The Polynomial Method

Professor Larry Guth

Friday, October 5

Today will be the last background lecture in incidence geometry. We finish it off with a discussion of a cool new way to approach the distinct distance problem; this approach, due to Elekes, has connections with the incidence geometry of lines in $\mathbb{R}^3$. Before going into this, let's have a brief recap of the problem we were interested in.

Problem 1 (Review). *Suppose there are N points in $\mathbb{R}^2$, with the number of distinct distances between pairs of these points equal to $t \ll N$. What can we say about the incidence geometry?*

The way we were thinking about this was to draw circles around the points under consideration, and noting that we expect a great many points to lie on the boundaries of other circles. But clearly, in that setting, we are not using all the information we have; in particular, we are never accounting for the fact that some of the circles may have equal radii, which would also decrease the value of t. How can we somehow encode this information?

Suppose we denote our set of points in the plane by $P \subset \mathbb{R}^2$; let $d(P)$ be the set of nonzero distances between points in P, and $Q(P)$ be a measure of how two different pairs of points can have the same nonzero distance between them. Formally speaking,

$$d(P) := \{|p_1 - p_2| : (p_1, p_2) \in P^2\},$$

and

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

Since P is a fixed set, and we are given $|d(P)|$ is large, we expect $|Q(P)|$ to be small. And indeed, this turns out to be the case.

Lemma 1. *With $d(P)$ and $Q(P)$ defined as above, we have $|d(P)| \cdot |Q(P)| \geq (N^2 - N)^2 \gtrsim N^4$.*

Proof. Suppose $d(P) = \{d_1, \cdots, d_s\}$ be the s possible nonzero distances in P, with $|d(P)| = s$. For $1 \leq j \leq s$, define

$$n_j = \Bigg|\{(p_1, p_2) \in P^2 : |p_1 - p_2| = d_j\}\Bigg|.$$

We immediately have $\sum_j n_j = N^2 - N$, since the left hand side just counts the number of ordered pairs of points with nonzero distance between them, which is just the number of ordered pairs $(p_1, p_2) \in P^2$ with $p_1 \neq p_2$, which is $2\binom{N}{2} = N^2 - N$.

Now, we also have $|Q(P)| = \sum_j n_j^2$. This is because we can pick some distance d_j, and then count (p_1, q_1, p_2, q_2) with $|p_1 - q_1| = |p_2 - q_2| = d_j$. So we want to choose two elements[1] from the set $\{(p_1, p_2) \in P^2 : |p_1 - p_2| = d_j\}$, which can be done in n_j^2 ways. Putting everything together, we can combine them using Cauchy-Schwarz as follows:

$$N^2 - N = \sum_{j=1}^{s} n_j \leq \left(\sum_{j=1}^{s} n_j^2\right)^{1/2} \cdot \left(\sum_{j=1}^{s} 1\right)^{1/2} = |Q(P)|^{1/2} \cdot s^{1/2} = |Q(P)|^{1/2} \cdot |d(P)|^{1/2},$$

so that $|Q(P)| \cdot |d(P)| \geq (N^2 - N)^2 \gtrsim N^4$, as desired. □

Lemma 1 is not surprising, because if there are few distances, we expect there to be a lot of quadruples. We want to somehow count these quadruples in another way so as to preserve some more information. To this end, define G to be the group of orientation-preserving rigid motions of the plane.

Lemma 2. *Suppose $p_1 \neq p_2$. Then we have $|p_1 - q_1| = |p_2 - q_2|$ if and only if there exists a unique $g \in G$ such that $g(p_1) = p_2$ and $g(q_1) = q_2$.*

Proof. This is trivial, essentially by inspection. For the $\Longrightarrow$ direction, note that there is certainly some $g \in G$ with $g(p_1) = p_2$ and $g(q_1) = g(q_2)$, defined by first taking p_1 to p_2 by a translation, and then rotating about p_1 until q_1 goes to q_2. Uniqueness follows from the uniqueness of these two steps. The $\Longleftarrow$ direction is trivial from the fact that G preserves orientations. □

Now, which rigid motions take p_1 to p_2? To better answer this question, we need to somehow find geometric structures that encode this group theoretic information. So let

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

This is a 1-dimensional curve in G, which is a 3-dimensional Lie group. We can now restate Lemma 2 in a slightly different way (the proof is the same, hence omitted). Furthermore, define $\mathbb{S} := \{S_{p_1,p_2}\}_{p_1,p_2 \in P}$. In other words, $\mathbb{S}$ is the collection of all these curves inside G. Clearly, since $|P| = N$, $\mathbb{S}$ consists of N^2 curves in G.

Lemma 3. *Suppose $p_1 \neq p_2$. Then,*

$$|p_1 - q_1| = |p_2 - q_2| \Longrightarrow |S_{p_1,p_2} \cap S_{q_1,q_2}| = 1;$$
$$|p_1 - q_1| \neq |p_2 - q_2| \Longrightarrow |S_{p_1,p_2} \cap S_{q_1,q_2}| = 0.$$

The problem, therefore, reduces to looking at the incidence pattern of curves in $\mathbb{S}$. It is simple to check that a point lies on two of these curves if and only if it corresponds to exactly two quadruples, and a point lies on three of these curves if and only if it corresponds to exactly three quadruples, and so on. This naturally gives way to the following definition.

$$G_{=k} := \{g \in G : g \text{ lies in exactly } k \text{ curves of } \mathbb{S}.\}.$$

[1] Note that we do not need *distinct* elements here, because of the way we have defined $Q(P)$, although this observation does not matter too much.

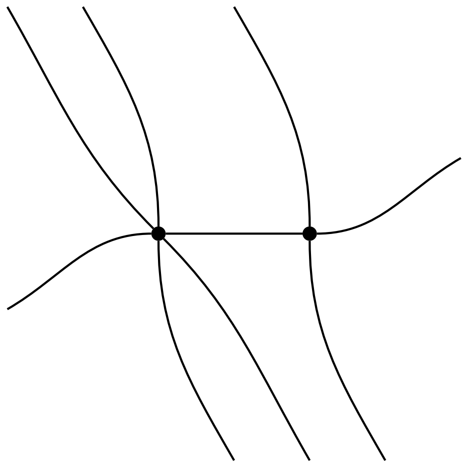


Figure 1: The bold lines represent curves in $\mathbb{S}$. The point on the left represents six quadruples, while the one on the right represents just two.

Furthermore, let $E : Q(P) \to G$ be given by Lemma 3, where E is the map that takes any quadruple to the corresponding element $g \in G$. Since quadruples correspond to at least two curves in $\mathbb{S}$ intersecting, it follows that

$$\mathrm{im}(E) \subseteq \bigcup_{k \geq 2} G_{=k}.$$

Now consider some $g \in G_{=k}$. Since the order of curves within the quadruples does not matter, we also have

$$\left| E^{-1}(g) \right| = 2\binom{k}{2},$$

since any two of the curves through g in $\mathbb{S}$ are mapped by E to g, with the factor of 2 arising due to the fact that we consider ordered pairs. The following lemma is immediate.

Lemma 4. *We have the estimate*

$$|Q(P)| = \sum_{k \geq 2} |G_{=k}| \cdot 2\binom{k}{2}.$$

Proof. This is immediate from the previous paragraph; any quadruple corresponds to precisely one k, and in $G_{=k}$, precisely $2\binom{k}{2}$ quadruples map to the same point. □

Usually, instead of the somewhat awkward $G_{=k}$, we find it easier to deal with the quantity

$$G_k := \{g \in G : g \text{ lies in} \geq k \text{ curves in } \mathbb{S}\}.$$

With that definition, Lemma 4 can be rewritten as

Lemma 5. *We have* $|Q(P)| \sim 2\sum_{k \geq 2} k|G_k|$.

Proof. Using Lemma 4, we immediately get

$$\begin{aligned}
|Q(P)| &= \sum_{k\geq 2} |G_{=k}| \cdot 2\binom{k}{2} \\
&= \sum_{k\geq 2} \left(|G_k| - |G_{k+1}|\right)(k^2 - k) \\
&= \sum_{\ell\geq 2} |G_\ell| \cdot \left((\ell^2 - \ell) - ((\ell-1)^2 - (\ell - 1))\right) \\
&= \sum_{\ell\geq 2} |G_\ell| \cdot \left(\ell^2 - \ell - \ell^2 + 2\ell - 1 - \ell + 1\right) \\
&= \sum_{\ell\geq 2} |G_\ell| \cdot (2\ell - 2) \\
&\sim 2\sum_{\ell\geq 2} \ell \cdot |G_\ell|.
\end{aligned}$$

□

Another way to look at G_k is to notice the following alternative formulation.

Lemma 6. *We have*

$$G_k = \{g \in G : |gP \cap P| \geq k\}.$$

Proof. This follows trivially from the way we defined the group G. A way to view any $g \in G$ is to note that triangles transform to congruent (orientation-preserving) triangles under g, and then note that for each such transformation, the image is in both gP and in P. □

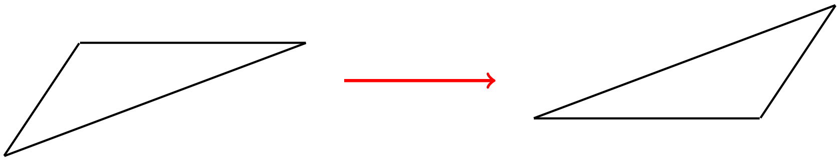


Figure 2: Triangles map to congruent triangles under $g \in G$.

Since this kind of generalizes specific notions of symmetry (relaxing the condition $gP = P$ a little bit), these can be thought of as "partial" symmetries, in a loose sense of the term.

It is time for an example.

Example. Suppose P is an $s \times s$ square grid, with $N = s^2$. What is $|G_{s^2}|$? This is easy, because the only transformations where all s^2 of the points map to themselves in some order are just the four rotations (by 0, $\pi/2$, π and $3\pi/2$ respectively), and hence, $|G_{s^2}| = 4$. What about $G_{s^2/10}$? For this and other similar examples, it can be proven that $|G_k| \lesssim N^3 k^{-2}$ for all $2 \leq k \lesssim N/10$; the proof is nontrivial, and will be presented later using the polynomial method. It is worth remarking, however, that a lower bound of $\sim s^2$ can be immediately seen by "shifting" along both axes. The result above used to be a conjecture, so we state it for the sake of completeness. We will prove it later in class.

We now come to the two major conjectures due to Elekes and Sharir that we are concerned with. The proofs are left for later. We state the first one now, and state the second one a little later in the explosition.

Conjecture 1 (ES1)**.** *If $P \subset \mathbb{R}^2$ is defined as above, with $|P| = N$, and $2 \leq k \leq N$, then $|G_k| \lesssim N^3 k^{-2}$.*

At the outset, note that if Conjecture 1 were true, it would have a couple of nice immediate corollaries.

Corollary. *We have $|Q(P)| \lesssim 2\sum_{k\geq 2} k|G_k| \lesssim \sum_{k\geq 2} N^3 k^{-1} \lesssim N^3 \log(N)$.*

Corollary. *We have $|d(P)| \gtrsim N^4/|Q(P)| \gtrsim N/\log(N)$.*

This chain of consequences will be shown to be true using the polynomial method. For now, let us make a few remarks about the tightness of the bounds given: the first corollary can be shown to be tight, up to a constant factor, since each inequality within the statement is essentially tight. The second, however, is unclear, since we used Cauchy-Schwarz in getting the result, and so we could have lost quite a bit of sharpness. In fact, probabilistically, it is reasonable to expect something like $N/\sqrt{\log(N)}$ for arbitrary $d(P)$. In fact, recall that we proved this exact expression earlier for the square grid.

Let's work with some specific instances of these rigid motions. First we have the translations $T \subset G$. As a group, it is obvious that T is congruent to $\mathbb{R}^2$. So now, we have the following lemma.

Lemma 7. *We have $|T \cap G_k| \lesssim N^3 k^{-2}$.*

Proof. Consider the set of translation quadruples $Q_T \subset Q(P)$, defined as

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

First observe that $|Q_T| \lesssim N^3$, since as soon as we pick any three of the points p_1, q_1, p_2, q_2, there remains at most one choice for the fourth one. Recall our definition of the map E from our earlier discussions. Clearly, that map induces a map between the subgrups $E : Q_T \to T$, where the left side sits inside $Q(P)$ and the right side sits inside G, in the same way as before. So our earlier arguments follow through within these subgroups, if $g \in G_k$, then $|E^{-1}(g)| \sim k^2$. In particular, as before, we have

$$|Q_T| \gtrsim |G_k \cap T| \cdot 2\binom{k}{2},$$

that is,

$$N^3 \gtrsim |G_k \cap T| \cdot k^2 \iff |T \cap G_k| \lesssim N^3 k^{-2},$$

as desired. □

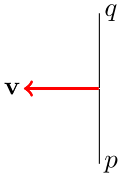
It remains to deal with $G' := G/T$. In fact, we can reduce this to the study of the incidence theory of lines and points in three-dimensional Euclidean space. We can do this by a process called "straightening". To this end, observe that G' can be viewed as the group of rotations about a **unique** fixed point $(x, y) \in \mathbb{R}^2$ by a **unique** angle $\theta \in (0, 2\pi)$, where 0 is excluded because we want nontrivial rigid motions. So now we can define the map $\rho : G' \to \mathbb{R}^3$ by

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

Before we can proceed further, we need the following proposition.

Proposition 1. *For any $p, q \in P$, the curve $\rho(S_{p,q} \cap G')$ is a* ***straight line*** *in $\mathbb{R}^3$.*

Proof. The key is to notice that when we rotate from p to q, the point of rotation lies on the perpendicular bisector of p and q. A little bit of trigonometry then yields the result.

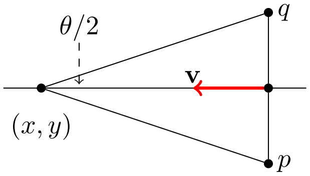


In the diagram, $\mathbf{v}$ is the perpendicular bisector of q and p, and is of length $|q-p|/2$. Furthermore, it represents the rotation of $(q-p)/2$ by $\pi/2$ in the positive direction. □

We can strengthen the above proposition a little bit.

Proposition 2. *For any $p, q \in \mathbb{R}^2$, let $\mathbf{v} = (\frac{p_2-q_2}{2}, \frac{q_1-p_1}{2})$, that is, $\mathbf{v}$ is the vector perpendicular to $p - q$ with length $|p - q|/2$. Furthermore, let $a = (p + q)/2$. Then, the curve $\rho(S_{p,q} \cap G')$ is the line parametrized by $\ell_{p,q} : t \mapsto (a + t\mathbf{v}, t)$.*

Proof. We have the following diagram.



If $g \in S_{p,q}$, suppose g has coordinates (x, y, θ). Now, we know (x, y) lies in the perpendicular bisector of the line segment pq, so that $(x, y) = a + t\mathbf{v}$ for some t. To find the t, simply observe that $\cot(\theta/2) = t \cdot |\mathbf{v}|/|\mathbf{v}| = t$, to finish off the proof. □

Let us put everything together now. Define $\mathscr{L} = \{\ell_{p,q}\}_{p,q\in P}$ be the set under consideration, with $\sim N^2$ lines by easy arguments. $|G'_k|$ is the number of points that lie on $\geq k$ lines in $\mathscr{L}$. Note that the incidence geometry depends on whether these lines are coplanar or not. We can handle this with the following quick lemma.

Lemma 8. *If $q \neq r$, then $\ell_{p,q}$ and $\ell_{p,r}$ are skew.*

Proof. First note that $\ell_{p,q}$ and $\ell_{p,r}$ do not intersect: this is because $S_{p,q} = \{g \in G : g(p) = q\}$, and $S_{p,r} = \{g \in G : g(p) = r\}$, and so if $S_{p,q} \cap S_{p,r} \neq \varnothing$, then there is some $g \in G$ with $g(p) = q$ and $g(p) = r$, so that $q = r$, contradiction. So $S_{p,q} \cap S_{p,r} = \varnothing$, and hence $\ell_{p,q} \cap \ell_{p,r} = \varnothing$. To show that they are not parallel, consider their three-dimensional "slopes". We have

$$\text{slope}(\ell_{p,q}) = ((dx/dz, dy/dz)) = \mathbf{v}(p, q),$$

and similarly for $\ell_{p,r}$, and so if they were the same, then $\mathbf{v}(p, q) = \mathbf{v}(p, r)$, which means

$$\left(\frac{p_2 - q_2}{2}, \frac{q_1 - p_1}{2}\right) = \left(\frac{p_2 - r_2}{2}, \frac{r_1 - p_1}{2}\right) \iff (q_1, q_2) = (r_1, r_2),$$

so that $q = r$, contradiction. So their slopes are different, proving skewness. □

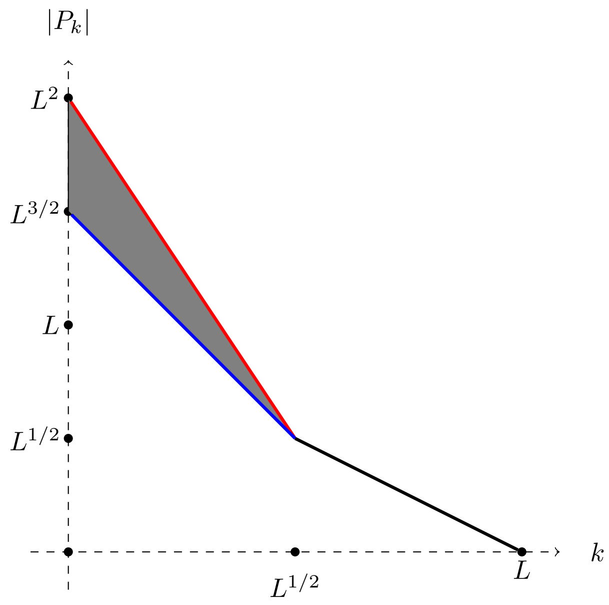


Figure 3: The solid red line and the solid blue line give the upper bounds corresponding to Szemerédi-Trotter and today's methods respectively. The solid black line is common to both results. The gray triangle is the area we improved by.

This has the following corollary.

Corollary. *There are at most N lines of $\mathscr{L}$ through any point, and at most N lines of $\mathscr{L}$ through any plane.*

Quite a bit harder is to prove that there are also at most N lines of $\mathscr{L}$ through any degree-2 surface. This will also be proven later in class. Let us finish up with two major conjectures.

Conjecture 2 (ES2A)**.** *If $\mathscr{L}$ is a set of L lines with at most $L^{1/2}$ in any plane or degree-2 surface, then $|P_2| \lesssim L^{3/2}$.*

Conjecture 3 (ES2B)**.** *If $\mathscr{L}$ is a set of L lines with at most $L^{1/2}$ in any plane, and $3 \leq k \leq L^{1/2}$, then $|P_k| \lesssim L^{3/2}k^{-2}$.*

To summarize, we may draw yet another log-log graph of our current bounds. This is depicted in Figure 3. Today's method improves over the Szemerédi-Trotter bound by a small triangle in out plot!

This finishes the background on incidence geometry. We will continue with the polynomial method from Wednesday.