YUFEI ZHAO'S POLYNOMIAL METHODS IN COMBINATORICS

ERIC NASLUND

1. Lecture 1

This is based on Lary Guth's course at MIT, and his subsequent book which is soon to be published.

1.1. **Motivation.**

1.1.1. *Kakeya Problem.* How "small" can a set in $\mathbb{R}^n$ be if it contains a line segment in every direction? Besicovitch famously proved that it can have measure zero.

Conjecture 1. *This set must be n-dimensional.*

There is a finite field "toy model" of this problem. A set $A \subset \mathbb{F}_q^n$ is called a Kakeya set if it contains a line in every direction, and the question is, what is the smallest possible size of K?

Theorem 2. *(Dvir 2008) If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then*

$$|K| \geq c_n q^n.$$

This was a huge surprise not only because it solved the problem, but because the solution was so short. Dvir's solution led to several subsequent developments in the years to come.

1.1.2. *Joints Problem.* Let $\mathcal{L}$ be a set of lines in $\mathbb{R}^3$. A point x is called a joint if it is incident to at least three non-coplanar lines in $\mathcal{L}$. Question: Given L lines, what is the maximum number of joints? It is possible to get on the order of $L^{3/2}$ using a cube-like grid in three dimensions. Prior to Guth and Katz the best upper bound was $L^{1.62}$. Using similar techniques to Dvir, months after his result appeared, Guth and Katz proved that:

Theorem 3. *(Guth-Katz 2008) A set of lines in $\mathbb{R}^3$ form $O(L^{3/2})$ joints.*

1.1.3. *Erdos distinct distances problem.* The quesiton is, if I have N points in $\mathbb{R}^2$ what's the minimum number of distinct pairwise distances that can occur? N generic points will have $\binom{N}{2}$ distances. Using a square grid we will have at least $CN/\sqrt{\log N}$ distances occuring. Prior to Dvir's work, the best lower bound was $N^{0.86}$.

Theorem 4. *(Guth-Katz 2010) The number of distinct differences is*

$$\gg \frac{N}{\log N}.$$

1.2. The polynomial method and Dvir's proof.

Problem 5. Find a polynomial $P(X,Y)$ such that $P(j,2^j) = 0$ for all $j = 1,2,\dots,10^6$. What is the smallest possible degree of this polynomial?

Proof. We could choose $(X-1)\cdots(X-10^6)$, however this has degree 10^6. In fact, we can find a polynomial of degree < 2000 using linear algebra. Consider

$$P(X,Y) = \sum_{r+s<2000} a_{r,s} X^r Y^s.$$

There will be $\binom{2001}{2} > 10^6$ coefficients to choose 10^6 constraints. In general we expect this to be optimal unless there is algebraic structure in the set we are looking at, and this will be a theme of this course. □

Given a field $\mathbb{F}$, let $\mathrm{Poly}_D(\mathbb{F}^n)$ be the space of polynomials in n variables of total degree $\leq D$. This type of construction used above is called parameter counting and is sumarised in the following proposition:

Proposition 6. *Given a finite set $S \subset \mathbb{F}^n$ if $\dim \mathit{Poly}_D(\mathbb{F}^n) > |S|$ then there exists a nonzero polynomial $P \in \mathit{Poly}_D(\mathbb{F}^n)$ vanishing on S.*

A classic ball and urn counting shows that

$$\dim \mathrm{Poly}_D(\mathbb{F}^n) = \binom{D+n}{n} \geq \left(\frac{D}{n}\right)^n,$$

and so for any set S there is a polynomial of degree $\leq n|S|^{1/n}$ that vanishes on S.

Lemma 7. *(Vanishing Lemma) If $n = 1$ and $P \in \mathit{Poly}_D(\mathbb{F})$ vanishes at $D+1$ points, then $P \equiv 0$.*

Corollary 8. *If $P \in \mathit{Poly}_D(\mathbb{F}^n)$ vanishes at $D+1$ points on some line ℓ then it vanishes on all of ℓ.*

Before we turn to the Kekaya problem, we look at the finite field Nikodym problem. $N \subset \mathbb{F}_q^n$ is a Nikodym set if for all $x \in \mathbb{F}_q^n$ there exists a line $L(x)$ containing x such that $L(x)\backslash\{x\} \subset N$.

Theorem 9. *(Dvir 2008) Any Nikodym set $N \subset \mathbb{F}_q^n$ has $|N| \geq c_n q^n$ where $c_n = (10n)^{-n}$.*

Proof. By contradiction suppose that N is a Nikodym set with $|N| < (10n)^{-n} q^n$. By Parameter counting there is a non-zero polynomial vanishing on N such that $\deg P \leq n|N|^{1/n} \leq \frac{q}{10} < q-1$.

Claim. P vanishes at every point in $\mathbb{F}_q^n$.

Proof. Given $x \in \mathbb{F}_q^n$ there exists $L(x)\backslash\{x\} \subset N$. Since P vanishes on N, it vanishes at $\geq q-1$ points on $L(x)$ and hence equals 0 on that line. Thus P vanishes everywhere. □

We are not quite done yet since in finite fields there are polynomials like $x^q - x$ which is nonzero and vanishes everywhere.

Lemma. *If $P \in \mathit{Poly}_{q-1}(\mathbb{F}_q^n)$ vanishes at every point of $\mathbb{F}_q^n$, then $P \equiv 0$.*

Proof. This lemma is proven by induction on n. When $n = 1$ this is the vanishing lemma, and for larger n we can look at this as a lower degree polynomial. □

The lemma and the claim together prove our desired result. □

Now we will prove the finite field Kakeya problem.

Proof. Given a Kakeya set K, for every $a \in \mathbb{F}_q^n \backslash \{0\}$ there exists $b \in \mathbb{F}_q^n$ such that $\{at + b : \ t \in \mathbb{F}_q\} \subset K$. Suppose that

$$|K| < (10n)^{-n} q^n.$$

As we did for the Nikodym problem, we can find a polynomial $P \in \mathrm{Poly}_{q-2}\left(\mathbb{F}_q^n\right)$ vanishing on K. Write $P = P_D + Q$ where P_D has degree exactly D, and Q has degree $< D$, where we are assuming that P_D is not identically zero. Let $a \in \mathbb{F}_q^n \backslash \{0\}$. Let $b \in \mathbb{F}_q^n$ be such that

$$\{at + b| \ t \in \mathbb{F}_q\} \subset K.$$

Let

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

which vanishes for every $t \in \mathbb{F}_q$. We have that $\deg R < q$, and so R is actually the all zero polynomial. Since $P(at + b) = P_D(at + b) + Q(at + b)$, we see that the coefficient of t^D in $\mathcal{R}$ is $P_D(a)$, and in particular this must be zero. Now, since a was arbitrary we see that $P_D(a) = 0$ for all $a \in \mathbb{F}_q^n \backslash \{0\}$, and since it is homogenous, we see that it vanishes everywhere. As its degree was less than Q, it must vanish everywhere, which is a contradiction, and concludes the proof. □

Alternate view point of this proof: If K is a small Kakeya set, then there exists P of degree $< q - 1$ vanishing on K. Since P vanishes on a line of every direction, P must vanish on all the points at infinity in projective space. In other words, in projective space.

1.3. **The Joints Problem.** Let $\mathcal{L}$ be a set of lines in $\mathbb{R}^3$. Consider a set of S planes in general position. There are $\binom{S}{2}$ lines from pairs of planes and $\binom{S}{3}$ triples of intersections, or joints. It's possible that this is indeed the optimal example.

Theorem 10. *(Guth-Katz, later simplified by Kaplan-Sharir-Shustin/Quilodran) Any L lines in $\mathbb{R}^3$ determine at most $10L^{3/2}$ joints.*

Proof. We begin with a lemma

Lemma. *(Main Lemma) Given a set $\mathcal{L}$ of lines in $\mathbb{R}^3$ with J joints, then one of the lines contains $\leq 3J^{1/3}$ joints.*

Proof. Let P be the minimum degree nonzero polynomial vanishing at every joint. By parameter counting, $\deg P \leq 3J^{1/3}$. If every line contains $> 3J^{1/3}$ joints, then P vanishes at all lines in $\mathcal{L}$. Now, if x is a joint in $\mathcal{L}$ and if a smooth function $F : \mathbb{R}^3 \to \mathbb{R}$ vanishes on all lines in $\mathcal{L}$ then ∇F vanishes at x. This is because if v_1, v_2, v_3 are the directional vectors of the 3 lines through x, then the directional derivatives of F in those directions $\nabla F(x) \cdot v_i = 0$, and so $\nabla F(x) = 0$. Thus ∇P vanishes at all joints. By the minimality of $\deg P$, we have that ∇F must be identically zero, and this implies that P is the constant function. □

To prove the theorem using this lemma, let $J(L)$ be the maximum number of joints with L lines. Then

$$J(L) \leq J(L-1) + 3J(L)^{1/3}.$$

Iterating this,

$$J(L) \leq L \cdot 3(L)^{1/3},$$

and so

$$J(L) \leq 10L^{1/3}.$$

□

This approach if optimized can give a constant of $4/3$ in front of the $L^{3/2}$, however the conjectured optimal is $\sqrt{2}/3K^{3/2}$.

2. Lecture 2

The basic method application of the polynomial method that we used last time involves

- Parameter Counting: For $n \geq 2$, $S \subset \mathbb{F}^n$ there exists a non-zero polynomial P of deg $\leq n|S|^{1/n}$ vanishing on S.
- Vanishing Lemma: If you have a polynomial of degree at most D that vanishes at more than D points on a line, then the polynomial vanishes on the entire line.

Question: Why do these methods work so well? To answer this, first we'll take a step back, and look at the methods used before Dvir solved the Kakeya problem. We will see that there are some very interesting reasons for why these earlier methods failed.

2.1. Finite Field Kakeya Without Polynomials.

Proposition 11. *Suppose that I have $s \leq q$ lines $\ell_1 \ldots, \ell_s$ in $\mathbb{F}_q^n$. Then the union of these lines has size at least*

$$|\cup \ell_i| \geq \frac{qs}{2}.$$

Corollary 12. *If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then $|K| \geq q^2/2$.*

Proof. (Of proposition) Working greedily, line ℓ_i introduces at least $q - i + 1$ new points, and so

$$|\cup \ell_i| \geq q + (q-1) + \cdots + (q-s) \geq \frac{qs}{2}.$$

□

Let's try using the fact that there are a lot more lines than this.

Proposition 13. *(Bush Method) Given $\ell_1, \ldots, \ell_M$ lines in $\mathbb{F}_q^n$, then*

$$|\cup \ell_i| \geq \frac{1}{2} q M^{1/2}.$$

Corollary 14. *If $K \subset \mathbb{F}_q^n$ is Kakeya, then*

$$|K| \geq \frac{1}{2} q^{\frac{n+1}{2}}.$$

Proof. Let $X = \cup \ell_i$. Then each line contains q points in X. There exists $x \in X$ contained in

$$\geq \frac{qM}{|X|}.$$

This is called a "bush" of lines.

$$\#\text{points in bush} \geq (q-1)\frac{qM}{|X|},$$

but this is $\leq |X|$, and so

$$|X| \geq \frac{1}{2}qM^{1/2}.$$

□

Our first non-trivial bound takes advantage of the fact that the lines in a Kakeya set are all pointing in different directions.

Proposition 15. *(Hairbrush method of Wolff) Given $\ell_1, \ldots, \ell_M$ lines in $\mathbb{F}_q^n$ with at most $q+1$ lines in every plane. Then*

$$|\cup \ell_i| \geq \frac{1}{3}q^{3/2}M^{1/2}.$$

Corollary 16. *If $K \subset \mathbb{F}_q^n$ is a Kakeya set, then*

$$|K| \geq \frac{1}{2}q^{\frac{n+2}{2}}.$$

Specifically, for $n = 3$ this gives $|K| \geq q^{5/2}$.

Proof. A "Hairbrush" is all the lines ℓ_j that meet a fixed ℓ_i, not including ℓ_i itself. On average every point lies in $\frac{qM}{|X|}$ lines. If all the points behaved on average, then each hairbrush contains $\gtrsim \frac{q^2M}{|X|}$ lines. It is then an exercise that a there exists a hairbrush containing $\geq \frac{1}{2}\frac{q^2M}{|X|}$ lines. For each 2-plane π containing the stem, let $H(\pi)$ denote the set of lines of the hairbrush contained in π, and so

$$\sum_{\pi} H(\pi) \geq \frac{1}{2}\frac{q^2M}{|X|}.$$

By our first method,

$$\left|\bigcup_{\ell_j \in H(\pi)} \ell_j\right| \geq \frac{1}{3}|H(\pi)|q.$$

Thus the union of the lines in the hairbrush has size at least

$$\sum_{\pi} \frac{1}{3}|H(\pi)|q \geq \frac{1}{6}\frac{q^3M}{|X|},$$

and from this we obtain

$$|X| \geq \frac{1}{3}q^{3/2}M^{1/2}.$$

□

Question: Is the hypothesis of this proposition enough for the Kakeya problem? The answer is no, and a counterexample is given by a Hermitian Variety, but only when $q = p^2$. Ellenberg-Hablicsek proved that the hypothesis *is* enough when q is a prime.

The Hermitian Variety is a surface $H \subset \mathbb{F}_q^3$, where $q = p^2$, p prime, is defined by

$$x^{p+1} + y^{p+1} + z^{p+1} = 1.$$

Proposition 17. *The Hermitian variety H contains $\Theta\left(q^{5/2}\right)$ points $\Theta\left(q^2\right)$ lines and $\lesssim q^{1/2}$ lines in every plane.*

Proof. We will use the fact that $\mathbb{F}_p^\times \subset \mathbb{F}_q^\times$ sits inside as a subgroup of order $p-1$, where $|\mathbb{F}_q^\times| = q-1 = (p-1)(p+1)$. In particular $\mathbb{F}_p^\times = \left\{y \in \mathbb{F}_q^\times : \; y^{p-1} = 1\right\}$. Furthermore, $x^{p+1} \in \mathbb{F}_p$ for all $x \in \mathbb{F}_q$ since $x^{(p+1)(p-1)} = x^{q-1} = 1$, and $x^{p+1} = y$ has exactly $p+1$ solutions in $\mathbb{F}_q$ for all $y \in \mathbb{F}_p^\times$.

Since there are precisely p^2 such solutions to

$$X + Y + Z = 1,$$

and if $X \neq 0$ there are $p+1$ solutions to $x^{p+1} = X$, it follows that H has size $\approx p^5$. Now, define conjugation to be $\overline{x} = x^p$ for all $x \in \mathbb{F}_q$. (In fact, if $p \equiv 3 \bmod 4$, then $\mathbb{F}_q = \mathbb{F}_p[i]$, and $\overline{x+iy} = x - iy$.) Thus H is the analogue of the complex unit sphere

$$x\overline{x} + y\overline{y} + z\overline{z} = 1.$$

Defining the inner product

$$\langle v, w\rangle = \sum_{i=1}^{3} v_i \overline{w_i},$$

then the action of the unitary group

$$U\left(\mathbb{F}_q^n\right) = \left\{g \in \mathrm{GL}\left(\mathbb{F}_q^n\right) : \langle v, w\rangle = \langle gv, gw\rangle \;\forall\; v, w \in \mathbb{F}_q^n\right\}$$

on H is transitive. Consider the lines in H through $(1,0,0)$,

$$\ell = \left\{(1+at, bt, ct) : \; t \in \mathbb{F}_q, \; a, b, c \in \mathbb{F}_q, \; (1+at)(1+a^p t^p) + b^{p+1}t^{p+1} + c^{p+1}t^{p+1} = 1 \;\forall t \in \mathbb{F}_q\right\}.$$

For such an equation of degree $p+1$ to hold for all $t \in \mathbb{F}_q$, all the coefficients must match. Hence $a = 0$,$b^{p+1} = -c^{p+1}$ and so

$$\ell_b = \left\{(1, bt, t) : \; t \in \mathbb{F}_q : b^{p+1} = -1, \; b \in \mathbb{F}_q\right\},$$

and there are just $p+1$ lines. Counting all the points and all the lines, we get p^6 lines, but each line is counted q times, and so this gives a final count of q^2. □

What's so special about polynomials? Let $W = \mathrm{Poly}_D\left(\mathbb{F}^n\right)$, $\dim W \asymp D^n$, if $P \in W$ vanishes at $> D$ poitns on a line, then it vanishes on ℓ. Comparing this function space to the space of trigonometric polynomials

$$f(x) = \sum_{\substack{\omega \in \mathbb{Z}^n \\ |\omega_j| \le D}} a(\omega) e^{2\pi i \omega \cdot x},$$

when we restrict to a generic, non-axis parallel line, the degrees of freedom do not drop at all.

Problem 18. (Open) Suppose that $W \subset \mathrm{Functions}(\mathbb{F}^n, \mathbb{F})$ be a vector space of functions. Suppose that $\forall\; \ell \subset \mathbb{F}^n$,

$$\dim W\Big|_{\ell} \le D + 1.$$

What's the maximum possible dim of W?

Problem 19. (Open) What's the maximum dimension of $W \subset \mathrm{Functions}(\mathbb{F}^n, \mathbb{F})$ that satisfies the degree D vanishing lemma, that is if $f \in W$ vanishes at $> D$ points on a line, then f vanishes on the entire line ℓ.

This problem has an upper bound

Exercise. If $|\mathbb{F}| \geq D+1$, then $\dim W \leq (D+1)^n$.

Guo, Kopparty, Sudan constructed a larger space of functions to give a better bound on the Nikodym problem.

2.2. **Lines in $\mathbb{R}^3$.** Given L lines in $\mathbb{R}^3$, what is the maximum number of intersection points? Answer: $\binom{L}{2}$. Instead, suppose we forbid too many lines on a plane, less than a constant C say. How many intersections can there be? Once again it is $\Theta(L^2)$. This is obtained by considering the surface $z = xy$.

- For every y_0, there is the horizontal line $\gamma(t) = (t, y_0, y_0 t)$
- For every x_0, there is the horizontal line $\gamma(t) = (x_0, t, x_0 t)$

Every pair intersects at $(x_0, y_0, x_0 y_0)$. This give an example of what is called a doubly ruled surface, as it is a grid projected up onto the hyperboloid. Another example is given by a Regulus, which is the union of lines passing through three pairwise skew lines. (Two lines are skew lines if the do not interesect in projective space)

Question: Suppose that I have L lines in $\mathbb{R}^3$, and at most C lines in every plane, or degree 2 algebraic surface. Then what's the maximum number of intersection points?

A key ingredient of Guth-Katz's work is that this will be $\lesssim L^{3/2}$.

3. Lecture 3

Last time: What's so special about polynomials?

- Polynomials of deg $\leq D$ have $\Theta(D^n)$ degrees of freedom as functions on $\mathbb{F}^n$.
- There are approximately D degrees of freedom when restricted to a line. The vanishing lemma states that if a polynomial vanishes at $> D$ pts, then vanishes on the whole line.

Remark 20. Last week a paper was posted on the arxiv proving that

Theorem. *(Croot-Lev-Pach) Given $A \subset \mathbb{Z}_4^n$ with no non-trivial solutions to $x+y = 2z$ then $|A| \leq 4^{0.93n}$.*

In this paper they use paramter counting and a modified vanishing lemma:

Lemma. *If P is a multilinear polynomial in n variables over $\mathbb{F}$ with $\deg \leq d$ and $A \subset \mathbb{F}^n$, $|A| > 2\sum_{i=0}^{d/2}\binom{n}{i}$. If $P(a-b) = 0$ for all $a, b \in A$ with $a \neq b$, then $P(0) = 0$.*

Proof. Let $m = \sum_{i \leq \frac{d}{2}} \binom{n}{i}$. Then

$$P(x-y) = \sum_{\substack{I, J \subset \{1, \dots, n\} \\ I \cap J \neq 0 \\ |I| + |J| \leq d}} C_{I,J} x^I y^J$$

where $x^I = \prod_{i \in I} x_i$. This equals

$$\langle u(x), v(y) \rangle$$

where we are in $\mathbb{F}^{2m}$, and the inner product is chosen so that we are pairing up x^I with $\sum_J C_{I,J} y^J$ when $|I| \leq \frac{d}{2}$, and pairing y^J with $\sum_I C_{I,J} x^I$ when $|J| \leq \frac{d}{2}$. Now, assume to obtain a contradiction that

$$\langle u(a), v(b) \rangle = P(a-b) = \begin{cases} 0 & \text{if } a \neq b \in A \\ \neq 0 & \text{if } a = b \in A \end{cases}.$$

Then $\{u(a)\}_{a \in A}$ must be linearly independent, since if there exists λ_a such that $\sum_a \lambda_a u(a) = 0$, then

$$0 = \langle \sum \lambda_a u(a), v(b) \rangle = \lambda_b \langle u(b), v(b) \rangle$$

which implies that $\lambda_b = 0$ for all b, which is a contradiction. □

The method of proof used above is known as the linear algebraic method in combinatorics, originally due to Babai and Frankl

3.1. **Linear Algebraic Method in Combinatorics.**

Theorem 21. *(Larman, Rogers, Seide 1977) Let $P \subset \mathbb{R}^n$ contain $\leq s$ distinct distances. Then*

$$|P| \leq \binom{n+s+1}{s}.$$

Example 22. If $P \subset \mathbb{R}^n$, $|P| = \binom{n+1}{s}$ has s distances. In $\mathbb{R}^{n+1}$ take points in $\{0,1\}^{n+1}$ with exactly s 1's.

Proof. Let $P = \{p_1, \dots, p_N\}$ and suppose we have distances $d_1, \dots, d_s$. Then define

$$f_j(x) = \prod_{r=1}^{s} \left(|x - p_j|^2 - d_r^2 \right)$$

for $x \in \mathbb{R}^n$. Then

$$f_j(p_i) = \begin{cases} 0 & \text{if } i \neq j \\ \neq 0 & \text{if } i = j \end{cases}.$$

Claim. $f_1, \dots, f_N$ are linearly independent.

Proof. If not, then there exists λ_i such that

$$\sum_{i=1}^{N} \lambda_i f_i = 0.$$

Evaluating at p_j we have that

$$\lambda_j f_j(p_j) = 0$$

and hence $\lambda_j = 0$ for all j, which is a contradiction. □

For all $f_1, \dots, f_N \in \text{Poly}_{2s}(\mathbb{R}^n)$, which is a space of dimension at most $\binom{n+2s}{2s}$, and so

$$N \leq \binom{n+2s}{2s}.$$

We can improve upon this slightly by considering the space in which the f_i lie. We have that

$$|x - p_j|^2 - d_r^2 \in \text{span}\left\{1, x_1, \dots, x_n, x_1^2 + x_2^2 + \dots + x_n^2\right\}.$$

Then each of the f_i can be expressed as a degree s polynomial in $x_1, \ldots, x_n, x_1^2 + \cdots + x_n^2$, which is a subspace in $\mathrm{Poly}_{2s}(\mathbb{R}^n)$ of dimension

$$\binom{n+s+1}{s},$$

and so by linear independence

$$N \leq \binom{n+s+1}{s}.$$

□

3.2. **Polynomial Method in Error-Correcting Codes.** Suppose that $Q : \mathbb{F}_q \to \mathbb{F}_q$ a polynomial of degree

$$\deg \leq cq$$

where $1 > c > 0$. Some of the data gets corrupted, and now we have a function $F : \mathbb{F}_q \to \mathbb{F}_q$ such that $Q(x) = F(x)$ for some fraction of $x \in \mathbb{F}_q$.

Claim 23. Suppose that $F : \mathbb{F}_q \to \mathbb{F}_q$, and let $\epsilon > c/2 > 0$. Then there is at most one polynomial $Q \in \mathrm{Poly}_{cq}(\mathbb{F}_q)$ agreeing with F for $> 0.5 + \epsilon$ proportion of values of $\mathbb{F}_q$.

Proof. If $Q_1, Q_2 \in \mathrm{Poly}_{cq}(\mathbb{F}_q)$ both agree with F at more than a $0.5+\epsilon$ proportion of the points of $\mathbb{F}_q$, then $Q_1(x) = Q_2(x)$ for at least

$$2\epsilon q$$

values of x. Now,

$$Q_1 - Q_2 \in \mathrm{Poly}_{cq}(\mathbb{F}_q)$$

and hence by the vanishing lemma since $2\epsilon > c$, we have that $Q_1 - Q_2 \equiv 0$. □

Can we recover Q from F efficiently?

Berlekamp-Welch algorithm:

Input: $F : \mathbb{F}_q \to \mathbb{F}_q$.

Output: Polynomial $Q : \mathbb{F}_q \to \mathbb{F}_q$ with degree at most cq such that $Q(x) = F(x)$ for at least $(0.5+\epsilon)q$ values of x if such a Q exists, where $c < \epsilon$.

To recover the algebraic structure we will find a low degree polynomial that vanishes on the graph of F, that is the set

$$\left\{(x,y) \in \mathbb{F}_q^2 : \; y = F(x)\right\}.$$

We are trying to find $y - Q(x)$.

Proposition 24. *There is a polynomial time algorithm such that if $S \subset \mathbb{F}_q^2$, we can find $P(x,y) = P_0(x) + yP_1(x)$ vanishing on S such that* $\max(\deg P_i) \leq |S|/2$.

Proof. The dimension of the space of such polynomials is given by $2D + 2$ where $\deg P_i \leq D$, and so the proposition follows by parameter counting. To find these polynomials explicitly we can solve the linear system. □

Since $P(x, F(x)) = 0$ for all $x \in \mathbb{F}_q$, and since F agrees with Q for at least a $0.5+\epsilon$ proportion of points, it follows that

$$P(x, Q(x)) = 0$$

for at least $(0.5+\epsilon)q$ points of $\mathbb{F}_q$. Hence

$$P_0(x) + Q(x)P_1(x) = 0$$

and

$$\deg \leq \deg Q + D < cq + \frac{q}{2} < \left(\frac{1}{2} + \epsilon\right) q.$$

Thus the vanishing lemma implies that $P(x, Q(x)) = 0$ for all $x \in \mathbb{F}_q$m and hence

$$-P_0(x) = Q(x)P_1(x) \Rightarrow Q(x) = \frac{P_0(x)}{P_1(x)}.$$

Visually, we have that

$$P(x, y) = c(y - Q(x)) \prod_{e \in E} (x - e) \tag{3.1}$$

where E is the set of corrupted values. To see why this is the case, note that since $P(x, Q(x)) \equiv 0$, it follows that

$$P(x, y) = (y - Q(x))R(x).$$

Furthermore, we must have that $R(e) = 0$ for every $e \in E$, and so $(x - e)|R(x)$. Furthermore since $P(x)$ has minimal degree, we obtain equation (3.1).

The above gives rise to the Reed-Soloman code where we encrypt a message by considering it as the coefficients of a polynomial. When the corruption proportion is higher than $\frac{1}{2}$, there will multiple possible polynomials that fits the original, and the goal is then to find a list of all such polynomials quickly.

Proposition 25. *(Sudan list decoding algorithm) Given $F : \mathbb{F}_q \to \mathbb{F}_q$ we can output a list of all possible polynomials of degree $< \frac{c}{2}\sqrt{q}$ agreeing with F at $\geq cq$ values of x.*

Proof. By parameter counting there exists $P(x, y)$, a nonzero polynomial of dgree at most $2\sqrt{q}$ canishing on the graph of F. Hence

$$P(x, F(x)) = 0$$

for all $x \in \mathbb{F}_q$. Suppose that $Q(x) = F(x)$ for at least $c\sqrt{q}$ values of x. Then

$$P(x, Q(x)) = 0$$

for at least cq values of x, but this has degree at most

$$(\deg P)(\deg Q) < 2\sqrt{q}\left(\sqrt{q}\frac{c}{2}\right) = cq$$

and so $P(x, q(x)) \equiv 0$. Hence

$$y - Q(x)|P(x, y).$$

There exists a polynomial time algorithm for factoring $P(x, y)$ into irreducible factors. The number of factors is $\leq \deg P \leq 2\sqrt{q}$, and we can check all of them. □

Sudan calls this "the resilience of polynomials, and the above proposition gives rise to the Reed-Muller code which is based on polynomials in $\mathbb{F}_q^n$. It is locally decodable and corruption resistent. Suppose we want to store the function

$$g : \{0, \ldots, D\}^n \to \mathbb{F}_q.$$

Then g extends uniquely to a polynomial $P : \mathbb{F}_q^n \to \mathbb{F}_q$ where $\deg_{x_i} P \leq D$. The coding is to store the values of P.

4. Lecture 4

We will now turn to incidence geometry, and the Guth-Katz theorem on distinct distances.

4.1. The Szemeredi-Trotter Theorem.

Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^2$, and let $\mathcal{S}$ be a set of S points in $\mathbb{R}^2$. **Question:** What is the maximum number of incidences between $\mathcal{L}$ and $\mathcal{S}$.

$$I\left(\mathcal{S},\mathcal{L}\right)=\left\{(p,l):\ p\in S,\ l\in\mathcal{L},\ p\in l\right\}.$$

Theorem 26. *(Szemeredi-Trotter Theorem) We have that*

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

Define $P_r\left(\mathcal{L}\right)$ to be the set of points in $\mathcal{S}$ that lie in at least r lines. We call these the r-rich points. Then the Szemeredi-Trotter theorem is equivalent to the statement that

$$P_r(\mathcal{L})\ll\frac{L^2}{r^3}+\frac{L}{r},$$

and proving this equivalence is left to the reader.

Example. If $r\geq\sqrt{L}$, then the term L/r dominates. This bound can be achieved by consider bundles of at least r-lines all around the same point. For r small compared to L, we consider many lines with slopes $\frac{a}{b}$ where $a,b\leq\sqrt{r}$, and through each point in a grid. Then this will achieve the L^2/r^3 bound.

Consider the case where $S=L=n$, and create a grid that is $n^{1/3}\times 2n^{2/3}$ in the plane. This will be the set of points. The set of lines will be given by $y=mx+b$ where $1\leq m\leq n^{1/3}$ and $1\leq b\leq n^{2/3}$, and here the number of incidences will be $n\cdot n^{1/3}\approx n^{4/3}$.

Remark 27. The Szemeredi-Trotter theorem is not true over finite fields. In $\mathbb{F}_q^2$ there are $N=q^2$ points and $N=q^2$ lines , and hence $N^{3/2}=q^3$ incidences, which is more than the theorem would allow in the plane. As a result the proof must take into account the topology of the plane and make use of the fact that we are in $\mathbb{R}^2$.

Let's begin with an easy lemma.

Lemma 28. *We have that*

$$I(\mathcal{S},\mathcal{L})\ll SL^{1/2}+L$$

and

$$I(\mathcal{S},\mathcal{L})\ll S^{1/2}L+S^{1/2}.$$

Remark. Due to line-plane duality, we need only prove one of these bounds.

Proof. We have that

$$\begin{aligned}|I(\mathcal{S},\mathcal{L})|^2 &= \left(\sum_{l\in\mathcal{L}}|l\cap\mathcal{S}\right)^2\\ &\leq L\cdot\sum_{l\in\mathcal{L}}|\mathcal{L}\cap\mathcal{S}|^2\end{aligned}$$

where we have used Cauchy-Schwarz to obtain the inequality above. We then have that

$$\begin{aligned} L \cdot \sum_{l \in \mathcal{L}} |\mathcal{L} \cap \mathcal{S}|^2 &= L \cdot \sum_{l \in \mathcal{L}} (|l \cap \mathcal{S}| + |\{p, q \in l \cap \mathcal{S} : \ p \neq q\}|) \\ &= L \cdot \left(I(\mathcal{L}, \mathcal{S}) + S^2\right) \end{aligned}$$

since between any pair of distinct points there is at most one line going through them. Thus

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

□

Remark 29. This is related to C_4-free graphs, and the maximum number of edges in a C_r-free graph.

The above lemma did not using anything about the topology of the plane, and to obtain better bounds we will need to do so. We will use what is known as the *Cutting Method.* We will cut the plane into pieces, nicely dividing the plane, and then apply lemma 28 to each piece, and aggregate the resulting bounds. This is fundamentally using the topology of the plane since there is no notion of a connected component in $\mathbb{F}_q^2$.

Heuristics:

- D auxilliary lines used to cut.
- Cut the plane into $\asymp D^2$ components
- Each $l \in \mathcal{L}$ enters $\leq D + 1$ cells
- And average cell contains $\asymp \frac{S}{D^2}$ points of $\mathcal{S}$.
- Average cell contains $\asymp \frac{L}{D}$ lines of $\mathcal{L}$.

If the cuts divided $\mathcal{S}$ and $\mathcal{L}$ evenly, then we could hope that every cell contains at most $C\frac{S}{D^2}$ points of $\mathcal{S}$ and at most $C\frac{L}{D}$ lines $\mathcal{L}$ for some fixed constant $C > 1$. Then, applying the easy bound, lemma 28 we have that the number of incidences in each cell is

$$\ll \left(\frac{S}{D^2}\right)\left(\frac{L}{D}\right)^{1/2} + \frac{L}{D}.$$

Adding over all D^2 cells we obtain the upper bound

$$\frac{SL^{1/2}}{D^{1/2}} + LD,$$

and so we shooe $D \sim S^{2/3}L^{-1/3}$ to obtain

$$\ll S^{2/3}L^{2/3}$$

as an upper bound. We note that the average does not require that every cell has both the correct number of points and lines for each cell, and instead only that it has at most $C\frac{S}{D^2}$ points of $\mathcal{S}$ for every cell or at most $C\frac{L}{D}$ lines $\mathcal{L}$ in each cell. The strategy for the cellular method is to choose the cutting lines randomly from $\mathcal{L}$, and to make sure that the cells do not have too many lines going through them. While this would lead to a proof of the theorem, we will use a different method that is based on dividing up the set of points $\mathcal{S}$.

We note that arranging points in a circle shows that we cannot use lines to partition points as desired, and instead we need to use a polynomials to create a polynomial partition. An added benefit of this is that it works in arbitrary dimensions as well.

Theorem 30. *(Polynomial Partitioning Theorem) Given $X \subset \mathbb{R}^n$ and $D > 0$ then there is a non-zero polynomial $P \in Poly_D(\mathbb{R}^n)$ such that*

$$\mathbb{R}^n \backslash Z(P)$$

is a disjoint union of $\ll D^n$ open sets and each of them contains

$$\leq C(n)\frac{|X|}{D^n}.$$

Caveat: Some or all of the points of X may lie in $Z(P)$. However, if too many of the points lie in $Z(P)$, then we will utilize the structure of the algebraic set $Z(P)$.

Remark. Since $\dim \mathrm{Poly}_D(\mathbb{R}^n) \approx D^n$, and so we have many more degrees of freedom than we did when choosing lines, and that allows us to cut any set up into regions according to the theorem above.

We will make use of the Polynomial Ham Sandwich theorem.

Theorem 31. *(Ham-Sandwich) If $U_1, \dots, U_n$ are finite positive volume open sets in $\mathbb{R}^n$, then there is a hyperplane that bisects each U_i.*

This can be proven using the Borsak-Ulam theorem.

Theorem 32. *(Polynomial Ham-Sandwich theorem) If $U_1, \dots, U_N$ are finite volume open sets in $\mathbb{R}^n$. If $N < \binom{D+n}{n}$, then there is a non-zero polynomial $P \in Poly_D(\mathbb{R}^n)$ that bisects each U_i.*

We say that P bisects a finite set S if the volume, or number of points. above and below the plane are equal. In particular, this means that many points may lie on the plane. The polynomial ham-sandwich theorem also applies to finite set U_i, and can be proven by replacing points with δ-balls.

Remark 33. Theorem 31 implies theorem 32 for finite sets via the *Veronese embedding,*

$$(x_1, \dots, x_n) \to (x_1, x_2, \dots, x_n, x_1^2, x_1x_2, \dots).$$

Proof. (Of Theorem 30 using Theorem 32) First find $P_1 \in \mathrm{Poly}_1(\mathbb{R}^n)$ bisecting X into X_1^1 and X_2^1. Then find P_2 of low degree that bisects X_1^1 and X_2^1 simultaneous giving rise to four equal size sets $X_1^2, \dots, X_4^2$. Doing this J times we have 2^J sets $X_1^J, \dots, X_{2^J}^J$ of equal size, and a polynomial

$$P = P_1 \cdot P_2 \cdots P_J.$$

We may choose

$$\deg P_j \ll C(n) 2^{j/n}$$

by the polynomial ham sandwich theorem, and hence

$$\deg P \leq C(n) \sum_{j=1}^{T} 2^{j/n} \ll 2^{J/n}.$$

Choosing J such that $2^{J/n} \asymp D$, we get at most D^n open sets each with $|X|/2^J$ points. □

Next class we will use what has been done so far to prove the Szemeredi-Trotter theorem.

5. Lecture 5

Last time we proved Theorem 30, the Polynomial Partitioning Theorem. It states that if $n \geq 2$, $X \subset \mathbb{R}^n$ and D is a parameter, then there is a non-zero polynomial $P \in \mathrm{Poly}_D(\mathbb{R}^n)$ such that $\mathbb{R}^n \backslash Z(P)$ is a disjoint union of $\ll D^n$ open sets each containing $\ll |X|/D^n$ points of X. To prove this we used repeated applications of the polynomial ham sandwich theorem, theorem 32. Today we will finish the proof of Theorem 26, the Szemeredi-Trotter Theorem.

Proof. (Of theorem 26) If $L > S^2$ or $S > L^2$, then the theorem follows from the simple estimate of lemma 28, and so we will assume that

$$S^{1/2} \leq L \leq S.$$

Applying the polynomial partition theorem with parameter $D > 0$, we obtain a polynomial of degree D such that each cell contains

$$\ll \frac{S}{D^2}$$

points of $\mathcal{S}$. Define $\mathcal{S}_{cell}$ to be the cellular points outside of $Z(P)$, and divide this up into

$$\mathcal{S}_{cell} = \cup_i \mathcal{S}_i$$

where $\mathcal{S}_i$ denotes the points of $\mathcal{S}$ in the i^{th} cell. Similarly define $\mathcal{S}_{alg}$ to be the set of points of $\mathcal{S}$ lying in $Z(P)$. Then

$$|I(\mathcal{S},\mathcal{L})| \leq |I(\mathcal{S}_{cell},\mathcal{L})| + |I(\mathcal{S}_{alg},\mathcal{L}_{cell})| + |I(\mathcal{S}_{alg},\mathcal{L}_{alg})| \tag{5.1}$$

where we have divided $\mathcal{L} = \mathcal{L}_{cell} \cup \mathcal{L}_{alg}$ where $\mathcal{L}_{alg}$ denotes the lines lying inside $Z(P)$, and $\mathcal{L}_{cell}$ denotes the lines that do not. Our goal will be to bound each one of these terms individually. Any line in $\mathcal{L}_{cell}$ meets $Z(P)$ at $\leq D$ points and thus enters at most $D+1$ cells. Thus

$$\sum L_i \leq (D+1)L$$

where $L_i = |\mathcal{L}_i|$. Applying the bound of lemma 28, we have that

$$I(\mathcal{S}_i, \mathcal{L}_i) \leq L_i + S_i^2,$$

and hence

$$\begin{aligned} I(\mathcal{S}_{cell},\mathcal{L}) &\leq \sum_i I(\mathcal{S}_i,\mathcal{L}_i) \\ &\leq \sum_i (L_i + S_i^2) \\ &\ll LD + \frac{S}{D^2}\sum_i S_i \\ &\leq LD + \frac{S^2}{D^2}. \end{aligned}$$

To deal with $\mathcal{S}_{alg}$, we first deal with the cellular lines $\mathcal{L}_{cell}$. Each line in $\mathcal{L}_{cell}$ meets $Z(P)$ in $\leq P$ points, and so

$$|I(\mathcal{S}_{alg},\mathcal{L}_{cell})| \leq LD.$$

For the final term of equation (5.1), $|I(\mathcal{S}_{alg},\mathcal{L}_{alg})|$, we note that $|\mathcal{L}_{alg}| \leq D$, and so

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

by lemma 28. Thus we obtain an upper bound of the form

$$\ll LD + \frac{S^2}{D^2} + S + D^2.$$

To minimize this we will chose $D = S^{2/3}L^{-1/3}$, which is ≥ 1 ssince $S^2 \geq L$. Hence $D^2 \asymp S^{4/3}L^{-2/3} \leq S^{2/3}L^{2/3}$ since $S \leq L^2$, and this results in an upper bound of $S^{2/3}L^{2/3}$. □

5.1. **Distinct Distance Theorem.**

Theorem 34. *(Guth-Katz) Let $P \subset \mathbb{R}^2$ be a set of points with $|P| = N$. Then P determines has at least $\frac{N}{\log N}$ distinct distances.*

Partial Symmetries: *(Elekes-Sharir):* Let G be a group of orientation preserving rigid motions of the plane,

$$G_r(P) = \{g \in G : \ |g(P) \cap P| \geq r\}.$$

For a generic set of N points we have that Le

$$|G_r(P)| = \begin{cases} \binom{N}{2} + 1 & r = 2 \\ 1 & r \geq 3 \end{cases}.$$

For the square $\sqrt{N} \times \sqrt{N}$ grid

$$|G_r(P)| \asymp \frac{N^3}{r^2}$$

for all $2 \leq r \leq \frac{N}{2}$.

Theorem 35. *(Elekes-Sharir $r = 3$, Guth-Katz for $r \geq 2$) Given $P \subset \mathbb{R}^2$, $|P| = N$ we have that*

$$|G_r(P)| \ll \frac{N^3}{r^2}$$

for all $r \geq 2$.

Let $d(P)$ be the set of distances, and set

$$Q(P) = \left\{(p_1, q_1, p_2, q_2) \in P^4 : \ |p_1 - q_1| = |p_2 - q_2| \neq 0\right\}.$$

Lemma 36. *Let $P \subset \mathbb{R}^2$, $|P| = N$. Then*

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

Proof. Let the i^{th} distance d_i occur n_i times as $|p - q|$, $p, q \in P$. Then

$$|Q(P)| = \sum_{i=1}^{|d(P)|} n_j^2 \geq \frac{1}{|d(P)|}\left(\sum n_j\right)^2 = \frac{1}{|d(P)|}(N^2 - N)^2.$$

□

To prove a lower bound on $d(P)$ we need to prove an upper bound on $Q(P)$, and this is related to the partial symmetries.

Proposition 37. *The number of quadruples is*

$$|Q(p)| = \sum_{r \geq 2} (2r - 2)|G_r(P)|.$$

Using the estimate $|G_r(P)| \ll \frac{N^3}{r^2}$, we find that

$$|Q(P)| \ll \sum_{r=2}^{N} \frac{N^3}{r} \sim N^3 \log N,$$

and the distinct distances theorem follows from the lemma.

Proof. (Of lemma 37) Let $E : Q(P) \to G_2(P)$ be defined by sending $(p_1, q_1, p_2, q_2) \in Q$ to the unique g such that

$$g(p_1) = p_2,\ g(q_1) = q_2.$$

The map E is not necessarily injective since if $|g(P) \cap P| = r$ then

$$|E^{-1}(g)| = 2\binom{r}{2}.$$

Write

$$G_{=r}(P) = \{g \in P :\ |g(P) \cap P| = r\}.$$

Then

$$Q(P) = \sum_{r=2}^{|P|} 2\binom{r}{2}|G_{=r}(P)|,$$

and

$$|G_{=r}(P)| = |G_r(P)| - |G_{r+1}(P)|,$$

and so

$$\begin{aligned} Q(P) &= \sum_{r\geq 2} |G_r(P)| \left(2\binom{r}{2} - 2\binom{r-1}{2}\right) \\ &= \sum_{r\geq 2} (2r-2)|G_r(P)|. \end{aligned}$$

□

Given $p_1, p_2 \in \mathbb{R}^2$ define

$$S_{p_1,p_2} = \{g \in G :\ g(p_1) = p_2\}.$$

This set is a 1-dimensional smooth curve that is diffeomorphic to a circle in G, which is a 3-dimensional space. $G_r(p)$ is exactly the set of $g \in G$ that lie in $\geq r$ points of the curves

$$\{S_{p_1,p_2}\}_{p_1,p_2 \in P}.$$

Thus our problem now begins to be a problem in incidence geometry if we can straighten the coordinates of G so that the S_{p_1,p_2} are lines. Let $G^{trans} \subset G$ be the translations inside G. The following lemma will allow us to ignore them from now on.

Lemma 38. *Given $P \subset \mathbb{R}^2$, $|P| = N$, then*

$$|G_r(P) \cap G^{trans}| \ll \frac{N^3}{r^2}.$$

Proof. Let g be a translation. The number of quadruples (p_1, q_1, p_2, q_2) such that $g(p_1) = p_2$ and $g(q_1) = q_2$ is at most N^3 since three points determine the fourth. Furthermore, $2\binom{r}{2}$ of such quadruples are associated to each $G_r(P) \cap G^{trans}$. Thus

$$|G_r(P) \cap G^{trans}| \leq \frac{N^3}{2\binom{r}{2}} \ll \frac{N^3}{r^2}.$$

□

Let $G' = G \backslash G^{trans}$ be the set of rotations in the plane. Define

$$\rho : G' \to \mathbb{R}^3$$

by

$$\rho(g) = (x, y, \cot\theta/2)$$

where (x, y) are the coordinates of the center and θ is the angle of rotation. This will be a bijection.

Lemma 39. *We have that*

$$\rho(S_{p_1,p_2} \cap G')$$

is a line ℓ_{p_1,p_2} in $\mathbb{R}^3$.

Proof. (Sketch) Given p_1, p_2, where $g(p_1) = p_2$, we must have that the center of the rotation of g is on the perpendicular bisector of p_1, p_2. Then $\cot\theta/2$ depends linearly on the position of the center of the rotation on that line, which gives a linear relation and hence a line in $\mathbb{R}^3$. □

Lemma 40. *The lines $\{\ell_{p_1,p_2}\}_{p_1,p_2\in\mathbb{R}^2}$ are all distinct.*

Proof. They represent different sets of rigid motions. □

Lemma 41. *We have that*

$$|G(P) \cap G'| = |P_r(\mathcal{L}(P))|$$

where $\mathcal{L}(P) = \{\ell_{p_1,p_2}\}_{p_1,p_2\in P}$ and $P_r(\mathcal{L})$ denotes the r-rich points, that is points in at least r lines.

Thus we would like to prove that

$$|P_r(\mathcal{L}(P))| \ll \frac{N^3}{r^2} \asymp \frac{|\mathcal{L}(P)|^{3/2}}{r^2},$$

and so the question is now: "What is the maximum number of r-rich points in a set of L lines?" We want this to be $\ll L^{3/2}/r^2$, but in general this is not true. It can fail if the lines cluster on some plane, or degree two surface. For example the grid construction gives L lines with L^2/r^3 r-rich points.\

6. Lecture 6

Let $\mathcal{L}(P) = \{\ell_{p_1,p_2}\}_{p_1,p_2\in P}$ and $P_r(\mathcal{L})$ denote the r-rich points, that is points in at least r lines. We would like to prove that

$$|P_r(\mathcal{L}(P))| \ll \frac{N^3}{r^2} \asymp \frac{|\mathcal{L}(P)|^{3/2}}{r^2},$$

and so the question is now: "What is the maximum number of r-rich points in a set of L lines?" We want this to be $\ll L^{3/2}/r^2$, but in general this is not true. It can fail if the lines cluster on some plane, or degree two surface. For example the grid construction gives L lines with L^2/r^3. We need to use the fact that the lines come from this specific algebraic construction.

Lemma 42. *$\mathcal{L}(P)$ contains at most $O(N)$ lines in any plane or degree 2 surface.*

We will prove this just for the plane.

Proof. For a fixed p, any two lines $\ell_{p,q}, \ell_{p,q'}$ are skew, meaning they are neither parallel nor intersecting. That is, they do not interesect in projective space. To see that they are disjoint, suppose $g(p) = q$. Then we cannot have $g(p) = q'$. Similarly, they cannot be parallel either. Hence for each $p \in P$ only one of $\ell_{p,q}$ can lie in a given plane, and so $S_0 \leq N$ lines in this plane. □

Theorem 43. *(Ket Incidence Estimate of Guth-Katz) $\mathcal{L}$ is a set of L lines in $\mathbb{R}^3$.*
(a) If there are at most $L^{1/2}$ lines in any degree 2 surface then $|P_2(\mathcal{L})| \ll L^{3/2}$.
(b) If there are at most $L^{1/2}$ lines in any plane, then for all $3 \leq r \leq 2L^{1/2}$

$$|P_2(\mathcal{L})| \ll \frac{L^{3/2}}{r^2}.$$

Reguli

Proposition 44. *For any 3 lines in $\mathbb{F}^3$ there is a non-zero polynomial of degree ≤ 2 vanishing on them.*

Proof. Pick three points on every line. Then since $\dim \mathrm{Poly}_2(\mathbb{F}_3^n)$ there exists a polynmial of degree at most 2 vanishing on these 9 points. Thus it vanishes on all three lines. □

Proposition 45. *If ℓ_1, ℓ_2, ℓ_3 are pairwise skew lines in $\mathbb{F}^3$ then there is an irreducible algebraic surface $R(\ell_1, \ell_2, \ell_3)$ which contains every line that intersects ℓ_1, ℓ_2, ℓ_3.*

This surface is called a *Regulus.*

Example 46. Let $S^1(q, r)$ denote the circle around q of radius r. Consider

$$\{g \in G' : \ g(p) \in S^1(q, r)\}.$$

First ruling: $\{\ell_{p,q'} : q' \in S^1(q, r)\}$
Second ruling: $\{\ell_{p',q} : p' \in S^1(p, r)\}$
Every $q \in R$ lies on one line from each ruling.

Theorem 47. *There exists a constant K such that if $\mathcal{L}$ is a set of L lines in $\mathbb{R}^3$ with $|P_3(\mathcal{L})| \geq KL^{3/2}$ then there is a plane that contains $\geq 10L^{1/2}$ lines of $\mathcal{L}$.*

Idea: Combinatorial Structure in the form of a polynomial of low degree vanishing on $\mathcal{L}$ –> Algebraic Struture $Z(P)$ has many flat points –> Geometric struture, this must be a plane.

Corollary 48. *If $\mathcal{L}$ is a set of L lines in $\mathbb{R}^3$ then there is a set of planes $\pi_1, \ldots, \pi_S$ where $S \leq L^{1/2}$ and disjoint $\mathcal{L}_i \subset \mathcal{L}$ so that $\mathcal{L}_i$ is contained in π_i and*

$$|P_3(\mathcal{L}) \backslash \cup_i P_3(\mathcal{L}_i)| \leq KL^{3/2}.$$

This corollary can be proven from the theorem using induction.

6.1. **Degree Reduction.** We begin by stating two well known theorems in algebraic geometry.

Theorem 49. *(Bezout's Theorem) Let $P, Q \in$ Poly$(\mathbb{F}^2)$ be two polynomials with no common factor. Then*

$$Z(P,Q) \leq (\deg P)(\deg Q).$$

Counting multiplicity in an algebraically closed field, this is an equality.

Theorem 50. *(Bezout's theorem for lines) $\mathbb{F}$ an infinite field. Then given $P, Q \in$ Poly $\left(\mathbb{F}^3\right)$ have no common factors. Then $Z(P,Q)$ has at most $(\deg P)(\deg Q)$ lines.*

Recall that if $S \subset \mathbb{F}^n$, $|S| < \dim \text{Poly}_D(\mathbb{F}^n) = \binom{D+n}{n}$, then $\deg S \leq D$, and $\deg(S) \leq n|S|^{1/n}$. Further more, if $\mathcal{L}$ is a set of L lines in $\mathbb{F}^n$, if $(D+1)L < \dim \text{Poly}_D(\mathbb{F}^n) = \binom{D+n}{n}$, then $\deg(\mathcal{L}) \leq D$ and $\deg(\mathcal{L}) \leq (2n+1)L^{1/(n-1)}$.

Proposition 51. *Let $\mathcal{L}$ be a set of lines over $\mathbb{F}^3$. Each line of $\mathcal{L}$ contains $\geq A$ points of $P_2(\mathcal{L})$. Then $\deg(\mathcal{L}) \ll \frac{L}{A}$.*

This is interesting when A is much greater than L. The bound cannot be improved below $L/(A+1)$ when $A \geq \sqrt{L}$. Take $L/(A+1)$ planes and $A+1$ lines in general position in each plane. Then the product of linear polynomials has degree $L/(A+1)$. Cannot do better. If P vanishes on $\mathcal{L}$. By Bezout's theorem for lines, either $\deg(P) \geq A+1$ or $Q_i | P$ for each linear factor Q_i, and so once again P has large degree. Hence

$$\deg P \geq \min\left\{A+1, \frac{L}{A+1}\right\}.$$

Thus when $A \geq L^{1/2}$, $\deg P \geq \frac{L}{A+1}$. To prove the proposition, we use a *contagious vanishing argument*

By parameter counting we may find a polynomial of degree $D \asymp \frac{L}{A}$ that vanishes on D^2 lines of $\mathcal{L}$. (Interesting case is when $D^2 \ll L$) Initially we use P to kill D^2 random lines, and we called these lines "infected." For each $\ell \in \mathcal{L}$, expected $\gg AD^2/L$ infected intersection points. If this is $> 10D$ then we expect P to vanish on most lines in $\mathcal{L}$.

Proof. (Of proposition) Let $p = \frac{1}{20}\frac{D^2}{L}$. Infect each line with probability p. Then with high probability

$$\#\text{infected lines} \leq \frac{1}{10}D^2.$$

Find a polynomial of degree $\ll D$ vanishing on the infected lines. Fix $\ell \in \mathcal{L}$. The expected number of infected points on ℓ is $\geq Ap = \frac{1}{20}D^2A/L \geq 10^4 D$ so now $D \approx 10^6 L/A$. If ℓ has $> D$ infected points then $P = 0$ on ℓ. This occurs with probability

$$> 1 - e^{-100D} > 1 - e^{10^7 L/A}.$$

If $L/A > 10^{-5}\log L$ then with high probability P vanishes on every line. If $L/A \leq 10^{-5}\log L$, then with high probability P vanishes on $\geq 99/100L$ lines of $\mathcal{L}$. To turn this in 100% of lines on $\mathcal{L}$ we use induction. The induction hypothesis is that $\deg(\mathcal{L}) \leq 10^7\frac{L}{A}$. There exists P_1 that vanishes on $\mathcal{L}_1 \subset L$, where $|\mathcal{L}_1| \geq \frac{99}{100}L$ does not vanish on $\mathcal{L}_2$, $|\mathcal{L}_2| \leq \frac{1}{100}L$. Each line intersects $Z(P)$ at $\leq \deg(P_1)$ so it has $\geq A - \deg(P_1)$ intersection points with other lines in $\mathcal{L}_2$. $A \geq 10^5 L/\log L$,

$\deg P_1 \leq 10^6 L/A \leq 10 \log L$ which is $\geq 9A/10$. By induction, $\deg(\mathcal{L}_2) \leq 10^6 L/A$ and so the degree of the entire set of lines

$$\deg(\mathcal{L}) \leq \deg(\mathcal{L}_1) + \deg(\mathcal{L}_2) \leq 10^7 L/A,$$

which finishes the proof. □

The main take away from this lecture was degree reduction. To first get the polynomial to vanish on a small fraction of the lines and then "infect" the rest. The reason for this is that low degree polynomial conditions are contagious, since the vanishing lemma tells us that if it vanishes on a certain small set of points, then it vanishes on an entire line.

7. Lecture 7

Last time we discussed the key incidence estimates for $\mathcal{L}$ a set of L lines in $\mathbb{R}^3$:
(a) If there are $\leq \sqrt{L}$ lines lying in any plane or degree two surface, then $|P_2(\mathcal{L})| \ll L^{3/2}$
(b) If there are $\leq \sqrt{L}$ lines in any plane, then $|P_r(\mathcal{L})| \ll L^{3/2}/r^2$ for every $3 \leq r \leq 2\sqrt{L}$
Planar Clustering

Theorem 52. *Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$. Then there exists a constant K such if each line contains $\geq A = KL^{1/2}$ points of $P_3(\mathcal{L})$, then $\mathcal{L}$ lies in $\leq KL/A$ planes.*

Corollary 53. *Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$ where there are $\leq B$ lines in any plane. If $B \geq \sqrt{L}$, then $|P_3(\mathcal{L})| \ll BL$.*

Degree Reduction

- Let P be the minimum degreee non-zero polynomial vanishing on $\mathcal{L}$.
- $\deg P \ll L/A$
- *Goal:* Show that P is a product of linear factors. ($Z(P)$ is a union of at most L/A planes)
- $x \in P_3(\mathcal{L})$
- If 3 lines are not coplanar, then x is a critical point of P
- If 3 lines are coplanar, then $Z(P)$ is *flat* at x.

Lemma 54. *Every point of $P_3(\mathcal{L})$ is either a critical point or a flat point of $Z(P)$.*

Being critical/flat is contagious because it is a low-degree polynomial condition.

Lemma 55. *For any polynomial $P \in Poly_D(\mathbb{R}^3)$, then there is a list of 9 polynomials*

$$SP_1, \ldots, SP_9 \in Poly_{3D}(\mathbb{R}^3)$$

such that $x \in Z(P)$ is critical or flat if and only if

$$SP_1(x) = \cdots = SP_9(x) = 0.$$

In particular this lemma implies that being critical or flat is a contagious condition since if $\ell \in \mathcal{L}$ contains $\geq A > 3D$ points of $P_3(\mathcal{L})$, then SP_j vanishes on ℓ, and so ℓ is critical or flat.
Flat Points

Definition 56. Let $\mathcal{M}$ be a smooth 2-manifold in $\mathbb{R}^3$, and let $x \in \mathcal{M}$. By a coordinate change we can assume that $x = 0$, and that the tangent plane at x is $x_3 = 0$. Locally near 0 $\mathcal{M}$ is described by a fucntion

$$x_3 = h(x_1, x_2)$$

where $h(0) = 0$ and $\nabla h(0) = 0$. We say that x is *flat* if and only if the second derivative of h vanish.

Equivalently, we can define flatness by the normal vector.

Definition 57. Let $\mathcal{M}$ be a smooth 2-manifold in $\mathbb{R}^3$, and let $N : \mathcal{M} \to S^2$ be the unit normal vector. We say that $x \in \mathcal{M}$ is *flat* if the derivatives of N vanish at x. In otherwords $dN_x : T_x M \to T_{N(x)} S$ is zero.

Lemma 58. *Suppose that x lies in 3 lines in $Z(P)$. Then x is either critical or a flat point of $Z(P)$.*

Proof. There are two cases. When the there lines are non-coplanar, then $\nabla P(x) \cdot u = 0$ in each of the three directions u corresponding to the three lines. This implies that $\nabla P(x) = 0$ since the lines are not coplanar, and so x is a critical point. For the second case, suppose that $\nabla P(x) \neq 0$. Then we can translate and rotate so that $x = 0$ and $Z(P)$ is given by $x_3 = h(x_1, x_2)$ locally at the origin, and the tangent plane is the horizontal plane. Taylor expanding we have that

$$h(x_1, x_2) = h_2(x_1, x_2) + O(|x|^3),$$

and $h_2(x_1, x_2)$ is a homogenous polynomial of degree 2. This polynomial must vanish on 3 lines in the $x_1 x_2$-plane. By the vanishing lemma, this implies that $h_2 \equiv 0$, and so x is a flat point. □

Flatness as an algebraic condition

It is easy to see that being critical is an algebraic condition, since x is a critical point for P if and only if $\nabla P(x) = 0$, and this gives rise to three degree $D - 1$ polynomials, all of which need to equal 0.

Suppose that x is a non-critical point of $Z(P)$. Let $N = \frac{\nabla P}{|\nabla P|}$ be the unit normal to $Z(P)$. Then if x is flat, $\partial_v N(x) = 0$ for all $v \in T_x Z(P)$. How can we write this as a polynomial condition? Observe that if

(1) $\partial_v N = 0$ if and only if $\partial_v \nabla P$ is parallel to ∇P, if and only if $\partial_v \nabla P \times \nabla P = 0$.

(2) $\{e_1 \times \nabla P, e_2 \times \nabla P, e_3 \times \nabla P\}$ is a spanning set for $T_x Z(P)$.

Now, define

$$SP(x) : \left\{\partial_{e_j \times \nabla P} \nabla P \times \nabla P\right\}_{j=1,2,3},$$

and

$$\deg SP_j \leq 3 \deg P.$$

This whole discussion proves the following propostion:

Proposition 59. *If $x \in Z(P)$, $SP(x) = 0$ if and only if x is critical or flat.*

What happens if every point of $Z(P)$ is flat?

Lemma 60. *Let P be an irreducible polynomial in $\mathbb{R}^3$ and suppose that SP vanishes on $Z(P)$. Then if $Z(P)$ contains a non-critical point, we must have that $\deg P = 1$ and $Z(P)$ is a plane.*

The condition that $Z(P)$ contains at least one non-critical point is to avoid degeneracies, such as those given by $x_1^2 + x_2^2 = 0$.

Proof. Let $x \in Z(P)$ be the non-critical point. Then in a neighborhood of x $Z(P)$ is a flat submanifold, so it's normal vector is constant and it's neighborhood must be an open subset of the plane. By the vanishing lemma, $Z(P)$ contains a whole plane, and so P is divisible by a linear polynomial. Since P is irreducible, this implies that $\deg P = 1$. □

We sum up the work so far the following lemma.

Lemma 61. *(Plane detection lemma) For every $P \in Poly(\mathbb{R}^3)$ there exists a list of nine polynomials $SP(x) = (SP_1(x), \ldots, SP_9(x))$ such that*

(1) *If $x \in Z(P)$, then $SP(x) = 0$ if and only if x is critical or flat.*

(2) *If x is contained in 3 lines in $Z(P)$ then $SP(x) = 0$.*

(3) $\deg SP \leq 3 \deg P$

(4) *If P is irreducible, SP vanishes on $Z(P)$ and $Z(P)$ contains a non-critical point, then $Z(P)$ is a plane.*

Using this lemma we will prove the plane clustering lemma.

Proof. Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$. Each contains $\geq A \geq KL^{1/2}$ points of $P_3(\mathcal{L})$. Let P be the minimum degree non-zero polynomial vanishing on $\mathcal{L}$. By degree reduction, $\deg P \ll \frac{L}{A} \leq \frac{\sqrt{L}}{A}$. Factor P into irreducibles

$$P = \prod_j P_j$$

and let $\mathcal{L}_{mult}$ be the lines in $\mathcal{L}$ lying in multiple $P_j's$. By Bezout's lemma for lines,

$$|\mathcal{L}_{mult}| \leq \sum_{j,j'} (\deg P_j)(\deg P_{j'}) = (\deg P)^2 \leq \frac{L}{10^4}.$$

Let $\mathcal{L}_j$ be lines of $\mathcal{L}$ in $Z(P_j)$ but not other $Z(P_j')'s$.

Claim. Each $\ell \in \mathcal{L}_j$ contains at least $\frac{99}{100}A$ points of $P_3(\mathcal{L})$.

Proof. ℓ contains $\geq A$ poitns of $P_3(\mathcal{L})$ and has few interesections with lines from other $Z(P_j')$ because ℓ can only intersect $Z(P_{j'})$ at $\leq \deg P_{j'}$ points. □

Since P is the minimum degree polynomial that vanishes on L, this implies that P_j is the minimum degree polynomial vanishing on $\mathcal{L}_j$, and so

$$\deg P_j \leq \frac{|\mathcal{L}_j|}{A} \leq \frac{\sqrt{L}}{100}.$$

At each $x \in P_3(\mathcal{L}_j)$ we have that $SP_j(x) = 0$. Now we use the contagious structure. Each $\ell \in \mathcal{L}_j$ contains $\geq \frac{99}{100}A > 3 \deg P_j$ points of $P_3(\mathcal{L}_j)$. SP_j vanishes on $P_3(\mathcal{L}_j)$ implies that SP_j vanishes on all of $\mathcal{L}_j$. Since P_j is irreducible, Bezout's theorem for lines implies that SP_j vanishes on $Z(P_j)$, or $Z(SP_j) \cap Z(P_j)$ has at most

$$\begin{aligned} (\deg SP_j)(\deg P_j) &\leq 3(\deg P_j)^2 \\ &< |\mathcal{L}_j| \end{aligned}$$

lines. Since the second case has too few lines, we must have that SP_j vanishes on $Z(P_j)$. It remains to show that $Z(P)$ contains a regular point. If not, then ∇P vanishes everywhere, and hence on all of the lines. But this contradicts the minimum degree hypothesis in the same way that it did for the joints problem. Hence $Z(P_j)$ must be a plane for each j. Thus

$$\#\text{planes} \leq \deg P \ll \frac{L}{A}.$$

This finishes the proof of the plane clustering theorem. □

8. Lecture 8

We will need a version of the plane detection lemma that applies to 2-rich points, and handles reguli.

Theorem 62. *(Guth-Katz) Let $\mathcal{L}$ be a set of L lines in $\mathbb{R}^3$ or $\mathbb{C}^3$ with $\leq B$ lines in any plane or degree 2 surface. Then*

$$|P_2(\mathcal{L})| \ll LB + L^{3/2}.$$

Recall that for a regulus (e.g. $z = xy$) L lines can make $\frac{1}{4}L^2$ intersections, and there are $\frac{L}{B}$ planes/reguli, and B lines on each forming $\frac{1}{4}B^2$ 2-rich points.

Remark 63. When $B = 10$, there are no good examples, and so whether or not this can be improved is an open question.

8.1. Classification of doubly ruled surfaces.

Theorem 64. *Given an irreducible polynomial $P \in Poly(\mathbb{C}^3)$, if $Z(P)$ is doubly-ruled, that is if every point in $Z(P)$ is contained in 2 lines in $Z(P)$, then $\deg P =$ 1 or 2, and so $Z(P)$ is a plane or a regulus.*

Remark 65. Theorem 62 of Guth and Katz is a strong quantitative version of theorem 64 above.

Next we introduce a notion that is helpful for understanding ruled surfaces.

Definition 66. We say that $z \in Z(P)$ is *flecnodal* if P vanishes at z to third order in some direction.

In particular, if $z \in Z(P)$ lies in a line in $Z(P)$ then it is flecnodal. This is not the only such situation, in the early 20th century Salmon gave what is known as Salmon's Flecnodal polynomial, $\text{Flec}P \in \text{Poly}(\mathbb{C}^3)$. This polynomial satisfies $\text{Flec}P \leq 11 \deg P$ and $z \in Z(P)$ is flecnodal if and only if $\text{Flec}P(z) = 0$.

Theorem 67. *(Local-to-Global, Monge-Cayley-Salmon) If $P \in Poly(\mathbb{C}^3)$ and every point on $Z(P)$ is flecnodal, then $Z(P)$ is ruled.*

Guth an Katz generalized this theorem to *doubly flecnodal points.*

Theorem 68. *(Guth-Katz) If $P \in Poly(\mathbb{C}^3)$ is doubly flecnodal at every point, then $\deg P = 1$ or 2, and $Z(P)$ is a plane or regulus. Furthermore, there is a list of $O(1)$ polynomials of degree $O(\deg P)$ that detects whether $Z \in Z(P)$ is doubly flecnodal.*

Using this result, we can extend the Szemeredi-Trotter theorem, theorem 26, to $\mathbb{R}^3$.

Theorem 69. *(Guth-Katz) Let $\mathcal{S}$ be a set of S points, and $\mathcal{L}$ a set of L lines in $\mathbb{R}^3$, such that there are $\leq B$ lines of $\mathcal{L}$ in any plane where $B \geq \sqrt{L}$. Then*

$$I(\mathcal{S}, \mathcal{L}) \ll S^{1/2}L^{3/4} + B^{1/3}L^{1/3}S^{2/3} + L + S.$$

Each of these three terms above can be shown to be optimal by considering explicit examples. Firstly, let

$$\mathcal{S} = \left\{(a, b, \epsilon) : \ 1 \leq a, b \leq L^{1/4}, \ \epsilon \in \{0, 1\}\right\},$$

and let $\mathcal{L}$ be the set of all lines connecting an element of one plane to an element of the other. This yields $L = S^{1/2}L^{3/4}$. The second example is given by L/B planes and B lines on each plane, using the grid example for the Szemeredi-Trotter theorem.

To prove this theorem we will use the polynomial partitioning theorem. Let P have degree $\leq D$, and split $\mathbb{R}^2 \backslash Z(P)$ into cells of $\ll S/D^2$ points. Split up the incidences into three sets

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

For $\mathbb{R}^3$, we apply a similar strategy as we did in $\mathbb{R}^2$. Control $I(\mathcal{S}_{alg}, \mathcal{L}_{alg})$, and divide $Z(P)$ into planar and non-planar parts.

$$I(\mathcal{S}_{alg}, \mathcal{L}_{alg}) = I(\mathcal{S}_{alg}, \mathcal{L}_{pl}) + I(\mathcal{S}_{alg}, \mathcal{L}_{alg} \backslash \mathcal{L}_{pl})$$

where $\mathcal{L}_{pl}$ are those points in planes, to which we may apply Szemeredi-Trotter. Define the special points to be those that are flat or non-critical. Then

$$I(\mathcal{S}_{alg}, \mathcal{L}_{alg} \backslash \mathcal{L}_{pl}) \leq I(\mathcal{S}_{non-sp}, \mathcal{L}_{alg}) + I(\mathcal{S}_{sp}, \mathcal{L}_{non-sp}) + I(\mathcal{S}_{sp}, \mathcal{L}_{sp} \backslash \mathcal{L}_{pl}).$$

Each of these terms can be bounded using our previous lemmas.