Chapter 8: Distinct intersection points

Adam Sheffer

May 10, 2015

This Chapter is a continuation of Chapters 6 and 7, and in it we conclude the proof of the Guth-Katz distinct distances theorem [3].

1 Degree reduction

Before completing the distinct distances proof, we introduce another useful technique that involves polynomials: *degree reduction*. The beginning of this section, as well as the proof of Claim 2.2 below, are based on lecture notes by Guth [2]. We begin by deriving the following simple claim.

Claim 1.1. *Let $\mathcal{L}$ be a set of n lines in $\mathbb{R}^3$. Then there exists a nontrivial polynomial $f \in \mathbb{R}[x_1, x_2, x_3]$ of degree smaller than $3\sqrt{n}$ that vanishes on all the lines of $\mathcal{L}$.*

Proof. Let $\mathcal{P}$ be a set of at most $4n^{3/2}$ points, that is obtained by arbitrarily choosing $4\sqrt{n}$ points from every line of $\mathcal{L}$. Since $\binom{3\sqrt{n}+3}{3} > 4n^{3/2}$, by Lemma 2.1 of Chapter 5 there exists a nontrivial polynomial $f \in \mathbb{R}[x_1, x_2, x_3]$ of degree at most $3\sqrt{n}$ that vanishes on $\mathcal{P}$. Consider a line $\ell \in \mathcal{L}$. Since f vanishes on at least $4\sqrt{n}$ points of ℓ, Bézout's theorem implies that ℓ is contained in $Z(f)$. □

When every line of $\mathcal{L}$ contains many intersection points with other lines of $\mathcal{L}$, we can improve the bound of Claim 1.1. The proof of the following lemma combines ideas from the polynomial method with ideas from the probabilistic method.

Lemma 1.2. *Let $\mathcal{L}$ be a set of n lines in $\mathbb{R}^3$, such that each line of $\mathcal{L}$ contains at least k distinct points where it intersects other lines of $\mathcal{L}$ (k may depend on n). Then there exists a nontrivial polynomial $f \in \mathbb{R}[x_1, x_2, x_3]$ of degree $O\left(n^{3/4}/\sqrt{k}\right)$ that vanishes on all the lines of $\mathcal{L}$.*

Proof. When $k \le 50^2\sqrt{n}$, the lemma is implied by Claim 1.1. Thus, we may assume that $k > 50^2\sqrt{n}$. Moreover, we may assume that n is sufficiently large, since otherwise the lemma is obtained by taking a large constant in the $O(\cdot)$-notation.

We set a probability $p = 100\sqrt{n}/k$, and consider a subset $\mathcal{L}' \subset \mathcal{L}$ that is obtained by choosing every line of $\mathcal{L}$ with probability p. With positive probability, $|\mathcal{L}'| < 200n^{3/2}/k$ and every line of $\mathcal{L} \setminus \mathcal{L}'$ has at least $\sqrt{n}$ intersection points with lines of $\mathcal{L}'$. The full details of this standard probabilistic calculation can be found in appendix

A. Since this scenario occurs with positive probability, there indeed exists a subset $\mathcal{L}'$ that satisfies these properties. We consider such a subset.

By Claim 1.1, there exists a nontrivial polynomial $f \in \mathbb{R}[x_1, x_2, x_3]$ of degree at most $3 \cdot \sqrt{200}n^{3/4}/\sqrt{k} < 45n^{3/4}/\sqrt{k}$ that vanishes on every line of $\mathcal{L}'$. Consider a line $\ell \in \mathcal{L} \setminus \mathcal{L}'$. Since $k > 50^2\sqrt{n}$, we have that $\deg f < \sqrt{n}$. Since f vanishes on at least $\sqrt{n}$ points of ℓ, Bézout's theorem implies that ℓ is contained in $Z(f)$. □

2 Ruled surfaces

We now recall where we stand in the proof of the distinct distances theorem, after Chapters 6 and 7. In this proof, we consider a set $\mathcal{P}$ of n points in $\mathbb{R}^2$, and show that it determines $\Omega(n/\sqrt{\log n})$ distinct distances. Given two points $a, b \in \mathcal{P}$, we define the line

$$\ell_{ab} = \left(\frac{a_x + b_x}{2}, \frac{a_y + b_y}{2}, 0\right) + t\left(\frac{b_y - a_y}{2}, \frac{a_x - b_x}{2}, 1\right), \qquad \text{for } t \in \mathbb{R}. \tag{1}$$

We consider the set of n^2 lines

$$\mathcal{L} = \{\ell_{ab} : a, b \in \mathcal{P}\}. \tag{2}$$

Let $N_{\geq k}$ denote the number of points in $\mathbb{R}^3$ that are incident to at least k lines of $\mathcal{L}$. By using the ESGK framework, we reduced the distinct distances problem to the problem of proving the bound

$$N_{\geq k} = O\left(\frac{n^3}{k^2}\right), \qquad \text{for every } 1 \leq k \leq n^2. \tag{3}$$

In Chapter 7, we proved (3) for every $k \geq 3$ (for $k > n$, we proved that $N_{\geq k} = 0$). In this chapter we complete the proof by showing that $N_{\geq 2} = O(n^3)$. Notice that this case is about bounding the number of points in $\mathbb{R}^3$ where lines of $\mathcal{L}$ intersect. As in the case of $k \geq 3$, the bound $N_{\geq 2} = O(n^3)$ does not hold for every set of lines in $\mathbb{R}^3$. For example, by placing n^2 lines in a common plane, we can easily obtain $\Theta(n^4)$ intersection points. In Chapter 6 we proved the following lemma.

Lemma 2.1. *Let $\mathcal{P}$ be a set of n points in $\mathbb{R}^2$, and let $\mathcal{L}$ be the set of n^2 lines that is defined in* (2)*. Then every plane in $\mathbb{R}^3$ contains at most n lines of $\mathcal{L}$.*

Lemma 2.1 implies that the problematic case of many lines in a common plane cannot occur. However, in the case of $k = 2$ other problematic constructions exist.

By saying that a set is a *surface*, we mean that it is a hypersurface in $\mathbb{R}^3$ (for the definition of a hypersurface, see Chapter 2). An irreducible surface U is said to be *ruled* if for every point $p \in U$ there exists a line that is contained in U and incident to p. Simple examples of ruled surfaces are a plane, a cylinder, and a conical surface. A surface U is said to be *doubly-ruled* if for every point $p \in U$ there exist two lines that are contained in U and incident to p. Similarly, a plane is said to be *infinitely-ruled*, and ruled surfaces that are not doubly-ruled are said to be *singly-ruled*.

A *regulus* is a surface that is the union of all lines that intersect three given pairwise-skew lines ℓ_1, ℓ_2, ℓ_3. We can use a polynomial argument to obtain a basic property of the reguli.

Claim 2.2. *Every regulus in $\mathbb{R}^3$ is an irreducible surface of degree 2.*

Proof. Consider a regulus R that is defined by the three pairwise-skew lines ℓ_1, ℓ_2, ℓ_3. We first claim that there exists a nontrivial polynomial of degree two that vanishes on all three lines. Arbitrarily choose three points out of each of the lines ℓ_1, ℓ_2, ℓ_3, obtaining a total of nine points. Since $\binom{2+3}{3} = 10 > 9$, by Lemma 2.1 of Chapter 6 there exists a nontrivial polynomial f of degree at most two that vanishes on all nine points. By Bézout's theorem, since ℓ_1 intersects $Z(f)$ in at least three points, we have $\ell_1 \subset Z(f)$. A symmetric argument applies to ℓ_2 and ℓ_3. Also, f cannot be of degree one, since this would imply that ℓ_1, ℓ_2, ℓ_3 are coplanar.

Consider a line ℓ' that intersects all three lines ℓ_1, ℓ_2, ℓ_3. The three intersection points are distinct since ℓ_1, ℓ_2, ℓ_3 are disjoint. As before, since ℓ' intersects $Z(f)$ in at least three points, by Bézout's theorem $\ell' \subset Z(f)$. This in turn implies that $R \subset Z(f)$. Since ℓ_1, ℓ_2, ℓ_3 are skew, R is not a plane, and we have $R = Z(f)$. This establishes that R is a surface of degree 2. To establish that R is irreducible, it suffices to show that R is not the union of two planes. This is also immediate from ℓ_1, ℓ_2, ℓ_3 being skew. □

Since there is a simple characterization of the possible types of quadratic surfaces in $\mathbb{R}^3$, one can go over these types and check which ones are reguli (e.g., see [4, Section 1.3]). By doing that, we find that there are only two types of reguli: *hyperboloids of one sheet* and *hyperbolic paraboloids* (see Figure 1). In general, three lines ℓ_1, ℓ_2, ℓ_3 define a hyperboloid of one sheet, unless they are all parallel to one plane (but not to each other) and then they define a hyperbolic paraboloid.

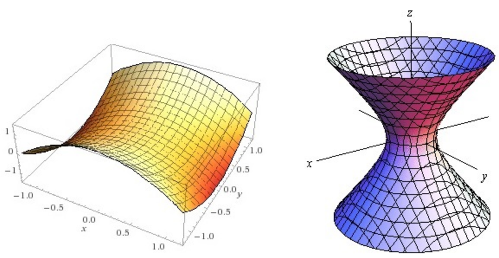

Figure 1: Left: The hyperbolic paraboloid $Z(y^2 - x^2 - z)$. Right: The hyperboloid of one sheet $Z(x^2 + y^2 - z^2 - 1)$.

Given a singly-ruled surface U, a line $\ell \subset U$ is said to be *exceptional* if every point of ℓ is intersected by another line that is fully contained in U. The following lemma lists several properties of ruled surfaces.

Lemma 2.3. *(a) All of the reguli are doubly-ruled.*
(b) Every irreducible singly-ruled surface has at most two exceptional lines.
(c) Except for planes and reguli, all of the ruled surfaces are singly-ruled.

(d) Let U be an irreducible singly-ruled surface of degree k. Then every non-exceptional line in U has $O(k_U)$ intersection points with the other lines in U.
(e) Every non-ruled surface of degree k contains $O(k^2)$ lines.

Proof sketch. The following is a very partial and non-rigorous proof sketch. A rigorous proof would require a whole chapter, which I consider adding at some point.[1] For more details, see for example [2, 3, 5].

A *ruling* of a ruled surface U is a family of lines $\mathcal{L}$ such that $\bigcup_{\ell \in \mathcal{L}} \ell = U$ and a generic point of U is incident to a single line of $\mathcal{L}$. It can be shown that every ruled surface has a ruling, and that every doubly-ruled surface has two disjoint rulings.

For (a), consider a regulus R that is defined by the three pairwise-skew lines ℓ_1, ℓ_2, and ℓ_3. One ruling of R is the set of lines that intersect all three lines ℓ_1, ℓ_2, and ℓ_3. Consider three lines ℓ'_1, ℓ'_2, and ℓ'_3 of this ruling. The set of lines that intersect ℓ'_1, ℓ'_2, and ℓ'_3 (which includes ℓ_1, ℓ_2, and ℓ_3) is the second ruling of R.

For (b), assume for contradiction that an irreducible singly-ruled surface U contains three exceptional lines ℓ_1, ℓ_2, and ℓ_3. Then U contains infinitely many lines that intersect ℓ_1, ℓ_2, and ℓ_3, which implies that U is either a plane or a regulus (depending on whether ℓ_1, ℓ_2, and ℓ_3 are coplanar or not). This contradicts U being singly-ruled.

For (c), consider a ruled surface U that is not singly-ruled. The proof is based on showing that there exist three lines ℓ_1, ℓ_2, and ℓ_3 that are contained in U such that there are infinitely many lines in U that intersect ℓ_1, ℓ_2, and ℓ_3. If ℓ_1, ℓ_2, and ℓ_3 are coplanar then U must be a plane, and otherwise it is a regulus. □

Reguli can be used to show that the case of $k = 2$ of (3) does not hold for general sets of n^2 lines in $\mathbb{R}^3$, even if we forbid many lines in a common plane. Indeed, let $R \subset \mathbb{R}^3$ be a regulus, let $\mathcal{L}_1$ be a set of $n^2/2$ lines of the first ruling of R, and let $\mathcal{L}_2$ be a set of $n^2/2$ lines of the second ruling of R, such that every line of $\mathcal{L}_1$ intersects every line of $\mathcal{L}_2$. Then $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2$ is a set of n^2 lines, and $\Theta(n^4)$ points of $\mathbb{R}^3$ are intersection points between lines of $\mathcal{L}$.

Guth and Katz [3] derived the following lemma, which we present here without proof.

Lemma 2.4. *Let $\mathcal{P}$ be a set of n points in $\mathbb{R}^2$, and let $\mathcal{L}$ be the set of n^2 lines in $\mathbb{R}^3$ that is defined in* (2)*. Then every regulus contains $O(n)$ lines of $\mathcal{L}$.*

3 Proving the case of $k = 2$

We are now ready to prove the case of $k = 2$ of (3).

Theorem 3.1. *Let $\mathcal{L}$ be a set of n^2 lines in $\mathbb{R}^3$, such that every plane and regulus contains at most βn lines of $\mathcal{L}$ (for a constant β). Then $O(n^3)$ points of $\mathbb{R}^3$ are intersection points between lines of $\mathcal{L}$.*

[1] Specifically, the "nice" way to prove the lemma involves moving to a complex projective space, which I wish to avoid at this point.

Proof. Let α be a sufficiently large constant. We prove by induction on n that given a set of n^2 lines in $\mathbb{R}^3$ with at most βn in any plane and regulus, the number of intersection points between the lines is at most αn^3. For the induction basis, when n is sufficiently small (say, when $n \le 100$) the claim holds for sufficiently large α.

We consider the induction step. Let $\mathcal{P}_0$ denote the set of points of $\mathbb{R}^3$ where lines of $\mathcal{L}$ intersect, and let a be a large constant that will be determined below. We repeatedly remove lines that have fewer than an points of intersection with other lines of $\mathcal{L}$, until no such lines remain. Notice that removing a line from $\mathcal{L}$ may result in additional lines having fewer than an such points. Let $\mathcal{P}$ be the set of points of $\mathbb{R}^3$ where lines of the updated $\mathcal{L}$ intersect. Notice that, $|\mathcal{P}_0| \le |\mathcal{P}| + an^3$.

Since every remaining line of $\mathcal{L}$ contains at least an intersection points with the other remaining lines of $\mathcal{L}$, we can apply Lemma 1.2 on $\mathcal{L}$ with $k = an$ (and n^2 lines). This implies that there exists a polynomial $f \in \mathbb{R}[x_1, x_2, x_3]$ of degree $O(n/\sqrt{a})$ that vanishes on all of the lines of $\mathcal{L}$.

Consider a line $\ell \in \mathcal{L}$ and let $\Omega_1, \ldots, \Omega_c$ denote the components of $Z(f)$ that do not contain ℓ. Since the degree of $\Omega_1 \cup \cdots \cup \Omega_c$ is $O(n/\sqrt{a})$, by Bézout's theorem ℓ intersects $\Omega_1 \cup \cdots \cup \Omega_c$ in $O(n/\sqrt{a})$ points. Thus, the number of points of $\mathcal{P}$ that are intersection points between two lines of $\mathcal{L}$ that are not contained in the same component of $Z(f)$ is $O(n^3/\sqrt{a})$.

It remains to bound the number of intersection points between lines of $\mathcal{L}$ that are in the same component of $Z(f)$. We first consider components of $Z(f)$ that are either planes or reguli. By the condition of the induction, a component Ω that is either a plane or a regulus contains at most βn lines of $\mathcal{L}$, so there are $O(\beta^2 n^2)$ intersection points between the lines that are contained in Ω. Since f is of degree $O(n/\sqrt{a})$, there are $O(n/\sqrt{a})$ planes and reguli in $Z(f)$, and these contain a total of $O(\beta^2 n^3/\sqrt{a})$ such intersection points.

By Lemma 2.3(c), every component of $Z(f)$ that is not a plane or a regulus is either singly-ruled or not ruled. Denote the singly-ruled components of $Z(f)$ as $\Omega_{s,1}, \ldots, \Omega_{s,c'}$. For $1 \le i \le c'$, let k_i denote the degree of $\Omega_{s,i}$. Notice that $\sum_{i=1}^{c'} k_i = O(n/\sqrt{a})$. By Lemma 2.3(b,d), at most two lines of $\mathcal{L}$ are exceptional lines of $\Omega_{s,i}$, and every other line of $\mathcal{L}$ that is contained in $\Omega_{s,i}$ intersects $O(k_i)$ other lines of $\Omega_{s,i}$. That is, the number of intersection points between lines of $\mathcal{L}$ that are in $\Omega_{s,i}$ is $O(n^2 k_i)$ (where n^2 is an upper bound on the number of lines that are contained in $\Omega_{s,i}$). Summing the number of such intersection points over all of the singly-ruled surfaces $\Omega_{s,1}, \ldots, \Omega_{s,c'}$ yields

$$\sum_{i=1}^{c'} O(n^2 k_i) = O\left(n^2 \sum_{i=1}^{c'} k_i\right) = O(n^3/\sqrt{a})$$

Denote the non-ruled components of $Z(f)$ as $\Omega_{\mathrm{NR},1}, \ldots, \Omega_{\mathrm{NR},c''}$, and let $\hat{k}_i$ denote the degree of $\Omega_{\mathrm{NR},i}$. Notice that $\sum_{i=1}^{c''} \hat{k}_i = O(n/\sqrt{a})$. By Lemma 2.3(e), the component $\Omega_{\mathrm{NR},i}$ contains $O(\hat{k}_i^2)$ lines of $\mathcal{L}$. By convexity, the number of lines that $\Omega_{\mathrm{NR},1} \cup \cdots \cup \Omega_{\mathrm{NR},c''}$ can contain is maximized when there is a single component of degree $O(n/\sqrt{a})$, and then this number is $O(n^2/a)$. By taking a to be sufficiently large, we may assume that the number of lines in the non-ruled components is at most $n^2/100$. We denote the set of these lines as $\mathcal{L}_{NR}$.

We do not care about the exact size of $|\mathcal{L}_{NR}|$, and assume that it is exactly $n^2/100$. A smaller size would only improve the bound on the number of intersections between these lines (a reader who is uncomfortable with this idea can instead add to $\mathcal{L}_{NR}$ generic lines that do not intersect any other lines). We would like to apply the induction hypothesis on $\mathcal{L}_{NR}$. This requires the assumption that no plane or regulus contains more than $\beta n/10$ lines of $\mathcal{L}_{NR}$, which might be false. Assume that there exists a plane or a regulus R that contains more than $\beta n/10$ lines of $\mathcal{L}_{NR}$. Let $\mathcal{L}_R$ denote the lines of $\mathcal{L}_{NR}$ that are contained in R, and remove $\mathcal{L}_R$ from $\mathcal{L}_{NR}$. Since R is either a plane or a regulus, we have $|\mathcal{L}_R| \le \beta n$. Thus, there are $O(\beta^2 n^2)$ line intersections between the lines of $\mathcal{L}_R$. Since every line of $\mathcal{L}_{NR} \setminus \mathcal{L}_R$ intersects R in at most two points, the number of intersections between lines of $\mathcal{L}_{NR} \setminus \mathcal{L}_R$ and lines of $\mathcal{L}_R$ is $O(\beta^2 n^2)$.

We repeat the pruning process in the previous paragraph until no plane or regulus contains more then $\beta n/10$ lines of $\mathcal{L}_{NR}$. Since we remove at least $\beta n/10$ lines at each step, there are $O(n)$ steps. The total number of intersections that involve lines that were removed at any step is $O(n^3)$.

Finally, by the induction hypothesis, the number of intersection points between the remaining lines of $\mathcal{L}_{NR}$ is at most $\alpha n^3/10^3 < \alpha n^3/2$. Excluding the intersection points between the remaining lines of $\mathcal{L}_{NR}$, the total number of intersection points in all of the previous cases is $O\left((a+\beta^2)n^3\right)$. By taking α to be sufficiently large with respect to a and β, we may assume that this number is at most $\alpha n^3/2$. This completes the induction step and the proof of the theorem. □

We are finally done proving the distinct distances theorem of Guth and Katz!

References

[1] N. Alon and J. H. Spencer, *The probabilistic method*, John Wiley & Sons, 2004.

[2] L. Guth, Lecture notes for the course "The Polynomial Method", `http://math.mit.edu/~lguth/PolynomialMethod.html`.

[3] L. Guth and N. H. Katz, On the Erdős distinct distances problem in the plane, *Annals of Mathematics*, **181** (2015), 155–190.

[4] D. Hilbert and S. Cohn-Vossen, *Geometry and the Imagination*, American Mathematical Soc., 1999.

[5] M. Sharir and N. Solomon, Incidences between points and lines on a two-dimensional variety, arXiv:1501.01670.

A Computing the probabilities

In this appendix we prove the probabilistic statement that was made in the proof of Lemma 1.2. We begin by recalling some basic probability. A random variable with a *binomial distribution* $B(n,p)$ represents the number coin flips that landed on heads when performing n independent coin flips, each with a probability of p for landing heads. For a proof of the following lemma, see for example [1, Theorem A.1.15].

Lemma A.1 (Chernoff bounds). *Let $X \sim B(n,p)$ (where $0 < p < 1$), and let $\delta > 0$. Then*

$$\Pr[X \geq (1+\delta)np] \leq \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}}\right)^{np}.$$

$$\Pr[X \leq (1-\delta)np] \leq e^{-pn\delta^2/2}.$$

We are now ready to prove the asserted probabilistic result.

Lemma A.2. *Let $\mathcal{L}$ be a set of n lines, each containing at least k intersection points with other lines of $\mathcal{L}$, where $2500\sqrt{n} < k < n$ and n is sufficiently large. Let $p = 100\sqrt{n}/k$ and let $\mathcal{L}'$ be a subset of $\mathcal{L}$ that is obtained by choosing every line of $\mathcal{L}$ with probability p. Then with positive probability: $|\mathcal{L}'| < 200n^{3/2}/k$ and every line of $\mathcal{L} \setminus \mathcal{L}'$ contains at least $\sqrt{n}$ distinct intersection points with lines of $\mathcal{L}'$.*

Proof. Notice that $|\mathcal{L}'| \sim B(n,p)$. By Lemma A.1 with $\delta = 1$,

$$\Pr[|\mathcal{L}'| \geq 200n^{3/2}/k] \leq \left(\frac{e}{4}\right)^{100n^{3/2}/k} < \left(\frac{3}{4}\right)^{100\sqrt{n}}.$$

Next, let ℓ be a line in $\mathcal{L} \setminus \mathcal{L}'$, and let X_ℓ denote the number of intersection points that ℓ has with lines of $\mathcal{L}'$. By considering exactly k intersection points of ℓ with other lines of $\mathcal{L}$ (even if more exist) we get $X_\ell \sim B(k,p)$. By Lemma A.1 with $\delta = 1/2$, we have

$$\Pr[X_\ell < \sqrt{n}] < \Pr[X_\ell \leq 50\sqrt{n}] = \Pr[X_\ell \leq kp/2] \leq e^{-100\sqrt{n}/8} < e^{-10\sqrt{n}}.$$

Recall the union bound principle, which states that the probability that at least one event out of some set of events happens is at most the sum of the probabilities of the individual events. In our case, the probability that $|\mathcal{L}'| \geq 200n^{3/2}/k$ or that at least one of the lines of $\mathcal{L} \setminus \mathcal{L}'$ has fewer than $\sqrt{n}$ intersection points with the lines of $\mathcal{L}'$ is smaller than

$$\left(\frac{3}{4}\right)^{100\sqrt{n}} + ne^{-10\sqrt{n}}.$$

When n is sufficiently large, this probability is smaller than 0.01 (or than any other constant that we choose). Thus, with (large) positive probability, $|\mathcal{L}'| < 200n^{3/2}/k$ and every line of $\mathcal{L} \setminus \mathcal{L}'$ has at least $\sqrt{n}$ intersection points with the lines of $\mathcal{L}'$. □