Math 307: The Polynomial Method
Personal Notes

Adel Saleh

March 4, 2021

Contents

Introduction

1 The Tools for the Polynomial Method

Definition. *Suppose that $\mathbb{F}$ is a field, D a non-negative integer and $n \in \mathbb{N}^*$. The space of polynomials in n variables over $\mathbb{F}$ of degree atmost D will be denoted by $\mathcal{P}_D(\mathbb{F}^n)$.*

An element in P in $\mathcal{P}_D(\mathbb{F}^n)$ can be written as

$$P = \sum_{k=0}^{D} P_k \quad \text{where} \quad P_k(x_1, \dots, x_n) = \sum_{i_1=1}^{n} \dots \sum_{i_k=1}^{n} c_{i_1,\dots,i_k} x_{i_1} \dots x_{i_k}$$

where $x_1, \dots, x_n$ are coordinates in $\mathbb{F}^n$. We note that P_k is homogeneous in degree k, ie $P_k(\lambda x) = \lambda^k P_k(x)$ for all $\lambda \in \mathbb{F}$.

Lemma 1.1. *$\mathcal{P}_D(\mathbb{F}^n)$ is a vector space over $\mathbb{F}$ of dimension $\binom{D+n}{n}$. In particular, $\operatorname{Dim} \mathcal{P}(\mathbb{F}^n) \geq \frac{D^n}{n!}$.*

Proof. It is clear that $\mathcal{P}_D(\mathbb{F})^n$ is a vector space over $\mathbb{F}$. It is also clear that the set

$$\left\{ x_1^{D_1} \dots x_n^{D_n} : D_i \geq 0 \text{ and } \sum_{i=1}^{n} D_i \leq D \right\}$$

forms a basis for $\mathcal{P}_D(\mathbb{F}^n)$. We write each monomial $x_1^{D_1} \dots x_n^{D_n}$ as $1^{D_0} x_1^{D_1} \dots x_n D_n$ with $D_0 \geq 0$ abd $\sum_{i=0}^{n} D_i = D$. So the problem of counting the monomials becomes a problem of counting the number of ways we can place D balls into $n+1$ jars so the answer is $\binom{D+1}{n}$. A simple computation shows that $\binom{D+1}{n} \geq \frac{D^n}{n!}$. ■

Consider the following problem. Suppose we are in $\mathbb{R}^2$ and consider the set of points

$$S_{10000} = \{(1,1), (2,-2), \dots, (10000, -10000)\}.$$

We want to find a polynomial P of two variables that vanishes on S. One easy solution is the polynomial

$$Q(x,y) = \prod_{n=1}^{10000} (x-n)$$

and the degree of P is the cardinality of S which is 10000. The following lemma provides us with a smaller degree polynomial that vanishes on S.

Lemma 1.2. *Suppose that $\mathbb{F}$ is a field and $S \subset \mathbb{F}^n$. Let $D = \min \left\{ d \in \mathbb{N} : \frac{d^n}{n!} > |S| \right\}$ then*

(i) $\dfrac{D^n}{(2^n)(n!)} \leq |S| < \dfrac{D^n}{n!}$

(ii) *There is a non-zero polynomial $P \in \mathcal{P}_D(\mathbb{F}^n)$ such that P vanishes on S.*

Proof. We define a linear map $\Phi : \mathcal{P}_D(\mathbb{F}^n) \to \mathbb{F}^S$ by $\Phi(P) = P|_S$. By lemma 1, $\operatorname{Dim} \mathcal{P}_D(\mathbb{F}^n) \geq D^n/n!$ and $\operatorname{Dim} \mathbb{F}^S = |S| < D^n/n!$ and thus Φ is not injective. Therefore there is a non zero polynomial $P \in \mathcal{P}_D(\mathbb{F}^n)$ such that $P|_S = 0$. This proves (ii).

To prove (i), we notice from the definition of D that

$$\frac{(D-1)^n}{n!} \leq |S|$$

which means

$$D - 1 \leq \sqrt[n]{n!}|S|^{1/n} \implies D \leq \sqrt[n]{n!}|S|^{1/n} + 1 \leq \sqrt[n]{n!}|S|^{1/n} + \sqrt[n]{n!}|S|^{1/n} = 2\sqrt[n]{n!}|S|^{1/n}$$

giving the desired bound on D. ■

Thus the above lemma tells us that there is a polynomial of degree at most $2\sqrt[n]{n!}|S|^{1/n}$ that vanishes on S. So if we apply this to the above example, we get a polynomial of degree at most 300 that vanishes in S_{10000}.

Lemma 1.3. *Suppose that $P \in \mathcal{P}_D(\mathbb{F})$ and $x_0 \in \mathbb{F}$. Then there is a polynomial $Q \in \mathcal{P}_{D-1}(\mathbb{F})$ and an element $r \in \mathbb{F}$ such that*

$$P(x) = (x - x_0)Q(x) + r.$$

Proof. We use induction on D. If $D = 0$ then P is the constant polynomial and the result is trivial.

Suppose that $D \geq 1$ and the result is true for $D - 1$. We write

$$P(x) = \sum_{k=0}^{D} a_k x^k$$

and we let

$$Q(x) = P(x) - a_D x^{D-1}(x - x_0)$$

Clearly, Q has degree smaller than or equal to $D - 1$ and thus by the induction hypothesis, there is a polynomial $Q' \in \mathcal{P}_{D-2}(\mathbb{F})$ and an $r' \in \mathbb{F}$ such that

$$Q(x) = (x - x_0)Q'(x) + r'$$

this yields

$$P(x) = (x - x_0)(Q'(x) + a_D x^{D-1}) + (r + r')$$

where $r + r' \in \mathbb{F}$ and $Q'(x) + a_D x^{D-1} \in \mathcal{P}_{D-1}(\mathbb{F})$ which proves the lemma.

■

Lemma 1.4. *Let $P \in \mathcal{P}_D(\mathbb{F})$. If P vanishes on $D + 1$ points of $\mathbb{F}$, then P is the zero polynomial.*

Proof. If $D = 0$, then $P(x) = r$ for some constant $r \in \mathbb{F}$. Since P vanishes on some point of $\mathbb{F}$, then $r = 0$ and hence P is the zero polynomial.

We suppose that $D \geq 1$ and the result is true for $D - 1$. We know that the degree of P is less than or equal to D and P vanishes on points say $x_1, x_2, \ldots, x_{D+1} \in \mathbb{F}$. We write using the above lemma

$$P(x) = (x - x_1)Q(x) + r$$

. Plugging in for x_1 we see that $r = 0$ and hence $P(x) = (x - x_1)Q(x)$. This means that Q vanishes on $x_2, \ldots, x_{D+1}$. But Q has degree smaller than or equal to $D - 1$ and vanishes on D points of $\mathbb{F}$ thus by the induction hypothesis $Q = 0$ and therefore $P = 0$. ■

Definition. *Let $\mathbb{F}$ be a field and $a, b \in \mathbb{F}^n$ such that $a \neq 0$. The set $\{at + b : t \in \mathbb{F}\}$ is called a line in $\mathbb{F}^n$.*

Lemma 1.5 (Vanishing Lemma)**.** *Let $P \in \mathcal{P}_D(\mathbb{F}^n)$. Suppose that $L \subset \mathbb{F}^n$. If P vanishes on $D+1$ points of L, the P is vanishes on L.*

Proof. Let us write $L = \{at + b : t \in \mathbb{F}\}$. We define a polynomial $Q \in \mathcal{P}_D(\mathbb{F})$ by

$$Q(t) = P(at + b)$$

Then Q vanishes at $D+1$ points of $\mathbb{F}$. The above lemma tells us that Q is the zero polynomial and thus P vanishes on L. ■

Throughout the course, $\mathbb{F}_q$ will denote a finite field with q elements.

Lemma 1.6. *If $P \in \mathcal{P}_{q-1}(\mathbb{F}_q^n)$ vanishes on the entire space $\mathbb{F}_q^n$ then P is the zero polynomial.*

Proof. We induct on the dimension n.

For $n = 1$ we have a polynomial in one variable of degree smaller than or equal to $q - 1$ which vanishes on q points. By a previous lemma, q is the zero polynomial.

We now suppose that $n \geq 2$ and that the lemma is true for $n - 1$. We write

$$P(x) = P(x_1, \ldots, x_n) = \sum_{j=1}^{q-1} P_j(x_1, \ldots, x_{n-1}) x_n^j \, .$$

We fix values for $x_1, \ldots, x_{n-1}$ and we consider P as a polynomial in one variable. The new polynomial has degree at most $q-1$ and vanishes on all of the q points of $\mathbb{F}_q$. This means that the new polynomial is the zero polynomial and therefore all of it's coefficients are zero. Therefore each P_j vanishes on $\mathbb{F}_q^{n-1}$. This means by induction that each P_j is the zero polynomial and thus P is the zero polynomial. ■

2 Polynomial Method for Kakeya and Nikodym Problems

Definition. *A Kakeya set in $\mathbb{F}_q^n$ is a set K satisfying the following condition: to every $a \in \mathbb{F}_q^n \setminus \{0\}$ there is a vector $b \in \mathbb{F}_q^n$ such that the line $\{at + b : t \in \mathbb{F}\}$ is contained in K.*

Conjecture 1 (Finite-Field Kakeya Conjecture)**.** *The cardinality of any Kakeya set in the space $\mathbb{F}_q^n$ has cardinality greater than or equal to $\frac{q^n}{2^n n!}$.*

The above conjecture is obviously true for $n = 1$, for any line in $\mathbb{F}_q$ contains all q points of $\mathbb{F}_q$ therefore any Kakeya set has cardinality greater than or equal to $q/2$.

Notice that any Kakeya set K in $\mathbb{F}_q^n$ where $n \geq 2$ has cardinality at least

$$\frac{q^n - 1}{q - 1} \geq q^{n-1} \geq q.$$

This proves the conjecture for $n = 2$.

Proposition 2.1. *A Kakeya set K contains at least $(q^n - 1)/q - 1$ lines.*

Proof. Let us pretend that each line pays 1\$ to each point it passes through. But each line passes through q points, then it pays q\$. So the lines of K pay at least

$$q\frac{q^n-1}{q-1}\$$$

By the Pigeon Hole principle there is a point $x \in K$ which makes at least

$$\frac{q}{|K|} \cdot \frac{q^n-1}{q-1}$$

and therefore K contains a least the above number of lines. But each of these lines contains $q-1$ points other than x, so their union contains

$$(q-1) \cdot \frac{q}{|K|} \cdot \frac{q^n-1}{q-1} = \frac{q(q^n-1)}{|K|}$$

and therefore

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

∎

Definition. *A set $N \subset \mathbb{F}_q^n$ is called a Nikodym set if to every $x \in \mathbb{F}_q^n$ there is a line $L(x)$ such that*

(i) $x \in L(x)$.

(ii) $L(x) \setminus \{x\} \subset N$.

Theorem 2.2 (Dvir, 2009)**.** *If N is a Nikodym set in $\mathbb{F}_q^n$*

$$|N| \geq \frac{q^n}{(q^n)(n!)}$$

Proof. There is an integer D and an non-zero polynomial $P \in \mathcal{P}_D(\mathbb{F}_q^n)$ such that

$$\frac{D^n}{(2^n)(n!)} \leq |N| \leq \frac{D^n}{n!}$$

and P vanishes on N. We are going to show that $D \geq q-1$. Suppose $D < q-1$. Given an $x \in \mathbb{F}_q^n$ then there is a line $L(x)$ containing x and $L(x) \setminus \{x\} \subset N$. Since P vanishes on N, P vanishes on $L(x) \setminus \{x\}$ which is a set of $q-1 > D$ points. This implies that P vanishes on $L(x)$. Since x was arbitrary, P vanishes on all $\mathbb{F}_q^n$ and $D < q-1$ therefore P is the zero polynomial which is a contradiction. This tells us that

$$q \leq D+1 \leq 2D \leq 2\sqrt[n]{2^n\, n!\, |N|} \leq 4^n \sqrt[n]{n!}\, |N|^{\frac{1}{n}},$$

which is the desired result. ∎

Theorem 2.3 (Dvir, 2009)**.** *If K is a Kakeya set in $\mathbb{F}_q^n$ then*

$$|K| \geq \frac{q^n}{2^n\, n!}.$$

Proof. There is an integer D and a polynomial $P \in \mathcal{P}_D(\mathbb{F}_q^n)$ such that

$$\frac{D^n}{(2^n)(n!)} \leq |N| \leq \frac{D^n}{n!}$$

and P vanishes on K. We are going to show that $D \geq q-1$. Suppose that $D < q-1$ and let $\bar{D}$ be the degree of P. Then $\bar{D} \geq 1$ and $1 \leq \bar{D} \leq D$. We write $P = \sum_{k=0}^{\bar{D}} P_k$ where P_k is a homogenous polynomial of degree k. In fact,

$$P_k(x) = P_k(x_1, \dots, x_n) = \sum_{i_1=1}^{n} \dots \sum_{i_k=1}^{n} c_{i_1,\dots,i_k} x_{i_1} \dots x_{i_k}$$

Since the degree of P is $\bar{D}$ then $P_{\bar{D}}$ is a non zero polynomial. Given a point $a \in \mathbb{F}_q^n \setminus 0$, we know that P vanishes on the line $\left\{at + b : b \in \mathbb{F}_q^n\right\}$. Therefore $P(at+b) = 0$ for all $t \in \mathbb{F}_q$. Now consider $P(at+b)$ as a polynomial in one variable t. This polynomial vanishes on all q points of $\mathbb{F}_q$, and it's degree is $\bar{D} < D < q-1$ and so it is the zero polynomial. Therefore the leading coefficients of $P(at+b)$ are 0. But the leading coefficient is $P_{\bar{D}}(a)$, so $P_{\bar{D}}(a) = 0$. Also, $P_{\bar{D}}(0) = 0$ since it is homogeneous. Since this is true for all $a \in \mathbb{F}_q^n$, $P_{\bar{D}}$ is the zero polynomial. With the same reasoning as the above proof we get the desired result. ■

Definition. *Let $\mathfrak{L}$ be a set of lines in $\mathbb{R}^3$ and let $L = |\mathfrak{L}|$. The set of joints of $\mathfrak{L}$ is defined to be*

$$J = \left\{x \in \mathbb{R}^3 : \text{ there are linearly independent lines } l_1, l_2, l_3 \in \mathfrak{L} \text{ such that } x \in l_1 \cap l_2 \cap l_3 \text{ and } \right\}.$$

Conjecture 2. *Let $\mathfrak{L}$ be a finite set of lines in $\mathbb{R}^3$ and let J be the set of joints of $\mathfrak{L}$ then*

$$|J| \leq 7L^{\frac{3}{2}}.$$

This conjecture was solved in 2010 by Guth and Katz using the polynomial method. To prove this conjecture, we need the following lemma.

Lemma 2.4. *There is a line $l \in \mathfrak{L}$ such $|l \cap J| \leq 2\sqrt[3]{6}|J|^{\frac{1}{3}}$.*

Proof. There is an integer D and a non-zero polynomial $P \in \mathcal{P}_D(\mathbb{R}^3)$ such that $D^3/(2^3)(3!) \leq |J| < D^3/3!$ and P vanishes on J. Let Q be the polyomial of minimal degree that vanishes on J and let $\bar{D}$ be it's degree. Of course, $1 \leq \deg Q \leq D$. Suppose that there is no line of $\mathfrak{L}$ that satisfies $|l \cap J| \leq 2\sqrt[3]{6}|J|^{\frac{1}{3}}$. Let $l \in \mathfrak{L}$ then Q vanishes on $l \cap J$. Also, $\deg Q \leq D \leq 2\sqrt[3]{3!}|J|^{\frac{1}{3}} < |l \cap J|$ by assumption and so Q vanishes on l and therefore Q vanishes on all of the lines of $\mathfrak{L}$.

Now let $x \in J$, then there are three linearly independent lines $l_1, l_2, l_3 \in \mathfrak{L}$ containing x. Let v_1, v_2 and v_3 be their respective directions. Since Q is zero on these lines we get

$$\nabla Q(x) \cdot v_1 = \nabla Q(x) \cdot v_2 = \nabla Q(x) \cdot v_3 = 0.$$

Since v_1, v_2 and v_3 are linearly independent then it follows that $\nabla Q(x) = 0$. Therefore ∇Q vanishes on J and thus its components $\partial_i Q$ vanish on J for $i = 1, 2, 3$. But $\partial_i Q$ is a polynomial of degree less than that of Q. But Q is the non-zero polynomial with the smallest degree that vanishes on J therefore $\nabla Q = 0$ and Q is a constant. But this is not possible since $\deg Q \geq 1$. ■

3 Polynomial Method in Error Correcting Codes

Lemma 3.1. *Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a map. Let $|A|$ be a subset of $\mathbb{F}_q$ with $|A| \geq 51/100$. Then there is at most one polynomial $Q \in \mathcal{P}_{\frac{q}{2}}(\mathbb{F}_q)$ which agrees with F on A.*

Proof. Suppose that $Q_1, Q_2 \in \mathcal{P}_{\frac{q}{2}}(\mathbb{F}_q)$ such that Q_1 and Q_2 agree with F on A. Let $P = Q_1 - Q_2$ then $p \in \mathcal{P}_{\frac{q}{2}}(\mathbb{F}_q)$ and P vanishes on A but $\deg P \leq q/2 < \frac{51}{100}q \leq |A|$. So P is the zero polynomial and so $Q_1 = Q_2$. ■

Definition. *We define Poly$(\mathbb{F}^2)$ to be the set of all polynomials in two variables over the field $\mathbb{F}$. Define Poly$_{D,E}(\mathbb{F}^2)$ to be the set of all polynomials $P(x,y)$ of two variables such that $\deg_x P \leq D$ and $\deg_y P \leq E$.*

We note that $\left\{x^a y^b : 0 \leq a \leq D,\ 0 \leq b \leq E\right\}$ is a basis of $\mathrm{Poly}_{D,E}(\mathbb{F}^2)$ and therefore we get $\mathrm{Dim}\,\mathrm{Poly}_{D,E}(\mathbb{F}^2) = (D+1)(E+1)$.

Proposition 3.2. *Let $\mathbb{F}$ be a field and $S \subset \mathbb{F}^2$ with $4 \leq |S| < \infty$. Let $D = \min\left\{d \in \mathbb{N} : 2d + 2 > |S|\right\}$ then*

(i) $\dfrac{|S|}{2} - 1 \leq D \leq \dfrac{|S|}{2}$

(ii) *There is a polynomial $P \in$ Poly$_{D,E}(\mathbb{F}^2)$ that vanishes on S.*

Proof. We define a linear map $\Phi : \mathrm{Poly}_{D,1}(\mathbb{F}^2) \to \mathbb{F}^S$ by $\Phi(P) = P|_S$. The dimension of the domain is $2D + 1$ and the dimension of the range is $|S| < 2D + 2$. Therefore, the map is not injective and there is a non zero element P in it's kernel which satisfied $P|_S = 0$. On the other hand, $D - 1 \notin \left\{d \in \mathbb{N} : 2d + 2 > |S|\right\}$ therefore $2(D-1) + 2 \leq |S|$ proving part (i). ■

Lemma 3.3. *Let $\mathbb{F}$ be a field and let $P \in \mathbb{F}[x,y]$ with $\deg_y P \leq D$ for some $D \in \mathbb{N}$. Let $Q \in \mathbb{F}[x]$, then there are polynomials $P_1 \in \mathbb{F}[x,y]$ and $R \in \mathbb{F}[x]$ such that*

(i) $P(x,y) = (y - Q(x))P_1(x,y) + R(x)$,

(ii) $\deg_y P_1 \leq D - 1$

Proof. We induct on D. If $D = 0$, then $P(x,y) = 0$ is a polynomial in $x = R(x)$ and the conclusion follows. We assume $D \geq 1$ and the result is true for $D - 1$. We write

$$P(x,y) = \sum_{j=0}^{D} a_j(x) y^j$$

with $a_0(x), \ldots a_D(x) \in \mathbb{F}[x]$. Then using the division algorithm get

$$\bar{P}(x,y) = P(x,y) - a_D(x) y^{D-1}(y - Q(x))$$

so $\deg_y(\bar{P}) \leq D - 1$. So by induction there are polynomials $\bar{P}_1(x,y) \in \mathcal{P}(\mathbb{F}^2)$ and $R(x) \in \mathcal{P}(\mathbb{F})$ such that $\deg_y \bar{P}_2 \leq D - 2$ and $\bar{P}(x,y) = (y - Q(x))\bar{P}_1(x,y) + R(x)$. Therefore

$$P(x,y) = \bar{P}(x,y) + a_D(x) y^{D-1}(y - Q(x))$$

and thus

$$\begin{aligned}P(x,y) &= (y - Q(x))\bar{P}_1(x,y) + a_D y^{D-1}(y - Q(x)) + R(x)\\ &= (y - Q(x))(\bar{P}_1(x,y) + a_D y^{D-1}) + R(x)\end{aligned}$$

Letting $P_1(x,y) = \bar{P}_1(x,y) + a_D(x)y^{D-1}y^{D-1}$, we get the desired polynomial. ■

Lemma 3.4. *Suppose that $\mathbb{F}$ is a field and let $P(x,y) \in \mathcal{P}(\mathbb{F}^2)$ with $\deg_y P \leq D$ and $Q(x) \in \mathcal{P}(\mathbb{F})$. Then if $P(x, Q(x))$ is the zero polynomial then there is polynomial $P_1(x,y) \in \mathcal{P}(\mathbb{F}^2)$ such that*

(i) $\deg_y P_1 \leq D - 1$,

(ii) $P(x,y) = (y - Q(x))P_1(x,y)$.

Proof. The above lemma provides us with polynomials $P_1(x,y) \in \mathcal{P}(\mathbb{F}^2)$ and $R(x) \in \mathcal{P}(\mathbb{F})$ such that $\deg_y P_1 \leq D - 1$ and $P(x,y) = (y - Q(x))P_1(x,y) + R(x)$. This gives

$$P(x, Q(x)) = (Q(x) - Q(x))P_1(x, Q(x)) + R(x) = R(x),$$

but $P(x, Q(x))$ is the zero polynomial. Hence $R(x)$ is the zero polynomial and $P(x,y) = (y - Q(x))P_1(x,y)$. ■

Theorem 3.5. *Let q be an integer greater than 4. $A \subset \mathbb{F}_q$ with $|A| \geq \frac{51}{100}q$ Let $d < \frac{q}{100}$, $Q \in \mathcal{P}_q(\mathbb{F})_q$ and $F : \mathbb{F}_q \to \mathbb{F}_q$ be a function, then there is a polynomial time algorithm that recovers Q from F.*

Proof. We let S be the graph of F in $\mathbb{F}_q^2$. Then $|S| \geq 1$ and thus proposition 3.2 provides us with an integer $\widetilde{D}$ and a non zero polynomial $\widetilde{P} \in poly_{\widetilde{D},1}(\mathbb{F}^2)$ such that $|S|/2 - 1 < \widetilde{D} \leq |S|/2$ and $\widetilde{P}$ vanishes on S. We let P be the non-zero polynomial in $\mathcal{P}(\mathbb{F}^2)$ of minimal degree that vanishes on S. Setting $D = \deg P$, we have $D \leq \widetilde{D} \leq |S|/2$ and we write $P(x,y) = P_0(x) + yP_1(x)$ with $P_0, P_2 \in \mathcal{P}_D(\mathbb{F}_q)$. We prove that $P(x, Q(x))$ is the zero polynomial. Indeed, looking at the polynomial $P(x, Q(x)) = P_0(x) + Q(x)P_1(x)$, we see that this polynomial has degree at most $D + d$. Since $P(x, F(x)) = 0$ for all $x \in \mathbb{F}_q$ so that $P(x, Q(x)) = P(x, F(x)) = 0$ for all $x \in A$ so our polynomial has degree at most $D + d > |S|/2 + q/100 = 51/100q$ and vanishes on the set A which has greater than or equal to $51/100q$ points. Therefore, P is the zero polynomial. This implies that $P_0(x) + Q(x)P_1(x) = 0$ is the zero polynomial and therefore $Q(x) = -P_0(x)/P_1(x)$.

Let $E = \{e \in \mathbb{F}_q : F(e) \neq Q(e)\}$ then $P(x,y) = c(y - Q(x)) \prod_{e \in E}(x - e)$ where c is a constant.

Now we prove the second claim. The fact that P is the zero polynomial and lemma 3.4 tells us that there a polynomial $P_1 \in \mathcal{P}_(\mathbb{F}_q)$ such that $P(x,y) = (y - Q(x))P_1(x)$. Now let $e \in E$ then $0 = P(e, F(e)) = (F(e) - Q(e))P_1(e)$. This implies that $P_1(e) = 0$ therefore $P(x,y) = (y - Q(x)) \prod_{e \in E}(x - e)P_2(x)$. Since P has minimal degree, $P_2(x)$ must be a constant c. Since P is non zero, this constant is different from 0. ■

4 The Polynomial Method and Distance Sets

4.1 Some Results on Erdos and Falconer's Distance Set Conjectures

Suppose that $P \subset \mathbb{R}^2$ is a set with N points. The distance set of P is defined to be

$$d(P) = \left\{ |p - q| : p, q \in P \text{ and } p \neq q \right\}.$$

Conjecture 3 (Erdős)**.** *There is a constant C such that for any set $P \subset \mathbb{R}^2$ with N points then we have*

$$|d(P)| \geq C \frac{N}{\sqrt{\log(N)}}.$$

The best known result so far is the Gutz-Katz theorem which was proven in 2010.

Theorem 4.1 (Guth-Katz,2010)**.** *There is a constant C such that for any finite set $P \subset \mathbb{R}^2$ with $N := |P|$, we have*

$$|d(P)| \geq C \frac{N}{\log(N)}.$$

Here is an implication of the theorem. Let $\epsilon > 0$, since $\log(N^\epsilon) \leq N^\epsilon$, we have $1/\log(N) \geq \epsilon/N^\epsilon$. Thus by the Guth-Katz theorem we have

$$|d(P)| \geq \underbrace{\epsilon C}_{C_\epsilon} N^{1-\epsilon}$$

We put this result into a theorem.

Theorem 4.2 (Guth, 2014)**.** *To every $\epsilon > 0$ there is a constant C_ϵ such that $d(P) \geq C_\epsilon N^{1-\epsilon}$.*

Of course Guth-Katz implies Guth, but Guth's theorem is easier to prove and contains the main ideas. The distance set problem is the discrete version of a very important conjecture in geometric measure theory.

Conjecture 4 (Falconer)**.** *Let K be a compact subset of $\mathbb{R}^n$ with Hausdorff dimension greater than or equal to $n/2$, then the set $\left\{ |x - y| : x, y \in K \right\}$ has positive one dimensional Lebesgue measure.*

Falconer proved that Borel sets with Hausdorff dimension greater than $(d + 1)/2$ have distance sets with nonzero measure [**?**]. For points in the Euclidean plane, a variant of Falconer's conjecture states that a compact set whose Hausdorff dimension is greater than or equal to one must have a distance set of Hausdorff dimension one. Falconer himself showed that this is true for compact sets with Hausdorff dimension at least 3/2, and subsequent results lowered this bound to 4/3.[**?**, **?**] It is also known that, for a compact planar set with Hausdorff dimension at least one, the distance set must have Hausdorff dimension at least 1/2.[**?**] In 2018, Guth, Iosevich, Ou and Wang [**?**] proved that if the Hausdorff dimension of a planar set is greater than 5/4, then there exists a point in the set such that the Lebesgue measure of the distances from the set to this point is positive.

We now develop the results needed to prove Guth's theorem.

Lemma 4.3. *Suppose that P is a subset of $\mathbb{R}^2$ with N points. Let*

$$\boxed{Q(P) = \left\{ (p, q, r, s) \in P^4 : |p - q| = |r - s| \neq 0 \right\}}$$

then $(N^2 - N)^2 \leq |d(P)||Q(P)|$.

Proof. We write $d(P) = \{d_1, \dots, d_n\}$ with $n = |d(P)|$. Now notice that

$$\bigcup_{i=1}^{n} \Big\{(p,q) \in P^2 : |p-q| = d_i\Big\} = \Big\{(p,q) \in P^2 : p \neq 0\Big\}.$$

Also notice that this union is disjoint so that if n_i is the cardinality of i-th set in the above union then

$$\left|\Big\{(p,q) \in P^2 : p \neq q\Big\}\right| = \sum_{i=1}^{n} n_i.$$

Also we have

$$\bigcup_{i=1}^{n} \Big\{(p,q,r,s) \in P^4 : |p-q| = |r-s| = d_i\Big\} = Q(P),$$

where the union is disjoint and therefore

$$|Q(P)| = \sum_{i=1}^{n} \left|\Big\{(p,q,r,s) \in P^4 : |p-q| = |r-s| = d_i\Big\}\right| = \sum_{i=1}^{n} n_i^2.$$

It is clear that $N^2 - N = \left|\Big\{(p,q) \in P^2 : p \neq q\Big\}\right|$ and thus

$$N^2 - N = \sum_{i=1}^{n} n_i \leq \left(\sum_{i=1}^{n} 1^2\right)^{\frac{1}{2}} \left(\sum_{i=1}^{n} n_i^2\right)^{\frac{1}{2}} = \sqrt{n} \cdot \sqrt{|Q(P)|}$$

and finally

$$(N^2 - N)^2 \leq n|Q(P)| = |d(P)||Q(P)|,$$

which concludes the proof. ■

Given the above, we have changed the problem from finding a lower bound of $|d(P)|$ to finding an upper bound for $|Q(P)|$. The set $Q(P)$ is related to an important set of lines which we subsequently introduce.

4.2 The Sets $Q(P)$, $\mathfrak{L}(P)$ and $P_r(\mathfrak{L})$ in relation to $d(P)$

Definition. *Let $p = (p_1, p_2)$ and $q = (q_1, q_2)$ be points in $\mathbb{R}^2$. We define $\ell_{p,q} \subset \mathbb{R}^3$ to be the line given by*

$$\ell_{p,q} := \left\{\left(\frac{p_1+q_1}{2} + \frac{p_2-q_2}{2}\,t,\ \frac{p_2+q_2}{2} + \frac{q_1-p_2}{2}\,t,\ t\right) : t \in \mathbb{R}\right\}. \tag{1}$$

If $P \subset \mathbb{R}^2$, we define

$$\boxed{\mathfrak{L}(P) := \Big\{\ell_{p,q} : (p,q) \in P^2\Big\}} \tag{2}$$

The set $\mathfrak{L}(P)$ will play an important role in the theory. Here are some basic but essential properties of these lines.

Lemma 4.4. *Let $p, q, r, s \in \mathbb{R}^2$. Consider the lines $\ell_{p,r}$ and $\ell_{q,s}$ be defined as above, then we have the following properties:*

(i) $\ell_{p,r}$ *is parallel to* $\ell_{q,s}$ *if and only if* $p - q = r - s$*,*

(ii) *If* $\ell_{p,r}$ *is not parallel to* $\ell_{q,s}$ *then* $\ell_{p,r} \cap \ell_{q,s} \neq \emptyset$*,*

(iii) $\ell_{p,r} = \ell_{q,s}$ *if and only* $p = q$ *and* $r = s$*.*

Proof. We start with an elementary observation. Suppose that L_1 and L_2 are two lines in $\mathbb{R}^3$ given by

$$L_1(t) = \begin{cases} x = x_0 + \alpha t \\ y = y_0 + \beta t \\ z = z_0 + \gamma t \end{cases} \qquad L_2(t) = \begin{cases} x = u_0 + \bar{\alpha} t \\ y = v_0 + \bar{\beta} t \\ z = w_0 + \bar{\gamma} t \end{cases}$$

Suppose that L_1 and L_2 are not parallel then $L_1 \cap L_2 \neq \emptyset$ if and only if

$$(\beta\bar{\gamma} - \bar{\beta}\gamma)(u_0 - x_0) - (\alpha\bar{\gamma} - \bar{\alpha}\gamma)(v_0 - y_0) + (\alpha\bar{\beta} - \bar{\alpha}\beta)(w_0 - z_0) = 0$$

We let $\mathcal{P}$ be the plane through L_1 which is parallel to L_2. Then the normal vector of $\mathcal{P}$ is

$$\begin{vmatrix} i & j & k \\ \alpha & \beta & \gamma \\ \bar{\alpha} & \bar{\beta} & \bar{\gamma} \end{vmatrix} = (\alpha\bar{\gamma} - \bar{\beta}\gamma)i - (\alpha\bar{\gamma} - \bar{\alpha}\gamma)j + (\alpha\bar{\beta} - \bar{\alpha}\beta)k$$

so the equation of $\mathcal{P}$ is

$$(\beta\bar{\gamma} - \bar{\beta}\gamma)(x - x_0) - (\alpha\bar{\gamma} - \bar{\alpha}\gamma)(y - y_0) + (\alpha\bar{\beta} - \bar{\alpha}\beta)(z - z_0) = 0$$

So $L_1 \cap L_2 \neq \emptyset$ if and only if $L_2 \subset \mathcal{P}$ if and only if $(u_0, v_0, w_0) \in \mathcal{P}$ if and only if

$$(\beta\bar{\gamma} - \bar{\beta}\gamma)(u_0 - x_0) - (\alpha\bar{\gamma} - \bar{\alpha}\gamma)(v_0 - y_0) + (\alpha\bar{\beta} - \bar{\alpha}\beta)(w_0 - z_0) = 0.$$

Now notice that the two lines $\ell_{p,r}$ and $\ell_{q,s}$ are given by

$$\ell_{p,r}(t) = \begin{cases} x = \dfrac{p_1 + r_1}{2} + \dfrac{p_2 - r_2}{2} t \\ x = \dfrac{p_2 + r_2}{2} + \dfrac{r_1 - p_1}{2} t \\ z = t \end{cases} \qquad \ell_{q,s}(t) = \begin{cases} x = \dfrac{q_1 + s_1}{2} + \dfrac{q_2 - s_2}{2} t \\ x = \dfrac{q_2 + s_2}{2} + \dfrac{s_1 - q_1}{2} t \\ z = t \end{cases}$$

So $\ell_{p,r}$ is parallel to $\ell_{q,s}$ if and only if the direction vector of $\ell_{p,r}$ is parallel to the direction vector of $\ell_{q,s}$ if and only if $(\frac{p_2 - r_2}{2}, \frac{r_1 - p_1}{2}, 1) = \lambda(\frac{q_2 - s_2}{2}, \frac{s_1 - q_1}{2}, 1)$ for some $\lambda \in \mathbb{R}$ if and only if $\lambda = 1$ if and only if $\frac{p_2 - r_2}{2} = \frac{q_2 - s_2}{2}$ and $\frac{r_1 - p_1}{2} = \frac{s_1 - q_2}{2}$ if and only if

$$\begin{cases} p_2 - r_2 = q_2 - s_2 \\ r_1 - p_1 = s_1 - q_1 \end{cases} \iff \begin{cases} p_1 - r_1 = r_1 - s_1 \\ p_2 - q_2 = r_2 - s_2 \end{cases} \iff p - q = r - s \iff |p - q| = |r - s|$$

Also by the elementary observation, if $\ell_{p,r}$ and $\ell_{q,s}$ are not parallel, then $\ell_{p,r} \cap \ell_{q,s} \neq \emptyset$ if and only if

$$\left(\frac{r_1 - p_1}{2} - \frac{s_1 - q_1}{2}\right)\left(\frac{q_2 + s_1}{2} - \frac{p_1 + r_1}{2}\right) - \left(\frac{p_2 - r_2}{2} - \frac{q_2 - s_2}{2}\right)\left(\frac{q_2 + s_2}{2} - \frac{p_2 - r_2}{2}\right) = 0$$

if and only if

$$\left[(r_1 - s_1) - (p_1 - q_2)\right]\left[(r_1 - s_1) - (p_1 - q_1)\right] = \left[-(r_2 - s_2) + (p_2 - q_2)\right]\left[(r_2 - s_2) + (p_2 - q_2)\right]$$

if and only if

$$(r_1 - s_1)^2 - (p_1 - q_1)^2 = (p_2 - q_2)^2 - (r_2 - s_2)^2$$

if and only if

$$(r_1 - s_1)^2 + (r_2 - s_2)^2 = (p_2 - q_2)^2 + (p_1 - q_1)^2$$

if and only if

$$|p - q|^2 = |r - s|^2 \iff |p - q| = |r - s|$$

We have proved (i) and (ii). We still need to prove (iii). The reverse implication is clear. Suppose that the lines are equal then $\ell_{p,r} \cap \{z = 0\} = \ell_{q,s} \cap \{z = 0\}$ and so $p_1 + r_1 = q_1 + s_1$ and $p_1 + r_2 = q_2 + s_2$ therefore $p - q = s - r$. But also $\ell_{p,r} = \ell_{q,s}$ says that the lines are parallel which means that $p - q = r - s$. Hence the lines being equal implies $r = s$ and $p = q$. ■

Corollary 4.4.1. *Suppose that $p \in \mathbb{R}^2$ then any two lines of the set $\left\{\ell_{p,q} : q \in \mathbb{R}^2\right\}$ are skew.*

Proof. Let $q_1, q_2 \in \mathbb{R}^2$. One hand that if ℓ_{p,q_1} and ℓ_{p,q_2} are parallel then by Lemma 4.4(i) we have that $q_1 = q_2$ and hence the lines are equal. On the other hand, if ℓ_{p,q_1} and ℓ_{p,q_2} are not parallel they have non-empty intersection if and only if $|p - q_1| = |p - q_2|$ so that $\ell_{p,q_1} = \ell_{p,q_2}$. ■

Lemma 4.5. *$Q(P)$ can be written as the disjoint union of*

$$Q(P)_{para} = \left\{(p, q, r, s) \in P^4 : \ell_{p,r} \mid\mid \textit{and } p \neq q\right\}$$

and

$$Q(P)_{inter} = \left\{(p, q, r, s) \in P^4 : \ell_{p,r} \cap \ell q, s \neq \emptyset \textit{ and } p \neq q\right\}.$$

Proof. Suppose that $(p, q, r, s) \in Q(P)$ and $(p, q, r, s) \not\subset Q(P)_{para}$ then $|p - q| = |r - s|$ where $p \neq q$ and $\ell_{p,r}$ is not parallel $\ell_{q,s}$. This implies that $\ell_{p,r} \cap \ell_{q,s} \neq \emptyset$ and thus $(p, q, r, s) \in P^4$. Hence $Q(P) \subset Q(P)_{para} \cup Q(P)_{inter}$.

On the other hand, $(p, q, r, s) \in Q(P)_{para}$ and $\ell_{p,r}$ is parallel $\ell_{q,s}$ and $p \neq q$. This means $p - q = r - s$ and $p \neq q$ and $|p - q| = |r - s|$. Finally we get $(p, q, r, s) \in Q(P)$. Therefore $Q(P)_{para} \subset Q(P)$. Also, $(p, q, r, s) \in Q(P)_{inter}$ implies the lines $\ell_{p,r}$ and $\ell_{q,s}$ intersect and are not parallel so that $|p - q| = |r - s|$ and therefore $(p, q, r, s) \in Q(P)$ and thus $Q(P)_{inter} \subset Q(P)$. Thus $Q(P) \supset Q(P)_{inter} \cup Q(P)_{inter}$ and hence $Q(P) = Q(P)_{para} \cup Q(P)_{inter}$.

To show that the union is disjoint, pick $(p, q, r, s) \in Q(P)_{para} \cap Q(P)_{inter}$. This means that $\ell_{p,r}$ is parallel to $\ell_{q,s}$ and both lines intersect with $p \neq q$. Thus the lines are equal and so $p = q$ which is a contradiction. ■

Lemma 4.6. *Let P be a set of N points in the plane and let $\mathfrak{L} = \mathfrak{L}(P)$. Let*

$$\Lambda = \left\{(L_1, L_2) \in \mathfrak{L}^2 : L_1 \cap L_2 \neq \emptyset \textit{ and } L_1 \neq L_2\right\}.$$

If $Q(P)_{inter}$ is defined as in above lemma, then $|Q(P)_{inter}| = |\Lambda|$.

Proof. We define a map $\Phi : Q(P)_{inter} \to \Lambda$ by $\Phi(p,q,r,s) = (\ell_{p,r}, \ell_{q,s})$. This map is a bijection.Indeed, it is injective since if $\Phi(p,q,r,s) = \Phi(p',q',r',s')$ then $(\ell_{p,r}, \ell_{q,s}) = (\ell_{p',r'}, \ell_{q',s'})$ so that $p = p'$, $r = r'$, $q = q'$ and $s = s'$ and thus the map is injective. Φ is also surjective since $(L_1, L_2) \in \Lambda$ then $L_1 = \ell_{p,r}$, $L_2 = \ell_{q,s}$, $L_1 \cap L_2 \neq \emptyset$ and $L_1 \neq L_2$. Since $L_1 \cap L_2 \neq \emptyset$ and $L_1 \neq L_2$ then L_1 and L_2 are not parallel and therefore $|p-q| = |r-s|$ and $p \neq q$ and $\ell_{p,r} \cap \ell_{q,s} \neq \emptyset$. This means $(p,q,r,s) \in Q(P)_{inter}$ and $(L_1, L_2) = \Phi(p,q,r,s)$. Since Φ is a bijection, $|Q(P)_{inter}| = |\Lambda|$. ■

Definition. *Suppose that $\mathfrak{L}$ is a set of lines in $\mathbb{R}^3$ and $\rho > 2$ is an integer. We set*

$$\boxed{P_\rho(\mathfrak{L}) = \Big\{x \in \mathbb{R}^3 : x \textit{ belongs to at least } \rho \textit{ lines of } \mathfrak{L}\Big\}}$$

and

$$P_{=\rho}(\mathfrak{L}) = \{x \in \mathbb{R}^3 : x \textit{ belongs to exactly } \rho \textit{ lines of } \mathfrak{L}\}.$$

We note that $P_{=\rho}(\mathfrak{L}) = P_\rho(\mathfrak{L}) \setminus P_{\rho+1}(\mathfrak{L})$.

Claim. *Suppose P is a set of N points in the plane let $\mathfrak{L} = \mathfrak{L}(P)$. If $P_\rho(\mathfrak{L}) \neq \emptyset$ then $\rho \leq N$.*

Proof. Let $x \in \mathbb{R}^3$. Given a $p \in P$, then Corollary 4.4.1 tells us that x belongs to at most one line from the set $\big\{\ell_{p,q} : q \in \mathbb{R}^2\big\}$. Since there are N such sets (one for each $q \in P$), x belongs to at most N lines from $\mathfrak{L}$. Therefore $P_\rho(\mathfrak{L}) \neq \emptyset$ implies $\rho \leq N$. ■

Lemma 4.7. *Suppose that P is a set of N points in the plane and let $\mathfrak{L} = \mathfrak{L}(P)$. If Λ is defined as in Lemma 4.6 then we have*

$$|\Lambda| \leq \sum_{\rho=2}^{N} 2(\rho-1) P_\rho(\mathfrak{L}).$$

Proof. Define $\Psi : \Lambda \to \bigcup_{\rho=2}^{N} P_\rho(\mathfrak{L})$ by $\Psi(L_1, L_2) = L_1 \cap L_2$. We let $\Lambda_\rho = \Psi^{-1}(P_{=\rho}(\mathfrak{L}))$. Then the map $\Psi|_{\Lambda_\rho} : \Lambda_\rho \to P_{=\rho}(\mathfrak{L})$ is a $\binom{\rho}{2} = \rho(\rho-1)$-to-one map. Therefore, $|\Lambda_\rho| = \rho(\rho-1)|P_{=\rho}(\mathfrak{L})|$. Since it Λ is the disjoint union of the Λ_ρ's it follows that

$$\begin{aligned}
|\Lambda| &= \sum_{\rho=2}^{N} |\Lambda_p| = \sum_{\rho=2}^{N} \rho(\rho-1)|P_{=\rho}(\mathfrak{L})| = \sum_{\rho=1}^{N} \rho(\rho-1)|P_\rho(\mathfrak{L}) \setminus P_{\rho+1}(\mathfrak{L})| \\
&= \sum_{\rho=2}^{N} \rho(\rho-1)\big(|P_\rho(\mathfrak{L})| - |P_{\rho+1}(\mathfrak{L})|\big) = \sum_{\rho=2}^{N} \rho(\rho-1)|P_\rho(\mathfrak{L})| - \sum_{\rho=2}^{N} \rho(\rho-1)|P_{\rho+1}(\mathfrak{L})| \\
&= \sum_{\rho=2}^{N} \rho(\rho-1)|P_\rho(\mathfrak{L})| - \sum_{\rho=3}^{N+1} (\rho-1)(\rho-2)|P_\rho(\mathfrak{L})| \\
&= \sum_{\rho=2}^{N} \rho(\rho-1)|P_\rho(\mathfrak{L})| - \sum_{\rho=2}^{N} (\rho-1)(\rho-2)|P_\rho(\mathfrak{L})| \\
&= \sum_{\rho=2}^{N} 2(\rho-1)|P_\rho(\mathfrak{L})|.
\end{aligned}$$

Which is the desired result. ■

Theorem 4.8. *If P is a subset of the plane with N points and $\mathfrak{L} = \mathfrak{L}(P)$ then*

$$|Q(P)| \leq N^3 + \sum_{\rho=2}^{N} 2(\rho-1)|P_\rho(\mathfrak{L})|.$$

Proof. Using Lemma 4.5 we have $|Q(P)| = |Q(P)_{\text{para}}| + |Q(P)_{\text{inter}}|$. Clearly, $|Q(P)_{\text{para}}| \leq |P \times P \times P| = N^3$. On the other hand, by the above lemma we have

$$|Q(P)_{\text{inter}}| \leq \sum_{\rho=2}^{N} 2(\rho-1)P_\rho(\mathfrak{L}),$$

and the result follows. ∎

4.3 Lines in $\mathbb{R}^n$ and Algebraic Surfaces

Definition. *A regulus is a quadratic sufrace in $\mathbb{R}^3$ which is doubly ruled, that is each point in the surface lies in two lines in the surface.*

An example of such a surface is $\{(x, y, z) \in \mathbb{R}^3 : z = xy\}$. Any point (a, b, c) in the surface lies in the lines

$$\begin{cases} x = a \\ z = ay \end{cases} \qquad\qquad \begin{cases} y = b \\ z = xb \end{cases}$$

both of which are subsets of that surface.

Theorem 4.9 (Guth-Katz, 2010)**.** *To every constant B there is a constant C such that if $\mathfrak{L}$ is a set of L lines in $\mathbb{R}^3$ with at most $B\sqrt{L}$ lines in any plane or regulus, then*

$$|P_r(\mathfrak{L})| \leq CL^{\frac{3}{2}}r^{-2} \quad \textit{for} \quad r = 2, 3, \ldots, \lfloor\sqrt{L}\rfloor.$$

Corollary 4.9.1. *Theorem 4.9 implies Theorem 4.1.*

Proof. By Theorem 4.8,

$$|Q(P)| \leq N^3 + \sum_{\rho=2}^{N} 2(\rho-1)|P_\rho(\mathfrak{L})|.$$

We have that $|\mathfrak{L}(P)| = N^2$. In addition, Lemma 4.11, tells us that $\mathfrak{L}(P)$ satisfies the conditions of Theorem 4.9. Therefore, Theorem 4.9 tells us that

$$|P_r(\mathfrak{L})| \leq \frac{CL^{\frac{3}{2}}}{r^2} \quad \text{for} \quad 2 \leq r \leq \sqrt{L} = N,$$

and using Lemma 4.3 we get

$$\begin{aligned} |Q(P)| &\leq N^3 + \sum_{r=2}^{N} 2(r-1)\frac{CN^3}{r^2} \leq N^3 + 2CN^3 \sum_{r=2}^{N} \frac{1}{r} \leq N^3 + 2CN^3 \int_1^N \frac{1}{t}dt \\ &= N^3 + 2CN^3 \ln(N) \leq (1+2C)N^3 \ln(N). \end{aligned}$$

Combining this with Lemma 4.3 we get that

$$(N^2 - N)^2 \leq |d(P)||Q(P)| \leq (1 + 2C)(N^3 \ln(N))|d(P)|,$$

and hence

$$|d(P)| \geq \frac{1}{1+2C} \cdot \frac{N^4 - 2N^3 + N^2}{N^3 \ln(N)} \geq C_1 \frac{N^4}{N^3 \ln(N)} = C_1 \frac{N}{\ln(N)},$$

as conjectured. ■

Here is a weaker version of Theorem 4.1.

Theorem 4.10 (Guth, 2014)**.** *For every $\epsilon > 0$, there are constants C_ϵ and K_ϵ such that if $\mathfrak{L}$ is a set of L lines in $\mathbb{R}^3$ with less than $L^{\frac{1}{2}+\epsilon}$ lines in any irreducible algebraic surface of degree at most D_ϵ then*

$$|P_r(\mathfrak{L})| \leq K_\epsilon \frac{L^{\frac{3}{2}+\epsilon}}{r^2} \quad \text{for} \quad r = 2, 3, \ldots, \lfloor \sqrt{L} \rfloor.$$

Corollary 4.10.1. *Lemma 4.11 and Theorem 4.10 imply Theorem 4.2.*

Proof. We have

$$\begin{aligned}
|Q(P)| &\leq N^3 + \sum_{r=1}^{N} 2(r-1)|P_r(\mathfrak{L})| && \text{(by Theorem 4.6)} \\
&\leq N^3 + 2K_\epsilon (N^2)^{\frac{3}{2}+\epsilon} \sum_{r=2}^{N} \frac{r-1}{r^2} && \text{(by Theorem 4.8)} \\
&\leq N^3 + 2K_\epsilon N^{3+2\epsilon} \sum_{r=1}^{N} \frac{1}{r} \leq N^3 + 2K_\epsilon N^{3+2\epsilon} \ln(N) \\
&\leq N^{3+3\epsilon} + 2\frac{K_\epsilon}{\epsilon} N^{3+3\epsilon} = \left(1 + 2\frac{K_\epsilon}{\epsilon}\right) N^{3+3\epsilon}.
\end{aligned}$$

Hence by Lemma 4.3 we get

$$(N^2 - N)^2 \leq \underbrace{\left(1 + 2\frac{K_\epsilon}{\epsilon}\right)}_{\text{write as } 1/\bar{K}_\epsilon} N^{3+3\epsilon} |d(P)|,$$

and thus

$$|d(P)| \geq \bar{K}_\epsilon \frac{N^4}{N^{3+3\epsilon}} = \bar{K}_\epsilon N^{1-\epsilon},$$

which is the desired result. ■

4.4 Non-Clustering Lemma

In the above proof we have used the following lemma, also called the "Non-Clustering Lemma". It says the following.

Lemma 4.11 (Non-Clustering Lemma)**.** *To every integer $D \geq 1$, there is a constant C_D such that if $P \subset \mathbb{R}^2$ is a set of N points then $\mathfrak{L}(P)$ contains at most $C_D N$ lines in any algebraic surface of degree at most D.*

We now state several results needed to prove Lemma 4.11.

Lemma 4.12. *Fix $p = (p_1, p_2) \in \mathbb{R}^2$. To every point $(x, y, z) \in \mathbb{R}^3$, there is a unique point $q \in \mathbb{R}^2$ such that (x, y, z) belongs to the unique line $\ell_{p,q} \in \mathfrak{L}_p$. Also, if*

$$V_p(x, y, z) := (p_2 - y - p_1 z,\ x - p_1 - p_2 z,\ 1) + z(x, y, z). \tag{3}$$

then $V_p(x, y, z)$ is tangent to $\ell_{p,q}$.

Proof. For part (i), notice that

$$\begin{aligned}
(x,y,z) \in \ell_{p,q} &\iff \begin{cases} x = \frac{p_1+q_1}{2} + \frac{p_2-q_2}{2}t \\ y = \frac{p_2+q_2}{2} + \frac{q_1-p_1}{2}t \\ z = t \end{cases} \iff \begin{cases} q_1 - 2q_2 = 2x - p_1 - p_2 z \\ zq_1 + q_2 = 2y - p_2 + p_1 z \end{cases} \\
&\iff q_1 = \frac{\begin{vmatrix} 2x - p_1 - p_2 z & -z \\ 2y - p_2 + p_1 z & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -z \\ z & 1 \end{vmatrix}}, \quad q_2 = \frac{\begin{vmatrix} 1 & 2x - p_1 - p_2 z \\ z & 2y - p_2 + p_1 z \end{vmatrix}}{\begin{vmatrix} 1 & -z \\ z & 1 \end{vmatrix}} \\
&\iff \begin{cases} (1+z^2)q_1 = 2x - p_1 - 2p_2 z + 2yz + p_1 z^2 \\ (1+z^2)q_2 = 2y - p_2 + 2p_1 z - 2xz + p_2 z^2 \end{cases}
\end{aligned}$$

It is easy to see that this system has a unique solution $q = (q_1, q_2)$. As for part (ii), notice that a vector parallel to $\ell_{p,q}$ is

$$\begin{aligned}
(1+z^2)\left(\frac{p_2 - q_2}{2}, \frac{q_1 - p_1}{2}, 1\right) &= \left(\frac{p_2 + p_2 z^2 - (1+z^2)q_2}{2}, \frac{(1+z^2)q_1 - p_1 - p_1 z^2}{2}, 1 + z^2\right) \\
&\ \ \vdots \\
&= (p_2 - y - p_1 z + xz, x - p_1 - p_2 z + yz, 1 + z^2) \\
&= (p_2 - y - p_1 z, x - p_1 - p_2 z, 1) + z(x, y, z),
\end{aligned}$$

then V_p evaluated at (x, y, z) is tangent to the unique line $\ell_{p,q}$ passing through (x, y, z). ∎

The next lemma that we state and prove implies Lemma 4.11. This fact is left for the reader as an exercise.

Lemma 4.13. *Suppose that $D \geq 2$ is an integer and $Q \in \mathcal{P}_D(\mathbb{R}^3)$ is irreducible. Set $\mathfrak{L}_p = \{\ell_{p,q} : q \in \mathbb{R}^2\}$ where $\ell_{p,q}$ is defined in (1). Then the set*

$$E = \left\{p \in \mathbb{R}^2 : Z(Q) \text{ contains greater than or equal to } 2D^2 \text{ lines of } \mathfrak{L}_p\right\}$$

contains at most one point.

The proof of Lemma 4.13 require several basic ideas from differential geometry and algebraic geometry. One of which is the *Bézout Theorem for Lines* which is stated as follows.

Theorem 4.14 (Bézout's Theorem for Lines)**.** *If $P, Q \in \mathbb{R}[x, y, z]$ have no common factors, then*

$$\#\text{ of lines in } Z(P) \cap Z(Q) \ \leq (\deg P)(\deg Q).$$

Proof. See Section 5.2. ∎

Proof of Lemma 4.13. The proof is divieded into three steps.

Step 1: $V_p \cdot \nabla Q$ vanishes on $Z(Q)$ for all $p \in E$.

For all $p \in E$, we have $V_p \cdot \nabla Q$ vanishes on $Z(Q)$. Indeed, let $p \in E$ then we have that $Z(Q)$ contains $\ell_1, \ldots, \ell_m \in \mathfrak{L}_p$ with $m \geq 2D^2$. Fix j between 1 and m. Since Q vanishes on ℓ_j, if follows that

$$\nabla Q(x, y, z) \cdot v_j = 0 \text{ for all } (x, y, z) \in \ell_j,$$

where v_j is directional vector of the line ℓ_j. But v_j and $V_p(x, y, z)$ are parallel so that

$$\nabla Q(x, y, z) \cdot V_p(x, y, z) = 0 \text{ for all } (x, y, z) \in \ell_j.$$

This means that the polynomial $V_p \cdot \nabla Q$ vanishes on ℓ_j since $V_p \cdot \nabla Q$ is a polynomial of degree at most $D + 1$. Therefore $V_p \cdot \nabla Q$ vanishes on all $\ell_1, \ldots, \ell_m$.

Now we have that Q and $V_p \cdot \nabla Q$ have a common factor since if we suppose they don't, then both Q and $V_p \cdot \nabla Q$ vanish on the lines $\ell_1, \ldots, \ell_m$ and by above theorem we have $m \leq (\deg Q)(\deg V_p \cdot \nabla Q)$ but $m \geq 2D^2$ so $2D^2 \leq D^2 + D$ and thus $D \leq 1$ which contradicts our assumption that $D \geq 2$. Since Q is irreducible, we have that Q divides $V_p \cdot \nabla Q$. This implies that $V_p \cdot \nabla Q$ vanishes on $Z(Q)$.

Step 2: ∇Q does not vanish on $Z(Q)$.

Suppose that ∇Q vanishes on $Z(Q)$ then $\partial_i Q$ and Q have a common factor. Indeed, for suppose they don't. Then $Z(Q)$ has at most $(\deg P) \cdot (\deg \partial_i Q)$ lines. But we already know that Q vanishes on $\ell_1, \ldots, \ell_m$ which are $2D^2$ lines. So $2D^2 \leq D(D - 1)$ and thus $D^2 \leq D$ which is absurd. Now Q being irreducible tells us that it divides $\partial_i Q$. But $\partial_i Q$ having degree less than that of Q can only be the zero polynomial, implying that $\deg Q = 0$ which is a contradiction.

Step 3: If E contains two points then there is some $x_0 \in Z(P)$ such that infinitely many lines are contained in $Z(Q)$ and $T_{\mathbf{x}_0} Z(Q)$.

We assume that E contains two distinct points p and $\tilde{p}$ and obtain a contradiction.

Let $\mathbf{x}_0 \in Z(Q)$ be a non-singular point, that is $\nabla Q(\mathbf{x}_0)$ is not zero. Such a point is guaranteed to exist by Step 2. By the Implicit Function Theorem, $\mathbf{x}_0$ has a smooth neighbourhood $U_{\mathbf{x}_0} \subset Z(Q)$ where ∇Q never vanishes. Now define V_p and $V_{\tilde{p}}$ as in (3). Notice that if $t \in \mathbb{R}$ and $p_t = (1-t)p + t\widetilde{p}$ then

$$V_{p_t} = V_{(1-t)p+t\tilde{p}} = (1 - t)V_p + tV_{\tilde{p}},$$

and therefore

$$V_{p_t} \cdot \nabla Q = (1 - t)V_p \cdot \nabla Q + tV_{\tilde{p}} \cdot \nabla Q,$$

and hence $V_{p_t} \cdot \nabla Q$ vanishes on $U_{\mathbf{x}_0} \subset Z(Q)$ by Step 1. This combined with the fact that ∇Q doesn't vanish on $U_{\mathbf{x}_0}$ tells us that V_{p_t} is a vector field on $U_{\mathbf{x}_0}$ for all t. Therefore the integral curve of this vector field that passes through $\mathbf{x}_0$ intersects U_{x_0} (and hence $Z(Q)$) infinitely often. But this integral curve is the unique line from $\mathfrak{L}_{p_t}$ that passes through $\mathbf{x}_0$ as shown in Lemma 4.12 and thus it is contained in $Z(Q)$ by Lemma 1.5. Now if $t_1 \neq t_2$ then $\mathfrak{L}_{p_{t_1}} \cap \mathfrak{L}_{p_{t_2}} = \emptyset$ therefore by varying t we obtain infinitely many lines passing through $\mathbf{x}_0$ and entirely contained in $Z(Q)$. Also, each of these lines lie in the tangent plane $T_{\mathbf{x}_0}Z(Q)$ as shown in Lemma 4.12.

Conclusion: We have found a point $\mathbf{x}_0$ in Step 3, such that $T_{\mathbf{x}_0}Z(Q)$ and $Z(Q)$ contain infinitely many lines in common. So let $P \in \mathcal{P}_1(\mathbb{R}^3)$ be the polynomial such that $Z(P) = T_{\mathbf{x}_0}Z(Q)$. By the converse of Theorem 4.14 we get that Q and P have a common factor[1]. But Q is irreducible, so Q divides P and hence $\deg Q \leq 1$ which is a contradiction. Therefore our assumption that E contains two points is wrong and hence E contains at most one point. ■

[1] $Z(P)$ and $Z(Q)$ share infinitely many lines and therefore the number of lines in $Z(P) \cap Z(Q)$ is strictly greater than $(\deg P) \cdot (\deg Q)$.

5 The Bézout Theorem

Our goals in this section are to prove the Bézout theorem in the plane and the Bézout Theorem for lines used in the proof of Lemma 4.13.

5.1 Bézout's Theorem in the Plane

Theorem 5.1 (Bézout's Theorem in the Plane)**.** *Suppose $\mathbb{F}$ is a field and $P, Q \in \mathcal{P}(\mathbb{F}^2)$ are polynomials. Let $Z(P,Q) = \{(x,y) \in \mathbb{F}^2 : P(x,y) = Q(x,y) = 0\}$. If P and Q have no common factors, then $|Z(P,Q)| \le (\deg P) \cdot (\deg Q)$.*

We need several lemmas before proving this theorem.

Lemma 5.2. *Suppose $\mathbb{F}$ is a field and $X \subset \mathbb{F}^n$ is a finite set. Let $f : X \to \mathbb{F}$ be a function, then there is a polynomial $p \in \mathcal{P}(\mathbb{F}^n)$ such that*

(i) $\deg P \le |X| - 1$.

(ii) $P = f$ *on* X.

Proof. Let $p \in X$. We're going to construct a polynomial $P_p \in \mathcal{P}(\mathbb{F}^n)$ such that $\deg P_p \le |X| - 1$, $P_p(p) = 1$ and $P_p(q) = 0$ for all $q \in X \setminus \{p\}$. Let $q \in X \setminus p$, then q has coordinate which is different from p, say q_j and $1 \le j \le n$. Define the polynomial $L_q(\mathbf{x}) = x_j - q_j$ then $L_q(q) = 0$ and $L_p(q) \neq 0$. Define

$$P_p(\mathbf{x}) = C \prod_{q \in X \setminus \{p\}} L_q(\mathbf{x})$$

and observe that $\deg P = |X| - 1$, $P_p(q) = 0$ and choosing C appropriately we get that $P_p(p) = 1$. Finally, we construct P using the P_p's by

$$P(\mathbf{x}) = \sum_{p \in X} f(p) P_p(\mathbf{x})$$

and P has the desired properties. ∎

Definition. *Suppose $I \subset \mathcal{P}(\mathbb{F}^n)$ is an ideal and $D \ge 0$ is an integer. We define*

$$Z(I) = \{\mathbf{x} \in \mathbb{F}^n : P(\mathbf{x}) = 0 \textit{ for all } P \in I\} \quad \textit{and} \quad I_D = I \cap \mathcal{P}_D(\mathbb{F}^n). \tag{4}$$

We note that the injective linear map that goes from $\mathcal{P}_D(\mathbb{F}^n)/I_D$ to $\mathcal{P}(\mathbb{F}^n)/I$ and takes $P + I_D \to P + I$ allows us to view $\mathcal{P}_D(\mathbb{F}^n)/I_D$ as a vector subspace of $\mathcal{P}(\mathbb{F}^n)/I$ over the field $\mathbb{F}$.

Lemma 5.3. *Suppose that $I \subset \mathcal{P}(\mathbb{F}^n)$ is an ideal then $|Z(I)| \le \mathrm{Dim}(\mathcal{P}(\mathbb{F}^n)/I)$.*

Proof. We show that if $X \subset Z(I)$ which is finite, then $|X| \le \mathrm{Dim}(\mathbb{F}^n)/I$. Define the map

$$\Phi : \mathcal{P}(\mathbb{F}^n) \to \mathbb{F}^X \text{ such that } \Phi(P) = P|_X.$$

Above lemma tells us that Φ is surjective. Also, $I \subset \ker \Phi$ so $\Phi : \mathcal{P}(\mathbb{F}^n)/I \to \mathbb{F}^X$ becomes a surjective map so that $|X| = \mathrm{Dim}\, F^X \le \mathrm{Dim}(\mathcal{P}(\mathbb{F}^n)/I)$. ∎

Definition. *We use the following notation. For $P, Q \in \mathbb{F}[x, y, z]$ we set*

$$(P, Q) = \left\{P_1P + Q_1Q : P_1, P_2 \in \mathbb{F}(x, y, z)\right\},$$

and

$$Z(P, Q) = \{x \in \mathbb{F}^n : P_1P + Q_1Q = 0\}.$$

Notice that $Z(P, Q) = Z(P) \cap Z(Q)$.

Lemma 5.4. *Let $P \in \mathbb{F}[x_1, \ldots, x_n]$ be a non zero polynomial. Let $D \geq \deg P$ be an integer. Let $J = (P)$ be the ideal generated by P then*

$$\operatorname{Dim} \mathcal{P}_{D-\deg P}(\mathbb{F}^n) = \operatorname{Dim}(J_D).$$

Proof. Define a linear map $\Phi : \mathcal{P}_{D-\deg P} \to J_D$ by $\Phi(R) = PR$. Since P is non zero, $\ker \Phi$ is trivial and the map is injective. Also $S \in J_D$ implies $S = PR$ for some $R \in \mathcal{P}_{D-\deg P}(\mathbb{F}^n)$. So $S = \Phi(R)$ and thus the map is surjective. ■

Lemma 5.5. *Let $P \in \mathcal{P}(\mathbb{F}^n)$ be a non-zero polynomial and $D \geq \deg P$ be an integer. Let $J = (P)$ then*

$$\operatorname{Dim}(\mathcal{P}_D(\mathbb{F}^n)/J_D) = \binom{D+n}{n} - \binom{D - \deg P + n}{n}.$$

Proof. We define a linear map $\alpha : \mathcal{P}_D(\mathbb{F}^n) \to \mathcal{P}_D(\mathbb{F})^n/J_D$ given by $\alpha(R) = R + J_D$. Then clearly, α is surjective and $\ker \alpha = J_D$ so $\operatorname{Dim}(\operatorname{Im} \alpha) = \operatorname{Dim}(\mathcal{P}_D(\mathbb{F}^n)) - \operatorname{Dim}(\ker \alpha)$ by Rank-Nullity. Since

$$\operatorname{Dim}(\mathcal{P}_D(\mathbb{F}^n)) = \binom{D+n}{n} \text{ and } \operatorname{Dim} J_D = \binom{D - \deg P + n}{n}$$

and the map is surjective, the result follows. ■

Proposition 5.6. *Let $P, Q, R \in \mathcal{P}_D(\mathbb{F}^n)$ be polynomials such that P divides QR, P and Q are relatively prime. Then P divides R.*

The proof is left for the reader.

Lemma 5.7. *Let $P, Q \in \mathcal{P}(\mathbb{F}^n)$ be two relatively prime polynomials and let $D \geq \deg P$ be an integer. Let $I = (P)$ and $J = (P, Q)$ be the ideals generated by P, and P and Q respectively then*

$$\operatorname{Dim}(\mathcal{P}_D(\mathbb{F}^n/I_D)) \leq \operatorname{Dim}(\mathcal{P}_D(\mathbb{F}^n)/J_D) - \operatorname{Dim}(\mathcal{P}_{D-\deg Q}(\mathbb{F}^n)/J_{D-\deg Q}).$$

Proof. ■

Remark. *Let V be a vector space over a field $\mathbb{F}$ and let $\{V_D\}_{D\in\mathbb{N}}$ be an increasing sequence of subspaces of V such that $V = \bigcup_{D=1}^{\infty} V_n$. Then we have $\dim V = \lim_{D\to\infty} \dim V_D$.*

Proof. We have $\dim V_1 \leq \dim V_2 \leq \cdots \leq \dim V$ and so $\lim_{D\to\infty} \dim V_D \leq \dim V$. Set $L = \lim_{D\to\infty} \dim V_D$ and suppose that $\dim V > L$. Then V has n linearly independent vectors with $n > L$. Since $V = \bigcup_{D=1}^{\infty} V_D$ then there is an integer D_0 such that n linearly independent vectors belong to V_{D_0}. This a contradiction since we assumed that $\dim V_{D_0} \leq L < n$. Therefore we get $\dim V \leq L$ and thus $\dim V = L$. ■

proof of Theorem 5.1. Apply the above remark with $V = \mathbb{F}(x,y)/I$ and $V_D = \mathcal{P}_D(\mathbb{F}^2)/I_D$. We know that $\dim V_D \leq (\deg P)\cdot(\deg Q)$ and so

$$\dim V = \lim_{D\to\infty} \dim V_D \leq (\deg P)\cdot(\deg Q).$$

But by Lemma 5.3 we have $|Z(I)| \leq \dim V$ and thus $|Z(I)| \leq (\deg P)\cdot(\deg Q)$. ■

5.2 Bézout's Theorem for Lines

We now prove the Bézout theorem for lines. We need several lemmas to do so.

Lemma 5.8. *Let V be a vector space over an infinite field $\mathbb{F}$ and suppose $\operatorname{Dim} V \geq 2$ then V can't be written as finite union of one dimensional subspaces.*

Proof. Suppose that $V = \langle v_1\rangle \cup \langle v_2\rangle \cup \cdots \cup \langle v_n\rangle$ where $v_1, \ldots, v_n \in V$. Let e_1 and e_2 be two linearly independent elements in V. Then $e_1 \in \langle v_i\rangle$ and $e_2 \in \langle v_j\rangle$ where $i \neq j$. Consider the set $E = \{ae_1 + e_2 : a \in \mathbb{F}\}$ and note that $a \neq b$ if and only if $ae_1 + e_2 \neq be_1 + b_2$. By the Pigeonhole Principle, there are two different elements of E that fall in the same subspace $\langle v_k\rangle$ so that there are $a, b, a_1, b_1 \in \mathbb{F}$ such that $ae_1 + e_2 = a_1 v_k$ and $be_1 + e_2 = b_1 v_k$ so that

$$\left(\frac{a}{a_1} - \frac{b}{b_1}\right) e_1 + \left(\frac{1}{a_1} - \frac{1}{a_2}\right) e_2 = 0.$$

This means $a_1 = a_2$ and $ab_1 = ba_1$ and therefore $a = b$ contradicting our assumption. ■

Lemma 5.9. *Let $\mathbb{F}$ be an infinite field and V be a vector space over $\mathbb{F}$ with $n = \dim V \geq 2$. Then V can't be written as the finite union of proper subspaces of V.*

Proof. Suppose not, then $V = V_1 \cup \cdots \cup V_k$ where the V_i's are finite dimensional proper subspaces. If $e_1, \ldots, e_n$ are linearly independent vectors, then at least 2 of them will lie in different subspaces (or else $V = V_k$ for some k contradicting the proper assumption). Let e_i and e_j be those two vectors and let $W = \operatorname{span}\{e_1, e_2\}$. Let $W_k = W \cap V_k$ and therefore $W = \bigcup_{k=1}^n W_k$. Since $W_k \subset W$, $\dim W_k \leq 1$ ($\dim V_k \leq 1$ and not 2 since if $\dim W_k = 2$ for some k then $W_k = W$ and therefore $e_1, e_2 \in W_k$ contradicting the above). Hence W is a union of one dimensional subspaces contradicting the above lemma. ■

Let $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ be two vectors in $\mathbb{F}^n$. We equip $\mathbb{F}^n$ with the inner product

$$\langle \mathbf{x}, \mathbf{y}\rangle := \mathbf{x}\cdot\mathbf{y} := \sum_{i=1}^n x_i y_i.$$

Lemma 5.10. *Let $\mathbb{F}$ be an infinite field and $n \geq 2$. Let $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{F}^n$ be non zero vectors then there is a vector $\mathbf{y} \in \mathbb{F}^n$ such that $\mathbf{y}\cdot\mathbf{a}_i \neq 0$ for all $i = 1, \ldots, m$.*

Proof. Let $V_i = \{\mathbf{x} \in \mathbb{F}^n : \mathbf{a}_i \cdot \mathbf{x} = 0\}$. Since $\mathbf{a}_i \neq 0$, V_i is a proper subspace of $\mathbb{F}^n$. Suppose that no such $\mathbf{y}$ exists then $\mathbb{F}^n = \bigcup_{i=1}^m V_i$ which contradicts the above lemma. ■

Lemma 5.11 (Main Lemma)**.** *Suppose that $\mathbb{F}$ is an infinite field. Let $\ell_1, \ldots, \ell_m$ be lines in $\mathbb{F}^n$ and set $X = \ell_1 \cup \cdots \cup \ell_m$. Then to every integer $D > m$ there is a set $X_0 \subset X$ such that*

(i) $|X_0| = mD - m^2$.

(ii) *To every function* $f : X_0 \to \mathbb{F}$ *there is a polynomial* $p \in \mathcal{P}_D(\mathbb{F}^n)$ *such that* $P = f$ *on* X_0.

Proof. We let $a_1, \ldots, a_m$ be the directional vectors of $\ell_1, \ldots, \ell_m$, then $a_1, \ldots, a_m$ are non zero vectors in $\mathbb{F}^n$ and by the above lemma there is a $b \in \mathbb{F}^n$ such that $b \cdot a_i \neq 0$ for all $i = 1, \ldots, m$. This means that non of the lines $\ell_1, \ldots, \ell_m$ is parallel to the hyperplane $b \cdot x = 0$. We let $e_1, \ldots, e_m$ be the standard basis of $\mathbb{F}^n$. Define $T : \mathbb{F}^n \to \mathbb{F}^n$ such that

$$T(b) = e_n \text{ and } T(\{b \cdot x = 0\}) = \mathbb{F}^{n-1}.$$

We let $L_1, \ldots, L_m$ be $T\ell_1, \ldots, T\ell_m$ then non of these lines is parallel to $\mathbb{F}^{n-1}$. This implies that each hyperplane of the form $x_n = h$ ($h \in \mathbb{F}$) intersects each line L_i at exactly one point. In other words, x_n is transverse to L_i. We let $\overline{X} = L_1 \cup \ldots \cup L_m = TX$. Since $\mathbb{F}$ is infinite and $D - m > 0$, there is a set $\{h_1, \ldots, h_{D-m}\} \subset \mathbb{F}$ such that

$$|\left\{x_n = h_j\right\} \cap \overline{X}| = m \text{ for all } j = 1, \ldots, D - m.$$

Next we let

$$\overline{X}_0 = \bigcup_{j=1}^{D-m} \left\{x_n = h_j \cap \overline{X}\right\}$$

then clearly $|\overline{X}_0| = m(D - m) = mD - m^2$. We let $X_0 = T^{-1}\overline{X}_0$ then $X_0 \subset X$ and $|X_0| = |\overline{X}_0|$. Suppose we are given a function $f : X_0 \to \mathbb{F}$. We let $\bar{f} : \overline{X_0} \to \mathbb{F}$ be $\bar{f} = f \circ T^{-1}$. We are now going to find a polynomial $\bar{P} \in \mathcal{P}_D(\mathbb{F}^n)$ such that $\bar{P} = \bar{f}$ on $\overline{X}_0$ and defining $P = \bar{P} \circ T$ gives the desired polynomial since

$$P(x) = \bar{P} \circ T(x) = \bar{P}(Tx) = \bar{f}T(x) = f \circ T^{-1}(Tx) = f(x).$$

We now construct $\bar{P}$. Write

$$\left\{x_n = h_j\right\} \cap \overline{X} = \left\{(y_{k,j}, h_j) : k = 1, \ldots, m\right\}.$$

By lemma 5.2, we can find a polynomial $\overline{P}_j \in \mathcal{P}_m(\mathbb{F}^n)$ such that $\overline{P}_j(y_{k,j}) = \overline{f}(y_{k,j}, h_j)$. We need to find a polynomial

$$(*) \quad \overline{P}(y, h_j) = \overline{P}_j \quad \text{for} \quad j = 1, \ldots, D_m.$$

We expand

$$P_j(y) = \sum_{|\alpha| \le m} c_\alpha(j) y^\alpha \quad \text{and} \quad \overline{P}(y, x_n) = \sum_{|\alpha| \le m} P_j(x_n) y^\alpha$$

for $\overline{P}$ to satisfy $(*)$, we need $P_\alpha(h_j) = c_\alpha(j)$ for $j = 1, \ldots, D_m$. But we can get a polynomial P_α by applying Lemma 5.2. ■

Lemma 5.12 (Essential Lemma)**.** *Suppose that* $\mathbb{F}$ *is an infinite field. Let* $\ell_1, \ldots, \ell_m$ *be lines in* $\mathbb{F}^3$ *and* $P, Q \in \mathbb{F}[x, y, z]$ *be polynomials that vanish on* $X := \ell_1 \cup \cdots \cup \ell_m$. *Then to every integer* $D > m$, *if* $I_D = (P, Q) \cap \mathcal{P}_D(\mathbb{F}^3)$ *then*

$$\dim\left(\mathcal{P}_D(\mathbb{F}^3)/I_D\right) \ge mD - m^2.$$

Proof. Let X_0 be the set obtained from Lemma 5.11. Define the linear map $\Phi : \mathcal{P}_D(\mathbb{F}^3) \to \mathbb{F}^X$ by $\Phi(R) = R|_X$. By the proof of Lemma 5.11 we have $\mathbb{F}^{X_0} \subset \operatorname{Im}\Phi$ and

$$\dim(\operatorname{Im}\Phi) \geq \dim \mathbb{F}^{X_0} = |X_0| = mD - m^2.$$

Now let $R \in I_D$. Since both P and Q vanish on X then R vanishes on X then $\Phi(R) = 0$ and thus $I_D \subset \ker \Phi$. So Φ descends to a linear map from $\mathcal{P}_D(\mathbb{F}^3)/I_D$ to $\mathbb{F}^X$. Thus

$$\dim\left(\mathcal{P}_D(\mathbb{F}^3)/I_D\right) \geq \dim(\operatorname{Im}\Phi) \geq mD - m^2,$$

as desired. ■

Remark. Let $P, Q \in \mathbb{F}[x, y, z]$. Set $I = (P, Q)$ and $J = (P)$ and I_D and J_D as in (4). Then there is a constant C depending only on $\deg P$ such that

$$\dim\left(\mathcal{P}_D(\mathbb{F}^3)/I_D\right) \leq (\deg P)(\deg Q)D - \frac{1}{2}(\deg P)(\deg Q)^2 + C(\deg Q).$$

Proof. The proof is computational and so is left for the reader to check. ■

We are finally ready to prove Bézout's Theorem for Lines.

Theorem 5.13 (Bézout's Theorem for Lines)**.** *Suppose that $\mathbb{F}$ is an infinite field and suppose that $\ell_1, \dots, \ell_m$ are line in $\mathbb{F}^3$ and that $P, Q \in \mathbb{F}[x, y, z]$ are relatively prime polynomials that vanish on $\ell_1, \dots, \ell_m$. Then*

$$m \leq (\deg P)(\deg Q).$$

Proof. Fix any integer $D > m$. Combining the above remark with Lemma 5.12 we get that

$$mD - m^2 \leq (\deg P)(\deg Q)D - \frac{1}{2}(\deg P)(\deg Q)^2 + C(\deg Q).$$

Dividing by D on both sides and rearranging we get

$$m \leq (\deg P)(\deg Q) - \frac{1}{2D}(\deg P)(\deg Q)^2 + \frac{1}{D}C(\deg Q) + \frac{1}{2D}m^2.$$

Using the remark after Lemma 5.7 and letting $D \to \infty$ we get the desired result. ■

6 Polynomial Partitioning

6.1 Polynomial Ham Sandwich and Polynomial Partitioning

Theorem 6.1 (Lebesgue's Dominated Convergence). *Let $(X, \mathfrak{M}, \mu)$ be a measure space and suppose $\{f_n\}$ is a sequence of functions that converge pointwise on X to a function f. If there is a non-negative function $g \in L^1(\mu)$ such that $|f_n| \leq g$ for all n then $\lim_{n\to\infty} \int_X f_n d\mu = \int_X f d\mu$.*

For a proof of the above theorem see [**?**, **?**].

Lemma 6.2 (Continuity Lemma). *Suppose $(X, \mathfrak{M}, \mu)$ is a measure space and $\{f_n\}$ is a sequence of functions that converges pointwise on X to a function $f \in \mathcal{O}$. Let $w \in L^1(\mu)$ be such that*

$$\int_{\{f=0\}} w d\mu = 0 \quad \textit{then} \quad \int_{\{f_n>0\}} w d\mu \longrightarrow \int_{\{f>0\}} w d\mu.$$

Proof. First we notice that

$$\begin{aligned}\int_{\{f_n>0\}} w d\mu &= \int_{\{f_n>0\}\cap\{f>0\}} w d\mu + \int_{\{f_n>0\}\cap\{f<0\}} w d\mu \\ &= \int_X \left(\chi_{\{f_n>0\}}\, \chi_{\{f>0\}} + \chi_{\{f_n>0\}}\, \chi_{\{f<0\}}\right) w d\mu.\end{aligned}$$

We have that

$$\lim_{n\to\infty} \chi_{\{f_n>0\}}(x)\, \chi_{\{f>0\}}(x) = \begin{cases} 1 & \text{if } f(x) > 0, \\ 0 & \text{if } f(x) \leq 0. \end{cases}$$

and

$$\lim_{n\to\infty} \chi_{\{f_n>0\}}(x)\, \chi_{\{f<0\}}(x) = 0,$$

so that

$$\lim_{n\to\infty} \chi_{\{f_n>0\}}\, \chi_{\{f>0\}} + \chi_{\{f_n>0\}}\, \chi_{\{f<0\}} = \chi_{\{f>0\}}\,.$$

We have that

$$\left|\left(\chi_{\{f_n>0\}}\, \chi_{\{f>0\}} + \chi_{\{f_n>0\}}\ \ Chi_{\{f<0\}}\right) w\right| \leq w,$$

and w's integral over X is finite, so by Theorem 6.1 we get that

$$\lim_{n\to\infty} \int_{\{f_n>0\}} w d\mu = \lim_{n\to\infty} \int_X \chi_{\{f_n>0\}}\, w d\mu = \int_X \chi_{\{f>0\}}\, w d\mu = \int_{\{f>0\}} w d\mu,$$

which finishes the proof. ■

We recall a theorem of fundamental importance from algebraic topology.

Theorem 6.3 (Borsuk-Ulam). *Suppose $F : S^N \to \mathbb{R}^N$ is a continuous map. If $F(-u) = -F(u)$ for all $u \in S^N$, then there is a $v \in S^N$ such that $F(v) = 0$.*

For a proof, see [**?**, **?**]. The Borsuk-Ulam theorem is an essential ingredient in the proof of the following, equally important theorem.

Theorem 6.4 (General Ham Sandwish Theorem, Stone and Tukey, 1942)**.** *Suppose* $W_1, \ldots, W_N \in L^1(\mathbb{R}^n)$ *are functions and* V *is a subspace of* $\mathcal{O}_\mathbb{R}$ *of dimension greater than* N*. Suppose*

$$\int_{\{u=0\}} w_j d\lambda = 0 \text{ for all } u \in V \setminus \{0\} \text{ and } j = 1, \ldots, n.$$

Then there is a function $v \in V \setminus \{0\}$ *such that*

$$\int_{\{v>0\}} W_j d\lambda = \int_{\{v<0\}} W_j d\lambda.$$

Proof. Without loss of generality, suppose that $\operatorname{Dim} V = N+1$. We can identify V with $\mathbb{R}^{n+1}$ so that S^N can be seen as a subset of $V \setminus \{0\}$. We define $F : V \setminus \{0\} \to \mathbb{R}^N$ by setting the j'th coordinate to

$$F_j(u) = \int_{\{u>0\}} W_j d\lambda - \int_{\{u<0\}} W_j d\lambda.$$

Clearly F_j is antipodal and so F is antipodal. Since $\int_{\{u=0\}} W_j d\lambda = 0$ for all $u \in V \setminus \{0\}$, Lemma 6.2 tells us that F is continuous. By Theorem 6.3, there is a $v \in V \setminus \{0\}$ such that $F(v) = 0$ which finishes the proof. ∎

Corollary 6.4.1 (Polynomial Ham Sandwish Theorem)**.** *Let* $W_1, \ldots, W_N \in L^1(\mathbb{R}^n)$ *then to every integer* D *such that* $N < \binom{D+n}{n}$*, there is a polynomial* $P \in \mathcal{P}_D(\mathbb{R}^n)$ *such that*

$$\int_{\{P>0\}} W_j d\lambda = \int_{\{P<0\}} W_j d\lambda \quad \text{for} \quad j = 1, \ldots, N$$

Proof. Apply Theorem 6.4 to $V = \mathcal{P}_D(\mathbb{R}^n)$. We can do this since if P is any non zero polynomial in $\mathcal{P}_D(\mathbb{R}^n)$ then $\lambda(Z(P)) = 0$ and thus $\int_{Z(P)} f d\lambda = 0$ for all $f \in L^1(\mathbb{R}^n)$. ∎

Definition. Let $S \subset \mathbb{R}^n$ is finite and $P \in \mathbb{R}[x_1, \ldots, x_n]$ be a non zero polynomial. Then

1. if S is finite, we say that P bisects S if $|\{P < 0\} \cap S| \leq |S|/2$ and $|\{P > 0\} \cap S| \leq |S|/2$.

2. if S is infinite and has non-zero measure, we say that P bisects S if $\lambda\left(\{P < 0\} \cap S\right) = \lambda\left(\{P > 0\} \cap S\right) = \lambda(S)/2$.

Corollary 6.4.2. *Suppose that* $S_1, \ldots, S_N \subset \mathbb{R}^n$ *are finite sets. To every positive integer* D *satisfying* $N < \binom{D+n}{n}$ *there is a* $P \in \mathcal{P}_D(\mathbb{R}^n)$ *that bisects each* S_j*.*

Proof. Let $N_0 = \binom{D+n}{n} - 1$ then $N \leq N_0$ and $\binom{D+n}{n} = N_0 + 1$, so we can identify $\mathcal{P}_D(\mathbb{R}^n)$ with $\mathbb{R}^{N_0+1}$ with a map Φ. This allows us to have $S^{N_0} \underset{\Phi}{\subset} \mathcal{P}_D(\mathbb{R}^n) \setminus \{0\}$.
Now for each $\delta > 0$, we set

$$\Omega_{j,\delta} = \bigcup_{x \in S_j} B(x, \delta).$$

Then Corollary 6.4.1 provides us with a non zero polynomial $P_\delta \in \mathcal{P}_D(\mathbb{R}^n)$ that bisects each $\Omega_{j,\delta}$. In particular,

$$\lambda\left(\{P_\delta > 0\} \cap \Omega_{j,\delta}\right) = \lambda\left(\{P_\delta < 0\} \cap \Omega_{j,\delta}\right) = \frac{1}{2}\lambda(\Omega_{j,\delta}), \tag{5}$$

for all $j = 1, \ldots, N$.

It can be shown that for all $\delta > 0$, one can take $P_\delta \underset{\Phi}{\in} S^{N_0}$ and still satisfy the above property (ie the Euclidean norm of the vector containing the coefficients of P_δ is 1). Since S^{N_0} is compact, we can find a sequence of real positive numbers $\{\delta_m\}$ and polynomials $P_{\delta_m} \underset{\Phi}{\in} S^{N_0}$ such that $\delta_m \to 0$ and $P_{\delta_m} \to P \underset{\Phi}{\in} S^{N_0}$ as $m \to \infty$. This means that the coefficients of P_{δ_m} converge to the coefficients of P and thus P_{δ_m} converges to P locally uniformly on bounded subsets of $\mathbb{R}^n$. We claim that this P bisects each S_j. Indeed, suppose this was not the case. Then there is some index j such that $|\{P > 0\} \cap S_j| > |S_j|/2$. For any $\delta > 0$, we let

$$S_j^+ = \{P > 0\} \cap S_j \quad \text{and} \quad \Omega_{j,\delta}^+ = \bigcup_{x \in S_j^+} B(x, \delta).$$

Since $\{P > 0\}$ is open, there is some $\epsilon > 0$ such that

$$y \in \Omega_{j,\epsilon}^+ = \bigcup_{x \in S_j^+} B(x, \epsilon) \subset \{P > 0\},$$

and the above union is actually disjoint. Now, since P_{δ_m} converges to P uniformly on bounded sets, there an integer M such that for all $m \geq M$, we have $\delta_m < \epsilon$ and $P_{\delta_m}(y) > 0$ for all $y \in \Omega_{j,\epsilon}^+$. In other words we have $\Omega_{j,\delta_m}^+ \subset \Omega_{j,\epsilon}^+ \subset \{P_{\delta_m} > 0\}$. But then

$$\begin{aligned}
\lambda\left(\{P_{\delta_m} > 0\} \cap \Omega_{j,\delta_m}\right) &= \lambda(\Omega_{j,\delta_m}^+) = \lambda\left(\dot{\bigcup_{x \in S_j^+}} B(x, \delta_m)\right) \\
&= |S_j^+|\, \lambda\left(B(x, \delta_m)\right) > \frac{|S_j|}{2}\, \lambda\left(B(x, \delta_m)\right) \\
&= \frac{1}{2} \lambda(\Omega_{j,\delta_m}),
\end{aligned}$$

contradicting (5). ■

Corollary 6.4.3. *Let $S_1, \ldots, S_N \subset \mathbb{R}^n$ be finite sets then there is a positive integer D and a polynomial $P \in \mathcal{P}_D(\mathbb{R}^n) \setminus \{0\}$ such that*

$$\frac{D^n}{2^n n!} \leq N < \frac{D^n}{n!}$$

and P bisects each S_j.

Proof. We let $D = \min\left\{d \in \mathbb{N} : d^n/n! > N\right\}$ then $D^n/n! > N$ therefore $D^n > n!N \geq 1$ so that $D \geq 2$. But also, $(D-1)^n/n! \leq N$ and since $D - 1 \geq D/2$ then $(1/n!)(D/2)^n \leq N$.

Part (ii) is clear since $N < D^n/n! < \binom{D+n}{n}$ and we can get P from Corollary 6.4.2. ■

Lemma 6.5. *To every finite set $S \subset \mathbb{R}^n$, there is a sequence of integers $\{D_k\}$ and a sequence of polynomials $\{P_k\}$ in $\mathcal{P}_{D_k}(\mathbb{R}^n) \setminus \{0\}$ such that:*

(i) *For each $k \in \mathbb{N}$,*

$$\frac{D_k^n}{2^n (n!)} \leq 2^{k-1} < \frac{D_k^n}{n!}.$$

(ii) *For each $k \in \mathbb{N}$,*

$$\mathbb{R}^n \setminus Z(P_1 \dots P_k) = \bigcup_{\alpha_k \in I_k} \Omega^{\alpha_k},$$

where $I_k = \{+,-\}^k$ and the Ω^{α_k} are open and disjoint.

(iii) *For each $k \in \mathbb{N}$,*

$$|\Omega^{\alpha_k} \cap S| \le \frac{|S|}{2^k}$$

for all $\alpha_k \in I_k$.

Proof. We use induction. By Corollary 6.4.2 there is an integer $D_1 \in \mathbb{N}$ and $P_1 \in \mathcal{P}_{D_1}(\mathbb{R}^n) \setminus \{0\}$ such that

$$\frac{D_1^n}{2^n n!} \le 1 \le \frac{D_1^n}{n!} \text{ and } P \text{ bisects } S.$$

We let $\Omega^+ = \{P_1 > 0\}$ and $\Omega^- = \{P_1 < 0\}$ then

$$\mathbb{R}^n \setminus Z(P_1) = \Omega^+ \cup \Omega^- = \bigcup_{\alpha \in I_1} \Omega^{\alpha_1}$$

where $I_1 = \{+,-\}$ and $|\Omega^{\alpha_1} \cap S| \le S/|2|$.

Apply Corollary 6.4.2 again to get an integer $D \in \mathbb{N}$ and a polynomial $P_2 \in \mathcal{P}_{D_2}(\mathbb{R}^n) \setminus \{0\}$ such that

$$\frac{D_2^n}{2^n n!} \le 2 \le \frac{D_2^n}{n!} \text{ and } P_2 \text{ bisects } \Omega^{\alpha_1} \cap S.$$

Let $\Omega_2^+ = \{P_2 > 0\}$ and $\Omega_2^- = \{P_2 < 0\}$ then

$$\mathbb{R}^n \setminus Z(P_1 P_2) = Z(P_1)^c \cap Z(P_2)^c = \left(\bigcup_{\alpha_1 \in I_1} \Omega^{\alpha_1} \right) \cap \left(\Omega_2^+ \cup \Omega_2^- \right) = \bigcup_{\alpha_2 \in I_2} \Omega^{\alpha_2}$$

where $I_2 = \{+,-\}^2$ and $|\Omega^{\alpha_2} \cap S| \le |S|/2^2$. ∎

Theorem 6.6 (Polynomial Partitioning, Guth-Katz)**.** *To every finite set $S \subset \mathbb{R}^n$ and integer $D \in \mathbb{N}$ there is a polynomial $P \in \mathrm{Poly}_D(\mathbb{R}^n) \setminus \{0\}$ such that $\mathbb{R}^n \setminus Z(P)$ is a disjoint union of at most $2D^n$ open sets O_i each containing*

$$\le \frac{(2^{n+4})(n!)}{(2^{1/n} - 1)^n} \, |S| \, D^{-n}$$

points of S.

Proof. We have two cases.

<u>Case 1:</u> Consider the case when

$$1 \le D < \frac{2\sqrt[n]{n!}}{2^{1/n} - 1} 2^{5/n}.$$

Since $1 < \binom{1+n}{n}$, Corollary 6.4.2 provides us with a polynomial $P \in \mathrm{Poly}_1(\mathbb{R}^n) \setminus \{0\}$ satisfying

$$|\{P > 0\} \cap S|, \, |\{P < 0\} \cap S| \le \frac{|S|}{2}.$$

We let $O_1 = \{P > 0\}$ and $O_2 = \{P < 0\}$. Then O_1 and O_2 are open, and

$$\mathbb{R}^n \setminus Z(P) = O_1 \cup O_2 = \text{ disjoint union of two open sets.}$$

Also, $2 \leq 2D^n$ and hence

$$|O_i \cap S| \leq \frac{|S|}{2} = \Big(\frac{2\sqrt[n]{n!}\,2^{5/n}}{2^{1/n}-1}\Big)^n \frac{|S|}{2}\Big(\frac{2^{1/n}-1}{2\sqrt[n]{n!}\,2^{5/n}}\Big)^n < \frac{(2^{n+4})(n!)}{(2^{1/n}-1)^n}|S|D^{-n}.$$

Case 2: Suppose now that

$$\frac{2\sqrt[n]{n!}}{2^{1/n}-1}\,2^{5/n} \leq D.$$

We let

$$K = \max\Big\{k \in \mathbb{N} : \frac{2\sqrt[n]{n!}}{2^{1/n}-1}\,2^{k/n} \leq D\Big\}.$$

Then it is easy to see that $K \geq 5$ and that

$$\frac{2\sqrt[n]{n!}}{2^{1/n}-1}\,2^{K/n} \leq D < \frac{2\sqrt[n]{n!}}{2^{1/n}-1}\,2^{(K+1)/n}. \tag{6}$$

Let $\{D_k\}$ and $\{P_k\}$ be the sequences provided by Lemma 6.5 and define $P = P_1 \dots P_K$. Note that

$$\deg P = \sum_{k=1}^{K} \deg P_k \leq \sum_{k=1}^{K} D_K \leq \sum_{k=1}^{K} 2\sqrt[n]{n!}\,2^{(k-1)/n} = 2\sqrt[n]{n!}\frac{1-2^{K/n}}{1-2^{1/n}} < \frac{2\sqrt[n]{n!}}{2^{1/n}-1}\,2^{K/n} \leq D,$$

Let $\{O_i\} = \{\Omega^{\alpha_K} : \alpha_K \in I_K\}$ be defined as in Lemma 6.5. Then the O_i's are open and disjoint and

$$|O_i \cap S| = |\Omega^{\alpha_K} \cap S| \leq \frac{|S|}{2^K} = \frac{2|S|}{2^{K+1}}.$$

But by inequality (6) we have

$$\frac{(2^{1/n}-1)^n}{2^n(n!)}\,D^n < 2^{K+1},$$

and so

$$|O_i \cap S| < \frac{2|S|}{\frac{(2^{1/n}-1)^n}{2^n(n!)}D^n} = \frac{2^{n+1}(n!)}{(2^{1/n}-1)^n}\,|S|\,D^{-n}.$$

Also,

$$|\{i\}| \leq 2^K \leq \frac{(2^{1/n}-1)^n}{2^n(n!)}\,D^n < \frac{2}{2^n(n!)}\,D^n \leq D^n,$$

which concludes the proof. ■

6.2 Szémerdi-Trotter Theorem and Applications

Definition. *Let $\mathcal{S}$ denote a finite set points in the plane. Let $\mathfrak{L}$ denote a finite set of lines in the plane. Then*

$$I(\mathcal{S}, \mathfrak{L}) = \big\{(p,\ell) \in \mathcal{S} \times \mathfrak{L} : p \in \ell\big\}.$$

Each pair in $I(\mathcal{S}, \mathfrak{L})$ is called an *incidence* and the whole set is called the *the set of incidences.*

Lemma 6.7. *With $\mathcal{S}$ and $\mathfrak{L}$ defined as above,*

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

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

Proof. (i) We write

$$\begin{aligned} I(\mathcal{S}, \mathfrak{L}) &= \{(p, l) \in \mathcal{S} \times \mathfrak{L} : p \text{ lies in exactly one line of } \mathfrak{L}\} \\ &\quad \cup \{(p, l) \in \mathcal{S} \times \mathfrak{L} : p \text{ lies in at least two lines of } \mathfrak{L}\}. \end{aligned}$$

The points of the first set generate $\leq S$ incidences. A line $l \in \mathfrak{L}$ can pass through at most $L-1$ points from the second set, and hence produces $\leq L-1$ incidences. Therefore, the points of the second set generate $\leq L(L-1)$ incidences and thus $|I(\mathcal{S}, \mathfrak{L})| \leq S + L(L-1) \leq S + L^2$.

For part (ii), we write

$$\begin{aligned} I(\mathcal{S}, \mathfrak{L}) &= \{(p, l) \in \mathcal{S} \times \mathfrak{L} : l \text{ passes through exactly one point of } \mathcal{S}\} \\ &\quad \cup \{(p, l) \in \mathcal{S} \times \mathfrak{L} : l \text{ passes through at least two points of } \mathcal{S}\}. \end{aligned}$$

The lines of the first set generate $\leq L$ incidences. Also, a point $p \in \mathcal{S}$ can belong to at most $S-1$ lines from the second set, and hence produces $\leq S-1$ incidences. Therefore, the lines of the second set generate $\leq S(S-1)$ incidences and therefore,

$$|I(\mathcal{S}, \mathfrak{L})| \leq L + S(S-1) \leq L + S^2.$$

as desired. ∎

Theorem 6.8 (Szmerédi-Trotter)**.** *If $\mathcal{S}$ is a set of S points in the plane and $\mathcal{L}$ is a set of L lines in the plane then*

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

for some constant C independent of S and L.

Proof. Let's consider three cases.
If $L^2 \leq S$, then the result follows directly from Lemma 6.7 since

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

If $S^2 \leq L$ then also from Lemma 6.7 we have

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

For the rest of the proof, assume that $\sqrt{S} \leq L \leq S^2$. Let $D \in \mathbb{N}$ then Corollary 6.4.2 provides us with a non zero polynomial $P \in \mathcal{P}_D(\mathbb{R}^2)$ such that $\mathbb{R}^2 \setminus Z(P) = \dot\bigcup_i \mathcal{O}_i$ with $\mathcal{O}_i$ open, $2 \leq |\{i\}| \leq 2D^2$ and

$$|\mathcal{O}_i \cap \mathcal{S}| \leq \frac{2^6 2!}{(2^{1/2}-1)^2} \cdot \frac{S}{D^2} < 747\frac{S}{D^2}.$$

We will call the $\mathcal{O}_i$ cells. For each i, we let $\mathcal{S}_i = \mathcal{S} \cap \mathcal{O}_i$, $\mathfrak{L}_i = \left\{\ell \in \mathfrak{L} : \ell \cap \mathcal{O}_i \neq \emptyset\right\}$, $S_i = |\mathcal{S}_i|$ and $L_i = |\mathfrak{L}_i|$. We also let $\mathcal{S}_{cell} = \bigcup_i \mathcal{S}_i$ and $\mathcal{S}_{alg} = S \cap Z(P)$. It is clear that $\mathcal{S} = \mathcal{S}_{cell} \cupdot \mathcal{S}_{alg}$. Thus one can write

$$I(\mathcal{S}, \mathfrak{L}) = I(\mathcal{S}_{cell}, \mathfrak{L}) \cupdot I(\mathcal{S}_{alg}, \mathfrak{L})$$

so that

$$|I(\mathcal{S}, \mathfrak{L})| = |I(\mathcal{S}_{cell}, \mathfrak{L})| + |I(\mathcal{S}_{alg}, \mathfrak{L})|.$$

We start by estimating

$$\begin{aligned}
|I(\mathcal{S}_{cell}, \mathfrak{L})| &= \left|\dot{\bigcup_i} I(\mathcal{S}_i, \mathfrak{L})\right| = \sum_i |I(\mathcal{S}_i, \mathfrak{L})| \\
&= \sum_i |I(\mathcal{S}_i, \mathfrak{L}_i) \cup |I(\mathcal{S}_i, \mathfrak{L} \setminus \mathfrak{L}_i)| \\
&= \sum_i |I(\mathcal{S}_i, \mathfrak{L}_i) \cup \emptyset| && \text{(by the definition of } \mathfrak{L}_i) \\
&\leq \sum_i (L_i + S_i^2) && \text{(by lemma 6.6)} \\
&\leq \sum_i L_i + \sum_i S_i(747S/D^2) && \text{(since } \mathcal{S}_i < 747\frac{S}{D^2}) \\
&\leq \sum_i L_i + (747S/D^2) \sum_i S_i \\
&= \sum_i L_i + 747S^2/D^2 && \text{(since } \textstyle\sum_i S_i = S)
\end{aligned}$$

If a line intersects $Z(P)$ at $D+1$ points of a line then P vanishes on the line. So a line can enter at most $D+1$ of the cells $\mathcal{O}_i$. So that

$$\sum_i L_i \leq (D+1)L \quad \text{and therefore} \quad |I(\mathcal{S}_{cell}, \mathfrak{L})| \leq (D+1)L + 747S^2D^{-2}.$$

It remains to estimate $|I(\mathcal{S}_{alg}, \mathfrak{L})|$. Start by writing $\mathfrak{L} = \mathfrak{L}_{cell} \cup \mathfrak{L}_{alg}$. where $\mathfrak{L}_{alg}$ is the set of lines of $\mathfrak{L}$ that lie in $Z(P)$. The union is clearly disjoint, therefore

$$I(\mathcal{S}_{alg}, \mathfrak{L}) = I(\mathcal{S}_{alg}, \mathfrak{L}_{cell}) \cupdot I(\mathcal{S}_{alg}, \mathfrak{L}_{alg}).$$

Notice first that each line in $\mathfrak{L}_{cell}$ has at most D points of intersections with $Z(P)$, so each line in $\mathfrak{L}_{cell}$ has at most D incidences with $\mathcal{S}_{alg}$ and so $|I(\mathcal{S}_{alg}, \mathfrak{L}_{cell})| \leq DL$. Now there are at most D lines of $\mathfrak{L}$ that lie in $Z(P)$ so by lemma 6.6, $|I(\mathcal{S}_{alg}, \mathfrak{L}_{alg})| \leq S + D^2$.

Putting all of this together

$$\begin{aligned}
|I(\mathcal{S}, \mathfrak{L})| &\leq (D+1)L + 747S^2D^{-2} + DL + S + D^2 \\
&\leq (2D+1)L + 747S^2D^{-2} + S + D^2 \\
&\leq 3DL + 747S^2D^{-2} + S + D^2
\end{aligned}$$

It remains to find a D such that the main inequality holds. To do that, we want to minimize $y(D) = 3DL + 747S^2D^{-2}$. We start by computing the derivative of y,

$$y'(D) = 3L - \frac{(2)(747)}{D^3}\, S^2.$$

and we solve the equation $y'(D) = 0$ and we get $D^3 = \frac{498S^2}{L}$. Define

$$D = \min\left\{d \in \mathbb{N} : d^3 \geq \frac{498S^2}{L}\right\}.$$

then

$$D \geq \frac{\sqrt[3]{498} \cdot S^{2/3}}{L^{1/2}} \geq \sqrt[3]{498} > 7$$

and

$$D - 1 < 498\frac{S^2}{L} \quad \text{and thus} \quad D < 2\sqrt[3]{498}\frac{S^{2/3}}{L^{1/2}}$$

and thus

$$\begin{aligned}
|I(\mathcal{S}, \mathfrak{L})| &\leq \frac{6\sqrt[3]{498} \cdot S^{2/3}}{L^{1/3}} \cdot L + 747\left(\frac{L^{1/3}}{\sqrt[3]{498}} \cdot S^{2/3}\right)^2 S^2 + S + \left(\frac{2\sqrt[3]{498}S^{2/3}}{L^{1/3}}\right)^2 \\
&= 6\sqrt[3]{498} \cdot S^{2/3}L^{2/3} + \frac{747}{498^{2/3}} \cdot L^{2/3} \cdot S^{2/3} + S + \left(\frac{2\sqrt[3]{498}S^{2/3}}{L^{1/3}}\right)^2 \\
&\leq 63S^{2/3} \cdot L^{2/3} + S + \frac{4(64)S^{4/3}}{(\sqrt{s})^{2/3}} + (4)(498)^{1/3}L^{-2/3} \\
&= 63S^{2/3} \cdot L^{2/3} + S + 256S = 63S^{2/3} \cdot L^{2/3} + 257S \\
\therefore |I(\mathcal{S}, \mathfrak{L})| &\leq 63S^{2/3} \cdot L^{2/3} + 257S + S + L \\
&= 63S^{2/3}L^{2/3} + 258S + L \\
&\leq 258(S^{2/3}L^{2/3} + S + L)
\end{aligned}$$

which concludes the proof. ■

Corollary 6.8.1. *Let $\mathfrak{L}$ be a set of lines in the plane then*

$$|P_r(\mathfrak{L})| \leq (3C)^3\left(\frac{L^2}{r^3} + \frac{L}{r}\right)$$

where C is the constant from above theorem.

Proof. By Theorem 6.8 applied to $\mathcal{S} = P_r(\mathfrak{L})$ we have that

$$r|P_r(\mathfrak{L})| \leq \Big|I\left(P_r(\mathfrak{L}), \mathfrak{L}\right)\Big| \leq C\left(|P_r(\mathfrak{L})|^{2/3}L^{2/3} + |P_r(\mathfrak{L})| + L\right).$$

We consider three cases:

(i) Suppose $r|P_r(\mathfrak{L})| \leq 3C|P_r(\mathfrak{L})|^{2/3}L^{2/3}$ then $r|P_r(\mathfrak{L})|^{1/3} \leq 3CL^{2/3}$ so that $|P_r(\mathfrak{L})| \leq (3C)^3L^2r^{-3}$.

(ii) Suppose that $r|P_r(\mathfrak{L})| \leq 3CL$ then $|P_r(\mathfrak{L})| \leq 3CLr^{-1}$.

(iii) Suppose that $r|P_r(\mathfrak{L})| \leq 3C|P_r(\mathfrak{L})|$ then $r \leq 3C$ so that

$$|P_r(\mathfrak{L})| \leq \binom{L}{2} = \frac{L(L-1)}{2} \leq \frac{L^2}{2} \cdot \frac{3C^3}{3C^3} \leq \frac{3C^3}{2} \cdot \frac{L^2}{r^3},$$

which finishes the proof. ■

The reader is invited to employ ideas similar to the above to prove the following results.

Proposition 6.9. *Suppose that $\mathcal{S}$ is a set of S points in the plane and $\mathcal{C}$ be a set of C circles in the plane with same radius. Then*

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

This implies that if P is a set of N points in the plane then $|d(P)| \gtrsim N^{2/3}$.

Proposition 6.10. *Suppose that P is a set of N points in the plane and fix $A > 0$. Let $\mathcal{T}_A(P)$ be the set of all triangles with vertices in P and of area A. Prove that $|\mathcal{T}_A(P)| \lesssim N^{7/3}$.*

In the next part of the chapter, we prove Theorem 4.10 using the theorems and lemmas developed so far.

6.3 Proof of Guth's 2014 Theorem

Lemma 6.11. *Let $a_1, \ldots, a_N \in \mathbb{C}$ and $\alpha, \beta > 0$. Furthermore, suppose that $|a_i| \leq \alpha|a_1 + \cdots + a_N|$ for each i. Then*

$$\left|\{j : |a_j| > \beta|a_1 + \cdots + a_N|\}\right| \geq \frac{1 - N\beta}{\alpha}.$$

Proof. Let $\{\ell\} = \{j\}^c$ then

$$|a_1 + \cdots + a_N| \leq \sum_j |a_j| + \sum_\ell |a_\ell| \leq \sum_j \alpha|a_1 + \cdots + a_N|,$$

so that

$$|a_1 + \cdots + a_N| \leq |a_1 + \cdots + a_N| \left(\sum_j \alpha + \sum_j \beta + \sum_\ell 1\right),$$

and therefore

$$1 \leq \sum_j \alpha + \sum_\ell \beta = \alpha|\{j\}| + \beta N,$$

and the result follows. ■

Lemma 6.12. *Suppose that $S \subset \mathbb{R}^n$ is finite. Let D be an integer and $P \in \mathcal{P}_D(\mathbb{R}^n)$. Furthermore, suppose that*

(i) $\mathbb{R}^n \setminus Z(P) = \dot\bigcup_i \mathcal{O}_i$ *where each $\mathcal{O}_i$ is open and $|\{i\}| \leq D^n$.*

(ii) $|\mathcal{O}_i \cap S| \leq C_n|S|D^{-n}$ *where C_n is a constant depending only on the dimension n.*

(iii) *Let $S_{cell} = \dot\bigcup_i O_i \cap S$ and $S_{alg} = S \cap Z(P)$.*

If $|S_{cell}| \geq |S_{alg}|$ then

$$\left|\left\{j : \frac{1}{8}D^{-n}|S| \leq |\mathcal{O}_j \cap S| \leq C_n D^{-n}|S|\right\}\right| \geq \frac{1}{4C_n}D^n. \tag{7}$$

Proof. For proof of existence of a polynomial P satisfying (i)-(iii), check Theorem 6.6. Now, it is cleat that $S = S_{\text{cell}} \uplus S_{\text{alg}}$ and therefore $|S| \leq 2|S_{\text{cell}}|$. If $N = |\{i\}|$ and $|a_i| = |\mathcal{O}_i \cap S|$, then $|a_1 + \cdots + a_N| = |S_{\text{cell}}|$ and

$$a_i \leq |\mathcal{O}_i \cap S| \leq C_n D^{-n}|S| \leq 2C_n D^{-n}|S_{\text{cell}}|.$$

Therefore, we can apply the above lemma with $\alpha = 2C_n D^{-n}$ and $\beta = (2N)^{-1}$ to

$$\left|\left\{j : |\mathcal{O}_j \cap S| > \frac{1}{2N}|S_{\text{cell}}|\right\}\right| \geq \frac{D^n}{4C_n}.$$

But $(2N)^{-1} \leq (4D)^{-n}$ and therefore

$$\left\{j : |\mathcal{O}_j \cap S| > \frac{1}{2N}|S_{\text{cell}}|\right\} \subset \left\{j : |\mathcal{O}_j \cap S| > \frac{1}{8}D^{-n}|S|\right\},$$

and hence

$$\left|\left\{j : |\mathcal{O}_j \cap S| > \frac{1}{8}D^{-n}|S|\right\}\right| \geq \frac{D^n}{4C_n},$$

as desired. ∎

Proposition 6.13. *Pick $B \in \mathbb{N}^*$. Suppose that $\mathfrak{L}$ is a set of L lines in $\mathbb{R}^3$ satisfying*

$$\left|\left\{\ell \in \mathfrak{L} : \ell \in Z(P)\right\}\right| \leq B,$$

for all polynomials $P \in \mathcal{P}_D(\mathbb{R}^3)$. Then to every $\epsilon > 0$, there is a constant C_ϵ such that

$$|P_r(\mathfrak{L})| \leq C_\epsilon B^{1/2-\epsilon} L^{3/2+\epsilon},$$

for all $L \geq B$ and $r \geq 2$.

Proof. Suppose that $\epsilon \geq 1/2$ then

$$|P_r(\mathfrak{L})| \leq L^2 = L^{1/2-\epsilon}L^{3/2+\epsilon} = \left(\frac{1}{L}\right)^{\epsilon-1/2} L^{3/2+\epsilon} \leq \left(\frac{1}{B}\right)^{\epsilon-1/2} L^{3/2+\epsilon} = B^{1/2-\epsilon}L^{3/2+\epsilon}.$$

Hence the result is clearly true for $C_\epsilon = 1$.

For the rest of the proof suppose that $0 < \epsilon < 1/2$. We are going to induct on L. In particular, we will assume that the theorem is true for $L \leq R$ and then prove it true for $L \leq 2R$.
To establish the base case for the induction, we note that if $L \leq 2B$ then

$$|P_r(\mathfrak{L})| \leq L^2 = L^{1/2-\epsilon}L^{3/2+\epsilon} = L^{1/2-\epsilon}L^{3/2+\epsilon} \leq (2B)^{1/2-\epsilon}L^{3/2+\epsilon} = \sqrt{2}B^{1/2-\epsilon}L^{3/2+\epsilon}.$$

Now let $S = P_r(\mathfrak{L})$ and Let $D \in \mathbb{N}$ be a parameter that we choose later. Theorem 6.6 provides us with a polynomial $P \in \mathcal{P}_D(\mathbb{R}^3)$ that satisfies properties (i)-(iii) of the above lemma. Define S_{cell} and S_{alg} as in the above lemma. We consider two cases

Case 1: If $|S_{\text{cell}}| \leq |S_{\text{alg}}|$ then the above lemma applies and we have a constant C (that depends only on the dimension of $\mathbb{R}^3$) and at least $(4C)^{-1}D^3$ cells $\mathcal{O}_j$ such that

$$\frac{1}{8}D^{-3}|S| \leq |\mathcal{O}_j \cap S| \leq CD^{-3}|S|, \tag{8}$$

for all j (C is the same constant as Theorem 6.6). For each j, we let

$$\mathfrak{L}_j = \{\ell \in \mathfrak{L} : \ell \cap \mathcal{O}_j \neq \emptyset\}.$$

and $L_j = |\mathfrak{L}_j|$. By Lemma 1.5, a line that does not lie entirely in $Z(P)$ can intersect $Z(P)$ in at most D points. Hence if a line intersects a cell, then it can intersect at most $D+1$ cells in total. Therefore, $\sum L_j \leq (D+1)L$ which implies that there is a cell $\mathcal{O}_\alpha$ with $\alpha \in \{j\}$ such that

$$(4C)^{-1}D^3 L_\alpha \leq 2DL.$$

Since we are assuming that $L \leq 2R$ and provided that $D \geq 4\sqrt{C}$, we therefore get

$$L_\alpha \leq 8CD^{-2}L \leq 8CD^{-2}2R \leq R.$$

So we assume D satisfies the above. By the induction hypothesis applied to $\mathfrak{L}_\alpha$ we get a constant C_ϵ such that

$$|\mathcal{O}_\alpha \cap S| \leq P_r(\mathfrak{L}_\alpha) \leq C_\epsilon B^{1/2-\epsilon} L_\alpha^{3/2+\epsilon} \leq C_\epsilon B^{1/2-\epsilon}(8CD^{-2}L)^{3/2+\epsilon},$$

and combining this with (8) we have that

$$\frac{1}{8}D^{-3}|S| \leq D^{-3-2\epsilon}(8C)^{3/2+\epsilon}C_\epsilon B^{1/2-\epsilon}L^{3/2+\epsilon},$$

and therefore, provided that $D \geq \left(8(8C)^{3/2+\epsilon}\right)^{\frac{1}{2\epsilon}}$ we get

$$|P_r(\mathfrak{L})| = |S| \leq 8(8C)^{3/2+\epsilon}D^{-2\epsilon}C_\epsilon B^{1/2-\epsilon}L^{3/2+\epsilon} \leq C_\epsilon B^{1/2-\epsilon}L^{3/2+\epsilon},$$

provided $D \geq \max\left(4\sqrt{C}, \left(8(8C)^{3/2+\epsilon}\right)^{\frac{1}{2\epsilon}}\right)$ which concludes Case 1.

Case 2: Suppose $|S_{\text{alg}}| \geq |S_{\text{cell}}|$. We know therefore that $|S| \leq 2|S_{\text{alg}}|$. We partition S onto the following

$$S_2 = \left\{p \in S_{\text{alg}} : p \text{ belongs to at least two lines of } \mathfrak{L} \text{ that lie in } Z(P)\right\},$$

and $S_1 = S \setminus S_2$. Recalling that $B \leq L$ we have that

$$S_2 \leq \binom{B}{2} \leq B^2 = B^{1/2-\epsilon}B^{3/2+\epsilon} \leq B^{1/2-\epsilon}L^{3/2+\epsilon}.$$

On the other hand, if $p \in S_1$ then p belongs to a line of $\mathfrak{L}$ that doesn't lie in $Z(P)$ (this is true since every point in S lies in at least r lines from $\mathfrak{L}$ and $r \geq 2$). But such a lines intersects $Z(P)$ in at most D points and therefore $S_1 \leq DL$. This implies that

$$|S_{\text{alg}}| \leq B^{1/2-\epsilon}L^{3/2+\epsilon} + DL \leq (D+1)B^{1/2-\epsilon}L^{3/2+\epsilon}.$$

If we take

$$C_\epsilon \geq D + 2 = \max\left(4\sqrt{C}, \left(8(8C)^{3/2+\epsilon}\right)^{\frac{1}{2\epsilon}}\right) + 2,$$

then this choice C_ϵ guarantees that the base and and the two other cases are correct. ■

Proposition 6.14 (Shayya)**.** *Suppose the positive integers L, r and D satisfy*

$$r > \frac{4DL}{D + \sqrt{D^2 + 4L}}.$$

Also suppose S is a set of courses and $\mathfrak{L}$ is a set of students such that

(i) *Each course in S has at least r students.*

(ii) *Any group of $D^2 + 1$ students can take at most one course together.*

Then

$$|S| \leq \frac{2L}{D^2 + r + \sqrt{(D^2 + r)^2 - 4D^2 L}}.$$

Proof. Suppose that D^2 from each course take another set of common courses $E \subset S$ so that $D^2(|E| - 1)$ of the students in each course will take common courses. What remains is $r - D^2(|E| - 1)$ in each course. Taking into consideration all courses in E

$$|E| \left(r - D^2(|E| - 1) \right) \leq L,$$

for every $E \subset S$ such that $|E| \leq 1 + D^{-2} r$. This means that

$$|E|(r - D^2|E| + D^2) \leq L$$

and and therefore

$$D^2 E^2 - (D^2 + r)|E| + L \geq 0,$$

for all $E \subset S$ such that $|E| \leq 1 + D^{-2} r$. We now consider the inequality $D^2 x^2 - (D^2 + r)x + L \geq 0$. If

$$\Delta = (D^2 + r)^2 - 4D^2 L,$$

then roots are

$$(x_1, x_2) = \frac{1}{2D^2} \left(D^2 + r - \sqrt{\Delta}, D^2 + r + \sqrt{\Delta} \right),$$

and thus

$$x_1 - x_2 = \frac{\sqrt{\Delta}}{D^2} > 1 \iff \Delta > D^4 \iff r > \frac{4DL}{D + \sqrt{D^2 + 4L}}.$$

We note that

$$x_1 = \frac{(D^2 + r)^2 - \Delta}{2D^2(D^2 + r + \sqrt{\Delta}} = \frac{2L}{D^2 + r + \sqrt{(D^2 + r)^2 - 4D^2}}.$$

So it is to be proved that $|S| \leq x_1$. Since $x_2 - x_1 > 1$, then there is a smallest integer N such that $x_1 \leq N \leq x_2$ and consider two cases.

<u>Case 1</u>: If $N = x_1$, then $N + 1 < x_2$. Suppose that $|S| > x_1$. Then $|S| \geq N + 1$ so that S has a subset E with $|E| = N + 1$. This implies that

$$x_1 = N < |E| = N + 1 < x_2,$$

so that

$$D^2|E|^2 - (D^2 + r)|E| + L < 0.$$

On the other hand,

$$|E| = N + 1 < x_2 < \frac{D^2 + r + \sqrt{(D^2+r)^2}}{2D^2} = 1 + D^2 - r,$$

and so $D^2|E| - (D^2 + r)|E| + L \geq 0$ and this is a contradiction and hence $|S| \leq x_1$

Case 2: Now suppose that $N > x_1$ and that $|S| > x_1 = N$. It follows that S has a subset E with $|E| = N$. This implies that $x_1 < N = |E| < x_2$ so that

$$D^2|E|^2 - (D^2 + r)|E| + L < 0.$$

On the other hand, $|E| = N < x_2$ and so

$$D^2|E|^2 - (D^2 + r)|E| + L \geq 0,$$

which is a contradiction and thus $|S| \leq x_1$. ∎

Corollary 6.14.1. *Suppose that the positive integers L and r satisfy*

$$r > \frac{4L}{1 + \sqrt{1 + 4L}},$$

and let $\mathfrak{L}$ be a set of L lines in $\mathbb{R}^n$. Then

$$|P_r(\mathfrak{L})| \leq \frac{2L}{1 + r + \sqrt{(1+r)^2 - 4L}}.$$

Proof. Apply the above proposition with $D = 1$. ∎

Corollary 6.14.2. *Suppose that the integers L, r and D satisfy*

$$r > \frac{4DL}{D + \sqrt{D^2 + 4L}}.$$

Let $\mathfrak{L}$ be a set of L lines in $\mathbb{R}^3$ and $\mathcal{Y}$ be a set of irreducible algebraic surfaces in $\mathbb{R}^3$ of degree at most D such that each $Z \in \mathcal{Y}$ contains at least r lines from $\mathfrak{L}$. Then

$$|\mathcal{Y}| \leq \frac{2L}{D^2 + r + \sqrt{(D^2+r)^2 - 4D^2L}}.$$

Proof. Theorem 4.14 tells us that we can apply the above proposition. ∎

We recall Thorem 4.10.

Theorem 6.15 (Guth, 2014)**.** *To every $\epsilon > 0$, there a positive integer D and a number $K \in [4(2D)^{2/\epsilon}, \infty)$ such that if $\mathfrak{L}$ is a set of L lines in $\mathbb{R}^3$ satisfying*

$$\left|\left\{\ell \in \mathfrak{L} : \ell \in Z(P)\right\}\right| < L^{1/2-\epsilon},$$

for all irreducible $P \in \mathcal{P}_D(\mathbb{R}^n)$ and $2 \leq r \leq 2\sqrt{L}$ then

$$|P_r(\mathfrak{L})| \leq KL^{3/2+\epsilon}r^{-2}.$$

The fact that the next theorem proves Guth's 2014 theorem is left as an exercise for the reader.

Theorem 6.16. *To every $\epsilon > 0$ there a positive integer D and a number $K \in [4(2D)^{2/\epsilon}, \infty)$ such that the following holds. If $\mathfrak{L}$ is a set of L lines in $\mathbb{R}^3$ and $2 \le r \le 2\sqrt{L}$, then there is a set $\mathcal{Z}$ of algebraic surfaces in $\mathbb{R}^3$ such that*

(i) *Each $Z \in \mathcal{Z}$ is irreducible and of degree at most D.*

(ii) *For each $Z \in \mathcal{Z}$ we have $\big|\{\ell \in \mathfrak{L} : \ell \in Z\}\big| \ge L^{1/2+\epsilon}$.*

(iii) *$|\mathcal{Z}| \le 2L^{1/2-\epsilon}$.*

(iv) *If $r' = \lfloor (9/10)r \rfloor + 1$ and $\mathfrak{L}_Z = \{\ell \in \mathfrak{L} : \ell \in Z\}$ then*

$$\left| P_r(\mathfrak{L}) \setminus \bigcup_{Z \in \mathcal{Z}} P_{r'}(\mathfrak{L}_Z) \right| \le K L^{3/2+\epsilon} r^{-2}.$$

Proof. If $\epsilon \ge 1/2$, then the result follows from Corollary 6.14.1 since

$$|P_r(\mathfrak{L})| \le \frac{L(L-1)}{r(r-1)} \le \frac{L^2}{r(r/2)} \le \frac{2L^{3/2}L^{1/2}}{r^2} \le 2L^{3/2+\epsilon} r^{-2}.$$

In this case $\mathcal{Z}$ is the empty set.

For the rest of the proof, we suppose that $\epsilon < 1/2$. We will use induction in the following manner: we suppose that the result is true for $L \le R$ and then prove it true for all $L \le 2R$.

<u>**Base Case:**</u> The base case will be taken to be $L \le (2D)^{1/\epsilon}$. We have

$$|P_r(\mathfrak{L})| \le \binom{L}{2} \le L^2 \le (2D)^{1/\epsilon} \le \frac{K}{4} \le \frac{KL}{4L} \le \frac{KL}{r^2} \le KL^{3/2+\epsilon} r^{-2}.$$

The reader is invited to check each one of the inequalities used above. Again, $\mathcal{Z}$ in this case is the empty set.

<u>**Inductive Step:**</u> We now let $D \in \mathbb{N}$ be a degree that that we choose later and let $S := P_r(\mathfrak{L})$. Theorem 6.6 provides us with a polynomial $P \in \mathcal{P}_D(\mathbb{F}^3)$ such that $\mathbb{R}^n \setminus Z(P)$ is a disjoint union of at most $2D^3$ open sets $\mathcal{O}_i$ such that for each i we have

$$|\mathcal{S} \cap \mathcal{O}_i| \le \frac{2^{3+4}(3!)}{(\sqrt[3]{2}-1)^3} |S| D^{-3} < 43736 |S| D^{-3}. \tag{9}$$

Define $\mathfrak{L}_i$ and L_i as in the proof of Theorem 6.8 and we note that

$$S \cap \mathcal{O}_i \subset P_r(\mathfrak{L}) \cap \mathcal{O}_i \subset P_r(\mathfrak{L}_i) \quad \text{and} \quad \sum_i L_i \le (D+1)L \le 2DL.$$

We let $\beta > 0$ be a parameter that we choose later. We will say a cell $\mathcal{O}_i$ is β-good if $L_i \le \beta D^{-2} L$. We say $\mathcal{O}_i$ is β-bad if it is not β-good. First of all notice that since

$$\big|\{i : \mathcal{O}_i \text{ is } \beta\text{-bad}\}\big| \cdot \beta D^{-2} L \le \sum_{\mathcal{O}_i \text{ is } \beta\text{-bad}} L_i \le \sum_i L_i \le 2DL,$$

then

$$\big|\{i : \mathcal{O}_i \text{ is } \beta\text{-bad}\}\big| \le 2\beta^{-1}D^3,$$

and therefore

$$\begin{aligned}
\sum_{\mathcal{O}_i \text{ is } \beta\text{-bad}} |\mathcal{S} \cap \mathcal{O}_i| &\le \sum_{\mathcal{O}_i \text{ is } \beta\text{-bad}} 43736|S|D^{-3} && \big(\text{by inequality (9)}\big)\\
&\le \big|\{i : \mathcal{O}_i \text{ is } \beta\text{-bad}\}\big| \cdot 43736|S|D^{-3}\\
&\le 87472\,\beta^{-1}|S|\\
&\le \frac{|S|}{100} && (\text{provided } \beta = 8747157).
\end{aligned}$$

We fix β to the above value for the rest of the proof and assume that $BD^{-1/2} \le 1/2$ so that $D \ge \sqrt{2\beta} \ge 4181$. This says that for all good cells $\mathcal{O}_i$ we get

$$L_i \le \frac{1}{2}L \le \frac{1}{2}(2R) = R,$$

and therefore the induction hypothesis applies to each good cell. To proceed, we distinguish two cases for the integer r:

<u>Case 1:</u> $r \le 2\sqrt{L_i}$**.**

The induction hypothesis provides us with a set $\mathcal{Z}_i$ of algebraic surface that satisfy (i)-(iv). In particular,

$$|\mathcal{Z}_i| \le 2L_i^{1/2-\epsilon} \le 2(BD^{-2}L)^{1/2-\epsilon}.$$

We therefore get

$$\begin{aligned}
\Big|\mathcal{O}_i \cap S \setminus \bigcup_{Z\in\mathcal{Z}_i} P'_r(\mathfrak{L})\Big| &\le \Big|P_r(\mathfrak{L}_i) \setminus \bigcup_{Z\in\mathcal{Z}_i} P'_r(\mathfrak{L})\Big| && (\text{since } \mathcal{O}_i \cap S \subset P_r(\mathfrak{L}_i) \cap S)\\
&\le KL_i^{3/2-\epsilon}r^{-2} && (\text{by induction hypothesis})\\
&\le K(\beta D^{-2}L)^{3/2+\epsilon}r^{-2} && (\text{since } \mathcal{O}_i \text{ is } \beta\text{-good})\\
&\le K\beta^{3/2+\epsilon}D^{-3-2\epsilon}L^{3/2+\epsilon}r^{-2}\\
&< K\beta^2D^{-3-2\epsilon}L^{3/2+\epsilon}r^{-2}, && (\text{since } \epsilon < 1/2)
\end{aligned}$$

which the desired result.

<u>Case 2:</u> $r > 2\sqrt{L_i}$**.**

By Corollary 6.14.1 we have

$$|S \cap \mathcal{O}_i| \le P_r(\mathfrak{L}_i) \le 2\frac{L_i}{1+r} \le \frac{2L}{r} \le \frac{4\sqrt{L}L}{2\sqrt{L}r} \le 4L^{3/2}r^{-2} \le K\beta^2D^{-3-2\epsilon}L^{3/2+\epsilon}r^{-2},$$

provided that that $4 \le K\beta^2D^{-3-2\epsilon}$. Solving for D one gets

$$4 \le K\beta^2D^{-3-2\epsilon} \le (2D)^{2/\epsilon}\beta^2D^{-3-2\epsilon},$$

and after some calculation we get that

$$D \geq \left(\frac{1}{4}\right)^{\frac{\epsilon}{2-3\epsilon^2-2\epsilon^3}} \cdot \left(4\beta^{-2}\right)^{\frac{\epsilon^2}{2-3\epsilon^2-2\epsilon^3}}.$$

Summing over all good cells we get

$$\begin{aligned}
\sum_{\mathcal{O}_i \text{ is } \beta\text{-good}} \left| S \cap \mathcal{O}_i \setminus \bigcup_{Z \in \mathcal{Z}_i} P_{r'}(\mathfrak{L}_Z) \right| &\leq \sum_{\mathcal{O}_i \text{ is } \beta\text{-good}} K\beta^2 D^{-3-2\epsilon} L^{3/2+\epsilon} r^{-2} \\
&\leq |\{i : \mathcal{O}_i \text{ is } \beta\text{-good}\}| K\beta^2 D^{-3-2\epsilon} L^{3/2+\epsilon} r^{-2} \\
&\leq |\{i\}| K\beta^2 D^{-3-2\epsilon} L^{3/2+\epsilon} r^{-2} \\
&\leq
\end{aligned}$$

■