

Higher Distance Energies and Expanders with Structure

Cosmin Pohoata* Adam Sheffer†

September 21, 2017

Abstract

We adapt the idea of higher moment energies, originally used in Additive Combinatorics, so that it would apply to problems in Discrete Geometry. This new approach leads to a variety of new results, such as

- (i) Improved bounds for the problem of distinct distances with local properties.
- (ii) Improved bounds for problems involving expanding polynomials in $\mathbb{R}[x, y]$ (Elekes–Rónyai type bounds) when one or two of the sets have structure.

Higher moment energies seem to be related to additional problems in Discrete Geometry, to lead to new elegant theory, and to raise new questions.

1 Introduction

In this work we use techniques from Additive Combinatorics to derive new results for Discrete Geometry problems. We obtain two types of results by using similar techniques: new bounds for several distinct distances problems and new bounds for expanding polynomials when the sets have some kind of structure.

The *Erdős distinct distances problem* is a main problem in Discrete Geometry, which asks for the minimum number of distinct distances spanned by a set of n points in \mathbb{R}^2 . That is, denoting the distance between two points $p, q \in \mathbb{R}^2$ as $|pq|$, the problem asks for $\min_{|\mathcal{P}|=n} |\{ |pq| : p, q \in \mathcal{P} \}|$. Note that n equally spaced points on a line span $n - 1$ distinct distances. Erdős [10] observed that a $\sqrt{n} \times \sqrt{n}$ section of the integer lattice \mathbb{Z}^2 spans $\Theta(n/\sqrt{\log n})$ distinct distances. Proving that every point set determines at least some number of distinct distances turned out to be a deep and challenging problem.

The above problem is just one out of a large family of distinct distances problems, including higher-dimensional variants, structural problems, and many other types of problems (for example, see [28]). The main problems in this family were proposed by Erdős and have been studied for decades. After over 60 years and many works on distinct distances problems, Guth and Katz [14] almost settled the original question by proving that every set of n points in \mathbb{R}^2 spans $\Omega(n/\log n)$ distinct distances. Surprisingly, so far this major discovery was not followed by significant progress in the other main distinct distances problems.

In recent years various results in Additive Combinatorics have been obtained by using *higher moment energies*, which generalize the concept of additive energy (e.g., see [23, 24, 25]). When studying distinct distances problems, one often relies on a set of quadruples that can be thought of as a variant of additive energy (for example, see [4, 13, 14, 19, 26]).

*California Institute of Technology, Pasadena, CA, USA apohoata@caltech.edu.

†Department of Mathematics, Baruch College, City University of New York, NY, USA. adamsh@gmail.com. Supported by NSF grant DMS-1710305

It seems fitting to refer to this object as the *distance energy* of a point set. We extend the idea of higher moment energies by defining the concept of *higher distance energy*. This concept is described in Section 2.

The use of higher distance energy leads to several new distinct distances results, and to possible strategies for studying other such problems. Moreover, it turns out that just thinking of distinct distances in terms of energy leads to various new observations. A similar situation occurs for the family of problems involving expanding polynomials. We believe that this work exposes just another part of a strong connection between the fields of Additive Combinatorics and Discrete Geometry. Our hope is that this connection will continue to unfold, and we plan to continue pursuing this direction.

Distinct distances with local properties. Let $\phi(n, k, l)$ denote the minimum number of distinct distances that are determined by a planar n point set \mathcal{P} with the property that any k points of \mathcal{P} determine at least l distinct distances. That is, by having a local property of every small subset of points, we wish to obtain a global property of the entire point set.

For example, the value of $\phi(n, 3, 3)$ is the minimum number of distinct distances that are determined by a set of n points that do not span any isosceles triangles (including degenerate triangles with three collinear vertices). Since no isosceles triangles are allowed, every point determines $n - 1$ distinct distances with the other points of the set, and we thus have $\phi(n, 3, 3) = \Omega(n)$. Erdős [7] observed the following upper bound for $\phi(n, 3, 3)$. Behrend [2] proved that there exists a set A of positive integers $a_1 < a_2 < \dots < a_n$ such that no three elements of A determine an arithmetic progression and $a_n < n2^{O(\sqrt{\log n})}$. Therefore, the point set $\mathcal{P}_1 = \{(a_1, 0), (a_2, 0), \dots, (a_n, 0)\}$ does not span any isosceles triangles. Since $\mathcal{P}_1 \subset \mathcal{P}_2 = \{(1, 0), (2, 0), \dots, (a_n, 0)\}$ and $D(\mathcal{P}_2) < n2^{O(\sqrt{\log n})}$, we have $\phi(n, 3, 3) < n2^{O(\sqrt{\log n})}$.

For any $k \geq 4$ we have

$$\phi\left(n, k, \binom{k}{2} - \lfloor k/2 \rfloor + 2\right) = \Omega(n^2),$$

since in this case every distance can occur at most $\lfloor k/2 \rfloor - 1$ times. A result of Erdős and Gyárfás [11] implies

$$\phi\left(n, k, \binom{k}{2} - \lfloor k/2 \rfloor + 1\right) = \Omega(n^{4/3}).$$

That is, the boundary between a trivial problem and a non-trivial one passes between $\ell \geq \binom{k}{2} - \lfloor k/2 \rfloor + 2$ and $\ell \leq \binom{k}{2} - \lfloor k/2 \rfloor + 1$.

Recently, Fox, Pach, and Suk [13] showed that for any $\varepsilon > 0$

$$\phi\left(n, k, \binom{k}{2} - k + 6\right) = \Omega(n^{8/7-\varepsilon}).$$

We will prove the following by using higher distance energies.

Theorem 1.1. *For any integers $c, d \geq 2$ we have¹*

$$\phi\left(n, c(d+1), \binom{c(d+1)}{2} - dc + (d+1)\right) = \Omega\left(n^{1+\frac{1}{d}}\right).$$

¹Here and in the following theorems and lemmas, the hidden constant of the asymptotic notation depends on the constants defined in the theorem. For example, the $\Omega(\cdot)$ -notation in the bound of Theorem 1.1 depends on c and d .

For example, by applying Theorem 1.1 with $d = 2$ we get the bound

$$\phi\left(n, k, \binom{k}{2} - 2k/3 + 7\right) = \Omega\left(n^{3/2}\right).$$

(We have $+7$ rather than $+3$ due to cases where k is not divisible by 3.) While there are many problems in which the conjectured number of distinct distances is about n^2 , we are very far from deriving this bound for any of those. As far as we know, the above is the first case where a bound stronger than $\Omega(n^{4/3})$ is obtained for a non-trivial distinct distances problem.

Recall that Erdős and Gyárfás derived a bound of $\Omega(n^{4/3})$ distinct distances when $\ell = \binom{k}{2} - \lfloor k/2 \rfloor + 1$. Theorem 1.1 implies this bound already when $\ell \geq \binom{k}{2} - 3k/4 + 10$. Finally, Theorem 1.1 leads to a better bound than the one of Fox, Pach, and Suk [13] whenever $\ell \geq \binom{k}{2} - 7k/8 + 22$.

The proof of Theorem 1.1 is presented in Section 4.

Expanding polynomials with structure. Given polynomials $f \in \mathbb{R}[x]$ and $g \in \mathbb{R}[x, y]$, and sets $A, B \subset \mathbb{R}$, we write

$$f(A) = \{f(a) : a \in A\} \quad \text{and} \quad g(A, B) = \{g(a, b) : a \in A, b \in B\}.$$

That is, $g(A, B)$ is the set of distinct values that can be obtained by applying g on the lattice $A \times B$.

Elekes and Rónyai [6] proved that $|f(A, B)|$ must be large, unless the polynomial has one of the special forms $f = h(g_1(x) + g_2(y))$ and $f = h(g_1(x) \cdot g_2(y))$, for some $h, g_1, g_2 \in \mathbb{R}[x]$. The current best bound for this problem is the following one by Raz, Sharir, and Solymosi [21].

Theorem 1.2. *Let $A, B \subset \mathbb{R}$ be finite sets, and let $f \in \mathbb{R}[x, y]$ be of a constant-degree. Then, unless $f = h(g_1(x) + g_2(y))$ or $f = h(g_1(x) \cdot g_2(y))$ for some $h, g_1, g_2 \in \mathbb{R}[x]$, we have*

$$f(A, B) = \Omega\left(\min\left\{|A|^{2/3}|B|^{2/3}, |A|^2, |B|^2\right\}\right).$$

Theorem 1.2 generalizes many problems from Discrete Geometry and Additive Combinatorics, and thus has many applications (for example, see [21]).

Given a finite set $A \subset \mathbb{R}$, the *difference set* of A is defined as $A - A = \{a - a' : a, a' \in A\}$. When $A - A$ is small, we say that the set A has an “additive structure” (for details about the meaning of this structure, see for example [32, Chapter 2]). We now derive a stronger Elekes-Rónyai bound when the sets have such an additive structure. We say that a polynomial $f \in \mathbb{R}[x, y]$ is *additively degenerate* if $f = g \circ L$ for some $g \in \mathbb{R}[z]$ and a linear $L \in \mathbb{R}[x, y]$.

Theorem 1.3. *Let $A, B \subset \mathbb{R}$ be finite sets and let $f \in \mathbb{R}[x, y]$ be a polynomial of degree at most d that is not additively degenerate. Then for any $\varepsilon > 0$ we have*

$$|f(A, B)| = \Omega\left(\min\left\{\frac{|A|^{16/9-\varepsilon}|B|^{16/9-\varepsilon}}{|A-A||B-B|}, |A|^2, |B|^2\right\}\right).$$

In the extreme case of $|A - A| = \Theta(|A|)$ and $|B - B| = \Theta(|B|)$, Theorem 1.3 leads to the improved bound $|f(A, B)| = \Omega(|A|^{7/9-\varepsilon}|B|^{7/9-\varepsilon})$. More generally, Theorem 1.3 is stronger than Theorem 1.2 when $|A - A||B - B| = O(|A|^{10/9-\varepsilon}|B|^{10/9-\varepsilon})$ (both theorems

give the same bound when A and B are of significantly different sizes). Moreover, Theorem 1.3 holds for a larger family of polynomials in $\mathbb{R}[x, y]$.

The above result holds only for sets with an additive structure. We can often generalize that result to a much broader definition of structure. We say that a polynomial $p \in \mathbb{R}[x, y]$ is *decomposable* if there exists a univariate polynomial p_1 of degree at least two and $p_2 \in \mathbb{R}[x, y]$ such that $p(x, y) = p_1(p_2(x, y))$. A polynomial that is not decomposable is said to be *indecomposable*. Given a polynomial $\tau \in \mathbb{R}[x]$, we say that a function $\phi : \tau(\mathbb{R}) \rightarrow \mathbb{R}$ is a *one-sided inverse* of τ if it satisfies the following: For every $a \in \tau(\mathbb{R})$ there exists $b \in \mathbb{R}$ such that $\tau(b) = a$ and $\phi(a) = b$. That is, we have that $f(f^{-1}(x)) = x$ for every $x \in \tau(\mathbb{R})$ but not necessarily $f^{-1}(f(y)) = y$ for every $y \in \mathbb{R}$. Note that τ is not required to be injective and the one-sided inverse is not necessarily unique.

Theorem 1.4. *Let $A, B \subset \mathbb{R}$ be finite sets and let $f \in \mathbb{R}[x, y]$ be of degree at most d . Let $\tau_A, \tau_B \in \mathbb{R}[x]$ be of degree at most d , let $\deg \tau_B \geq 2$, and let τ_A^{-1} and τ_B^{-1} be respective one-sided inverses. Assume that $f(\tau_A(x), \tau_B(y))$ is indecomposable, that $A \subset \tau_A(\mathbb{R})$, and that $B \subset \tau_B(\mathbb{R})$. Then for any $\varepsilon > 0$ we have*

$$|f(A, B)| = \Omega \left(\min \left\{ \frac{|A|^{16/9-\varepsilon} |B|^{16/9-\varepsilon}}{|\tau_A^{-1}(A) - \tau_A^{-1}(A)| |\tau_B^{-1}(B) - \tau_B^{-1}(B)|}, |A|^2, |B|^2 \right\} \right).$$

To get some intuition for Theorem 1.4, consider the case where

$$A = B = \left\{ \frac{1^5 - 1^2}{2}, \frac{2^5 - 2^2}{2}, \frac{3^5 - 3^2}{2}, \dots, \frac{n^5 - n^2}{2} \right\}.$$

By setting $\tau_A(x) = \tau_B(x) = (x^5 - x^2)/2$ we get $f(A, B) = \Omega(n^{14/9-\varepsilon})$ for any $f \in \mathbb{R}[x, y]$ for which $f((x^5 - x^2)/2, (y^5 - y^2)/2)$ is indecomposable. More generally, this argument holds for any A and B that contain large subsets of $\tau_A(\{1, 2, 3, \dots\})$ and $\tau_B(\{1, 2, 3, \dots\})$, as long as $f(\tau_A(x), \tau_B(y))$ is indecomposable and τ_B is nonlinear. We thus get a good expansion for sets with a variety of types of polynomial structure. Note that in some cases we also get an expansion for the special forms $f = h(g_1(x) + g_2(y))$ and $f = h(g_1(x) \cdot g_2(y))$.

Asking for $f(\tau_A(x), \tau_B(y))$ to be indecomposable may seem restrictive, but it is not difficult to find interesting applications with this restriction. For example, the problem of distinct distances between two lines (see Section 5) can be reduced to an expansion problem where $f(\tau_A(x), \tau_B(y))$ is indecomposable for *any* τ_A and τ_B .

One expects $f(A, B)$ to be larger when A and B do not have much structure. For example, we expect to obtain non-trivial upper bounds for $f(A, B)$ by taking sets A and B that have some type of structure. Theorems 1.3 and 1.4 are somewhat surprising in the sense that they show that $f(A, B)$ is large when A and B do have structure. One possible approach for improving Theorem 1.2 is to prove that $f(A, B)$ is large when A and B have no structure. Surprisingly, this seems to be the harder case.

Our techniques allow the derivation of many additional related results, such as for the case where only one of the two sets has structure and cases where the sets have a multiplicative structure. We decided not to include such additional results, so as not to make this work too repetitive.

Section 5 contains a proof of Theorems 1.3 and 1.4, and discusses a couple of applications of these theorems.

Bipartite distinct distances. In a bipartite distinct distances problem we have two point sets $\mathcal{P}_1, \mathcal{P}_2$ and are interested only in distances between a point from \mathcal{P}_1 and another

from \mathcal{P}_2 . One basic bipartite problem is when $\mathcal{P}_1, \mathcal{P}_2 \subset \mathbb{R}^2$, all of the points of \mathcal{P}_1 are on a given line, and the points of \mathcal{P}_2 are unrestricted. Elekes [12] derived the following non-intuitive result for this problem.

Theorem 1.5. *If the positive integers n and m satisfy $n \geq 4m^3$, then there exist a set \mathcal{P}_1 of m points on a line ℓ in \mathbb{R}^2 and a set \mathcal{P}_2 of n unrestricted points in \mathbb{R}^2 such that $D(\mathcal{P}_1, \mathcal{P}_2) = O(m^{1/2}n^{1/2})$.*

One non-intuitive consequence of Theorem 1.5 is that the number of distances between n points and a constant number of points can be as small as $\Theta(n^{1/2})$. Elekes asked how close the bound of Theorem 1.5 is to being tight. As far as we know, previously no non-trivial results were known for this question. Brunner and Sharir [3] derived a lower bound on the number of distinct distances between a set of points on a line and another point set. However, their second point set has additional restrictions that forbid Elekes' construction.

By relying on a higher distance energies, we derive the following bound.

Theorem 1.6. *Let \mathcal{P}_1 be a set of m points on a line ℓ in \mathbb{R}^2 and let \mathcal{P}_2 be set of n points in \mathbb{R}^2 . Then*

$$D(\mathcal{P}_1, \mathcal{P}_2) = \begin{cases} \Omega(m^{1/2}n^{1/2} \log^{-1/2} n), & \text{when } m = \Omega(n^{1/2}/\log^{1/3} n), \\ \Omega(n^{3/8}m^{3/4}), & \text{when } m = O(n^{1/2}/\log^{1/3} n) \text{ and } m = \Omega(n^{3/10}), \\ \Omega(n^{1/2}m^{1/3}), & \text{when } m = O(n^{3/10}). \end{cases}$$

Note that when $m = \Omega(n^{1/2}/\log^{1/3} n)$, Theorem 1.6 matches Elekes' bound $O(m^{1/2}n^{1/2})$ up to the $\sqrt{\log n}$. However, Elekes' construction only holds in the separate range $m = O(n^{1/3})$. It is not clear whether similar constructions exist for larger values of m , and it is also possible that when $m > (n/4)^{1/3}$ the number of distinct distances jumps to $\Omega(n/\sqrt{\log n})$.

While it is conjectured that every set of n points in \mathbb{R}^2 spans $\Omega(n/\sqrt{\log n})$ distinct distances, the Guth–Katz analysis [14] leads to the slightly weaker bound $\Omega(n/\log n)$. In Theorem 1.6, when $m = \Omega(n^{1/2}/\log^{1/3} n)$ the distinct distances bound does contain $\sqrt{\log n}$. In fact, the bound $D(\mathcal{P}_1, \mathcal{P}_2) = \Omega(m^{1/2}n^{1/2} \log^{-1/2} n)$ is what one might expect to obtain for the general bipartite variant of the distinct distances problem. This leads to asking whether the third distance energy could lead to such a distinct distances bound in more general cases.

A proof of Theorem 1.6 can be found in Section 6.

Subsets with few repeating distances. Erdős [8, 9] made the following conjecture.

Conjecture 1.7. *Let \mathcal{P} be a set of n points in \mathbb{R}^2 . Then there exists a subset $\mathcal{P}' \subset \mathcal{P}$ such that $|\mathcal{P}'| = \Omega(n^{1/2})$ and no distance is spanned by two pairs of points of \mathcal{P}' .*

In other words, the conjecture suggests that every planar point set contains a large subset with no repeating distances. Charalambides [4] showed that the Guth–Katz result [14] implies the existence of a subset of size $\Omega(n^{1/3} \log^{-1/3} n)$ with no repeating distances. This is the current best bound. By using higher distance energies, we can show that there exists a larger subset with no distance repeating more than twice.

Theorem 1.8. *Let $\mathcal{P} \subset \mathbb{R}^2$ be a set of n points. Then there exists a subset $\mathcal{P}' \subset \mathcal{P}$ of size $\Omega(n^{22/63} \log^{-13/63} n)$ such that no distance is spanned by more than four pairs of points of \mathcal{P}' . Similarly, there exists a subset $\mathcal{P}' \subset \mathcal{P}$ of size $\Omega(n^{12/35} \log^{-9/35} n)$ such that no distance is spanned by more than two pairs of points of \mathcal{P}' .*

Once again, our techniques can lead to a variety of related results but we decided not to include too many similar results. The proof of Theorem 1.8 and one of its variants can be found in Section 7.

Acknowledgements. The second author would like to thank Micha Sharir for several useful discussions.

2 Higher distance energies

For $a, b \in \mathbb{R}^2$, we denote by $|ab|$ the Euclidean distance between these two points. Let \mathcal{P} be a set of n points in \mathbb{R}^2 and let $d \geq 1$ be an integer. We define the d 'th distance energy of \mathcal{P} as

$$E_d(\mathcal{P}) = \left| \left\{ (a_1, b_1, \dots, a_d, b_d) \in \mathcal{P}^{2d} : |a_1 b_1| = \dots = |a_d b_d| > 0 \right\} \right|. \quad (1)$$

The $2d$ -tuples are ordered, so $(a_1, b_1, a_2, b_2, \dots, a_d, b_d)$ and $(b_1, a_1, a_2, b_2, \dots, a_d, b_d)$ are considered as two distinct tuples in the above set.

Let $\Delta = \Delta(\mathcal{P})$ be the set of distances that are spanned by pairs of points of \mathcal{P} . For a distance $\delta \in \Delta$, we denote by m_δ the number of ordered pairs $(a, b) \in \mathcal{P}^2$ such that $|ab| = \delta$. Note that the number of $2d$ -tuples in (1) that correspond to a specific $\delta \in \Delta$ is exactly m_δ^d . This implies that

$$E_d(\mathcal{P}) = \sum_{\delta \in \Delta} m_\delta^d. \quad (2)$$

Since every ordered pair of distinct points $(a, b) \in \mathcal{P}^2$ contributes to exactly one m_δ , we have that $\sum_{\delta \in \Delta} m_\delta = 2 \binom{n}{2} = n^2 - n$. Let $D = D(\mathcal{P}) = |\Delta|$ be the number of distinct distances spanned by point of \mathcal{P} . By Hölder's inequality, for any $d \geq 2$ we have

$$E_d(\mathcal{P}) = \sum_{\delta \in \Delta} m_\delta^d \geq \frac{(\sum_{\delta \in \Delta} m_\delta)^d}{D^{d-1}} = \frac{(n^2 - n)^d}{D^{d-1}} = \Omega\left(\frac{n^{2d}}{D^{d-1}}\right). \quad (3)$$

Using somewhat different notation, Guth and Katz [14] derived the tight upper bound

$$E_2(\mathcal{P}) = O(n^3 \log n). \quad (4)$$

Also using different notation, Spencer, Szemerédi, and Trotter [30] proved that every $\delta \in \Delta$ satisfies

$$m_\delta = O(n^{4/3}). \quad (5)$$

For any integer $d \geq 2$, combining (4) and (5) implies

$$E_d(\mathcal{P}) = \sum_{\delta \in \Delta} m_\delta^d = O\left(\left(n^{4/3}\right)^{d-2} \sum_{\delta \in \Delta} m_\delta^2\right) = O\left(n^{(4d+1)/3} \log n\right).$$

It seems reasonable to make the following conjecture

Conjecture 2.1. For every set \mathcal{P} of n points in \mathbb{R}^2 , integer $d \geq 2$, and $\varepsilon > 0$,

$$E_d(\mathcal{P}) = O(n^{d+1+\varepsilon}).$$

The unit distances conjecture suggests that $m_\delta = O(n^{1+\varepsilon})$ for every $\delta \in \Delta$, which would immediately imply conjecture 2.1. In Section 7 we use geometric incidences to prove the stronger bound $E_3(\mathcal{P}) = O\left(n^{30/7} \log^{9/7} n\right)$. Similar techniques lead to improved bounds for $E_d(\mathcal{P})$ when $d \geq 4$. Further improving these bounds would immediately improve the results of Section 7, and possibly other parts of this paper.

Distance energy variants. For finite sets $\mathcal{P}_1, \mathcal{P}_2 \subset \mathbb{R}^2$ and an integer $d \geq 2$, we define the d 'th distance energy of \mathcal{P}_1 and \mathcal{P}_2 as

$$E_d(\mathcal{P}_1, \mathcal{P}_2) = \left\{ (a_1, \dots, a_d, b_1, \dots, b_d) \in \mathcal{P}_1^d \times \mathcal{P}_2^d : |a_1 b_1| = \dots = |a_d b_d| > 0 \right\}.$$

Note that in this case we are only interested in distances between points from different sets, and ignore the distances between points in the same set. This corresponds to a bipartite distinct distances problem, as defined in the introduction. For such problems we define $\Delta = \Delta(\mathcal{P}_1, \mathcal{P}_2)$ to be the set of distances spanned by pairs of $\mathcal{P}_1 \times \mathcal{P}_2$. The number of distinct distances is defined accordingly as $D = D(\mathcal{P}_1, \mathcal{P}_2) = |\Delta|$. By imitating the argument that led to (3), we obtain the bound

$$E_d(\mathcal{P}_1, \mathcal{P}_2) = \Omega\left(\frac{|\mathcal{P}_1|^d |\mathcal{P}_2|^d}{D^{d-1}}\right). \quad (6)$$

Finally, for a point set $\mathcal{P} \subset \mathbb{R}^2$ and a positive integer $d \geq 2$, we define

$$E_d^*(\mathcal{P}) = \left\{ (a_1, b_1, \dots, a_d, b_d) \in \mathcal{P}^{2d} : |a_1 b_1| = \dots = |a_d b_d| \text{ and the } 2d \text{ points are distinct} \right\}.$$

In other words, $E_d^*(\mathcal{P})$ is a variant of $E_d(\mathcal{P})$ that considers only tuples with $2d$ distinct elements. By definition $E_d^*(\mathcal{P}) < E_d(\mathcal{P})$.

3 Geometric preliminaries

Tools from Discrete Geometry. Given a set \mathcal{P} of points and a set Γ of curves in \mathbb{R}^2 (such as lines, circles, or sine waves), an *incidence* is a pair $(p, \gamma) \in \mathcal{P} \times \Gamma$ such that the point p is contained in the curve γ . The number of incidences in $\mathcal{P} \times \Gamma$ is denoted as $I(\mathcal{P}, \Gamma)$. The *incidence graph* of $\mathcal{P} \times \Gamma$ is a bipartite graph $G = (\mathcal{P} \cup \Gamma, E)$, where an edge $(v_j, v_k) \in E$ implies that the point that corresponds to v_j is incident to the curve that corresponds to v_k ; that is, there is a bijection between the edges of E and the incidences in $\mathcal{P} \times \Gamma$. The following incidence bound is by Pach and Sharir [18].

Theorem 3.1. *Let \mathcal{P} be a set of m points and let Γ be a set of n distinct irreducible algebraic curves of degree at most k , both in \mathbb{R}^2 . If the incidence graph of $\mathcal{P} \times \Gamma$ contains no copy of $K_{2,t}$, then*

$$I(\mathcal{P}, \Gamma) = O\left(m^{2/3} n^{2/3} + m + n\right).$$

The following incidence bound is a combination of results from several papers (for example, see Sharir and Zahl [27]).

Theorem 3.2. *Let \mathcal{P} be a set of m points and let Γ be a set of n circles, both in \mathbb{R}^2 . Then*

$$I(\mathcal{P}, \Gamma) = O\left(m^{6/11} n^{9/11} \log^{2/11} n + m^{2/3} n^{2/3} + m + n\right).$$

The following incidence result is by Sharir and Zahl [27].

Theorem 3.3. *Let \mathcal{P} be a set of m points and let Γ be a set of n irreducible algebraic curves of degree at most k in \mathbb{R}^2 . Assume that we can parameterize these curves using s parameters. Then for every $\varepsilon > 0$ we have*

$$I(\mathcal{P}, \Gamma) = O\left(m^{\frac{2s}{5s-4} + \varepsilon} n^{\frac{5s-6}{5s-4}} + m^{2/3} n^{2/3} + m + n\right).$$

Note that Theorem 3.3 almost generalizes Theorem 3.2, except that m^ε is asymptotically larger than $\log^{2/11} n$ (for the range of m and n in which the term $m^{6/11} n^{9/11}$ dominates the bound).

We will rely on the following distinct distances result of Pach and de Zeeuw [19].

Theorem 3.4. *Let γ_1 and γ_2 be two distinct irreducible algebraic curves of degree at most d in \mathbb{R}^2 , which are not parallel lines, orthogonal lines, or concentric circles. Let \mathcal{P}_1 be a set of m points that are incident to γ_1 and let \mathcal{P}_2 be a set of n points incident to γ_2 . Then*

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega\left(\min\left\{m^{2/3} n^{2/3}, m^2, n^2\right\}\right).$$

For a point set $\mathcal{P} \subset \mathbb{R}^2$, let $t(\mathcal{P})$ denote the number of isosceles triangles that are spanned by \mathcal{P} (that is, isosceles triangles that have their three vertices in \mathcal{P}). The following result is by Pach and Tardos [17].

Theorem 3.5. *Let \mathcal{P} be a set of n points in \mathbb{R}^2 . Then $t(\mathcal{P}) = O(n^{2.137})$*

Tools from Algebraic Geometry. For a polynomial $f \in \mathbb{R}[x_1, \dots, x_d]$ we denote by $\mathbf{V}(f)$ the variety defined by f (that is, the set of points in \mathbb{R}^d on which f vanishes).

Theorem 3.6 (Milnor–Thom [16]). *Let $f_1, \dots, f_m \in \mathbb{R}[x_1, \dots, x_d]$ be of degree at most k . Then the number of connected components of $\mathbf{V}(f_1, \dots, f_m)$ is at most*

$$k(2k - 1)^{d-1}.$$

A polynomial $f \in \mathbb{R}[x, y]$ is said to be *reducible* if there exist polynomials $f_1, f_2 \in \mathbb{R}[x, y]$ of positive degrees such that $f(x, y) = f_1(x, y) \cdot f_2(x, y)$. A polynomial that is not reducible is said to be *irreducible*. The following result is a combination of [1] and [31] (for more details, see for example [21]).

Theorem 3.7. *If $f \in \mathbb{R}[x, y]$ is indecomposable, then the polynomial $f(x, y) - \lambda$ is reducible for at most $\deg f$ values of $\lambda \in \mathbb{R}$.*

Finally, we will rely on the following Schwartz–Zippel variant in \mathbb{R}^2 .

Lemma 3.8. *Let $f \in \mathbb{R}[x, y]$ be a polynomial of degree $d > 0$, and let $A, B \subset \mathbb{R}$ be finite sets. Then*

$$|\mathbf{V}(f) \cap (A \times B)| = O(|A| + |B|).$$

4 Distinct Distances with Local Properties

In this section we prove Theorem 1.1. We begin by recalling the statement of this theorem.

Theorem 1.1. *For any integers $c, d \geq 2$ we have*

$$\phi\left(n, c(d+1), \binom{c(d+1)}{2} - dc + (d+1)\right) = \Omega\left(n^{1+\frac{1}{d}}\right).$$

To prove the theorem, we will rely on the following simple counting lemma (for example, see [15, Lemma 2.3]).

Lemma 4.1. *Let A be a set of n elements and let $d \geq 2$ be an integer. Let A_1, \dots, A_k be subsets of A , each of size at least m . If $k \geq 2dn^d/m^d$ then there exist $1 \leq j_1 < \dots < j_d \leq d$ such that $|A_{j_1} \cap \dots \cap A_{j_d}| \geq \frac{m^d}{2n^{d-1}}$.*

Proof of Theorem 1.1. Let \mathcal{P} be a set of n points such that every $c(d+1)$ points of \mathcal{P} span at least $\binom{c(d+1)}{2} - dc + (d+1)$ distinct distances. We say that a point $p \in \mathcal{P}$ *spans* a distance δ if there exists a point $q \in \mathcal{P}$ such that $|pq| = \delta$. We begin by studying some configurations that cannot occur in \mathcal{P} .

Forbidden configurations. Assume that a point $p \in \mathcal{P}$ is at a distance of δ from at least $dc - d + 1$ points of \mathcal{P} . Let $\mathcal{P}' \subset \mathcal{P}$ consist of p , of $dc - d + 1$ points of \mathcal{P} that are at a distance of δ from p , and of $d + c - 2$ additional points of \mathcal{P} . Then \mathcal{P}' is a set of $c(d+1)$ points of \mathcal{P} that span at most $\binom{c(d+1)}{2} - dc + d$ distinct distances, contradicting the assumption on \mathcal{P} . This contradiction implies that for every $p \in \mathcal{P}$ and distance δ , at most $dc - d$ points of \mathcal{P} are at a distance of δ from p . This in turn implies that every distance is spanned by at most $d(c-1)n/2$ pairs of \mathcal{P}^2 .

Let $\delta_1, \dots, \delta_d$ be distinct distances and let $\mathcal{P}' \subset \mathcal{P}$ be a set of c points, such that every $p \in \mathcal{P}'$ spans each of the distances $\delta_1, \dots, \delta_d$ with a point of $\mathcal{P} \setminus \mathcal{P}'$. We construct a set \mathcal{P}'' by going over every point $p \in \mathcal{P}$ and distance δ_j , and adding to \mathcal{P}'' one point of $\mathcal{P} \setminus \mathcal{P}'$ that is at a distance of δ_j from p . If a point $q \in \mathcal{P} \setminus \mathcal{P}'$ was added several times to \mathcal{P}'' , we consider \mathcal{P}'' as containing one instance of q (that is, \mathcal{P}'' is not a multiset). We get that $\mathcal{P}' \cup \mathcal{P}''$ is a set of at most $c(d+1)$ points, with at least c pairs of points at distance δ_j for every $1 \leq j \leq d$. That is, the set $\mathcal{P}' \cup \mathcal{P}'' \subset \mathcal{P}$ spans at most $\binom{c(d+1)}{2} - dc + d$ distinct distances. This contradicts the assumption on \mathcal{P} , and implies that \mathcal{P} cannot contain such a configuration.

Next, we slightly change the case studied in the previous paragraph: We assume that every point of \mathcal{P}' spans the distances $\delta_1, \dots, \delta_d$ with points of \mathcal{P} (rather than of $\mathcal{P} \setminus \mathcal{P}'$) and that each of the distances $\delta_1, \dots, \delta_d$ is spanned by at least c pairs of points of \mathcal{P} . We construct the set $\mathcal{P}'' \subset \mathcal{P}$ as in the previous paragraph: For every $p \in \mathcal{P}$ and distance δ_j , if there exist points of $\mathcal{P} \setminus \mathcal{P}'$ at distance δ_j from p then we add one such point to \mathcal{P}'' . For $1 \leq j \leq d$, let k_j denote the number of points of \mathcal{P}' that are not at distance δ_j from any point of $\mathcal{P} \setminus \mathcal{P}'$. By the previous paragraph, the case where $k_1 = \dots = k_d = 0$ is forbidden. Note that for every $1 \leq j \leq d$, at least $k_j/2$ pairs of points of \mathcal{P}' are at distance δ_j . That is, $\mathcal{P}^* = \mathcal{P}' \cup \mathcal{P}''$ is a set of at most $(d+1)c - \sum_{j=1}^d k_j$ points of \mathcal{P} and at least $c - k_j/2$ pairs of points at distance δ_j . For $1 \leq j \leq d$, we add $\lfloor k_j/2 \rfloor$ additional pairs at distance δ_j by adding at most k_j vertices of \mathcal{P} to \mathcal{P}^* . This is possible by the assumption that δ_j is spanned by at least c pairs of points of \mathcal{P} . Since the resulting set \mathcal{P}^* contradicts the assumption about \mathcal{P} , this configuration is also forbidden.

Rich distances. For an integer j , let Δ_j be the set of distances spanned by at least j pairs of points of \mathcal{P} , and set $k_j = |\Delta_j|$. Let \mathcal{P}_δ be the set of points of \mathcal{P} that span δ .

Fix $j \geq d(2c^{d+1}n^{d-1})^{1/d}$ and let $\delta \in \Delta_j$. Since every point spans δ with at most $dc - d$ points of \mathcal{P} , we get that $|\mathcal{P}_\delta| \geq \frac{2j}{dc-d} > \frac{j}{dc}$. By the last forbidden configuration above, for any choice of $\delta_1, \dots, \delta_d \in \Delta_j$ we have $|\mathcal{P}_{\delta_1} \cap \dots \cap \mathcal{P}_{\delta_d}| < c$. By the assumption on j we have $c \leq \frac{j^d}{2c^d d^d n^{d-1}}$. We may thus apply the contrapositive of Lemma 4.1 on the sets \mathcal{P}_δ with $\delta \in \Delta_j$ and with $m = \frac{j}{dc}$. This implies

$$k_j < \frac{2dn^d}{(j/dc)^d} = \frac{2n^d d^{d+1} c^d}{j^d}. \quad (7)$$

For $j < d(2c^{d+1}n^{d-1})^{1/d}$ (and also for larger values of j), we have the straightforward bound

$$k_j < n^2/j. \quad (8)$$

An energy argument. Recall the notation Δ , D , and m_δ from Section 2. Since no distance is spanned by more than $d(c-1)n/2$ pairs of points of \mathcal{P} , we have that $m_\delta \leq d(c-1)n$ for every $\delta \in \Delta$. Let $m = \lfloor \log d(2c^{d+1}n^{d-1})^{1/d} \rfloor$. By dyadic pigeonholing together with (7) and (8), we obtain

$$\begin{aligned} E_d(\mathcal{P}) &= \sum_{\delta \in \Delta} m_\delta^d = \sum_{j=0}^{\log(dcn)} \sum_{\substack{\delta \in \Delta \\ 2^j \leq m_\delta < 2^{j+1}}} m_\delta^d < \sum_{j=0}^{\log(dcn)} k_{2^j} (2^{j+1})^d \\ &= \sum_{j=0}^m k_{2^j} 2^{d(j+1)} + \sum_{j=m+1}^{\log(dcn)} k_{2^j} 2^{d(j+1)} \\ &= O\left(n^{2+(d-1)^2/d}\right) + O\left(n^d \log n\right) = O\left(n^{2+(d-1)^2/d}\right). \end{aligned}$$

Recall from (3) that $E_d(\mathcal{P}) = \Omega\left(\frac{n^{2d}}{D^{d-1}}\right)$. Combining these two bounds on $E_d(\mathcal{P})$ yields the assertion of the theorem. \square

One way to improve the proof of Theorem 1.1 might be to derive an upper bound on k_j stronger than the straightforward bound of (8) when $j \approx n^{(d-1)/d}$.

5 Elekes–Ronyai bounds with additive structure

In this section we prove Theorems 1.3 and 1.4, and discuss some of their applications. We begin by recalling the statement of Theorem 1.3.

Theorem 1.3. *Let $A, B \subset \mathbb{R}$ be finite sets and let $f \in \mathbb{R}[x, y]$ be a polynomial of degree at most d that is not additively degenerate. Then for any $\varepsilon > 0$ we have*

$$|f(A, B)| = \Omega\left(\min\left\{\frac{|A|^{16/9-\varepsilon}|B|^{16/9-\varepsilon}}{|A-A||B-B|}, |A|^2, |B|^2\right\}\right).$$

Theorem 1.3 has many applications, and we now present a couple of those. We begin with the following distinct distances result from [26].

Theorem 5.1. *Let ℓ_1 and ℓ_2 be two lines in \mathbb{R}^2 that are neither parallel nor orthogonal. Let \mathcal{P}_1 and \mathcal{P}_2 be sets of points in \mathbb{R}^2 of size n and m respectively, such that \mathcal{P}_1 is contained in ℓ_1 , and \mathcal{P}_2 is contained in ℓ_2 . Then*

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega \left(\min \left\{ n^{2/3} m^{2/3}, n^2, m^2 \right\} \right).$$

One reason for why the above distinct distances problem is considered interesting is that it has many generalizations (such as Theorem 1.2). Improving the known bounds for the distances problem tends to lead to improvements for various generalizations. Quoting Hilbert [22]: “The art of doing mathematics is finding that special case that contains all the germs of generality.” The following is an easy corollary of Theorems 1.3 and 1.4.

Corollary 5.2.

(a) *Let ℓ_1 and ℓ_2 be two lines in \mathbb{R}^2 that are neither parallel nor orthogonal. Let \mathcal{P}_1 and \mathcal{P}_2 be sets of points in \mathbb{R}^2 of size n and m respectively, such that $\mathcal{P}_1 \subset \ell_1$ and $\mathcal{P}_2 \subset \ell_2$. Let A be the set of x -coordinates of the points of \mathcal{P}_1 , and let B be the set of x -coordinates of the points of \mathcal{P}_2 (assuming the neither line is parallel to the y -axis). Then*

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega \left(\min \left\{ \frac{m^{16/9-\varepsilon} n^{16/9-\varepsilon}}{|A - A||B - B|}, m^2, n^2 \right\} \right).$$

(b) *Let $\tau_A, \tau_B \in \mathbb{R}[x]$ be of degree at most d , let $\deg \tau_B \geq 2$, and let τ_A^{-1} and τ_B^{-1} be respective one-sided inverses. Assume that $f(\tau_A(x), \tau_B(y))$ is indecomposable, that $A \subset \tau_A(\mathbb{R})$, and that $B \subset \tau_B(\mathbb{R})$. Then for any $\varepsilon > 0$*

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega \left(\min \left\{ \frac{m^{16/9-\varepsilon} n^{16/9-\varepsilon}}{|\tau_A^{-1}(A) - \tau_A^{-1}(A)||\tau_B^{-1}(B) - \tau_B^{-1}(B)|}, m^2, n^2 \right\} \right).$$

Proof sketch. In [26] the distinct distances problem is reduced to showing that the polynomial $f(x, y) = x^2 - 2xy + (1 + s^2)y^2$ expands (where $s \in \mathbb{R} \setminus \{0\}$ depends on the angle between ℓ_1 and ℓ_2). It can be easily verified that $f(x, y)$ is indecomposable, so we can apply Theorem 1.3 with it. Plugging the resulting expansion bound in the analysis of [26] immediately leads to the bound of part (a).

For τ_A and τ_B of respective degrees d and $d' \geq 2$, assume for contradiction that $f(\tau_A(x), \tau_B(y))$ is decomposable. That is, there exist $g \in \mathbb{R}[x, y]$ and $h \in \mathbb{R}[z]$ of degree at least two such that $f(\tau_A(x), \tau_B(y)) = h(g(x, y))$. Note that $f(\tau_A(x), \tau_B(y))$ contains terms of the form $(c \cdot x)^{2d}$ and $(1 + s^2)(c' \cdot y)^{2d'}$ where $c, c' \in \mathbb{R} \setminus \{0\}$. In every other term of $f(\tau_A(x), \tau_B(y))$ the degree of x is smaller than $2d$ and the degree of y is smaller than $2d'$. This implies that $2d = \deg h \cdot \deg_x g$, and that $2d' = \deg h \cdot \deg_y g$.

By the above, $f(\tau_A(x), \tau_B(y))$ should also contain a term where x is of degree $2d \cdot \frac{\deg h - 1}{\deg h}$ and y is of degree at least one. By the definition of $f(x, y)$, we note that $f(\tau_A(x), \tau_B(y))$ does not contain terms with an exponent of x larger than d that also involve y . We thus get that $\deg h = 2$. Let c_2 be the coefficient of z^2 in $h \in \mathbb{R}[z]$. Recalling the terms $(c \cdot x)^{2d}$ and $(1 + s^2)(c' \cdot y)^{2d'}$, we get that $g(x, y)$ contains the terms $c_2^{-1/2}(c \cdot x)^d$ and $c_2^{-1/2}(1 + s^2)^{1/2}(c' \cdot y)^{d'}$. This in turn implies that $f(\tau_A(x), \tau_B(y))$ should also contain the term $2(c \cdot x)^d(1 + s^2)^{1/2}(c' \cdot y)^{d'}$. From the definition of $f(x, y)$ we note that $f(\tau_A(x), \tau_B(y))$ contains the slightly different term $2(c \cdot x)^d(c' \cdot y)^{d'}$. Since $s \neq 0$ we get a contradiction, so $f(\tau_A(x), \tau_B(y))$ must be indecomposable. Applying Theorem 1.4 with $f(\tau_A(x), \tau_B(y))$ immediately leads to part (b). \square

For example, when $|A - A| = \Theta(n)$ and $|B - B| = \Theta(m)$ we have $D(\mathcal{P}_1, \mathcal{P}_2) = \Omega(\min\{m^{7/9-\varepsilon}n^{7/9-\varepsilon}, m^2, n^2\})$. One approach to improving Theorem 5.1 is to improve the case where A and B have no additive or polynomial structure.

We next consider a result of Shen [29].

Theorem 5.3. *Let $f \in \mathbb{R}[x, y]$ be a polynomial of a constant-degree that is not additively degenerate, and let $A \subset \mathbb{R}$ be finite. Then*

$$|A + A| + |f(A, A)| = \Omega(|A|^{5/4}).$$

Theorem 1.3 implies a better lower bound for $|f(A, A)|$ when $|A + A| = O(|A|^{83/72-\varepsilon})$.² Thus, to improve the bound of Theorem 5.3 it remains to handle the case where $|A + A| = \Omega(|A|^{83/72})$ and $|A + A| = O(|A|^{5/4})$.

Theorems 1.3 and 1.4 have many additional applications. See for example the applications presented in [21].

Proof of Theorem 1.3. If f is decomposable, then there exist a univariate f_1 of degree at least two and $f_2 \in \mathbb{R}[x, y]$ such that $f(x, y) = f_1(f_2(x, y))$. Let (f_1, f_2) be a pair of such polynomials that minimizes the degree of f_2 . In particular, this implies that f_2 is indecomposable. Since f is of degree at most d , so are f_1 and f_2 . Since f_1 is univariate, for every $a \in \mathbb{R}$ there exist at most d numbers $b \in \mathbb{R}$ such that $f_1(b) = a$. Thus, if $|f_2(A, B)| \geq x$ for some x , then $|f(A, B)| \geq x/d$. It then remains to derive the bound of the theorem to the indecomposable f_2 . Since f is assumed not to be additively degenerate, so is f_2 . With an abuse of notation, we will refer to f_2 as f . We may thus assume that f is indecomposable.

Let $\Delta = \{f(a, b) : a \in A, b \in B\}$, and let $D = |\Delta|$. For $\delta \in \Delta$, let

$$m_\delta = |\{(a, b) \in A \times B : f(a, b) = \delta\}|.$$

In other words, m_δ is the number of representations of δ as $f(a, b)$. For an integer $j \geq 1$, let Δ_j be the set of $\delta \in \Delta$ that satisfy $m_\delta \geq j$, and let $k_j = |\Delta_j|$.

Imitating the concept of bipartite distance energy, we define the energy

$$E_f(A, B) = |\{(a_1, a_2, b_1, b_2) \in A^2 \times B^2 : f(a_1, b_1) = f(a_2, b_2)\}|.$$

Note that $m_\delta = |\mathbf{V}(f - \delta) \cap (A \times B)|$. By Lemma 3.8, every $\delta \in \Delta$ satisfies $m_\delta = O(|A| + |B|)$. That is, there exists a constant μ such that $k_{\mu(|A|+|B|)} = 0$. We thus have

$$E_f(A, B) = \sum_{\delta \in \Delta} m_\delta^2 = \sum_{j=0}^{\log \mu(|A|+|B|)} \sum_{\substack{\delta \in \Delta \\ 2^j \leq m_\delta < 2^{j+1}}} m_\delta^2 < \sum_{j=0}^{\log \mu(|A|+|B|)} 2^{2j+2} k_{2^j}. \quad (9)$$

Since every $(a, b) \in A \times B$ contributes to one m_δ , we have that $\sum_{\delta \in \Delta} m_\delta = |A||B|$. By the Cauchy-Schwarz inequality, we obtain

$$E_f(A, B) = \sum_{\delta \in \Delta} m_\delta^2 \geq \frac{(\sum_{\delta \in \Delta} m_\delta)^2}{D} = \frac{|A|^2 |B|^2}{D}. \quad (10)$$

²In Theorem 1.3 it is easy to replace $A - A$ with $A + A$: In the proof we take $\alpha \in A + A$, replace $x + \alpha$ with $\alpha - x$, and handle β in a symmetric manner. The rest of the proof remains the same.

A set of curves. For a fixed $j \geq 2d$, consider the set of curves

$$\Gamma_j = \{\mathbf{V}(f(x + \alpha, y + \beta) - \delta) : \alpha \in A - A, \beta \in B - B, \delta \in D_j\}.$$

Assume for contradiction that there exist $(\alpha, \beta, \delta), (\alpha', \beta', \delta') \in (A - A) \times (B - B) \times D_j$ and $r \in \mathbb{R}$ such that

$$f(x + \alpha, y + \beta) - \delta = r \cdot (f(x + \alpha', y + \beta') - \delta').$$

For the maximum degree terms on both sides to have the same coefficients, we must have $r = 1$. We replace x with $x - \alpha'$ and y with $y - \beta'$ (that is, we translate the plane by $-\alpha'$ in the x -direction and by $-\beta'$ in the y -direction). Setting $\alpha_0 = \alpha - \alpha'$ and $\beta_0 = \beta - \beta'$ leads to

$$f(x + \alpha_0, y + \beta_0) = f(x, y) - \delta' + \delta. \quad (11)$$

One obvious solution to (11) is $\alpha_0 = \beta_0 = 0$ and $\delta = \delta'$. We now assume that this is not the case. Without loss of generality we assume that $\beta_0 \neq 0$ and let k be the degree of x in f (otherwise, $\alpha_0 \neq 0$ and we take k to be the degree of y). We claim that in this case $f(x, y) = h(x + cy)$ where $c = -\alpha_0/\beta_0$ and $h \in \mathbb{R}[z]$, and prove this by induction on k . For the induction basis, consider the case of $k = 0$. Since f does not depend on x and is of degree at least two, we get from (11) that f is a constant function. The claim follows by taking h to be the same constant function.

For the induction step, consider $k \geq 1$. For $0 \leq \ell \leq k$, let $f_\ell \in \mathbb{R}[y]$ be the coefficient of x^ℓ in f . That is,

$$f(x, y) = \sum_{\ell=0}^k x^\ell f_\ell(y).$$

From (11) and the assumption $\beta_0 \neq 0$, we have that $f_k(y)$ is constant. We set $g(x, y) = f(x, y) - (x + cy)^k \cdot f_k(y)$, and note that $g(x, y)$ is of degree $k - 1$ in x . By (11) and the definition of c , we have that

$$\begin{aligned} g(x + \alpha_0, y + \beta_0) &= f(x + \alpha_0, y + \beta_0) - (x + \alpha_0 + c(y + \beta_0))^k \cdot f_k(y) \\ &= f(x, y) - \delta' + \delta - (x + cy)^k \cdot f_k(y) = g(x, y) - \delta' + \delta. \end{aligned}$$

We may thus apply the induction hypothesis on g , and obtain that $g = h'(x + cy)$ for some $h' \in \mathbb{R}[z]$. Since $g(x, y) = f(x, y) - (x + cy)^k \cdot f_k(y)$ and $f_k(y)$ is constant, we conclude that $f = h(x + cy)$ for some $h \in \mathbb{R}[z]$. This implies that f is additively degenerate also before the aforementioned translation of \mathbb{R}^2 .

To recap, we proved that either $\alpha_0 = \beta_0 = 0$ and $\delta = \delta'$, or f is additively degenerate. Since the latter contradicts the assumption, we are in the former case. This in turn implies that Γ_j is a set of $|A - A||B - B|k_j$ curves that are defined by distinct polynomials. Moreover, no polynomial is a constant multiple of another. While the polynomials are distinct, the curves of Γ_j may still have common components.

Studying rich δ 's. Since f is indecomposable, Theorem 3.7 implies that there are at most d values of $\delta \in \Delta$ such that $f(x, y) - \delta$ is reducible. For any $\alpha, \beta \in \mathbb{R}$, since $\mathbf{V}(f(x + \alpha, y + \beta) - \delta)$ is a translation of $\mathbf{V}(f(x, y) - \delta)$, either both curves are reducible or both are irreducible. Thus, at most $d|A - A||B - B|$ curves of Γ_j are reducible.

If $k_j \geq 2d$, then after removing the reducible curves from Γ_j we still have $|\Gamma_j| = \Theta(|A - A||B - B|k_j)$. Assume that we are in this case, and let $\mathcal{P} = A \times B \subset \mathbb{R}^2$. By

applying Theorem 3.3 with $s = 3$, we obtain

$$I(\mathcal{P}, \Gamma_j) = O\left(|A|^{6/11+\varepsilon'}|B|^{6/11+\varepsilon'}|A-A|^{9/11}|B-B|^{9/11}k_j^{9/11} + |A|^{2/3}|B|^{2/3}k_j^{2/3}|A-A|^{2/3}|B-B|^{2/3} + k_j|A-A||B-B| + |A||B|\right). \quad (12)$$

Since $k_j < |A||B|$, $|A-A| > |A|$, $|B-B| > |B|$, $|A-A| < |A|^2$, and $|B-B| < |B|^2$, we get that the bound on the right-hand side of (12) is always dominated by its first term. That is, we have

$$I(\mathcal{P}, \Gamma_j) = O\left(|A|^{6/11+\varepsilon'}|B|^{6/11+\varepsilon'}|A-A|^{9/11}|B-B|^{9/11}k_j^{9/11}\right). \quad (13)$$

For every $\delta \in D_j$, there are at least j pairs $(a, b) \in A \times B$ that satisfy $f(a, b) = \delta$. Fix such a pair (a, b) . Then for every $a' \in A$ and $b' \in B$, there exist $\alpha \in A - A$ and $\beta \in B - B$ such that $f(a' + \alpha, b' + \beta) = f(a, b) = \delta$. Thus, every $\delta \in D_j$ has at least $j|A||B|$ corresponding incidences in $\mathcal{P} \times \Gamma_j$. By summing this over every $\delta \in D_j$ with irreducible curves we get that $I(\mathcal{P}, \Gamma_j) = \Omega(j|A||B|k_j)$. Combining this with (13) gives

$$j|A||B|k_j = O\left(|A|^{6/11+\varepsilon'}|B|^{6/11+\varepsilon'}|A-A|^{9/11}|B-B|^{9/11}k_j^{9/11}\right).$$

Rearranging leads to

$$k_j = O\left(\frac{|A-A|^{9/2}|B-B|^{9/2}}{|A|^{5/2-11\varepsilon'/2}|B|^{5/2-11\varepsilon'/2}j^{11/2}}\right).$$

Recall that the above analysis holds only when $k_j \geq 2d$. Let J be the set of integers $j \geq 1$ that satisfy $1 \leq k_j < 2d$. Since every $\delta \in \Delta_j$ has at least j corresponding distinct pairs in $A \times B$, we have the straightforward bound

$$k_j = O(|A||B|/j).$$

We set $\varepsilon = 11\varepsilon'/9$ and $\gamma = \frac{|A-A||B-B|}{|A|^{7/9-\varepsilon}|B|^{7/9-\varepsilon}}$. Combining (9) with both of the above upper bounds for k_j implies

$$\begin{aligned} E_f(A, B) &< \sum_{j=0}^{\log \mu(|A|+|B|)} 2^{2j+2}k_{2j} \leq 4 \sum_{j=0}^{\log \gamma} 2^{2j}k_{2j} + 4 \sum_{\log \gamma+1}^{\log \mu(|A|+|B|)} 2^{2j}k_{2j} \\ &= O\left(\sum_{j=0}^{\log \gamma} |A||B|2^j + \sum_{j=\log \gamma+1}^{\log \mu(|A|+|B|)} \frac{|A-A|^{9/2}|B-B|^{9/2}}{|A|^{5/2-11\varepsilon'/2}|B|^{5/2-11\varepsilon'/2}2^{7j/2}} + \sum_{j \in J} 2^{2j} \cdot 2d\right) \\ &= O\left(|A|^{2/9+\varepsilon}|B|^{2/9+\varepsilon}|A-A||B-B| + |A|^2 + |B|^2\right). \end{aligned}$$

Combining this with (10) immediately implies the assertion of the theorem. \square

We next recall the statement of Theorem 1.4.

Theorem 1.4. *Let $A, B \subset \mathbb{R}$ be finite sets and let $f \in \mathbb{R}[x, y]$ be of degree at most d . Let $\tau_A, \tau_B \in \mathbb{R}[x]$ be of degree at most d , let $\deg \tau_B \geq 2$, and let τ_A^{-1} and τ_B^{-1} be respective*

one-sided inverses. Assume that $f(\tau_A(x), \tau_B(y))$ is indecomposable, that $A \subset \tau_A(\mathbb{R})$, and that $B \subset \tau_B(\mathbb{R})$. Then for any $\varepsilon > 0$ we have

$$|f(A, B)| = \Omega \left(\min \left\{ \frac{|A|^{16/9-\varepsilon} |B|^{16/9-\varepsilon}}{|\tau_A^{-1}(A) - \tau_A^{-1}(A)| |\tau_B^{-1}(B) - \tau_B^{-1}(B)|}, |A|^2, |B|^2 \right\} \right).$$

Unfortunately it is possible for $f(x, y)$ to be indecomposable and for $f(\tau_A(x), \tau_B(y))$ to be decomposable. For example, $f(x, y) = xy$ is clearly indecomposable. However, setting $\tau_A(x) = \tau_B(x) = x^2$ leads to $f(\tau_A(x), \tau_B(y)) = x^2 y^2$ which is decomposable. Characterizing exactly when this happens would lead to a stronger variant of Theorem 1.4.

Proof of Theorem 1.4. We use a variant of the proof of Theorem 1.3. In particular, we define $\Delta, \mu, D, D_j, k_j, E_f(A, B)$, and m_δ as in the proof of Theorem 1.3. Recall that every $\delta \in \Delta$ satisfies $m_\delta = O(|A| + |B|)$. That is, there exists a constant μ such that $k_{\mu(|A|+|B|)} = 0$. As in (9), we have

$$E_f(A, B) = \sum_{\delta \in \Delta} m_\delta^2 = \sum_{j=0}^{\log \mu(|A|+|B|)} \sum_{\substack{\delta \in \Delta \\ 2^j \leq m_\delta < 2^{j+1}}} m_\delta^2 < \sum_{j=0}^{\log \mu(|A|+|B|)} 2^{2j+2} k_{2^j}. \quad (14)$$

As in (10), we have

$$E_f(A, B) = \sum_{\delta \in \Delta} m_\delta^2 \geq \frac{(\sum_{\delta \in \Delta} m_\delta)^2}{D} = \frac{|A|^2 |B|^2}{D}. \quad (15)$$

For brevity, we write $A_\tau = \tau_A^{-1}(A) - \tau_A^{-1}(A)$ and $B_\tau = \tau_B^{-1}(B) - \tau_B^{-1}(B)$. For a fixed j , consider the set of curves

$$\Gamma_j = \left\{ \mathbf{V}(f(\tau_A(x + \alpha), \tau_B(y + \beta)) - \delta) : \alpha \in A_\tau, \beta \in B_\tau, \delta \in D_j \right\}.$$

Assume for contradiction that there exist $(\alpha, \beta, \delta), (\alpha', \beta', \delta') \in A_\tau \times B_\tau \times D_j$ and $r \in \mathbb{R}$ such that

$$f(\tau_A(x + \alpha), \tau_B(y + \beta)) - \delta = r \cdot (f(\tau_A(x + \alpha'), \tau_B(y + \beta')) - \delta').$$

For the maximum degree terms on both sides to have the same coefficients, we must have $r = 1$. We replace x with $x - \alpha'$ and y with $y - \beta'$ (that is, we translate the plane by $-\alpha'$ in the x -direction and by $-\beta'$ in the y -direction). Setting $\alpha_0 = \alpha - \alpha'$ and $\beta_0 = \beta - \beta'$ leads to

$$f(\tau_A(x + \alpha_0), \tau_B(y + \beta_0)) = f(\tau_A(x), \tau_B(y)) - \delta' + \delta. \quad (16)$$

One obvious solution to (16) is $\alpha_0 = \beta_0 = 0$ and $\delta = \delta'$. We assume for contradiction that this is not the case. As explained in the proof of Theorem 1.3, this implies that $f(\tau_A(x), \tau_B(y)) = h(x + cy)$ where $c = -\alpha_0/\beta_0$ and $h \in \mathbb{R}[z]$. Since $\deg \tau_B \geq 2$, we also have that $\deg h \geq 2$. This in turn implies that $f(\tau_A(x), \tau_B(y))$ is decomposable, contradicting the assumption.

To recap, we proved that Γ_j is a set of $|A_\tau| |B_\tau| k_j$ curves that are defined by distinct polynomials. Moreover, no polynomial is a constant multiple of another. While the polynomials are distinct, the curves of Γ_j may still have common components.

By Theorem 3.7, there are at most d^2 elements $\delta \in \Delta$ for which $f(\tau_A(x), \tau_B(y)) - \delta$ is reducible. For any $\alpha, \beta \in \mathbb{R}$, since $\mathbf{V}(f(\tau_A(x + \alpha), \tau_B(y + \beta)))$ is a translation of $\mathbf{V}(f(\tau_A(x), \tau_B(y)) - \delta)$, either both curves are reducible or both are irreducible. Thus, at most $d|A - A||B - B|$ curves of Γ_j are reducible.

If $k_j \geq 2d^2$, then after removing the reducible curves from Γ_j we still have $|\Gamma_j| = \Theta(|A_\tau||B_\tau|k_j)$. Assume that we are in this case, and let $\mathcal{P} = \tau_A^{-1}(A) \times \tau_B^{-1}(B) \subset \mathbb{R}^2$. Note that τ_A^{-1} and τ_B^{-1} are injective, so $\mathcal{P} = |A||B|$. By repeating the above derivation of (13), we obtain

$$I(\mathcal{P}, \Gamma_j) = O\left(|A|^{6/11+\varepsilon'}|B|^{6/11+\varepsilon'}|A_\tau|^{9/11}|B_\tau|^{9/11}k_j^{9/11}\right). \quad (17)$$

For every $\delta \in D_j$, there are at least j pairs $(a, b) \in A \times B$ that satisfy $f(a, b) = \delta$. For every $a' \in \tau_A^{-1}(A)$ and $b' \in \tau_B^{-1}(B)$, there exist $\alpha \in A_\tau$ and $\beta \in B_\tau$ such that $f(\tau_A(a' + \alpha), \tau_B(b' + \beta)) = f(a, b) = \delta$. Thus, every $\delta \in D_j$ whose curves are irreducible has at least $j|A||B|$ corresponding incidences in $\mathcal{P} \times \Gamma_j$. By summing this over every $\delta \in D_j$ with irreducible curves we get $I(\mathcal{P}, \Gamma_j) = \Omega(j|A||B|k_j)$. Combining this with (17) gives

$$j|A||B|k_j = O\left(|A|^{6/11+\varepsilon'}|B|^{6/11+\varepsilon'}|A_\tau|^{9/11}|B_\tau|^{9/11}k_j^{9/11}\right).$$

Rearranging leads to

$$k_j = O\left(\frac{|A_\tau|^{9/2}|B_\tau|^{9/2}}{|A|^{5/2-11\varepsilon'/2}|B|^{5/2-11\varepsilon'/2}j^{11/2}}\right).$$

We also recall the straightforward bound

$$k_j = O(|A||B|/j).$$

Let J be the set of integers $j \geq 1$ that satisfy $1 \leq k_j < 2d^2$. We set $\varepsilon = 11\varepsilon'/9$ and $\gamma = \frac{|A_\tau||B_\tau|}{|A|^{7/9-\varepsilon}|B|^{7/9-\varepsilon}}$. Combining (14) with both of the above bounds for k_j implies

$$\begin{aligned} E_f(A, B) &< \sum_{j=0}^{\log \mu(|A|+|B|)} 2^{2j+2}k_{2j} \leq 4 \sum_{j=0}^{\log \gamma} 2^{2j}k_{2j} + 4 \sum_{\log \gamma+1}^{\log \mu(|A|+|B|)} 2^{2j}k_{2j}. \\ &= O\left(\sum_{j=0}^{\log \gamma} |A||B|2^j + \sum_{j=\log \gamma+1}^{\log \mu(|A|+|B|)} \frac{|A_\tau|^{9/2}|B_\tau|^{9/2}}{|A|^{5/2-11\varepsilon'/2}|B|^{5/2-11\varepsilon'/2}2^{7j/2}} + \sum_{j \in J} 2^{2j} \cdot 2d^2\right) \\ &= O\left(|A|^{2/9+\varepsilon}|B|^{2/9+\varepsilon}|A_\tau||B_\tau| + |A|^2 + |B|^2\right). \end{aligned}$$

Combining this with (15) completes the proof. \square

6 Bipartite distinct distances

In this Section we prove Theorem 1.6. We begin by recalling the statement of this theorem.

Theorem 1.6. *Let \mathcal{P}_1 be a set of m points on a line ℓ in \mathbb{R}^2 and let \mathcal{P}_2 be set of n points in \mathbb{R}^2 . Then*

$$D(\mathcal{P}_1, \mathcal{P}_2) = \begin{cases} \Omega(m^{1/2}n^{1/2} \log^{-1/2} n), & \text{when } m = \Omega(n^{1/2}/\log^{1/3} n), \\ \Omega(n^{3/8}m^{3/4}), & \text{when } m = O(n^{1/2}/\log^{1/3} n) \text{ and } m = \Omega(n^{3/10}), \\ \Omega(n^{1/2}m^{1/3}), & \text{when } m = O(n^{3/10}). \end{cases}$$

Proof. For any $b \in \mathcal{P}_2$ and distance δ , at most two points of ℓ are at a distance of δ from b . This implies that $D(\mathcal{P}_1, \mathcal{P}_2) \geq D(\mathcal{P}_1, \{b\}) \geq m/2$ (for an arbitrary $b \in \mathcal{P}_2$). When $m = \Omega(n/\log n)$ this implies that $D(\mathcal{P}_1, \mathcal{P}_2) = \Omega(m^{1/2}n^{1/2}\log^{-1/2}n)$ and completes the proof. We may thus assume that $m = O(n/\log n)$.

If at least half of the points of \mathcal{P}_2 are contained in ℓ , then for an arbitrary $a \in \mathcal{P}_1$ we have $D(\mathcal{P}_1, \mathcal{P}_2) \geq D(\{a\}, \mathcal{P}_2 \cap \ell) = \Theta(n) = \Omega(n^{1/2}m^{1/2})$. We may thus assume that at most half of the points of \mathcal{P}_2 are in ℓ . Let $\mathcal{P}'_2 = \mathcal{P}_2 \setminus \ell$, and note that $|\mathcal{P}'_2| = \Theta(n)$.

We rotate the plane so that ℓ becomes the x -axis. If at least half of the points of \mathcal{P}'_2 have a negative y -coordinate then we reflect \mathbb{R}^2 about the x -axis. Let \mathcal{P}''_2 be the set of points of \mathcal{P}'_2 with a positive y -coordinate, and note that $|\mathcal{P}''_2| = \Theta(n)$. Since $D(\mathcal{P}_1, \mathcal{P}_2) \geq D(\mathcal{P}_1, \mathcal{P}''_2)$, it suffices to derive a lower bound on $D(\mathcal{P}_1, \mathcal{P}''_2)$. Abusing notation, in the remainder of the proof we will refer to \mathcal{P}''_2 as \mathcal{P}_2 and refer to the size of this set as n .

The rest of the proof is based on double counting $E_3(\mathcal{P}_1, \mathcal{P}_2)$. By (6) we have

$$E_3(\mathcal{P}_1, \mathcal{P}_2) = \Omega\left(\frac{m^3 n^3}{D(\mathcal{P}_1, \mathcal{P}_2)^2}\right). \quad (18)$$

As before, for every $\delta \in \Delta$ we denote by m_δ the number of ordered pairs $(a, b) \in \mathcal{P}^2$ such that $|ab| = \delta$. Recall that for fixed $\delta \in \Delta$ and $b \in \mathcal{P}_2$ at most two points $a \in \mathcal{P}_1$ satisfy $|ab| = \delta$. This implies that $m_\delta \leq 2n$ for every $\delta \in \Delta$. Let Δ_j be the set of distances $\delta \in \Delta$ that satisfy $m_\delta \geq j$, and set $k_j = |\Delta_j|$. A dyadic decomposition argument gives

$$E_3(\mathcal{P}_1, \mathcal{P}_2) = \sum_{j=0}^{\log(2n)} \sum_{\substack{\delta \in \Delta \\ 2^j \leq m_\delta < 2^{j+1}}} m_\delta^3 < \sum_{j=0}^{\log(2n)} \sum_{\substack{\delta \in \Delta \\ 2^j \leq m_\delta < 2^{j+1}}} (2^{j+1})^3 \leq 8 \sum_{j=0}^{\log(2n)} 2^{3j} k_{2^j}. \quad (19)$$

Studying rich distances. Fix a positive integer j . With (19) in mind, we now study how large $j^3 k_j$ can be. Consider the set of circles

$$\Gamma_j = \{\mathbf{V}((x - a_x)^2 + y^2 - \delta^2) \subset \mathbb{R}^2 : \delta \in \Delta_j, (a_x, 0) \in \mathcal{P}_1\}.$$

Note that Γ_j is a set of mk_j distinct circles. Since the centers of the circles are on the x -axis, two such circles intersect in at most one point with a positive y coordinate. Thus, the incidence graph of $\mathcal{P}_2 \times \Gamma_j$ contains no $K_{2,2}$. By Theorem 3.1

$$I(\mathcal{P}_2, \Gamma_j) = O\left(m^{2/3}n^{2/3}k_j^{2/3} + n + mk_j\right). \quad (20)$$

We divide the analysis into cases according to the term that dominates the bound of (20). If $m^{2/3}n^{2/3}k_j^{2/3} = O(mk_j)$ then $D(\mathcal{P}_1, \mathcal{P}_2) \geq k_j = \Omega(n^2/m) = \Omega(n^{1/2}m^{1/2})$. This completes the proof, so we may ignore this case. If $m^{2/3}n^{2/3}k_j^{2/3} = O(n)$ then $k_j = O(n^{1/2}/m)$. This in turn implies

$$j^3 k_j = O\left(j^3 n^{1/2}/m\right).$$

Finally, consider the case where $m^{2/3}n^{2/3}k_j^{2/3}$ dominates the bound of (20). For a distance $\delta \in \Delta_j$, every representation of δ as a distance between $a \in \mathcal{P}_1$ and $b \in \mathcal{P}_2$ corresponds to an incidence between b and the circle defined by a and δ . Since each of the k_j distances of Δ_j has at least j such representations, we get that $I(\mathcal{P}, \Gamma_j) \geq jk_j$. Combining this with (20) gives $jk_j = O(m^{2/3}n^{2/3}k_j^{2/3})$. Tidying up leads to

$$j^3 k_j = O(m^2 n^2).$$

By combining the two bounds for $j^3 k_j$ with (19), we obtain

$$\begin{aligned} E_3(\mathcal{P}_1, \mathcal{P}_2) &< 8 \sum_{j=0}^{\log(2n)} 2^{3j} k_{2^j} = O\left(\sum_{j=0}^{\log(2n)} \left(m^2 n^2 + \frac{2^{3j} n^{1/2}}{m}\right)\right) \\ &= O\left(m^2 n^2 \log n + \frac{n^{7/2}}{m}\right). \end{aligned} \quad (21)$$

When $m = \Omega(n^{1/2}/\log^{1/3} n)$, we get that $E_3(\mathcal{P}_1, \mathcal{P}_2) = O(m^2 n^2 \log n)$. Combining this with (18) implies the asserted bound

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega\left(n^{1/2} m^{1/2} \log^{-1/2} n\right).$$

The case of small m . We now consider the case where $m = O(n^{1/2}/\log^{1/3} n)$. We present two different arguments that lead to the two remaining bounds in the statement of the theorem. First, assume that there exists $\delta \in \Delta$ such that $m_\delta \geq n^{1/2} m^{4/3}$. Let \mathcal{C} be the set of circles of radius δ that are centered at points of \mathcal{P}_1 , and note that $I(\mathcal{P}_2, \mathcal{C}) \geq n^{1/2} m^{4/3}$. By the pigeonhole principle there exists a circle $\gamma \in \mathcal{C}$ that is incident to at least $n^{1/2} m^{1/3}$ points of \mathcal{P}_2 . For an arbitrary $a \in \mathcal{P}_1$ that is not the center of γ , we get that $D(\mathcal{P}_1, \mathcal{P}_2) \geq D(\{a\}, \mathcal{P}_2 \cap \gamma) \geq n^{1/2} m^{1/3}/2$.

Next, assume that every $\delta \in \Delta$ satisfies $m_\delta < n^{1/2} m^{4/3}$. Since every pair $\delta \in \Delta_j$ corresponds to at least j distinct ordered pairs of $\mathcal{P}_1 \times \mathcal{P}_2$, we have the straightforward bound $k_j \leq mn/j$. We use this bound for $j = O(m^{1/2} n^{1/2})$, and for larger values of j we use the bound $k_j = O(n^{1/2} m^{-1} + m^2 n^2 j^{-3})$ derived in the previous part of this proof. Repeating the argument in (19) for $E_2(\mathcal{P}_1, \mathcal{P}_2)$, we get that

$$\begin{aligned} E_2(\mathcal{P}_1, \mathcal{P}_2) &< 4 \sum_{j=0}^{\log n^{1/2} m^{4/3}} 2^{2j} k_{2^j} = 4 \sum_{j=0}^{\log \sqrt{mn}} 2^{2j} k_{2^j} + 4 \sum_{j=\log \sqrt{mn}}^{\log n^{1/2} m^{4/3}} 2^{2j} k_{2^j} \\ &= O\left(\sum_{j=0}^{\log \sqrt{mn}} mn 2^j + \sum_{j=\log \sqrt{mn}}^{\log n^{1/2} m^{4/3}} \left(2^{2j} n^{1/2} m^{-1} + m^2 n^2 2^{-j}\right)\right) = O\left(n^{3/2} m^{5/3}\right). \end{aligned}$$

By (6) we have

$$E_2(\mathcal{P}_1, \mathcal{P}_2) = \Omega\left(\frac{m^2 n^2}{D(\mathcal{P}_1, \mathcal{P}_2)}\right). \quad (22)$$

Combining the two above bounds for $E_2(\mathcal{P}_1, \mathcal{P}_2)$ gives $D(\mathcal{P}_1, \mathcal{P}_2) = \Omega(n^{1/2} m^{1/3})$. Thus, in either case we have that

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega\left(n^{1/2} m^{1/3}\right).$$

For our final bound, assume that $m = \Omega(n^{3/10})$ (and $m = O(n^{1/2}/\log^{1/3} n)$). If there exists $\delta \in \Delta$ such that $m_\delta \geq n^{9/16} m^{9/8}$, repeating the above argument involving the set of circles \mathcal{C} gives a circle γ that contains $\Omega(n^{9/16} m^{1/8})$ points of \mathcal{P}_2 . By Theorem 3.4, we have

$$\begin{aligned} D(\mathcal{P}_1, \mathcal{P}_2) &\geq D(\mathcal{P}_1, \mathcal{P}_2 \cap \gamma) = \Omega\left(\min\left\{|\mathcal{P}_2 \cap \gamma|^{2/3} m^{2/3}, |\mathcal{P}_2 \cap \gamma|^2, m^2\right\}\right) \\ &= \Omega\left(\min\left\{n^{3/8} m^{3/4}, n^{9/8} m^{1/4}, m^2\right\}\right) = \Omega\left(n^{3/8} m^{3/4}\right). \end{aligned}$$

On the other hand, if every $\delta \in \Delta$ satisfies $m_\delta < n^{9/16}m^{9/8}$ then

$$\begin{aligned} E_2(\mathcal{P}_1, \mathcal{P}_2) &< 4 \sum_{j=1}^{\log n^{9/16}m^{9/8}} 2^{2j} k_{2j} < 4 \sum_{j=1}^{\log \sqrt{mn}} 2^{2j} k_{2j} + 4 \sum_{j=\log \sqrt{mn}}^{\log n^{9/16}m^{9/8}} 2^{2j} k_{2j} \\ &= O \left(\sum_{j=1}^{\log \sqrt{mn}} mn 2^j + \sum_{j=\log \sqrt{mn}}^{\log n^{9/16}m^{9/8}} \left(2^{2j} n^{1/2} m^{-1} + m^2 n^2 2^{-j} \right) \right) = O \left(n^{13/8} m^{5/4} \right). \end{aligned}$$

Combining this with (22) implies $D(\mathcal{P}_1, \mathcal{P}_2) = \Omega \left(n^{3/8} m^{3/4} \right)$. Thus, in either case we get

$$D(\mathcal{P}_1, \mathcal{P}_2) = \Omega \left(n^{3/8} m^{3/4} \right).$$

□

7 Subsets with few repeating distances

In this section we prove Theorem 1.8 and another related result. We begin by recalling the statement of this theorem.

Theorem 1.6. *Let $\mathcal{P} \subset \mathbb{R}^2$ be a set of n points. Then there exists a subset $\mathcal{P}' \subset \mathcal{P}$ of size $\Omega(n^{22/63} \log^{-13/63} n)$ such that no distance is spanned by more than four pairs of points of \mathcal{P}' . Similarly, there exists a subset $\mathcal{P}' \subset \mathcal{P}$ of size $\Omega(n^{12/35} \log^{-9/35} n)$ such that no distance is spanned by more than two pairs of points of \mathcal{P}' .*

Proof. Let Δ_j be the set of distances that are spanned by at least j pairs of points of \mathcal{P} . Set $k_j = |\Delta_j|$. We begin the proof by studying how large k_j can be.

For a fixed j , consider the set of circles

$$\Gamma_j = \left\{ \mathbf{V} \left((x - a_x)^2 + (y - a_y)^2 - \delta^2 \right) : \delta \in \Delta_j, a \in \mathcal{P} \right\}.$$

Note that Γ_j is a set of nk_j distinct circles. By Theorem 3.2 and the trivial bound $k_j = O(n^2)$, we have

$$\begin{aligned} I(\mathcal{P}, \Gamma_j) &= O \left(n^{6/11} (nk_j)^{9/11} \log^{2/11} (nk_j) + n^{2/3} (nk_j)^{2/3} + n + nk_j \right) \\ &= O \left(n^{15/11} k_j^{9/11} \log^{2/11} n \right). \end{aligned} \quad (23)$$

For every distance $\delta \in \Delta_j$ there are at least j pairs of points in \mathcal{P} that span δ . Each such pair corresponds to two incidences in $\mathcal{P} \times \Gamma_j$, so

$$I(\mathcal{P}, \Gamma_j) \geq 2jk_j.$$

Combining this with (23) yields

$$k_j = O \left(\frac{n^{15/2} \log n}{j^{11/2}} \right). \quad (24)$$

Let Δ be the set of distances spanned by pairs of points of \mathcal{P} . A dyadic pigeonholing argument gives

$$\begin{aligned} \sum_{\delta \in \Delta} m_\delta^{11/2} &= \sum_{j=0}^{2 \log n} \sum_{\substack{\delta \in \Delta \\ 2^j \leq m_\delta < 2^{j+1}}} m_\delta^{11/2} < \sum_{j=0}^{2 \log n} k_{2^j} (2^{j+1})^{11/2} = O \left(\sum_{j=0}^{2 \log n} n^{15/2} \log n \right) \\ &= O \left(n^{15/2} \log^2 n \right). \end{aligned}$$

Recall from (4) that $\sum_{\delta \in \Delta} m_\delta^2 = O(n^3 \log n)$. By Hölder's inequality

$$\begin{aligned} E_5^*(\mathcal{P}) &\leq E_5(\mathcal{P}) = \sum_{\delta \in \Delta} m_\delta^5 = \sum_{\delta \in \Delta} m_\delta^{33/7} m_\delta^{2/7} \leq \left(\sum_{\delta \in \Delta} m_\delta^{11/2} \right)^{6/7} \left(\sum_{\delta \in \Delta} m_\delta^2 \right)^{1/7} \\ &= O \left(\left(n^{15/2} \log^2 n \right)^{6/7} \left(n^3 \log n \right)^{1/7} \right) = O \left(n^{48/7} \log^{13/7} n \right). \quad (25) \end{aligned}$$

A probabilistic argument. For $0 < p < 1$ that will be determined below, let \mathcal{P}'' be a set that is obtained by taking every point of \mathcal{P} with probability p . Note that³ $\mathbb{E}[|\mathcal{P}''|] = pn$, that $\mathbb{E}[E_5^*(\mathcal{P}'')] = p^{10} \cdot E_5^*(\mathcal{P})$, and that the expected number of isosceles triangles is $\mathbb{E}[t(\mathcal{P}'')] = p^3 \cdot t(\mathcal{P})$. By linearity of expectation, Theorem 3.5, and (25), we have that

$$\begin{aligned} \mathbb{E} \left[|\mathcal{P}''| - E_5^*(\mathcal{P}'') - t(\mathcal{P}'') \right] &= pn - p^{10} \cdot E_5^*(\mathcal{P}) - p^3 \cdot t(\mathcal{P}) \\ &\geq pn - cp^{10} n^{48/7} \log^{13/7} n - cp^3 n^{2.137}, \end{aligned}$$

for a sufficiently large constant c .

To asymptotically maximize the above expectation, we set $p = \left(2cn^{41/7} \log^{13/7} n \right)^{-1/9}$. This implies

$$\begin{aligned} \mathbb{E} \left[|\mathcal{P}''| - E_5^*(\mathcal{P}'') - t(\mathcal{P}'') \right] &\geq \frac{n^{22/63}}{\left(2c \log^{13/7} n \right)^{1/9}} - \frac{n^{22/63}}{2 \left(2c \log^{13/7} n \right)^{1/9}} - \frac{(c)^{2/3} n^{0.184}}{\left(2 \log^{13/7} n \right)^{1/3}} \\ &= \Omega \left(n^{22/63} \log^{-13/63} n \right). \end{aligned}$$

By the above, there exists $\mathcal{P}'' \subset \mathcal{P}$ such that $|\mathcal{P}''| - E_5^*(\mathcal{P}'') - t(\mathcal{P}'') = \Omega(n^{22/63} \log^{-13/63} n)$. We create $\mathcal{P}' \subset \mathcal{P}''$ by taking \mathcal{P}'' and arbitrarily removing one vertex from every isosceles triangle that is spanned by \mathcal{P}'' and from every 10-tuple that contributes to $E_5^*(\mathcal{P}'')$. By the above, $|\mathcal{P}'| = \Omega(n^{22/63} \log^{-13/63} n)$. Note that no distance is spanned by more than four pairs of points of \mathcal{P}' . This completes the proof of the first statement of the theorem.

A subset with no distance repeating more than twice. We now prove the second statement of the theorem. The proof is almost identical to the preceding one, except that

³We denote by $\mathbb{E}[X]$ the expectation of the random variable X , to distinguish it from the energy notation $E(X)$.

$E_5^*(\mathcal{P})$ is replaced with $E_3^*(\mathcal{P})$. By Hölder's inequality

$$\begin{aligned} E_3^*(\mathcal{P}) &\leq E_3(\mathcal{P}) = \sum_{\delta \in \Delta} m_\delta^3 = \sum_{\delta \in \Delta} m_\delta^{11/7} m_\delta^{10/7} \leq \left(\sum_{\delta \in \Delta} m_\delta^{11/2} \right)^{2/7} \left(\sum_{\delta \in \Delta} m_\delta^2 \right)^{5/7} \\ &= O\left(\left(n^{15/2} \log^2 n \right)^{2/7} \left(n^3 \log n \right)^{5/7} \right) = O\left(n^{30/7} \log^{9/7} n \right). \end{aligned} \quad (26)$$

We randomly generate \mathcal{P}'' as above. By linearity of expectation, Theorem 3.5, and (26), we have

$$\begin{aligned} \mathbb{E} \left[|\mathcal{P}''| - E_3^*(\mathcal{P}'') - t(\mathcal{P}'') \right] &= pn - p^6 \cdot E_3^*(\mathcal{P}) - p^3 \cdot t(\mathcal{P}) \\ &\geq pn - cp^6 n^{30/7} \log^{9/7} n - cp^3 n^{2.137}, \end{aligned}$$

for a sufficiently large constant c .

To asymptotically maximize the above expectation, we set $p = \left(2cn^{23/7} \log^{9/7} n \right)^{-1/5}$. This implies

$$\begin{aligned} \mathbb{E} \left[|\mathcal{P}''| - E_3^*(\mathcal{P}'') - t(\mathcal{P}'') \right] &\geq \frac{n^{12/35}}{\left(2c \log^{9/7} n \right)^{1/5}} - \frac{n^{12/35}}{2 \left(2c \log^{9/7} n \right)^{1/5}} - \frac{(c)^{2/5} n^{0.166}}{\left(2 \log^{9/7} n \right)^{3/5}} \\ &= \Omega\left(n^{12/35} \log^{-9/35} n \right). \end{aligned}$$

The final part of the argument is identical to the one in the previous case. \square

If Conjecture 2.1 holds, then the proof of Theorem 1.8 would imply significantly stronger results. For example, if $E_3(\mathcal{P}) = O(n^{4+\varepsilon})$ then we would get that there exists a subset $\mathcal{P}' \subset \mathcal{P}$ of size $\Omega(n^{2/5-\varepsilon})$ such that no distance is spanned more than twice by pairs of points of \mathcal{P}' .

There are many variants of Conjecture 1.7, and we can derive similar style results for most of those by using higher distance energies. We now present one such variant by Raz [20].

Theorem 7.1. *Let $\gamma \subset \mathbb{R}^d$ be an irreducible algebraic curve of degree k and let \mathcal{P} be a set of n points on γ . Then there exists a subset $\mathcal{P}' \subset \mathcal{P}$ of size $\Omega(n^{4/9})$ that does not span any distance more than once.*

Combining Theorem 7.1 with a work of Conlon et al. [5] leads to a family of results involving subsets that do not span simplices with repeating volumes. As an upper bound for Theorem 7.1, when taking a set of n equally spaced points on a line we get that every subset of size $\Omega(\sqrt{n})$ contains a repeating distance (this is the *Sidon set* problem). By using higher distance energies, we obtain the following variant.

Theorem 7.2. *Let $\gamma \subset \mathbb{R}^d$ be an irreducible algebraic curve of degree k and let \mathcal{P} be a set of n points on γ . Then for every integer $m \geq 2$ there exists a subset $\mathcal{P}' \subset \mathcal{P}$ such that $|\mathcal{P}'| = \Omega\left(n^{\frac{3m-2}{6m-3}} \right)$ and no distance is spanned by more than $m-1$ pairs of points of \mathcal{P}' .*

Theorem 7.2 implies that for every $\varepsilon > 0$ there exists $\mathcal{P}' \subset \mathcal{P}$ such that $|\mathcal{P}'| = \Omega(n^{0.5-\varepsilon})$ and every distance is spanned by $O(1)$ pairs of points of \mathcal{P}' .

Proof. By the proof of Theorem 4.1 in [20], either there exists a subset of $\Theta(n^{1/2})$ points of \mathcal{P} that do not span any distance more than once, or there exists a subset $\mathcal{T} \subset \mathcal{P}$ such that $|\mathcal{T}| = \Theta(n)$ and $E_2(\mathcal{T}) = O(|\mathcal{T}|^{8/3})$. In the former case we are done, so assume that the latter case holds. Set $n_{\mathcal{T}} = |\mathcal{T}| = \Theta(n)$.

Consider a point $p \in \mathcal{T}$ and a distance δ . The points of \mathbb{R}^d that are at a distance of δ from p form a hypersphere S centered at p . Note that $\gamma \not\subset S$, since $p \in \gamma \setminus S$. Since γ and S are irreducible varieties with no common components, we get that $\gamma \cap S$ is a finite point set. Theorem 3.6 implies that $|\gamma \cap S| = O(1)$. That is, p is at a distance of δ from $O(1)$ points of \mathcal{T} . This in turn implies that $t(\mathcal{T}) = O(n_{\mathcal{T}}^2)$.

For an integer $m \geq 2$, we consider the size of $E_m(\mathcal{T})$. Since $E_2(\mathcal{T}) = O(n_{\mathcal{T}}^{8/3})$, there are $O(n_{\mathcal{T}}^{8/3})$ quadruples $(a_1, a_2, b_1, b_2) \in \mathcal{T}$ such that $|a_1 b_1| = |a_2 b_2|$. Fix such a quadruple (a_1, a_2, b_1, b_2) , together with additional points $a_3, \dots, a_m \in \mathcal{T}$. By the previous paragraph, there are $O(1)$ choices of $b_3, \dots, b_m \in \mathcal{T}$ such that $|a_1 b_1| = |a_2 b_2| = \dots = |a_m b_m|$. This implies that

$$E_m^*(\mathcal{T}) \leq E_m(\mathcal{T}) = O\left(n_{\mathcal{T}}^{m+2/3}\right). \quad (27)$$

A probabilistic argument. For $0 < p < 1$ that will be determined below, let \mathcal{P}'' be a set that is obtained by taking every point of \mathcal{T} with probability p . Note that $\mathbb{E}[|\mathcal{T}|] = pn_{\mathcal{T}}$, that $\mathbb{E}[E_m^*(\mathcal{T})] = p^{2m} \cdot E_m^*(\mathcal{T})$, and that $\mathbb{E}[t(\mathcal{P}'')] = p^3 \cdot t(\mathcal{T})$. By linearity of expectation, the aforementioned bound $t(\mathcal{T}) = O(n_{\mathcal{T}}^2)$, and (27), we have that

$$\begin{aligned} \mathbb{E}\left[|\mathcal{P}''| - E_m^*(\mathcal{P}'') - t(\mathcal{P}'')\right] &= pn_{\mathcal{T}} - p^{2m} \cdot E_m^*(\mathcal{T}) - p^3 \cdot t(\mathcal{T}) \\ &\geq pn_{\mathcal{T}} - cp^{2m} n_{\mathcal{T}}^{m+2/3} - cp^3 n_{\mathcal{T}}^2, \end{aligned}$$

for a sufficiently large constant c (which may depend on d, k , and m).

To asymptotically maximize the above expectation, we set $p = \left(2cn_{\mathcal{T}}^{m-1/3}\right)^{-1/(2m-1)}$. This implies

$$\begin{aligned} \mathbb{E}\left[|\mathcal{P}''| - E_m^*(\mathcal{P}'') - t(\mathcal{P}'')\right] &\geq \frac{n_{\mathcal{T}}^{\frac{3m-2}{6m-3}}}{(2c)^{\frac{1}{2m-1}}} - \frac{n_{\mathcal{T}}^{\frac{3m-2}{6m-3}}}{2(2c)^{\frac{1}{2m-1}}} - \frac{c^{\frac{2m-4}{2m-1}} n_{\mathcal{T}}^{\frac{m-1}{2m-1}}}{2^{\frac{3}{2m-1}}} \\ &= \Omega\left(n_{\mathcal{T}}^{\frac{3m-2}{6m-3}}\right) = \Omega\left(n^{\frac{3m-2}{6m-3}}\right). \end{aligned}$$

By the above, there exists $\mathcal{P}'' \subset \mathcal{T}$ such that $|\mathcal{P}''| - E_m^*(\mathcal{P}'') - t(\mathcal{P}'') = \Omega\left(n^{\frac{3m-2}{6m-3}}\right)$. We create $\mathcal{P}' \subset \mathcal{P}''$ by taking \mathcal{P}'' and arbitrarily removing one vertex from every isosceles triangle that is spanned by \mathcal{P}'' and from every $2m$ -tuple that contributes to $E_m^*(\mathcal{P}'')$. By the above, $|\mathcal{P}'| = \Omega\left(n^{\frac{3m-2}{6m-3}}\right)$. No distance is spanned by more than $m-1$ pairs of points of \mathcal{P}' . \square

References

- [1] M. Ayad, Sur les polynômes $f(X, Y)$ tels que $K[f]$ est intégralement fermé dans $K[X, Y]$, *Acta Arith.* **105** (2002), 9–28.

- [2] F. A. Behrend, On sets of integers which contain no three terms in arithmetical progression, *Proc. Natl. Acad. Sci. U.S.A.* **32** (1946), 331.
- [3] A. Bruner and M. Sharir, Distinct distances between a collinear set and an arbitrary set of points, *Discrete Math.*, to appear.
- [4] M. Charalambides, A note on distinct distance subsets, *Journal of Geometry* **104** (2013), 439–442.
- [5] D. Conlon, J. Fox, W. Gasarch, D. G. Harris, D. Ulrich, and S. Zbarsky, Distinct volume subsets, *SIAM J. Discrete Math.* **29** (2015), 472–480.
- [6] G. Elekes and L. Rónyai, A combinatorial problem on polynomials and rational functions, *J. Combin. Theory Ser. A* **89** (2000), 1–20.
- [7] P. Erdős, On some metric and combinatorial geometric problems, *Discrete Math.* **60** (1986), 147–153.
- [8] P. Erdős, Nehány geometriai problémáról (in Hungarian), *Matematikai Lapok*, **8** (1957), 86–92.
- [9] P. Erdős, R. K. Guy, Distinct distances between lattice points, *Elemente Math.* **25** (1970) 121–123.
- [10] P. Erdős, On sets of distances of n points, *Amer. Math. Monthly* **53** (1946), 248–250.
- [11] P. Erdős and A. Gyárfás, A variant of the classical Ramsey problem, *Combinatorica* **17** (1997), 459–467.
- [12] G. Elekes, Circle grids and bipartite graphs of distances, *Combinatorica* **15** (1995), 167–174.
- [13] J. Fox, J. Pach, and A. Suk, More distinct distances under local conditions, *Combinatorica*, to appear.
- [14] L. Guth and N.H. Katz, On the Erdős distinct distances problem in the plane, *Annals Math.* **181** (2015), 155–190.
- [15] S. Jukna, *Extremal combinatorics: with applications in computer science*, Springer Science, 2011.
- [16] J. Milnor, On the Betti numbers of real varieties, *Proc. Amer. Math. Soc.* **15** (1964), 275–280.
- [17] J. Pach and G. Tardos, Isosceles triangles determined by a planar point set, *Graphs Combin.* **18** (2002), 769–779.
- [18] J. Pach and M. Sharir, Repeated angles in the plane and related problems, *J. Combinat. Theory Ser. A* **59** (1992), 12–22.
- [19] J. Pach and F. de Zeeuw, Distinct distances on algebraic curves in the plane, *Comb. Probab. Comp* **26** (2017): 99–117.
- [20] O. E. Raz, A note on distinct distances, arXiv:1603.00740.

- [21] O. E. Raz, M. Sharir, and J. Solymosi, Polynomials vanishing on grids: The Elekes-Rónyai problem revisited, *Amer. J. Math.* **138** (2016), 1029–1065.
- [22] C. Reid, *Hilbert: with an appreciation of Hilbert's mathematical work by Hermann Weyl*, Springer, 1970.
- [23] T. Schoen, New bounds in Balog-Szemerdi-Gowers theorem, *Combinatorica*, to appear.
- [24] T. Schoen and I. D. Shkredov, Higher moments of convolutions, *Journal of Number Theory* **133** (2013), 1693–1737.
- [25] T. Schoen and I. D. Shkredov, On sumsets of convex sets, *Comb. Probab. Comp.* **20** (2011), 793–798.
- [26] M. Sharir, A. Sheffer, and J. Solymosi, Distinct distances on two lines, *J. Combinat. Theory A* **120** (2013), 1732–1736.
- [27] M. Sharir and J. Zahl, Cutting algebraic curves into pseudo-segments and applications, *J. Combinat. Theory Ser. A*, to appear.
- [28] A. Sheffer, Distinct Distances: Open Problems and Current Bounds, arXiv:1406.1949.
- [29] C. Shen, Algebraic methods in sum-product phenomena, *Israel J. Math.* **188** (2012), 123–130.
- [30] J. Spencer, E. Szemerédi, and W. T. Trotter, Unit distances in the Euclidean plane, *Graph Theory and Combinatorics* (ed. B. Bollobás), Academic Press, 1984.
- [31] Y. Stein, The total reducibility order of a polynomial in two variables, *Israel J. Math.* **68** (1989), 109–122.
- [32] T. Tao and V. H. Vu, *Additive combinatorics*, Cambridge University Press, 2006.