Expansion of Trivariate Polynomials Using Proximity

Orit E. Raz
Department of Mathematics, Ben-Gurion University of the Negev, Be'er Sheva, Israel

Abstract

We extend the proximity technique of Solymosi and Zahl [9] to the setting of trivariate polynomials. In particular, we prove the following result: Let $f(x,y,z) = (x-y)^2+(\varphi(x)-z)^2$, where $\varphi(x) \in \mathbb{R}[x]$ has degree at least 3. Then, for every finite $A, B, C \subset \mathbb{R}$ each of size n, one has $|f(A,B,C)| = \Omega(n^{5/3-\varepsilon})$, for every $\varepsilon > 0$, where the constant of proportionality depends on ε and on $\deg(\varphi)$. This improves the previous exponent 3/2, due to Raz, Sharir, and De Zeeuw [7]. To the best of our knowledge, prior to this work no trivariate polynomial was known to have expansion exceeding $\Omega(n^{3/2})$.

2012 ACM Subject Classification Mathematics of computing → Combinatoric problems

Keywords and phrases Polynomial Expansion, Elekes–Rónyai theorem

Digital Object Identifier 10.4230/LIPIcs.SoCG.2026.86

1 Introduction

In many cases in combinatorial geometry, counting questions involving distances, slopes, collinearity, etc., can be reformulated as analogous counting questions involving grid points lying on certain algebraic varieties. A unified study of such problems began with a question of Elekes [1] about expansion of bivariate real polynomials $f(x,y)$. Specifically, he asked: For a bivariate polynomial $f \in \mathbb{R}[x,y]$ and given finite sets $A, B \subset \mathbb{R}$, how small can be the image set

$$f(A,B) = \{f(a,b) \mid a \in A, b \in B\}.$$

Elekes conjectured that the image of f on an $n \times n$ Cartesian product must be of cardinality superlinear in n, unless f has a very concrete *special form*. This was confirmed in 2000 by Elekes and Rónyai [2], who proved the following dichotomy: Either f is one of the forms

$$\begin{aligned} &f(x,y) = h(p(x)+q(y)) \quad \text{or} \\ &f(x,y) = h(p(x)q(y)), \end{aligned} \tag{1}$$

for some univariate real polynomials p, q, h, or, otherwise, for every finite $A, B \subset \mathbb{R}$, each of size n, we have

$$|f(A,B)| = \omega(n). \tag{2}$$

In [8], Raz, Sharir and Solymosi introduced a new proof of the Elekes–Rónyai theorem, which also yields improved bounds on the expansion of f. Roughly speaking, for a given $f \in \mathbb{R}[x,y]$ and two finite sets $A, B \subset \mathbb{R}$, they bounded the number of quadruples $((a,b),(a',b')) \in (A \times B)^2$ satisfying $f(a,b) = f(a',b')$ by reducing it to a point-curve incidence problem in the plane. Concretely, incidences between the point set $A \times A$ and the family of curves $\{\gamma_{b,b'} \mid (b,b') \in B \times B\}$, where $\gamma_{b,b'}$ is given by the equation

$$f(x,b) = f(y,b').$$

If these curves are distinct, known incidence bounds can be applied to obtain the desired estimate. However, it may happen that many of the curves coincide, in which case the

© Orit E. Raz;
licensed under Creative Commons License CC-BY 4.0

incidence bound breaks down. Raz, Sharir, and Solymosi showed that this "failure" occurs if and only if f has a special form, namely one of the forms described in (1). In the non-special case, their analysis yields the lower bound $\Omega(n^{4/3})$

Solymosi and Zahl [9] recently improved the expansion bound for f in the non-special case, establishing the lower bound $\Omega(n^{3/2})$. Their argument builds on the framework of [8], but applies the incidence bound to carefully selected subsets of points and curves. In particular, they restrict to points $(a, a') \in A \times A$ with a and a' sufficiently close, and, similarly, to curves $\gamma_{b,b'}$ with parameters $(b, b') \in B \times B$ with b and b' sufficiently close. This refinement, referred to as the *proximity method*, overcomes a loss incurred in the earlier argument from an application of the Cauchy–Schwarz inequality.

A 3-variate analogue of the Elekes–Rónyai theorem was studied in Raz, Sharir, and De Zeeuw [7]. The case of $k \geq 4$ variables is studied by Raz and Shem Tov in [4].

▶ **Theorem 1** ([7, 4]). *Let $k \geq 3$ and assume that $f \in \mathbb{R}[x_1, \ldots, x_k]$ depends non-trivially on each of its varaiables. Then one of the following holds:*

(i) *For every finite $A_1, \ldots, A_k \subset \mathbb{R}$, with $|A_i| = n$, for $i = 1, \ldots, k$, one has*

$$|f(A_1, \ldots, A_k)| = \Omega(n^{3/2}),$$

where the constant of proportionality depends only on $\deg(f)$ and on k.

(ii) *f is of one of the special forms*

$$f(x_1, \ldots, x_k) = h(p_1(x_1) + \cdots + p_k(x_k)) \tag{3}$$
$$f(x_1, \ldots, x_k) = h(p_1(x_1) \cdot \ldots \cdot p_k(x_k))$$

for some univariate real polynomials $p_1, \ldots, p_k, h$.

Similar to the bivariate case, the analysis for $k = 3$ also reduces to a point-curve incidence problem in the plane. Specifically, for a trivariate polynomial $f \in \mathbb{R}[x, y, z]$ and finite sets $A, B, C \subset \mathbb{R}$, define $D := f(A, B, C)$ and consider incidences between the point set $A \times D$ and the family of curves $\{\gamma_{b,c} \mid (b, c) \in B \times C\}$, where $\gamma_{b,c}$ is given by the equation

$$w = f(x, b, c).$$

In some respects, the trivariate case is simpler than the bivariate one. Here, the structure of f is more directly reflected in properties of the variety $w = f(x, y, z)$, whereas in the bivariate case one must analyze the more intricate variety $f(x, y) = f(z, w)$. Moreover, in the trivariate setting the argument avoids an application of the Cauchy–Schwarz inequality, therefore eliminating the loss in the estimate that arises in the bivariate case.

As mentioned above, the proximity method of Solymosi and Zahl [9] improves the bivariate bound precisely by overcoming this loss from the Cauchy–Schwarz step. For this reason, it is not immediately clear how their method could extend to the trivariate case.

In this paper, we show how proximity can in fact be used to obtain a stronger expansion bound for trivariate polynomials. In particular, we establish an improved bound for a concrete family of trivariate polynomials. Namely, we prove the following main result.

▶ **Theorem 2.** *Let*

$$f(x, y, z) = (x - y)^2 + (\varphi(x) - z)^2,$$

where $\varphi(x)$ is a univariate real polynomial of degree at least 3. Then, for every $\varepsilon > 0$ and any finite sets $A, B, C \subset \mathbb{R}$, each of size n, we have

$$|f(A, B, C)| = \Omega(n^{5/3-\varepsilon}),$$

where the constant of proportionality depends on $\deg \varphi$ and on ε.

This improves upon the previous bound of $\Omega(n^{3/2})$, which follows from Theorem 1. To the best of our knowledge, prior to this work no trivariate polynomial was known to have expansion exceeding $\Omega(n^{3/2})$.

We remark that our approach is more general and extends to other trivariate polynomials. A natural direction for future research is to determine the precise subfamily of polynomials $\mathcal{F} \subset \mathbb{R}[x,y,z]$ for which the method yields the improved lower bound $\Omega(n^{5/3-\varepsilon})$.

2 Preliminaries

2.1 Point-curve incidences in the plane

For a finite set of points $\mathcal{P} \subset \mathbb{R}^2$ and a finite set of planar curves $\mathcal{C}$, we let $I(\mathcal{P},\mathcal{C})$ denote the set of point-curve incidences; that is

$$I(\mathcal{P},\mathcal{C}) = \{(p,\gamma) \in \mathcal{P} \times \mathcal{C} \mid p \in \gamma\}.$$

The classical Szemerédi–Trotter theorem [10] asserts that, for the special case where $\mathcal{C}$ is a set of lines, and putting $m := |\mathcal{P}|$ and $n := |\mathcal{C}|$, one has

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

Since the Szemerédi–Trotter paper, numerous alternative proofs and related problems have been studied. For our result, we require an extension of Szemerédi–Trotter to point-curve incidence problems, established by Sharir and Zahl [6], in which the curves are algebraic and form an s-dimensional family. We now recall the relevant definitions from their work.

A bivariate polynomial $h \in \mathbb{R}[x,y]$ of degree at most D is a linear combination of the form $h(x,y) = \sum_{0\le i+j\le D} c_{ij}x^iy^j$. Note that the number of monomials x^iy^j such that $0 \le i+j \le D$ is $\binom{D+2}{2}$. In this sense, every point $\vec{c} \in \mathbb{R}^{\binom{D+2}{2}}$ (other than the all-zero vector) can be associated with a curve in $\mathbb{R}^2$, given by the zeroset of the bivariate polynomial whose coefficients are the entries of $\vec{c}$. If $\lambda \neq 0$, then f and λf have the same zero-set. Thus, the set of algebraic curves that can be defined by a polynomial of degree at most D in $\mathbb{R}^2$ can be identified with the points in the projective space $\mathbf{P}\mathbb{R}^{\binom{D+2}{2}}$.

Define an *s-dimensional family of plane curves of degree at most D* to be an algebraic variety $F \subset \mathbf{P}R^{\binom{D+2}{2}}$ such that $\dim(F) = s$. We will call the degree of the variety F the *complexity of the family*.

They then proved the following incidence bound:

▶ **Theorem 3** (Sharir–Zahl [6]). *Let Γ be a set of n algebraic plane curves that belong to an s-dimensional family of curves of degree at most D of constant complexity at most K, no two of which share a common irreducible component. Let P be a set of m points in the plane. Then for any $\varepsilon > 0$, the number of incidences $|I(P,\Gamma)|$ between the points of P and the curves of Γ satisfies*

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

where the constant of proportionality depends on s, K, D, and in the first term also on ε.

2.2 Symmetry of curves

Given a set $S \subset \mathbb{R}^2$ and a transformation $T : \mathbb{R}^2 \to \mathbb{R}^2$, we say that T *fixes* S if $T(S) = S$. We say that a transformation T is a *symmetry* of a plane algebraic curve C if T is an isometry of $\mathbb{R}^2$ and fixes C. Recall that an isometry of $\mathbb{R}^2$ is either a rotation, a translation, or a glide reflection (a reflection combined with a translation).

The following lemma is proved by Pach and De Zeeuw [3, Lemma 2.5].

▶ **Lemma 4** (Pach and De Zeeuw [3, Lemma 2.5])**.** *An irreducible plane algebraic curve of degree d has at most $4d$ symmetries, unless it is a line or a circle.*

2.3 Complete bipartite graphs

We introduce some notation and recall some properties in the spirit of Raz–Solymosi [5, Section 3]. For completeness we give all the details here. Let $\mathbf{p} = (p_1, \ldots, p_k), \mathbf{p}' = (p'_1, \ldots, p'_k) \in \mathbb{R}^2 \times \cdots \times \mathbb{R}^2 \cong \mathbb{R}^{2k}$ be two k-tuples of points in $\mathbb{R}^2$. Define

$$\Sigma_{\mathbf{p},\mathbf{p}'} = \{(q, q') \in \mathbb{R}^2 \times \mathbb{R}^2 \mid \|p_i - q\| = \|p'_i - q'\| \text{ for each } i = 1, \ldots, k\} \subset \mathbb{R}^2 \times \mathbb{R}^2.$$

Let $\sigma_{\mathbf{p},\mathbf{p}'}$ (respectively, $\sigma'_{\mathbf{p},\mathbf{p}'}$) denote the projection of $\Sigma_{\mathbf{p},\mathbf{p}'}$ to the first (respectively, last) copy of $\mathbb{R}^2$ in $\mathbb{R}^2 \times \mathbb{R}^2$.

▶ **Lemma 5.** *Let $\mathbf{p} = (p_1, p_2, p_3), \mathbf{p}' = (p'_1, p'_2, p'_3) \in (\mathbb{R}^2)^3$, and assume that p_1, p_2, p_3 are pairwise distinct. Then either*
(i) $\mathbf{p}$ and $\mathbf{p}'$ are congruent, or
(ii) $\Sigma_{\mathbf{p},\mathbf{p}'}$ is at most one-dimensional, and each of $\sigma_{\mathbf{p},\mathbf{p}'}$ and $\sigma'_{\mathbf{p},\mathbf{p}'}$ is contained in an algebraic curve of degree at most two.

Proof. By definition, for $(q, q') \in \Sigma_{\mathbf{p},\mathbf{p}'}$ we have

$$\|p_i - q\|^2 = \|p'_i - q'\|^2, \quad i = 1, 2, 3$$

or

$$\|p_i\|^2 - 2p_i \cdot q + \|q\|^2 = \|p'_i\|^2 - 2p'_i \cdot q' + \|q'\|^2, \quad i = 1, 2, 3.$$

Subtracting the 3rd equation from each of the first two equations, we get the system

$$\begin{aligned} \|p_1\|^2 - \|p_3\|^2 - 2(p_1 - p_3) \cdot q &= \|p'_1\|^2 - \|p'_3\|^2 - 2(p'_1 - p'_3) \cdot q' \\ \|p_2\|^2 - \|p_3\|^2 - 2(p_2 - p_3) \cdot q &= \|p'_2\|^2 - \|p'_3\|^2 - 2(p'_2 - p'_3) \cdot q' \\ \|p_3\|^2 - 2p_3 \cdot q + \|q\|^2 &= \|p'_3\|^2 - 2p'_3 \cdot q' + \|q'\|^2. \end{aligned} \tag{4}$$

The system can be rewritten as

$$\begin{aligned} \tfrac{1}{2}u - Aq &= \tfrac{1}{2}v - Bq', \\ \|p_3\|^2 - 2p_3 \cdot q + \|q\|^2 &= \|p'_3\|^2 - 2p'_3 \cdot q' + \|q'\|^2, \end{aligned}$$

where A (resp., B) is a 2×2 matrix whose ith row equals $p_i - p_3$ (resp., $p'_i - p'_3$), for $i = 1, 2$, and

$$u = \begin{pmatrix} \|p_1\|^2 - \|p_3\|^2 \\ \|p_2\|^2 - \|p_3\|^2 \end{pmatrix}, \quad v = \begin{pmatrix} \|p'_1\|^2 - \|p'_3\|^2 \\ \|p'_2\|^2 - \|p'_3\|^2 \end{pmatrix}$$

are vectors in $\mathbb{R}^2$.

Assume first that p'_1, p'_2, p'_3 are not collinear. So the matrix B is invertible and we have

$$q' = B^{-1}Aq + w,$$

for $w = \frac{1}{2}B^{-1}(v - u) \in \mathbb{R}^2$. Let $T(q) := B^{-1}Aq + w$. So $(q, q') \in \Sigma_{\mathbf{p},\mathbf{p}'}$ if and only if $q' = T(q)$. Plugging this in the 3rd equation in (4) we get

$$\|p_3\|^2 - 2p_3 \cdot q + \|q\|^2 = \|p'_3\|^2 - 2p'_3 \cdot T(q) + \|T(q)\|^2, \tag{5}$$

which defines $\sigma_{\mathbf{p},\mathbf{p}'}$. Note that this gives a conic section unless (5) is trivial, i.e., the zero equation. Note that for this to happen the quadratic part has to be zero. That is,

$$\langle q, q\rangle = \langle B^{-1}Aq, B^{-1}Aq\rangle$$

or

$$\langle q, \left(I - (B^{-1}A)^{tr}B^{-1}A\right) q\rangle = 0$$

This defines a trivial quadratic equation if and only if

$$I - (B^{-1}A)^{tr}B^{-1}A = 0$$

or

$$(B^{-1}A)^{tr} = (B^{-1}A)^{-1},$$

which means that T is an isometry of $\mathbb{R}^2$. This implies that $\mathbf{p}$ and $\mathbf{p}'$ are congruent. We conclude that $\sigma_{\mathbf{p},\mathbf{p}'}$ is either conic section given by (5) or $\mathbf{p}$ and $\mathbf{p}'$ are congruent, which completes the proof for the case that p'_1, p'_2, p'_3 are non-collinear.

By symmetry, same analysis applies also when p_1, p_2, p_3 are non-collinear. So we need to prove the lemma for the case that each of the triples p_1, p_2, p_3 and p'_1, p'_2, p'_3 is collinear. In this case we may assume without loss of generality that $p_3 = p'_3 = (0, 0)$, and $p_1 = (a, 0)$, $p'_1 = (a', 0)$, $p_2 = (b, 0)$, and $p'_2 = (b', 0)$. Note that our assumption that p_1, p_2, p_3 are pairwise distinct implies $b \neq a \neq 0$. Writing $q = (x, y)$ and $q' = (x', y')$, the system of equations defining $\Sigma_{\mathbf{p},\mathbf{p}'}$ in this case becomes

$$\begin{aligned}(x-a)^2 + y^2 &= (x'-a')^2 + (y')^2\\ (x-b)^2 + y^2 &= (x'-b')^2 + (y')^2\\ x^2 + y^2 &= (x')^2 + (y')^2\end{aligned}$$

or

$$\begin{aligned}-2ax + a^2 &= -2a'x' + (a')^2\\ -2bx + b^2 &= -2b'x' + (b')^2\\ x^2 + y^2 &= (x')^2 + (y')^2.\end{aligned}$$

Recalling our assumption that p_1, p_2, p_3 are distinct, we have $b \neq a \neq 0$. Thus the first two equations give

$$\begin{aligned}x &= (a'/a)x' - (a')^2/(2a) + a/2\\ x &= (b'/b)x' - (b')^2/(2b) + b/2.\end{aligned}$$

So we either get unique values for x, x' or otherwise $a'/a = b'/b$. In the former case both $\sigma_{\mathbf{p},\mathbf{p}'}$ and $\sigma'_{\mathbf{p},\mathbf{p}'}$ are lines parallel to the y-axis, and so in particular (ii) holds. In the latter case, write $a'/a = b'/b = t$. Assume first that $t \neq 0$. Then

$$\begin{aligned}x &= tx' + (a/2)(1-t^2)\\ x &= tx' + (b/2)(1-t^2),\end{aligned}$$

and so either $t = \pm 1$, in which case $\mathbf{p}$ and $\mathbf{p}'$ are congruent, or $a = b$ which is a contradiction to our assumption that p_1, p_2, p_3 are distinct. So we may assume that $t = 0$, which means

that $a' = b' = 0$. Assume $(q, q') \in \Sigma_{\mathbf{p},\mathbf{p}'}$ and write $q = (x, y)$ and $q' = (x', y')$. Let $r := (x')^2 + (y')^2$. So $q = (x, y)$ must satisfy the system

$$\begin{aligned}(x-a)^2 + y^2 &= r\\ (x-b)^2 + y^2 &= r\\ x^2 + y^2 &= r.\end{aligned}$$

However, recalling that $b \neq a \neq 0$, this system has no solutions. So $\Sigma_{\mathbf{p},\mathbf{p}'}$ is empty in this case. This completes the proof of the lemma. ◀

3 Proof of Theorem 2

Let f be as in the statement and let $A, B, C \subset \mathbb{R}$ be finite sets, each of size n. Set

$$D := f(A, B, C).$$

Our goal is to lower bound $|D|$.

Let

$$t = n^{3/2}/(s|D|^{1/2}),$$

where $s > 0$ is a sufficiently large constant, to be determined later. Consider the partition of each A, B, C into t consecutive segments, each containing at most $\lceil n/t \rceil$ elements. Let $\{A_i\}_{i=1}^t$, $\{B_i\}_{i=1}^t$, $\{C_i\}_{i=1}^t$ stand for the corresponding partitions. We write $a \sim a'$ if $a \neq a'$ and there exists some index $i \in [t]$ such that $a, a' \in A_i$. We write similarly $b \sim b'$ and $c \sim c'$ according to the partitions of B and C respectively. Define

$$Q := \{((a,b,c),(a',b',c')) \in (A \times B \times C)^2 \mid f(a,b,c) = f(a',b',c'),\ \ a \sim a',\ b \sim b',\ c \sim c'\}$$

We prove a lower bound on $|Q|$.

▶ **Proposition 6.** *We have*

$$|Q| = \Omega(sn^3), \tag{6}$$

where the constant of proportionality depends only on $\deg(\varphi)$.

Proof. For each $d \in D$ let

$$G_d := \{(a,b,c) \in A \times B \times C \mid f(a,b,c) = d\}.$$

This defines a partition $A \times B \times C = \bigcup_{d \in D} G_d$, and thus in particular

$$\sum_{d \in D} |G_d| = n^3.$$

Let

$$D' := \{d \in D \mid |G_d| \geq n^3/(10|D|)\}.$$

Note that

$$\begin{aligned} n^3 &= \sum_{d \in D} |G_d| \\ &= \sum_{d \in D'} |G_d| + \sum_{d \in D \setminus D'} |G_d| \\ &\leq \sum_{d \in D'} |G_d| + n^3/(10|D|) \cdot |D| \end{aligned}$$

and so

$$\sum_{d\in D'} |G_d| \geq (9/10)n^3. \tag{7}$$

Next, fix $d \in D'$. Note that for each $(i,j,k) \in [t]^3$, the set $A_i \times B_j \times C_k$ is contained in an axis-parallel box in $\mathbb{R}^3$. Moreover, the boundaries of those boxes lie in the union of $3t$ planes. Let $T_d \subset [t]^3$ denote the subset of 3-tuples of indices of boxes that intersect the surface $f(x,y,z) = d$. Note that $|T_d| = O(t^2)$, with constant of proportionality that depends only on $\deg(\varphi)$. Let $T'_d \subset T_d$ be those 3-tuples of indices for which $|G_d \cap (A_i \times B_j \times C_k)| \geq s$.

We have

$$\begin{aligned}
|G_d| &= \sum_{(i,j,k)\in T_d} |G_d \cap (A_i \times B_j \times C_k)| \\
&= \sum_{(i,j,k)\in T'_d} |G_d \cap (A_i \times B_j \times C_k)| + \sum_{(i,j,k)\in T_d \setminus T'_d} |G_d \cap (A_i \times B_j \times C_k)| \\
&\leq \sum_{(i,j,k)\in T'_d} |G_d \cap (A_i \times B_j \times C_k)| + s \cdot O(t^2) \\
&\leq \sum_{(i,j,k)\in T'_d} |G_d \cap (A_i \times B_j \times C_k)| + O(n^3/(s|D|)) \\
&\leq \sum_{(i,j,k)\in T'_d} |G_d \cap (A_i \times B_j \times C_k)| + |G_d|/2,
\end{aligned}$$

where the inequality on the fourth line is by our choice of t, and the inequality on the last line is because $d \in D'$ and assuming $s > 0$ is taken sufficiently large. Thus

$$\sum_{(i,j,k)\in T'_d} |G_d \cap (A_i \times B_j \times C_k)| \geq |G_d|/2. \tag{8}$$

Using $\binom{m}{2} \geq cm$ for $m \geq 2c+1$, we conclude that, for every $d \in D'$, one has

$$\begin{aligned}
\sum_{(i,j,k)\in T'_d} \left| \binom{G_d \cap (A_i \times B_j \times C_k)}{2} \right| &\geq \frac{s-1}{2} \sum_{(i,j,k)\in T'_d} |G_d \cap (A_i \times B_j \times C_k)| \\
&\geq \frac{s-1}{4}|G_d| \\
&\geq \frac{s}{5}|G_d|,
\end{aligned}$$

where the last inequality assumes $s \geq 5$. Thus we get

$$\begin{aligned}
|Q| &= \sum_{d\in D} \sum_{(i,j,k)\in[t]^3} \left| \binom{G_d \cap (A_i \times B_j \times C_k)}{2} \right| \\
&\geq \sum_{d\in D'} \sum_{(i,j,k)\in T'_d} \left| \binom{G_d \cap (A_i \times B_j \times C_k)}{2} \right| \\
&\geq \frac{s}{5} \sum_{d\in D'} |G_d| \\
&\geq (9/50)sn^3,
\end{aligned}$$

where the last inequality uses (7). This completes the proof of Proposition 6. ◀

Next we prove an upper bound on $|Q|$.

▶ **Proposition 7.** *For every $\varepsilon > 0$, we have*

$$|Q| \leq O_\varepsilon\left((s^2 n|D|)^{9/8+\varepsilon}\right) + 4\deg(\varphi)n^3.$$

Proof. We reduce the problem of upper bounding Q to a point-curve incidence problem in the plane. For this, we associate with each $((b,c),(b',c')) \in (B\times C)^2$ the planar curve (with coordinates (x,x')), denoted by $\gamma_{b,c,b',c'}$, given by the equation

$$f(x,b,c) = f(x',b',c').$$

Note that distinct choices of $((b,c),(b',c'))$ might give rise to the same curve, or to distinct curves that share an irreducible component. Let

$$\Gamma := \{\gamma \subset \gamma_{b,c,b',c'} \text{ is irreducible} \mid ((b,c),(b',c')) \in (B\times C)^2,\ b\sim b',\ c\sim c'\}.$$

Consider the set of parameters associated with the curves, that is, the set

$$\hat{\Gamma} := \{((b,c),(b',c')) \in (B\times C)^2 \mid\ b\sim b',\ c\sim c'\}.$$

Let $\Gamma_0 \subset \Gamma$ be the set of isolated points in Γ. We first observe that

$$|\{((a_0,b,c),(a_0',b',c')) \in Q \mid (a_0,a_0') \text{ isolated point of } \gamma_{b,c,b',c'} \text{ for } ((b,c),(b',c')) \in \hat{\Gamma}\}| = O(|\hat{\Gamma}|). \quad (9)$$

Indeed, for every $((b,c),(b',c')) \in \hat{\Gamma}$, the curve $\gamma_{b,c,b',c'}$ has $O(1)$ isolated points, each giving rise to exactly one element of Q. Thus (9) follows.

We are now interested in one-dimensional components in Γ. For each $\gamma \in \Gamma$ we define

$$m(\gamma) = \{((b,c),(b',c')) \in \hat{\Gamma} \mid \gamma \subset \gamma_{b,c,b',c'}\}$$

We show that there exists a finite subset $\Gamma_1 \subset \Gamma\setminus\Gamma_0$ such that for every $\gamma \in \Gamma\setminus(\Gamma_1\cup\Gamma_0)$ we have $|m(\gamma)| \leq 4$. Indeed, let $\gamma \in \Gamma\setminus\Gamma_0$ and suppose that $|m(\gamma)| \geq 5$. So there are three pairs $p_i := (b_i,c_i)$, $p_i' := (b_i',c_i')$, with $(p_i,p_i') \in m(\gamma)$ for $i = 1,2,3$, such that without loss of generality p_1,p_2,p_3 are distinct.

Let $\mathbf{p} = (p_1,p_2,p_3)$ and $\mathbf{p'} = (p_1',p_2',p_3')$ and recall the definition of $\Sigma_{\mathbf{p},\mathbf{p'}}$ from Section 2.3. By definition of $m(\gamma)$, this means that for every $(x,x') \in \gamma$ one has

$$((x,\varphi(x)),(x',\varphi(x'))) \in \Sigma_{\mathbf{p},\mathbf{p'}}.$$

By Lemma 5, either $\mathbf{p},\mathbf{p'}$ are congruent, or $\sigma_{\mathbf{p},\mathbf{p'}}$ is a conic section. In the latter case this implies that $\{(t,\varphi(t)) \mid t\in\mathbb{R}\}$ is a conic section, which is a contradiction because $\deg(\varphi) \geq 3$ and this curve is irreducible. Thus necessarily $\mathbf{p}$ and $\mathbf{p'}$ are congruent. Thus, there exists an isometry of $\mathbb{R}^2$, R, such that

$$(x',\varphi(x')) = R(x,\varphi(x)),\ \text{for every } (x,x') \in \gamma.$$

Since γ is infinite, this implies that R maps $(t,\varphi(t))$ to itself. By Lemma 4, we have that R is one of at most $4\deg(\varphi)$ possible isometries, which in turn determines the corresponding curve γ up to at most $4\deg(\varphi)$ possibilities. We conclude that

$$|\Gamma_1| \leq 4\deg(\varphi)$$

and

$$\text{for every } \gamma \in \Gamma\setminus(\Gamma_1\cup\Gamma_0) \text{ we have } |m(\gamma)| \leq 4. \quad (10)$$

Next, let

$$\hat{\Gamma}_1 := \{((b,c),(b',c')) \in \hat{\Gamma} \mid \text{there exists } \gamma \in \Gamma_1 \setminus \Gamma_0 \text{ such that } \gamma \subset \gamma_{b,c,b',c'}\}.$$

We claim that

$$|\{((a,b,c),(a',b',c')) \in Q \mid ((b,c),(b',c')) \in \hat{\Gamma}_1\}| \leq 4\deg(\varphi)n^3. \tag{11}$$

Indeed, by what has just been argued, there exists an isometry R of $\mathbb{R}^2$, one of at most $4\deg(\varphi)$ possibilities, such that $(b',c') = R(b,c)$ and $(a',\varphi(a')) = R(a,\varphi(a))$. In other words, (a',b',c') is determined by (a,b,c), up to at most $4\deg(\varphi)$ possibilities. Thus (11) follows.

Finally, let

$$P = \{(a,a') \in A \times A \mid a \sim a'\},$$

and apply Theorem 3 to bound to $|I(P, \Gamma \setminus \Gamma_1)|$. Note that

$$|P| = \Theta\left(\binom{n/t}{2}t\right) = \Theta(n^2/t) = \Theta(sn^{1/2}|D|^{1/2})$$

and

$$\begin{aligned}|\Gamma \setminus (\Gamma_0 + \Gamma_1)| \leq \deg(f)|\hat{\Gamma}| &= \Theta\left(\binom{n/t}{2}\binom{n/t}{2}t^2\right)\\ &= \Theta(n^4/t^2)\\ &= \Theta(s^2 n|D|).\end{aligned}$$

We get

$$\begin{aligned}|Q| &\leq 4|I(P,\Gamma \setminus (\Gamma_0 \cup \Gamma_1))| + 4\deg(\varphi)n^3 + O(|\hat{\Gamma}|),\\ &= O_\varepsilon\left((sn^{1/2}|D|^{1/2})^{9/4+2\varepsilon}\right) + 4\deg(\varphi)n^3.\end{aligned}$$

This proves Proposition 7. ◀

Finally, combining the inequalities from Proposition 6 and Proposition 7, we conclude that

$$sn^3 \leq |Q| = O_\varepsilon\left((n|D|)^{9/8+\varepsilon}\right) + 4\deg(\varphi)n^3.$$

Choosing $s > 8\deg(\varphi)$ and rearranging, we get

$$|D| = \Omega_\varepsilon(n^{5/3-\varepsilon'}).$$

This completes the proof of Theorem 2. □

References

1. G. Elekes. On linear combinatorics, I. *Combinatorica*, 17(4):447–458, 1997.
2. G. Elekes and L. Rónyai. A combinatorial problem on polynomials and rational functions. *J. Combin. Theory Ser. A*, 89(1):1–20, 2000. doi:10.1006/JCTA.1999.2976.
3. J. Pach and F. de Zeeuw. Distinct Distances on Algebraic Curves in the Plane. *Combinat., Probab. Comput.*, 26(1):99–117, 2017. doi:10.1017/S0963548316000225.
4. O. E. Raz and Z. Shem-Tov. Expanding polynomials: A genralization of the Eleke–Rónyai theorem to d variables. *Combinatorica*, 40(5):721–748, 2020. doi:10.1007/S00493-020-4041-0.

5 O. E. Raz and J. Solymosi. Dense graphs have rigid parts. *Discrete Cumput. Geom.*, 69:1079–1094, 2023. doi:10.1007/S00454-022-00477-7.

6 M. Sharir and J. Zahl. Cutting algebraic curves into pseudo-segments and applications. *J. Combin. Theory, Ser. A*, 150:1–35, 2017. doi:10.1016/J.JCTA.2017.02.006.

7 O. E. Raz M. Sharir and F. de Zeeuw. The Elekes–Szabó theorem in four dimensions. *Israel J. Math.*, 227:663–690, 2018.

8 O. E. Raz M. Sharir and J. Solymosi. Polynomials vanishing on grids: The Elekes-Rònyai problem revisited. *Amer. J. Math.*, 138(4):1029–1065, 2016.

9 J. Solymosi and J. Zahl. Improved Elekes–Szabó type estimates using proximity. *J. Comb. Theory, Ser. A*, 201:105813, 2024. doi:10.1016/J.JCTA.2023.105813.

10 E. Szemerédi and W. T Trotter. A Combinatorial Distinction Between the Euclidean and Projective Planes. *European Journal of Combinatorics*, 4:385–394, 1983. doi:10.1016/S0195-6698(83)80036-5.