Beck's theorem for plane curves

Mario Huicochea
CONACyT/UAZ
Zacatecas, México
dym@cimat.mx

Submitted: Jun 18, 2020; Accepted: Dec 14, 2020; Published: Dec 24, 2020

Abstract

Let $d \in \mathbb{Z}^+$, $\mathbb{K}$ be a field of characteristic zero and A be a nonempty finite subset of $\mathbb{K}^2$. Denote by $\mathcal{C}_{d,\mathbb{K}}$ the family of algebraic curves of degree d in $\mathbb{K}^2$ and $\mathcal{C}_{\leqslant d,\mathbb{K}} := \bigcup_{e=1}^{d} \mathcal{C}_{e,\mathbb{K}}$. For any $C_1 \in \mathcal{C}_{d,\mathbb{K}}$, we say that C_1 is determined by A if for any $C_2 \in \mathcal{C}_{d,\mathbb{K}}$ such that $C_2 \cap A \supseteq C_1 \cap A$, we have that $C_1 = C_2$; we denote by $\mathcal{D}_{d,\mathbb{K}}(A)$ the family of elements of $\mathcal{C}_{d,\mathbb{K}}$ determined by A. Beck's theorem establishes that if $\mathbb{K} = \mathbb{R}$ and A is not collinear, then

$$|\mathcal{D}_{1,\mathbb{R}}(A)| = \Theta\left(|A| \min_{C \in \mathcal{C}_{1,\mathbb{R}}} |A \setminus C|\right).$$

In this paper we generalize Beck's theorem showing that for all $d \in \mathbb{Z}^+$, there exists a constant $c = c(d) > 0$ such that if $\min_{C \in \mathcal{C}_{\leqslant d,\mathbb{K}}} |A \setminus C| > c$, then

$$|\mathcal{D}_{d,\mathbb{K}}(A)| = \Theta_d\left(|A|^d \prod_{e=1}^{d} \left(\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C|\right)^{d-e+1}\right).$$

Mathematics Subject Classifications: 14N10, 52C10

1 Introduction

In this paper $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}^+, \mathbb{Z}_0^+$ denote the set of real numbers, complex numbers, rational numbers, integers, positive integers and nonnegative integers, respectively. For any $n, m \in \mathbb{Z}$, we write $[n, m] := \{k \in \mathbb{Z} : \ n \leqslant k \leqslant m\}$. Let $d, n \in \mathbb{Z}^+$ and $\mathbb{K}$ be a field of characteristic zero. A *(plane) curve of degree d in $\mathbb{K}^2$* is a subset C of $\mathbb{K}^2$ which is the zero set of a polynomial in $\mathbb{K}[x, y]$ of degree d; we denote by $\mathcal{C}_{d,\mathbb{K}}$ the family of curves of degree d in $\mathbb{K}^2$ and $\mathcal{C}_{\leqslant d,\mathbb{K}} := \bigcup_{e=1}^{d} \mathcal{C}_{e,\mathbb{K}}$. For each nonempty finite subset A of $\mathbb{K}^2$, we say that $C_1 \in \mathcal{C}_{d,\mathbb{K}}$ is *determined by A* if for any $C_2 \in \mathcal{C}_{d,\mathbb{K}}$ satisfying that $C_2 \cap A \supseteq C_1 \cap A$, we have that $C_1 = C_2$; we denote by $\mathcal{D}_{d,\mathbb{K}}(A)$ the family of elements

of $\mathcal{C}_{d,\mathbb{K}}$ which are determined by A. Thus, for instance, $\mathcal{D}_{1,\mathbb{K}}(A)$ is the family of lines L in $\mathbb{K}^2$ such that $|L \cap A| \geqslant 2$. Denote by $S_{\mathbb{K}}$ the family of finite subsets of $\mathbb{K}^2$. As usual, for any maps $\varphi, \tau : S_{\mathbb{K}} \to \mathbb{R}$ and parameters $d_1, d_2, \ldots$, we write $\varphi(A) = O_{d_1,d_2,\ldots}(\tau(A))$ (resp. $\varphi(A) = \Omega_{d_1,d_2,\ldots}(\tau(A))$) if there are constants $c = c(d_1, d_2, \ldots), c' = c'(d_1, d_2, \ldots)$ such that for all $A \in S_{\mathbb{K}}$ satisfying that $|A| \geqslant c$, we have that $\varphi(A) \leqslant c'\tau(A)$ (resp. $\varphi(A) \geqslant c'\tau(A)$); the notation $\varphi(A) = \Theta_{d_1,d_2,\ldots}(\tau(A))$ means that $\varphi(A) = O_{d_1,d_2,\ldots}(\tau(A))$ and $\varphi(A) = \Omega_{d_1,d_2,\ldots}(\tau(A))$.

An important problem in combinatorial geometry is to know how many lines are determined by a nonempty finite subset of $\mathbb{R}^2$. P. Erdős conjectured in [8](see also [9], [10]) that if A is a nonempty finite subset of $\mathbb{R}^2$ which is not collinear, then $|\mathcal{D}_{1,\mathbb{R}}(A)| = \Omega\left(|A| \min_{C\in\mathcal{C}_{1,\mathbb{R}}} |A \setminus C|\right)$. L. M. Kelly and W. Moser proved in [15, Thm. 4.1] that if $|A| = \Omega(\min_{C\in\mathcal{C}_{1,\mathbb{R}}} |A \setminus C|^2)$, then the conjecture of Erdős holds. Later in [1], J. Beck proved the conjecture of Erdős unconditionally. Beck's theorem can be stated as follows.

Theorem 1. *Let A be a finite subset of $\mathbb{R}^2$ such that $\min_{C\in\mathcal{C}_{1,\mathbb{R}}} |A \setminus C| \geqslant 1$. Then*

$$|\mathcal{D}_{1,\mathbb{R}}(A)| = \Theta\left(|A| \min_{C\in\mathcal{C}_{1,\mathbb{R}}} |A \setminus C|\right).$$

Proof. See [1, Thm. 1.2]. □

Beck's theorem has important applications in different areas of mathematics, and it has opened a new research field in combinatorial geometry, see for instance [1], [4], [6], [7], [13], [16]. Another important family of problems in combinatorial geometry is to bound the number of curves with a given degree that are determined by A and satisfy other conditions (for example, in the Sylvester-Gallai type results, the curves have to pass through few points of A), see for instance [2], [3], [5], [19]. Thus it seems natural and important to ask if Beck's theorem can be generalized for conics, cubics, etc. and arbitrary fields. This question is the motivation for the main result of this paper.

Theorem 2. *For any $d \in \mathbb{Z}^+$, there is $c_1 = c_1(d) > 0$ with the following property. Let $\mathbb{K}$ be a field of characteristic zero and A be a finite subset of $\mathbb{K}^2$ such that $\min_{C\in\mathcal{C}_{\leqslant d,\mathbb{K}}} |A\setminus C| \geqslant c_1$. Then*

$$|\mathcal{D}_{d,\mathbb{K}}(A)| = \Theta_d\left(|A|^d \prod_{e=1}^{d} \left(\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C|\right)^{d-e+1}\right).$$

A number of consequences can be obtained from Theorem 2. An immediate consequence of Theorem 2 is a lower bound of the number of curves of degree d determined by A.

Corollary 3. *For any $d \in \mathbb{Z}^+$, there is $c_1 = c_1(d) > 0$ with the following property. Let $\mathbb{K}$ be a field of characteristic zero and A be a finite subset of $\mathbb{K}^2$ such that $\min_{C\in\mathcal{C}_{\leqslant d,\mathbb{K}}} |A\setminus C| \geqslant c_1$. Then*

$$|\mathcal{D}_{d,\mathbb{K}}(A)| = \Omega_d\left(|A|^d\right).$$

A straightforward consequence of Theorem 1 is that there is a line which contains several points of A or A determines a quadratic number of lines. Using Theorem 2, we can generalize this for curves.

Corollary 4. *For any $d \in \mathbb{Z}^+$, there are $c_1 = c_1(d), c_2 = c_2(d), c_3 = c_3(d) > 0$ with the following property. Let $\mathbb{K}$ be a field of characteristic zero, A be a finite subset of $\mathbb{K}^2$ such that $\min_{C \in \mathcal{C}_{\leqslant d,\mathbb{K}}} |A \setminus C| \geqslant c_1$ and $e \in [1, d]$. Then one of the following claims holds:*

i) There is $C \in \mathcal{C}_{\leqslant e,\mathbb{K}}$ such that $|A \cap C| \geqslant c_2|A|$.

ii) $|\mathcal{D}_{d,\mathbb{K}}(A)| \geqslant c_3|A|^{d+e(d-\frac{e-1}{2})}$.

The proof of Theorem 2 has 3 main steps that we sketch now.

- Using the Veronese map $\psi_{d,\mathbb{K}} : \mathbb{K}^2 \to \mathbb{K}^{\frac{d(d+3)}{2}}$, the problem of counting curves of degree d determined by A in $\mathbb{K}^2$ is almost equivalent to count the number of hyperplanes in $\mathbb{K}^{\frac{d(d+3)}{2}}$ which are generated (as flats) by $\psi_{d,\mathbb{K}}(A)$. This is a consequence of Corollary 7 and Lemma 12.

- The number of hyperplanes in $\mathbb{C}^{\frac{d(d+3)}{2}}$ generated by $\psi_{d,\mathbb{C}}(A)$ can be bounded using Lund's theorem (see Theorem 10). Lund's theorem is given in terms of essential dimension, maximal subsets with a given essential dimension, etc. Hence, to be able to conclude the proof of Theorem 2 when $\mathbb{K} = \mathbb{C}$, we need to translate the information about flats in $\mathbb{C}^{\frac{d(d+3)}{2}}$ provided by Lund's theorem into the information about curves in $\mathbb{C}^2$. The tools we use to do this are well known properties of the Veronese map and Bezout's theorem (see Theorem 5). The key lemma in this part of the proof is Lemma 16.

- Lund's theorem works only for $\mathbb{K} = \mathbb{C}$ (and $\mathbb{K} = \mathbb{R}$) so, to conclude the proof of Theorem 2 for arbitrary fields of characteristic zero, we need a Lefschetz principle type results. In this part of the proof of Theorem 2, Lemma 18 is the result that allows us complete the proof for arbitrary fields of characteristic zero.

This paper is organized as follows. In Section 2 we state some auxiliary results. As it is explained above, we need to bound the number of hyperplanes generated by the image of A under the Veronese map, and then to translate this information into the original problem. This is done in Section 3. The conclusion of the proof of Theorem 2 is given in Section 4. Also, after we conclude the proof of Theorem 2, we discuss some facts about the constants in Theorem 2, possible generalizations, etc.

2 Preliminaries

In this section we state some results needed in the proof of Theorem 2.

Let $\mathbb{K}$ be a field and $n \in \mathbb{Z}^+$. For any $q(x_1, x_2, \ldots, x_n) \in \mathbb{K}[x_1, x_2, \ldots, x_n]$, we denote by $\mathcal{Z}(q(x_1, x_2, \ldots, x_n))$ its zero set in $\mathbb{K}^n$ and by $\deg(p(x_1, x_2, \ldots, x_n))$ its degree. We

say that $p(x,y) \in \mathbb{K}[x,y]$ is *irreducible* if $\deg(p(x,y)) > 0$ and for any factorization $p(x,y) = p_1(x,y)p_2(x,y)$, we get that $p_i(x,y) \in \mathbb{K}$ for some $i \in \{1,2\}$. We say that $\mathcal{Z}(p(x,y))$ is *irreducible* if $p(x,y)$ is irreducible. We start with a weak version of Bezout's theorem.

Theorem 5. *Let $\mathbb{K}$ be a field of characteristic zero and $C_1, C_2 \in \mathcal{C}_{d,\mathbb{K}}$ be irreducible. If $C_1 \neq C_2$, then*

$$|C_1 \cap C_2| \leqslant d^2.$$

Proof. See [12, Cor. I.7.8]. □

The curves $C = \mathcal{Z}(p(x,y))$ are not always uniquely determined by the polynomial $p(x,y)$ (for instance, $\mathcal{Z}(x+y) = \mathcal{Z}((x+y)^2)$). However, as we will see later, the next lemma is a useful tool to know when $\mathcal{Z}(p(x,y)) = \mathcal{Z}(q(x,y))$ with $p(x,y)$ irreducible.

Lemma 6. *Let $\mathbb{K}$ be a field and $p(x,y), q(x,y) \in \mathbb{K}[x,y]$ with $p(x,y)$ an irreducible polynomial. If $q(x,y)$ is not divisible by $p(x,y)$, then $\mathcal{Z}(p(x,y)) \cap \mathcal{Z}(q(x,y))$ is finite.*

Proof. See [17, Ch. 1.1]. □

Let $d \in \mathbb{Z}^+$ and $\mathbb{K}$ a field of characteristic zero. Write

$$\mathbb{K}_d[x,y] := \{p(x,y) \in \mathbb{K}[x,y] : \ \deg(p(x,y)) \in [1,d]\}.$$

In $\mathbb{K}[x,y]$, we define the relation $p(x,y) \sim q(x,y)$ if there is $r \in \mathbb{K} \setminus \{0\}$ such that $p(x,y) = r \cdot q(x,y)$, and we denote by $[p(x,y)]$ the class of $p(x,y)$ and by $\mathbb{K}[x,y]/\sim$ the set of classes. For any subset X of $\mathbb{K}[x,y]$, we write

$$X/\sim := \{[p(x,y)] \in \mathbb{K}[x,y]/\sim : \ [p(x,y)] \cap X \neq \emptyset\}.$$

Note that for any $p(x,y), q(x,y) \in \mathbb{K}[x,y]$ such that $[p(x,y)] = [q(x,y)]$, we have that $\deg(p(x,y)) = \deg(q(x,y))$ and $\mathcal{Z}(p(x,y)) = \mathcal{Z}(q(x,y))$; thus the map $\sigma_{d,\mathbb{K}}$ defined below is well defined

$$\sigma_{d,\mathbb{K}} : \mathbb{K}_d[x,y]/\sim \longrightarrow \mathcal{C}_{\leqslant d,\mathbb{K}}, \qquad \sigma_{d,\mathbb{K}}([p(x,y)]) = \mathcal{Z}(p(x,y)).$$

Let $p(x,y) \in \mathbb{K}[x,y]$ be such that $\deg(p(x,y)) > 0$ and consider a factorization $p(x,y) = r\prod_{i=1}^{n} p_i(x,y)^{m_i}$ with $m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$, $r \in \mathbb{K}$, $[p_i(x,y)] \neq [p_j(x,y)]$ for all $i,j \in [1,n]$ such that $i \neq j$, and $p_i(x,y)$ irreducible for each $i \in [1,n]$. Then the irreducible curves $\mathcal{Z}(p_1(x,y)), \mathcal{Z}(p_2(x,y)), \ldots, \mathcal{Z}(p_n(x,y))$ are known as the *irreducible components of* $\mathcal{Z}(p(x,y))$. The irreducible components satisfy that

$$\mathcal{Z}(p(x,y)) = \bigcup_{i=1}^{n} \mathcal{Z}(p_i(x,y)) = \mathcal{Z}\left(\prod_{i=1}^{n} p_i(x,y)\right)$$

and

$$\deg(p(x,y)) = \sum_{i=1}^{n} m_i \deg(p_i(x,y)) \geqslant \sum_{i=1}^{n} \deg(p_i(x,y)).$$

For any $q(x,y) \in \mathbb{K}[x,y]$ such that $\mathcal{Z}(p(x,y)) = \mathcal{Z}(q(x,y))$, take a factorization $q(x,y) = s\prod_{i=1}^{l} q_i(x,y)^{k_i}$ with $k_1, k_2, \ldots, k_l \in \mathbb{Z}^+$, $s \in \mathbb{K}$, $[q_i(x,y)] \neq [q_j(x,y)]$ for all $i,j \in [1,l]$ such that $i \neq j$, and $q_i(x,y)$ irreducible for each $i \in [1,l]$. Since $\mathbb{K}$ is infinite, we have that $\mathcal{Z}(p_1(x,y)), \ldots \mathcal{Z}(p_n(x,y)), \mathcal{Z}(q_1(x,y)), \ldots \mathcal{Z}(q_l(x,y))$ are infinite sets. On the one hand, for each $i \in [1,n]$, we have that $\mathcal{Z}(p_i(x,y)) \subseteq \mathcal{Z}(p(x,y)) = \mathcal{Z}(q(x,y))$ so Lemma 6 applied to $p_i(x,y)$ and $q(x,y)$ implies that $p_i(x,y)$ divides $q(x,y)$. On the other hand, for each $i \in [1,l]$, we have that $\mathcal{Z}(q_i(x,y)) \subseteq \mathcal{Z}(q(x,y)) = \mathcal{Z}(p(x,y))$ so Lemma 6 applied to $q_i(x,y)$ and $p(x,y)$ implies that $q_i(x,y)$ divides $p(x,y)$. Hence, since $\mathbb{K}[x,y]$ is a unique factorization domain, we get that $q(x,y) = t\prod_{i=1}^{n} p_i(x,y)^{k_i}$ for some $k_1, k_2, \ldots, k_n \in \mathbb{Z}^+$ and $t \in \mathbb{K}$. As a consequence of these facts, the irreducible components of C do not depend on the polynomial from which C is the zero set, and we get the following corollary.

Corollary 7. *Let $\mathbb{K}$ be field of characteristic zero, $d \in \mathbb{Z}^+$ and $C \in \mathcal{C}_{\leqslant d,\mathbb{K}}$ with pairwise distinct irreducible components $\mathcal{Z}(p_1(x,y)), \mathcal{Z}(p_2(x,y)), \ldots, \mathcal{Z}(p_n(x,y))$. Then*

$$\sigma_{d,\mathbb{K}}^{-1}(C) = \left\{ \left[\prod_{i=1}^{n} p_i^{m_i} \right] \in \mathbb{K}_d[x,y]/\sim:\ m_1, m_2, \ldots, m_n \in \mathbb{Z}^+,\ \sum_{i=1}^{n} m_i \deg(p_i) \leqslant d \right\}.$$

Since the number of solutions $(m_1, m_2, \ldots, m_n) \in \mathbb{Z}^{+n}$ of $\sum_{i=1}^{n} m_i \deg(p_i) \leqslant d$ is bounded by d^d, we get in particular that

$$|\sigma_{d,\mathbb{K}}^{-1}(C)| \leqslant d^d.$$

Let $\mathbb{K}$ be a field and $d, e \in \mathbb{Z}_0^+$ with $e \leqslant d$. A translation F of a vectorial subspace V of $\mathbb{K}^d$ will be called a *flat*. We write $\dim F := \dim V$, and also if V is an e-dimensional subspace, we say that F is an e-flat; in particular, 1-flats are lines and $d-1$-flats are hyperplanes. The family of e-flats in $\mathbb{K}^d$ will be denoted by $\mathcal{G}_{e,\mathbb{K}}$. For any subset S of $\mathbb{K}^d$, we denote by $\mathrm{Fl}(S)$ the smallest flat (with respect to $\subseteq$) which contains S and we write $\dim S := \dim \mathrm{Fl}(S)$. If $S = \{\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n\}$, we write $\mathrm{Fl}(\mathbf{s}_1, \mathbf{s}_2, \ldots, \mathbf{s}_n) := \mathrm{Fl}(S)$. The family of e-flats F in $\mathbb{K}^d$ such that there is a subset R of S satisfying that $F = \mathrm{Fl}(R)$ will be denoted by $\mathcal{G}_{e,\mathbb{K}}(S)$.

A fundamental tool in this paper is the Veronese map. Let $d \in \mathbb{Z}^+$ and $\mathbb{K}$ be a field. Write $I_d := \left\{ (n,m) \in \mathbb{Z}_0^{+2} :\ n+m \in [1,d] \right\}$ so $|I_d| = \binom{d+2}{2} - 1 = \frac{d(d+3)}{2}$. The *$d$-Veronese map* is the map

$$\psi_{d,\mathbb{K}} : \mathbb{K}^2 \longrightarrow \mathbb{K}^{\frac{d(d+3)}{2}}, \qquad \psi_{d,\mathbb{K}}(a_1, a_2) = \left(a_1^n a_2^m\right)_{(n,m)\in I_d}.$$

To avoid confusion, the ring of polynomials which corresponds to $\mathbb{K}^2$ will be denoted by $\mathbb{K}[x,y]$ and the ring of polynomials which corresponds to $\mathbb{K}^{\frac{d(d+3)}{2}}$ will be denoted by $\mathbb{K}[z_{(n,m)}]_{(n,m)\in I_d}$. The Veronese map has some well-known properties that we will need later. The proof of the following facts can be found in standard algebraic geometry books, see for instance [12, Ch. I], [17, Ch. 1].

Remark 8. Let $d \in \mathbb{Z}^+$ and $\mathbb{K}$ be a field of characteristic zero.

i) The map $\psi_{d,\mathbb{K}}$ is an isomorphism onto its image.

ii) The map

$$\tau_{d,\mathbb{K}} : \mathbb{K}_d[x,y]/\sim \longrightarrow \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{K}},$$

$$\tau_{d,\mathbb{K}}\left(\left[r_{(0,0)} + \sum_{(n,m)\in I_d} r_{(n,m)}x^n y^m\right]\right) = \mathcal{Z}\left(r_{(0,0)} + \sum_{(n,m)\in I_d} r_{(n,m)}z_{(n,m)}\right)$$

is a bijection. Note that for any $[p(x,y)] \in \mathbb{K}_d[x,y]/\sim$, we have that

$$\psi_{d,\mathbb{K}}(\mathcal{Z}(p(x,y))) = \tau_{d,\mathbb{K}}([p(x,y)]) \cap \psi_{d,\mathbb{K}}(\mathbb{K}^2).$$

Another important property of $\psi_{d,\mathbb{K}}$ is that the image of any $d+1$ elements of $\mathbb{K}^2$ cannot be contained in a $d-1$-flat.

Theorem 9. *Let $d \in \mathbb{Z}^+$, $\mathbb{K}$ be a field and A a subset of $\mathbb{K}^2$. If $|A| > d$, then $\dim \psi_{d,\mathbb{K}}(A) \geqslant d$.*

Proof. See [14, Thm. 1.1]. □

Let $d \in \mathbb{Z}^+$ and S be a nonempty subset of $\mathbb{C}^d$. The smallest $e \in \mathbb{Z}_0^+$ such that there is a collection of flats $\{F_i\}_{i\in I}$ in $\mathbb{C}^d$ satisfying that

- $S \subseteq \bigcup_{i\in I} F_i$
- $\dim F_i \geqslant 1$ for all $i \in I$
- $\sum_{i\in I} \dim F_i = e$

will be called the *essential dimension* of S and we will denote it by $\overline{\dim}\, S$. For instance, if S is the union of two skew lines in $\mathbb{C}^3$, then $\dim S = 3$ and $\overline{\dim}\, S = 2$. For each $e \in [0,d]$, denote by $\mathcal{F}_e(S)$ the family of subsets R of S such that $\overline{\dim}\, R \leqslant e$, and we write

$$\phi_e(S) := \max_{R\in\mathcal{F}_e(S)} |R|.$$

In other words, $\phi_e(S)$ is the maximum size which can have a subset of S with essential dimension at most e. A fundamental tool in the proof of Theorem 2 is the following weak version of a theorem showed by B. Lund.

Theorem 10. *For any $e \in \mathbb{Z}^+$, there is $c_5 = c_5(e) > 0$ with the following property. Let $d \in \mathbb{Z}^+$ be such that $d \geqslant e$ and S be a subset of $\mathbb{C}^d$ such that $|S| - \phi_e(S) \geqslant c_5$. Then*

$$|\mathcal{G}_{e,\mathbb{C}}(S)| = \Theta_e\left(\prod_{f=0}^{e}(|S| - \phi_f(S))\right).$$

Proof. See [16, Thm. 2]. □

We conclude this section with a Lefschetz principle type result.

Theorem 11. *Let $\mathbb{K}$ be a finitely generated field over $\mathbb{Q}$. Then there is an injective morphism of fields $\rho : \mathbb{K} \longrightarrow \mathbb{C}$.*

Proof. See [18, Prop. 4]. □

3 Curves and hyperplanes

In this section we prove some results which are needed in the proof of Theorem 2. The first result of this section shows that for any field $\mathbb{K}$ of characteristic zero, there is an important relation between the family of hyperplanes generated by $\psi_{d,\mathbb{K}}(A)$ in $\mathbb{K}^{\frac{d(d+3)}{2}}$ and the family of curves of degree d in $\mathbb{K}^2$ determined by A. This is done using the maps $\sigma_{d,\mathbb{K}}$ and $\tau_{d,\mathbb{K}}$ defined in the previous section.

Lemma 12. *Let $d \in \mathbb{Z}^+$, $\mathbb{K}$ be a field of characteristic zero and A be a nonempty subset of $\mathbb{K}^2$ satisfying that there is no element of $\mathcal{C}_{\leqslant d,\mathbb{K}}$ which contains A. Then*

$$\tau_{d,\mathbb{K}}\left(\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right) = \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{K}}(\psi_{d,\mathbb{K}}(A)).$$

Proof. Write $\tau := \tau_{d,\mathbb{K}}, \sigma := \sigma_{d,\mathbb{K}}, \psi := \psi_{d,\mathbb{K}}, \mathcal{D} := \mathcal{D}_{d,\mathbb{K}}(A)$ and $\mathcal{G} := \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{K}}(\psi_{d,\mathbb{K}}(A))$. First we show that

$$\tau(\sigma^{-1}(\mathcal{D})) \subseteq \mathcal{G}. \tag{1}$$

Take $[p_1] \in \sigma^{-1}(\mathcal{D})$ and write $C_1 := \mathcal{Z}(p_1)$. From Remark 8.ii, we know that $\tau([p_1]) \in \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{K}}$ and

$$\psi(C_1 \cap A) \subseteq \psi(C_1) = \tau([p_1]) \cap \psi(\mathbb{K}^2) \subseteq \tau([p_1]);$$

in particular, $\mathrm{Fl}(\psi(C_1 \cap A)) \subseteq \tau([p_1])$. By contradiction, we prove that

$$\mathrm{Fl}(\psi(C_1 \cap A)) = \tau([p_1]). \tag{2}$$

If $\mathrm{Fl}(\psi(C_1 \cap A))$ is contained properly in $\tau([p_1])$, then

$$\dim \mathrm{Fl}(\psi(C_1 \cap A)) < \dim \tau([p_1]) = \frac{d(d+3)}{2} - 1.$$

Since A is not contained in an element of $\mathcal{C}_{\leqslant d,\mathbb{K}}$ by assumption, we get that $A \nsubseteq C_1$. Take $\mathbf{a} \in A \setminus C_1$. Since $\dim \mathrm{Fl}(\psi(C_1 \cap A)) < \frac{d(d+3)}{2} - 1$, there is a hyperplane H in $\mathbb{K}^{\frac{d(d+3)}{2}}$ such that it contains $\{\psi(\mathbf{a})\}$ and $\mathrm{Fl}(\psi(C_1 \cap A))$. From Remark 8.ii, there is $[p] \in \mathbb{K}_d[x,y]/\sim$ such that $\tau([p]) = H$. Write $C := \mathcal{Z}(p)$. Insomuch as $\psi(C_1 \cap A) \subseteq H = \tau([p])$, Remark 8.ii leads to

$$\psi(C_1 \cap A) \subseteq \tau([p]) \cap \psi(\mathbb{K}^2) = \psi(C),$$

and the injectivity of ψ yields that $C_1 \cap A \subseteq C \cap A$. We construct a curve C_2 as follows.

- Assume that $\deg(p) = d$. Write $C_2 := C$. On the one hand, since $\mathbf{a} \notin C_1$ and $\mathbf{a} \in \psi^{-1}(H) = C$, we get that $C_1 \neq C_2$. On the other hand, $C_1 \cap A \subseteq C \cap A = C_2 \cap A$.
- Assume that $\deg(p) < d$. Choose a polynomial $q(x,y) \in \mathbb{K}[x,y]$ such that $\deg(q) = d - \deg(p)$. Write $C_2 := \mathcal{Z}(pq)$. Since $\deg(q) = d - \deg(p)$, we get that $C_2 \in \mathcal{C}_{d,\mathbb{K}}$. Inasmuch as $\mathbf{a} \notin C_1$ and $\mathbf{a} \in \psi^{-1}(H) = C \subseteq C_2$, we have that $C_1 \neq C_2$. Since $C_1 \cap A \subseteq C \cap A = \mathcal{Z}(p(x,y)) \cap A$, we get that $C_1 \cap A \subseteq \mathcal{Z}(p(x,y)q(x,y)) \cap A = C_2 \cap A$.

In any case we constructed a $C_2 \in \mathcal{C}_{d,\mathbb{K}} \setminus \{C_1\}$ such that $C_1 \cap A \subseteq C_2 \cap A$; however, this is impossible since $C_1 \in \mathcal{D}$. Thereby (2) is true and this implies that $\tau([p_1]) \in \mathcal{G}$ concluding the proof of (1).

Now we show that

$$\tau(\sigma^{-1}(\mathcal{D})) \supseteq \mathcal{G}. \tag{3}$$

Take $H_1 \in \mathcal{G}$. Remark 8.ii implies that there is $[p_1] \in \mathbb{K}_d[x,y]/\sim$ such that $\tau([p_1]) = H_1$. Write $C_1 := \mathcal{Z}(p_1)$ so $\psi(C_1) = H_1 \cap \psi(\mathbb{K}^2)$ by Remark 8.ii. Since H_1 is generated as a flat by elements of $\psi(A)$, we get that

$$H_1 = \mathrm{Fl}(H_1 \cap \psi(A)) = \mathrm{Fl}(\psi(C_1) \cap \psi(A)) = \mathrm{Fl}(\psi(C_1 \cap A)). \tag{4}$$

We prove by contradiction that $\deg(p_1) = d$. If $\deg(p_1) < d$, then we can take $q \in \mathbb{K}[x,y]$ such that $\deg(q) = d - \deg(p_1)$, and write $C := \mathcal{Z}(p_1 \cdot q)$. Since $\deg(p_1) < \deg(p_1 \cdot q)$, we get that $[p_1] \neq [p_1 \cdot q]$. Now

$$C_1 \cap A = \mathcal{Z}(p_1) \cap A \subseteq \mathcal{Z}(p_1 \cdot q) \cap A = C \cap A$$

so (4) leads to

$$\tau([p_1]) = H_1 = \mathrm{Fl}(\psi(C_1 \cap A)) \subseteq \mathrm{Fl}(\psi(C \cap A)) \subseteq \mathrm{Fl}(\psi(C)) \subseteq \tau([p_1 \cdot q]),$$

but this is impossible since both $\tau([p_1])$ and $\tau([p_1 \cdot q])$ are different hyperplanes (because $[p_1] \neq [p_1 \cdot q]$). Therefore $\deg(p_1) = d$. It remains to prove that C_1 is determined by A. Assume that there is $C_2 \in \mathcal{C}_{d,\mathbb{K}}$ such that $C_1 \cap A \subseteq C_2 \cap A$, and fix $[p_2] \in \mathbb{K}_d[x,y]/\sim$ such that $C_2 = \mathcal{Z}(p_2)$. Then $\psi(C_1 \cap A) \subseteq \psi(C_2 \cap A)$, and (4) leads to

$$\tau([p_1]) = H_1 = \mathrm{Fl}(\psi(C_1 \cap A)) \subseteq \mathrm{Fl}(\psi(C_2 \cap A)) \subseteq \mathrm{Fl}(\psi(C_2)) \subseteq \tau([p_2]).$$

Thereby, since $\tau([p_1])$ and $\tau([p_2])$ are hyperplanes, the previous inclusion implies that $\tau([p_1]) = \tau([p_2])$; from Remark 8.ii, this gives that $[p_1] = [p_2]$ and then $C_1 = C_2$. This shows that $C_1 \in \mathcal{D}$, and it proves (3). The lemma is a consequence of (1) and (3). □

For technical reasons, write $\mathcal{C}_{\leqslant 0,\mathbb{K}} := \emptyset$ for any field $\mathbb{K}$.

Lemma 13. *Let $\mathbb{K}$ be a field of characteristic zero and C be a curve in $\mathbb{K}^2$. For any $d \in \mathbb{Z}_0^+$, there is a subset A of $\mathbb{K}^2 \setminus C$ such that $|A| = \binom{d+2}{2}$ and there is no element of $\mathcal{C}_{\leqslant d,\mathbb{K}}$ which contains A.*

Proof. Since $\mathbb{K}^2$ is a surface and C a curve, we have that $\mathbb{K}^2 \setminus C \neq \emptyset$. Therefore, if $d = 0$, the statement holds taking $A = \{\mathbf{a}\}$ for some $\mathbf{a} \in \mathbb{K}^2 \setminus C$.

We assume that $d > 0$ from now on. Write $\psi := \psi_{d,\mathbb{K}}$, $\tau := \tau_{d,\mathbb{K}}$, $\mathcal{G} := \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{K}}$ and $\mathcal{C} := \mathcal{C}_{\leqslant d,\mathbb{K}}$. We claim for all $H \in \mathcal{G}$, we have that H does not contain $\psi(\mathbb{K}^2 \setminus C)$. Indeed, assume that there is $H \in \mathcal{G}$ such that $\psi(\mathbb{K}^2 \setminus C) \subseteq H$. From Remark 8.ii, there is $[p] \in \mathbb{K}_d[x,y]/\sim$ such that $H = \tau([p])$. Hence, since $\psi(\mathcal{Z}(p)) = H \cap \psi(\mathbb{K}^2)$ by Remark 8.ii, we get that $\psi(\mathbb{K}^2 \setminus C) \subseteq \psi(\mathcal{Z}(p))$. Since ψ is injective by Remark 8.i, the last inclusion leads to $\mathbb{K}^2 \subseteq C \cup \mathcal{Z}(p)$; however, this is impossible since $\mathbb{K}^2$ is a surface

while $C \cup \mathcal{Z}(p)$ is a curve. The fact that there is no hyperplane in $\mathbb{K}^{\frac{d(d+3)}{2}}$ which contains $\psi(\mathbb{K}^2 \setminus C)$ leads to $\dim \psi(\mathbb{K}^2 \setminus C) = \frac{d(d+3)}{2}$. Therefore there exists $S \subseteq \psi(\mathbb{K}^2 \setminus C)$ such that $|S| = \binom{d+2}{2} = \frac{d(d+3)}{2} + 1$ and $\dim S = \frac{d(d+3)}{2}$. Write $A := \psi^{-1}(S)$ so $|A| = |S| = \binom{d+2}{2}$. On the one hand, $A \subseteq \mathbb{K}^2 \setminus C$ since $S \subseteq \psi(\mathbb{K}^2 \setminus C)$. On the other hand, $\dim S = \frac{d(d+3)}{2}$ so there is no hyperplane containing S, and hence, by Remark 8.ii, we have that $\psi^{-1}(S) = A$ cannot be contained in an element of $\mathcal{C}$. □

Lemma 14. *Let $\mathbb{K}$ be a field of characteristic zero, $d, e \in \mathbb{Z}^+$ be such that $e \leqslant d$ and $q(x,y) = \prod_{i=1}^{n} q_i(x,y)$ with $\deg(q(x,y)) = e$ and $q_1(x,y), q_2(x,y), \ldots, q_n(x,y) \in \mathbb{K}[x,y]$ irreducible polynomials satisfying that $[q_i(x,y)] \neq [q_j(x,y)]$ for all $i, j \in [1,n]$ such that $i \neq j$. Then*

$$\dim \psi_{d,\mathbb{K}}(\mathcal{Z}(q(x,y))) = \binom{d+2}{2} - \binom{d+2-e}{2} - 1.$$

Proof. Write $\psi := \psi_{d,\mathbb{K}}$, $\tau := \tau_{d,\mathbb{K}}$, $\mathcal{G} := \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{K}}$ and $\mathcal{C} := \mathcal{C}_{\leqslant d,\mathbb{K}}$. Also write $C := \mathcal{Z}(q)$.

First we show that

$$\dim \psi(C) \leqslant \binom{d+2}{2} - \binom{d+2-e}{2} - 1. \tag{5}$$

We assume that (5) is false and we will reach a contradiction. Suppose that

$$\dim \psi(C) > \binom{d+2}{2} - \binom{d+2-e}{2} - 1. \tag{6}$$

From Remark 8.ii, we get that $\psi(\mathbb{K}^2)$ cannot be contained in a hyperplane of $\mathbb{K}^{\frac{d(d+3)}{2}}$ (otherwise, $\mathbb{K}^2$ is contained in a curve). Thus $\dim \psi(\mathbb{K}^2) = \frac{d(d+3)}{2}$, and therefore there exists a subset R of $\psi(\mathbb{K}^2) \setminus \psi(C)$ such that $|R| = \frac{d(d+3)}{2} - \dim \psi(C)$ and $\dim \psi(C) \cup R = \frac{d(d+3)}{2}$. Fix a subset S of R such that $|R \setminus S| = 1$. Then

$$|S| = |R| - 1 = \frac{d(d+3)}{2} - 1 - \dim \psi(C) = \binom{d+2}{2} - 2 - \dim \psi(C)$$

and $\dim \psi(C) \cup S = \binom{d+2}{2} - 2$. Set $A := \psi^{-1}(S)$. From (6),

$$|A| = |S| = \binom{d+2}{2} - 2 - \dim \psi(C) < \binom{d-e+2}{2} - 1. \tag{7}$$

Consider the coefficients of the polynomial $p(x,y) = r_{(0,0)} + \sum_{(n,m)\in I_{d-e}} r_{(n,m)} x^n y^m$ as variables. On the one hand, if $r_{(d-e,0)} = 1$ and $p(\mathbf{a}) = 0$ for all $\mathbf{a} \in A$, then the coefficients $\{r_{(0,0)}\} \cup \{r_{(n,m)}\}_{(n,m)\in I_{d-e}}$ satisfy at most $\binom{d-e+2}{2} - 1$ linear equations by (7). On the other hand, the coefficients $\{r_{(0,0)}\} \cup \{r_{(n,m)}\}_{(n,m)\in I_{d-e}}$ are $\binom{d-e+2}{2}$ variables. Hence the difference between the number of variables and the number of linear equations leads to the existence of $p_1(x,y), p_2(x,y) \in \mathbb{K}[x,y]$ with $\deg(p_1) = \deg(p_2) = d-e$ such that $p_1(x,y) \neq r \cdot p_2(x,y)$

for all $r \in \mathbb{K}$ and $p_1(\mathbf{a}) = p_2(\mathbf{a}) = 0$ for all $\mathbf{a} \in A$. Define $C_1 := \mathcal{Z}(q \cdot p_1)$ and $C_2 := \mathcal{Z}(q \cdot p_2)$, and notice that $[q \cdot p_1] \neq [q \cdot p_2]$ since $p_1 \neq r \cdot p_2$ for all $r \in \mathbb{K}$. For $i \in \{1, 2\}$, we have that $A \subseteq \mathcal{Z}(p_i)$ so

$$C \cup A \subseteq \mathcal{Z}(q \cdot p_i) = C_i;$$

applying ψ to both sides of the previous inclusion, we obtain that

$$\psi(C) \cup S \subseteq \psi(C_i),$$

and then Remark 8.ii gives

$$\psi(C) \cup S \subseteq \psi(C_i) = \tau([q \cdot p_i]) \cap \psi(\mathbb{K}^2) \subseteq \tau([q \cdot p_i]). \tag{8}$$

Recall that $\dim \psi(C) \cup S = \binom{d+2}{2} - 2$; hence, since $\tau([q \cdot p_1])$ and $\tau([q \cdot p_1])$ are hyperplanes, they are flats with $\dim \tau([q \cdot p_1]) = \dim \tau([q \cdot p_2]) = \binom{d+2}{2} - 2$, and then (8) implies that $\tau([q \cdot p_1]) = \tau([q \cdot p_2])$. However, this is impossible since $[q \cdot p_1] \neq [q \cdot p_2]$ and τ in injective by Remark 8.ii. This contradiction proves (5).

Now we show by contradiction that

$$\dim \psi(C) \geqslant \binom{d+2}{2} - \binom{d+2-e}{2} - 1. \tag{9}$$

Suppose that

$$\dim \psi(C) < \binom{d+2}{2} - \binom{d+2-e}{2} - 1. \tag{10}$$

From Lemma 13, we know there is a subset A of $\mathbb{K}^2 \backslash C$ such that $|A| = \binom{d+2-e}{2}$ and there is no element of $\mathcal{C}_{\leqslant d-e,\mathbb{K}}$ which contains A. Since $|A| = \binom{d+2-e}{2}$, we get that $|\psi(A)| = \binom{d+2-e}{2}$, and hence (10) leads to

$$\dim \psi(C \cup A) = \dim \psi(C) \cup \psi(A) < \binom{d+2}{2} - 1 = \frac{d(d+3)}{2}. \tag{11}$$

From (11), there is $H_1 \in \mathcal{G}$ such that $\psi(C \cup A) \subseteq H_1$. From Remark 8.ii, there is $[p] \in \mathbb{K}_d[x, y]/\sim$ such that $\tau([p]) = H_1$ and $\psi(\mathcal{Z}(p)) = \tau([p]) \cap \psi(\mathbb{K}^2)$. Set $C_1 := \mathcal{Z}(p)$. Then, since $\psi(C \cup A) \subseteq H_1$, we get that

$$\psi(C \cup A) \subseteq H_1 \cap \psi(\mathbb{K}^2) = \tau([p]) \cap \psi(\mathbb{K}^2) = \psi(C_1),$$

and the injectivity of ψ implies that

$$C \cup A \subseteq C_1. \tag{12}$$

Consider a factorization $p(x, y) = r \prod_{i=1}^{l} p_i(x, y)^{m_i}$ with $m_1, m_2, \ldots, m_l \in \mathbb{Z}^+$, $r \in \mathbb{K}$, $[p_i(x, y)] \neq [p_j(x, y)]$ for all $i, j \in [1, l]$ such that $i \neq j$, and $p_i(x, y)$ irreducible for each $i \in [1, l]$. Then $\mathcal{Z}(p_1), \mathcal{Z}(p_2), \ldots, \mathcal{Z}(p_l)$ are the pairwise distinct irreducible components of C_1. From (12), C is the union of some irreducible components of C_1; hence we can assume

without loss of generality that there is $m \in [1,l]$ such that $C = \bigcup_{i=1}^{m} \mathcal{Z}(p_i)$. However, also $C = \mathcal{Z}(q) = \bigcup_{i=1}^{n} \mathcal{Z}(q_i)$. Hence, from Corollary 7, we get that

$$\left[\prod_{i=1}^{n} q_i\right] = \left[\prod_{i=1}^{m} p_i\right];$$

thus there is $s \in \mathbb{K}$ such that $q(x,y) = s\prod_{i=1}^{m} p_i(x,y)$. Write $C_2 := \mathcal{Z}\left(\prod_{i=m+1}^{l} p_i\right)$ so $C_1 = C \cup C_2$. On the one hand, $A \cap C = \emptyset$ so (12) leads to

$$A \subseteq C_1 \setminus C \subseteq C_2. \tag{13}$$

On the other hand,

$$\deg\left(\prod_{i=1}^{m} p_i\right) + \deg\left(\prod_{i=m+1}^{l} p_i\right) \leqslant \deg\left(\prod_{i=1}^{l} p_i^{m_i}\right). \tag{14}$$

Then

$$\begin{aligned}
\deg\left(\prod_{i=m+1}^{l} p_i\right) &\leqslant \deg(p) - \deg(q) && \Big(\text{by (14)}\Big)\\
&= \deg(p) - e && \Big(\text{since } \deg(q) = e\Big)\\
&\leqslant d - e. && \Big(\text{since } \deg(p) \leqslant d\Big) \qquad (15)
\end{aligned}$$

However, (13) and (15) contradict the fact that there is no element of $\mathcal{C}_{\leqslant d-e,\mathbb{K}}$ which contains A. This contradiction proves (9). The claim follows from (5) and (9). □

Lemma 15. *Let $\mathbb{K}$ be a field of characteristic zero, $d, e \in \mathbb{Z}^+$ be such that $e \leqslant d$, F be a flat in $\mathbb{K}^{\frac{d(d+3)}{2}}$ such that $\dim F < \binom{d+2}{2} - \binom{d+1-e}{2} - 1$ and A be a subset of $\psi_{d,\mathbb{K}}^{-1}(F)$ such that $|A| > d^{\binom{d+2}{2}+1}$. Then there is a curve $C \in \mathcal{C}_{\leqslant e,\mathbb{K}}$ such that $\psi_{d,\mathbb{K}}(C) \subseteq F$ and $|A \setminus C| \leqslant d^{\binom{d+2}{2}+1}$.*

Proof. Write $\psi := \psi_{d,\mathbb{K}}$, $\tau := \tau_{d,\mathbb{K}}$ and $\mathcal{C} := \mathcal{C}_{\leqslant e,\mathbb{K}}$. If $\dim F = \frac{d(d+3)}{2} - 1$, then F is a hyperplane and $e = d$. Thus, in this case, Remark 8.ii implies that there is $[p] \in \mathbb{K}_d[x,y]/\sim$ such that $\tau([p]) = F$, and also it satisfies that $\psi(\mathcal{Z}(p)) = F \cap \psi(\mathbb{K}^2)$. Therefore $\psi(\mathcal{Z}(p)) \subseteq F$ and $A \subseteq \mathcal{Z}(p)$ meaning that $\mathcal{Z}(p)$ satisfies the desired properties.

From now on, we assume that $\dim F < \frac{d(d+3)}{2} - 1$ and set $f := \frac{d(d+3)}{2} - \dim F$. Since F is a flat with codimension $f \geqslant 2$ in $\mathbb{K}^{\frac{d(d+3)}{2}}$, there are $H_1, H_2, \ldots, H_f$ hyperplanes in $\mathbb{K}^{\frac{d(d+3)}{2}}$ such that $F = \bigcap_{i=1}^{f} H_i$. For each $i \in [1,f]$, Remark 8.ii warranties the existence of $[p_i] \in \mathbb{K}_d[x,y]/\sim$ such that $\tau([p_i]) = H_i$, and we set $C_i := \mathcal{Z}(p_i)$. Hence, since $\psi(C_i) = H_i \cap \psi(\mathbb{K}^2)$ for each $i \in [1,f]$ by Remark 8.ii, we get that

$$\psi^{-1}(F) = \psi^{-1}\left(\bigcap_{i=1}^{f} H_i\right) = \bigcap_{i=1}^{f} \psi^{-1}(H_i) = \bigcap_{i=1}^{f} C_i. \tag{16}$$

For each $i \in [1,f]$, let $\mathcal{Z}(p_{i,1}), \mathcal{Z}(p_{i,2}), \ldots, \mathcal{Z}(p_{i,n_i})$ be the pairwise distinct irreducible components of C_i; for each $j \in [1,n_i]$, write $C_{i,j} := \mathcal{Z}(p_{i,j})$. Note that C is an irreducible curve contained in $\psi^{-1}(F)$ if and only if C is an irreducible component of C_i for all $i \in [1,f]$. Thus, relabelling if necessary, assume that there is $g \in \mathbb{Z}_0^+$ such that

i) For all $h \in [1,g]$, we have that $C_{1,h} = C_{2,h} = \cdots = C_{f,h}$.

ii) For all $h > g$ and $i \in [1,f]$, there is $j \in [1,f]$ such that $C_{i,h} \notin \{C_{j,1}, C_{j,2}, \ldots, C_{j,n_j}\}$;

notice that g can be zero if $\psi^{-1}(F)$ does not contain irreducible curves. Set

$$\begin{aligned} J &:= [1,n_1] \times [1,n_2] \times \cdots \times [1,n_f] \\ I &:= \{\mathbf{j} = (j_1, j_2, \ldots, j_f) \in J : \ j_1 = j_2 = \cdots = j_f \text{ and } j_1 \in [1,g]\} \\ K &:= J \setminus I. \end{aligned}$$

Insomuch as $\sum_{j=1}^{n_i} \deg(p_{i,j}) \leqslant \deg(p_i) \leqslant d$ and $\deg(p_{i,j}) \geqslant 1$ for all $i \in [1,f]$ and $j \in [1,n_i]$, we get that

$$|K| \leqslant |J| = \prod_{i=1}^{f} n_i \leqslant d^f \leqslant d^{\frac{d(d+3)}{2}}. \tag{17}$$

For each $\mathbf{j} \in J$, we write $\mathbf{j} = (j_1, j_2, \ldots, j_f)$. Since $C_i = \bigcup_{j=1}^{n_i} C_{i,j}$ for each $i \in [1,f]$, we get from (16) that

$$\psi^{-1}(F) = \bigcap_{i=1}^{f} C_i = \bigcap_{i=1}^{f} \bigcup_{j=1}^{n_i} C_{i,j} = \bigcup_{\mathbf{j} \in J} \bigcap_{i=1}^{f} C_{i,j_i} = \left(\bigcup_{\mathbf{j} \in I} \bigcap_{i=1}^{f} C_{i,j_i} \right) \cup \left(\bigcup_{\mathbf{j} \in K} \bigcap_{i=1}^{f} C_{i,j_i} \right). \tag{18}$$

Write $C := \mathcal{Z}\left(\prod_{k=1}^{g} p_{1,k}\right)$. Then the definition of I leads to

$$C = \mathcal{Z}\left(\prod_{k=1}^{g} p_{1,k} \right) = \bigcup_{k=1}^{g} C_{1,k} = \bigcup_{k=1}^{g} \bigcap_{i=1}^{f} C_{i,k} = \bigcup_{\mathbf{j} \in I} \bigcap_{i=1}^{f} C_{i,j_i}.$$

From i) and ii), notice that for all $\mathbf{j} \in K$, there are $k, l \in [1,f]$ such that $C_{k,j_k} \neq C_{l,j_l}$, and then Theorem 5 leads to

$$|C_{k,j_k} \cap C_{l,j_l}| \leqslant d^2.$$

Thus, for all $\mathbf{j} \in K$,

$$\left| \bigcap_{i=1}^{f} C_{i,j_i} \right| \leqslant d^2. \tag{19}$$

We get that

$$\begin{aligned}
|A \setminus C| &\leqslant |\psi^{-1}(F) \setminus C| && \Big(\text{since } A \subseteq \psi^{-1}(F)\Big) \\
&\leqslant \left| \bigcup_{\mathbf{j} \in K} \bigcap_{i=1}^{f} C_{i,j_i} \right| && \Big(\text{by (18)}\Big) \\
&\leqslant |K|\, d^2 && \Big(\text{by (19)}\Big) \\
&\leqslant d^{\frac{d(d+3)}{2}+2}. && \Big(\text{by (17)}\Big) \qquad (20)
\end{aligned}$$

Since $|A| > d^{\binom{d+2}{2}+1}$, we conclude from (20) that $C \neq \emptyset$ (i.e. $g > 0$). Now we apply Lemma 14 to the polynomial $\prod_{k=1}^{g} p_{1,k}$

$$\binom{d+2}{2} - \binom{d+2-\deg\left(\prod_{k=1}^{g} p_{1,k}\right)}{2} - 1 = \dim \psi(C).$$

Since $C \subseteq \psi^{-1}(F)$ by (18), we have that $\dim \psi(C) \leqslant \dim F$ so the previous equality yields that

$$\begin{aligned}
\binom{d+2}{2} - \binom{d+2-\deg\left(\prod_{k=1}^{g} p_{1,k}\right)}{2} - 1 &= \dim \psi(C) \\
&\leqslant \dim F \\
&< \binom{d+2}{2} - \binom{d+1-e}{2} - 1;
\end{aligned}$$

thus $\deg\left(\prod_{k=1}^{g} p_{1,k}\right) \leqslant e$ and therefore $C \in \mathcal{C}$. This fact and (20) conclude the proof. □

It looks like the upper bound $|A \setminus C| \leqslant d^{\binom{d+2}{2}+1}$ in Lemma 15 is not optimal. It would be an interesting problem by its own right to improve this upper bound.

Recall that if S is a subset of $\mathbb{C}^d$ and $e \in [1, d]$, then $\phi_e(S)$ is the the size of a largest subset of S with essential dimension $\leqslant e$.

Lemma 16. *Let $d, e \in \mathbb{Z}^+$ be such that $e \leqslant d$ and A be a nonempty finite subset of $\mathbb{C}^2$. For any $f \in \left[\binom{d+2}{2} - \binom{d+2-e}{2} - 1, \binom{d+2}{2} - \binom{d+1-e}{2} - 2\right]$,*

$$|A| - \phi_f(\psi_{d,\mathbb{C}}(A)) \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |A \setminus C| \leqslant |A| - \phi_f(\psi_{d,\mathbb{C}}(A)) + \frac{d(d+3)}{2} \cdot d^{\binom{d+2}{2}+1}.$$

Proof. Write $\psi := \psi_{d,\mathbb{C}}$, $\mathcal{C} := \mathcal{C}_{\leqslant e,\mathbb{C}}$ and $\phi := \phi_f$. First we show that

$$|A| - \phi(\psi(A)) \leqslant \min_{C \in \mathcal{C}} |A \setminus C|. \qquad (21)$$

Take $C_1 \in \mathcal{C}$. Then there is $p(x, y) \in \mathbb{K}[x, y]$ with $\deg(p(x, y)) \in [1, e]$ such that $C_1 = \mathcal{Z}(p(x, y))$. Now, if $\mathcal{Z}(p_1), \mathcal{Z}(p_2), \ldots, \mathcal{Z}(p_n)$ are the pairwise distinct irreducible components of C_1, then Corollary 7 yields that $[p] = [\prod_{i=1}^{n} p_i^{m_i}]$ for some $m_1, m_2, \ldots, m_n \in \mathbb{Z}^+$.

Therefore

$$\deg\left(\prod_{i=1}^{n} p_i\right) \leqslant \deg\left(\prod_{i=1}^{n} p_i^{m_i}\right) = \deg(p) \leqslant e,$$

and applying Lemma 14 to the polynomial $\prod_{i=1}^{n} p_i$, we obtain that

$$\begin{aligned}\dim \psi(C_1) &= \dim \psi\left(\mathcal{Z}\left(\prod_{i=1}^{n} p_i\right)\right)\\ &= \binom{d+2}{2} - \binom{d+2-\deg\left(\prod_{i=1}^{n} p_i\right)}{2} - 1\\ &\leqslant \binom{d+2}{2} - \binom{d+2-e}{2} - 1. \end{aligned} \tag{22}$$

We claim that

$$\overline{\dim}\, \psi(C_1 \cap A) \leqslant \binom{d+2}{2} - \binom{d+2-e}{2} - 1. \tag{23}$$

Indeed, set $F := \mathrm{Fl}(\psi(C_1))$. Then the family (with only one flat) $\{F\}$ satisfies that $\psi(C_1 \cap A) \subseteq F$ and $1 \leqslant \dim F \leqslant \binom{d+2}{2} - \binom{d+2-e}{2} - 1$ by (22). Hence the definition of essential dimension leads to (23). Now, since $f \geqslant \binom{d+2}{2} - \binom{d+2-e}{2} - 1$ and $\psi(C_1 \cap A) \subseteq \psi(A)$, we get from (23) that

$$\phi(\psi(A)) = \max_{R \in \mathcal{F}_f(\psi(A))} |R| \geqslant |\psi(C_1 \cap A)| = |C_1 \cap A|. \tag{24}$$

Since C_1 is arbitrary, (24) implies that

$$\phi(\psi(A)) \geqslant \max_{C \in \mathcal{C}} |C \cap A|. \tag{25}$$

Inasmuch as

$$\max_{C \in \mathcal{C}} |C \cap A| = |A| - \min_{C \in \mathcal{C}} |A \setminus C|,$$

we have that (21) is a consequence of (25).

It is time to show that

$$\min_{C \in \mathcal{C}} |A \setminus C| \leqslant |A| - \phi(\psi(A)) + \frac{d(d+3)}{2} \cdot d^{\binom{d+2}{2}+1}. \tag{26}$$

Fix an $R \in \mathcal{F}_f(\psi(A))$ such that $\phi(\psi(A)) = |R|$. Since $R \in \mathcal{F}_f(\psi(A))$, we have that $\overline{\dim}\, R \leqslant f$. Therefore we can fix a family $\{F_i\}_{i \in [1,n]}$ of flats in $\mathbb{C}^{\frac{d(d+3)}{2}}$ satisfying that

$$R \subseteq \bigcup_{i=1}^{n} F_i, \tag{27}$$

$$\dim F_i \geqslant 1 \qquad \text{for all } i \in [1, n] \tag{28}$$

and

$$\sum_{i=1}^{n} \dim F_i = \overline{\dim}\ R \leqslant f \leqslant \frac{d(d+3)}{2} - 1. \tag{29}$$

For each $i \in [1,n]$, let $\mathcal{C}_i$ be the family of curves C in $\mathbb{C}^2$ such that $\psi(C) \subseteq F_i$. Relabelling if necessary, we assume that there is $m \in [0,n]$ such that $\mathcal{C}_i \neq \emptyset$ for all $i \in [1,m]$ and $\mathcal{C}_i = \emptyset$ for all $i \in [m+1,n]$ (m can be zero if $\mathcal{C}_i = \emptyset$ for all $i \in [1,n]$). For each $i \in [1,m]$, fix a $C_i \in \mathcal{C}_i$ such that

$$|\psi^{-1}(R \cap F_i) \setminus C_i| = \min_{C \in \mathcal{C}_i} |\psi^{-1}(R \cap F_i) \setminus C|,$$

and fix irreducible polynomials $p_{i,1}(x,y), p_{i,2}(x,y), \ldots, p_{i,n_i}(x,y) \in \mathbb{C}[x,y]$ such that $\mathcal{Z}(p_{i,1}), \mathcal{Z}(p_{i,2}), \ldots, \mathcal{Z}(p_{i,n_i})$ are the pairwise distinct irreducible components of C_i.

We claim that for all $i \in [1,m]$,

$$|\psi^{-1}(R \cap F_i) \setminus C_i| \leqslant d^{\binom{d+2}{2}+1}. \tag{30}$$

If (30) is false, then the set $\psi^{-1}(R \cap F_i) \setminus C_i$ and the flat F_i satisfy the assumptions of Lemma 15 so there is a curve $D_i \in \mathcal{C}_{\leqslant d,\mathbb{C}}$ such that $|(\psi^{-1}(R \cap F_i) \setminus C_i) \setminus D_i| \leqslant d^{\binom{d+2}{2}+1}$ and $\psi(D_i) \subseteq F_i$. Nonetheless, this means that the curve $E_i := C_i \cup D_i$ satisfies that $\psi(E_i) \subseteq F_i$ and

$$|\psi^{-1}(R \cap F_i) \setminus C_i| > d^{\binom{d+2}{2}+1} \geqslant |\psi^{-1}(R \cap F_i) \setminus E_i|,$$

but this is impossible by the way we chose C_i.

Now we show by contradiction that for all $i \in [m+1,n]$,

$$|\psi^{-1}(R \cap F_i)| \leqslant d^{\binom{d+2}{2}+1}. \tag{31}$$

Indeed, if (31) does not hold, then the set $\psi^{-1}(R \cap F_i)$ and the flat F_i satisfy the assumptions of Lemma 15. Therefore there is a curve $C_i \in \mathcal{C}_{\leqslant d,\mathbb{C}}$ such that $\psi(C_i) \subseteq F_i$ which is impossible since $\mathcal{C}_i = \emptyset$.

The conclusion of the proof of (26) is divided into two cases.

- Suppose that $m = 0$. Fix any $D \in \mathcal{C}$. Then

$$\begin{aligned}
|\psi^{-1}(R) \setminus D| &\leqslant \sum_{i=1}^{n} |\psi^{-1}(R \cap F_i) \setminus D| && \Big(\text{by (27)}\Big) \\
&\leqslant \sum_{i=1}^{n} |\psi^{-1}(R \cap F_i)| \\
&\leqslant n d^{\binom{d+2}{2}+1} && \Big(\text{by (31)}\Big) \\
&\leqslant \frac{d(d+3)}{2} \cdot d^{\binom{d+2}{2}+1}. && \Big(\text{by (28), (29)}\Big)
\end{aligned} \tag{32}$$

Thus

$$\begin{aligned}
\min_{C\in\mathcal{C}} |A\setminus C| &\leqslant |A\setminus D| \\
&\leqslant |A\setminus \psi^{-1}(R)| + |\psi^{-1}(R)\setminus D| && \Big(\text{since } R\subseteq\psi(A)\Big)\\
&= |A| - |R| + |\psi^{-1}(R)\setminus D| && \Big(\text{by Rem. 8.i}\Big)\\
&= |A| - \phi(\psi(A)) + |\psi^{-1}(R)\setminus D| \\
&\leqslant |A| - \phi(\psi(A)) + \frac{d(d+3)}{2}\cdot d^{\binom{d+2}{2}+1}, && \Big(\text{by (32)}\Big)
\end{aligned}$$

and this completes the proof of (26) in this case.

- Suppose that $m>0$. Set $D := \mathcal{Z}\left(\prod_{i=1}^m\prod_{j=1}^{n_i} p_{i,j}\right) = \bigcup_{i=1}^m C_i$. Note that

$$\begin{aligned}
&\sum_{i=1}^m \left(\binom{d+2}{2} - \binom{d+2-\deg\left(\prod_{j=1}^{n_i} p_{i,j}\right)}{2} - 1\right)\\
=&\sum_{i=1}^m \dim\psi\left(\mathcal{Z}\left(\prod_{j=1}^{n_i} p_{i,j}\right)\right) && \Big(\text{by Lemma 14}\Big)\\
=&\sum_{i=1}^m \dim\psi(C_i)\\
\leqslant&\sum_{i=1}^m \dim F_i && \Big(\text{since } \psi(C_i)\subseteq F_i\Big)\\
\leqslant& f && \Big(\text{by (29)}\Big)\\
<&\binom{d+2}{2} - \binom{d+2-(e+1)}{2} - 1. && (33)
\end{aligned}$$

Since the map $x\mapsto \binom{d+2}{2} - \binom{d+2-x}{2} - 1$ is convex, we conclude from (33) that

$$\deg\left(\prod_{i=1}^m\prod_{j=1}^{n_i} p_{i,j}\right) = \sum_{i=1}^m \deg\left(\prod_{j=1}^{n_i} p_{i,j}\right) < e+1$$

and then

$$D\in\mathcal{C}. \tag{34}$$

Also note that

$$\begin{aligned}
|\psi^{-1}(R)\setminus D| &\leqslant \sum_{i=1}^{n}|\psi^{-1}(R\cap F_i)\setminus D| && \Big(\text{by (27)}\Big)\\
&\leqslant \sum_{i=1}^{m}|\psi^{-1}(R\cap F_i)\setminus C_i| + \sum_{i=m+1}^{n}|\psi^{-1}(R\cap F_i)|\\
&\leqslant nd^{\binom{d+2}{2}+1} && \Big(\text{by (30), (31)}\Big)\\
&\leqslant \frac{d(d+3)}{2}\cdot d^{\binom{d+2}{2}+1}. && \Big(\text{by (28), (29)}\Big)
\end{aligned} \tag{35}$$

Finally

$$\begin{aligned}
\min_{C\in\mathcal{C}}|A\setminus C| &\leqslant |A\setminus D| && \Big(\text{by (34)}\Big)\\
&\leqslant |A\setminus\psi^{-1}(R)| + |\psi^{-1}(R)\setminus D| && \Big(\text{since } R\subseteq\psi(A)\Big)\\
&= |A| - |R| + |\psi^{-1}(R)\setminus D| && \Big(\text{by Rem. 8.i}\Big)\\
&= |A| - \phi(\psi(A)) + |\psi^{-1}(R)\setminus D|\\
&\leqslant |A| - \phi(\psi(A)) + \frac{d(d+3)}{2}\cdot d^{\binom{d+2}{2}+1}, && \Big(\text{by (35)}\Big)
\end{aligned}$$

and this completes the proof of (26). □

As we explained in the introduction, Lund's theorem (i.e. Theorem 10) is not proven for arbitrary fields of characteristic zero. Therefore we need to reduce Theorem 2 to the complex case and this is what we will do in the last part of this section. Before we state and proof Lemma 18, we need some notation and observations.

Let $d\in\mathbb{Z}^+$ and $\mathbb{K},\mathbb{L},\mathbb{M}$ be fields such that $\mathbb{M}\subseteq\mathbb{K}$. For any injective morphism of fields $\rho:\mathbb{L}\longrightarrow\mathbb{K}$, abusing of notation, we denote by $\rho:\mathbb{L}^d\longrightarrow\mathbb{K}^d$ the map $(a_1,a_2,\ldots,a_d)\mapsto(\rho(a_1),\rho(a_2),\ldots,\rho(a_d))$. For any subset S of $\mathbb{K}[x_1,\ldots,x_d]$, $\mathcal{Z}_{\mathbb{K}}(S)$ will denote the common zero set of the polynomials in $\mathbb{K}^d$ (this to distinguish in which affine space we are taking the zero set of a family of polynomials). For any subset S of $\mathbb{K}[x_1,\ldots,x_d]$, we say that $V=\mathcal{Z}_{\mathbb{K}}(S)$ is *defined over* $\mathbb{M}$ if $S\subseteq\mathbb{M}[x_1,\ldots,x_d]$. On the one hand, since $\mathbb{M}[x_1,\ldots,x_d]\subseteq\mathbb{K}[x_1,\ldots,x_d]$, we have the injection of affine varieties of $\mathbb{M}^d$ into the affine varieties of $\mathbb{K}^d$ given by $\mathcal{Z}_{\mathbb{M}}(S)\mapsto\mathcal{Z}_{\mathbb{K}}(S)$ for any $S\subseteq\mathbb{M}[x_1,\ldots,x_d]$. On the other hand, if F is a flat in $\mathbb{K}^d$ such that there is a subset A of $\mathbb{M}^d$ satisfying that $F=\mathrm{Fl}(A)$, then F is defined over $\mathbb{M}$. Indeed, translating F if necessary, assume that F is a linear subspace of $\mathbb{K}^d$. Since $F=\mathrm{Fl}(A)$ with $A\subseteq\mathbb{M}^d$, we get that F has a basis formed by elements in $\mathbb{M}^d$. Thereby, there are linear equations with coefficients in $\mathbb{M}$ such that this vector space is the common zero set of these linear equations, and hence F is defined over $\mathbb{M}$. These two ideas give the following facts for flats.

Remark 17. Let $e,d\in\mathbb{Z}^+$ be such $e\leqslant d$, $\mathbb{K}$ be a field and $\mathbb{M}$ a subfield of $\mathbb{K}$.

i) For each $F \in \mathcal{G}_{e,\mathbb{M}}$, fix a set of linear polynomials $S_F \subseteq \mathbb{M}[x_1, \ldots, x_d]$ such that $F = \mathcal{Z}_{\mathbb{M}}(S_F)$. For any subset R of $\mathbb{M}^d$, the map

$$\mathcal{G}_{e,\mathbb{M}}(R) \longrightarrow \mathcal{G}_{e,\mathbb{K}}(R), \qquad F = \mathcal{Z}_{\mathbb{M}}(S_F) \mapsto \mathcal{Z}_{\mathbb{K}}(S_F)$$

is injective; in particular, $|\mathcal{G}_{e,\mathbb{M}}(R)| \leqslant |\mathcal{G}_{e,\mathbb{K}}(R)|$.

ii) If $F \in \mathcal{G}_{e,\mathbb{K}}$ is such that $F = \mathrm{Fl}(S)$ for some subset S of $\mathbb{M}^d$, then F is defined over $\mathbb{M}$. Then, for any subset R of $\mathbb{M}^d$, the following map is well defined and injective

$$\mathcal{G}_{e,\mathbb{K}}(R) \longrightarrow \mathcal{G}_{e,\mathbb{M}}(R), \qquad F \mapsto F \cap \mathbb{M}^d;$$

in particular, $|\mathcal{G}_{e,\mathbb{K}}(R)| \leqslant |\mathcal{G}_{e,\mathbb{M}}(R)|$.

Now we are ready to state and proof the last result of this section.

Lemma 18. *Let $d \in \mathbb{Z}^+$, $\mathbb{K}$ be a field of characteristic zero and A a nonempty finite subset in $\mathbb{K}^2$. Then there are a subfield $\mathbb{L}$ of $\mathbb{K}$ such that $A \subseteq \mathbb{L}^2$ and an injective morphism of fields $\rho : \mathbb{L} \longrightarrow \mathbb{C}$ such that for all $e \in [1, d]$,*

$$\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C| \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| + d^{\binom{d+2}{2}+1} \tag{36}$$

and

$$\left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right| = \left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A))\right|. \tag{37}$$

Proof. Since $\mathbb{K}$ is a field of characteristic zero, its prime subfield is isomorphic to $\mathbb{Q}$ so we may assume that $\mathbb{K}$ is an extension of $\mathbb{Q}$. Let S_1 be the set of all the entries of all the elements of A. For each class $U \in \sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))$, fix a polynomial $p_U(x, y)$ in it. Let S_2 be the set of all the coefficients of the polynomials in $\{p_U(x, y) : U \in \sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\}$. Since A is finite, the number of hyperplanes generated by $\psi_{d,\mathbb{K}}(A)$ in $\mathbb{K}^{\frac{d(d+3)}{2}}$ is finite, and then Lemma 12 yields that $\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))$ is finite; therefore S_2 is finite. For each $e \in [1, d]$, fix a curve $C_e \in \mathcal{C}_{\leqslant e,\mathbb{K}}$ such that

$$|A \setminus C_e| = \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C|,$$

and fix $q_e(x, y) \in \mathbb{K}[x, y]$ such that $C_e = \mathcal{Z}_{\mathbb{K}}(q_e(x, y))$. Let S_3 be the set of all the coefficients of the polynomials in $\{q_e(x, y) : e \in [1, d]\}$. Write $\mathbb{L} := \mathbb{Q}(S_1 \cup S_2 \cup S_3)$. We have seen that S_1, S_2 and S_3 are finite so $\mathbb{L}$ is finitely generated over $\mathbb{Q}$. Also notice that $\mathbb{L} \subseteq \mathbb{K}$. Since the entries of the elements of A are in $\mathbb{Q}(S_1) \subseteq \mathbb{L}$, we get that

$$A \subseteq \mathbb{L}^2. \tag{38}$$

Insomuch as $\mathbb{L} \subseteq \mathbb{K}$, we have that $\mathbb{L}[x, y] \subseteq \mathbb{K}[x, y]$ and hence $\left|\sigma_{d,\mathbb{L}}^{-1}(\mathcal{D}_{d,\mathbb{L}}(A))\right| \leqslant \left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right|$. On the other hand, by the construction of S_2, each class of $\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))$

has a representative with all its coefficients in $\mathbb{Q}(S_2) \subseteq \mathbb{L}$ so $\left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right| \leqslant \left|\sigma_{d,\mathbb{L}}^{-1}(\mathcal{D}_{d,\mathbb{L}}(A))\right|$, and hence

$$\left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right| = \left|\sigma_{d,\mathbb{L}}^{-1}(\mathcal{D}_{d,\mathbb{L}}(A))\right|. \tag{39}$$

Inasmuch as $\mathbb{L} \subseteq \mathbb{K}$, we have that $\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C| \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{L}}} |A \setminus C|$ for all $e \in [1,d]$. Now, for $e \in [1,d]$, the construction of S_3 yields that the minimum of $\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C|$ is achieved by $C_e = \mathcal{Z}_{\mathbb{K}}(q_e(x,y))$ with $q_e(x,y) \in \mathbb{Q}(S_3)[x,y] \subseteq \mathbb{L}[x,y]$; then

$$\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{L}}} |A \setminus C| \leqslant |A \setminus \mathcal{Z}_{\mathbb{L}}(q_e(x,y))| = |A \setminus \mathcal{Z}_{\mathbb{K}}(q_e(x,y))| = \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C|,$$

and thereby

$$\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C| = \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{L}}} |A \setminus C|. \tag{40}$$

Since $\mathbb{L}$ is finitely generated over $\mathbb{Q}$, Theorem 11 establishes the existence of an injective morphism of fields $\rho : \mathbb{L} \to \mathbb{C}$. Since $A \subseteq \mathbb{L}^2$ by (38), it remains to prove that ρ satisfies (36) and (37).

Write $\mathbb{M} := \rho(\mathbb{L})$. The isomorphism of fields $\rho : \mathbb{L} \to \mathbb{M}$ leads to

$$\left|\sigma_{d,\mathbb{L}}^{-1}(\mathcal{D}_{d,\mathbb{L}}(A))\right| = \left|\sigma_{d,\mathbb{M}}^{-1}(\mathcal{D}_{d,\mathbb{M}}(\rho(A)))\right|, \tag{41}$$

and for all $e \in [1,d]$,

$$\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{L}}} |A \setminus C| = \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{M}}} |\rho(A) \setminus C|. \tag{42}$$

The next step is to show that

$$\left|\sigma_{d,\mathbb{M}}^{-1}(\mathcal{D}_{d,\mathbb{M}}(\rho(A)))\right| = \left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right|. \tag{43}$$

Since $\mathbb{M} \subseteq \mathbb{C}$ and $\rho(A) \subseteq \mathbb{M}^2$, we have that $\psi_{d,\mathbb{M}}(\rho(A)) = \psi_{d,\mathbb{C}}(\rho(A))$; write $T := \psi_{d,\mathbb{C}}(\rho(A))$. From Lemma 12, we have that

$$\begin{aligned} \tau_{d,\mathbb{M}}\left(\sigma_{d,\mathbb{M}}^{-1}(\mathcal{D}_{d,\mathbb{M}}(\rho(A)))\right) &= \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{M}}(T) \\ \tau_{d,\mathbb{C}}\left(\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right) &= \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{C}}(T). \end{aligned} \tag{44}$$

Insomuch as $\rho(A) \subseteq \mathbb{M}^2$, notice that $T \subseteq \mathbb{M}^{\frac{d(d+3)}{2}}$. Then Remark 17.i and Remark 17.ii applied to T lead to

$$|\mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{M}}(T)| = |\mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{C}}(T)|. \tag{45}$$

Since $\tau_{d,\mathbb{M}}$ and $\tau_{d,\mathbb{C}}$ are bijections by Remark 8.ii, we have that (43) is a consequence of (44) and (45).

Now we prove that for all $e \in [1,d]$,

$$\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{M}}} |\rho(A) \setminus C| \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| + d^{\binom{d+2}{2}+1}. \tag{46}$$

Since $\mathbb{M}$ is a subfield of $\mathbb{C}$, the left-hand side inequality of (46) is true. Next we prove that

$$\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{M}}} |\rho(A)\setminus C| \leqslant \min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\setminus C| + d^{\binom{d+2}{2}+1}. \tag{47}$$

Considering that $|\rho(A)| = |\rho(A)\setminus C| + |\rho(A)\cap C|$ for any curve C, we have that (47) is equivalent to

$$\max_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\cap C| \leqslant \max_{C\in\mathcal{C}_{\leqslant e,\mathbb{M}}} |\rho(A)\cap C| + d^{\binom{d+2}{2}+1} \tag{48}$$

so it is enough to prove (48). Take $D\in\mathcal{C}_{\leqslant e,\mathbb{C}}$ such that $|\rho(A)\cap D| = \max_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\cap C|$. For any point there is always a curve $C\in\mathcal{C}_{\leqslant e,\mathbb{C}}$ passing through it, then from the maximality of $|\rho(A)\cap D|$, it is clear that $\rho(A)\cap D\neq\emptyset$. Fix $q_1,q_2,\ldots,q_n\in\mathbb{C}[x,y]$ such that $\mathcal{Z}(q_1),\mathcal{Z}(q_2),\ldots,\mathcal{Z}(q_n)$ are the pairwise distinct irreducible components of D. From Corollary 7, any $q\in\mathbb{C}_d[x,y]$ such that $\mathcal{Z}(q)=D$ needs to satisfy that $[q]=[\prod_{i=1}^n q_i^{m_i}]$ for some $m_1,m_2,\ldots,m_n\in\mathbb{Z}^+$. Hence, since $D\in\mathcal{C}_{\leqslant e,\mathbb{C}}$, we conclude that

$$\deg\left(\prod_{i=1}^n q_i\right)\leqslant e. \tag{49}$$

Write $B:=\rho(A)\cap D$ and $G:=\mathrm{Fl}(\psi_{d,\mathbb{C}}(B))$ in $\mathbb{C}^{\frac{d(d+3)}{2}}$. Since $B\subseteq\rho(A)\subseteq\mathbb{M}^d$, we get that $\psi_{d,\mathbb{C}}(B)\subseteq\mathbb{M}^{\frac{d(d+3)}{2}}$ and then Remark 17.ii indicates that $F:=G\cap\mathbb{M}^{\frac{d(d+3)}{2}}$ satisfies that

$$\dim F=\dim G \tag{50}$$

(note that $\dim F$ is the dimension of F as a $\mathbb{M}$-flat and $\dim G$ is the dimension of G as a $\mathbb{C}$-flat). If $|B|\leqslant d^{\binom{d+2}{2}+1}$, then (48) is true so we assume from now on that

$$|B|>d^{\binom{d+2}{2}+1}. \tag{51}$$

Because $B\subseteq D$, notice that

$$\dim G\leqslant\dim\psi_{d,\mathbb{C}}(D). \tag{52}$$

Hence

$$\begin{aligned}
\dim F &= \dim G && \Big(\text{by (50)}\Big)\\
&\leqslant \dim\psi_{d,\mathbb{C}}(D) && \Big(\text{by (52)}\Big)\\
&= \dim\psi_{d,\mathbb{C}}\left(\mathcal{Z}\left(\prod_{i=1}^n q_i\right)\right)\\
&= \binom{d+2}{2}-\binom{d+2-\deg\left(\prod_{i=1}^n q_i\right)}{2}-1 && \Big(\text{by Lemma 14}\Big)\\
&< \binom{d+2}{2}-\binom{d+1-e}{2}-1. && \Big(\text{by (49)}\Big)
\end{aligned} \tag{53}$$

From (51) and (53), the set B, the flat F and the field $\mathbb{M}$ satisfy the assumptions of Lemma 15. Thus there is $E \in \mathcal{C}_{\leqslant e,\mathbb{M}}$ such that $|B \setminus E| \leqslant d^{\binom{d+2}{2}+1}$. Then

$$\begin{aligned}
\max_{C\in\mathcal{C}_{\leqslant e,\mathbb{M}}} |\rho(A)\cap C| &\geqslant |\rho(A)\cap E| && \left(\text{since } E \in \mathcal{C}_{\leqslant e,\mathbb{M}}\right)\\
&\geqslant |B\cap E| && \left(\text{since } B \subseteq \rho(A)\right)\\
&= |B| - |B\setminus E|\\
&\geqslant |B| - d^{\binom{d+2}{2}+1} && \left(\text{since } |B\setminus E| \leqslant d^{\binom{d+2}{2}+1}\right)\\
&= \max_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\cap C| - d^{\binom{d+2}{2}+1},
\end{aligned}$$

which implies (48) (and hence (47)).

On the one hand, (36) is a direct consequence of (40), (42) and (46). On the other hand, (37) follows from (39), (41) and (43). □

4 Proof of Theorem 2

In this section we complete the proof of Theorem 2, and then we discuss about some details of this theorem.

Proof. (Theorem 2). Let $c_5 = c_5\left(\frac{d(d+3)}{2} - 1\right)$ be a constant satisfying Theorem 10 for $\frac{d(d+3)}{2} - 1$ and write

$$c_1 := \max\{c_5, 1\} + (d+3)\cdot d^{\binom{d+2}{2}+2}.$$

From Lemma 18, there exists a subfield $\mathbb{L}$ of $\mathbb{K}$ such that $A \subseteq \mathbb{L}^2$ and an injective morphism of fields $\rho : \mathbb{L} \longrightarrow \mathbb{C}$ such that for all $e \in [1,d]$,

$$\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\setminus C| \leqslant \min_{C\in\mathcal{C}_{\leqslant e,\mathbb{K}}} |A\setminus C| \leqslant \min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\setminus C| + d^{\binom{d+2}{2}+1} \tag{54}$$

and

$$\left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right| = \left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A))\right|. \tag{55}$$

From Corollary 7, we get that

$$|\mathcal{D}_{d,\mathbb{K}}(A)| \leqslant \left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right| \leqslant d^d\,|\mathcal{D}_{d,\mathbb{K}}(A)|. \tag{56}$$

Since $\mathcal{C}_{\leqslant e,\mathbb{K}} \subseteq \mathcal{C}_{\leqslant d,\mathbb{K}}$ for all $e \in [1,d]$ and $\min_{C\in\mathcal{C}_{\leqslant d,\mathbb{K}}} |A\setminus C| \geqslant c_1$ by assumption, we get that $\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{K}}} |A\setminus C| \geqslant c_1$ for all $e \in [1,d]$. Then, since $c_1 \geqslant 1$, we get from (54) that for all $e \in [1,d]$,

$$\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\setminus C| \leqslant \min_{C\in\mathcal{C}_{\leqslant e,\mathbb{K}}} |A\setminus C| \leqslant 2d^{\binom{d+2}{2}+1} \min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A)\setminus C|. \tag{57}$$

Now we prove that

$$\left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right| = \Theta_d\left(|\rho(A)|^d \prod_{e=1}^{d}\left(\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}}|\rho(A)\setminus C|\right)^{d-e+1}\right). \tag{58}$$

Write $S := \psi_{d,\mathbb{C}}(\rho(A)))$. From Lemma 12,

$$\tau_{d,\mathbb{C}}\left(\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right) = \mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{C}}(S),$$

and by Remark 8.ii, $\tau_{d,\mathbb{C}}$ is a bijection so

$$\left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right| = |\mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{C}}(S)|. \tag{59}$$

On the one hand, for each $f \in [0, d-1]$, fix $R \in \mathcal{F}_f(S)$ such that $\phi_f(S) = |R|$ and also fix a family of flats $\{F_i\}_{i\in I}$ in $\mathbb{C}^{\frac{d(d+3)}{2}}$ satisfying that

$$R \subseteq \bigcup_{i\in I} F_i, \tag{60}$$

$$\sum_{i\in I}\dim F_i = \overline{\dim}\ R \leqslant f, \tag{61}$$

and for all $i \in I$,

$$\dim F_i \geqslant 1. \tag{62}$$

Theorem 9 implies that for any $g \in [0, d-1]$, we have that any g-flat in $\mathbb{C}^{\frac{d(d+3)}{2}}$ can contain at most $g+1$ elements of R; hence, since $f \leqslant d-1$, (61) yields that for all $i \in I$,

$$|R \cap F_i| \leqslant \dim F_i + 1. \tag{63}$$

Thus, for all $f \in [0, d-1]$,

$$\begin{aligned}
\phi_f(S) &= |R| \\
&\leqslant \sum_{i\in I}|R\cap F_i| && \Big(\text{by (60)}\Big) \\
&\leqslant \sum_{i\in I}(\dim F_i + 1) && \Big(\text{by (63)}\Big) \\
&\leqslant f + |I| && \Big(\text{by (61)}\Big) \\
&\leqslant 2f. && \Big(\text{by (61),(62)}\Big)
\end{aligned} \tag{64}$$

Hence, since $|S| = |\rho(A)| > c_1 \geqslant 4d$, we have by (64) that for all $f \in [0, d-1]$,

$$|S| - \phi_f(S) \leqslant |\rho(A)| \leqslant 2(|S| - \phi_f(S)). \tag{65}$$

On the other hand, for all $e, f \in \mathbb{Z}^+$ such that $e \in [1, d]$ and $f \in \left[\binom{d+2}{2} - \binom{d+2-e}{2} - 1, \binom{d+2}{2} - \binom{d+1-e}{2} - 2\right]$, Lemma 16 applied to A yields that

$$|S| - \phi_f(S) \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| \leqslant |S| - \phi_f(S) + \frac{d(d+3)}{2} \cdot d^{\binom{d+2}{2}+1}. \tag{66}$$

Then

$$\begin{aligned}
\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| &\geqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{K}}} |A \setminus C| - d^{\binom{d+2}{2}+1} && \Big(\text{by (54)}\Big) \\
&\geqslant \min_{C \in \mathcal{C}_{\leqslant d,\mathbb{K}}} |A \setminus C| - d^{\binom{d+2}{2}+1} && \Big(\text{since } e \leqslant d\Big) \\
&\geqslant c_1 - d^{\binom{d+2}{2}+1} \\
&\geqslant c_5 + \frac{d(d+3)}{2} \cdot d^{\binom{d+2}{2}+1}
\end{aligned}$$

so we get from (66) that

$$|S| - \phi_f(S) \geqslant c_5 \tag{67}$$

and

$$|S| - \phi_f(S) \leqslant \min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| \leqslant 2(d+3) \cdot d^{\binom{d+2}{2}+2}(|S| - \phi_f(S)). \tag{68}$$

Taking $f = \frac{d(d+3)}{2} - 1$ in (67), we get that the assumptions of Theorem 10 are satisfied by S and $\frac{d(d+3)}{2} - 1$. Then Theorem 10 implies that

$$|\mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{C}}(S)| = \Theta_d \left(\prod_{f=0}^{\frac{d(d+3)}{2}-1} (|S| - \phi_f(S)) \right). \tag{69}$$

Thus

$$\begin{aligned}
&\left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right| \\
=&|\mathcal{G}_{\frac{d(d+3)}{2}-1,\mathbb{C}}(S)| && \Big(\text{by (59)}\Big) \\
=&\Theta_d \left(\prod_{f=0}^{\frac{d(d+3)}{2}-1} (|S| - \phi_f(S)) \right) && \Big(\text{by (69)}\Big) \\
=&\Theta_d \left(|\rho(A)|^d \prod_{e=1}^{d} \left(\min_{C \in \mathcal{C}_{\leqslant e,\mathbb{C}}} |\rho(A) \setminus C| \right)^{d-e+1} \right), && \Big(\text{by (65), (68)}\Big)
\end{aligned}$$

and it concludes the proof of (58).

Finally,

$$\begin{aligned}
|\mathcal{D}_{d,\mathbb{K}}(A)| &= \Theta_d\left(\left|\sigma_{d,\mathbb{K}}^{-1}(\mathcal{D}_{d,\mathbb{K}}(A))\right|\right) && \Big(\text{by (56)}\Big)\\
&= \Theta_d\left(\left|\sigma_{d,\mathbb{C}}^{-1}(\mathcal{D}_{d,\mathbb{C}}(\rho(A)))\right|\right) && \Big(\text{by (55)}\Big)\\
&= \Theta_d\left(|\rho(A)|^d \prod_{e=1}^{d}\left(\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{C}}}|\rho(A)\setminus C|\right)^{d-e+1}\right) && \Big(\text{by (58)}\Big)\\
&= \Theta_d\left(|A|^d \prod_{e=1}^{d}\left(\min_{C\in\mathcal{C}_{\leqslant e,\mathbb{K}}}|A\setminus C|\right)^{d-e+1}\right), && \Big(\text{by (57)}\Big)
\end{aligned}$$

and this completes the proof. □

As it can be noted in the first part of the proof of Theorem 2, the constant $c_1 = c_1(d) \geqslant 0$ depends on the constant $c_5 = c_5\left(\frac{d(d+3)}{2} - 1\right)$ of Theorem 10. It can be noticed in [16, Sec. 7] that the constant c_5 is not easy to compute; nonetheless, Lund proves that $c_5(d) \geqslant d - O(1)$ and he gives a conjecture of a stronger lower bound of $c_5(d)$.

Theorem 2 holds for fields of characteristic zero. Many tools of the proof are true also for more general fields. Nevertheless, Theorem 11 (and therefore Lemma 18) is a fundamental tool in the proof of Theorem 2. Perhaps, using some ultralimits techniques, Theorem 2 can be extended to fields with positive characteristic. Also, maybe some ideas and results established by C. Grosu in [11] are helpful to prove Theorem 2 in $\mathbb{Z}/p\mathbb{Z}$ (however, it seems that Grosu's results cannot be applied directly to achieve this goal so new ideas are required).

Another interesting problem is to generalize Theorem 1.2 to higher dimensional affine algebraic subsets.

Acknowledgements

We would like to thank the referees for their positive and insightful comments and advices to improve this paper.

References

[1] J. Beck, *On the lattice property of the plane and some problems of Dirac, Motzkin and Erdős in combinatorial geometry.* Combinatorica 3, 281-297 (1983).

[2] P. Borwein and W. O. J. Mosser, *A survey of Sylvester's problem and its generalizations*, Aequationes Math 40, 111-135 (1990).

[3] T. Boys, C. Valculescu and F. de Zeeuw, *On the number of ordinary conics*, SIAM J. Discrete Math. 30, 1644-1659 (2016).

[4] P. Brass, W. Moser and J. Pach, *Research problems in discrete geometry*, Springer Science and Business Media, (2005).

[5] A. Czaplinski, M. Dumnicki, L. Farnik, J. Gwozdziewicz, M. Lampa-Baczynska, G. Malara, T. Szemberg, J. Szpond, and H. Tutaj-Gasinska, *On the Sylvester-Gallai theorem for conics*, Rend. Semin. Mat. Univ. Padova 136, 191-203 (2016).

[6] T. Do, *Extending Erdős-Beck's theorem to higher dimensions.* Comput. Geom. 90, 101625 (2020).

[7] E. Elekes, C.D. Tóth, *Incidences of not too degenerate hyperplanes*, Proc. 21st Annu. ACM Sympos. Comput. Geom. 16-21 (2015).

[8] P. Erdős, *On some geometrical problems*, Matematikai Lapok 8, 86-92 (1957).

[9] P. Erdős, *On some problems of elementary and combinatorial geometry*, Annali di Mat. Pura et Applicata 103, 99-108 (1975).

[10] P. Erdős, *On the combinatorial problems which I would most like to see solved*, Combinatorica 1, 25-42 (1981).

[11] C. Grosu, $\mathbb{F}_p$ *is locally like* $\mathbb{C}$, J. Lond. Math. Soc. 89, 724-744 (2014).

[12] R. Hartshorne, *Algebraic Geometry*, Springer, (1977).

[13] A. Iosevich, M. Rudnev, Y. Zhai, *Areas of triangles and Beck's theorem in planes over finite fields*, Combinatorica 35, 295-308 (2015).

[14] W. M. Kantor and E. E. Shult, *Veroneseans, power subspaces and independence*, Adv. Geom. 13, 511-531 (2013).

[15] L. M. Kelly and W. Moser, *On the number of ordinary lines determined by n points*, Canad. J. Math. 10, 210-219 (1958).

[16] B. Lund, *Essential dimension and the flats spanned by a point set.* Combinatorica 38, 1149-1174 (2018).

[17] I. Shafarevich, *Basic Algebraic Geometry 1*, Springer Third Ed., (2013).

[18] T. Tao, *Rectification and the Lefschetz principle*, 14 March 2013, http://terrytao.wordpress.com/2013/03/14/rectification-and-the-lefschetz-principle.

[19] J. Wiseman and P. Wilson, *A Sylvester Theorem for Conic Sections*, Discrete Comput. Geom. 3, 295-305 (1988).