Polynomials Vanishing on Cartesian Products: The Elekes-Szabó Theorem Revisited*

Orit E. Raz[1], Micha Sharir[1], and Frank de Zeeuw[2]

1 **School of Computer Science, Tel Aviv University**
Tel Aviv 69978, Israel
{oritraz,michas}@post.tau.ac.il

2 **École Polytechnique Fédérale de Lausanne**
Lausanne, Switzerland
fdezeeuw@gmail.com

Abstract

Let $F \in \mathbb{C}[x, y, z]$ be a constant-degree polynomial, and let $A, B, C \subset \mathbb{C}$ with $|A| = |B| = |C| = n$. We show that F vanishes on at most $O(n^{11/6})$ points of the Cartesian product $A \times B \times C$ (where the constant of proportionality depends polynomially on the degree of F), unless F has a special group-related form. This improves a theorem of Elekes and Szabó [2], and generalizes a result of Raz, Sharir, and Solymosi [9]. The same statement holds over $\mathbb{R}$. When A, B, C have different sizes, a similar statement holds, with a more involved bound replacing $O(n^{11/6})$.

This result provides a unified tool for improving bounds in various Erdős-type problems in combinatorial geometry, and we discuss several applications of this kind.

1998 ACM Subject Classification G.2 Discrete Mathematics

Keywords and phrases Combinatorial geometry, incidences, polynomials

Digital Object Identifier 10.4230/LIPIcs.SOCG.2015.522

1 Introduction

In 2000, Elekes and Rónyai [1] proved the following result. Given a constant-degree real polynomial $f(x, y)$, and finite sets $A, B, C \subset \mathbb{R}$ each of size n, we have

$$\left| \left\{ (x, y, z) \in \mathbb{R}^3 \mid z - f(x, y) = 0 \right\} \cap (A \times B \times C) \right| = o(n^2),$$

unless f has one of the forms $f(x, y) = g(h(x) + k(y))$ or $f(x, y) = g(h(x)k(y))$, with univariate real polynomials g, h, k. Recently, Raz, Sharir, and Solymosi [9] extended an argument introduced in [11] to improve the upper bound (when f does not have one of the special forms) to $O(n^{11/6})$ (where the constant of proportionality depends polynomially on the degree of f).

Elekes and Szabó [2] generalized the result of [1] to any complex algebraic surface

$$Z(F) := \left\{ (x, y, z) \in \mathbb{C}^3 \mid F(x, y, z) = 0 \right\},$$

* Work on this paper by Orit E. Raz and Micha Sharir was supported by Grant 892/13 from the Israel Science Foundation and by the Israeli Centers of Research Excellence (I-CORE) program (Center No. 4/11). Work by Micha Sharir was also supported by Grant 2012/229 from the U.S.–Israel Binational Science Foundation and by the Hermann Minkowski-MINERVA Center for Geometry at Tel Aviv University. Work on this paper by Frank de Zeeuw was partially supported by Swiss National Science Foundation Grants 200020-144531 and 200021-137574.

where F is an irreducible polynomial in $\mathbb{C}[x,y,z]$. They showed that if $A,B,C \subset \mathbb{C}$ are finite sets, each of size n, then $|Z(F) \cap (A \times B \times C)|$ is subquadratic in n, unless F has a certain exceptional form. The exceptional form of F in this statement is harder to describe (see (ii) in Theorem 1.1 below), but is related to an underlying group structure that describes the dependencies of F on each of the variables (similar to the addition or multiplication that appear in the exceptional forms of $F(x,y,z) = z - f(x,y)$ in [1, 9]). The upper bound that Elekes and Szabó obtained, when F is not exceptional, was $|Z(F) \cap (A \times B \times C)| = O(n^{2-\eta})$, for a constant $\eta > 0$ that depends on the degree of F, and which they did not make explicit.

Our results. In this paper, we show that the theorem of Elekes and Szabó holds for $\eta = 1/6$, thereby extending the strengthened result of [9] to the generalized setup in [2]. More precisely, our main result is the following theorem.

▶ **Theorem 1.1** (Balanced case). *Let $F \in \mathbb{C}[x,y,z]$ be an irreducible polynomial of degree d, and assume that none of the derivatives $\partial F/\partial x$, $\partial F/\partial y$, $\partial F/\partial z$ is identically zero. Then one of the following two statements holds.*

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

$$|Z(F) \cap (A \times B \times C)| = O(d^{13/2} n^{11/6}).$$

(ii) *There exists a one-dimensional subvariety $Z_0 \subset Z(F)$, such that for every $v \in Z(F) \setminus Z_0$, there exist open sets $D_1, D_2, D_3 \subset \mathbb{C}$ and analytic functions $\varphi_i : D_i \to \mathbb{C}$ for $i = 1,2,3$, such that $v \in D_1 \times D_2 \times D_3$, and, for every $(x,y,z) \in D_1 \times D_2 \times D_3$,*

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

When property (ii) holds, property (i) fails. Indeed, consider any $v = (x_0, y_0, z_0)$ and φ_i, D_i as in property (ii). If we set $t_1 = \varphi_1(x_0)$, $t_2 = \varphi_2(y_0)$, and $t_3 = \varphi_3(z_0)$, then we have $t_1 + t_2 + t_3 = 0$. Now choose $A \subset D_1$, $B \subset D_2$, and $C \subset D_3$ so that $\varphi_1(A) = \{t_1 + a, t_1 + 2a, \ldots, t_1 + na\}$, $\varphi_2(B) = \{t_2 + a, t_2 + 2a, \ldots, t_2 + na\}$, and $\varphi_3(C) = \{t_3 - a, t_3 - 2a, \ldots, t_3 - na\}$; this is clearly possible for $a \in \mathbb{C}$ with a sufficiently small absolute value. Then $|Z(F) \cap (A \times B \times C)| \geq n^2/4$.

Our proof also works when the sets A, B, C do not have the same size. Such an "unbalanced" form was not considered in [1] or [2], but similar unbalanced bounds were obtained in [9], and they are useful in applications where the roles of A, B, C are not symmetric. We obtain the following result, which subsumes Theorem 1.1; we have stated both for clarity.

▶ **Theorem 1.2** (Unbalanced case). *In Theorem 1.1, property* (i) *can be replaced by:*

(i*) *For all triples $A,B,C \subset \mathbb{C}$ of finite sets, we have*

$$\begin{aligned} |Z(F) \cap (A \times B \times C)| = O\Big(\min \Big\{ & d^{\frac{13}{2}} |A|^{\frac{1}{2}} |B|^{\frac{2}{3}} |C|^{\frac{2}{3}} + d^{\frac{17}{2}} |A|^{\frac{1}{2}} \Big(|A|^{\frac{1}{2}} + |B| + |C| \Big), \\ & d^{\frac{13}{2}} |B|^{\frac{1}{2}} |A|^{\frac{2}{3}} |C|^{\frac{2}{3}} + d^{\frac{17}{2}} |B|^{\frac{1}{2}} \Big(|B|^{\frac{1}{2}} + |A| + |C| \Big), \\ & d^{\frac{13}{2}} |C|^{\frac{1}{2}} |A|^{\frac{2}{3}} |B|^{\frac{2}{3}} + d^{\frac{17}{2}} |C|^{\frac{1}{2}} \Big(|C|^{\frac{1}{2}} + |A| + |B| \Big) \Big\} \Big). \end{aligned}$$

We also have the following specialization of Theorem 1.2 when F is a real polynomial. Note that, when F is real, it does not immediately follow from Theorems 1.1 and 1.2 that, in property (ii) there, the functions φ_i can be chosen so that they map $\mathbb{R}$ to $\mathbb{R}$. We write $Z_{\mathbb{R}}(F)$ for the real zero set of a real polynomial defined over $\mathbb{R}$.

▶ **Theorem 1.3** (Real case). *Let $F \in \mathbb{R}[x, y, z]$ be a polynomial of degree d that is irreducible over $\mathbb{R}$. Assume that $Z_{\mathbb{R}}(F)$ has dimension two. Then property* (ii) *in both Theorems 1.1 and 1.2 can be replaced by:*

(ii)$_{\mathbb{R}}$ *There exists a one-dimensional subvariety $Z_0 \subset Z_{\mathbb{R}}(F)$ (whose degree is polynomial in d), such that for every $v \in Z_{\mathbb{R}}(F) \setminus Z_0$, there exist open intervals $I_1, I_2, I_3 \subset \mathbb{R}$, and real-analytic functions $\varphi_i : I_i \to \mathbb{R}$ for $i = 1, 2, 3$, such that $v \in I_1 \times I_2 \times I_3$, and, for every $(x, y, z) \in I_1 \times I_2 \times I_3$,*

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

The proof of Theorem 1.3 is omitted in this version.

Discussion. Although the results in this paper generalize those of Raz et al. [9], the analysis here is quite different and considerably more involved. The overlap between the two studies is only in the initial reduction of the problem to an incidence problem between points and curves (see below). The remaining and major part of the paper applies totally different machinery. Instead of the purely algebraic study of properties of polynomials that was used in [9], the approach here requires more advanced tools from algebraic geometry, and applies them in a considerably more involved style, inspired in part by a technique used by Tao [14] for a problem in finite fields.

That the current problem is considerably more difficult than the Elekes–Rónyai problem (in spite of their similarities) can also be seen by comparing the original respective studies in [1] and in [2]. We regard the considerable simplification (on top of the improvement in the bound) of the analysis of Elekes and Szabó in [2] as a major outcome of this paper.

We note that the polynomial dependence of our bound on the degree of F is also a significant feature, because it allows us to obtain non-trivial bounds for polynomials of non-constant degree. This arises for example in the application of obtaining lower bounds for the number of distinct distances between points on an algebraic curve (as discussed below), where the bound is still non-trivial when the degree of the curve is non-constant. An improved dependence on d would allow us to treat more general sets of points, and get closer (and perhaps even reconstruct) the general lower bound of Guth and Katz [6].

Consequences. Besides being an interesting problem in itself, the Elekes-Szabó setup arises in many problems in combinatorial geometry. To demonstrate this, consider the problem of obtaining a lower bound for the number of distinct distances determined between three *non-collinear* points p_1, p_2, p_3 and a set P of n other points in the plane, studied in [2, 12]. To cast this problem into the Elekes–Szabó mold, let D denote the set of the squared distances between the points p_i and those of P. Write $p_i = (a_i, b_i)$, for $i = 1, 2, 3$. A point $q = (t, s) \in \mathbb{R}^2$ determines three squared distances to p_1, p_2, p_3, given by

$$X = (t - a_1)^2 + (s - b_1)^2, \quad Y = (t - a_2)^2 + (s - b_2)^2, \quad Z = (t - a_3)^2 + (s - b_3)^2.$$

Eliminating t and s from these equations yields a quadratic equation $F(X, Y, Z) = 0$. By construction, for each point $q \in P$, each of the corresponding squared distances X, Y, Z belongs to D. Moreover, the resulting triples (X, Y, Z) are all distinct, and so F vanishes at n triples of $D \times D \times D$. Moreover, since p_1, p_2, p_3 are non-collinear, one can show that F does not have the special form in property (ii)$_{\mathbb{R}}$ of Theorem 1.3. So one gets $n = O(|D|^{11/6})$, or $|D| = \Omega(n^{6/11})$, which is the same lower bound obtained in [12], using a direct ad-hoc analysis. Note that for p_1, p_2, and p_3 collinear, F becomes a linear polynomial, in which

case it certainly satisfies property (ii)$_{\mathbb{R}}$, and the above bound on $|D|$ does not hold – it can be $\Theta(n^{1/2})$ in this case.

Geometric questions which involve Euclidean distances, slopes, or collinearity often lead to polynomial relations of the form $F(x, y, z) = 0$, and can be reduced to studying the number of zeros of such polynomials attained on a Cartesian product. The following is a sample of problems that fit into this framework: (i) Bounding from below the number of distinct distances [8, 11] determined by a set of n points lying on a planar algebraic curve. (ii) Bounding from above the number of triple intersection points for three families of n unit circles, each consisting of circles that pass through a fixed point [4, 10]. (iii) Bounding from below the number of collinear triples among n points on an algebraic curve in $\mathbb{R}^2$ [3].

Due to lack of space, many details are omitted in this abstract and are given in the full version of the paper.

2 Proof of Theorem 1.2

In this section we prove Theorem 1.2, up to the crucial Proposition 2.3 that we prove in Section 3. Let $F \in \mathbb{C}[x, y, z]$ be an irreducible polynomial of degree d. Let $A, B, C \subset \mathbb{C}$ be finite, and put $M := |Z(F) \cap (A \times B \times C)|$; this is the quantity we wish to bound. The strategy of the proof is to transform the problem of bounding M into an incidence problem for points and curves in $\mathbb{C}^2$. The latter problem can then be tackled using a Szemerédi-Trotter-like incidence bound, *provided* that the resulting curves have well-behaved intersections, in the following sense.

▶ **Definition 2.1.** We say that a system (Π, Γ), where Π is a finite set of distinct points in $\mathbb{C}^2$, and Γ is a finite multiset of curves in $\mathbb{C}^2$, has (λ, μ)-*bounded multiplicity* if

(a) for any curve $\gamma \in \Gamma$, there are at most λ curves $\gamma' \in \Gamma$ (counted with multiplicity) such that there are more than μ points contained in both γ and γ'; and

(b) for any point $p \in \Pi$, there are at most λ points $p' \in \Pi$ such that there are more than μ curves (counted with multiplicity) that contain both p and p'.

A major component of the proof is to show that if the points and curves that we are about to define fail to satisfy the conditions of (λ, μ)-bounded multiplicity, then $Z(F)$ must have the special form described in property (ii) of Theorem 1.2.

Quadruples. Define $Q := \{(b, b', c, c') \in B^2 \times C^2 \mid \exists a \in A \text{ s.t. } F(a, b, c) = F(a, b', c') = 0\}$. The following inequality bounds M in terms of $|Q|$.

▶ **Lemma 2.2.** *We have* $M = O\left(d^{1/2}|A|^{1/2}|Q|^{1/2} + d^2|A|\right)$.

Proof. For each $a \in A$, we write $(B \times C)_a := \{(b, c) \in B \times C \mid F(a, b, c) = 0\}$. Using the Cauchy-Schwarz inequality, we have

$$M = \sum_{a \in A} |\,(B \times C)_a\,| \leq |A|^{1/2} \Big(\sum_{a \in A} |\,(B \times C)_a\,|^2 \Big)^{1/2}.$$

Define $R := \{(a, b, b', c, c') \in A \times B^2 \times C^2 \mid F(a, b, c) = F(a, b', c') = 0\}$, and consider the standard projection $\tau : \mathbb{C} \times \mathbb{C}^4 \to \mathbb{C}^4$ (in which the first coordinate is discarded). We have $Q = \tau(R)$ and $M \leq |A|^{1/2}|R|^{1/2}$.

We claim that $|R| \leq d|Q| + d^4|A|$. To prove this, let

$$S := \left\{(b, b', c, c') \in B^2 \times C^2 \mid F(a, b, c) \equiv 0 \text{ and } F(a, b', c') \equiv 0 \text{ (as polynomials in } a)\right\}.$$

We prove in the full version that $|S| = O(d^4)$. Observe that for $(b, b', c, c') \in Q \backslash S$ we have $|\tau^{-1}(b, b', c, c') \cap R| \leq d$, while for $(b, b', c, c') \in S$ we have $|\tau^{-1}(b, b', c, c') \cap R| = |A|$. Thus

$$|R| = |\tau^{-1}(Q)| = |\tau^{-1}(Q \backslash S)| + |\tau^{-1}(S)| \leq d|Q| + d^4|A|,$$

which proves the claim and the lemma. ◀

In what follows, we derive an upper bound on $|Q|$. It will turn out that, when we fail to obtain the bound we are after, F must have the special form in property (ii).

Curves and dual curves. For every point $(y, y') \in \mathbb{C}^2$, we define

$$\gamma_{y,y'} := \mathrm{Cl}\left(\left\{(z, z') \in \mathbb{C}^2 \mid \exists x \in \mathbb{C} \text{ such that } F(x, y, z) = F(x, y', z') = 0\right\}\right),$$

where $\mathrm{Cl}(X)$ stands for the Zariski closure of X. We show in the full version that there exists an exceptional set $\mathcal{S} \subset \mathbb{C}^2$ of size $O(d^4)$, such that for every $(y, y') \in \mathbb{C}^2 \backslash \mathcal{S}$ the set $\gamma_{y,y'}$ is an algebraic curve of degree at most d^2, or an empty set (a possibility we can safely ignore).

We define, in an analogous manner, a dual system of curves by switching the roles of the y- and z-coordinates, as follows. For every point $(z, z') \in \mathbb{C}^2$, we define

$$\gamma^*_{z,z'} := \mathrm{Cl}\left(\left\{(y, y') \in \mathbb{C}^2 \mid \exists x \in \mathbb{C} \text{ such that } F(x, y, z) = F(x, y', z') = 0\right\}\right).$$

As above, here too our (omitted) analysis yields an exceptional set $\mathcal{T}$ of size $O(d^4)$, such that for every $(z, z') \in \mathbb{C}^2 \backslash \mathcal{T}$ the set $\gamma^*_{z,z'}$ is an algebraic curve of degree at most d^2 (or empty).

By a standard argument (omitted here), the closure in the definitions of $\gamma_{y,y'}$ and $\gamma^*_{z,z'}$ adds only finitely many points. It follows that, for all but finitely many points $(z, z') \in \gamma_{y,y'}$, we have $(y, y') \in \gamma^*_{z,z'}$. Symmetrically, for all but finitely many $(y, y') \in \gamma^*_{z,z'}$ we have $(z, z') \in \gamma_{y,y'}$.

We set $m := d^4$ throughout this proof. We say that an irreducible algebraic curve $\gamma \subset \mathbb{C}^2$ is a *popular curve* if there exist at least $m + 1$ distinct points $(y, y') \in \mathbb{C}^2 \backslash \mathcal{S}$ such that $\gamma \subset \gamma_{y,y'}$. We denote by $\mathcal{C}$ the set of all popular curves. Similarly, we say that an irreducible algebraic curve $\gamma^* \subset \mathbb{C}^2$ is *a popular dual curve*, if there exist at least $m + 1$ distinct points $(z, z') \in \mathbb{C}^2 \backslash \mathcal{T}$ such that $\gamma^* \subset \gamma^*_{z,z'}$. We denote by $\mathcal{D}$ the set of all popular dual curves.

The main step in our proof is the following proposition, whose proof takes up Section 3. Note that its statement is only about F and does not involve the specific sets A, B, C.

▶ **Proposition 2.3.** *Either F satisfies property* (ii) *of Theorem 1.2, or the following holds.*

(a) *There exists an algebraic curve $\mathcal{X} \subset \mathbb{C}^2$ of degree $O(d^{11})$ containing $\mathcal{S}$, such that for every $(y, y') \in \mathbb{C}^2 \backslash \mathcal{X}$, no irreducible component of $\gamma_{y,y'}$ is a popular curve.*

(b) *There exists an algebraic curve $\mathcal{Y} \subset \mathbb{C}^2$ of degree $O(d^{11})$ containing $\mathcal{T}$, such that for every $(z, z') \in \mathbb{C}^2 \backslash \mathcal{Y}$, no irreducible component of $\gamma^*_{z,z'}$ is a popular dual curve.*

Incidences. We continue with the analysis, assuming the truth of Proposition 2.3. We introduce the following set of points and *multiset* of curves:

$$\Pi := (C \times C) \backslash \mathcal{Y} \qquad \text{and} \qquad \Gamma := \{\gamma_{b,b'} \mid (b, b') \in (B \times B) \backslash \mathcal{X}\}.$$

By definition, for every $(b, b', c, c') \in Q$, we have $(c, c') \in \gamma_{b,b'}$ and $(b, b') \in \gamma^*_{c,c'}$ (albeit not necessarily vice versa, because the definition of the curves involves a closure, and does not require x to be in A). This lets us relate $|Q|$ to $I(\Pi, \Gamma)$, the number of incidences between these points and curves; since Γ is a multiset, these incidences are counted with the multiplicity of the relevant curves. Specifically, we show in the full version:

▶ **Lemma 2.4.** *We have* $|Q| \leq I(\Pi, \Gamma) + O\left(d^{13}|B||C| + d^4|B|^2 + d^4|C|^2\right)$.

Bounded multiplicity. We claim that the system (Π, Γ) has (d^6, d^4)-bounded multiplicity. Indeed, by Proposition 2.3(a) and the fact that we have avoided $\mathcal{X}$ when defining Γ, any component of a curve $\gamma \in \Gamma$ is not in $\mathcal{C}$, and is thus shared with at most $m = d^4$ other curves. The curve γ has at most d^2 irreducible components, so there are at most $md^2 = d^6$ curves $\gamma' \in \Gamma$ such that γ and γ' have a common component. Curves γ' that do not have a common component with γ intersect it in at most d^4 points by Bézout's inequality; thus condition (a) in the definition of (d^6, d^4)-bounded multiplicity is satisfied. The argument for condition (b) is fully symmetric.

Incidence bound. In the full version of this paper we derive an incidence bound, based on that of Solymosi and De Zeeuw [13], resembling the classical Szemerédi-Trotter point-line incidence bound. It applies to a set Π of points and a multiset Γ of algebraic curves, each of degree at most δ, in $\mathbb{C}^2$, such that Π is a Cartesian product and (Π, Γ) have (λ, μ)-bounded multiplicity as in Definition 2.1. The analysis culminates in the incidence bound

$$I(\Pi, \Gamma) = O\left(\delta^{4/3}\lambda^{4/3}\mu^{1/3}|\Pi|^{2/3}|\Gamma|^{2/3} + \lambda^2\mu|\Pi| + \delta^4\lambda|\Gamma|\right).$$

Specializing this, with $\delta = d^2$, $\lambda = d^6$, and $\mu = d^4$, we get

$$\begin{aligned} I(\Pi, \Gamma) &= O\left((d^2)^{4/3}(d^6)^{4/3}(d^4)^{1/3}|B|^{4/3}|C|^{4/3} + (d^6)^2d^4|B|^2 + (d^2)^4d^6|C|^2\right) \\ &= O\left(d^{12}|B|^{4/3}|C|^{4/3} + d^{16}|B|^2 + d^{14}|C|^2\right), \end{aligned}$$

which, together with Lemma 2.4, gives

$$|Q| = I(\Pi, \Gamma) + O\left(d^{13}|B||C| + d^4|B|^2 + d^4|C|^2\right) = O(d^{12}|B|^{4/3}|C|^{4/3} + d^{16}|B|^2 + d^{14}|C|^2).$$

Then, from Lemma 2.2, we get

$$\begin{aligned} M &\le d^{1/2}|A|^{1/2}|Q|^{1/2} + d^2|A| \\ &= O\left(d^{13/2}|A|^{1/2}|B|^{2/3}|C|^{2/3} + d^{17/2}|A|^{1/2}|B| + d^{15/2}|A|^{1/2}|C| + d^2|A|\right), \end{aligned}$$

which gives the first of the three bounds in Theorem 1.2(i). The other two follow symmetrically.

3 Proof of Proposition 2.3

3.1 Overview of the proof

We adapt an idea used by Tao [14] to study the expansion of a polynomial $P(x, y)$ over finite fields. As part of his analysis he considered the map $\Psi : \mathbb{C}^4 \to \mathbb{C}^4$ defined by

$$\Psi : (a, b, c, d) \mapsto (P(a, c), P(a, d), P(b, c), P(b, d)).$$

Tao showed that if the image $\Psi(\mathbb{C}^4)$ is four-dimensional, then lower bounds on the expansion of P can be derived. On the other hand, if the image has dimension at most three, then P must have one of the special forms $G(H(x) + K(y))$ or $G(H(x)K(y))$, for polynomials G, H, K (as in [1, 9]; see also the introduction). Tao proved this by observing that in this case the determinant of the Jacobian matrix of Ψ must vanish identically, leading to an identity for the partial derivatives of P, from which the special forms of P can be deduced.

Following Tao's general scheme, albeit in a different context, we define a variety

$$V := \big\{(x,x',y,y',z_1,z_2,z_3,z_4) \in \mathbb{C}^8 \mid F(x,y,z_1) = F(x,y',z_2) = F(x',y,z_3) = F(x',y',z_4) = 0\big\}. \tag{1}$$

Note that if we fix y, y' in V and eliminate x, x', the range of the last four coordinates of V is $\gamma_{y,y'} \times \gamma_{y,y'}$ (up to the closure operation). Near most points $v \in V$, we use the implicit function theorem to represent V as the graph of a locally defined analytic function (which serves as a local analogue of the map Ψ above)

$$\Phi_v : (x,x',y,y') \mapsto \big(g_1(x,y),\ g_2(x,y'),\ g_3(x',y),\ g_4(x',y')\big).$$

If the determinant of the Jacobian of Φ_v vanishes at v, for all v in some relatively open subset of V, it leads to the special form of F. This derivation is similar to that of Tao, but our special form requires a somewhat different treatment.

The other side of our argument, when the determinant of the Jacobian is not identically zero, as above, is very different from that of Tao. Here we want to show that there are only finitely many popular curves. (The actual property that we show is somewhat different, but this is the spirit of our analysis.) We show that if γ is a popular curve (i.e., there are more than d^4 curves $\gamma_{y,y'} \in \Gamma$ that contain γ), then it is *infinitely* popular, in the sense that there is a one-dimensional curve γ^* of pairs $(y,y') \in \mathbb{C}^2$ for which $\gamma_{y,y'}$ contains γ. For V, this implies that if we restrict (y,y') to γ^* and project to the last four coordinates, then the image is contained in $\gamma \times \gamma$. In other words, the local map Φ_v sends an open subset of the three-dimensional variety $\mathbb{C}^2 \times \gamma^*$ to an open subset of the two-dimensional variety $\gamma \times \gamma$. The inverse mapping theorem now tells us that the determinant of the Jacobian of Φ_v vanishes on the three-dimensional variety $\mathbb{C}^2 \times \gamma^*$. Given that this determinant is not identically zero, its zero set is three-dimensional, so $\mathbb{C}^2 \times \gamma^*$ must be one of its $O_d(1)$ irreducible components. It follows that there are only $O_d(1)$ popular curves, which essentially establishes Proposition 2.3.

3.2 The varieties V, V_0 and W

Consider the variety $V \subset \mathbb{C}^8$ as defined in (1). V is not empty since, for any point $(x,y,z) \in Z(F)$, it contains (x,x,y,y,z,z,z,z) . It follows that V has dimension at least four; it can in fact be shown that V is four-dimensional. However, our analysis requires that the projection of V to the first four coordinates is four-dimensional, which does not follow directly. We show this in the following lemma. Throughout Section 3 we write $\pi_1 : \mathbb{C}^8 \to \mathbb{C}^4$ and $\pi_2 : \mathbb{C}^8 \to \mathbb{C}^4$ for the standard projections onto the first and the last four coordinates, respectively.

▶ **Lemma 3.1.** *We have* $\mathrm{Cl}(\pi_1(V)) = \mathbb{C}^4$.

Proof. Let $(x_0,x_0',y_0,y_0') \in \mathbb{C}^4$. There exist $z_1,z_2,z_3,z_4 \in \mathbb{C}$ such that

$$F(x_0,y_0,z_1) = F(x_0,y_0',z_2) = F(x_0',y_0,z_3) = F(x_0',y_0',z_4) = 0,$$

unless we have $F(x_0,y_0,z) \equiv c$ for some nonzero $c \in \mathbb{C}$, or a similar identity holds for one of the pairs (x_0,y_0'), (x_0',y_0), (x_0',y_0'). In other words, we have $(x_0,x_0',y_0,y_0') \in \pi_1(V)$ unless one of these exceptions holds.

Let $\sigma := \mathrm{Cl}\big(\{(x_0,y_0) \in \mathbb{C}^2 \mid \exists c \text{ such that } F(x_0,y_0,z) \equiv c\}\big)$ (note that here we include the case $c = 0$). We show (in the full version) that $\dim(\sigma) \le 1$, so the set

$$\sigma' := \{(x,x',y,y') \mid \text{one of } (x,y),(x,y'),(x',y),(x',y') \text{ is in } \sigma\}$$

has dimension at most 3. By standard properties of the closure operation, we have $\mathrm{Cl}(\mathbb{C}^4\backslash\sigma') = \mathbb{C}^4$. As observed above, we have $\mathbb{C}^4\backslash\sigma' \subset \pi_1(V)$, so we get $\mathbb{C}^4 = \mathrm{Cl}(\mathbb{C}^4\backslash\sigma') \subset \mathrm{Cl}(\pi_1(V)) \subset \mathbb{C}^4$ and hence $\mathrm{Cl}(\pi_1(V)) = \mathbb{C}^4$. ◀

We use the implicit function theorem to locally express each of the variables z_1, z_2, z_3, z_4 in terms of the corresponding pair of the first four variables x, x', y, y'. To facilitate this we first exclude the subvariety of V defined by $V_0 := V_1 \cup V_2 \cup V_3$, where

$$V_i := \{(x, x', y, y', z_1, z_2, z_3, z_4) \in V \mid F_i(x, y, z_1)F_i(x, y', z_2)F_i(x', y, z_3)F_i(x', y', z_4) = 0\},$$

and F_i stands for the derivative of F with respect to its ith variable, for $i = 1, 2, 3$.

The following lemma, whose proof we omit, asserts that $\mathrm{Cl}(\pi_1(V_0))$ is a subvariety of V of dimension ≤ 3. This property allows us to exclude $\mathrm{Cl}(\pi_1(V_0))$ in most of our proof.

▶ **Lemma 3.2.** *$\mathrm{Cl}(\pi_1(V_0))$ has dimension at most three.*

As explained in Section 3.1, we want to view V, around most of its points, as the graph of a locally defined mapping. We now define this mapping.

▶ **Lemma 3.3.** *For each point $v \in V\backslash V_0$, there is an open neighborhood $N_v \subset \mathbb{C}^8$ of v such that $V_0 \cap N_v = \emptyset$, and an analytic mapping $\Phi_v : \pi_1(N_v) \to \pi_2(N_v)$, such that $V \cap N_v = \{(u, \Phi_v(u)) \mid u \in \pi_1(N_v)\}$.*

Proof. Let $v = (a, a', b, b', c_1, c_2, c_3, c_4) \in V\backslash V_0$ be an arbitrary point. We apply the implicit function theorem (see [5]) to the equation $F(x, y, z_1) = 0$ at the point (a, b, c_1). Since $v \notin V_0$, we have $F_3(a, b, c_1) \neq 0$. We thus obtain neighborhoods U of (a, b) in $\mathbb{C}^2$ and V of c_1 in $\mathbb{C}$, and an analytic mapping $g_1 : U \to V$ such that

$$\{(x, y, z_1) \in U \times V \mid F(x, y, z_1) = 0\} = \{(x, y, g_1(x, y)) \mid (x, y) \in U\}.$$

We can do the same at each of the points $(a, b', c_2), (a', b, c_3), (a', b', c_4)$, leading to analogous mappings g_2, g_3, g_4. It follows that we can find neighborhoods N_1 of a, N_2 of a', N_3 of b, and N_4 of b', such that the mapping

$$\Phi_v : (x, x', y, y') \mapsto \big(g_1(x, y),\ g_2(x, y'),\ g_3(x', y),\ g_4(x', y')\big)$$

is defined and analytic over $N_1 \times N_2 \times N_3 \times N_4$. Then

$$N_v := (N_1 \times N_2 \times N_3 \times N_4) \times \Phi_v(N_1 \times N_2 \times N_3 \times N_4)$$

is a neighborhood of v in $\mathbb{C}^8$ satisfying the conclusion of the lemma. If needed, we can shrink it to be disjoint from V_0. ◀

Let G be the polynomial in $\mathbb{C}[x, x', y, y', z_1, z_2, z_3, z_4]$ given by

$$\begin{aligned} G = {} & F_2(x, y, z_1)F_1(x, y', z_2)F_1(x', y, z_3)F_2(x', y', z_4) \\ & - F_1(x, y, z_1)F_2(x, y', z_2)F_2(x', y, z_3)F_1(x', y', z_4). \end{aligned}$$

Consider the subvariety $W := V \cap Z(G)$ of V. The significance of W (and of G) lies in the following lemma.

▶ **Lemma 3.4.** *For $v \in V\backslash V_0$ we have $v \in W$ if and only if $\det(J_{\Phi_v}(\pi_1(v))) = 0$.*

Proof. We write g_{ij} for the derivative of the function g_i (from the proof of Lemma 3.3), within its domain of definition, with respect to its jth variable, for $i = 1, 2, 3, 4$, and $j = 1, 2$. The Jacobian matrix of Φ_v, evaluated at $u = (x, x', y, y') \in \pi_1(N_v)$, where N_v is the neighborhood of v given in Lemma 3.3, equals

$$J_{\Phi_v}(u) = \begin{pmatrix} g_{11}(x,y) & g_{21}(x,y') & 0 & 0 \\ 0 & 0 & g_{31}(x',y) & g_{41}(x',y') \\ g_{12}(x,y) & 0 & g_{32}(x',y) & 0 \\ 0 & g_{22}(x,y') & 0 & g_{42}(x',y') \end{pmatrix}, \tag{2}$$

or, by implicit differentiation,

$$J_{\Phi_v}(u) = \begin{pmatrix} -\frac{F_1(x,y,z_1)}{F_3(x,y,z_1)} & -\frac{F_1(x,y',z_2)}{F_3(x,y',z_2)} & 0 & 0 \\ 0 & 0 & -\frac{F_1(x',y,z_3)}{F_3(x',y,z_3)} & -\frac{F_1(x',y',z_4)}{F_3(x',y',z_4)} \\ -\frac{F_2(x,y,z_1)}{F_3(x,y,z_1)} & 0 & -\frac{F_2(x',y,z_3)}{F_3(x',y,z_3)} & 0 \\ 0 & -\frac{F_2(x,y',z_2)}{F_3(x,y',z_2)} & 0 & -\frac{F_2(x',y',z_4)}{F_3(x',y',z_4)} \end{pmatrix},$$

for $z_1 = g_1(x, y)$, $z_2 = g_2(x, y')$, $z_3 = g_3(x', y)$, and $z_4 = g_4(x', y')$. Since $N_v \cap V_0 = \emptyset$, all the denominators are non-zero (and, for that matter, also all the numerators). Write $v = (a, a', b, b', c_1, c_2, c_3, c_4)$. Computing this determinant explicitly at the point $u = \pi_1(v) = (a, a', b, b')$, noticing that by construction $c_1 = g_1(a, b)$, $c_2 = g_2(a, b')$, $c_3 = g_3(a', b)$, and $c_4 = g_4(a', b')$, and clearing denominators, gives exactly $G(v)$, where G is the polynomial defining W. Thus, $\det J_{\Phi_v}(\pi_1(v)) = 0$ if and only if $G(v) = 0$. ◀

3.3 The varieties V_γ

We now make precise what it means for a popular curve to be infinitely popular.

▶ **Definition 3.5.** Let $\gamma \subset \mathbb{C}^2$ be an irreducible curve. An irreducible curve $\gamma^* \subset \mathbb{C}^2$ is an *associated curve* of γ if for all but finitely many $(y, y') \in \gamma^*$ we have $\gamma \subset \gamma_{y,y'}$.

Throughout this section, we will let γ denote a popular curve and γ^* an associated curve of γ. In Section 3.4, we will show that every γ has at least one associated curve. With each $\gamma \in \mathcal{C}$, we associate the variety

$$V_\gamma := \mathrm{Cl}\left(V \cap (\mathbb{C}^2 \times \gamma_r^* \times \gamma_r \times \gamma_r)\right) \subset \mathbb{C}^8,$$

where γ^* is any curve associated to γ, and γ_r^*, γ_r denote the subsets of regular points of γ^*, γ, respectively. It easily follows from the definition of V that, for most regular points $(z_1, z_2), (z_3, z_4) \in \gamma_r$ and for most regular points $(y, y') \in \gamma^*$, there exist $x, x' \in \mathbb{C}$ such that $(x, x', y, y', z_1, z_2, z_3, z_4) \in V_\gamma$. We have the following key property.

▶ **Lemma 3.6.** *For all $\gamma \in \mathcal{C}$ we have $V_\gamma \subset W \cup V_0$.*

Proof. It is sufficient to show that

$$V_\gamma' := V \cap (\mathbb{C}^2 \times \gamma_r^* \times \gamma_r \times \gamma_r) \subset W \cup V_0.$$

For this, let $v \in V_\gamma' \backslash V_0$. Then Lemma 3.3 gives an open neighborhood N_v of v, disjoint from V_0, so that $V \cap N_v$ is the graph of an analytic map $\Phi_v : B_1 \to B_2$, where $B_1 := \pi_1(N_v)$ and $B_2 := \pi_2(N_v)$.

Assume, for contradiction, that $v \notin W$. Then Lemma 3.4 gives $\det(J_{\Phi_v}(\pi_1(v))) \neq 0$. By the inverse mapping theorem (see [5]), Φ_v is bianalytic on a sufficiently small neighborhood of $\pi_1(v)$, which, by shrinking N_v if needed, we may assume to be B_1.

Consider the mapping $\overline{\Phi}_v := \Phi_v \circ \pi_1$ restricted to $V \cap N_v$. Note that $\overline{\Phi}_v$ is bianalytic. Indeed, π_1 restricted to $V \cap N_v$ is clearly bianalytic (its inverse is $u \mapsto (u, \Phi_v(u))$), so $\overline{\Phi}_v$ is the composition of two bianalytic functions, hence itself bianalytic. By definition of V_γ we have $\overline{\Phi}_v(V_\gamma \cap N_v) \subset \gamma \times \gamma$.

Write $v = (a, a', b, b', c_1, c_2, c_3, c_4)$, and note that, by the definition of V'_γ, $(c_1, c_2), (c_3, c_4)$ are regular points of γ and (b, b') is a regular point of γ^*. We claim that there exists an open $N \subset N_v$ such that $V_\gamma \cap N$ is locally three-dimensional. Indeed, we may assume, without loss of generality, that none of the tangents to γ at (c_1, c_2), (c_3, c_4), and to γ^* at (b, b') are vertical in the respective planes (otherwise, we simply switch the roles of the first and the second coordinate in the relevant copy of $\mathbb{C}^2$). Applying the implicit function theorem (see [5]) to γ and γ^* at these regular points, we may therefore write $z_2 = \rho_1(z_1)$, $z_4 = \rho_2(z_3)$, and $y' = \rho_3(y)$ in sufficiently small neighborhoods of (b, b'), (c_1, c_2), (c_3, c_4), along the respective curves, for analytic functions ρ_1, ρ_2, ρ_3. Similarly, applying the implicit function theorem to $Z(F)$ in sufficiently small neighborhoods of (a, b, c_1), (a', b, c_3) (which we may, since we are away from V_0), we may write $x = \sigma_1(y, z_1)$, $x' = \sigma_2(y, z_3)$, for analytic functions σ_1, σ_2. Combining the functions above, we obtain an open neighborhood N of v such that the map

$$(y, z_1, z_3) \mapsto (\sigma_1(y, z_1), \sigma_2(y, z_3), y, \rho_3(y), z_1, \rho_1(z_1), z_3, \rho_2(z_3))$$

is bianalytic from an open neighborhood of (b, c_1, c_3) to $V_\gamma \cap N$. This implies that $V_\gamma \cap N$ is locally three-dimensional. Since $\gamma \times \gamma$ has local dimension 2 at every pair of regular points, and $\overline{\Phi}_v$ preserves local dimension, since it is bianalytic, this yields a contradiction, which completes the proof of the lemma. ◀

▶ **Lemma 3.7.** *If $\gamma \in \mathcal{C}$ is not an axis-parallel line, then $\mathrm{Cl}(\pi_1(V_\gamma)) = \mathbb{C}^2 \times \gamma^*$.*

Proof. We clearly have $\pi_1(V_\gamma) \subset \pi_1(\mathbb{C}^2 \times \gamma^* \times \gamma \times \gamma) = \mathbb{C}^2 \times \gamma^*$, so, since $\mathbb{C}^2 \times \gamma^*$ is a variety, we get $\mathrm{Cl}(\pi_1(V_\gamma)) \subset \mathbb{C}^2 \times \gamma^*$.

By definition, there is a finite subset $S \subset \gamma^*$ such that, for all $(b, b') \in \gamma^* \backslash S$, $\gamma \subset \gamma_{b,b'}$; fix such a point (b, b') which is also a regular point of γ^*. Then, by definition of V, it is easily checked that

$$\pi_1(V_\gamma) \cap Z(y - b, y' - b') \supset \beta_{b,b'} \times \beta_{b,b'} \times \{(b, b')\},$$

where $\beta_{b,b'} := \{x \in \mathbb{C} \mid \exists (c_1, c_2) \in \gamma_r \text{ such that } F(x, b, c_1) = F(x, b', c_2) = 0\}$. Since γ is not a line parallel to any of the axes,[1] one can show (details in the full version) that $\mathrm{Cl}(\beta_{b,b'}) = \mathbb{C}$. Hence

$$\begin{aligned}\mathrm{Cl}(\pi_1(V_\gamma)) &\supset \mathrm{Cl}\Big(\bigcup_{(b,b') \in \gamma_r^* \backslash S} \beta_{b,b'} \times \beta_{b,b'} \times \{(b, b')\}\Big) \supset \bigcup_{(b,b') \in \gamma_r^* \backslash S} \mathrm{Cl}\big(\beta_{b,b'} \times \beta_{b,b'} \times \{(b, b')\}\big) \\ &= \mathbb{C}^2 \times \mathrm{Cl}\Big(\bigcup_{(b,b') \in \gamma_r^* \backslash S} \{(b, b')\}\Big) = \mathbb{C}^2 \times \mathrm{Cl}\big(\gamma_r^* \backslash S\big) = \mathbb{C}^2 \times \gamma^*,\end{aligned}$$

using that the closure of an infinite union *contains* the union of the closures, and that the closure of a product is the product of the closures. This completes the proof of the lemma. ◀

[1] If γ were such a line, one of the equations, say $F(x, b, c_1) = 0$ would have a fixed value of c_1, and only $O_d(1)$ values of x.

3.4 The associated curves

In this section we show that if a curve γ is popular, then it has at least one associated curve, of the sort defined in Definition 3.5. First we need the following sharpened form of Bézout's inequality for many curves. A proof can be found in Tao [15].

▶ **Lemma 3.8** (Bézout for many curves). *If $\mathcal{F}$ is a (possibly infinite) family of algebraic curves in $\mathbb{C}^2$, each of degree at most δ, then $\deg\left(\bigcap_{C\in\mathcal{F}} C\right) \le \delta^2$. In other words, either $\bigcap_{C\in\mathcal{F}} C$ is 0-dimensional and has cardinality at most δ^2, or it has dimension 1 and degree at most δ^2.*

Recall that $\mathcal{C}$ is the set of popular curves, i.e., irreducible curves γ that are contained in $\gamma_{y,y'}$ for more than d^4 points $(y,y') \in \mathbb{C}^2\backslash\mathcal{S}$ (where $\mathcal{S}$ is the set constructed in Section 2). Lemma 3.9 strengthens this property, by showing that if γ is popular, then there is a 1-dimensional set of curves $\gamma_{y,y'}$ that contain γ.

▶ **Lemma 3.9.** *Every $\gamma \in \mathcal{C}$ has at least one associated curve. More precisely, for every $\gamma \in \mathcal{C}$ there exists an algebraic curve $\gamma^* \subset \mathbb{C}^2$ of degree at most d^2 such that for all but finitely many $(y,y') \in \gamma^*$ we have $\gamma \subset \gamma_{y,y'}$.*

Proof. By definition of $\mathcal{C}$, if $\gamma \in \mathcal{C}$, then there exists a set $I \subset \mathbb{C}^2\backslash\mathcal{S}$ of size $|I| = d^4+1$ such that $\gamma \subset \gamma_{y,y'}$ for all $(y,y') \in I$. This means that for all $(y,y') \in I$ and for all but finitely many $(z,z') \in \gamma$, there is an $x \in \mathbb{C}$ such that $F(x,y,z) = F(x,y',z') = 0$, which implies that $(y,y') \in \gamma^*_{z,z'}$. Thus we have $I \subset \gamma^*_{z,z'}$ for all but finitely many $(z,z') \in \gamma$.

Let $\mathcal{F}$ be the infinite family of curves $\gamma^*_{z,z'}$ over all $(z,z') \in \gamma$ satisfying $I \subset \gamma^*_{z,z'}$, and define $S_I := \bigcap_{\gamma^*_{z,z'}\in\mathcal{F}} \gamma^*_{z,z'}$. Then we have $I \subset S_I$. Since all the curves in $\mathcal{F}$ have degree at most d^2, Lemma 3.8 implies that S_I has degree at most d^4. Since $|I| > d^4$, S_I must have dimension 1. Let γ^* be any irreducible component of S_I.

If $(y,y') \in \gamma^*$, then for all but finitely many $(z,z') \in \gamma$ we have $(y,y') \in \gamma^*_{z,z'}$. It follows that for all but finitely many $(y,y') \in \gamma^*$, and for all but finitely many $(z,z') \in \gamma$ (where the excluded points (z,z') depend on the choice of (y,y')), we have $(z,z') \in \gamma_{y,y'}$. Since both γ and $\gamma_{y,y'}$ are algebraic curves, and γ is irreducible, we have $\gamma \subset \gamma_{y,y'}$ for all but finitely many $(y,y') \in \gamma^*$. This means γ^* is an associated curve of γ. ◀

3.5 Case 1: $\dim \mathrm{Cl}(\pi_1(W)) \le 3$ implies few popular curves

Throughout this subsection we assume that $\dim \mathrm{Cl}(\pi_1(W)) \le 3$, and establish the existence of the set $\mathcal{X}$ in Proposition 2.3(a).

As the statement of Lemma 3.7 suggests, popular curves that are axis-parallel lines require a different treatment, provided by the following simple lemma, whose proof we omit.

▶ **Lemma 3.10.** *There is a 1-dimensional variety $\mathcal{X}_1 \subset \mathbb{C}^2$ with $\deg(\mathcal{X}_1) = O(d^2)$ containing $\mathcal{S}$, such that, for every $(y_1,y_2) \in \mathbb{C}^2\backslash\mathcal{X}_1$, the curve γ_{y_1,y_2} contains no axis-parallel line.*

We also need the following observation.

▶ **Lemma 3.11.** *An irreducible curve γ^* is associated to at most d^2 curves $\gamma \in \mathcal{C}$.*

Proof. Suppose there is a set $\mathcal{C}'$ of d^2+1 distinct curves $\gamma \in \mathcal{C}$ that γ^* is associated to. For each $\gamma \in \mathcal{C}'$, we have that, for all but finitely many $(y,y') \in \gamma^*$, γ is contained in $\gamma_{y,y'}$. It follows that there is a point $(y,y') \in \gamma^*$ such that $\gamma \subset \gamma_{y,y'}$ for all $\gamma \in \mathcal{C}'$. This is a contradiction, because $\gamma_{y,y'}$ has at most d^2 irreducible components. ◀

We are now ready to prove the key fact that the number of popular curves is bounded.

▶ **Lemma 3.12.** *There are $O(d^7)$ distinct popular curves $\gamma \in \mathcal{C}$ that are not axis-parallel lines, and there are $O(d^5)$ distinct associated curves of popular curves that are not axis-parallel lines.*

Proof. Let $\gamma \in \mathcal{C}$, assume that it is not an axis-parallel line, and let γ^* be an associated curve of γ. Since γ^* is irreducible, $\mathbb{C}^2 \times \gamma^*$ is an irreducible variety. Using Lemma 3.7 and Lemma 3.6, we have

$$\mathbb{C}^2 \times \gamma^* = \mathrm{Cl}(\pi_1(V_\gamma)) \subset \mathrm{Cl}(\pi_1(W \cup V_0)) = X \cup Y,$$

for $X := \mathrm{Cl}(\pi_1(W))$ and $Y := \mathrm{Cl}(\pi_1(V_0))$. We have $\dim(X) \leq 3$ by the assumption in this subsection, and $\dim(Y) \leq 3$ by Lemma 3.2. We also have $\deg(X) = O(d^5)$ and $\deg(Y) = O(d^5)$, since both are unions of closures of projections of varieties defined by five polynomials, each of degree at most $O(d)$. Since $X \cup Y$ is at most 3-dimensional, and each $\mathbb{C}^2 \times \gamma^*$ is an irreducible 3-dimensional subvariety of $X \cup Y$, it follows that $\mathbb{C}^2 \times \gamma^*$ is one of the finitely many irreducible components of $X \cup Y$.

Let T be the set of all associated curves of all curves $\gamma \in \mathcal{C}$ (excluding γ that are axis-parallel lines). The preceding argument shows that T is a finite set. Moreover, we have

$$\sum_{\gamma^* \in T} \deg(\gamma^*) = \sum_{\gamma^* \in T} \deg(\mathbb{C}^2 \times \gamma^*) \leq \deg(X \cup Y) = O(d^5).$$

This implies that the total number of distinct associated curves is $O(d^5)$. Since by Lemma 3.9 each popular curve has at least one associated curve, and by Lemma 3.11 each associated curve is associated to at most d^2 popular curves, it follows that the number of popular curves is bounded by $O(d^7)$. ◀

Finally, we show that the union of all the associated curves (which are not axis-parallel lines) has bounded degree.

▶ **Lemma 3.13.** *Let $\mathcal{X}_2 := \mathrm{Cl}(\{(y, y') \in \mathbb{C}^2 \mid \exists \gamma \in \mathcal{C},$ not axis-parallel line, s.t. $\gamma \subset \gamma_{y,y'}\})$. Then $\mathcal{X}_2$ is 1-dimensional; its purely 1-dimensional component has degree $O(d^7)$, and the number of 0-dimensional components is $O(d^{11})$.*

Proof. Any 1-dimensional irreducible component of $\mathcal{X}_2$ is an associated curve. By Lemma 3.12, there are $O(d^5)$ associated curves γ^*, and by Lemma 3.9 each is of degree at most $O(d^2)$. This implies that union of the purely 1-dimensional components of $\mathcal{X}_2$ has degree $O(d^7)$.

We next bound the number of 0-dimensional components of $\mathcal{X}_2$. By Lemmas 3.11 and 3.12, the number of popular curves $\gamma \in \mathcal{C}$ is at most $O(d^7)$. We show that, for each of them, the number of isolated points outside the associated curves is at most d^4. Let $\gamma \in \mathcal{C}$ and let $I \subset \mathbb{C}^2 \backslash \mathcal{S}$ denote the set consisting of isolated points, such that $\gamma \subset \gamma_{y,y'}$ for all $(y, y') \in I$. Exactly as in the proof of Lemma 3.9, there is a set S_I, which is the intersection of an infinite family of curves $\gamma^*_{z,z'}$ containing I. Thus we have $I \subset S_I$. By Lemma 3.8, S_I has degree at most d^4, and therefore contains at most d^4 isolated points. ◀

We put $\mathcal{X} := \mathcal{X}_1 \cup \mathcal{X}_2$. Combining Lemma 3.10 and Lemma 3.13, we get $\dim(\mathcal{X}) = 1$ and $\deg(\mathcal{X}) = O(d^{11})$. From the definitions of $\mathcal{X}_1$ and $\mathcal{X}_2$ it is clear that for $(y, y') \notin \mathcal{X}$, the curve $\gamma_{y,y'}$ does not contain any popular curve. This completes the proof of Proposition 2.3(a) in Case 1. Proposition 2.3(b) is proved in a fully symmetric manner.

3.6 Case 2: $\dim \mathrm{Cl}(\pi_1(W)) = 4$ implies a special form of F

Throughout this subsection we assume that $\dim \mathrm{Cl}(\pi_1(W)) = 4$. By definition, $W \subset V$, and we already know that $\dim V = 4$, so W must be four-dimensional too, which implies that there exists an irreducible component $V' \subset W$ such that $\dim V' = 4$ and $\mathrm{Cl}(\pi_1(V')) = \mathbb{C}^4$. We will work only with V' in the rest of this subsection. We first show that most points of $Z(F)$, excluding only a lower-dimensional subset, can be extended to points of V', in the following sense.

▶ **Lemma 3.14.** *There exists a one-dimensional subvariety $Z_0 \subset Z(F)$ such that, for every $(a, b, c_1) \in Z(F) \backslash Z_0$, there exist a', b', c_2, c_3, c_4 such that $(a, a', b, b', c_1, c_2, c_3, c_4)$ is a regular point of V' which is not in V_0.*

Proof. Let $\rho : \mathbb{C}^8 \to \mathbb{C}^6$ be the (permuted) projection map $\rho : (x, x', y, y', z_1, z_2, z_3, z_4) \mapsto (x, y, z_1, x', y', z_4)$. We claim that $\mathrm{Cl}(\rho(V')) = Z(F) \times Z(F)$. Since $Z(F) \times Z(F)$ is four-dimensional and irreducible, and since, by definition of V, $\rho(V') \subset Z(F) \times Z(F)$, it suffices to prove that $\mathrm{Cl}(\rho(V'))$ is four-dimensional. We observe that $\sigma(\rho(V')) = \pi_1(V')$, where $\sigma : (x, y, z_1, x', y', z_4) \mapsto (x, x', y, y')$. Because projections cannot increase dimension, we have $\dim \mathrm{Cl}(\rho(V')) \geq \dim \mathrm{Cl}(\pi_1(V')) = 4$, proving our claim.

By the standard properties of the closure operation, $U_1 := \mathrm{Cl}\big((Z(F) \times Z(F)) \backslash \rho(V')\big) = \mathrm{Cl}\big(\mathrm{Cl}(\rho(V')) \backslash \rho(V')\big)$ is at most three-dimensional, and $U_2 := \mathrm{Cl}(\rho(V_0 \cap V'))$ is clearly also at most three-dimensional. Since V' is irreducible, the subvariety V'_s of singular points of V' is at most three-dimensional, so $U_3 := \mathrm{Cl}(\rho(V'_s))$ is also at most three-dimensional. Hence, $U := U_1 \cup U_2 \cup U_3$ is a variety in $\mathbb{C}^6$ of dimension at most 3. We set

$$Z'_0 := \{p \in Z(F) \mid \dim\left((\{p\} \times Z(F)) \cap U\right) \geq 2\}.$$

In other words (using the fact that $\{p\} \times Z(F)$ is irreducible), $p \in Z'_0$ if and only if $\{p\} \times Z(F) \subset U$, so $Z'_0 \times Z(F) \subset U$. Since U is a variety, we have $\mathrm{Cl}(Z'_0) \times Z(F) = \mathrm{Cl}(Z'_0 \times Z(F)) \subset U$. Since U is at most three-dimensional and $Z(F)$ is two-dimensional, we must have that, for $Z_0 := \mathrm{Cl}(Z'_0)$, $\dim Z_0 \leq 1$.

Finally, let $(a, b, c_1) \in Z(F) \backslash Z_0$. By definition of Z_0, we have

$$\dim\left((\{(a, b, c_1)\} \times Z(F)) \cap U\right) \leq 1.$$

Thus there exists a point $(a, b, c_1, a', b', c_4) \in (Z(F) \times Z(F)) \backslash U$. By definition of U, this implies that $(a, b, c_1, a', b', c_4) \in \rho(V') \backslash U$, which in turn means that there exist $c_2, c_3 \in \mathbb{C}$ such that $(a, a', b, b', c_1, c_2, c_3, c_4) \in V' \backslash V_0$ is a regular point of V', as asserted. ◀

Let Z_0 be the variety given by Lemma 3.14.

▶ **Lemma 3.15.** *Let $u = (a, b, c_1) \in Z(F) \backslash Z_0$. Then there exist open sets $D_i \subset \mathbb{C}$ and analytic functions $\varphi_i : D_i \to \mathbb{C}$, for $i = 1, 2, 3$, such that $(a, b, c_1) \in D_1 \times D_2 \times D_3$ and*

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

for every $(x, y, z) \in D_1 \times D_2 \times D_3$.

Proof. By applying Lemma 3.14 to $u = (a, b, c_1)$, we obtain $a', b', c_2, c_3, c_4 \in \mathbb{C}$, such that $v := (a, a', b, b', c_1, c_2, c_3, c_4) \in V' \backslash V_0$ is a regular point of V'. By Lemma 3.3, there exist neighborhoods D_1 of a, D_2 of a', E_1 of b, and E_2 of b', and a mapping

$$\Phi_v : (x, x', y, y') \mapsto \big(g_1(x, y),\ g_2(x, y'),\ g_3(x', y),\ g_4(x', y')\big),$$

analytic over $D_1 \times D_2 \times E_1 \times E_2$, such that its graph is the intersection $V \cap N_v$, for some open neighborhood N_v of v in $\mathbb{C}^8$ (whose π_1-projection is $D_1 \times D_2 \times E_1 \times E_2$). Note that, since v is a regular point of V', $V' \cap N_v$ is necessarily four-dimensional, and so it must coincide with $V \cap N_v$. Thus, restricting the analysis to the neighborhood N_v, we may use V and V' interchangeably in what follows.

Since $V' \subset W$, we have, recalling the definition of the variety W, that

$$G(x, x', y, y', z_1, z_2, z_3, z_4) = 0,$$

for every $(x, x', y, y', z_1, z_2, z_3, z_4) \in V' \cap N_v$. By the implicit function theorem, the functions $g_1, \ldots, g_4$ satisfy, in a suitable neighborhood of v, $g_{1i}(x, y) = -\frac{F_i(x,y,g_1(x,y))}{F_3(x,y,g_1(x,y))}$, and similarly for g_2, g_3, g_4. By the definition of G, this is easily seen to imply that

$$g_{11}(x, y)g_{22}(x, y')g_{32}(x', y)g_{41}(x', y') = g_{12}(x, y)g_{21}(x, y')g_{31}(x', y)g_{42}(x', y'),$$

for every $(x, x', y, y') \in D_1 \times D_2 \times E_1 \times E_2$. In particular, fixing $x' = a'$ and $y' = b'$, there exists an open neighborhood $D_1 \times D_2$ of $(a, b) \in \mathbb{C}^2$, such that, for every $(x, y) \in D_1 \times D_2$,

$$g_{11}(x, y)g_{22}(x, b')g_{32}(a', y)g_{41}(a', b') = g_{12}(x, y)g_{21}(x, b')g_{31}(a', y)g_{42}(a', b'). \tag{3}$$

Because $v \notin V_0$, we have $g_{11}(a, b) = -\frac{F_1(a,b,c_1)}{F_3(a,b,c_1)} \neq 0$. Similarly, $g_{22}(a, b')$, $g_{32}(a', b)$, $g_{41}(a', b')$, $g_{12}(a, b)$, $g_{21}(a, b')$, $g_{31}(a', b)$, and $g_{42}(a', b')$ are all nonzero. The continuity of all the relevant functions implies that, by shrinking $D_1 \times D_2$ if needed, we may assume that neither side of (3) is zero for any $(x, y) \in D_1 \times D_2$. Thus we can rewrite (3) as

$$\frac{g_{11}(x, y)}{p(x)} = \frac{g_{12}(x, y)}{q(y)}, \tag{4}$$

where $p(x) = g_{21}(x, b')g_{42}(a', b')/g_{22}(x, b')$ is analytic and nonzero on D_1 and $q(y) = g_{32}(a', y)g_{41}(a', b')/g_{31}(a', y)$ is analytic and nonzero on D_2. By Lang [7, Theorem III.6.1], there exist analytic primitives φ_1, φ_2 so that $\varphi_1'(x) = p(x)$ on D_1 and $\varphi_2'(y) = q(y)$ on D_2.

We express the function $g_1(x, y)$ in terms of new coordinates (ξ, η), given by

$$\xi = \varphi_1(x) + \varphi_2(y), \quad \eta = \varphi_1(x) - \varphi_2(y). \tag{5}$$

Since p, q are continuous and nonzero at a, b, respectively, it follows that φ_1, φ_2 are injections in suitable respective neighborhoods of a, b, so by shrinking D_1 and D_2 still further, if needed, we may assume that the system (5) is invertible in $D_1 \times D_2$.

Returning to the standard notation, denoting partial derivatives by variable subscripts, we have $\xi_x = \varphi_1'(x)$, $\xi_y = \varphi_2'(y)$, $\eta_x = \varphi_1'(x)$, and $\eta_y = -\varphi_2'(y)$. Using the chain rule, we obtain

$$g_{11} = g_{1\xi}\xi_x + g_{1\eta}\eta_x = \varphi_1'(x)(g_{1\xi} + g_{1\eta}) = p(x)(g_{1\xi} + g_{1\eta})$$

$$g_{12} = g_{1\xi}\xi_y + g_{1\eta}\eta_y = \varphi_2'(y)(g_{1\xi} - g_{1\eta}) = q(y)(g_{1\xi} - g_{1\eta}),$$

which gives $\dfrac{g_{11}(x, y)}{p(x)} - \dfrac{g_{12}(x, y)}{q(y)} \equiv 2g_{1\eta}(x, y)$, on $D_1 \times D_2$. Combining this with (4), we get $g_{1\eta}(x, y) \equiv 0$. This means that g_1 depends only on the variable ξ, so it has the form $g_1(x, y) = \psi(\varphi_1(x)+\varphi_2(y))$, for a suitable analytic function ψ. The analyticity of ψ is an easy consequence of the analyticity of φ_1, φ_2, and g_1, and the fact that $\varphi_1'(x)$ and $\varphi_2'(y)$ are nonzero, combined with repeated applications of the chain rule. Let $E := \{\varphi_1(x) + \varphi_2(y) \mid (x, y) \in D_1 \times D_2\}$ and $D_3 := \{\psi(z) \mid z \in E\}$. We observe that $g_{11}(x, y) = \psi'(\varphi_1(x)+\varphi_2(y)) \cdot p(x)$. As

argued above, we have $g_{11}(x,y) \neq 0$ for all $(x,y) \in D_1 \times D_2$, implying that $\psi'(\varphi_1(x)+\varphi_2(y))$ is nonzero for $(x,y) \in D_1 \times D_2$. Therefore, $\psi : E \to D_3$ is invertible by the inverse mapping theorem (see [5]).

Letting $\varphi_3(z) := -\psi^{-1}(z)$, we get for $(x,y,z) \in D_1 \times D_2 \times D_3$ that $\varphi_1(x)+\varphi_2(y)+\varphi_3(z) = 0$ if and only if $(x,y,z) \in Z(F) \cap (D_1 \times D_2 \times D_3)$. This completes the proof of the lemma. ◀

Finally, Lemma 3.15 has established that F satisfies property (ii) of the theorem, which completes the proof of Proposition 2.3 for this case. ◀

Acknowledgements. Part of this research was performed while the authors were visiting the Institute for Pure and Applied Mathematics (IPAM), which is supported by the National Science Foundation. The authors deeply appreciate the stimulating environment and facilities provided by IPAM, which have facilitated the intensive and productive collaboration that have lead to this paper. The authors would also like to thank Hong Wang, Kaloyan Slavov and József Solymosi for several helpful discussions. Some of the insights in our analysis were inspired by talks given by Terry Tao at IPAM about his work [14].

References

1 G. Elekes and L. Rónyai, A combinatorial problem on polynomials and rational functions, *J. Combinat. Theory Ser. A* 89 (2000), 1–20.
2 G. Elekes and E. Szabó, How to find groups? (And how to use them in Erdős geometry?), *Combinatorica* 32 (2012), 537–571.
3 G. Elekes and E. Szabó, On triple lines and cubic curves: The Orchard Problem revisited, in `arXiv:1302.5777` (2013).
4 G. Elekes, M. Simonovits, and E. Szabó, A combinatorial distinction between unit circles and straight lines: How many coincidences can they have?, *Combinat. Probab. Comput.* 18 (2009), 691–705.
5 K. Fritzsche and H. Grauert, *From Holomorphic Functions to Complex Manifolds*, Springer-Verlag, New York, 2002.
6 L. Guth and N. H. Katz, On the Erdős distinct distances problem in the plane, Annals Math. 18 (2015), 155–190.
7 S. Lang, *Complex Analysis*, Springer-Verlag, New York, 1999.
8 J. Pach and F. de Zeeuw, Distinct distances on algebraic curves in the plane, in `arXiv:1308.0177` (2013).
9 O. E. Raz, M. Sharir, and J. Solymosi, Polynomials vanishing on grids: The Elekes-Rónyai problem revisited, *Amer. J. Math.*, to appear. Also in *Proc. 30th Annu. Sympos. Comput. Geom.*, 2014, 251–260. Also in `arXiv:1401.7419` (2014).
10 O. E. Raz, M. Sharir, and J. Solymosi, On triple intersections of three families of unit circles, *Proc. 30th Annu. Sympos. Comput. Geom.*, 2014, 198–205. Also in `arXiv:1407.6625` (2014).
11 M. Sharir, A. Sheffer, and J. Solymosi, Distinct distances on two lines, *J. Combinat. Theory Ser. A* 120 (2013), 1732–1736.
12 M. Sharir and J. Solymosi, Distinct distances from three points, *Combinat. Probab. Comput.*, to appear. Also in `arXiv:1308.0814` (2013).
13 J. Solymosi and F. de Zeeuw, Incidence bounds for complex algebraic curves on Cartesian products, in `arXiv:1502.05304` (2015).
14 T. Tao, Expanding polynomials over finite fields of large characteristic, and a regularity lemma for definable sets, in `arXiv:1211.2894` (2012).
15 T. Tao, *Bézout's inequality*, `http://terrytao.wordpress.com/2011/03/23/bezouts-inequality`.