Across all factors, there are at most $\lesssim d|L|$ such incidences.

Otherwise if $Z(p_i)$ is singly-ruled then we note that $d \lesssim |L'|^{1/2}$ (when C is chosen appropriately) so we can apply Proposition 6.5 to conclude that the number of such incidences is at most $\lesssim |L'|^{3/2}$ across all singly-ruled factors.

Hence altogether we get at most $d|L| + |L'|^{3/2} \lesssim |L|^{3/2}$ incidences of this form.

(iii) Let p_N be the product of factors p_i for which $Z(p_i)$ is not ruled. Denote by L' the set of lines $l \in L$ contained in $Z(p_N)$. Applying Proposition 6.3, we find that

$$|L'| \lesssim d^2 \lesssim \frac{1}{C}\alpha^2|L|.$$

We would like to apply the minimality of our original counterexample to conclude that L' determines at most $\lesssim |L|^{3/2}$ incidences.

Define β by $|L'| = \beta^2|L|$. We know that L' contains at most $|L|^{1/2}$ lines in any given plane or regulus, and we would like to show that L' contains at most $\beta|L|^{1/2}$ lines in any given plane or regulus so that we could apply induction. To do this, we repeatedly pass to smaller sets of lines by the following algorithm:

(1.) Set $A = L'$, and $B = \emptyset$.

(2.) If A contains at most $|A|^{1/2}$ lines in any given plane or regulus, stop.

(3.) Otherwise, let π be a plane or regulus containing more than $|A|^{1/2}$ lines of A. let L_π be the set of lines of A in π, and set

$$A = A \setminus L_\pi \quad \text{and} \quad B = B \cup L_\pi.$$

(4.) Return to step (2.).

This procedure can take at most $\lesssim |L|^{1/2}$ steps. Now the lines of B are contained in a surface $Z(q)$ which is the union of at most $\lesssim |L|^{1/2}$ planes and reguli, so by the argument from case (ii) they determine at most $\lesssim |L|^{3/2}$ incidences. Similarly, the argument from case (i) gives that there are at most $\lesssim |L|^{3/2}$ incidences between lines of A and B.

Finally since our original counterexample was optimal, by choosing C large enough we have

$$|A| < |L|$$

since $|A| \leq |L'| \lesssim \frac{1}{C}\alpha^2|L|$. Hence A must satisfy the conclusion of the theorem and so there are at most $\lesssim |L|^{3/2}$ incidences between lines in A.

In each case we have at most $\lesssim |L|^{3/2}$ incidences, so the proof is complete. □

Having seen the proofs of these two incidence theorems, we recap how Theorem 1.5 follows from these two results.

Theorem 1.5 (Guth-Katz, [27])**.** *Let P be a finite set of points in the plane. Then $d(P) \gtrsim |P|/\log|P|$.*

Proof. By Theorems 2.20 and 2.15, we have $|G_{\geq k}(P)| \lesssim |L|^{3/2}/k^2$ (recall the notation $G_{\geq k}(P)$ from pg. 8). Hence by (2.3),

$$|Q(P)| \lesssim \sum_{k=2}^{|P|} 2|L|^{3/2}(k-1)/k^2 \lesssim |P|^3 \log|P|.$$

Finally, by (2.1),

$$d(P) \gtrsim \frac{|P|^4 - 2|P|^3}{|P|^3 \log|P|} \gtrsim |P|/\log|P|. \qquad \square$$

In Chapters 1–6 we have studied how Guth and Katz came to their bound on the Erdos distinct distances problem. However, Guth and Katz work has applications outside of this problem. In the next section we give applications of their work to arithmetic combinatorics.

6.3 Applications to arithmetic combinatorics

In Chapter 7 we investigate the application of polynomial techniques to an old conjecture of Dirac and Motzkin. Crucial to this application are the tools of arithmetic (or additive) combinatorics. However, problems from combinatorial geometry do not merely use tools of arithmetic combinatorics—the relationship can also work the other way. In this chapter we see how some of the combinatorial geometric results we have seen can be applied to derive results in arithmetic combinatorics.

To begin with, we define some of the essential notation.

Definition 6.6. If A, B are sets in a group $(G, +)$ then the **sum-set** $A + B$ is

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

If we think of the operation as a product instead call AB the **product-set**. If A is a subset of a ring $(G, +, \cdot)$ then we also extend fractional notation to sets,

$$\frac{1}{A} = \{\frac{1}{a} \mid a \in A, a \neq 0\}.$$

For instance, if $A = \{1, 2, 4, 8 \ldots, 2^k\}$ then the sum-set is $A + A = \{2^i + 2^j \mid 0 \leq i, j \leq k\}$ while the product-set is $AA = \{1, 2, \ldots, 2^{2k}\}$. Note that $|A + A| = k(k + 1)$ while $|AA| = 2k + 1$ since A is a geometric progression. Similarly, the sum-set $A + A$ will be small if A is an arithmetic progression, while the product-set AA will be large. In fact, a converse statement holds in many situations. We state the following version for integers.

Definition 6.7. An **n-dimensional arithmetic progression** in $\mathbb{Z}$ is a set

$$\{a_0 + \sum_{i=1}^{k} a_i x_i \mid x_i \in \{0, \ldots, m_i\}\}$$

where $a_0, a_1, \ldots, a_k \in \mathbb{Z}$ and $m_1, \ldots, m_k \in \mathbb{Z}$ are constants.

Theorem 6.8 (Freiman's Theorem, [22])**.** *If $A \subset \mathbb{Z}$ is finite and $|A + A| \lesssim |A|$ then A is contained in an n-dimensional arithmetic progression P with $|P| \lesssim |A|$. The two implicit constants are dependent, on each other and on n.*

Much more precise statements can be made, but it will be useful to keep the idea of Freiman's theorem in mind as intuition for what sets with small sum- or product-sets look like.

We will now present a beautiful application due to Elekes' [15] of the Szemerédi-Trotter theorem (Theorem 5.1) to a sum- and product-set estimate. We have already seen that geometric progressions have a small product-set but large sum-set, and arithmetic progressions have a small sum-set but large product-set. Elekes' theorem proves that there is no way to strike a balance between these two extremes – either the sum- or product-set must be large. This is commonly known as the *sum-product phenomenon.*

Theorem 6.9 ([15]). *If $A \subset \mathbb{R}$ is a finite set, then*

$$\max\{|A+A|, |AA|\} \gtrsim |A|^{5/4}.$$

Proof. We define sets P and L of points and lines in $\mathbb{R}^2$ as follows:

$$P = (AA) \times (A+A),$$
$$L = \{l_{a,b} = \{(t, \tfrac{1}{a}t + b) \mid t \in \mathbb{R}\} \mid a \in A \setminus \{0\}, b \in A\}.$$

The line $l_{a,b}$ is incident to the point $(ax, x+b)$ for each $x \in A$, so each line l has $|A|$ incidences with P, giving at least $|L||A| \gtrsim |A|^3$ in total. By also applying Szemerédi-Trotter (Theorem 5.1), we get

$$|A|^3 \lesssim I(P,L) \lesssim |P|^{2/3}|L|^{2/3} + |P| + |L| \lesssim |AA|^{2/3}|A+A|^{2/3}|A|^{4/3}.$$

Hence by the pigeonhole principle one of $|AA|, |A+A|$ is $\gtrsim |A|^{5/4}$. □

Recently, the Guth-Katz incidence theorems (Theorems 2.15, 2.20) have found applications similar to Theorem 6.9 in arithmetic combinatorics. The first such application was due to Iosevich et al. [29].

Theorem 6.10 ([29, Corollary 1]). *If $A \subset \mathbb{R}$ is a finite set, then*

$$|AA \pm AA| \gtrsim \frac{|A|^2}{\log |A|}.$$

We also mention the following similar result of Roche-Newton and Rudnev [45]. The proof uses similar methods, following Elekes' reduction strategy to rephrase the problem as an incidence problem.

Theorem 6.11 ([45, (1)]). *If $A, B \subset \mathbb{R}$ are nonempty finite sets then*

$$|(A \pm B)(A \pm B)| \gtrsim \frac{|A||B|}{\log |A| + \log |B|}.$$

In this section we have seen that the Guth-Katz incidence theorems can be used to prove results in arithmetic combinatorics. In Chapters 7–10, we give an account of the recent resolution of the Dirac-Motzkin conjecture using polynomial methods.

Chapter 7

The Dirac-Motzkin Conjecture

We now turn our attention to another famous problem in discrete geometry, which has recently been solved using the algebraic method. As before, we are concerned with finite planar point sets $P \subset \mathbb{R}^2$. Our motivation for studying the distinct distances problem was understanding the distribution of distances determined by the point set P, and in particular which distributions can arise from finite point sets. In this chapter we will concern ourselves with another basic property of P—the distribution of P on *lines*. More formally,

Definition 7.1. For distinct $p, q \in P$, we denote by $\overline{pq}$ the line through p and q. A line L is called a **connecting line** of P if $L = \overline{pq}$ for some $p, q \in P$.

That is, the connecting lines are those lines containing at least two points of P. We would like to understand the distribution of P amongst those lines. In the same way as we did for the distinct distances problem, we define the connecting line distribution of P to be $c_P : \mathbb{Z}_{\geq 2} \to \mathbb{Z}_{\geq 0}$ given by

$$c_P(n) = |\{L \mid L \text{ is a connecting line of } P \text{ and } |L \cap P| = n\}|.$$

Some examples are given in Figure 7.1.

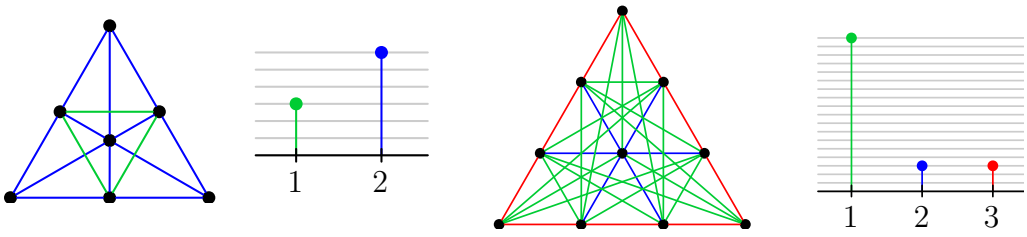


Figure 7.1: Connecting line distributions for some planar point sets.

As before there are many simple questions one could ask about the connecting line distributions. The first simple property to notice is that if P consists of $|P|$ points

on a line then $c_P(|P|) = 1$ and $c_P(n) = 0$ for other values of n, since P determines only one connecting line. In the other extreme, a point set P in general position has $c_P(2) = \binom{|P|}{2}$ and $c_P(n) = 0$ for other values of n. We give a special name to these connecting lines containing the fewest possible number of points

Definition 7.2. A connecting line L of P is called an **ordinary line** of P if $|L \cap P| = 2$.

The phenomenon that $c_P(2) \geq 1$ for non-collinear point sets was first noticed by Sylvester [53] who in 1893 conjectured that this always happens.

Theorem 7.3 (Sylvester-Gallai theorem)**.** *If P is a finite planar point set which is not all contained in a line, then P determines at least one ordinary line. (If $c_P(|P|) = 0$, then $c_P(2) \geq 1$.)*

This conjecture was resolved in 1944 when a proof was supplied by Gallai [23]. We give a slick proof due to Kelly which first appeared in [8], and gives a constructive way to find an ordinary line of P.

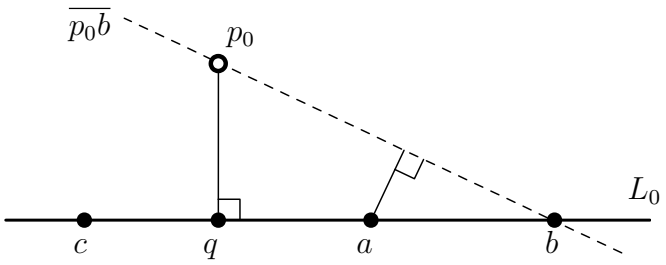


Figure 7.2: Kelly's proof by contradiction that L_0 is ordinary.

Proof. Consider all pairs (p, L) where $p \in P$, L is a connecting line of P and $p \notin L$. There is at least one such pair, since P is not all contained in one line. Let (p_0, L_0) be the pair amongst these which minimises the perpendicular distance between p and L. Now we claim that L_0 is ordinary. For if L_0 were not ordinary, we could find three distinct points $a, b, c \in P \cap L_0$. As in Figure 7.2, let q denote the point on L_0 closest to p_0. Then two of the points a, b, c lie on the same side of q on L_0 (one of the points could be q itself.) Without loss of generality, say a and b are on the same side, and a is closer to q than b is, as in Figure 7.2. Then the perpendicular distance between a and $\overline{p_0 b}$ is strictly smaller than the perpendicular distance between p_0 and L_0, contradicting the choice of (p_0, L_0). □

After computing the connecting lines of some point sets, one finds that $c_P(2)$ is actually fairly *large*. The result of Theorem 7.3 was improved ever so slightly by Melchior [37], who gave another slick proof, this time obtaining the result that non-collinear point sets P determine at least *three* ordinary lines.

Corollary 7.4 (Melchior's Inequality)**.** *If P is a finite planar point set which is not all contained in a line, then P determines at least three ordinary lines. (If $c_P(|P|) = 0$, then $c_P(2) \geq 3$.) In fact, for such P,*

$$c_P(2) \geq 3 + \sum_{k=4}^{\infty} (k-3)c_P(k).$$

While only obtaining a modest improvement to the result of Theorem 7.3, we will see in Chapter 9.1 that the ideas introduced by Melchior's proof played a crucial role in recent progress on this problem (we give Melchior's proof as Theorem 9.4). However, it had already been conjectured that there should be many more ordinary lines — $c_P(2)$ should scale at least linearly in $|P|$. Although apparently only Dirac [11] made this conjecture (c.f. the introduction in [25]) it has become known as the Dirac–Motzkin conjecture.

Conjecture 7.5 (Dirac–Motzkin conjecture)**.** *If P is a finite planar point set which is not all contained in a line, and $|P| \notin \{7, 13\}$, then P determines at least $|P|/2$ ordinary lines. (Or alternatively, without restriction on $|P|$, if $c_P(|P|) = 0$ then $c_P(2) \geq \lfloor |P|/2 \rfloor$.)*

The exceptions at $|P| = 7$ and $|P| = 13$ are due to two examples found by Kelly and Moser [33] and Crowe and McKee [9] which determine only 3 and 6 ordinary lines respectively. Kelly and Moser's 7 point example consists of the vertices, midpoints and centre of an equilateral triangle, as in Figure 7.1, and we illustrate the 13 point example in Figure 8.3.

Following Melchior's result, non-constant bounds were found, including:

- $c_P(2) > \sqrt{|P|}$ in 1951 due to Motzkin [40];
- $c_P(2) > 3|P|/7$ in 1958 due to Kelly and Moser [33];
- $c_P(2) > 6|P|/13$ in 1993 due to Csima and Sawyer [10].

Recently, Green and Tao posted to the arXiv '*On sets defining few ordinary lines*' [25], in which they resolve the Dirac–Motzkin conjecture in the large case.

Theorem 7.6 ([25, Theorem 2.2])**.** *Let $P \subset \mathbb{R}^2$ be a finite non-collinear point set, with $|P| \gtrsim 1$, then*

$$c_P(2) \geq \begin{cases} \frac{1}{2}|P| & \text{if } |P| \equiv 0, 2 \ (mod\ 4) \\ \frac{3}{4}(|P|-1) & \text{if } |P| \equiv 1 \ (mod\ 4) \\ \frac{3}{4}(|P|-3) & \text{if } |P| \equiv 3 \ (mod\ 4) \end{cases}.$$

In fact, Green and Tao prove a very strong *classification theorem* which not only allows for the deduction of Theorem 7.6 but also completely classifies the planar point sets P determining fewer than $|P| - C$ ordinary lines, where C is a constant. In the remainder of this thesis we give Green and Tao's application of the algebraic method to prove this classification theorem and hence Theorem 7.6. In the next chapter, we review basic concepts from projective space.

Chapter 8

Extremal Examples

In this chapter we give the construction of two families of examples of point sets determining few ordinary lines: the Böröczky and Sylvester examples. In section 8.1 we recall the relevant background material on projective planes.

8.1 Projective Space

It turns out that to understand point sets with few ordinary lines, it is useful to embed them inside projective space. As we will see, this is closely related to the phenomenon that algebraic curves over $\mathbb{R}^2$ become simpler to understand when we embed them inside projective space.

Definition 8.1. If $\mathbb{F}$ is a field, then the **projective plane** over $\mathbb{F}$ is

$$\mathbb{PF}^2 = \left(\mathbb{F}^3 \setminus \{(0,0,0)\}\right) / \sim$$

where the equivalence relation $\sim$ is defined by $(x,y,z) \sim \lambda(x,y,z)$ for all $(x,y,z) \in \mathbb{F}^3 \setminus \{(0,0,0)\}$ and $\lambda \in \mathbb{F} \setminus \{0\}$. The **affine part** of $\mathbb{PF}^2$ is $\{[x,y,1] \mid x,y \in \mathbb{F}\}$ and there is a natural embedding of $\mathbb{F}^2$ into the affine part of $\mathbb{PF}^2$ by sending $(x,y) \mapsto [x,y,1]$. The non-affine part of $\mathbb{PF}^2$ is $\{[x,y,0] \mid x,y \in \mathbb{F}\}$ and is called the **line at infinity**. We call $\mathbb{PR}^2$ the **real projective plane**.

A point in $\mathbb{PF}^2$ is an equivalence class consisting of the points on a line through the origin in $\mathbb{F}^3$, excluding the origin. Similarly, a line in $\mathbb{PF}^2$ is an equivalence class consisting of points on a plane through the origin. We will soon see several ways to visualise the projective plane, but one useful way is to imagine it as the disjoint union of the usual plane $\mathbb{F}^2$ with a line l_∞, which contains one point for each distinct *direction* of a line in $\mathbb{F}^2$, and defining lines to be either $l \cup \{p\}$ where l is a line in $\mathbb{F}^2$ and p is the point corresponding to the direction of p, or the line l_∞.

In the real case, it is handy to consider alternative ways of defining the real projective plane. In particular, we note that we could have equivalently defined

$$\mathbb{PR}^2 = \{\mathbf{x} \in \mathbb{R}^3 \mid ||\mathbf{x}|| = 1\} / \sim$$

to be the sphere with antipodal points identified, so that each point of $\mathbb{PR}^2$ corresponds to two points of in $\mathbb{R}^3$. One could go one step further and define

$$\mathbb{PR}^2 = \{\mathbf{x} = (x, y, z) \in \mathbb{R}^3 \mid ||\mathbf{x}|| = 1 \text{ and } z \geq 0\}/\sim$$

to be a closed hemisphere with antipodal points identified, so that the points in the affine part of $\mathbb{PR}^2$ correspond to exactly one point of $\mathbb{R}^3$, while points on the line at infinity correspond to exactly two points of $\mathbb{R}^3$. Since these alternate definitions amount to choosing subsets of the equivalence classes in Definition 8.1, these definitions are all equivalent.

With each of these definitions we can visualise point sets P in $\mathbb{PR}^2$ by drawing each point $p \in P$ as the equivalence class $[p] \subset \mathbb{R}^3$. The advantage of the alternative definitions is that the resulting images are much simpler. In Figures 8.1–8.3 we show the extremal 13-point example found by Crowe and McKee [9]. Figure 8.1 shows the example on the sphere with antipodal points identified, where the equivalence class of a line is a great circle on the sphere (an example is shown in green.) Similarly, Figure 8.2 shows the same example on the closed hemisphere with antipodal points identified. In the third example, Figure 8.3, we project onto the plane $z = 0$ to give a visualisation of the example on the closed disc.

When illustrating point sets in $\mathbb{PR}^2$, we will always use this third type of visualisation, in which the affine part of $\mathbb{PR}^2$ is contained in the interior of the disc and the line at infinity is the boundary. Note that projective lines correspond to *half-ellipses* joining antipodal points on the boundary of the disc (Figure 8.3 shows six ordinary lines, four of which are half-ellipses). We also stress that antipodal points on the boundary are identified, so the example in Figure 8.3 contains only 13 points.

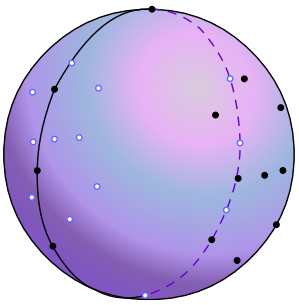


Figure 8.1: On the sphere with antipodal points identified.

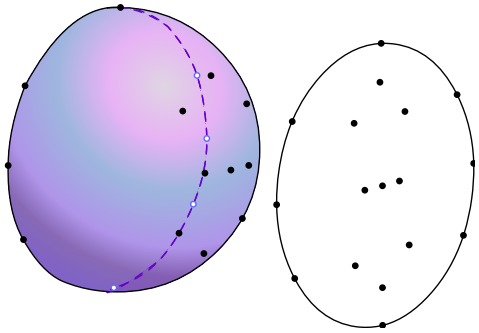


Figure 8.2: On the closed hemisphere with antipodal points identified

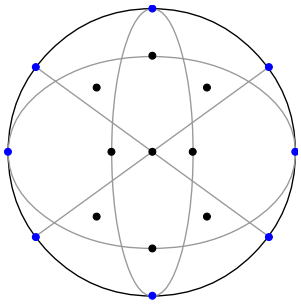


Figure 8.3: On the disc with antipodal points identified

One of the convenient properties of projective planes is that there is a natural duality between points and lines.

Definition 8.2. If $p = [x, y, z] \in \mathbb{PR}^2$, then the **dual** of p is the line

$$p^* = \{q = [a, b, c] \in \mathbb{PR}^2 \mid q \cdot p = ax + yb + zc = 0\}.$$

Similarly the dual of the line $l = \{p+qt \mid t \in \mathbb{R}\}$ is the point l^* such that $p \cdot l^* = q \cdot l^* = 0$. The notation extends naturally to sets by defining $S^* = \{s^* \mid s \in S\}$ for a set S of points or lines.

As the definition suggests, one can think of the dual of a point as the orthogonal complement of the equivalence class of the point, or in the case of a line orthogonal complement of the union of equivalence classes of points in the line. In this way, one can check that the dual is well-defined and that the following basic results hold.

Proposition 8.3. *Let $p \in \mathbb{PR}^2$ and $l \subset \mathbb{PR}^2$ be a point and line in the real projective plane, respectively. Then $(p^*)^* = p$ and $(l^*)^* = l$. Also, $p \in l$ if and only if $l^* \in p^*$.*

This duality allows for a translation between results about points lying on exactly k lines and results about lines containing exactly k points. In particular the number of ordinary lines of the point set P is the same as the number of *ordinary points* (points lying on exactly two connecting lines) of P^*. We will see in Chapter 9.1 how this observation was used by Melchior to solve Sylvester's problem.

To use polynomials over projective space, we will need to define what we mean by a polynomial and an algebraic curve over $\mathbb{PR}^2$.

Definition 8.4. A polynomial p is **homogeneous** if every monomial of p has the same degree.

Suppose $P \subset \mathbb{R}^2$ is a point set which lies in the zero set of a polynomial q. We have seen that P can be embedded into the affine part of $\mathbb{PR}^2$ in a natural way. It turns out that there is also a natural way to embed $Z(q)$ into $\mathbb{PR}^2$.

Definition 8.5. A **projective curve** is the zero set in $\mathbb{PR}^2$ of a homogeneous polynomial in $\mathbb{R}[x, y, z]$. If $q \in \mathbb{R}[x, y]$ has degree d then its **homogenisation** is $q^h(x, y, z) = z^d q(\frac{x}{z}, \frac{y}{z}) \in \mathbb{R}[x, y, z]$, and the **projectivisation** of $Z(q) \subset \mathbb{R}^2$ is $Z(q^h) \subset \mathbb{PR}^2$.

A projective curve is well-defined since for a homogeneous polynomial p, $\lambda^3 p(x, y, z) = p(\lambda x, \lambda y, \lambda z)$, and so $(x, y, z) \in Z(p)$ if and only if $\lambda(x, y, z) \in Z(p)$. An advantage of working over $\mathbb{PR}^2$ is that low-degree projective curves can be classified in a much simpler way than real algebraic curves.

Definition 8.6. A **projective transformation** is a map $f : \mathbb{PR}^2 \to \mathbb{PR}^2$ taking a point $p = [x, y, z]$ to the equivalence class of the point $A(p)$, where $A : \mathbb{R}^3 \to \mathbb{R}^3$ is an invertible linear transformation. Two sets $S, R \subset \mathbb{PR}^2$ are **projectively equivalent** if $S = f(R)$ for some projective transformation f.

In particular, one has the following results, classifying conics and cubics up to projective equivalence.

Proposition 8.7 ([3, Theorem 5.1])**.** *If $p \in \mathbb{R}[x, y, z]$ is irreducible and homogeneous of degree 2, then $Z(p)$ is projectively equivalent to $Z(x^2 + y^2 - z^2)$.*

We will also sometimes extend this concept the real algebraic curves, to say that $Z(p), Z(q) \subset \mathbb{R}^2$ are projectively equivalent if their projectivisations are projectively equivalent, and abusing notation we will say that $p = 0$ and $q = 0$ are projectively equivalent. Then the two preceding results give that nondegenerate conics in the plane are projectively equivalent to the unit circle. Cubic curves also admit a classification.

Proposition 8.8 ([3, Theorem 8.4])**.** *If $p \in \mathbb{R}[x, y]$ is irreducible of degree 3, then $Z(p)$ is projectively equivalent to one of:*

1. *(nodal case) $y^2 = x^2(x + 1)$;*
2. *(cuspidal case) $y^2 = x^3$;*
3. *(acnodal case) $y^2 = x^2(x - 1)$;*
4. *(elliptic curve) $y^2 = ax^3 + bx^2 + cx + d$ with $\Delta = -16(4a^3 + 27b^2) \neq 0$ (Δ is the* discriminant*).*

The Green and Tao proof works with point sets in projective space. In the remainder of the chapter we give the important extremal examples of point sets in $\mathbb{PR}^2$ that determine few ordinary lines.

8.2 The Böröczky examples

We first give the examples due to Böröczky and McKee [9], determining the fewest ordinary lines amongst all known constructions.

Definition 8.9. We define for each $n \geq 1$ subsets of $\mathbb{PR}^2$ by setting

$$\Delta_n = \{[\cos \frac{2\pi i}{n}, \sin \frac{2\pi i}{n}, 1] \mid i = 0, \ldots, n-1\}$$

to be an n-gon in the affine part of $\mathbb{PR}^2$, and

$$D_n = \{[\sin \frac{\pi i}{n}, \cos \frac{\pi i}{n}, 0] \mid i = 0, \ldots, n-1\}$$

to be the points on the line at infinity corresponding to the directions of the connecting lines of Δ_n. Then we set

$$X_{2n} = \Delta_n \cup D_n.$$

Note that $|\Delta_n| = n$ and $|D_n| = n$ so that $|X_{2n}| = 2n$.

The claim that D_n corresponds to the directions of the connecting lines of Δ_n follows from the observation that the angle a chord pq of Δ_n makes with the segment from p to $[0, 0, 1]$ is $(\pi - \theta)/2$ where θ is the angle subtended by pq. Hence the direction of $\overline{pq}$. The claim can also be verified by computing the direction of such a chord explicitly with some simple trigonometric identities.

The sets X_{2n} give examples of point sets defining few ordinary lines for even $|P|$, and slight variations give examples for odd $|P|$. The following proposition summarises these five classes of examples.

Proposition 8.10. *For $n \geq 1$ and $0 \leq i \leq 2n$,*

(1) $P = X_{2n}$ determines $n = \frac{1}{2}|P|$ ordinary lines, and $|P|$ is even;

(2) $P = X_{4n} \cup [0,0,1]$ determines $3n = \frac{3}{4}(|P|-1)$ ordinary lines, and $|P| \equiv 1 \pmod 4$;

(3) $P = X_{4n+2} \setminus [\sin\frac{\pi i}{2n+1}, \cos\frac{\pi i}{2n+1}, 0]$ determines $3n = \frac{3}{4}(|P|-1)$ ordinary lines, and $|P| \equiv 1 \pmod 4$;

(4) $P = X_{4n} \setminus [0,1,0]$ determines $3n-3 = \frac{3}{4}(|P|-3)$ ordinary lines, and $|P| \equiv 3 \pmod 4$;

(5) $P = X_{4n} \setminus [-\sin\frac{\pi}{2n}, \cos\frac{\pi}{2n}, 0]$ determines $3n = \frac{3}{4}(|P|+1)$ ordinary lines, and $|P| \equiv 3 \pmod 4$.

We will call examples (1)−(5) the **Böröczky examples**, though Green and Tao call example (5) the near-Böröczky example. These five classes of examples are illustrated in Figures 8.4–8.8.

Proof. (1) The only connecting lines of P which are ordinary are the tangents to Δ_n, of which there are precisely n.

(2) None of the tangents to Δ_{2n} pass through $[0,0,1]$ so all $2n$ of these are ordinary. Since $2n$ is even, only n of the lines joining $[0,0,1]$ to a point of D_{2n} are ordinary for P, so altogether P determines $3n$ ordinary lines.

(3) If i is even, the tangent line to $[\cos\frac{\pi i}{2n+1}, \sin\frac{\pi i}{2n+1}, 1]$ is not ordinary, and if i is odd the tangent line to $[-\cos\frac{\pi i}{2n+1}, -\sin\frac{\pi i}{2n+1}, 1]$ is not ordinary. However the remaining $2n$ tangents to Δ_{2n+1} are ordinary. In addition, if i is even the lines joining $[\cos\frac{\pi(i+2j)}{2n+1}, \sin\frac{\pi(i+2j)}{2n+1}, 1]$ to $[\cos\frac{\pi(i-2j)}{2n+1}, \sin\frac{\pi(i-2j)}{2n+1}$ for $j = 1, 2, \ldots, n$ are ordinary, and if i is odd then for $j = 1, 2, \ldots, n$ the lines joining $[-\cos\frac{\pi(i+2j)}{2n+1}, -\sin\frac{\pi(i+2j)}{2n+1}, 1]$ to $[-\cos\frac{\pi(i-2j)}{2n+1}, -\sin\frac{\pi(i-2j)}{2n+1}, 1]$ are ordinary.

(4) The tangent lines to $[1,0,1]$ and $[-1,0,1]$ are no longer ordinary as they only contain one point of P, but the remaining $2n-2$ tangents to Δ_{2n} are ordinary. In addition, if $[x,y,1] \in \Delta_{2n}$ with $[x,y,1] \neq [1,0,1], [-1,0,1]$ then the line joining $[x,y,1]$ to $[x,-y,1]$ is ordinary for P, giving a further $\frac{1}{2}(2n-2) = n-1$ ordinary lines.

(5) The $2n$ tangent lines to Δ_{2n} are ordinary, as are the n connecting lines of Δ_n in the direction $[-\sin\frac{\pi}{2n}, \cos\frac{\pi}{2n}, 0]$.

□

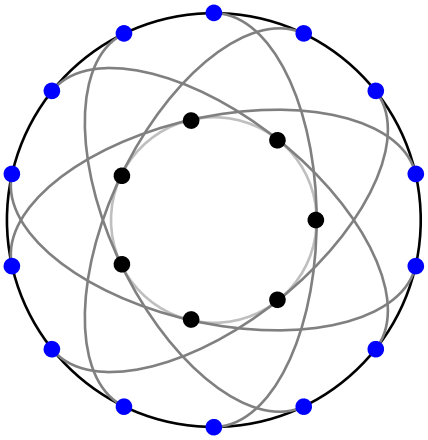


Figure 8.4: The type *(1)* Böröczky example X_{14}

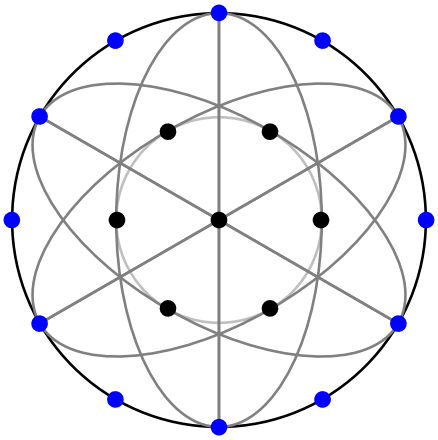


Figure 8.5: The type *(2)* Böröczky example $X_{12} \cup [0, 0, 1]$

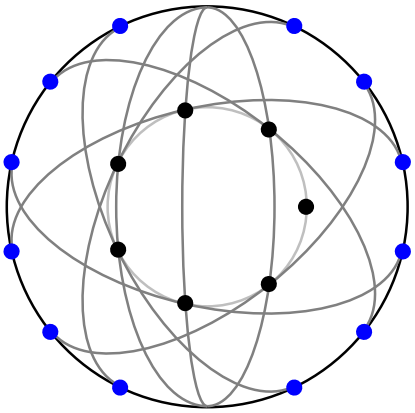


Figure 8.6: The type *(3)* Böröczky example $X_{14} \setminus [0, 1, 0]$

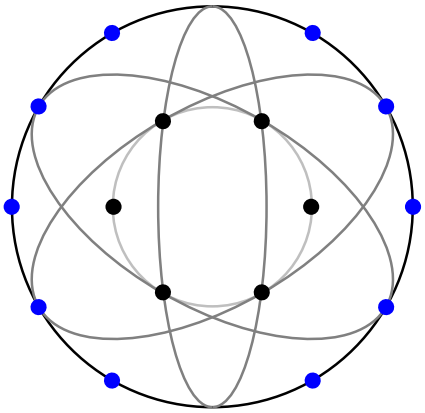


Figure 8.7: The type *(4)* Böröczky example $X_{12} \setminus [0, 1, 0]$

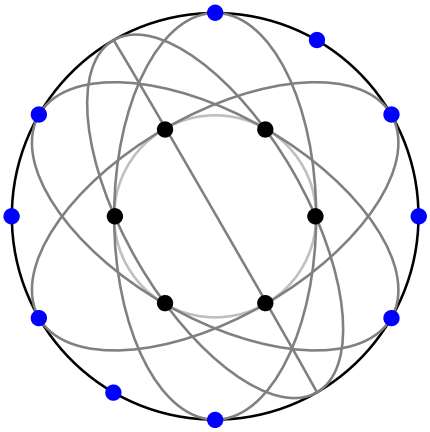


Figure 8.8: The type *(5)* Böröczky example $X_{12} \setminus [\frac{1}{2}, \frac{\sqrt{3}}{2}, 0]$

8.3 The Sylvester Examples

The Sylvester examples are determined by the group law on the set $Z(p)^*$ of non-singular points of a homogeneous degree 3 polynomial $p \in \mathbb{R}[x, y, z]$. For background about the group law on such curves, we refer the reader to Silverman and Tate [50].

We have already seen a classification of cubic curves up to projective equivalence in Proposition 8.8. Since the group law on a cubic is preserved under projective transformations, this classification can be used to produce a classification of the group $Z(p)^*$ in this case.

Proposition 8.11 ([50])**.** *Let $p \in \mathbb{R}[x, y]$ be irreducible and homogeneous of degree 3. Recall that Proposition 8.8 classifies such the curves $Z(p)$ up to projective equivalence. In the cases in the conclusion of this proposition, the group $Z(p)^*$ of non-singular points is isomorphic to:*

1. *(nodal case) $\mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$;*
2. *(cuspidal case) $\mathbb{R}$;*
3. *(acnodal case) $\mathbb{R}/\mathbb{Z}$;*
4. *(elliptic curve) $\mathbb{R}/\mathbb{Z}$ if $Z(p)$ has one connected component, or $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $Z(p)$ has two connected components.*

The Sylvester examples are either subgroups of these groups, or cosets of subgroups.

Definition 8.12. Let $Z(p)$ be an irreducible cubic curve, and E be a subgroup of $Z(p)^*$ with $|E| \geq 3$. Then we call the set $E \subset \mathbb{PR}^2$ a **Sylvester example**. In addition, if $x \in Z(p)^* \setminus E$ and $3x \in E$ then we call the coset $E \oplus x$ a **Sylvester example**.

Since we require the Sylvester examples to have size $|E| \geq 3$, these Sylvester examples only exist in the acnodal or elliptic curve case, since in these cases the group $Z(p)^*$ has finite subgroups of size greater than two.

Proposition 8.13. *Let E and $E \oplus x$ be Sylvester examples as per Definition 8.12. Recall that $c_P(2)$ denotes the number of ordinary lines spanned by P. Then*

$$c_E(2) = \begin{cases} |E| - 1 & \text{if } |E| \equiv 1, 2 \ (mod\ 3) \\ |E| - 3 & \text{if } |E| \equiv 0 \ (mod\ 3) \end{cases}.$$

and

$$c_{E \oplus x}(2) = |E| - 1.$$

Proof. Since $a \oplus b \oplus c = 0$ if and only if $a, b, c \in Z(p)^*$ are collinear, the number of ordinary lines in $E \oplus x$ is the number of elements $a \oplus x \in E \oplus x$ satisfying $a \oplus x \neq \ominus 2a \ominus 2x$. To see this, observe that $a \oplus x, \ominus 2a \ominus 2x$ are collinear, $\ominus 2a \ominus 2x = (\ominus 2a \ominus 3x) \oplus x \in E \oplus x$ (here we use that $3x \in E$), and the line joining them is tangent to $Z(p)$ at a, so meets

no other point of $Z(p)$.) Conversely, any ordinary line of $E \oplus x$ must be tangent to $Z(p)$ at a point $a \oplus x$, so is of this form.

So we just need to compute the number of solutions to $a \oplus x = \ominus 2a \ominus 2x$, i.e. $3(a \oplus x) = 0$. Since we are in the acnodal or elliptic curve case, $Z(p)^*$ is isomorphic to either $\mathbb{R}/\mathbb{Z}$ or $(\mathbb{R}/\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. If $|E| \equiv 0 \pmod 3$ and $x = 0$ then there are three solutions, and otherwise there is one solution $a \oplus x = 0$, so the proposition holds. □

A Sylvester example with $|E| = 6$ is given in Figure 8.9, and one can see that indeed $c_E(2) = 3$.

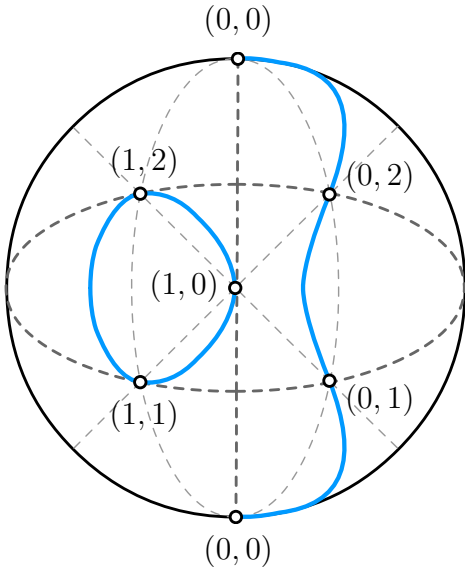


Figure 8.9: A 6-point Sylvester example on the elliptic curve $Z(p^h)$, where $p(x, y) = y^2 - x^3 - x^2 + x$. The Sylvester example is the subgroup $E = \{[0, 1, 0], [0, 0, 1], [1, 1, 1], [1, -1, 1], [-1, -1, 1], [1, 1, 1]\}$. In this case $E \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the points are labelled according to this isomorphism. All connecting lines of E are drawn, and the three ordinary lines are darkened.

8.4 An 'Almost Group Law' and the Böröczky examples

Recall that the group law on a cubic $Z(p)$ is determined by requiring that $a, b, c \in Z(p)^*$ are collinear precisely if

$$a \oplus b \oplus c = 0.$$

It turns out that the same construction can be applied in the case of some non-irreducible degree 3 polynomials to obtain an 'almost' group law. No true group law with these properties can exist on such a curve, as the curve necessarily has a linear

component and so any three points in this component must add to zero. The 'almost' group law gives an operation which achieves this whenever only one of a, b, c lies in the linear component.

Proposition 8.14 ([25, Proposition 7.3]). *Let $p = \sigma l \in \mathbb{R}[x, y, z]$, with σ and l irreducible of degree 2 and 1 respectively. Then there is an abelian group $(G, \oplus)$ with bijective maps*

$$\psi_\sigma : G \to Z(\sigma)^* \quad \text{and} \quad \psi_l : G \to Z(l)^*$$

so that $\psi_\sigma(a), \psi_\sigma(b)$, and $\psi_l(c)$ are collinear precisely if $a \oplus b \oplus c = 0$. Also, up to isomorphism we can classify G by

$$G \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R} & \text{if } |Z(\sigma) \cap Z(l)| = 2 \\ \mathbb{R} & \text{if } |Z(\sigma) \cap Z(l)| = 1 \\ \mathbb{R}/\mathbb{Z} & \text{if } |Z(\sigma) \cap Z(l)| = 0 \end{cases}$$

As we will see later, the Böröczky examples are all subgroups and cosets of subgroups arising from this almost group law.

Note that only in the case where the conic $Z(\sigma)$ and the line $Z(l)$ do not intersect can G have large finite subgroups, and indeed the Böröczky examples lie on the unit circle and the line at infinity which do not meet. For example Figure 8.10 we illustrate the Böröczky example X_{12} with points labelled according to the 'almost' group law.

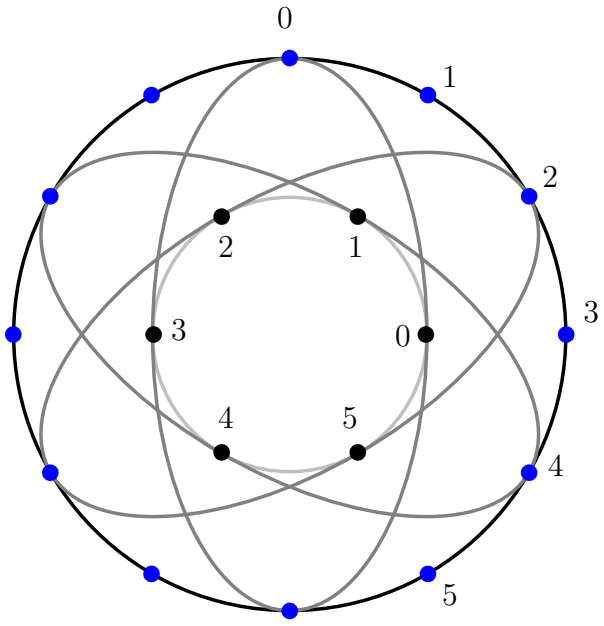


Figure 8.10: The 'almost' group law on the Böröczky example X_{12}. In this case $G \cong \mathbb{Z}/6\mathbb{Z}$ and we label the elements of X_{12} according to the bijections ψ_σ and ψ_l.

Chapter 9

Vanishing Polynomials

9.1 Melchior's Inequality

As we have seen, one of the advantages of working in projective space is that the natural duality between points and lines. In Section 8.1, we noted that this duality allowed us to translate incidence results into a dual version, replacing lines by points and points by lines. Melchior [37] noticed that looking at the dual P^* of P is a powerful tool for studying the ordinary lines of P.

Definition 9.1. Let $P \subset \mathbb{PR}^2$ be a finite point set with $|P| \geq 2$. The lines in P^* determine a (drawing of) a graph in $\mathbb{PR}^2$ by taking the vertices to be the points of intersection of lines in P^* and the edges to be the line segments joining them. We denote the (multi)graph obtained in this fashion (and, abusing notation, the drawing) by Γ_P and call it the **projective dual graph** of P.

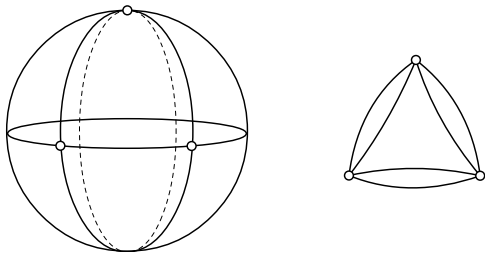


Figure 9.1: Projective Dual Graphs

For example in Figure 9.1, the point set $P = \{[0,0,1],[1,0,0],[0,1,0]\}$ has Γ_P isomorphic to the multigraph on three vertices with each pair joined by two edges (in this example the dual lines P^* are precisely the connecting lines of P.) Note that by construction the degree of each vertex is even, and for this example Γ_P is a multigraph. We remark that since when studying point sets with few ordinary lines we assume that not all points are on a line, we will always have $|P| \geq 2$. Melchior's key observation is that we can apply Euler's formula to this graph.

Definition 9.2. Let G be a graph and Σ be a surface. An embedding (i.e. a drawing) of G in Σ is a **2-cell embedding** if every face of the embedding is homeomorphic to an open disk.

For a thorough background on embedded graphs, the reader is advised to consult Mohar and Thomassen [38].

Theorem 9.3 (Euler's Formula)**.** *Let Σ be a surface. Then there exists a number χ called the* **Euler characteristic** *of Σ such that for any 2-cell embedding of a graph G in Σ,*

$$V - E + F = \chi,$$

where V, E, and F denote the number of vertices, edges and faces of the embedding, respectively.

When Σ is a plane we get the familiar result that planar graphs satisfy $V-E+F = 2$, since 2-cell embeddings into the plane are precisely planar drawings. We are concerned with the case $\Sigma = \mathbb{PR}^2$. Note that not every embedding is a 2-cell embedding; for instance the one-vertex graph with no edges has no 2-cell embedding into $\mathbb{PR}^2$, since every embedding has exactly one face ($\mathbb{PR}^2$ minus a point) which is homeomorphic to a Mobius strip. However the drawing Γ_P of the projective dual graph is always a 2-cell embedding when $|P| \geq 2$.

To compute the Euler characteristic of $\mathbb{PR}^2$, consider the one-vertex graph with one self loop. A 2-cell embedding is given by any line $l \subset \mathbb{PR}^2$ with a point $p \in l$; then the vertex in the drawing is p and the edge is $l \setminus p$. The embedding has only one face, $\mathbb{PR}^2 \setminus l$, which is indeed homeomorphic to an open disk. Thus $V-E+F = 1-1+1 = 1$, and the Euler number of $\mathbb{PR}^2$ is $\chi = 1$. Melchior applied Euler's formula to the dual graph to count the number of ordinary lines in the following way.

Theorem 9.4 (Melchior's Equality)**.** *Let $P \subset \mathbb{PR}^2$ be a finite set of points not all on a line. Let N_k denote the number of lines of P containing exactly k points and M_s denote the number of faces of Γ_P with exactly s edges. Then*

$$N_2 = 3 + \sum_{k=4}^{\infty}(k-3)N_k + \sum_{s=4}^{\infty}(s-3)M_s. \tag{9.1}$$

Proof. Applying Euler's formula to Γ_P gives $V - E + F = 1$. We can count V, E, F in the following ways:

$$V = \textstyle\sum_{k=2}^{\infty} N_k; \qquad 2E = \begin{array}{l}\sum_{k=2}^{\infty} 2kN_k \\ = \sum_{s=3}^{\infty} sM_s;\end{array} \qquad F = \textstyle\sum_{s=3}^{\infty} M_s.$$

These equalities follow since when we pass to the dual graph N_k is the number of vertices of degree $2k$, and we can count the number of edges either vertex-by-vertex (each is incident to 2 edges) or face-by-face (each is incident to 2 faces). We also use

the fact that $M_2 = 0$, which follows from the assumption that P is not all on one line. Now we can substitute

$$\begin{aligned} 0 &= 3 - 3F + 2E + E - 3V \\ &= 3 - 3\sum_{s=3}^{\infty} M_s + \sum_{s=3}^{\infty} sM_s + \sum_{k=2}^{\infty} kN_k - 3\sum_{k=2}^{\infty} N_k, \text{ and hence} \\ N_2 &= 3 + \sum_{k=4}^{\infty}(k-3)N_k + \sum_{s=4}^{\infty}(s-3)M_s. \end{aligned}$$

□

Since M_s and N_k are nonnegative, Melchior's equality implies Corollary 7.4 (which, as we have noted, shows that P determines at least *three* ordinary lines.) However, Melchior's inequality has much stronger consequences for point sets with few ordinary lines. Heuristically, if the number of ordinary lines N_2 is small, then each of the positive terms occurring on the right hand side of (9.1). That is, the dual graph Γ_P contains very few vertices of degree $2k$ for $k \geq 4$ (or indeed for $k = 2$) and contains very few faces with four or more edges. So we expect that *most faces are triangles* and *most vertices have degree 6.*

We now follow Green and Tao's argument that makes this heuristic observation precise, showing that the projective dual graph Γ_P has a triangular grid like structure.

Definition 9.5. Let $e = \{u, v\}$ be an edge of Γ_P. We say e is **good** if both u and v have degree six and the two faces adjacent to e are triangles. If e is not good we call it **bad.** We call e **k-good** if e is good and every path of length k from either u or v consists entirely of good edges. If e is not k-good we call it **k-bad**.

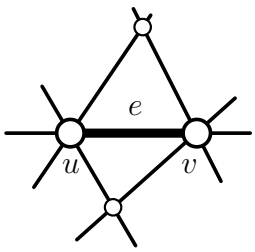


Figure 9.2: Locally, a good edge looks like part of a triangular grid.

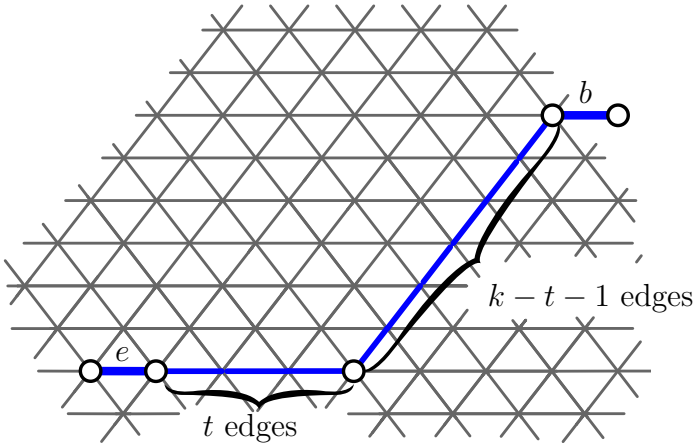


Figure 9.3: An example of a 9-good edge e, showing the existence of a path from e to a k-bad edge b which changes direction only once.

A good edge looks like a component of a triangular grid (Figure 9.2), and the k-neighborhood of a k-good edge is a triangular grid (Figure 9.3 shows a 9-good edge e

and part of it's k-neighborhood). Note that 0-good and 0-bad edges coincide with good and bad edges. By the preceding discussion we expect the number of bad edges to be very small for point sets determining few ordinary lines.

Theorem 9.6 ([25]). *Let $P \subset \mathbb{PR}^2$ be a finite set of points not all on a line which determines $\lesssim |P|$ ordinary lines. Then the number of bad edges in Γ_P is $\lesssim |P|$ and for each $k \geq 1$ the number of k-bad edges in Γ_P is $\lesssim k^2|P|$.*

Proof. If an edge $e = \{u, v\}$ is bad then either u or v has degree $2k$ for $k \neq 3$, or else one of the faces adjacent to e has four or more edges. Hence the number of bad edges is at most the number of edges adjacent to such a face or such a vertex,

$$4N_2 + \sum_{k=4}^{\infty} 2kN_k + \sum_{s=4}^{\infty} sM_s.$$

Note that $k \leq 4(k-3)$ if $k \geq 4$, so by Melchior's equality (9.1),

$$\sum_{k=4}^{\infty} 2kN_k + \sum_{s=4}^{\infty} sM_s \leq 8\sum_{k=4}^{\infty}(k-3)N_k + 4\sum_{s=4}^{\infty}(s-3)M_s \leq 8N_2.$$

So the number of bad edges is at most $12N_2 \lesssim |P|$.

To bound the number of k-bad edges, we first consider edges that are k-bad but not $(k-1)$-bad. If e is such an edge, then there is a bad edge b at distance k from e, while the $(k-1)$-neighborhood of e forms a triangular grid as in Figure 9.3. This triangular grid structure means we can find a path from e to b that changes direction only once, and has length k. Furthermore, the vertex of b in the interior of this path has degree 6, since it is adjacent to a good edge. In this way we can associate to every k-bad edge e a distinct path from a bad edge b to e with the aforementioned properties. However such a path is determined by the choice of b, the choice of direction to leave b, the number of steps in that direction, the direction to change to, and which endpoint of e to arrive at; hence the number of such paths is at most

$$(\#\text{ of bad edges}) \times 5 \times (k-1) \times 2 \lesssim k|P|.$$

Now the number of k-bad edges is the sum of the t-bad but not $(t-1)$-bad edges for $t = 0, \ldots, k$, which by the above is $\lesssim k^2|P|$. □

Thus for a fixed k, the number of k-bad edges is *linear* in the number of ordinary lines of P. If most points of P are contained in one line, the number of edges in Γ_P can be linear in $|P|$, but otherwise we expect the number of edges to be $\sim n^2$. So intuitively the previous lemma says that for fixed k *most* edges of Γ_P are k-good when $|P|$ is large enough.

9.2 Polynomials Vanishing on P

We have seen that a point set P with few ordinary lines will have large regions of triangular grid structure in its dual graph Γ_P. In this section we see how that triangular grid structure can be used to find especially low-degree vanishing polynomials.

Ultimately the reason that the triangular grid structure affords a particularly low degree vanishing polynomial is the following classical result of Chasles.

Proposition 9.7 (Chasles' Theorem)**.** *Suppose that two sets of three lines in $\mathbb{PR}^2$ define nine distinct points of intersection and suppose $p \in \mathbb{R}[X, Y, Z]$ is a homogeneous polynomial of degree at most 3. Then if eight of the intersection points are contained in $Z(p)$, so is the ninth.*

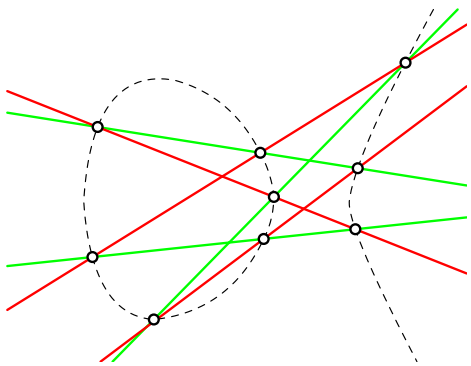


Figure 9.4: An illustration of Chasles theorem, showing two sets of three lines (light and dark) meeting at nine points, and a dashed cubic curve $Z(p)$ which necessarily contains all of these points since it contains eight of them.

We will soon see that Proposition 9.7 can find a *cubic* polynomial that vanishes on all the points whose duals have a triangular grid structure, *regardless of its size*. To make this precise, we define what is meant by a triangular grid.[1]

Definition 9.8. Let $P \subset \mathbb{PR}^2$ be a finite point set and let $I, J, K \subset \mathbb{Z}$ be finite contiguous subsets of $\mathbb{Z}$. A **triangular grid** with dimensions I, J, K in P is a collection of duals of points $(p_i^*)_{i\in I}$, $(q_j^*)_{j\in J}$, and $(r_k^*)_{k\in K}$, with all of p_i, q_j, r_k in P, satisfying:

(1) whenever $(i, j, k) \in I \times J \times K$ satisfy $i + j + k = 0$ the lines q_i^*, p_j^*, r_k^* meet at a point P_{ijk} which is incident to no other line $q_{i'}^*, p_{j'}^*, r_{k'}^*$ in the grid;

(2) the intersection points P_{ijk} arising from distinct triples are distinct;

(3) the points $(p_i)_{i\in I}$, $(q_j)_{j\in J}$, and $(r_k)_{k\in K}$ are all distinct.

An example of a triangular grid is given is Figure 9.7. Definition 9.8 sets up a convenient coordinate system on triangular grids. We will now translate Chasle's theorem into the language of triangular grids.

[1]Note that we have adopted a different definition than Green and Tao. As a result some of the forthcoming results are less general than those given in [25].

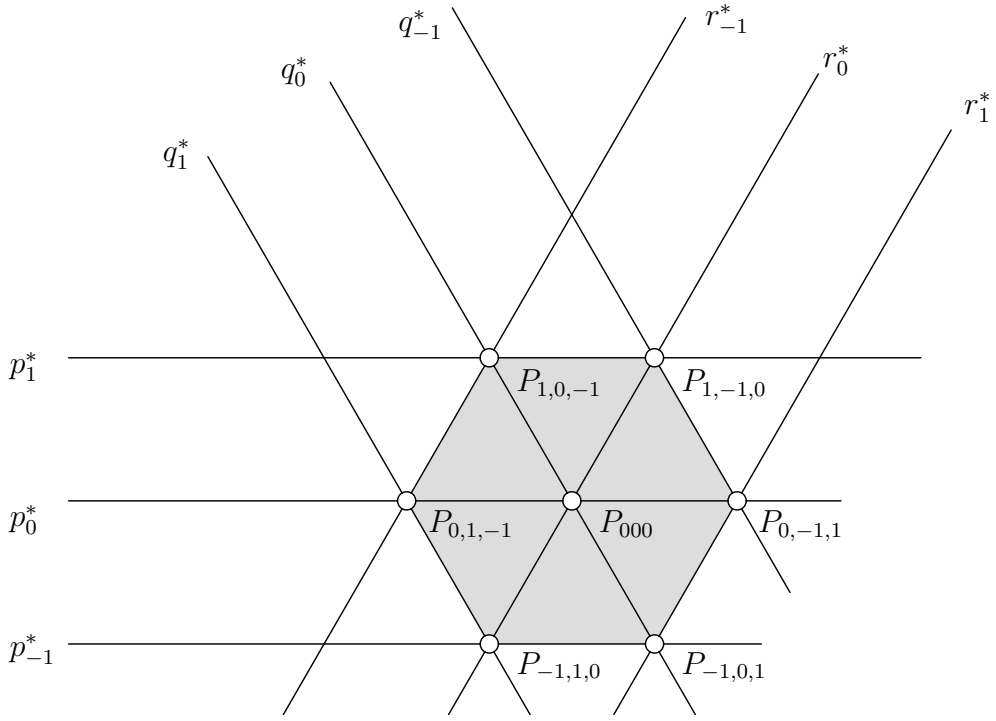


Figure 9.5: An example of a triangular grid.

Lemma 9.9 (Hexagon Completion Lemma, [25])**.** *Let $P \subset \mathbb{PR}^2$ be a finite point set. Suppose $(p^*_{-1}, p^*_0, p^*_1), (q^*_{-1}, q^*_0, q^*_1)$, and (r^*_{-1}, r^*_0, r^*_1) form a triangular grid with dimensions $I = J = K = \{-1, 0, 1\}$ in P. Then if $p \in \mathbb{R}[X, Y, Z]$ is a homogeneous polynomial of degree at most 3 and eight of the points p_i, q_j, r_k are contained in $Z(p)$, so is the ninth.*

Proof. The situation is shown in Figure 9.7. There are 9 lines p^*_i, q^*_j, r^*_k which all pass through one of the points $\{P_{0,-1,1}, P_{1,0,-1}, P_{-1,1,0}\}$ and also all pass through one of the points $\{P_{0,1,-1}, P_{-1,0,1}, P_{1,-1,0}\}$. Taking the dual, we see that the points p_i, q_i, r_k are the nine points of intersection of the two sets of lines $\{P^*_{0,-1,1}, P^*_{1,0,-1}, P^*_{-1,1,0}\}$ and $\{P^*_{0,1,-1}, P^*_{-1,0,1}, P^*_{1,-1,0}\}$. Furthermore, these points are distinct by the definition of a triangular grid, so Chasle's theorem applies to the nine points p_i, q_j, r_k, giving the statement of the lemma. □

The 'Completing a Hexagon' lemma gets its name from Figure 9.7, where a triangular grid with dimensions $I = J = K = \{-1, 0, 1\}$ consists of lines which intersect around a hexagon (the shaded area.) The hexagon completion lemma tells us that if a polynomial vanishes on eight of the duals of these lines, that polynomial will also vanish on the dual of the ninth – 'completing' the hexagon.

Having translated Chasle's theorem, we can now apply this result to show that arbitrarily large triangular grids can be covered by a single cubic polynomial. We can also check that this polynomial is not redundant in the sense that each irreducible component will itself contain many of the points.

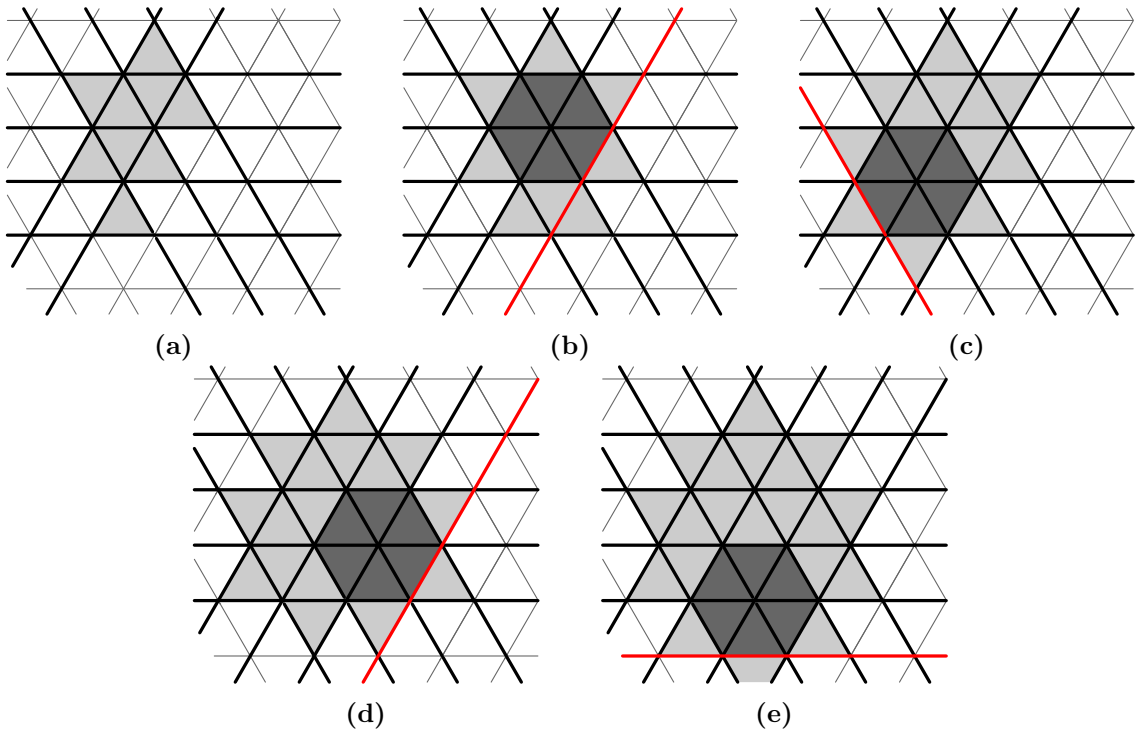


Figure 9.6: A pictorial view of the argument of Lemma 9.10. In (a) we see a section of a triangular grid, and take a polynomial p vanishing on the 10 thick lines. We shade those faces of the grid enclosed by lines whose duals are contained in $Z(p)$. In (b), applying the hexagon completion lemma to the darkened hexagon, we see that the dual of the red line is contained in $Z(p)$. Similarly in (c), (d), (e) we apply the hexagon completion lemma to different hexagons to find more lines with duals in $Z(p)$.

Lemma 9.10. *Let $k \geq 10$ and $m \geq 3k$ be parameters and suppose that $(p_i^*)_{i\in I}$, $(q_j^*)_{j\in J}$, and $(r_k^*)_{k\in K}$ form a triangular grid in P with dimensions $I = \{-2k, \ldots, 2k\}$, $J = \{-m, \ldots, 1\}$, and $K = \{1, \ldots, m\}$. Then there is a homogeneous polynomial $p \in \mathbb{R}[X, Y, Z]$ of degree at most 3 such that the points p_i, q_j, r_k are all contained in $Z(p)$ and for each irreducible factor h of p, $Z(h)$ contains at least k of these points.*

Proof. By the (proof of) Lemma 3.3, we can find a homogeneous polynomial p of degree at most 3 which vanishes on the points

$$p_{-1}, p_0, p_1, p_2, q_{-3}, q_{-2}, q_{-1}, r_1, r_2.$$

The aim is to repeatedly apply the hexagon completion lemma (Lemma 9.9) to conclude that p vanishes on the entire grid. Intuitively, we proceed as in Figure 9.6, using the hexagon completion lemma repeatedly to place the dual of every grid line inside $Z(p)$. Formally we apply the hexagon completion lemma in several steps as follows:

(i) place r_3 in $Z(p)$ by applying the hexagon completion lemma to

$$(p_0^*, p_1^*, p_2^*), (q_{-n}^*, q_{-n+1}^*, q_{-n+2}^*), (r_{n-3}^*, r_{n-2}^*, r_{n-1}^*)$$

(note that we can simply relabel the dimensions to $\{-1, 0, 1\}$ to apply the lemma)

(ii) for $n = 4, 5, \ldots, m$, place q_{-n} and r_n in $Z(p)$ by applying the hexagon completion lemma to

$$(p_0^*, p_1^*, p_2^*), (q_{-n}^*, q_{-n+1}^*, q_{-n+2}^*), (r_{n-3}^*, r_{n-2}^*, r_{n-1}^*)$$

and then to

$$(p_{-1}^*, p_0^*, p_1^*), (q_{-n}^*, q_{-n+1}^*, q_{-n+2}^*), (r_{n-2}^*, r_{n-1}^*, r_n^*)$$

(iii) for $n = 3, 4, \ldots, 2k$, place p_n in $Z(p)$ by applying the hexagon completion lemma to

$$(p_{n-2}^*, p_{n-1}^*, p_n^*), (q_{-n-2}^*, q_{-n-1}^*, q_{-n}^*), (r_1^*, r_2^*, r_3^*)$$

(note the assumption $m \geq 3k$ ensures this step is well-defined.)

(iv) for $n = 2, 3, \ldots, 2k$, place p_{-n} in $Z(p)$ by applying the hexagon completion lemma to

$$(p_{-n}^*, p_{-n+1}^*, p_{-n+2}^*), (q_{-3}^*, q_{-2}^*, q_{-1}^*), (r_n^*, r_{n+1}^*, r_{n+2}^*)$$

To investigate the number of points lying on each irreducible component, consider triples of points (p_i, q_j, r_k) with $i + j + k = 0$ whose duals lie in the grid. Observe that there are at most three triples for which the line P_{ijk}^* is contained in $Z(p)$, since the P_{ijk} are distinct (by definition of a triangular grid) and p has degree 3 so by Lemma 3.8, $Z(p)$ contains at most 3 lines. Now any *other* triple (p_i, q_j, r_k) contains at least one point in each irreducible component of $Z(p)$, since they are distinct points of intersection of the line P_{ijk}^* with $Z(p)$ and by Lemma 3.5 each irreducible component contains only as many points as its degree.

Hence we look at the $k + 3$ triples

$$(p_n, q_{1-2n}, r_{n+1})$$

for $n = 1, 2, \ldots, k + 3$. Note that $k + 3 \leq 2k$, $1 - 2(k + 3) = -2k - 5 \geq -3k \geq -m$ and $(k + 3) + 1 \leq 3k \leq m$. Thus the duals of the points in these triples are in the grid. Furthermore, the points appear in at most one triple and are distinct by the definition of a triangular grid. By the previous paragraph, except for at most 3 of these triples, each contains at least one point in each irreducible component. Hence by the distinctness of points across triples, each irreducible component contains at least k of the points p_i, q_j, r_k. □

Lemma 9.10 states the remarkable fact that the dual of an arbitrarily large triangular grid (with dimensions of the specified form) can be covered by a single cubic curve $Z(p)$. We now see how this is applicable to the triangular grid-like structure that arises from k-good edges.

Corollary 9.11. *Let $P \subset \mathbb{PR}^2$ be a finite point set which cannot be covered by $4k$ concurrent lines, and let $k \geq 1$ and $m \geq 3k$ be parameters. Suppose that $p_0^* \in P^*$ contains a segment s of m consecutive k-good edges of Γ_P, as well as at least $4k$ other edges. Denote by $P_{0,-1,1}, P_{0,-2,2}, \ldots, P_{0,-m,m}$ the ordered vertices in the segment s. Also let P_s be the set of points $q \in P \setminus \{p\}$ such that q^* is incident to one of the vertices $P_{0,-j,j}$ in s. Then there is a polynomial p of degree at most 3 such that $P_s \in Z(p)$, and each irreducible factor h of p satisfies $|Z(h) \cap P| \geq k$.*

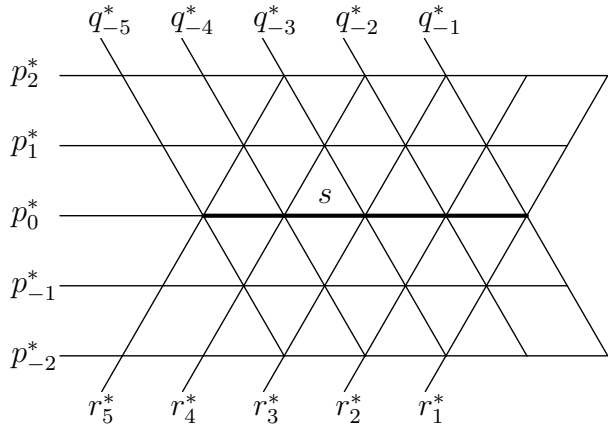


Figure 9.7: Labelling the 2-neighborhood of a segment s consisting of 4 consecutive 2-good edges ($k = 1, m = 4$)

Proof. The proof amounts to observing that the $2k$-neighborhood of the $2k$-good edges forms a triangular grid,

$$(p_{-2k}^*, \ldots, p_0^*, \ldots, p_{2k}^*), (q_{-m}^*, \ldots, q_{-1}^*), (r_1^*, \ldots, r_m^*)$$

with dimensions $\{-k, \ldots, 0, \ldots, k\}, \{-m, \ldots, -1\}, \{1, \ldots, m\}$. Formally, this can be checked by defining the p_i, q_j, r_k inductively using the definition of a good edge and the construction of the projective dual graph Γ_P. Labelling the lines of the grid as in Figure 9.7, the vertices P_{ijk} exist by construction and are incident to no other line since they have degree 6. Since P cannot be covered by $4k$ concurrent lines, and since p_0^* contains at least m extra edges outside the contiguous k-good ones, the collection of lines p_i^*, q_j^*, r_k^* are all distinct. Lastly, since these lines are distinct and each vertex has degree 6 the intersection points P_{ijk} must all be distinct also.

Having checked that this $2k$-neighborhood is indeed a triangular grid, the result follows from Lemma 9.10. □

We have already seen that in a point set P with few ordinary lines, we expect most edges to be k-good (for fixed k). Corollary 9.11 tells us that consecutive segments of k-good edges are intersected by lines p^* whose duals p all lie within a single low-degree polynomial. The next step is to look at all edges along a given line p_0^*, and apply Lemma 9.11 to clusters of k-good edges.

Lemma 9.12. *Let $k \geq 10$ be a parameter. Let $P \subset \mathbb{PR}^2$ be a finite point set, which spans at most $|P|$ ordinary lines and which cannot be covered by $4k$ concurrent lines. Then for every $q \in P$, there is a polynomial*

$$p = \prod_{i=1}^{N_q} p_i \prod_{i=1}^{M_q} l_i = p_1 p_2 \dots p_{N_q} l_1 l_2 \cdots l_{M_q}$$

and points sets $L_i \subset P$ for $i = 1, \dots, M_q$, and $P_i \subset P$ for $i = 1, \dots, N_q$ such that $P \subset Z(p)$, $L_i \subset Z(l_i)$, $P_i \subset Z(p_i)$ and

(i) $1 \leq deg(p_i) \leq 3$ *for all* $i = 1, \dots, N_q$ *and* $deg(l_i) = 1$ *(the l_i are lines);*

(ii) $q \in Z(l_i)$ *for* $i = 1, \dots, M_q$ *and* $q \in Z(p_i)$ *for* $i = 1, \dots, N_q$*;*

(iii) each irreducible factor h of p_i satisfies $|Z(h) \cap P| \geq k$;

(iv) the decomposition

$$P = \{q\} \cup L_1 \cup \cdots L_{M_q} \cup P_1 \cup \cdots \cup P_{N_q}$$

is a partition of P and the points in P_i can be partitioned into pairs (a, b) such that q, a, b are collinear and the line through these points meets no other point of P.

Furthermore, the number of factors $N_q + M_q$ can be bounded in aggregate as

$$\sum_{q \in P} (N_q + M_q) \lesssim k^3 |P|. \tag{9.2}$$

Proof. Consider the line q^*. Removing the $2k$-bad edges from this line leaves some number of segments consisting of only $2k$-good edges, which we denote $s_1, \dots, s_t$.Let $|s_i|$ denote the number of edges in the segment s_i and without loss of generality we assume $|s_1| \geq \cdots \geq |s_t|$. Also let $|q^*|$ denote the number of edges on q^*.

Construct the polynomial p according to one of the following cases:

Case 1: $|q^*| \leq 14k$**.**

Let $v_1, \dots, v_{M_q}$ be the vertices on q^*. For each $i = 1, \dots, M_q$ we let l_i be the linear polynomial with $Z(l_i) = v_i^*$, and take $p = l_1 \cdots l_{M_q}$.

Case 2: $|q^*| > 14k$**, and** $|q^*| - |s_1| \leq 4k$ **(s_1 contains all but $\leq 4k$ edges of q^*.)**

Let s_0 be the segment consisting of the first $|q^*| - 4k$ edges in s_1, and $v_1 \dots, v_{M_q}$ be the remaining vertices in q^* but not in s_0. As in Case 1, choose l_i with $Z(l_i) = v_i^*$. Apply Corollary 9.11 to the segment s_0 to construct a polynomial p_1 of degree at most 3 vanishing on P_{s_0}. Let $N_q = 1$ and $p = l_1 \cdots l_{M_q} p_1$, and define $P_1 = P_{s_0}$.

Case 3: $|q^*| > 14k$**, and** $|s_1| < |q^*| - 4k$ **(every segment contains** $< |q^*| - 4k$ **edges.)**

Let $s'_1, \ldots, s'_{N_q}$ be those segments of the s_i containing at least $10k$ edges, and let $v_1 \ldots, v_{M_q}$ be the remaining vertices in q^* not contained in any of the s'_i. As before we choose l_i with $Z(l_i) = v_i^*$, and apply Corollary 9.11 to each segment s'_i to construct a polynomial p_i of degree at most 3 vanishing on $P_{s'_i}$. This gives the polynomial $p = l_1 \cdots l_{M_q} p_1 \cdots p_{N_q}$, and we define $P_i = P_{s'_i}$.

It remains to define the sets L_i, which we do by letting in each case L_i be the set of $q \in P$ such that q^* is incident to v_i. We now check the statements *(i)–(iv)*.

(i) By construction each l_i is linear and each p_i is nonzero of degree at most 3.

(ii) Since q^* is incident to v_i, $q \in Z(l_i)$ for $i = 1, \ldots, M_q$. By construction of the p_i from Corollary 9.11, $q \in Z(p_i)$ for each $i = 1, \ldots, N_q$.

(iii) Since each p was constructed by applying Corollary 9.11, each irreducible factor h of p_i satisfies $|Z(h) \cap P| \geq k$.

(iv) If $q_0 \in P$ with $q_0 \neq q$ then q_0^* meets q^* in precisely one point. If this point is some v_i then $p \in L_i$, and if this point is in a segment s then $p \in P_s = P_j$ for some $j = 1, \ldots, N_q$. Since the segments and vertices v_i are in each case disjoint and exhaust the points on q^*, their union is a partition.

To see that points can be paired up, to each point $a \in P_i$ we can associate the point $b \in P_i$ where q^*, a^*, b^* meet (it exists since a^* meets q^* at an endpoint of a good edge, where three lines meet.) In this way the set can be partitioned into pairs and moreover since the vertex where q^*, a^*, b^* meet has degree exactly six, no other line c^* is incident to this point, so no other point is on the line through q, a, b.

Lastly, we wish to bound the sizes $N_q + M_q$ of the polynomials. Let B_q denote the number of $2k$-bad edges on q^*. Hence by Lemma 9.6, $\sum_{q \in P} B_q \lesssim k^2 |P|$. Then

$$M_q \leq \max\{14k, 4k, (10k+1)B_q\} \lesssim kB_q \quad \text{and} \quad N_q \leq B_q.$$

Therefore $N_q + M_q \lesssim kB_q$, and hence by Theorem 9.6,

$$\sum_{q \in P} (N_q + M_q) \lesssim k^3 |P| \qquad \square$$

To understand the previous result, note that a simple application is the following, which is proved separately in Green and Tao as [25, Proposition 5.1] and does not use most of the special structure of the constructed polynomial.

Corollary 9.13. *Let $P \subset \mathbb{PR}^2$ be a finite point set, which spans at most $|P|$ ordinary lines. Then there is a polynomial p of bounded degree, each irreducible factor of which has degree at most 3, such that $P \subset Z(p)$.*

Proof. Let $k = 10$ (we could just as well take any other fixed $k \geq 10$). If P can be covered by $4k$ concurrent lines then we simply take p such that $Z(p)$ is the union of these lines. Otherwise, we obtain the polynomial p by applying Lemma 9.12 for the $q \in P$ which minimises $N_q + M_q$, which must satisfy

$$N_q + M_q \leq \frac{1}{|P|} \sum_{q \in P} (N_q + M_q) \lesssim k^3.$$

Since k^3 is constant and the degree of p is at most $3(N_q + M_q)$, the corollary holds. □

We take a moment to remark on the strength of this result: an *arbitrarily large* point set can be placed inside the zero set of a *constant degree* polynomial, provided that the point set spans few ordinary lines!

9.3 Reducing to a single cubic

Lemma 9.12 shows that we can place P inside a polynomial of low degree with only linear, quadratic and cubic factors. The next step will be to show that in fact, all but one of those factors is linear.

Theorem 9.14. *Let $P \subset \mathbb{PR}^2$ be a finite point set which spans at most $|P|$ ordinary lines. Then there is a polynomial p and a partition $P = P' \cup P''$ such that $P' \subset Z(p)$ and either*

(1) $p = l_1 \cdots l_N$ where the l_i are linear, $N \lesssim 1$ and $|P''| \lesssim 1$;

(2) p is irreducible of degree 3, and $|P''| \lesssim 1$;

(3) p is irreducible of degree 2, $P' = Z(y_1) \cap P$, $P'' = Z(l_1 \cdots l_N) \cap P$ where $N \lesssim 1$ and the l_i are linear, $||P'| - |P''|| \lesssim 1$ and P'' spans $\lesssim |P|$ ordinary lines.

Proof. We split into cases:

Case 1: P **can be covered by** $\lesssim 1$ **concurrent lines.**

In this case we simply take the l_i to be the defining polynomials of these lines, and *(1)* holds.

If we are not in Case 1, then apply Lemma 9.13 to find a polynomial $y = y_1 \cdots y_m$ such that

$$P \subset Z(y) = Z(y_1) \cup \ldots \cup Z(y_m)$$

where $m \lesssim 1$ and each y_i is irreducible of degree at most 3.

Case 2: P ***cannot*** **be covered by** $\lesssim 1$ **concurrent lines, and there is no** y_i **of degree 2 or 3 satisfying** $|Z(y_i) \cap P| \gtrsim 1$**.**

In this case *(1)* holds if we take the l_i to be those factors y_j of degree one, so that $N \leq m \lesssim 1$. Since each non-linear factor contains $\lesssim 1$ points of P, there are $\lesssim 1$ points of P not lying on one of the lines $Z(l_i)$.

If we are not in Case 2 then there is some factor, without loss of generality y_1, which has degree 2 or 3 and satisfies

$$|Z(y_1) \cap P| \gtrsim 1. \tag{9.3}$$

We denote by P_0 those points of $P \cap Z(y_1)$ which are not contained in $Z(y_i)$ for any $i \neq 1$. By Bezout's Theorem (we state Theorem 4.3 in the plane, but it extends to the projective plane) each y_i, $i \neq 1$, satisfies $|Z(y_1) \cap Z(y_i)| \leq 9$. Hence

$$|P_0| \geq |P| - 9m \geq |P|/2. \tag{9.4}$$

Since we are not in Case 1, P cannot be covered by $\lesssim 1$ concurrent lines, so for any $q \in P$ we can apply Lemma 9.12 with $k = 10m$ to obtain a polynomial

$$p = l_1 \dots l_M p_1 \dots p_N$$

with $P \subset Z(p)$ and satisfying Lemma 9.12*(i)–(iv)*. By the pigeonhole principle, we can choose a point $q \in P'$ such that c_q is at most the average value for $q \in P'$. By (9.2) we thus fix q so that

$$N_q + M_q \leq \frac{1}{|P_0|} \sum_{r \in P'} (N_r + M_r) \leq \frac{1}{|P_0|} \sum_{r \in P} (N_r + M_r) \lesssim \frac{1}{|P_0|} |P|. \tag{9.5}$$

Recall that from Lemma 9.12*(ii)*, each irreducible component h of p_i satisfies $|Z(h) \cap P| \geq 10m$. If p_i does not have y_j as an irreducible component, then $|Z(h) \cap Z(y_j)| \leq 9$ by Bezout's Theorem, so

$$|Z(h) \cap P| \leq |Z(h) \cap Z(y)| \leq 9m.$$

Hence the irreducible components of p_i are each equal to y_j for some $j = 1, \dots, m$. By Lemma 9.12*(i)*, $q \in Z(p_i)$. However $q \in P_0$ so $q \in Z(y_1)$ and q is not contained in any other $Z(y_i)$. Hence every p_i contains y_1 as a factor. We now split into cases depending on the degree of y_1.

Case 3: P ***cannot*** **be covered by $\lesssim 1$ concurrent lines, and y_1 has degree 3.**

Every p_i contains y_1 as a factor, so since the p_i are distinct we must have $N_q = 1$ and $p_1 = y_1$. Let $P' = P \cap Z(p_1)$ and $P'' = P \setminus P'$. Since $q \in Z(l_i)$ for each i, l_i is not identical to any y_i, so

$$|L_i| \leq |Z(l_i) \cap P| \leq |Z(l_i) \cap Z(y)| \leq 3m$$

by Bezout's theorem. Hence $|P''| \leq \sum_{i=1}^{M_q} |L_i| \leq 3mM_q \lesssim \frac{|P|}{|P_0|} \lesssim 1$ and so statement *(2)* holds.

Case 4: P ***cannot*** **be covered by $\lesssim 1$ concurrent lines, and y_1 has degree 2.**

Every p_i contains y_1 as a factor. To see that no p_i can be of degree 2, recall from Lemma 9.12*(iv)* that there is a pair of points $a, b \in Z(p_i) \setminus \{q\}$ such that

$q, a, b \in Z(p_i)$ are collinear, which cannot happen if p_i has degree 2. Hence, for $i = 1, \ldots, N$, $p_i = y_1 v_i$ where v_i is linear and $v_i = y_j$ for some $j = 1, \ldots, m$.

Recall that Lemma 9.12*(iv)* partitions P_i into pairs, and observe that one member of each pair must lie on $Z(y_1)$ and one on $Z(v_i)$ (since any line through $Z(p)$ meeting three points must intersect $Z(y_1)$ twice and $Z(v_i)$ once.) Define

$$P' = P \cap Z(y_1) \quad \text{and} \quad P'' = P \cap Z(l_1 \cdots l_M v_1 \cdots v_N).$$

Then $|P'| + |P''| = |P|$ and $|P''|, |P'| \geq \sum_{i=1}^{M} |P_i|/2$. By Bezout's theorem as in Case 3, $|L_i| \leq 3m$ and hence $\sum_{i=1}^{M} |P_i| \geq |P| - C$ where $C \lesssim 1$. Thus $||P'| - |P''|| \lesssim 1$.

It remains to check how many ordinary lines are determined by P''. An ordinary line in this set is either:

(a) ordinary in P;

(b) contains a point of $P' \setminus P_0$ and exactly two points of P''; or

(c) contains a point of P_0 and exactly two points of P''.

There are at most $|P|$ ordinary lines of the type (a) by assumption. There are at most $|P''||P' \setminus P_0| \leq 9m|P''| \lesssim |P|$ of type (b) since $|P' \setminus P_0| \leq 9m$ (by (9.4)). Lastly consider an ordinary line of the type (c), passing through a point $a \in P'$. Applying Lemma 9.12 as we have already done, we get another polynomial $p = p'_1 \cdots p'_{N_a} l'_1 \cdots l'_{M_a}$ and partition L'_i, M'_i. As we have already seen, $p'_i = y_1 v_i$ for a linear factor $v_i = y_j$. By Lemma 9.12*(iv)*, any line through a and a point of P_i is incident to exactly one point of P'', so such a line cannot be ordinary in P''. Hence an ordinary of type (c) which passes through a must be one of the $Z(l'_i)$, and so there are at most M_a such lines. Summing over all $a \in P_0$, therefore by (9.2) there are $\lesssim |P| + \sum_{a \in P_0} M_a \lesssim |P|$ ordinary lines for P''.

Therefore statement *(2)* holds.

In each case one of the statements *(1)–(3)* holds, so we are done. □

Theorem 9.14 already classifies point sets with few ordinary lines to an extent, and it has been obtained using only polynomial and combinatorial methods. In Chapter 10 we give Green and Tao's introduction of ideas from arithmetic combinatorics to considerably simplify this classification.

Chapter 10

The Green-Tao proof

We have already seen in Section 6.3 how results in combinatorial geometry can be used to prove results in arithmetic combinatorics, by considering special point sets. In this chapter, we show that the inverse dynamic can hold: arithmetic combinatorics can prove results in combinatorial geometry. This will finally resolve Theorem 7.6 by giving a simple classification of point sets spanning at most $|P|$ ordinary lines.

10.1 Background Material

To begin, we present without proof the relevant results from arithmetic combinatorics. Some of the proofs can be found in [25, Appendix A], though as before the book [57] is an excellent reference.

We have already seen the Böröczky and Sylvester examples which lie on degree 3 algebraic curves, and we have seen that the relationship of collinearity gives rise to a group (or 'almost' group) structure on points of these curves. The following lemma relates point sets with few ordinary lines with the group structure.

Lemma 10.1 ([25, Proposition A.4])**.** *Let $(G,+)$ be an abelian group and A, B subsets of G, with $||A| - |B|| \lesssim 1$. If there are $\lesssim |A|$ pairs $(a,a') \in A^2$ for which $a + a' \notin B$, then there is a subgroup H of G and a coset $x + H$ such that*

$$|A \triangle (H + x)|, |B \triangle (H + 2x)| \lesssim 1.$$

Roughly speaking, Lemma 10.1 says that unless A is a coset of a subgroup of G, the sum $A + A$ in G will be larger than A. The reader should contrast this with Freiman's theorem, which similarly says there is additive structure in $A \subset \mathbb{Z}$ whenever $A + A$ is small.

We do not give the proof of the following result of Green and Tao, which rules out examples of point sets with few ordinary lines that lie on a small constant number of lines.

Lemma 10.2 ([25, Proposition 6.1])**.** *Let $P \subset \mathbb{PR}^2$ be a finite point set which spans $\lesssim |P|$ ordinary lines, and suppose that P is contained in the union of $\lesssim 1$ lines. Then if $|P| \gtrsim 1$, all except $\lesssim 1$ of the points of P lie on a single line.*

This result considerably simplifies the conclusion of Theorem 9.14, reducing in each case to just one line.

Theorem 10.3. *Let $P \subset \mathbb{PR}^2$ be a finite point set which spans at most $|P|$ ordinary lines, and suppose $|P| \gtrsim 1$. Then there is a subset $P_0 \subset P$ with $|P \setminus P_0| \lesssim 1$ and a homogeneous polynomial $p \in \mathbb{R}[x, y, z]$, satisfying $P_0 \subset Z(p)$, of one of the following forms:*

(1) p is irreducible of degree 1;

(2) p is irreducible of degree 3;

(3) $p = \sigma l$ where σ, l are irreducible and have degrees 2 and 1 respectively, and

$$||Z(\sigma) \cap P_0| - |Z(l) \cap P_0|| \lesssim 1.$$

That is, P' lies on either a line, an irreducible cubic curve, or on the union of an irreducible conic curve and a line.

Proof. We apply Theorem 9.14 to P. In cases *(1)* and *(3)*, we apply Lemma 10.2 to the points lying on $Z(l_1 \cdots l_N)$ to conclude all but $\lesssim 1$ of these points lie on a single line l. In case *(3)*, we then define $P_0 = Z(p) \cap P$ and can check that $Z(\sigma) \cap P_0 = P'$ and $||Z(l) \cap P_0| - |P''|| \lesssim 1$, so the result holds. □

Theorem 10.3 classifies point sets spanning few ordinary lines to a sufficient extent to solve the Dirac-Motzkin conjecture for large $|P|$. In the next section we give the resolution of the problem by applying Theorem 10.3.

10.2 The Green–Tao proof

The results of Section 10.1 together show that the Böröczky examples are the point sets determining fewest ordinary lines.

Theorem 10.4 ([25, Theorem 2.4])**.** *Let $P \subset \mathbb{PR}^2$ be a finite non-collinear point set which spans at most $|P| - C$ ordinary lines, where C is an absolute constant. Then P is projectively equivalent to one of the Böröczky examples (c.f. Proposition 8.10.)*

Proof. Since P spans at most $|P|$ ordinary lines, by Theorem 10.3 there is a subset $P' \subset P$ with $|P \setminus P'| \lesssim 1$ and a polynomial p with $P' \subset Z(p)$ and satisfying one of *(i)–(iii)*.

We redefine $P' = P' \cap Z(p)^*$, which removes at most two singular points from P'. Observe that the set P' itself spans $\lesssim |P|$ ordinary lines, since P spans at most

$|P|$, and the number of connecting lines of P' containing a point of $P \setminus P'$ is at most $|P||P \setminus P'| \lesssim |P|$.

We will now examine each possibility in Theorem 10.3.

Case (1). If p is irreducible of degree 1, then since the points are non-collinear we can choose $a \in P \setminus P'$. At most $\lesssim 1$ of the lines joining a to a point of P' are not ordinary, since such lines must contain another point of $P \setminus P'$. Hence P determines at least $|P| - C_1$ ordinary lines for some absolute constant $C_1 \lesssim 1$.

Case (2). If p is irreducible of degree 3, consider the group $Z(p)^*$. A pair of points $a, b \in P'$ determines an ordinary line of P' if and only if the point $\ominus a \ominus b$ is not in P'. Hence for all but $\lesssim |P|$ pairs $a, b \in P'$, $\ominus a \ominus b \in P'$ or equivalently $a \oplus b \in \ominus P'$.

Hence, applying Lemma 10.1 with $A = P', B = \ominus P'$, there is a subgroup E of $Z(p)^*$ and a coset $E \oplus x$ such that

$$|P' \triangle (E \oplus x)|, |\ominus P' \triangle (E \oplus 2x)| \lesssim 1.$$

So, P' is almost entirely a coset of a subgroup of $Z(p)^*$. Additionally, since $|\ominus P' \triangle (E \oplus 2x)| = |P' \triangle (E \ominus 2x)|$, we have $|(E \oplus 2x) \triangle (E \oplus x)| \lesssim 1$. However distinct cosets do not overlap, so if $|P|$ is large enough (this is ensured by taking the absolute constant C large enough) this implies $3x \in E$.

This shows that $E \oplus x$ is a Sylvester example, and $P'' = P \cap (E \oplus x)$ is almost all of P, since

$$|P \setminus P''| = |P \setminus (E \oplus x)| \leq |P \setminus P'| + |P' \triangle (E \oplus x)| \lesssim 1.$$

Now we wish to compute the number of ordinary lines spanned by P. Recall from Proposition 8.13 that $E \oplus x$ spans at least $|E| - 3$ ordinary lines, and each point of $E \oplus x$ lies on at most two ordinary lines. Hence after removing the points $(E \oplus x) \setminus P''$ from $E \oplus x$, at least $|E| - C_2'$ ordinary lines remain, where $C_2' \lesssim 1$. In addition, a point not lying in $Z(p)$ lies on at most 3 tangent lines to $Z(p)$, so after adding the points of $P \setminus P''$ at least $|E| - C_2$ ordinary lines remain, where $C_2 \lesssim 1$. Hence by taking C large enough, P spans at least $|P| - C$ ordinary lines in this case.

Case (3). If $p = \sigma l$ where σ, l are irreducible and have degrees 2 and 1 respectively, then consider the group G from Proposition 8.14 which imbues $Z(p)^*$ with an almost group structure. Write $P_\sigma = P' \cap Z(\sigma)^*$ and $P_l = P' \cap Z(l)^*$. Recalling the maps from G into $Z(\sigma)^*$ and $Z(l)^*$, we consider the preimages

$$\Sigma = \psi_\sigma^{-1}(P_\sigma) \quad \text{and} \quad L = \psi_l^{-1}(P_l).$$

As in Case (i), for all but $\lesssim |\Sigma|$ pairs $a, b \in \Sigma$, $a \oplus b \in \ominus L$. Furthermore $||\Sigma| - |L|| \lesssim 1$ by Theorem 10.3*(ii)*, since $|\Sigma| = |P_\sigma|$ and $|L| = |P_l|$.

Hence as before we can apply Lemma 10.1 with $A = P_\sigma, B = \ominus L$, to find a subgroup H of G and a coset $H \oplus x$ such that

$$|\Sigma \triangle (H \oplus x)|, |L \triangle (H \ominus 2x)| \lesssim 1.$$

For $|P|$ large enough we must have $|Z(\sigma) \cap Z(l)| = 0$, since otherwise $G \cong \mathbb{R}$ or $G \cong \mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$ and so G has no finite subgroups with more than two elements. Hence $G \cong \mathbb{R}/\mathbb{Z}$, and $H = \{i/m \mid i = \{0, 1, \ldots, m-1\}\}$.

We do not give the details (see [25, Proposition 7.3, Lemma 7.4, Proposition 8.2]) but with the explicit form of the bijections ψ_σ, ψ_l one can check that $\psi_\sigma(H \oplus x) \cup \psi_l(H \ominus 2x)$ is projectively equivalent to the set X_{2m}, and additionally that any set P with $|P \triangle X_{2m}| \lesssim 1$ and spanning at most $|P| - C_3$ ordinary lines is a Böröczky example, where $C_3 \lesssim 1$ is an absolute constant. Ensuring C is large enough, we conclude that P is a Böröczky example.

We see that for large enough C, only in case **(3)** can P span at most $|P| - C$ ordinary lines, and in this case P must be a Böröczky example. □

Theorem 10.4 is a strong classification of point sets determining few ordinary lines. From this, Green and Tao's bound for the Dirac-Motzkin conjecture for large $|P|$ follows.

Theorem 7.6 ([25, Theorem 2.2])**.** *Let $P \subset \mathbb{PR}^2$ be a finite non-collinear point set, with $|P| \gtrsim 1$, then*

$$c_P(2) \geq \begin{cases} \frac{1}{2}|P| & \text{if } |P| \equiv 0, 2 \ (mod\ 4) \\ \frac{3}{4}(|P| - 1) & \text{if } |P| \equiv 1 \ (mod\ 4) \\ \frac{3}{4}(|P| - 3) & \text{if } |P| \equiv 3 \ (mod\ 4) \end{cases}.$$

Proof. Applying Theorem 10.4, P is projectively equivalent to a Böröczky example. Since the number of ordinary lines is preserved under such transformations, the bounds on $c_P(2)$ hold by Proposition 8.10. □

Theorem 7.6 solves Dirac and Motzkin's Conjecture 7.5 for large $|P|$. The method of its proof, and in particular the use of additive combinatorics, suggest that this method can not be extended to cover the small $|P|$ case. We note that the implicit constant in Theorem 7.6 can be computed, and is sufficiently large that checking the remaining examples is impractical.

Chapter 11

Isosceles Triangles

Recall that Erdős' distinct distances problem asks for a lower bound on the number $d(P)$ of distinct distances determined by the finite point set P. A closely related problem is to bound the number of distances $d_a(P) = |\{||a-b|| \mid b \in P\}|$ around a single point $a \in P$. Denote

$$d^p(P) = \max_{p \in P}(d_p(P)).$$

Finding a tight lower bound for $d^p(P)$ is another open problem. The current best known bound is $d^p(P) \gtrsim |P|^{0.8641\ldots}$ due to Katz and Tardos [32]. In fact, until the result of Guth and Katz, every known lower bound for $d(P)$ proceeded by bounding $d^p(P)$ and using the trivial observation that $d^p(P) \leq d(P)$.

One can think of these distance problems as concerning properties of two-point subsets of P. From this point of view, it is natural to study properties of n-point subsets of P. A 3-point subset of P determines a triangle, and a natural subject to study has been the number of *isosceles* triangles,

$$i(P) = \{(a,b,c) \mid a,b,c \in P, |a-b| = |b-c| \neq 0\}.$$

Note that degenerate isosceles triangles are included in the count, and each isosceles triangle is counted more than once. A random point set will almost certainly contain no isosceles triangles, whereas a point set P consisting of a regular n-gon and its centre will determine $\gtrsim |P|^2$ isosceles triangles.

Intuitively, the number of isosceles triangles and the number of distinct distances should be related, because isosceles triangles arise from repeated distances from a single point. We can make this intuition precise.

Proposition 11.1. *Let $P \subset \mathbb{R}^2$ be a finite planar point set, then*

$$|i(P)|d^p(P) \gtrsim |P|^3.$$

Proof. Consider a single point $a \in P$. Partition $P = P_1 \cup \cdots \cup P_{d_a(P)}$ such that all the points in P_i are at the same distance from a. Then

$$i_a(P) = |\{(a,b,c) \mid b,c \in P, ||a-b|| = ||b-c||\}| = \sum_{i=1}^{d_a(P)} \binom{|P_i|}{2}. \tag{11.1}$$

Since $|P| = \sum_{i=1}^{d_a(P)} |P_i|$ is fixed, the sum (11.1) is minimised when $|P_i| = |P|/d_a(P)$, so $i_a(P) \geq |P|^2/d_a(P)$. Finally,

$$|i(P)| = \sum_{a \in P} i_a(P) \geq \sum_{a \in P} |P|^2/d_a(P) \geq |P|^3/d^p(P). \qquad \square$$

Proposition 11.1 suggests that one way to attack the distinct distances problem is by finding an upper bound on the number of isosceles triangles. The following proposition shows that this approach cannot improve on the Guth-Katz result (Theorem 1.5). The following computation first appears in Erdős and Purdy [20].

Proposition 11.2 ([20])**.** *Let $P = \{-2n, \ldots, 2n\}^2$ be a $(4n+1) \times (4n+1)$ grid in the plane. Then $|i(P)| \gtrsim |P|^2 \log |P|$.*

Proof. First consider the grid $P_0 = \{-n, \ldots, n\}^2$. Denote $i_0(P_0) = \{(0, a, b) \in i(P_0)\}$. Let $(0, a, b) \in i_0(P_0)$ be an isosceles triangle and let $a = (a_x, a_y)$ and $b = (b_x, b_y)$. Then $a_x^2 + a_y^2 = b_x^2 + b_y^2$ and $a_x^2 + a_y^2 \leq 2n^2$. Denote by $r_2(k)$ the number of pairs $(x, y) \in \mathbb{Z}^2$ satisfying $x^2 + y^2 = k$. Each pair (x, y) satisfying $x^2 + y^2 \leq n^2$ lies in P_0, so $|i_0(P_0)| \geq \sum_{k=0}^{n^2} r_2(k)^2$. Sums of this form have been well studied [28, 44, 4], and can be bounded as follows

$$|i_0(P_0)| \geq \sum_{k=0}^{n^2} r_2(k)^2 \gtrsim n^2 \log n. \tag{11.2}$$

Now consider the grid P. Note that $P_0 \subset P$ and that for each $a \in P_0$, $a + P_0 \subset P$. Since $a + P_0$ is a translate of P_0, by (11.2) there are $\gtrsim n^2 \log n$ isosceles triangles $(a, a+b, a+c) \in i(P)$ with b, c in P_0. Therefore

$$|i(P)| \geq |P_0| n^2 \log n \gtrsim |P|^2 \log |P|. \qquad \square$$

By Proposition 11.2, one cannot hope to find a better upper bound than $|i(P)| \lesssim |P|^2 \log |P|$ for general point sets. It is conjectured that this upper bound holds.

Conjecture 11.3. *If P is a finite point set in the plane, then $|i(P)| \lesssim |P|^2 \log |P|$.*

In the next section, we give a proof of a weaker bound than Conjecture 11.3 by the polynomial method.

11.1 An upper bound by the polynomial method

We begin by transforming the isosceles triangle problem to an incidence problem in the manner of Chapter 2. Recall that G is the group of orientation-preserving rigid motions of the plane (the translations and rotations). We first define all of our terms; the reader may wish to refer to Chapter 2 to see the correspondence with Elekes' reduction.

Definition 11.4. Define a map $F : i(P) \to G$ by letting $F(a, b, c)$ be the unique rotation g around a satisfying $gb = c$. Define

$$H_{=k}(P) = \{g \in G \mid g \text{ is a rotation about a point } a \in P \text{ and } |gP \cap P| = k\}$$

and $H_{\geq k} = \cup_{j=k}^{\infty} H_{=j}(P)$. Recall that we decomposed $G = G^{rot} \cup G^{trans}$ into rotations and translations. Let $H_{\geq k}^{trans}(P) = H_{\geq k}(P) \cap G^{trans}$ and $H_{\geq k}^{rot}(P) = H_{\geq k}(P) \cap G^{rot}$.

By analogy with Lemma 2.3, we get the following.

Lemma 11.5. *If $g \in H_{=k}(P)$ then $|F^{-1}(g)| = k - 1$.*

Proof. Let $gP \cap P = \{a, p_1, \ldots, p_{k-1}\}$. Then $p_i = gq_i$ for some $q_i \in P$, and hence $(a, q_i, p_i) \in F^{-1}(g)$. Conversely, if $(a, b, c) \in F^{-1}(g)$ then $gb = c$ so $c \in gP \cap P$. Hence $c = p_i$ for some i. □

If $g \in G$ is not a rotation about a point $a \in P$ then $F^{-1}(g) = \emptyset$, so

$$|i(P)| = \sum_{k=2}^{|P|} (k-1)|H_{=k}(P)| = \sum_{k=2}^{|P|} |H_{\geq k}(P)|. \tag{11.3}$$

To interpret bounding $|H_{\geq k}(P)|$ as an incidence problem, we get the following analogue of Lemma 2.4. Recall the definition $S_{p,q} = \{g \in G \mid gp = q\}$.

Lemma 11.6. *Suppose $2 \leq k \leq |P|$ and let $L = \{S_{p,q} \mid p, q \in P \text{ and } p \neq q\}$ and $R = \{S_{a,a} \mid a \in P\}$. Then $|H_{\geq k}(P)|$ is the number of elements $g \in G$ contained in a set $L_0 \in R$ and contained in at least $k - 1$ distinct sets $L_1, \ldots, L_{k-1} \in L$.*

As in Lemma 2.9, there cannot be too many such points that are translations.

Lemma 11.7. $|H_{\geq k}^{trans}(P)| \lesssim |P|^2/k$

We omit the proofs of Lemmas 11.7 and 11.6, as they are almost the same as the proofs of the quotes similar results. Recall the parameterisation $\rho : G^{rot} \to \mathbb{R}^3$ introduced by Guth and Katz in (2.4). From Lemma 2.10, the sets $L_{p,q} = \rho(S_{p,q} \cap G^{rot})$ are lines in $\mathbb{R}^3$. By Lemma 11.6, $|H_{\geq k}^{rot}(P)|$ is precisely the number of incidences between at least $k - 1$ lines $L_{p,q}$ with $p \neq q$ and a line $L_{a,a}$, where all of p, q, a are in P. This reduces the isosceles triangle problem to an incidence problem about lines in $\mathbb{R}^3$, as follows:

Definition 11.8. Define $L = \{L_{p,q} \mid p, q \in P \text{ and } p \neq q\}$ and $R = \{L_{a,a} \mid a \in P\}$.

As in Section 2.2, the sets of lines L and R have important properties.

Proposition 11.9.

(1) $|L| = |P|^2 - |P|$ and $|R| = |P|$;

(2) at most $|P|$ lines of $L \cup R$ lie in any given plane and $\lesssim |P|$ lines of $L \cup R$ lie in any given regulus;

(3) the lines of R all have the same direction, and the lines $L_{a,a}, L_{b,b}, L_{c,c} \in R$ lie in a plane if and only if $a, b, c \in P$ are collinear.

Proof. Property *(1)* follows from Proposition 2.11, and property *(2)* follows from Corollary 2.14 and Lemma 2.19. Property *(4)* follows by noting from (2.4) that if $a = (a_x, a_y) \in P$ then $L_{a,a} = \{(a_x, a_y, t) \mid t \in \mathbb{R})\}$. □

We conjecture that these properties are sufficient to imply Conjecture 11.3.

Conjecture 11.10. *Let L and R be arbitrary sets of lines in $\mathbb{R}^3$ satisfying the properties in Proposition 11.9. Let $I^R_{\geq k}(L)$ be the number of points on lines of R that are incident to at least $k-1$ lines in L. Then $I^R_{\geq k}(L) \lesssim |P|^2/k$.*

To see that this is enough to solve Conjecture 11.3, note that if Conjecture 11.10 holds then by Lemma 11.6, $|H^{rot}_{\geq k}(P)| \lesssim |P|^2/k$. Combining this with Lemma 11.7, $|H_{\geq k}(P)| \lesssim |P|^2/k$. Hence by (11.3),

$$i(P) = \sum_{k=2}^{|P|} |H_{\geq k}(P)| \lesssim \sum_{k=2}^{|P|} |P|^2/k \lesssim |P|^2 \log |P|.$$

The best result we have towards Conjecture 11.3 is the following, where we place certain regularity assumptions on the distribution of incidences on lines as in Theorem 6.1.

Theorem 11.11. *Let L and R be sets of lines in $\mathbb{R}^3$ satisfying the properties in Proposition 11.9. Additionally, suppose that each line of $L \cup R$ contains $\gtrsim |P|^{1/2}$ points of $I^R_{\geq k}(L)$. If $k \geq 3$, then $I^R_{\geq k}(L) \lesssim |P|^{5/2}$.*

Proof. For the sake of contradiction, suppose $I^R_{\geq k}(L) \gtrsim |P|^{5/2}$. By Lemma 4.16, there is a polynomial p of degree $d \lesssim |P|^{1/2}$ such that every line in R is contained in $Z(p)$. Each line of L contains $\gtrsim |P|^{1/2}$ points of $I^R_{\geq k}(L)$, and these points are contained in $Z(p)$. Hence by Lemma 3.5, every line of L is contained in $Z(p)$. However, by Lemma 4.15, $|L| \leq 4d^2 + Bd \lesssim 4|P| + |P||P|^{1/2}$, contradicting that $|L| \gtrsim |P|^2$. □

We also mention that it is an interesting question to determine the bound when the sizes of L and R are not fixed by Proposition 11.9*(1)*, but we have no convincing conjecture of what the tight bound is in this case.

11.2 Perpendicular bisectors

In Chapter 7 we discussed the ordinary line conjecture of Dirac and Motzkin, concerning how points can be distributed on connecting lines of P. In this chapter we introduce a new related problem which relates to the study of isosceles triangles in point sets, and give a conjecture.

Definition 11.12. Let P be a set of points in the plane. The **perpendicular bisector** for distinct $p, q \in P$ is the line perpendicular to the connecting line through p and q which passes through the midpoint of p and q. A line l is an **ordinary perpendicular bisector** for P if l is a perpendicular bisector for some $p, q \in P$ and no point of P lies on l.

A random point set will almost certainly determine only ordinary perpendicular bisectors. On the other hand, the $(2n+1)$-gon Δ_{2n+1} determines no ordinary perpendicular bisectors The relationship to isosceles triangles is clear: if the perpendicular bisector for $p, q \in P$ contains k points $p_1, \ldots, p_k \in P$ then each of the triangles (p_i, p, q) is isosceles. Just as Sylvester asked which point sets determine no ordinary lines, we ask which point sets determine no ordinary perpendicular bisectors.

Problem 11.13. *Which finite point sets $P \subset \mathbb{R}^2$ determine no ordinary perpendicular bisectors.*

In the ordinary line case, the answer (Theorem 7.3) is that only when the points are collinear is no ordinary line determined. The situation for ordinary perpendicular bisectors is more complicated. The following conjecture encapsulates all of the examples we have found.

Conjecture 11.14. *Suppose P is a finite point set which determines no ordinary perpendicular bisectors. Then P is either a regular $(2n+1)$-gon or is a finite subset of the equilateral triangular lattice.*

Some examples are given in Figure 11.1. Finally, we note that it is also an interesting question to decide *which* finite subsets of the equilateral triangular lattice have no ordinary perpendicular bisectors.

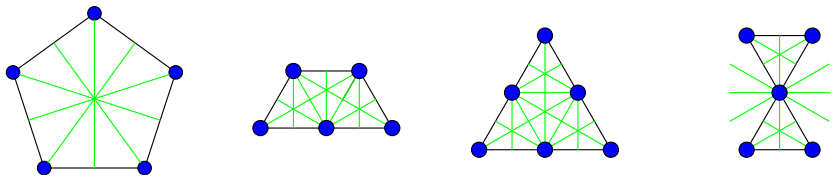


Figure 11.1: A 5-gon and two finite subsets of the equilateral triangular lattice which each determine no ordinary perpendicular bisectors. The perpendicular bisectors of the point sets are highlighted.

Bibliography

[1] Miklós Ajtai, Vašek Chvátal, Monroe M. Newborn, and Endre Szemerédi. Crossing-free subgraphs. *North-Holland Mathematics Studies*, 60:9–12, 1982.

[2] Noga Alon and Joel H. Spencer. *The probabilistic method*. Wiley, 2nd edition, 2004.

[3] Robert Bix. *Conics and Cubics: a concrete introduction to algebraic curves*. Springer, 2nd edition, 2006.

[4] Valentin Blomer and Andrew Granville. Estimates for representation numbers of quadratic forms. *Duke Mathematical Journal*, 135(2):261–302, 2006.

[5] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real algebraic geometry*. Springer Berlin, 1st edition, 1998.

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

[7] Kenneth L. Clarkson, Herbert Edelsbrunner, Leonidas J. Guibas, Micha Sharir, and Emo Welzl. Combinatorial complexity bounds for arrangements of curves and spheres. *Discrete & Computational Geometry*, 5(1):99–160, 1990.

[8] H.S.M. Coxeter. A problem of collinear points. *The American Mathematical Monthly*, 55(1):26–28, 1948.

[9] D.W. Crowe and T.A. McKee. Sylvester's problem on collinear points. *Mathematics Magazine*, 41(1):30–34, 1968.

[10] J. Csima and E.T. Sawyer. There exist $6n/13$ ordinary points. *Discrete & Computational Geometry*, 9(1):187–202, 1993.

[11] G.A. Dirac. Collinearity properties of sets of points. *The Quarterly Journal of Mathematics*, 2(1):221–227, 1951.

[12] Manfredo Perdigao Do Carmo. *Differential geometry of curves and surfaces*. Prentice-Hall, 1976.

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

[14] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 181–190. IEEE, 2009.

[15] György Elekes. On the number of sums and products. *Acta Arithmetica*, 81:365–367, 1997.

[16] György Elekes, Haim Kaplan, and Micha Sharir. On lines, joints, and incidences in three dimensions. *Journal of Combinatorial Theory, Series A*, 118(3):962–977, 2011.

[17] György Elekes and Micha Sharir. Incidences in three dimensions and distinct distances in the plane. In *Proceedings of the 2010 Annual Symposium on Computational geometry*, pages 413–422. ACM, 2010.

[18] Jordan Ellenberg, Richard Oberlin, and Terence Tao. The Kakeya set and maximal conjectures for algebraic varieties over finite fields. *Mathematika*, 56(1):1–25, 2009.

[19] Paul Erdős. On sets of distances of n points. *The American Mathematical Monthly*, 53(5):248–250, 1946.

[20] Paul Erdős and George Purdy. Some extremal problems in geometry III. *Congressus Numerantium*, 14:291–308, 1975.

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

[22] Gregory A. Freiman. *Foundations of a structural theory of set addition*. American Mathematical Society, 1973.

[23] Tibor Gallai. Solution to problem number 4065. *American Mathematical Monthly*, 51:169–171, 1944.

[24] Julia Garibaldi, Alex Iosevich, and Steven Senger. *The Erdős Distance Problem*. American Mathematical Society, 2011.

[25] Ben Green and Terence Tao. On sets defining few ordinary lines. *arXiv preprint arXiv:1208.4714*, 2012.

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

[27] Larry Guth and Nets Hawk Katz. On the Erdős distinct distance problem in the plane. *arXiv preprint arXiv:1011.4105*, 2010.

[28] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers*. Oxford University Press, 1979.

[29] Alex Iosevich, Oliver Roche-Newton, and Misha Rudnev. On an application of Guth-Katz theorem. *arXiv preprint arXiv:1103.1354*, 2011.

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

[31] Haim Kaplan, Micha Sharir, and Eugenii Shustin. On lines and joints. *Discrete & Computational Geometry*, 44(4):838–843, 2010.

[32] Nets Hawk Katz and Gábor Tardos. A new entropy inequality for the Erdős distance problem. *Contemporary Mathematics*, 342:119–126, 2004.

[33] Leroy M. Kelly and William O.J. Moser. On the number of ordinary lines determined by n points. *Canad. J. Math*, 10:210–219, 1958.

[34] Edmund Landau. *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*. 1909.

[35] Frank Thomson Leighton. *Complexity issues in VLSI: optimal layouts for the shuffle-exchange graph and other networks*. MIT press, 1983.

[36] Jiří Matoušek. *Lectures on discrete geometry*. Springer Verlag, 2002.

[37] Eberhard Melchior. Über vielseite der projektiven ebene. *Deutsche Math*, 5:461–475, 1940.

[38] Bojan Mohar and Carsten Thomassen. *Graphs on surfaces*. Johns Hopkins University Press Baltimore, 2001.

[39] Leo Moser. On the different distances determined by n points. *The American Mathematical Monthly*, 59(2):85–91, 1952.

[40] Theodore Motzkin. The lines and planes connecting the points of a finite set. *Transactions of the American Mathematical Society*, pages 451–464, 1951.

[41] János Pach and Pankaj K. Agarwal. *Combinatorial geometry*. Wiley New York, 1995.

[42] René Quilodrán. The joints problem in $\mathbb{R}^n$. *SIAM Journal on Discrete Mathematics*, 23(4):2211–2213, 2010.

[43] René Quilodrán. Introduction to the joints problem. `http://math.berkeley.edu/~rquilodr/Introduction_to_joints.pdf`, 2011.

[44] S. Ramanujan and G.H. Hardy. Collected works of srinivasa ramanujan. *Cambridge University Press*, 1927.

[45] Oliver Roche-Newton and Misha Rudnev. Areas of rectangles and product sets of sum sets. *arXiv preprint arXiv:1203.6237*, 2012.

[46] Keith McKenzie Rogers. The finite field Kakeya problem. *The American Mathematical Monthly*, 108(8):756–759, 2001.

[47] George Salmon. *A treatise on the analytic geometry of three dimensions*. Hodges, Smith, and co., 1865.

[48] Shubhangi Saraf and Madhu Sudan. Improved lower bound on the size of Kakeya sets over finite fields. *arXiv preprint arXiv:0808.2499*, 2008.

[49] Jacob T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[50] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Springer Verlag, 1992.

[51] József Solymosi and Csaba D. Tóth. Distinct distances in the plane. *Discrete & Computational Geometry*, 25(4):629–634, 2001.

[52] A.H. Stone and John W. Tukey. Generalized sandwich theorems. *Duke Mathematical Journal*, 9(2):356–359, 1942.

[53] Joseph Sylvester. Mathematical question 11851. Educational Times, 1893.

[54] László A. Székely. Crossing numbers and hard Erdős problems in discrete geometry. *Combinatorics, Probability, and Computing*, 6:353–358, 1997.

[55] Endre Szemerédi and William T. Trotter Jr. Extremal problems in discrete geometry. *Combinatorica*, 3(3-4):381–392, 1983.

[56] Terence Tao. The Szemerédi-Trotter theorem and the cell decomposition. `http://terrytao.wordpress.com/2009/06/12/the-szemeredi-trotter-theorem-and-the-cell-decomposition/`, 2009.

[57] Terence Tao and Van H. Vu. *Additive combinatorics*. Cambridge University Press, 2006.

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

[59] Richard Zippel. *Probabilistic algorithms for sparse polynomials*. Springer, 1979.