Combinatorics, Probability and Computing (2020), **29**, pp. 650–663
doi:10.1017/S096354832000022X

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

A note on distinct distances†

Orit E. Raz

Einstein Institute of Mathematics, Hebrew University of Jerusalem, Givat Ram, Jerusalem 91904, Israel
Email: oritraz@mail.huji.ac.il

(Received 7 March 2016; revised 14 April 2020; accepted 20 July 2018; first published online 16 July 2020)

Abstract

We show that, for a constant-degree algebraic curve γ in $\mathbb{R}^D$, every set of n points on γ spans at least $\Omega(n^{4/3})$ distinct distances, unless γ is an *algebraic helix*, in the sense of Charalambides [2]. This improves the earlier bound $\Omega(n^{5/4})$ of Charalambides [2].

We also show that, for every set P of n points that lie on a d-dimensional constant-degree algebraic variety V in $\mathbb{R}^D$, there exists a subset $S \subset P$ of size at least $\Omega(n^{4/(9+12(d-1))})$, such that S spans $\binom{|S|}{2}$ distinct distances. This improves the earlier bound of $\Omega(n^{1/(3d)})$ of Conlon, Fox, Gasarch, Harris, Ulrich and Zbarsky [4].

Both results are consequences of a common technical tool.

2020 MSC Codes: 52C10, 05D10

1. Introduction

In this paper we study two mildly related problems that involve distinct distances in a point set. The unifying theme of these problems is that they are both based on a common technical tool (Theorem 2.6 below).

Distinct distances on a curve. The distinct distances problem of Erdős [8] asks for the minimum number of distinct distances spanned by any set P of n points in the plane. The $\sqrt{n} \times \sqrt{n}$ integer grid in the plane induces $\Theta(n/\sqrt{\log n})$ distinct distances, and Erdős conjectured that this number is asymptotically tight. In a recent breakthrough, Guth and Katz [10] proved that every set of n points in the plane spans at least $\Omega(n/\log n)$ distinct distances, which almost matches Erdős's upper bound.

An instance of the problem suggested by Purdy (see *e.g.* [1, Section 5.5]) asks for the minimum number of distinct distances spanned by pairs of $P_1 \times P_2$, where, for each $i = 1, 2$, P_i is a set of n points that lie on a line ℓ_i. Elekes and Rónyai [6] showed that, in contrast with the general case, this number is at least $\omega(n)$, unless the lines ℓ_1, ℓ_2 are either orthogonal or parallel to one another (where in the latter cases sets with only $O(n)$ distinct distances between them can then be constructed). Sharir, Sheffer and Solymosi [14] strengthened the result by showing that the number of distinct distances spanned by $P_1 \times P_2$ in the non-parallel, non-orthogonal case is at least $\Omega(n^{4/3})$. This result was later generalized by Pach and de Zeeuw [12] to the case where, for $i = 1, 2$, P_i is a set of points that lie on some irreducible constant-degree algebraic curve γ_i in the

†Work on this paper was supported by Grant 892/13 from the Israel Science Foundation, by the Israeli Centers of Research Excellence (I-CORE) program (Center No. 4/11), and by a Shulamit Aloni Fellowship from the Israeli Ministry of Science.

© The Author(s), 2020. Published by Cambridge University Press.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

plane. They showed that in this case the number of distinct distances spanned by $P_1 \times P_2$ is again at least $\Omega(n^{4/3})$, unless γ_1, γ_2 is either a pair of orthogonal lines, a pair of (possibly coinciding) parallel lines, or a pair of (possibly coinciding) concentric circles.

The first to consider the distinct distances problem (in the plane and in higher dimensions), with points restricted to an arbitrary constant-degree algebraic curve, was Charalambides [2]. He showed that if a set P of n points lies on a constant-degree algebraic curve γ in $\mathbb{R}^D$, for any $D \geqslant 2$, then the number of distinct distances spanned by P is at least $\Omega(n^{5/4})$, unless γ is an *algebraic helix*, defined as follows (see Charalambides [2, Definition 1.5 and Lemma 7.4]).

Definition 1.1. An *algebraic helix* is an irreducible algebraic curve $\gamma \subset \mathbb{R}^D$ which is either a straight line, or has a parametrization of the form

$$\gamma(t) = (a_1 \cos(\lambda_1 t), a_1 \sin(\lambda_1 t), \ldots, a_k \cos(\lambda_k t), a_k \sin(\lambda_k t)) \in \mathbb{R}^{2k}, \tag{1.1}$$

for some embedding of $\mathbb{R}^{2k}$ in $\mathbb{R}^D$, with $k \leqslant D/2$, and where all the ratios λ_j/λ_i are rational, for $i, j = 1, \ldots, k$.

In the plane an algebraic helix is just a line or a circle, so the result of Pach and de Zeeuw provides a generalization (to the bipartite case) and an improved bound of Charalambides' result for the case $D = 2$.

The first main result of this paper is to show that the bound $\Omega(n^{5/4})$ in [2] can be replaced by $\Omega(n^{4/3})$ also for $D > 2$, essentially by combining the general result of Raz, Sharir and de Zeeuw [13] with the analysis in [2]. More precisely, we have the following theorem.

Theorem 1.2. *Let γ be an irreducible constant-degree algebraic curve in $\mathbb{R}^D$, for any $D \geqslant 3$. Then every set P of n points on γ spans at least $\Omega(n^{4/3})$ distinct distances, with a constant of proportionality that depends only on the degree of γ (and is independent of D), unless γ is an algebraic helix.*

The proof of Theorem 1.2 is given in Section 3.

Subsets with all-distinct distances. A related problem of Erdős [8] asks for $h_d(n)$, the maximum t such that every set P of n points in $\mathbb{R}^d$ contains a subset S of t points such that all $\binom{t}{2}$ distances between the pairs of points in S are distinct. Erdős conjectured that $h_1(n) = (1 + o(1))\sqrt{n}$. The set $P = \{1, \ldots, n\}$ gives the upper bound $h_1(n) = O(\sqrt{n})$, while a lower bound of the form $h_1(n) = \Omega(\sqrt{n})$ follows from a result of Komlós, Sulyok and Szemerédi [11] (see Section 2.1 for a proof of this fact and more details). In two dimensions, utilizing an important estimate from the work of Guth and Katz [10], Charalambides [3] proved that $h_2(n) = \Omega((n/\log n)^{1/3})$. The $\sqrt{n} \times \sqrt{n}$ grid has $O(n/\sqrt{\log n})$ distinct distances and it follows that $h_2(n) = O(n^{1/2}/(\log n)^{1/4})$. In higher dimensions, Thiele [15] showed that $h_d(n) = \Omega(n^{1/(3d-2)})$, and this was recently improved by Conlon, Fox, Gasarch, Harris, Ulrich and Zbarsky [4] to $h_d(n) = \Omega(n^{1/(3d-3)}(\log n)^{1/3-2/(3d-3)})$.

Conlon *et al.* [4] investigated the more general function $h_{a,d}(n)$, the largest integer t such that any set of n points in $\mathbb{R}^d$ contains a subset of t points for which all the non-zero $(a-1)$-dimensional volumes of the $\binom{t}{a}$ subsets of size a are distinct. Note that $h_{2,d}(n) = h_d(n)$. They showed that $h_{a,d}(n) = \Omega(n^{1/((2a-1)d)})$ for all (constant) a and d. In addition, and as a tool for bounding $h_{a,d}(n)$, they introduced a more general notion $h_a(V, n)$, for $V \subset \mathbb{R}^D$ a d-dimensional[1] irreducible variety, which is the largest integer t such that any set of n points in V contains a subset of t points for which all the non-zero $(a-1)$-dimensional volumes of the $\binom{t}{a}$ subsets of

[1] By a d-dimensional variety $V \subset \mathbb{R}^D$ we mean here that $V = V_{\mathbb{C}} \cap \mathbb{R}^D$, where $V_{\mathbb{C}}$ is a d-dimensional algebraic variety in $\mathbb{C}^D$ which is the zero set of a system of exactly $D - d$ polynomials of real coefficients.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

size a are distinct. They then consider the quantity $h_{a,d,r}(n) := \min_V h_a(V, n)$, where the minimum ranges over all d-dimensional irreducible varieties V of degree r. It was proved in [4] that $h_{a,d,r} = \Omega(n^{1/((2a-1)d)})$, with a constant of proportionality that depends on a, d and r. For the special case $a = 2$, namely the case of distinct distances, the bound is $h_{2,d,r} = \Omega(n^{1/(3d)})$.

The second main result of this paper is the following improvement to the bound, as just stated, on the quantity $h_{2,d,r}(n)$.

Theorem 1.3. *For all integers $d, r \geqslant 1$, we have*

$$h_{2,d,r}(n) = \Omega(n^{4/(9+12(d-1))}),$$

where the constant of proportionality depends on d and r.

The proof of Theorem 1.3 is given in Section 4.

The common technical core. As already noted, there is a technical core behind Theorems 1.2 and 1.3, which is an application of a recent result of Raz, Sharir and de Zeeuw [13] (which is a strengthened version of the Elekes–Szabó theorem [7]). More precisely, for our purposes we need a somewhat stronger version of the result of [13], that we establish in Theorem 2.6, which is the main technical tool used for our proofs.

Roughly speaking, Theorem 2.6 says that, in the context of distances[2] between points that lie on some constant-degree irreducible algebraic curve, there are two dichotomic types of curves. The first type is of curves that locally behave like a line, in the sense that, by choosing the right parametrization, the distance between a pair of points $p = \gamma(t), q = \gamma(s)$ on the curve, is given as a function of the difference $s - t$ of the parameters representing p and q. An example for a curve of this kind is a circle, say, $x^2 + y^2 = 1$, in $\mathbb{R}^2$. Fixing some small arc of the circle, the distance between a pair of points $p = e^{it}$ and $q = e^{is}$ is determined by $|t - s|$ (namely $\|p - q\| = 2 \sin(|t - s|/2)$).

The second kind of curves are those that are 'very different' from a line. One property that distinguishes such curves from lines is given in Theorem 2.6(i). As a consequence of our results, one can specify other properties that distinguish curves γ of the latter kind from a line. For example, no triangle with vertices supported by γ can be moved along γ while preserving its edge lengths (*a posteriori* this follows from the results of Charalambides [2], but we had to deduce this fact independently in order to show that this indeed characterizes curves of the second kind).

The difference between Theorem 2.6 and the result in [13] (see Lemma 2.3 for the relevant statement), is that the latter result, adapted to our context, is restricted to the 'bipartite case', where one places a set of points P on some small arc of a curve γ, and another set Q on some other small arc on γ and consider distances between pairs of points $(p, q) \in P \times Q$. Theorem 2.6 allows one to consider all pairwise distances spanned by a set P.

We view the results in this paper as a new type of application of the Elekes–Szabó theorem. We believe our approach, as well as Theorem 2.6, will be useful in future applications of this theorem.

2. Preliminary results

2.1 A theorem of Komlós, Sulyok and Szemerédi

A set $A = \{a_1, \ldots, a_n\}$ of positive integers is called B_2 (see [9]) if the sums $a_i + a_j$ are all distinct. Let $\Phi(n)$ denote the maximal size of a B_2 set consisting of positive integers not exceeding n. Erdős and Turán [9] have shown that $\Phi(n) = \Theta(n^{1/2})$. Komlós, Sulyok and Szemerédi [11] have shown that every set of n positive integers (not necessarily $\{1, \ldots, n\}$) contains a subset of size at least $c\Phi(n)$ which is B_2, for some constant $c > 0$. Combining these results we have the following result.

[2] In fact, instead of distances one may consider any other constant-degree polynomial function over $(\mathbb{R}^2)^2$.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

Theorem 2.1 ([9, 11])**.** *Let X be a set of n positive integers. Then there exists a subset $Y \subset X$ of size $\Omega(n^{1/2})$ which is B_2.*

The result in [11] can be extended to sets of positive real numbers (not necessarily integers), a fact which is also mentioned in [4]. Since we use it in our analysis, and for completeness, we provide a proof of this fact; I would like to thank an anonymous referee for showing me this simple reduction.

Lemma 2.2. *Let X be a set of n positive real numbers. Then there exists a subset $Y \subset X$ of size $\Omega(n^{1/2})$ which is B_2.*

Proof. Consider the vector space V over $\mathbb{Q}$ spanned by the elements of X, and let $B \subset V$ form a basis for this vector space; clearly V is finite-dimensional. Write $B = \{b_1, \ldots, b_k\}$ and consider the map $b_i \mapsto t^{i-1}$, which embeds V (and thus X and $X + X$) into the linear vector space of polynomials in $\mathbb{Q}[t]$ of degree at most $k-1$. Concretely, each $v \in V$ is associated with a polynomial $p_v(t)$ such that $p_v(t) = p_{v'}(t)$ if and only if $v = v'$ and $p_{v+v'}(t) = p_v(t) + p_{v'}(t)$. Fixing some integer N sufficiently large and applying Theorem 2.1 to $\{p_x(N) \mid x \in X\}$ proves the lemma. □

2.2 Distances between points lying on an algebraic curve

The results in this section essentially follow from the analysis in Raz, Sharir and de Zeeuw [13]. The main new observation here is in our formulation of Lemma 2.4.[3]

Lemma 2.3 (Raz, Sharir and de Zeeuw [13])**.** *Let $F \in \mathbb{R}[x, y, z]$ be a constant-degree irreducible polynomial, and assume that none of the derivatives F_x, F_y, F_z is identically zero. Then one of the following two statements holds.*

(I) *For all $A, B \subset \mathbb{R}$, with $|A| = |B| = n$, we have*

$$|\{(a, a', b, b') \in A \times A \times B \times B \mid \exists c \in \mathbb{R}.\ F(a, b, c) = F(a', b', c) = 0\}| = O(n^{8/3}).$$

(II) *There exists a one-dimensional subvariety $Z_0 \subset Z(F)$, such that, for all $v \in Z(F) \setminus Z_0$, there exist open intervals $I_1, I_2, I_3 \subset \mathbb{R}$ and one-to-one real-analytic functions $\varphi_i \colon I_i \to \mathbb{R}$ with analytic inverses, for $i = 1, 2, 3$, such that $v \in I_1 \times I_2 \times I_3$ and for all $(x, y, z) \in I_1 \times I_2 \times I_3$*

$$(x, y, z) \in Z(F) \quad \text{if and only if} \quad \varphi_1(x) + \varphi_2(y) + \varphi_3(z) = 0$$

Let γ be a constant-degree irreducible algebraic curve in $\mathbb{R}^D$, and let

$$\alpha(t) = (t, \alpha_2(t), \ldots, \alpha_D(t)), \quad t \in (0, 1),$$

be a real-analytic parametrization of some (relatively open connected) arc $\alpha \subset \gamma$. Define

$$\rho(x, y) := (x - y)^2 + \sum_{i=2}^{D} (\alpha_i(x) - \alpha_i(y))^2,$$

[3] The results in [13] characterize bivariate functions with certain properties as having the form $f(x, y) = h(\varphi(x) + \psi(y))$, over some domains $x \in I$ and $y \in J$. Here it is important for us to have x and y ranging over the same domain I, shared by both.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

which is the squared distance between the two points on α parametrized by x and y. Let ρ_i denote the derivative of the function ρ with respect to its ith variable, for $i = 1, 2$. Consider the transformation $T\colon (0,1)^4 \to \mathbb{R}^4$, given by

$$T(x, x', y, y') := (\rho(x, y), \rho(x, y'), \rho(x', y), \rho(x', y')).$$

Let J_T stand for the Jacobian matrix of T.

Lemma 2.4. *Let γ, α, ρ and T be as above. Assume that* $\det J_T = 0$ *over* $(0,1)^4$. *Then there exists an open sub-interval $I \subset (0,1)$, such that, for every $x, y \in I$,*

$$\rho(x, y) = h(\varphi(x) - \varphi(y)),$$

where φ, h are some univariate invertible analytic functions defined over I and $J := \varphi(I) - \varphi(I)$, respectively.

For the proof we need the following technical lemma.

Lemma 2.5. *Let γ, α and ρ be as above. Then either γ is a line, or there exist $a', b' \in (0,1)$ and a finite subset $I_0 \subset (0,1)$ (of size depending on the degree of γ), such that*

$$\rho_2(x, b')\rho_2(a', y)\rho_1(a', b')\rho_1(x, b')\rho_1(a', y)\rho_2(a', b') \neq 0,$$

for every $x, y \in (0,1) \setminus I_0$.

Proof. Assume, without loss of generality, that D is minimal, that is, γ is not contained in any hyperplane in $\mathbb{R}^D$. If $D = 1$, then γ is a line, and we are done. Otherwise we have

$$\frac{1}{2}\rho_1(x, y) = x - y + \sum_{i=2}^{D} \alpha_i'(x)(\alpha_i(x) - \alpha_i(y))$$

and

$$-\frac{1}{2}\rho_2(x, y) = x - y + \sum_{i=2}^{D} \alpha_i'(y)(\alpha_i(x) - \alpha_i(y)).$$

Fix any $x = a' \in (0,1)$. Then the zero set $\{\alpha(y) \mid y \in (0,1),\ \rho_1(a', y) = 0\}$ is contained in the hyperplane H given by

$$a' - \xi_1 + \sum_{i=2}^{D} \alpha_i'(a')(\alpha_i(a') - \xi_i) = 0.$$

By our assumption, γ is not contained in H, and hence must intersect it in at most a constant number of points.

Similarly, the zero set

$$H' := \{\alpha(y) \mid y \in (0,1),\ \rho_2(a', y) = 0\}$$

is given by

$$a' - y + \sum_{i=2}^{D} \alpha_i'(y)(\alpha_i(a') - \alpha_i(y)) = 0. \tag{2.1}$$

Note that if (2.1) holds identically for every y in some open sub-interval of $J \subset (0,1)$, then $\rho(a', y) = c$, for some constant $c > 0$ and for every $y \in (0,1)$. This would imply that γ is contained in the $(d-1)$-dimensional sphere of radius c centred at $\alpha(a')$ (recall that γ is irreducible).

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

However, since we assume $\alpha(a') \in \gamma$, this leads to a contradiction. Thus H' does not contain any portion of α.

Note also that, since γ is an algebraic curve, the squared distance between two points in $\mathbb{R}^D$ is a polynomial function in the coordinates of $(\mathbb{R}^D)^2$, and using the implicit function theorem to obtain a polynomial expression for the derivative ρ_2, H' is contained in some constant-degree (depending on the degree of γ) irreducible algebraic variety V. Since H' does not contain any portion of α, it must intersect it in at most a constant number of points (that depends on the degree of γ).

Define $I(a') \subset (0,1)$ to be the finite set of parameters representing $\alpha \cap (H \cup H')$, if any exist.

Next, fix some $y = b' \in (0,1) \setminus I(a')$. Then

$$\rho_1(a', b')\rho_2(a', b') \neq 0,$$

and, applying a symmetric argument to the one given above, there exists a finite set $I(b') \subset (0,1)$ such that

$$\rho_1(x, b')\rho_2(x, b') \neq 0,$$

for every $x \in (0,1) \setminus I(b')$. Letting $I_0 := I(a') \cup I(b')$, this completes the proof of the lemma. □

Proof of Lemma 2.4. If γ is a line the assertion is trivial. We may therefore assume this is not the case. By assumption, we have

$$\rho_1(x,y)\rho_2(x,y')\rho_2(x',y)\rho_1(x',y') = \rho_2(x,y)\rho_1(x,y')\rho_1(x',y)\rho_2(x',y'), \tag{2.2}$$

for every $(x, x', y, y') \in (0,1)^4$.

By Lemma 2.5, there exist $a', b' \in (0,1)$ and an open interval $I \subset (0,1)$, such that, for every $(x,y) \in I^2$,

$$\rho_2(x,b')\rho_2(a',y)\rho_1(a',b')\rho_1(x,b')\rho_1(a',y)\rho_2(a',b') \neq 0 \tag{2.3}$$

and, in view of (2.2),

$$\rho_1(x,y)\rho_2(x,b')\rho_2(a',y)\rho_1(a',b') = \rho_2(x,y)\rho_1(x,b')\rho_1(a',y)\rho_2(a',b'), \tag{2.4}$$

for every $(x,y) \in I^2$.

Rearranging (2.4), we have

$$\frac{\rho_1(x,y)}{\rho_2(x,y)} = \frac{p(x)}{q(y)}, \tag{2.5}$$

where

$$p(x) := \frac{\rho_1(x,b')\rho_2(a',b')}{\rho_2(x,b')} \quad \text{and} \quad q(y) := \frac{\rho_2(a',y)\rho_1(a',b')}{\rho_1(a',y)},$$

and each of them is well-defined and non-zero on I. We consider the real-analytic primitives φ, ψ so that $\varphi'(x) = p(x)$ on I and $\psi'(y) = q(y)$ on I. Since, by construction, φ', ψ' are non-zero, the inverse mapping theorem implies that each of φ, ψ has an analytic inverse on its image.

We repeat the analysis in [13, Lemma 3.17] to show that the differential equation (2.5) imposes a restrictive form on $\rho(x,y)$. Express the function $\rho(x,y)$ in terms of new coordinates (ξ, η), given by

$$\xi = \varphi(x) + \psi(y), \quad \eta = \varphi(x) - \psi(y). \tag{2.6}$$

Since each of φ, ψ is an injection in I, the system (2.6) is invertible in I^2. Returning to the standard notation, denoting partial derivatives by variable subscripts, we have

$$\xi_x = \varphi'(x), \quad \xi_y = \psi'(y), \quad \eta_x = \varphi'(x) \quad \text{and} \quad \eta_y = -\psi'(y).$$

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

Using the chain rule, we obtain

$$\rho_1 = \rho_\xi \xi_x + \rho_\eta \eta_x = \varphi'(x)(\rho_\xi + \rho_\eta) = p(x)(\rho_\xi + \rho_\eta),$$
$$\rho_2 = \rho_\xi \xi_y + \rho_\eta \eta_y = \psi'(y)(\rho_\xi - \rho_\eta) = q(y)(\rho_\xi - \rho_\eta),$$

which gives

$$\frac{\rho_1(x,y)}{p(x)} - \frac{\rho_2(x,y)}{q(y)} \equiv 2\rho_\eta(x,y)$$

on I^2. Combining this with (2.5), we get

$$\rho_\eta(x,y) \equiv 0.$$

This means that ρ depends (locally in I^2) only on the variable ξ, so it has the form

$$\rho(x,y) = h(\varphi(x) + \psi(y)),$$

for a suitable analytic function h. The analyticity of h is an easy consequence of the analyticity of φ, ψ and ρ, and the fact that $\varphi'(x)$ and $\psi'(y)$ are non-zero, combined with repeated applications of the chain rule (see also [13]). Let

$$J := \{\varphi(x) + \psi(y) \mid (x,y) \in I^2\} \quad \text{and} \quad T := \{h(z) \mid z \in J\}.$$

We observe that

$$\rho_1(x,y) = h'(\varphi(x) + \psi(y)) \cdot \varphi'(x).$$

As argued above, we have $\rho_1(x,y) \neq 0$ for all $(x,y) \in I^2$, implying that $h'(\varphi(x) + \psi(y))$ is non-zero for $(x,y) \in I^2$. Therefore, by the inverse mapping theorem, $h\colon J \to T$ is invertible. In particular, the equation $h(c) = 0$ has a unique solution c_0 over J (c_0 exists since $\rho(x,x) = 0$ for each $x \in I$, implying that $0 \in T$).

Finally, since $\rho(x,x) = 0$, for every $x \in I$, we must have $\psi(x) \equiv -\varphi(x) + c_0$ over I. Replacing h with $\tilde{h}(z) = h(z + c_0)$, $z \in I$, the lemma follows (for $\tilde{h}$ and φ). □

We obtain the following analogue of Lemma 2.3.

Theorem 2.6. *Let γ, α and ρ be as above. Then one of the following holds.*

(1) For every finite set $A \subset (0,1)$ of size n,

$$|\{(x,x',y,y') \in A^4 \mid \rho(x,y) = \rho(x',y')\}| = O(n^{8/3}).$$

(2) There exists an open sub-interval $I \subset (0,1)$, such that, for every $x, y \in I$,

$$\rho(x,y) = h(\varphi(x) - \varphi(y)),$$

where φ, h are some univariate invertible analytic functions defined over I and $J := \varphi(I) - \varphi(I)$, respectively.

Proof. Suppose that $\gamma \subset \mathbb{R}^D$ is given by the system

$$g_i(x_1, \ldots, x_D) = 0, \quad i = 1, \ldots, (D-1),$$

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

where each g_i is an irreducible constant-degree D-variate real polynomial.[4] For every pair of points $\mathbf{x} = (x_1, \ldots, x_D), \mathbf{y} = (y_1, \ldots, y_D) \in \gamma$ of distance $\delta^{1/2}$, with $\delta \geqslant 0$, we have

$$\begin{aligned} g_i(\mathbf{x}) &= 0, \quad i = 1, \ldots, (D-1), \\ g_i(\mathbf{y}) &= 0, \quad i = 1, \ldots, (D-1), \\ \|\mathbf{x} - \mathbf{y}\|^2 - \delta &= (x_1 - y_1)^2 + \cdots + (x_D - y_D)^2 - \delta = 0. \end{aligned} \tag{2.7}$$

The system (2.7) defines a two-dimensional variety V in $\mathbb{R}^{2D+1}$. Indeed, given a point $\mathbf{x} \in \gamma$ and a parameter $\delta \geqslant 0$, there exists at most $O(1)$ points $\mathbf{y} \in \gamma$ such that $\|\mathbf{x} - \mathbf{y}\|^2 = \delta$ (note that it is impossible for γ to be contained in a sphere of radius $\delta^{1/2}$ centred at $\mathbf{x}$, since $\mathbf{x} \in \gamma$). So locally V can be described (analytically) by two parameters.

We apply a projection $\pi : \mathbb{R}^{2D+1} \to \mathbb{R}^3$ onto the coordinates x_1, y_1, δ of $\mathbb{R}^{2D+1}$. By applying (in advance) a generic isometry in $\mathbb{R}^D$, we may assume that the pre-image of each of the elements of $\pi(V)$ is finite. Indeed, applying this generic isometry, we may assume that γ is not contained in a hyperplane of the form $\{\mathbf{x} = (x_1, \ldots, x_D) \in \mathbb{R}^D \mid x_1 = a\}$, for some constant $a \in \mathbb{R}$. So γ intersects such a hyperplane in at most $O(1)$ points.

By construction, we have

$$Z_\alpha := \{(x, y, \rho(x, y)) \mid (x, y) \in (0, 1)\} \subset \pi(V).$$

Since Z_α is a graph of a bivariate analytic function (and hence forms a two-dimensional manifold), and it is contained in a two-dimensional algebraic variety (namely the Zariski closure of $\pi(V)$), it follows that $Z_\alpha \subset Z(F)$, where F is some irreducible trivariate real polynomial, and $Z(F)$ stands for the zero set of F. Note that $Z(F) \subset \pi(V) \cup Z_0'$, where Z_0' is an algebraic variety in $\mathbb{R}^3$ which is at most one-dimensional.

Finally, we apply Lemma 2.3 to the polynomial F. Assume first that property (I) of Lemma 2.3 holds. Then, for every $A \subset (0, 1)$, with $|A| = n$, we have

$$|\{(a, a', b, b') \in A^4 \mid \exists c \in \mathbb{R}.\ F(a, b, c) = F(a', b', c) = 0\}| = O(n^{8/3}). \tag{2.8}$$

By construction, $Z(F)$ identifies with the graph of the function ρ over $(0, 1)^2$. Thus (2.8) becomes

$$|\{(a, a', b, b') \in A^4 \mid \exists c \in \mathbb{R}.\ \rho(a, b) - c = \rho(a', b') - c = 0\}| = O(n^{8/3}),$$

or

$$|\{(a, a', b, b') \in A^4 \mid \rho(a, b) = \rho(a', b')\}| = O(n^{8/3}),$$

and so property (i) of Theorem 2.6 follows for this case.

Assume next that property (II) of Lemma 2.3 holds for the polynomial F. Since $Z_0 \cup Z_0'$ is at most one-dimensional, where Z_0 is the excluded set given in property (II), there exists $\nu = (x_0, y_0, \delta_0) \in N \subset Z_\alpha \setminus (Z_0 \cup Z_0')$, where N is some open neighbourhood of ν in Z_α. By property (II), there exist open intervals $I_1, I_2 \subset (0, 1)$ containing x_0, y_0, respectively, and some neighbourhood I_3 of δ_0, and one-to-one real-analytic functions $\varphi_i \colon I_i \to \mathbb{R}$ with analytic inverses, for $i = 1, 2, 3$, such that

$$(x, y, \delta) \in Z(F) \quad \text{if and only if} \quad \delta = \varphi_3^{-1}(\varphi_1(x) + \varphi_2(y)),$$

for every $(x, y, \delta) \in I_1 \times I_2 \times I_3$. Equivalently, assuming that $I_1 \times I_2 \times I_3 \subset N$ (by possibly shrinking them if needed),

$$\rho(x, y) = \delta \quad \text{if and only if} \quad \delta = \varphi_3^{-1}(\varphi_1(x) + \varphi_2(y)),$$

[4] Note that by a curve $\gamma \subset \mathbb{R}^D$, we mean that $\gamma = \gamma_{\mathbb{C}} \cap \mathbb{R}^D$, where $\gamma_{\mathbb{C}}$ is a one-dimensional (irreducible) algebraic curve in $\mathbb{C}^D$ which is the zero set of a system of exactly $D - 1$ polynomials of real coefficients.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

for every $(x, y, \delta) \in I_1 \times I_2 \times I_3$, or

$$\rho(x, y) = \varphi_3^{-1}(\varphi_1(x) + \varphi_2(y)),$$

for every $(x, y) \in I_1 \times I_2$.

Observe that if the last identity holds, we get

$$\det J_T = \rho_1(x, y)\rho_2(x, y')\rho_2(x', y)\rho_1(x', y') - \rho_2(x, y)\rho_1(x, y')\rho_1(x', y)\rho_2(x', y') = 0$$

for every $(x, y) \in I_1 \times I_1 \times I_2 \times I_2$. Since T is analytic, this implies that $\det J_T = 0$ identically over $(0, 1)^4$. Applying Lemma 2.4, we get that property (ii) holds for this case. This completes the proof of the lemma. □

3. Distinct distances spanned by point sets lying on an algebraic curve

3.1 Proof of Theorem 1.2

Let γ be an irreducible constant-degree algebraic curve in $\mathbb{R}^D$, and let P be a set of n points on γ. Since γ has constant degree, $\Omega(n)$ of the points of P lie on some connected arc $\alpha \subset \gamma$, that has a parametrization of the form $\alpha(t) = (\alpha_1(t), \alpha_2(t), \ldots, \alpha_D(t))$, for $t \in (0, 1)$, where the α_i are analytic. Thus we may assume, without loss of generality, that $P \subset \alpha$. By applying (in advance) an isometry of $\mathbb{R}^D$, if needed, we may further assume that $\alpha_1(t) = t$ in this parametrization. Letting $A := \{t \in (0, 1) \mid \alpha(t) \in P\}$, we get that $|A| = |P| = n$, and elements of A correspond injectively to points of P.

Apply Theorem 2.6 to γ, α, ρ, where $\rho\colon (0, 1)^2 \to \mathbb{R}$ is defined as above. Then one of the properties (i) or (ii) in Theorem 2.6 holds.

Suppose first that property (i) holds. Let Δ denote the set of (squared) distances spanned by P. We have

$$\begin{aligned}
\binom{n}{2} &= \sum_{\delta \in \Delta} |\{(x, y) \in A^2 \mid \rho(x, y) = \delta\}| \\
&\leqslant |\Delta|^{1/2} \left(\sum_{\delta \in \Delta} |\{(x, x', y, y') \in A^4 \mid \rho(x, y) = \rho(x', y') = \delta\}| \right)^{1/2} \\
&\leqslant |\Delta|^{1/2} (|\{(x, x', y, y') \in A^4 \mid \rho(x, y) = \rho(x', y')\}|)^{1/2} \\
&= O(|\Delta|^{1/2} n^{4/3}),
\end{aligned}$$

where the inequality on the second line is due to the Cauchy–Schwarz inequality, and for the last line we used property (i). Rearranging, we get

$$|\Delta| = \Omega(n^{4/3}),$$

which completes the proof for this case.

Suppose next that property (ii) holds. Then there exists an open interval $I \subset (0, 1)$, such that $\rho(x, y) = h(\varphi(x) - \varphi(y))$, for every $x, y \in I$, where φ, h are some univariate invertible analytic functions defined over I, $J := \varphi(I) - \varphi(I)$, respectively.

Consider the transformation $S\colon I^3 \to \mathbb{R}$ defined as

$$S_3(x, y, z) := (\rho(x, y), \rho(y, z), \rho(x, z)).$$

That is, S maps a triple (x, y, z), which is associated with a triple of points $p := \alpha(x)$, $q := \alpha(y)$, $r := \alpha(z)$ on α, to the squared lengths of the edges of the triangle pqr spanned by this triple. It can be easily checked that the restrictive form of ρ, given by property (ii) in Theorem 2.6, implies that $\det J_S = 0$, for every $(x, y, z) \in I^3$. Hence, for every $(a, b, c) = (\rho(x_0, y_0), \rho(y_0, z_0), \rho(x_0, z_0))$ in the image of S, the pre-image $S^{-1}(a, b, c)$ is at least one-dimensional, and can be interpreted as an (at

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

least) one-dimensional family of triangles pqr with vertices lying on γ and with (squared) edge lengths a, b, c.

By Charalambides [2], as reviewed for completeness in Section 3.2 below, this implies that γ is an algebraic helix (specifically, see Corollary 3.8 below).

3.2 Flexible frameworks and algebraic helices

We provide a short review of (only the) relevant definitions and results from Charalambides [2], which we need for the last step in our proof of Theorem 1.2.[5] We start with the definition of a *flexible framework* on a smooth manifold $M \subset \mathbb{R}^d$. Informally, this is a vertex embedding of a graph into M which can be moved continuously while preserving the length of each edge of the graph.

Definition 3.1 (flexible framework [2, Definition 2.19])**.** Let $G = (V, E)$ be a graph and let $M \subset \mathbb{R}^d$ be a smooth embedded submanifold of $\mathbb{R}^d$. Let $\phi\colon V \to M$ be an injective embedding of V on M. We say that (G, ϕ) is a *flexible framework* if there exists

$$\Phi\colon V \times (-\delta, \delta) \to M,$$

for some $\delta > 0$, such that $\Phi(\cdot, 0) = \phi$, there exists $t_0 \in (-\delta, \delta)$ such that $\Phi(\cdot, t_0) \neq \phi$, and, for each edge $\{u, v\} \in E$, the function

$$t \mapsto \|\Phi(u, t) - \Phi(v, t)\|^2$$

is constant. If $\Phi(v, \cdot)$ is smooth, for each $v \in V$, we say that (G, ϕ) is *smoothly flexible* on M.

Definition 3.2 (degenerate curve [2, Definition 2.23])**.** Let G be a graph. A smooth embedded curve $\alpha \subset \mathbb{R}^d$ is called *G-degenerate* if, for every embedding ϕ of G on α, the framework (G, ϕ) is smoothly flexible.

Let K_n denote the complete graph on n vertices, for $n \geqslant 3$; note that K_3 is simply a triangle. As it turns out, the assumption that every triangle may be moved along a curve α while preserving the edge lengths implies that, in fact, any vertex embedding of any complete graph K_n into α may be moved freely.

Lemma 3.3 (Charalambides [2, Lemma 7.1])**.** *Let $\alpha\colon I \to \mathbb{R}^d$ be a real-analytic parametrization. Suppose that α is K_3-degenerate. Then α is K_n-degenerate, for every $n \geqslant 1$.*

This allows Charalambides to prove the following fact.

Lemma 3.4 (Charalambides [2, Lemma 7.2])**.** *Let $\alpha\colon I \to \mathbb{R}^d$ be a real-analytic parametrization. Suppose (as we may, without loss of generality), that α is a unit-speed parametrization. Assume that α is K_3-degenerate. Then, for each $k \geqslant 1$, the norm $\|\alpha^{(k)}\|$ of the kth derivative of α is constant.*

One may then apply the following result of D'Angelo and Tyson [5].

Theorem 3.5 (D'Angelo and Tyson [5, Corollary 3.8])**.** *Let $\alpha\colon I \to \mathbb{R}^d$ be a real-analytic parametrization. Suppose that, for each $k \geqslant 1$, the norm $\|\alpha^{(k)}\|$ of the kth derivative of α is constant. Then there exist an orthogonal decomposition of the target space $\mathbb{R}^d = \mathbb{R}^{2m} \oplus \mathbb{R}^p$, an invertible*

[5]Note that some of the definitions and lemmas are given in [2] in more generality, *e.g.* for a more general *distance function*.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

skew-symmetric linear map A on R^{2m}*, vectors* $v, v_0 \in \mathbb{R}^{2m}$ *and* $w, w_0 \in \mathbb{R}^p$*, such that*

$$\alpha(t) = ((\exp(At) - I)A^{-1}v + v_0,\ \ wt + w_0).$$

Combining Lemma 3.4 and Theorem 3.5, we have the following.

Corollary 3.6. *Let* $\alpha : I \to \mathbb{R}^d$ *be a real-analytic parametrization. Suppose (without loss of generality), that* α *is a unit-speed parametrization. Assume that* α *is* K_3*-degenerate. Then, up to a rigid motion,*

$$\alpha(t) = (\exp(At)v, tw, 0) \in \mathbb{R}^{2k} \times \mathbb{R}^l \times \mathbb{R}^{2d-2k-l}, \tag{3.1}$$

where $v \in \mathbb{R}^{2k}$*,* $w \in \mathbb{R}^l$ *and* $2k + l \leqslant d$*.*

Following Charalambides [2, Definition 1.5], we call a curve of the form (3.1) a *generalized helix*.

Recall that every $2k \times 2k$ invertible skew-symmetric matrix B can be brought (see *e.g.* [16]) to a block diagonal form Σ by an orthogonal linear transformation U of determinant 1, where Σ is of the form

$$\Sigma = \begin{bmatrix} \begin{matrix} 0 & \lambda_1 \\ -\lambda_1 & 0 \end{matrix} & 0 & \cdots & 0 \\ 0 & \begin{matrix} 0 & \lambda_2 \\ -\lambda_2 & 0 \end{matrix} & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \begin{matrix} 0 & \lambda_k \\ -\lambda_k & 0 \end{matrix} \end{bmatrix}$$

for some real $\lambda_1, \ldots, \lambda_k$. That is, $\Sigma = U^{-1}BU$, or $B = U\Sigma U^{-1}$. Simple manipulations then show that $\exp(B) = U \exp(\Sigma)U^{-1}$, and

$$\exp(\Sigma) = \begin{bmatrix} \begin{matrix} \cos\lambda_1 & \sin\lambda_1 \\ -\sin\lambda_1 & \cos\lambda_1 \end{matrix} & 0 & \cdots & 0 \\ 0 & \begin{matrix} \cos\lambda_2 & \sin\lambda_2 \\ -\sin\lambda_2 & \cos\lambda_2 \end{matrix} & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & \begin{matrix} \cos\lambda_k & \sin\lambda_k \\ -\sin\lambda_k & \cos\lambda_k \end{matrix} \end{bmatrix}.$$

In other words, Corollary 3.6 asserts that, for a suitable linear transformation U of the coordinate frame, we have

$$\alpha(t) = (r_1 \cos\lambda_1 t, r_1 \sin\lambda_1 t, \ldots, r_k \cos\lambda_k t, r_k \sin\lambda_k t, tw, 0), \tag{3.2}$$

for some $r_1, \ldots, r_k \in \mathbb{R} \setminus \{0\}$, $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$.

In our set-up, we only want to consider *algebraic* curves. The following lemma is due to Charalambides [2].

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

Lemma 3.7 (Charalambides [2, Lemma 7.4])**.** *Let $d > 0$, $l, k \geqslant 0$ and $l + 2k = d$. Let $I \subset \mathbb{R}$ be an open interval. Suppose that $\alpha : I \to \mathbb{R}^d$ is given by*

$$\alpha(t) = (r_1 \cos \lambda_1 t, r_1 \sin \lambda_1 t, \ldots, r_k \cos \lambda_k t, r_k \sin \lambda_k t, tw)$$

for some $r_1, \ldots, r_k, \lambda_1, \ldots, \lambda_k \in \mathbb{R} \setminus \{0\}$ and $w \in \mathbb{R}^l$. Then α parametrizes an open subset of a real algebraic curve if and only if either $l = 0$ and for each $1 \leqslant i, j \leqslant k$ ratio r_i/r_j is rational, or, alternatively, $k = 0$.

(Note that the implicit assumption $2k + l = d$ in the lemma involves no loss of generality.)

That is, a generalized helix is a real algebraic curve if and only if either $k = 0$ and $l > 0$ (in other words, it is a straight line) or, alternatively, $k > 0$, $l = 0$ and has a parametrization of the form (1.1).

We thus conclude the following.

Corollary 3.8. *Let γ be an irreducible algebraic curve in $\mathbb{R}^d$. Let $\alpha : I \to \mathbb{R}^d$ be a real-analytic parametrization with $\alpha(I) \subset \gamma$. Suppose (as we may, without loss of generality), that α is a unit-speed parametrization. Assume that α is K_3-degenerate. Then γ is an algebraic helix.*

4. Distinct distance subsets

4.1 Distinct distance subsets on algebraic curves

For the proof of Theorem 1.3 we use the same inductive argument over the dimension d, used in [4] (the relevant theorem is cited here as Lemma 4.2). The new ingredient in our proof is the following bound on the quantity $h_{2,1,r}$, which is the case $d = 1$ in Theorem 1.3. This will form the base case for the induction, and will allow us to improve the general bound. One can view Theorem 4.1 as an extension of the result of Komlós, Sulyok and Szemerédi [11] (see Lemma 2.2) to general algebraic curves, instead of the real line.

Theorem 4.1. *For every $r \geqslant 1$, we have*

$$h_{2,1,r}(n) = \Omega(n^{4/9}),$$

where the constant of proportionality depends on r.

Proof. Let γ be a constant-degree irreducible algebraic curve in $\mathbb{R}^D$, and let P be a set of n points on γ. Since γ has constant degree, $\Omega(n)$ of the points of P lie in some connected arc $\alpha \subset \gamma$, that has a parametrization of the form $\alpha(t) = (t, \alpha_2(t), \ldots, \alpha_D(t))$, for $t \in (0, 1)$. Thus we may assume, without loss of generality, that $P \subset \alpha$. Let $A := \{t \in (0, 1) \mid \alpha(t) \in P\}$. Then $|A| = |P| = n$, and elements of A correspond injectively to points of P.

As in Section 2, we define

$$\rho(x, y) := (x - y)^2 + \sum_{i=2}^{D} (\alpha_i(x) - \alpha_i(y))^2,$$

which is the squared distance between the two points on α parametrized by x and y, and the transformation $T : (0, 1)^4 \to \mathbb{R}^4$, given by

$$T(x, x', y, y') := (\rho(x, y), \rho(x, y'), \rho(x', y), \rho(x', y')).$$

Assume first that $\det J_T = 0$ over $(0, 1)^4$. By Lemma 2.4, ρ can be written as $\rho(x, y) = h(\varphi(x) - \varphi(y))$, for some univariate invertible analytic functions h, φ. Applying Lemma 2.2 to the image set $\varphi(A)$, and using the invertibility of h and of φ, we conclude that, in this case, there exists a subset $A' \subset A$ of size $\Omega(n^{1/2})$, such that all the non-zero values $\rho(x, y)$, with $x, y \in A'$, are distinct.

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

Assume next that $\det J_T$ is not identically zero over $(0,1)^4$. By Theorem 2.6, we have $|Q| = O(n^{8/3})$, where

$$Q = Q(A) := \{(x, x', y, y') \in A^4 \mid \rho(x, y) = \rho(x', y')\}.$$

Let

$$S(A) := \{(x, y, y') \in A^3 \mid \rho(x, y) = \rho(x, y')\}.$$

Note that since γ is irreducible and constant-degree, for every $p \in \gamma$, a circle centred at p, for some point $p \in \gamma$, intersects γ in at most $O(1)$ points, and thus contains $O(1)$ points of P. Thus $|S(A)| = O(n^2)$.

We now apply a probabilistic argument similar to the one used in [3]. We take a random subset $A_0 \subset A$, such that each point x of A is chosen in A_0 independently, with probability π. Let $Q(A_0)$ and $S(A_0)$ be as above. We remove one point from each quadruple in $Q(A_0)$ and one point from each triple in $S(A_0)$, and let $A' \subset A_0$ be the resulting set. Then, by construction, the distances spanned by A' are pairwise distinct.

We claim that for some choice of A_0, the set A' is large enough. Indeed,

$$\mathbb{E}(|A'|) = \mathbb{E}(|A_0|) - \mathbb{E}(|Q(A_0)|) - \mathbb{E}(|S(A_0)|),$$

$$\mathbb{E}(|A'|) \geqslant \pi n - \pi^4 C_1 n^{8/3} - \pi^3 C_2 n^2,$$

for some constants $C_1, C_2 > 0$. Choosing $\pi \geqslant C/n^{5/9}$, with $C > 0$ sufficiently small, we get

$$\mathbb{E}(|A'|) \geqslant (C - C_1 C^4) n^{4/9} - C_2 C^3 n^{1/3} = \Omega(n^{4/9}).$$

This completes the proof of Theorem 4.1. □

4.2 Proof of Theorem 1.3

Let $H_{a,d,r}(t)$ be the inverse function of $h_{a,d,r}(n)$. More precisely, $H_{a,d,r}(t)$ is the minimum n such that, for any d-dimensional irreducible variety V of degree r, any set of n points lying on V contains a subset of t points for which all the non-zero $(a-1)$-dimensional volumes of the $\binom{t}{a}$ subsets of size a are distinct. Conlon *et al.* [4] proved the following relation.

Lemma 4.2 ([4, Theorem 4.2]). *For all integers $r, d \geqslant 1$ and $a \geqslant 2$, there exist positive integers $r' = r'(a, d, r)$ and $C = C(a, d, r)$, such that, for all integers $t \geqslant a$,*

$$H_{a,d,r}(t) \leqslant C H_{a,d-1,r'}(t) t^{2a-1}. \tag{4.1}$$

By Lemma 4.2, applied with $a = 2$, we have

$$H_{2,d,r}(t) \leqslant C H_{2,d-1,r'}(t) t^3.$$

Iterating this recurrence relation $d-1$ times, we get

$$H_{2,d,r}(t) \leqslant \widetilde{C} H_{2,1,r}(t) t^{3(d-1)},$$

for some constant $\widetilde{C} = \widetilde{C}(d, r)$.

By Theorem 4.1, we have

$$H_{2,1,r}(t) = O(t^{9/4}).$$

Combining these two inequalities, Theorem 1.3 follows. □

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press

Acknowledgement

I would like to thank Micha Sharir for helpful comments on a preliminary version of the paper. I would like to thank an anonymous referee for valuable comments and for explaining to me how to simplify the reduction in Lemma 2.2.

References

[1] Brass, P., Moser, W. and Pach, J. (2005) *Research Problems in Discrete Geometry*, Springer.
[2] Charalambides, M. (2014) Distinct distances on curves via rigidity. *Discrete Comput. Geom.* **51** 666–701.
[3] Charalambides, M. (2013) A note on distinct distance subsets, *J. Geom.* **104** 439–442.
[4] Conlon, D., Fox, J., Gasarch, W., Harris, D. G., Ulrich, D. and Zbarsky, S. (2015) Distinct volume subsets. *SIAM J. Discrete Math.* **29** 472–480.
[5] D'Angelo, J. P. and Tyson, J. T. (2009) Helical CR structures and sub-Riemannian geodesics. *Complex Var. Elliptic Equ.* **54** 205–221.
[6] Elekes, G. and Rónyai, L. (2000) A combinatorial problem on polynomials and rational functions. *J. Combin. Theory Ser. A* **89** 1–20.
[7] Elekes, G. and Szabó, E. (2012) How to find groups? (And how to use them in Erdős geometry?) *Combinatorica* **32** 537–571.
[8] Erdős, P. (1946) On sets of distances of *n* points. *Amer. Math. Monthly* **53** 248–250.
[9] Erdős, P. and Turán, P. (1941) On a problem of Sidon in additive number theory, and on some related problems. *J. London Math. Soc.* **1.4** 212–215.
[10] Guth, L. and Katz, N. H. (2015) On the Erdős distinct distances problem in the plane. *Ann. of Math.* **181** 155–190.
[11] Komlós, J., Sulyok, M. and Szemerédi, E. (1975) Linear problems in combinatorial number theory. *Acta Math. Acad. Sci. Hungar.* **26** 113–121.
[12] Pach, J. and de Zeeuw, F. (2017) Distinct distances on algebraic curves in the plane. *Combin. Probab. Comput.* **26** 99–117.
[13] Raz, O. E., Sharir, M. and de Zeeuw, F. (2016) Polynomials vanishing on Cartesian products: the Elekes–Szabó theorem revisited. *Duke Math. J.* **165.18** 3517–3566.
[14] Sharir, M., Sheffer, A. and Solymosi, J. (2013) Distinct distances on two lines. *J. Combin. Theory Ser. A* **120** 1732–1736.
[15] Thiele, T. (1995) Geometric selection problems and hypergraphs. PhD thesis, Institut für Mathematik, Freie Universität Berlin.
[16] Youla, D. C. (1961) A normal form for a matrix under the unitary congruence group. *Canad. J. Math.* **13** 694–704.

Cite this article: Raz OE (2020). A note on distinct distances. *Combinatorics, Probability and Computing* **29**, 650–663. https://doi.org/10.1017/S096354832000022X

https://doi.org/10.1017/S096354832000022X Published online by Cambridge University Press