DISTINCT DISTANCES FROM POINTS ON A CIRCLE TO A GENERIC SET

Alex McDonald
Department of Mathematics, University of Rochester, Rochester, New York
amcdona5@ur.rochester.edu

Brian McDonald
Department of Mathematics, University of Rochester, Rochester, New York
bmcdon11@ur.rochester.edu

Jonathan Passant
Department of Mathematics, University of Rochester, Rochester, New York
jpassant@ur.rochester.edu

Anurag Sahay
Department of Mathematics, University of Rochester, Rochester, New York
asahay@ur.rochester.edu

Received: 5/5/20, Revised: 12/28/20, Accepted: 5/10/21, Published: 5/17/21

Abstract

Let S be a set of points in $\mathbb{R}^2$ contained in a circle and P an unrestricted point set in $\mathbb{R}^2$. We prove that the number of distinct distances between points in S and points in P is at least the minimum of $|S||P|^{1/4-\varepsilon}, |S|^{2/3}|P|^{2/3}, |S|^2$, and $|P|^2$. This builds on work of Pach and De Zeeuw, Bruner and Sharir, McLaughlin and Omar, and Mathialagan on distances between pairs of sets.

1. Introduction

In 1945 Erdős introduced his distinct distances problem, first stated in [5], asking for the minimum number of distinct distances an n point set can create in $\mathbb{R}^2$. Erdős showed that a square lattice Λ of n points determined $|\Delta(\Lambda)| \lesssim \frac{n}{\sqrt{\log n}}$ distances, where here and throughout, $\gtrsim$ and $\lesssim$ are used to suppress some constant independent of the controlling parameter and $\Delta(S)$ denotes the set of distances between elements of S. Similarly, $\Delta(S,T)$ will denote the set of distances between elements of S and elements of T. Erdős conjectured that this was essentially the best possible, i.e., for any set P of n points and any $\varepsilon > 0$ one has $|\Delta(P)| \gtrsim n^{1-\varepsilon}$. This question played a key role in combinatorial geometry for over 50 years, with many successive

improvements; see [1, Section 5.3] or [6]. In [7], Guth and Katz provided a solution utilizing significant new algebraic developments in what has become known as the polynomial method in combinatorics.

A natural variant of the distinct distances problem asks for the minimum number of distances between points $a \in A, b \in B$, where one or both of the finite sets A and B are constrained in some way. One version of this problem, attributed to Purdy (see [1, Section 5.5]), considers lines ℓ_1 and ℓ_2 in the plane, and sets A and B of n points on ℓ_1 and ℓ_2 respectively. Purdy observed that if ℓ_1 and ℓ_2 are parallel or perpendicular, then one may imitate the grid example given by Erdős to obtain at most n distances. Purdy conjectured that otherwise the number of distnaces was superlinear. More precisely, he conjectured that for every C there exists n_0 such that if $A \subset \ell_1, B \subset \ell_2$, each with size $n > n_0$, and determine at most Cn distances, then ℓ_1 and ℓ_2 are either parallel or perpendicular. Elekes and Rónyai [4] prove this conjecture from a statement about restricted polynomials, implicitly showing that there exists $\delta > 0$ such that $\Delta(A, B) \gtrsim n^{1+\delta}$ under the conditions of the conjecture. Elekes [3] subsequently showed that one can in fact take $\delta = \frac{1}{4}$. Schwartz, Solymosi, and de Zeeuw [13] prove that in the unbalanced version of the problem, where $|A| = n^{\frac{1}{2}+\varepsilon}$ and $|B| = n$, the number of distances is still superlinear. The results in both the balanced and unbalanced cases were improved by Sharir, Sheffer and Solymosi [14], who use algebraic techniques to show that sets A and B of size n and m, respectively, satisfying the hypotheses above, determine at least $\min\{n^{2/3}m^{2/3}, n^2, m^2\}$ distances.

This question has been generalized in two key ways. Pach and de Zeeuw [11], showed that if the point sets are each restricted to algebraic curves C_1 and C_2 of constant degree (constant with respect to n and m, the number of points on C_1 and C_2 respectively), then one has at least $\min\{n^{2/3}m^{2/3}, n^2, m^2\}$ distinct distances, provided the curves are not parallel lines, orthogonal lines, or concentric circles. It was essential to this argument that both point sets are on curves, so their roles could be interchanged. Further, the curves considered by Pach and de Zeeuw are not parallel lines, orthogonal lines, or concentric circles, as such curves share too many symmetries.

In a different direction, Bruner and Sharir [2] showed that when the first set P of m points is on a line and the second set P' of n points is unrestricted in the plane, one has

$$|\Delta(P, P')| \gtrsim \min\left\{n^{2/3}m^{2/3}, \frac{m^{10/11}n^{4/11}}{\log^{2/11} n}, n^2, m^2\right\}.$$

This result relied on the explicit parameterization of the line to build an incidence problem. Similarly, McLaughlin and Omar [10] showed that if a set P of m points is restricted to a curve of constant degree and a set P' of n points is unrestricted,

one has

$$|\Delta(P,P')| \gtrsim \begin{cases} m^{1/2}n^{1/2}\log^{-1/2} n & \text{when } m \gtrsim n^{1/2}\log^{-1/3} n, \\ m^{1/3}n^{1/2} & \text{when } m \lesssim n^{1/2}\log^{-1/3} n. \end{cases}$$

Finally, Mathialagan [9] extended these results in $\mathbb{R}^2$ to the setting where P and P' are both unrestricted point sets (of size m and n respectively)

$$|\Delta(P,P')| \gtrsim \begin{cases} m^{1/2}n^{1/2}\log^{-1} n & \text{when } n^{1/3} \leq m \leq n, \\ m^{1/2}n^{1/2} & \text{when } m \leq n^{1/3}. \end{cases}$$

Since P and P' are symmetric in this case, analogous bounds hold when $m \geq n$. In particular, this subsumes McLaughlin-Omar's result. In the balanced case ($n^{1/3} \leq m \leq n$), Mathialagan's result is obtained by adapting the Guth-Katz argument [7] to the question of distances determined by two sets (rather than one). In the unbalanced case ($2 \leq m \leq n^{1/3}$), Mathialagan shows that in fact there are at least $(nm)^{1/2}$ pinned distances determined by the bigger set and a single point in the smaller set.

It is interesting to compare this result to those which assume algebraic structure on one or both of the sets. In our result, as well as the results of Bruner-Sharir and Pach-de Zeeuw, the bounds obtained are better than Mathialagan's in the near-balanced case (how close to balanced the sets must be depends on the particular result), but in extremely lopsided cases, the $(mn)^{1/2}$ bound eventually wins.

The aim of this paper is to find similar results in the case where one set lies on a circle and the second set is essentially unrestricted. We obtain the following result.

Theorem 1. *Suppose that S is a point set on a circle in $\mathbb{R}^2$ and P is a point set in $\mathbb{R}^2$ such that no two points of P are on any circle concentric to the original circle. Then we have*

$$|\Delta(S,P)| \gtrsim \min(|S||P|^{1/4-\varepsilon}, |S|^{2/3}|P|^{2/3}, |S|^2, |P|^2).$$

For comparison with the theorems stated above, if $|S| = m$ and $|P| = n$ then we have

$$|\Delta(S,P)| \gtrsim \begin{cases} m^2, & m \lesssim n^{1/4-\varepsilon}, \\ mn^{1/4-\varepsilon}, & n^{1/4-\varepsilon} \lesssim m \lesssim n^{5/4-\varepsilon}, \\ m^{2/3}n^{2/3}, & n^{5/4-\varepsilon} \lesssim m \lesssim n^2, \\ n^2, & n^2 \lesssim m. \end{cases}$$

Note that the theorem would be false without the hypothesis that no two points in P lie on a circle concentric with S (though two could be replaced by another fixed constant). To see this, let S be a set of n points on the unit circle, evenly spaced. Let $P = \alpha S$ for some positive real number α. For any fixed $p \in P$, we have

$$|\Delta(\{p\}, S)| \leq |S| = n.$$

But by symmetry, $\Delta(\{p\}, S) = \Delta(\{p'\}, S)$ for any $p, p' \in P$. Thus, $|\Delta(P, S)| = |\Delta(\{p\}, S)| \leq n$, which would contradict the conclusion of the theorem.

When the points are not evenly spaced as in the example above, we obtain the following result.

Theorem 2. *Let S and P be finite sets on concentric planar circles with center O, and suppose α is such that for any $\theta \in [-\pi, \pi]$ we have*

$$|\{(p, q) \in P^2 : \angle pOq = \theta\}| \lesssim |P|^{2\alpha},$$

where $\angle pOq$ is the oriented angle between line segments $\overline{Op}$ and $\overline{Oq}$. Then

$$|\Delta(S, P)| \gtrsim |S|^{1/2}|P|^{1-\alpha}.$$

In particular, if no two points of P subtend the same angle, then we get $|S|^{1/2}|P|$ distances. One can check that this is better than the bound in Theorem 1 regardless of the relative size of the sets.

We note that Theorems 1 and 2 are probably far from sharp. The only cases we can find where two point sets S and P determine $o(|S||P|)$ distances are when S and P lie on concentric circles. We would be extremely interested in any examples of a point set S contained in a circle and P not on a concentric circle which determine $o(|S||P|)$ distances.

It is interesting to compare our result to the other theorems above, since each result answers the same question under different assumptions. Of particular interest is Mathialagan's result above, which makes no assumptions on the (finite) point sets in question. Our bound is better in the range $|P|^{1/2} \lesssim |S| \lesssim |P|^3$. Outside this range the bound $\Delta(P, S) \gtrsim (|P||S|)^{1/2}$ wins, showing our structural assumptions on our sets are only helping when the sizes of the sets are (at least somewhat) balanced.

It is also worth comparing our result to that of Pach and de Zeeuw, who obtain a lower bound for the number of distinct distances determined by point sets each contained on a real algebraic curve of bounded degree. We assume one of our sets lies on a circle (a much stronger assumption then a general curve) but the other is essentially arbitrary. Their bound is never weaker than ours, and is strictly stronger in the balanced case.

This paper will be structured as follows. In Section 2 we provide the initial framework for the bound on $|\Delta(S, P)|$, following the idea of Elekes that one can use pairs of repeated distances. We also introduce the incidence bound of Sharir and Zahl [15], which we will use to prove the main result. In Sections 3 and 4 we show that the hypotheses of the Sharir-Zahl incidence bound are satisfied in our setting.

2. Creating an Incidence Problem

Definition 1. Given any two finite sets $S, P \subset \mathbb{R}^2$, define the *distance set* and *quadruple set* of S and P, respectively, as

$$\Delta(S,P) = \{|u-p| : u \in S, p \in P\},$$

$$Q(S,P) = \{(u,v,p,q) \in S^2 \times P^2 : |u-p| = |v-q|\}.$$

Theorem 3. *For any sets of points $S, P \subset \mathbb{R}^2$, we have*

$$|\Delta(S,P)| \geq \frac{|S|^2|P|^2}{|Q(S,P)|}.$$

Proof. The statement follows directly from the classic Cauchy-Schwarz energy bound. Let $v(t) = \{(u,p) \in S \times P : |u-p| = t\}$ be the number of occurrences of the distance t. Then we have

$$|S|^2|P|^2 = \left(\sum_{t \in \Delta(S,P)} v(t)\right)^2 \leq |\Delta(S,P)| \sum_t v^2(t) = |\Delta(S,P)| \cdot |Q(S,P)|.$$

□

Therefore, an upper bound on the size of $Q(S,P)$ will yield a lower bound on the size of $\Delta(S,P)$. In order to bound $Q(S,P)$, we will follow the approach of Pach and de Zeeuw [11] and Bruner and Sharir [2] by setting up an incidence problem.

We start by making a few simple reductions. These are not additional hypotheses, but rather can be assumed without loss of generality.

- Without loss of generality, we may assume that S is contained in the unit circle centered at the origin, so all $u \in S$ satisfy $\|u\| = 1$.
- For technical reasons, we want P to have the property that distinct $p, q \in P$ always satisfy $\|p\| - \|q\| \neq 2$. This can be achieved by considering half open annuli of width 2, and assigning the annuli alternating colors. Since one of the colors must contain at least half of P, we may assume P has the desired property at the cost of a constant.
- We will assume $(-1,0) \notin S$ and $(0,0) \notin P$.

For any point $p \in P$ and distance t there are at most two choices of $u \in S$ for which $\|p-u\| = t$, since the circle centered at p of radius t can only intersect the unit circle twice. Therefore, the number of quadruples $(u,v,p,q) \in Q(S,P)$ with $p = q$ is on the order of $|S||P|$. It remains to bound our modified quadruple set

$$\widetilde{Q}(S,P) = \{(u,v,p,q) \in S^2 \times P^2 : p \neq q, \|p-u\| = \|q-v\|\}.$$

Let

$$f_{p,q}(u_1,u_2,v_1,v_2) = (p_1-u_1)^2+(p_2-u_2)^2-(q_1-v_1)^2-(q_2-v_2)^2.$$

It follows that for $u,v \in S$ and $p,q \in P$, we have $\|u-p\| = \|v-q\|$ if and only if $f_{p,q}(u,v) = 0$. This gives us an incidence problem between a set of points and hypersurfaces in $\mathbb{R}^4$, but we want to apply a point-curve incidence bound in $\mathbb{R}^2$. To do this we use the fact that S is contained in the unit circle, which admits a rational parametrization. If we define

$$\varphi(x) = \left(\frac{1-x^2}{1+x^2}, \frac{2x}{1+x^2}\right),$$

then φ is a homeomorphism from $\mathbb{R}$ to the unit circle with the point $(-1,0)$ removed. Recall $f_{p,q}$ is a quadratic in four variables; this means

$$F_{p,q}(x,y) := (1+x^2)^2(1+y^2)^2 f_{p,q}(\varphi(x),\varphi(y))$$

is a two variable polynomial of degree at most 12. Moreover, $F_{p,q}(x,y) = 0$ if and only if $f_{p,q}(\varphi(x),\varphi(y)) = 0$, which in turn happens if and only if (x,y) parametrizes a point $(u,v) \in S^1 \times S^1$ with $\|u-p\| = \|v-q\|$. If $\Pi = \{(x,y) : \varphi(x),\varphi(y) \in S\}$ and $\Gamma = \{Z(F_{p,q}) : p,q \in P, p \neq q\}$, then our observations can be summarized in the following lemma.

Lemma 1. *If S,P,Π,Γ are as above, then $|\Pi| = |S|^2, |\Gamma| \approx |P|^2$, and*

$$Q(S,P) \approx |S||P| + I(\Pi,\Gamma).$$

So, matters have been reduced to obtaining an incidence bound that applies to our sets Π and Γ.

The incidence bound we will use is due to Sharir and Zahl [15]. To use the result of Sharir and Zahl we will introduce their terminology. We identify polynomials of degree at most D with elements of $\mathbb{R}^{\binom{D+2}{2}}$, since each polynomial can be viewed as the vector of its coefficients. Since $Z(f) = Z(\lambda f)$ for nonzero scalars λ, we can identify algebraic plane curves of degree at most D as elements of $\mathbf{P}\mathbb{R}^{\binom{D+2}{2}}$. With this framework, Sharir and Zahl make the following definition.

Definition 2. An *s-dimenional family* of plane curves of degree at most D is an algebraic variety $\mathcal{F} \subset \mathbf{P}\mathbb{R}^{\binom{D+2}{2}}$ that has dimension s. We call the degree of $\mathcal{F}$ the *complexity* of the family.

Theorem 4 ([15], Theorem 1.3)**.** *Let $\mathcal{C}$ be a set of algebraic plane curves belonging to an s-dimensional family of curves of bounded degree, no two of which share a common irreducible component. Let $\mathcal{P}$ be a finite set of points in $\mathbb{R}^2$. For any $\varepsilon > 0$, we have*

$$I(\mathcal{P},\mathcal{C}) \lesssim |\mathcal{P}|^{\frac{2s}{5s-4}}|\mathcal{C}|^{\frac{5s-6}{5s-4}+\varepsilon} + |\mathcal{P}|^{\frac{2}{3}}|\mathcal{C}|^{\frac{2}{3}} + |\mathcal{P}| + |\mathcal{C}|,$$

where the constant depends on s, ε, the bound on the degree of the family of curves, and the complexity of that family.

In Section 4, we will prove that Γ lives in a 4-dimensional family of algebraic plane curves, and that no two curves of Γ have a common component. In order to prove this, we will first work with related curves in $\mathbb{R}^4$ before applying the rational parametrization to obtain curves in the plane. Recall that the polynomial $f_{p,q}$ defines an algebraic hypersurface in $\mathbb{R}^4$. We define $C_{p,q} = Z(f_{p,q}) \cap (S^1 \times S^1)$. Since $S^1 \times S^1$ is a real algebraic variety of dimension 2 and $f_{p,q}$ cannot vanish on all of $S^1 \times S^1$ (unless $p = q = 0$), it follows that $C_{p,q}$ is a real algebraic curve in $\mathbb{R}^4$. We will study these curves in Section 3.

3. Behavior of the Curves $C_{p,q}$ in $\mathbb{R}^4$

In this section, we will prove some results about our curves $C_{p,q} \subset \mathbb{R}^4$. These properties will be used in section 4 to prove that no two curves in Γ share a common component.

Lemma 2. *For any $p \neq q$, the curve $C_{p,q}$ does not contain any isolated points (in the Euclidean topology).*

Proof. Consider some $(u, v) \in C_{p,q}$. Since $u, v \in S^1$, $||p|| - 1 \leq ||u - p|| \leq ||p|| + 1$ and similarly $||q|| - 1 \leq ||v - q|| \leq ||q|| + 1$. Moreover, these inequalities are all strict since otherwise one of $\|p\| = \|q\|$ or $\|p\| = \|q\| + 2$ must hold. It follows that for some $\varepsilon > 0$ and for any $t \in (-\varepsilon, \varepsilon)$, there must be points $u_t, v_t \in S^1$ with $||u_t - p|| = ||u - p|| + t$ and $||v_t - q|| = ||v - q|| + t$. Hence $(u_t, v_t) \in C_{p,q}$. We may also require that u, u_t are on the same side of the circle in the sense that S^1 is divided into two semi-circles by the line through p and the origin. Making a similar restriction for v_t ensures that $t \mapsto (u_t, v_t)$ is continuous, hence $(u, v) \in C_{p,q}$ is not an isolated point. □

Lemma 3. *For any $p, q \in \mathbb{R}^2$ with $\|p\| \neq \|q\|$ and any 2-flat K, we have $|C_{p,q} \cap K| \leq 4$.*

Proof. Let $(u_1, v_1), (u_2, v_2), (u_3, v_3) \in C_{p,q} \cap K$. It follows that $K - (u_3, v_3)$ is the plane spanned by $\{(u_1, v_1) - (u_3, v_3), (u_2, v_2) - (u_3, v_3)\}$. If $(u, v) \in C_{p,q} \cap K$, then $(u, v) - (u_3, v_3)$ is in that plane as well, and therefore

$$(u, v) - (u_3, v_3) = x((u_1, v_2) - (u_3, v_3)) + y((u_2, v_2) - (u_3, v_3))$$

for some unique values of x and y. Equivalently, we have

$$\begin{aligned} u &= x(u_1 - u_3) + y(u_2 - u_3) + u_3, \\ v &= x(v_1 - v_3) + y(v_2 - v_3) + v_3. \end{aligned}$$

Since $\|u\| = \|v\| = 1$, this means x and y satisfy

$$\|x(u_1 - u_3) + y(u_2 - u_3) + u_3\| = 1,$$
$$\|x(v_1 - v_3) + y(v_2 - v_3) + v_3\| = 1.$$

This system has solutions $(x, y) = (1, 0), (0, 1), (0, 0)$ corresponding to the points $(u_1, v_1), (u_2, v_2), (u_3, v_3)$, respectively. To prove the lemma, it therefore suffices to show that this system has at most 4 solutions. We can assume that both equations are irreducible quadratics, dealing with the case that these are lines or the product of lines later. If both equations are irreducible, then by Bézout's theorem it suffices to prove that one is not a constant multiple of the other. Expanding each equation and focusing on the quadratic terms while ignoring the lower order terms, we have

$$\|u_1 - u_3\|^2 x^2 + \|u_2 - u_3\|^2 y^2 + 2\langle u_1 - u_3, u_2 - u_3\rangle xy + \cdots = 0,$$
$$\|v_1 - v_3\|^2 x^2 + \|v_2 - v_3\|^2 y^2 + 2\langle v_1 - v_3, v_2 - v_3\rangle xy + \cdots = 0.$$

Suppose for contradiction that one equation is a constant multiple of the other. This means we can normalize both equations so that the coefficient of x^2 is 1, and all other coefficients must be the same. In particular, this means we have $\frac{\|u_2-u_3\|}{\|u_1-u_3\|} = \frac{\|v_2-v_3\|}{\|v_1-v_3\|}$; denote this common value by t. Let $A = \|u_1 - u_3\|, B = \|v_1 - v_3\|$, define θ_u to be the angle between $u_1 - u_3$ and $u_2 - u_3$, and define θ_v similarly. Then our equations are

$$A^2x^2 + t^2A^2y^2 + (2tA^2\cos\theta_u)xy + \cdots = 0,$$
$$B^2x^2 + t^2B^2y^2 + (2tB^2\cos\theta_v)xy + \cdots = 0,$$

or, normalizing so that the x^2 coefficient is 1,

$$x^2 + t^2y^2 + (2t\cos\theta_u)xy + \cdots = 0,$$
$$x^2 + t^2y^2 + (2t\cos\theta_v)xy + \cdots = 0.$$

Comparing the xy coefficients, we conclude that $\theta_u = \pm\theta_v$. This means that the two triangles $\Delta u_1u_2u_3$ and $\Delta v_1v_2v_3$ are similar. They have common angle θ at the third vertex and, for some value of ℓ, side lengths of the form $\ell, t\ell$ from the third vertex to the first and second vertices, respectively ($\ell = A$ in the first triangle, and $\ell = B$ in the second).

We claim there is only one value of ℓ for which such a triangle has all its vertices on the unit circle. This in turn implies $\|p\| = \|q\|$, as the triangles Δu_1u_3p and Δv_1v_3q would be congruent, which is our contradiction. So, this suffices to prove the claim. Let O denote the origin, and let $\Delta\alpha\beta\gamma$ be any triangle with angle θ at α and side lengths $\alpha\beta = t\ell, \alpha\gamma = \ell$ (see figure 1).

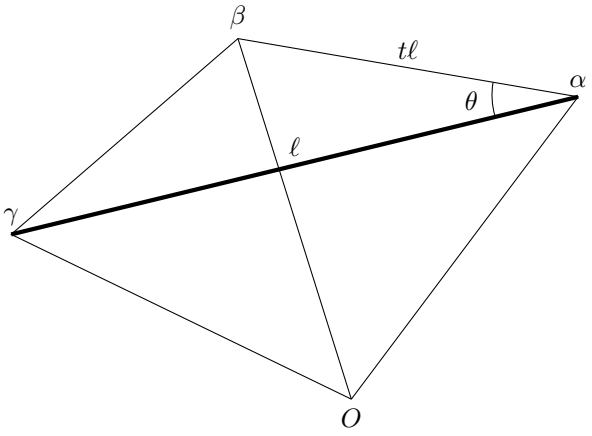

Figure 1: Triangle $\alpha\beta\gamma$.

If α, β, γ are on the unit circle then the triangle $\Delta O\alpha\gamma$ is an isosceles triangle with common side length 1 and base length ℓ, hence it has common base angle $\angle O\alpha\gamma = \arccos \ell/2$. This implies $\angle O\alpha\beta = \theta + \arccos \ell/2$. Similarly, $\Delta O\alpha\beta$ is an isosceles triangle with common side length 1 and base length $t\ell$, so the common base angle is $\angle O\alpha\beta = \arccos t\ell/2$. This means ℓ must satisfy

$$\begin{aligned}
\theta + \arccos \frac{\ell}{2} &= \arccos \frac{t\ell}{2} \\
\frac{\ell}{2}\cos\theta - \left(1 + \frac{\ell^2}{4}\right)^{1/2} \sin\theta &= \frac{t\ell}{2} \\
\left(\frac{\cos\theta - t}{2}\right)^2 \ell^2 &= \sin^2\theta \left(1 + \frac{\ell^2}{4}\right) \\
\left(\left(\frac{\cos\theta - t}{2}\right)^2 - \frac{\sin^2\theta}{4}\right) \ell^2 &= \sin^2\theta.
\end{aligned}$$

Note that the right-hand side cannot be zero, since that would imply three points on a circle were also on a line. So, there is at most one positive solution for ℓ.

We now show that the equations are irreducible quadratics. Recall the first few terms are

$$x^2 + t^2y^2 + (2t\cos\theta)xy + \cdots = 0.$$

If this is reducible, we can write it as a product $(x + ay)(x + by + c)$. Expanding, we must have

$$ab = t^2 \quad \text{and} \quad a + b = 2t\cos(\theta).$$

Plugging the first of these into the second gives the quadratic

$$\frac{1}{a}t^2 - 2\cos(\theta)t + a = 0,$$

which has a real solution only when $\cos(\theta) = \pm 1$. As noted above, this would mean that we have three points of a circle on a line, a contradiction. So we are not in the case where our quadratics are reducible and thus the above argument suffices. □

Lemma 4. *If $(p, q), (p', q') \in \mathbb{R}^4$ are distinct and $\|p\| \neq \|q\|$, then $|C_{p,q} \cap C_{p',q'}| \leq 4$.*

Proof. The curves $C_{p,q}$ are defined by the equations

$$u_1^2 + u_2^2 = 1 \tag{1}$$
$$v_1^2 + v_2^2 = 1 \tag{2}$$
$$(u_1 - p_1)^2 + (u_2 - p_2)^2 = (v_1 - q_1)^2 + (v_2 - q_2)^2. \tag{3}$$

Expanding equation (3) and substituting equations (1) and (2), we see that (3) can be replaced by

$$N_{p,q} \cdot (u, v) = \frac{\|p\|^2 - \|q\|^2}{2}, \tag{3'}$$

where $N_{p,q} = (p_1, p_2, -q_1, -q_2)$. It follows that for any scalar $t \neq 0, 1$, $(u, v) \in C_{tp,tq}$ must satisfy

$$N_{tp,tq} \cdot (u, v) = t^2 \frac{\|p\|^2 - \|q\|^2}{2},$$

or

$$N_{p,q} \cdot (u, v) = t \frac{\|p\|^2 - \|q\|^2}{2}.$$

This means that if (p, q) and (p', q') are distinct scalar multiples of each other, $C_{p,q}$ and $C_{p',q'}$ are contained in disjoint hyperplanes and thus have empty intersection. It remains to consider the case where $(p, q), (p', q')$ are distinct but not scalar multiplies of each other. In this case, $N_{p,q}$ and $N_{p',q'}$ are not scalar multiples of each other either, and hence $C_{p,q} \cap C_{p',q'}$ is contained in the intersection of two hyperplanes, which is a 2-flat. By Lemma 3, any such 2-flat can contain at most 4 points from $C_{p,q}$. □

4. Proofs of Theorems 1 and 2

4.1. Proof of Theorem 1

We are now ready to prove that our curves satisfy the hypotheses of the Sharir-Zahl incidence bound (Theorem 4). We must show that no two curves in Γ share a common irreducible component, and that Γ belongs to a 4-dimensional family.

To prove that no two curves of Γ share a common component, we use our work in Section 3. By Lemma 4 and the injectivity of φ, the intersection of any two curves of Γ is finite. Therefore, any common component must be zero dimensional, and hence an isolated point (x_0, y_0). Since $\varphi \times \varphi$ maps $Z(F_{p,q}) \to C_{p,q}$, we may consider

the point $(u_0, v_0) := (\varphi(x_0), \varphi(y_0)) \in C_{p,q}$. By Lemma 2, (u_0, v_0) is not isolated. This contradicts the continuity of φ^{-1}.

To prove Γ is contained in a 4-dimensional family, we will temporarily work over the field of complex numbers. Thus, we let p_1, p_2, q_1, and q_2 vary over $\mathbb{C}$ instead of $\mathbb{R}$. We observe that the coefficients of (complexified) curves in Γ are polynomials in our parameters p_1, p_2, q_1, q_2, and these polynomials do not simultaneously vanish unless $p = q = 0$. This map $\mathbb{C}^4 \setminus \{0\} \to \mathbb{C}^{\binom{D+2}{2}}$ is thus clearly a morphism of quasi-projective varieties. The natural surjection $\mathbb{C}^{\binom{D+2}{2}} \setminus \{0\} \twoheadrightarrow \mathbf{P}\mathbb{C}^{\binom{D+2}{2}}$ is also a morphism of quasi-projective varieties, and hence so is the composed map $\mathbb{C}^4 \setminus \{0\} \to \mathbf{P}\mathbb{C}^{\binom{D+2}{2}}$.

Thus, Γ is contained in the image of a morphism of quasi-projective varieties $\mathbb{C}^4 \setminus \{0\} \to \mathbf{P}\mathbb{C}^{\binom{D+2}{2}}$. After taking the Zariski closure of the image, if necessary, we see that Γ is contained in a variety in $\mathbf{P}\mathbb{C}^{\binom{D+2}{2}}$ of dimension at most 4, by invoking, for example [8, Theorem 11.12]. Thus, now restricting ourselves to $\mathbb{R}$ and using real dimension, Γ is contained in an family of dimension at most 4 (since the Sharir-Zahl incidence bound gets worse as s increases, this is enough).

Now that we have established that Theorem 4 applies to our curves, we are ready to complete the proof of Theorm 1. Applying Theorem 4 with $s = 4$, we get

$$I(\Pi, \Gamma) \lesssim |\Pi|^{1/2}|\Gamma|^{7/8+\varepsilon} + |\Pi|^{2/3}|\Gamma|^{2/3} + |\Pi| + |\Gamma|.$$

By Lemma 1, we have

$$Q(S, P) \lesssim |S||P|^{7/4+\varepsilon} + |S|^{4/3}|P|^{4/3} + |S|^2 + |P|^2.$$

By Theorem 3, this gives

$$\Delta(S, P) \gtrsim \min(|S||P|^{1/4-\varepsilon}, |S|^{2/3}|P|^{2/3}, |S|^2, |P|^2),$$

as claimed.

4.2. Proof of Theorem 2

We use the following well known theorem from additive combinatorics ([12], see also Lemma 2.6 in [16]).

Theorem 5 ([12], Ruzsa's Triangle Inequality)**.** *Let A, B, C be finite subsets of an abelian group. Then*

$$|A||B - C| \leq |A - B||A - C|.$$

To prove Theorem 2, we reduce matters to counting difference sets of angles. We first observe there is a line ℓ passing through O with the property that one side of ℓ contains a positive proportion of both S and P. To prove this, first note that we may assume that P is on either the upper or lower semicircle by throwing away up

to half of P. We can then choose a point on the semicircle such that the remaining points in P are evenly divided to the left and right. Let ℓ be the line through that point and O. By construction, both sides of ℓ contain at least $\frac{1}{4}|P|$ points of P. Since one side must contain $\frac{1}{2}|S|$ points of S, ℓ has the desired property.

For the remainder of the proof, we will assume both sets are contained entirely on one side of ℓ. For all p in either set, let θ_p be the angle from ℓ to the line segment $\overline{Op}$, so $\theta_p \in [0, \pi]$ for all $p \in S, P$. We also observe that $\angle pOq = \theta_p - \theta_q \in [-\pi, \pi]$. Let $A = \{\theta_p : p \in S\}$ and $B = \{\theta_p : p \in P\}$. If the circles containing the sets have radii r_1, r_2, then for any $u \in S, p \in P$ we have

$$\|p - u\| = \langle p - u, p - u\rangle = r_1^2 + r_2^2 - 2r_1 r_2 \cos(\theta_p - \theta_u),$$

hence $|\Delta(S, P)| \gtrsim |A - B|$ as cosine is 2-to-1 on $[-\pi, \pi]$. By assumption, the map $P^2 \to [-\pi, \pi]$ given by $(p, q) \mapsto \theta_p - \theta_q$ is, at worst, $|P|^{2\alpha}$-to-1, so $|B - B| \gtrsim |B|^{2-2\alpha}$. Applying Ruzsa's triangle inequality with $C = B$, we get

$$|A||B - B| \leq |A - B|^2,$$

or

$$|A|^{1/2}|B|^{1-\alpha} \leq |A - B|,$$

as claimed.

Acknowledgements. The authors wish to thank Adam Sheffer for introducing us to the problem, for pointing out the references [9] and [15], and encouragement. The third author wishes to thank Adam Sheffer, Josh Zahl and the participants of the MSRI summer school on the Polynomial Method for many helpful discussions and MSRI, Berkeley for hosting the workshop.

References

[1] P. Brass, W. Moser, and J. Pach, *Research Problems in Discrete Geometry*, Springer, New York, 2005.

[2] A. Bruner and M. Sharir, Distinct distances between a collinear set and an arbitrary set of points, *Discrete Math.* 341 (2018), no. 1, 261-265.

[3] G. Elekes, A note on the number of distinct distances, *Period. Math. Hungar.* 38 (1999), no. 3, 173-177.

[4] G. Elekes and L. Ronyai, A combinatorial problem on polynomials and rational functions, *J. Combin. Theory Ser.* A 89 (2000), no. 1, 1-20.

[5] P. Erdős, On sets of distances of n points, *Amer. Math. Monthly* 53 (1946), 248-250.

[6] J. Garibaldi, A. Iosevich, and S. Senger, *The Erdős Distance Problem*, American Mathematical Society, Providence, RI, 2011.

[7] L. Guth and N.H. Katz, On the Erdős distinct distances problem in the plane, *Ann. of Math.* (2) 181 (2015), no. 1, 155-190.

[8] J. Harris, *Algebraic Geometry: A First Course*, Graduate Texts in Mathematics, 133. Springer-Verlag, New York, 1995

[9] S. Mathialagan, On bipartite distinct distances in the plane. Preprint at https://arxiv.org/abs/1912.01883.

[10] B. McLaughlin and M. Omar, On distinct distances between a variety and a point set. Preprint at https://arxiv.org/abs/1812.03371

[11] J. Pach and F. de Zeeuw, Distinct distances on algebraic curves in the plane, *Combin. Probab. Comput.* 26 (2017), no. 1, 99-117.

[12] I. Ruzsa, Sums of finite sets, Number theory (New York, 1991-1995), 281-293, Springer, New York, 1996.

[13] R. Schwartz, J. Solymosi, and F. de Zeeuw, Extensions of a result of Elekes and Ronyai, *J. Combin. Theory Ser.* A 120 (2013), no. 7, 1695–1713.

[14] M. Sharir, A. Sheffer, and J. Solymosi, Distinct distances on two lines, *J. Combin. Theory Ser. A* 120 (2013), no. 7, 1732-1736.

[15] M. Sharir and J. Zahl, Cutting algebraic curves into pseudo-segments and applications, *J. Combin. Theory Ser. A* 150 (2017), 1-35.

[16] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2006.