Differential signatures of algebraic curves

Irina A. Kogan, Michael Ruddy, Cynthia Vinzant
North Carolina State University, Raleigh, NC, USA 27695

November 20, 2019

Abstract

In this paper, we adapt the differential signature construction to the equivalence problem for complex plane algebraic curves under the actions of the projective group and its subgroups. Given an action of a group G, a signature map assigns to a plane algebraic curve another plane algebraic curve (a signature curve) in such a way that two generic curves have the same signatures if and only if they are G-equivalent. We prove that for any G-action, there exists a pair of rational differential invariants, called classifying invariants, that can be used to construct signatures. We derive a formula for the degree of a signature curve in terms of the degree of the original curve, the size of its symmetry group and some quantities depending on a choice of classifying invariants. We show that all generic curves have signatures of the same degree and this degree is the sharp upper bound. For the full projective group, as well as for its affine, special affine and special Euclidean subgroups, we give explicit sets of rational classifying invariants and derive a formula for the degree of the signature curve of a generic curve as a quadratic function of the degree of the original curve.

Keywords: Algebraic curves; projective action; affine action; Euclidean action; equivalence classes of curves; differential invariants; classifying invariants; signatures; Fermat curves.

2010 Mathematics Subject Classification: 14H50; 14Q05; 14L24; 53A55; 68W30

1 Introduction

In the most general terms the group equivalence problem can be stated as follows: given an action of a group G on a set of objects, decide whether or not one object can be transformed to another by a group element. An elementary geometry problem of deciding whether or not two triangles are congruent under the action of the group of rigid motions (the Euclidean group) is an example. Many problems in mathematics and applications can be reformulated in this manner, and equivalence problems are closely related to many important classification problems.

In this paper we consider the problem of equivalence of algebraic plane curves under the action of the projective group and its subgroups. This problem plays an important role in algebraic geometry, in particular, in the classical invariant theory [1, 15, 19, 39] [50, Chapter 9] and in the problem of describing moduli spaces of curves [21]. The equivalence problem under the full projective group as well as its classical subgroups, such as (special) Euclidean and (special) affine subgroups naturally arises in computer vision and shape analysis. For a detailed exposition on how each of these groups appear in image processing and analysis, see, for instance, [11, 22]. The variety of applications include medical imaging, automated object and handwriting recognition, and automated assembly. In many of such applications differential signatures of smooth curves and their numerical approximations has been used [4, 6, 26, 16]. Since the differential signature construction originated in differential geometry, much less attention has been given to differential signatures of algebraic curves. However, since algebraic curves such as Bézier curves can be used to represent shapes [17, 46] differential signatures of algebraic

curves can be of interest in applications. One benefit of the algebraic setting is that we can take advantage of well-developed computational algebra algorithms to compute, compare and analyze signature curves.

The differential signature construction originated from Cartan's method for solving equivalence problems for smooth manifolds under Lie group actions [8]. For a modern exposition see [38, Chapter 8], in particular, the notion of classifying manifolds. The differential signature construction for curves consists of the following steps: (1) an action of a group on a plane is prolonged to the jet space of curves of sufficiently high order; (2) on this jet space, a pair of independent differential invariants is constructed; (3) the restriction of this pair to a given curve parametrizes a signature curve. Since the signature is based on invariants, two equivalent curves have the same signature. The challenge lies in finding a pair of invariants so that (most) non-equivalent curves have different signatures. In principle, such a pair of invariants can be found either by the classical moving frame method formulated by Cartan [7] or by its modern generalization given by Fels and Olver [12], although in practice this may be challenging for large groups. The invariants obtained by the moving frame method are, in general, only locally defined and are designed to solve local equivalence problems, i.e. a problem of deciding whether or not there exist segments of two smooth curves that are G-equivalent. The challenges arising when using these signatures for solving global equivalence problems for smooth curves, even in the case of the well-studied Euclidean action, are underscored in the works [24], [25] and [36]. In contrast with the smooth case, any two irreducible algebraic curves that are locally equivalent are also globally equivalent.

In order to take full advantage of the computational algebra algorithms, we need to build a signature from *rational invariants*, in which case the signature of an algebraic curve is again algebraic. The differential invariants obtained by the classical Cartan moving frame method (called normalized invariants) or their counterparts obtained by Fels-Olver generalization (called replacement invariants) are not rational in general. In fact, an algebraic adaptation of the Fels-Olver method given in [28] shows that local replacement invariants, in general, are algebraic over the field of global rational invariants.

As the first main result of this paper, we prove existence of two *rational* differential invariants that can be used to construct signatures with good separation properties:

Result 1. Let $G \subset \mathcal{PGL}(3)$ be any closed algebraic subgroup of the projective group of positive dimension. Then there exists *a pair of rational differential invariants*, called *classifying invariants*, of differential order at most equal to the $\dim G$, such that the signatures based on these invariants characterize equivalence classes of generic algebraic curves of degree d for all d such that $\binom{d+2}{2} - 2 \geq \dim G$. See Theorem 2.37.

Here and throughout the paper we formulate several results for a *generic curve* of degree d. This means that there exists a nonempty Zariski-open subset $\mathcal{P}_d$ of the vector space $\mathbb{C}[x, y]_{\leq d}$ of all polynomials of degree at most d, such that a result is valid for all curves whose defining polynomials lie in $\mathcal{P}_d$.

The result above can be compared with [34, Theorem 2] by Kruglikov and Lychagin, which asserts that, under appropriated conditions, the differential algebra of invariants with respect to an algebraic action of a Lie pseudogroup is generated by a finite set of rational differential invariants and rational differential operators. We note, however, that [34, Theorem 2] does not directly imply the existence of a pair of classifying invariants stated above. In addition, in the case of algebraic subgroups of the projective group considered in this paper, we are able to relax some of the assumptions of [34, Theorem 2], such as a transitivity assumption.

Given a pair of rational classifying invariants, the signature of a curve $X \subset \mathbb{C}^2$ is constructed as follows. The restriction of classifying invariants to an algebraic curve $X \subset \mathbb{C}^2$ defines a rational map $\sigma_X : X \dashrightarrow \mathbb{C}^2$ called the *signature map*. Its image $\mathcal{S}_X = \sigma_X(X)$ is called the *signature* of X, and it is a Zariski-dense[1] subset of its closure $\overline{\mathcal{S}_X}$, called the *signature curve of* X. The defining polynomial for the signature curve can be explicitly computed using elimination

[1]The density statement is not valid over $\mathbb{R}$. See, for instance, [5, Example 1].

algorithms, as was studied in [5]. However this computation is not always practically feasible and it is natural to ask what properties of signature curves can be determined a priori. As the first step in this direction, we obtain a formula for the degree of the signature curve.

Result 2. For a fixed algebraic group and a fixed set of classifying invariants, we derive a formula for the degree of the signature curve of an algebraic curve in terms of the degree of the original curve, the size of its symmetry group, and some quantities that depend on a choice of classifying invariants. See Theorem 3.8. We show that signatures of generic curves all have the same degree and this degree provides the strict upper abound. See Theorem 3.13

Additionally, one may construct a numerical "witness set" for the signature curve. A witness set for a variety encodes information, such as dimension and degree, and allows one to perform numerical procedures on the variety including component sampling and membership tests [2]. Prior knowledge of the degree provides a stopping criterion when using monodromy solvers to construct a witness set for the signature curve.

One of the consequences of Theorem 2.20 is that, over $\mathbb{C}$, a classifying set of differential invariants can be computed by an algorithm for computing generators for the field of rational invariants, such as algorithms presented in [9] and [27]. In fact by computing the graph-section ideal, as presented [27] (using classical geometric cross-sections), we were able to produce the classifying pairs of invariants for the special Euclidean $\mathcal{SE}(2)$, the special affine $\mathcal{SA}(2)$, and the affine $\mathcal{A}(2)$ subgroups of the projective $\mathcal{PGL}(3)$. For the full projective group, however, even the preprocessing step of computing the prolongation[2] of the action to a sufficiently high order was not computational feasible. Fortunately, for the actions of the full projective group $\mathcal{PGL}(3)$ and its classical subgroups one can easily build rational classifying invariants from the classical (non-rational) differential invariants. We give explicit formulas for the classifying pairs for the special Euclidean $\mathcal{SE}(2)$, the special affine $\mathcal{SA}(2)$, the affine $\mathcal{A}(2)$ and projective $\mathcal{PGL}(3)$ groups. These groups are especially relevant in computer vision and image processing. We derive formulas for the degrees of signatures of generic curves based on these pairs of invariants and show that these degrees are sharp upper bounds.

Result 3. For the actions of the full projective group $\mathcal{PGL}(3)$, and its subgroups such as the special Euclidean $\mathcal{SE}(2)$, the special affine $\mathcal{SA}(2)$, the affine $\mathcal{A}(2)$ and the classifying pairs of invariants given by (21), we find an upper bound for the degree of the algebraic signature of a plane curve of degree d. See Theorem 4.13. From Result 2 we know this bound is tight for generic curves.

While the results are proved for complex curves under the action of complex algebraic groups, for many practical applications solving equivalence problems over the real field is important. For this reason, throughout the paper we often compare and contrast with the real case. In particular, we would like to note that the pairs of classifying invariants (21) can be proved to be classifying over $\mathbb{R}$ (see [5]). Therefore, the signature of the real part of a complex curve X is contained in the real part of the signature curve $\overline{\mathcal{S}_X}$. As shown in [5, Example 1] and [42, Example 3.2.12], the real part of the signature curve can contain signatures of two non-equivalent (over the reals) curves, and so utilization of the signature curves for solving equivalence problems over reals becomes more subtle. Nonetheless, the degree results obtained in Theorem 4.13 are also applicable in the real case.

The paper is structured as follows. In Section 2 we review known results about actions and invariants of algebraic groups, as well as the results about the jet spaces and differential invariants. We then prove our first main result about the existence of a pair of classifying invariants. Additionally we establish some basic facts about the relationship of the symmetry group of a curve and the curve's signature map, which play an important role in the degree formulas. In Section 3 we review some necessary definitions and theorems of algebraic geometry and prove our second main result, which is a formula for the degree of the signature polynomial. We also show that signatures of generic curves all have the same degree and this degree provides

[2]We used MAPLE "DifferentialGeometry" package on Apple iMac, Intel Core i7, 3.4 GHz, 8 GB 1600 MHz DDR3.

the strict upper abound. In Section 4 we examine the signature polynomial for some specific examples of subgroups of the projective group and prove our third main result about the degree of signatures of the generic curves for these groups. We also consider the family of Fermat curves, defined by polynomials $F_d(x, y) = x^d + y^d + 1$, to show that the degree of a signature curve may be significantly lower than the generic degree. For this family, we give explicit formulas for signatures polynomials for all d under the actions of the projective and affine group.

Although the paper contains only few examples and computational details, the Maple code and a large selection of examples are available on an online supplementary material page `https://mgruddy.wixsite.com/home/dsag-supplementarymaterials`.

Acknowledgements. We would like to thank Bojko Bakalov, Peter Olver, Kristian Ranestad, and Dmitry Zenkov for helpful discussions and suggestions regarding this project. This work was supported in part by the National Science Foundation grants DMS-1620014 and CCF-1319632.

2 Differential invariants and signatures of algebraic curves

In this section, we prove our main structural results about the field of rational differential invariants and signatures of algebraic curves. We start by reviewing, in Section 2.1, known results about actions and invariants of algebraic groups. In Section 2.2, we consider the action of the projective group and its subgroups on algebraic curves, give definitions of equivalence and symmetry for algebraic curves, and prove some useful results about the symmetry groups of curves (Propositions 2.9-2.11). In Section 2.3 we prolong the action to the jet space of curves and define the notion of rational classifying differential invariants. We prove an important structural result about the field of rational differential invariants (Theorem 2.17), as well the existence of a classifying set (Theorem 2.20). In Section 2.4, we show how differential invariants are evaluated on an algebraic curve. We define the notion of exceptional curves and show that generic curves are non-exceptional (Theorem 2.27). Section 2.5, we define the signature map and the signature curve of a non-exceptional algebraic curve. We show that signatures characterize the equivalence classes of generic algebraic curves (Theorem 2.37) and prove that the signature map of a curve X is generically n to one where n is the cardinality of the symmetry group of X (Theorem 2.38).

2.1 Actions and invariants of algebraic groups

In this section, we review common definitions and known results about actions and invariants of algebraic groups on algebraic varieties. The exposition follows [50], and we refer to this publication for details, proofs, and further references.

Throughout the section the ground field is $\mathbb{C}$ and the terms "open" and "closed" refer to Zariski topology. An *algebraic group* is an algebraic variety equipped with a group structure.

Definition 2.1. Let $\mathcal{Y}$ be an affine or a projective variety. A *rational action* of an algebraic group G on $\mathcal{Y}$ is a rational map $\Phi\colon G \times \mathcal{Y} \dashrightarrow \mathcal{Y}$ that satisfies the following two properties:

1. $\Phi(e, p) = p$, $\forall p \in \mathcal{Y}$, where e is the identity in G, and
2. $\Phi(h, \Phi(g, p)) = \Phi(hg, p)$, for all $h, g \in G$ and $p \in \mathcal{Y}$, such that both sides are defined.

If the domain of Φ is all of $G \times \mathcal{Y}$ then Φ is a morphism and the action is called *regular*.

From now on, when the word "action" is used without an adjective, a rational action is assumed. We use the standard abbreviation $\Phi(g, p) = g \cdot p$ and state the following known definitions and results used in our paper.

Definition 2.2. For an action of G on a variety $\mathcal{Y}$ and a point $p \in \mathcal{Y}$, the *stabilizer of* p is the set

$$G_p = \{g \in G \mid g \cdot p = p\},$$

while the *orbit of* p is the set

$$Gp = \{q \in \mathcal{Y} \mid \exists g \in G, g \cdot p = q\},$$

We recall some basic properties of algebraic group actions. The following proposition is condensed from the results stated in Sections 1.3 and 1.4 in [50].

Proposition 2.3. Let G be an algebraic group acting on an affine (or projective) variety $\mathcal{Y}$. For any $p \in \mathcal{Y}$, the stabilizer G_p is a closed algebraic subgroup of G. The orbit Gp is a quasi-affine (or quasi-projective) variety and

$$\dim Gp = \dim G - \dim G_p.$$

If $\mathcal{Y}$ is irreducible then the set of all points whose orbit dimension is less than maximal (equivalently the dimension of the stabilizer group is greater than minimum) lies in a closed, proper subset of $\mathcal{Y}$. Finally, if G is irreducible, then for all $p \in \mathcal{Y}$ the closure of the orbit $\overline{Gp}$ is irreducible. This follows from the fact that the image of an irreducible variety under a rational map is in turn irreducible.

Definition 2.4. A rational function K on $\mathcal{Y}$ is G-invariant if

$$K(g \cdot p) = K(p), \text{ whenever both sides are defined.}$$

The set of all rational G-invariant functions is denoted by $\mathbb{C}(\mathcal{Y})^G$. It is easy to see that it is a subfield of the field $\mathbb{C}(\mathcal{Y})$ of all rational functions on $\mathcal{Y}$.

Definition 2.5. A subset $\mathcal{I} \subset \mathbb{C}(\mathcal{Y})^G$ is called *separating* if there exists a nonempty open subset $W \subset \mathcal{Y}$ such that for all $p, q \in W$,

$$q \in Gp \;\Leftrightarrow\; K(p) = K(q) \text{ for all } K \in \mathcal{I}.$$

The set W is called a *domain of separation* for $\mathcal{I}$, and we say $\mathcal{I}$ *separates orbits on* W. Due to the Noetherian property, there exists a *maximal* (with respect to inclusions) *domain of separation*. Since the invariants are constant on orbits, if p belongs to the maximal domain of separation, then so does the entire orbit Gp. Thus the maximal domain of separation is a union of orbits, and therefore is a G-invariant set.

In the following proposition, we summarize several important and non-trivial results about the structure of $\mathbb{C}(\mathcal{Y})^G$ stated in [50].[3]

Proposition 2.6.

1. The field $\mathbb{C}(\mathcal{Y})^G$ is finitely generated over $\mathbb{C}$. (See Lemma 2.1 and Theorem 2.3 in [50].)
2. A subset $\mathcal{I} \subset \mathbb{C}(\mathcal{Y})^G$ is generating if and only if it is separating.
3. The transcendence degree of $\mathbb{C}(\mathcal{Y})^G$ over $\mathbb{C}$ equals to $\dim \mathcal{Y} - \max\limits_{p \in \mathcal{Y}} \dim Gp$.
4. If the field $\mathbb{C}(\mathcal{Y})$ is rational[4] and the transcendence degree of $\mathbb{C}(\mathcal{Y})^G$ over $\mathbb{C}$ equals to 1 or 2, then $\mathbb{C}(\mathcal{Y})^G$ is rational over $\mathbb{C}$.

Remark 2.7. It is worthwhile mentioning that the second part of the proposition is not valid over real numbers. For example, the field of rational invariants for the action of the group $\mathbb{R}^*$ (non-zero real numbers under multiplication) on $\mathbb{R}^2$ defined by $(x, y) \mapsto (\lambda^2 x, \lambda^2 y)$ is generated by $K = \frac{x}{y}$, but K is not separating. Conversely, for the translation action of $\mathbb{R}$ on $\mathbb{R}^2$ defined by $(x, y) \mapsto (x + a, y)$, the invariant $K = y^3$ is separating but not generating.

[3] The first two bullets are direct consequences of Lemma 2.1 and Theorem 2.3 in [50]. The third bullet is the unnumbered Corollary stated on p.156 of [50] after Lemma 2.4. The fourth bullet is the result stated at the beginning of Section 2.9 on p.162 of [50] and attributed to Lüroth and Castelnuovo.

[4] i.e. isomorphic to a field of rational functions of a finite number of independent variables.

2.2 Equivalence classes and symmetries of algebraic curves

We now restrict our attention to regular actions of algebraic groups on the complex projective plane $\mathbb{CP}^2$. Such an action induces a homomorphism from G to $Aut(\mathbb{CP}^2) = \mathcal{PGL}(3)$, see [23, Example II.7.1.1]. Thus we view an algebraic group G acting on $\mathbb{CP}^2$ as a closed subgroup of the projective linear group $\mathcal{PGL}(3)$[5]. An element $g \in G$ can be represented by a 3×3 non-singular complex matrix A_g, which is defined up to scaling. We use homogeneous coordinates $[x_0 : x_1 : x_2]$ to represent a point $\mathbf{p} \in \mathbb{CP}^2$. Then the action of G on $\mathbb{CP}^2$ is defined by:

$$g \cdot \mathbf{p} = [\phi_0(g, \mathbf{p}) : \phi_1(g, \mathbf{p}) : \phi_2(g, \mathbf{p})], \text{ where } \begin{bmatrix} \phi_0(g, \mathbf{p}) \\ \phi_1(g, \mathbf{p}) \\ \phi_2(g, \mathbf{p}) \end{bmatrix} = A_g \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix}. \tag{1}$$

On $\mathbb{C}^2$, we use coordinates (x, y). For an affine point $p = (x, y) \in \mathbb{C}^2$, we use an abbreviation $[1 : p] = [1 : x : y]$ to denote the corresponding projective point. The action (1) induces a rational action $\Phi : G \times \mathbb{C}^2 \dashrightarrow \mathbb{C}^2$ given by

$$g \cdot p = \left(\frac{\phi_1(g, [1 : p])}{\phi_0(g, [1 : p])}, \frac{\phi_2(g, [1 : p])}{\phi_0(g, [1 : p])} \right). \tag{2}$$

We are interested in the characterization of the equivalence classes of algebraic curves under this action. Given a curve $X \subset \mathbb{C}^2$, let $g \cdot X$ denote the the image of X under g, namely $\Phi(g, X)$. As this is a rational action, the image may not be an algebraic curve, and so we will consider its Zariski closure $\overline{g \cdot X}$.

Definition 2.8. We say that an algebraic curve $X \subset \mathbb{C}^2$ is *G-equivalent* to an algebraic curve $Y \subset \mathbb{C}^2$ if there exists $g \in G$ such that $X = \overline{g \cdot Y}$.

Clearly G-equivalence satisfies all properties of an equivalence relation, and we use the notation $X \underset{G}{\cong} Y$ to denote the G-equivalence of curves X and Y. Elements $g \in G$ defining self-equivalences of X are called symmetries of X in G. The set of all symmetries

$$\mathrm{Sym}(X, G) = \{g \in G \mid X = \overline{g \cdot X}\}$$

form a closed algebraic subgroup of G, called the *symmetry group* of X with respect to G.

Note that the symmetries of X that fix every point of the curve form a normal subgroup of $\mathrm{Sym}(X, G)$, called the *stabilizer group* of X with respect to G:

$$\mathrm{Stab}(X, G) = \bigcap_{p \in X} G_p.$$

We show that for a natural class of curves, $\mathrm{Stab}(X, G)$ only consists of the identity element.

Proposition 2.9. For an irreducible curve $X \subset \mathbb{C}^2$ of degree greater than one, the stabilizer group $\mathrm{Stab}(X, G)$ consists of only the identity.

Proof. For $g \in G$ let $A_g \in \mathcal{GL}(3)$ be any of its representatives. Let $\mathbb{C}^2_g$ denote the set of points in $\mathbb{C}^2$ fixed by a particular element g, i.e.

$$\mathbb{C}^2_g = \{p \in \mathbb{C}^2 \, : \, g \cdot p = p\}.$$

A point $p \in \mathbb{C}^2$ is fixed by g if and only if $(1, p)$ is an eigenvector of A_g. Therefore, the set $\mathbb{C}^2_g$ is the intersection of the affine plane $\{x_0 = 1\}$ with the union of the eigenspaces of the matrix A_g. There are three possibilities: (1) A_g has three linearly independent eigenvectors, then $\mathbb{C}^2_g$ consists of at most[6] three distinct points, (2) A_g has an eigenspace of dimension 2 and

[5] From now on we will refer to $\mathcal{PGL}(3)$ as the projective group.

[6] "At most" because an eigenspace may be parallel to the $\{x_0 = 1\}$ plane.

an eigenspace of dimension 1, then $\mathbb{C}^2_g$ consists of at most a line and a point, (3) A_g has an eigenspace of dimension 3, then $\mathbb{C}^2_g = \mathbb{C}^2$.

If $g \in \mathrm{Stab}(X, G)$, then $X \subset \mathbb{C}^2_g$. Since X is irreducible of degree > 1, it follows that $\mathbb{C}^2_g = \mathbb{C}^2$. This implies that A_g is a scalar multiple of the identity matrix and g is the identity element of $\mathcal{PGL}(3)$. □

We finish this section by proving two useful propositions concerning the orbits of $\mathrm{Sym}(X, G)$.

Proposition 2.10. If X is irreducible of degree greater than one, then $|\mathrm{Sym}(X, G)|$ is infinite if and only if there exists a point $p \in X$ whose orbit under $\mathrm{Sym}(X, G)$ is dense in X.

Proof. Let $H = \mathrm{Sym}(X, G)$. This is an algebraic group acting on X.

($\Rightarrow$) Assume $|H|$ is infinite. Then since H is algebraic, $\dim H > 0$. Let H^0 denote the connected component of H containing e. By [48, Prop. 2.2.1], this is a closed normal subgroup of H of finite index and so $\dim H^0 > 0$. By Proposition 2.3, for any $p \in X$ the orbit $H^0 p$ is an irreducible quasi-affine subvariety of X. Since $\dim X = 1$, the dimension of $H^0 p$ is either zero or one. If for all $p \in X$, $\dim H^0 p = 0$, then $H^0 p = \{p\}$ for all $p \in X$. In this case, $\mathrm{Stab}(X, G)$ contains H^0, contradicting the statement of Proposition 2.9. Therefore, there exists $p \in X$ such that $\dim H^0 p = 1$. Since X is irreducible of dimension 1, this implies $\overline{H^0 p} = X$.

($\Leftarrow$) Assume there exists a point $p \in X$ whose orbit under H is dense in X. Then $\dim Hp = 1$. By Proposition 2.3, $\dim Hp \leq \dim H$. Therefore $\dim H > 0$ and so $|H|$ is infinite. □

Proposition 2.11. If X is irreducible of degree greater than one and $|\mathrm{Sym}(X, G)| = n < \infty$, then for all but finitely many points $p \in X$ the orbit under $\mathrm{Sym}(X, G)$ consists of exactly n distinct points.

Proof. Let $H = \mathrm{Sym}(X, G)$. For $g \in H$, define $X_g = \{p \in X \mid g \cdot p = p\}$. From the proof of Proposition 2.9 it follows that if $g \neq e$, then X_g is either empty or finite. Consider the set $E_g = \{p \in X \mid g \cdot p \text{ is undefined}\}$, which is also empty or finite. Since $|H|$ is finite, the set $\Delta = \cup_{g \in H}(E_g \cup X_g)$ is empty or finite. For all $p \in X \backslash \Delta$, $g \cdot p$ is defined for all $g \in H$ and the stabilizer is $H_p = \{e\}$. Then $|Hp| = |H|/|H_p| = n$. □

It is important to note that under the action $G \subset \mathcal{PGL}(3)$ described by (2) the degree and the irreducibility property are preserved. From now on and throughout the paper we will make the following assumptions:

Assumption 2.12.

1. A group G is a closed subgroup of $\mathcal{PGL}(3)$ with $\dim G > 0$.
2. The rational action of G on $\mathbb{C}^2$ is defined by (1) and (2).
3. $X \subset \mathbb{C}^2$ is an irreducible algebraic curve of degree greater than one.

2.3 Classifying differential invariants

To define differential invariants, we prolong the action of G to the jet space J^n of planar curves. For our purposes, we can ignore the points where the curve has vertical tangent[7] and identify J^n with $\mathbb{C}^{n+2}$. The coordinate functions on J^n are denoted by $(x, y, y^{(1)}, \ldots, y^{(n)})$. Although formally, $y^{(k)}$ is viewed as an independent coordinate function, we define the prolongation formulas keeping in mind that $y^{(k)}$ is the "place holder" for the k-th derivative of y with respect to x.

[7] By ignoring these points we restrict ourselves to a dense open subset of what in [37] is called an extended jet bundle. See Chapter 3 of [37] and in particular Definition 3.27 and Example 3.29 for a detailed discussion of the relationship between a local jet space and a global jet bundle of curves.

Definition 2.13. Let G act on $\mathbb{C}^2$. For $g \in G$, let $(\overline{x}, \overline{y}) = g \cdot (x, y)$. *The prolongation of the G-action from $\mathbb{C}^2$ to J^n* is a rational action defined by

$$g \cdot (x, y, y^{(1)}, \dots, y^{(n)}) = (\overline{x}, \overline{y}, \overline{y}^{(1)}, \dots, \overline{y}^{(n)})$$

where

$$\overline{y}^{(1)} = \frac{\frac{d}{dx}\left[\overline{y}(g, x, y)\right]}{\frac{d}{dx}\left[\overline{x}(g, x, y)\right]} \quad \text{and} \quad \overline{y}^{(k+1)} = \frac{\frac{d}{dx}\left[\overline{y}^{(k)}(g, x, y, y^{(1)}, \dots, y^{(k)})\right]}{\frac{d}{dx}\left[\overline{x}(g, x, y)\right]} \text{ for } k = 1, \dots, n-1.$$

The operator $\frac{d}{dx}$ is the *total derivative operator*. This is the unique $\mathbb{C}$-linear operator mapping $C(J^n) \to C(J^{n+1})$ for $n \geq 0$ satisfying the product rule, $\frac{d}{dx}(x) = 1$, and $\frac{d}{dx}(y^{(k)}) = y^{(k+1)}$ for $k \geq 0$. Here we use the convention that $y = y^{(0)}$ and coordinate functions of g are considered to be constant with respect to x.

This is illustrated for the prolongation of the action of $\mathcal{SE}(2)$ to J^2 in Example 2.39.

Definition 2.14. A rational function $K(x, y, y^{(1)}, \dots, y^{(n)})$ on J^n is called a *rational differential function*. The *differential order* of K is the maximal k, such that K explicitly depends on $y^{(k)}$:

$$\operatorname{ord}(K) = \max_i \left\{ i \,\middle|\, \frac{\partial K}{\partial y^{(i)}} \neq 0 \right\}.$$

If K is invariant under the prolonged action it is called a *rational differential invariant*.

Note that if $\operatorname{ord}(K) = k$, then $K \in \mathbb{C}(J^n)$ for all $n \geq k$. In Theorem 2.17, we show that the field $\mathbb{C}(J^r)^G$ of rational invariants of the order at most $r = \dim G$ has a very simple structure. We start by formulating (in our context) an important result originally due to Ovsiannikov [41] (see also [38, Theorem 5.11]).[8]

Proposition 2.15. Let a group G of dimension r act on $\mathbb{C}^2$. Then there is $k \geq 0$ such that, for all $n \geq k$, the maximal orbit dimension of the prolonged action on J^n is r.

We use the following lemma to prove Theorem 2.17. Under an assumption of *functional independence* it is proven in [38, Prop. 5.15].

Lemma 2.16. Assume K_1 and K_2 are two algebraically independent rational differential invariants, such that $\max\{\operatorname{ord}(K_1), \operatorname{ord}(K_2)\} = k$. Then

$$\frac{dK_2}{dK_1} := \frac{\frac{dK_2}{dx}}{\frac{dK_1}{dx}}$$

is a rational differential invariant of order $k + 1$.

Proof. Consider the rational map $\varphi : J^k \dashrightarrow \mathbb{C}^2$ defined by $\varphi = (K_1, K_2)$. Since K_1 and K_2 are algebraically independent, the image of φ is dense in $\mathbb{C}^2$. The map φ is regular on a Zariski-open subset of J^k, and hence by [45, Ch. 2, Sec. 6, Lem. 2.4], the differential $d_p\varphi$ is of full rank on a Zariski-open subset of J^k. It follows that two rational functions are functionally independent (see page 85 of [37]) and the result follows from [38, Prop. 5.15].

□

The proof of the next theorem invokes the line of the argument in the proof of Theorem 5.24 in [38] in combination with Proposition 2.6 stated above.

[8] We stated this result under Assumptions 2.12 given at the beginning of the section. For general actions of algebraic groups on algebraic varieties one needs to assume local effectiveness of the action (the set of elements in G with a trivial action is finite). The theorem was originally stated for Lie groups acting on smooth (non-algebraic) real manifolds, and in this setting, as was shown in [40], a stronger assumption of local effectiveness on all open subsets is required. The proof remains valid over $\mathbb{C}$.

Theorem 2.17. Let $\dim G = r$, then the field of $\mathbb{C}(J^r)^G$ of rational invariants on J^r is a rational field of transcendence degree two over $\mathbb{C}$. In other words, there exists two rational invariants K_1 and K_2 such that

$$\mathbb{C}(J^r)^G = \mathbb{C}(K_1, K_2). \tag{3}$$

Moreover K_1 and K_2 can be chosen so that K_1 is of differential order k, strictly less than r, and K_2 is of differential order r. In addition, the field $\mathbb{C}(J^k)^G$ of rational invariants on J^k is a rational field of transcendence degree one and

$$\mathbb{C}(J^k)^G = \mathbb{C}(K_1). \tag{4}$$

Proof. The dimension of an orbit can not exceed the dimension of the group. Therefore, since $\dim J^{r-1} = r+1$, the transcendence degree of $\mathbb{C}(J^{r-1})^G$ is at least 1 by Part 3. of Proposition 2.6. Thus there exists a rational invariant K_1 such that $\operatorname{ord}(K_1) = k_1 < r$. We may assume that the order k_1 of K_1 is minimal among all such invariants. Similarly, since $\dim J^r = r + 2$, the transcendence degree of $\mathbb{C}(J^{r-1})^G$ is at least 2, and there exists a rational invariant K_2, algebraically independent from K_1, such that $\operatorname{ord}(K_2) = k_2 \leq r$. By the minimality assumption on k_1, we have $k_1 \leq k_2$. Assume that $k_2 < r$. By Lemma 2.16, invariant $H_1 = \frac{dK_2}{dK_1}$ is of order $k_2 + 1$. For $i > 1$, we define invariants $H_i = \frac{dH_{i-1}}{dK_1}$. The $n+2$ invariants $K_1, K_2, H_1, H_2, \ldots, H_n$ are of orders $k_1, k_2, k_2 + 1, \ldots k_2 + n$, respectively. Since K_1 and K_2 are independent, and each subsequent invariant contains a new jet variable, the gradients of these invariants as functions on J^{k_2+n} are independent, and hence the invariants are independent. Therefore the maximal orbit dimension on J^{k_2+n} does not exceed $\dim J^{k_2+n} - (n + 2) = k_2$. Since n can be arbitrary large, it follows from Proposition 2.15 that $k_2 = r$. In summary, we proved so far

$$k_1 < k_2 = r$$

and that there are no differential invariants of orders strictly less than k_1, or strictly between k_1 and r.

Assume that there is an invariant K_3 of order r, independent of K_1 and K_2. Then by similar argument as in the above paragraph, the $n + 3$ invariants $K_1, K_2, K_3, H_1, H_2, \ldots, H_n$ of orders $k_1, r, r, r + 1, \ldots r + n$, respectively, are independent for all n. It follows that the maximal orbit dimension on J^{r+n} does not exceed $\dim J^{r+n} - (n + 3) = r - 1$ for all n. This contradicts Proposition 2.15.

We conclude that the transcendence degree of $\mathbb{C}(J^k)^G$ is 1 and the transcendence degree of $\mathbb{C}(J^r)^G$ is 2. Then (3) and (4) follow from Part 4 of Proposition 2.6. □

Remark 2.18. In fact, from Theorem 5.24 in [38] and Sophus Lie's classification of all infinitesimal group actions on the plane (see Table 5 in [38]) it follows that there are only three possibilities for the differential order k of the lower order classifying invariant K_1, namely $k = r - 1$, $k = r - 2$ and $k = 0$. For most of the actions (and all actions considered in Section 4 of this paper) $k = r - 1$. The case $k = 0$ occurs if and only if the action G is intransitive on $\mathbb{C}^2$. An example of such action is the action of a 2-dimensional subgroup of $\mathcal{PGL}(3)$, given by $(x, y) \to (\lambda x + a, y)$, where $\lambda \in \mathbb{C}^*$ is non-zero and $a \in \mathbb{C}$. Among subgroups of $\mathcal{PGL}(3)$, the third possibility, $k = r - 2 \neq 0$, occurs only for two actions: (1) a three-dimensional subgroup acting by $(x, y) \to (\lambda x + a, \lambda y + b)$, where $\lambda \in \mathbb{C}^*$ and $a, b \in \mathbb{C}$ and (2) a four-dimensional subgroup acting by $(x, y) \to (\lambda x + a, cx + \lambda^2 y + b)$, where $\lambda \in \mathbb{C}^*$ and $a, b, c \in \mathbb{C}$

We can use the same definition of the classifying invariants as was given in [5, Definition 7] in the real case.

Definition 2.19. Let an r-dimensional algebraic group G act on $\mathbb{C}^2$. Let K_1 and K_2 be *rational differential invariants* of orders $k < r$ and r, respectively. The set $\mathcal{I} = \{K_1, K_2\}$ is called *classifying* if K_1 separates orbits on a nonempty Zariski-open subset $W^k \subseteq J$ and $\mathcal{I}$ separates orbits on a nonempty Zariski-open subset $W^r \subseteq J^r$.

Over $\mathbb{C}$ we can prove existence of a classifying set of invariants of any group action:

Theorem 2.20. For any action of $G \subset \mathcal{PGL}(3)$ on $\mathbb{C}^2$ there exists a classifying set $\mathcal{I} = \{K_1, K_2\}$ of differential invariants. Moreover the set $\mathcal{I}$ is classifying if and only if $\mathcal{I}$ generates the field $\mathbb{C}(J^r)^G$ of rational differential invariants of order at most $r = \dim G$ and K_1 generates the field $\mathbb{C}(J^{r-1})^G$ of rational invariants of order at most $r-1$.

Proof. This result follows immediately from Theorem 2.17 and Part 2 of Proposition 2.6. □

Remark 2.7 underscores that over $\mathbb{R}$ the above proof of Theorem 2.20 is not valid. It is an interesting question, whether or not the statement of this theorem (or possibly some modification) is valid over $\mathbb{R}$. In Section 2.5 we show that signatures based on classifying invariants characterize the equivalence classes of generic algebraic curves. In Section 4.1 we list classifying sets of invariants for the full projective group and several of its classical subgroups. The following propositions asserts a simple relationship between any two classifying sets of invariants.

Proposition 2.21. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying sets of differential invariants for the action of G on $\mathbb{C}^2$. Let $\tilde{\mathcal{I}} = \{\tilde{K}_1, \tilde{K}_2\}$ be another pair of differential invariants. Then $\tilde{\mathcal{I}}$ is a classifying set if and only if there exist constants $a, b, c, d \in \mathbb{C}$, such that $ad - bc \neq 0$ and rational functions $\alpha, \beta, \gamma, \delta \in \mathbb{C}(\kappa)$, such that $\alpha\delta - \gamma\beta \neq 0$ such that

$$\tilde{K}_1 = \frac{aK_1 + b}{cK_1 + d} \text{ and } \tilde{K}_2 = \frac{\alpha(K_1)K_2 + \beta(K_1)}{\gamma(K_1)K_2 + \delta(K_1)}. \tag{5}$$

Proof. By Theorems 2.17 and 2.20, we know that $\mathbb{C}(J^k)^G = \mathbb{C}(K_1)$ and $\mathbb{C}(J^r)^G = \mathbb{C}(K_1, K_2)$ are rational fields of transcendence degrees 1 and 2 respectively for $r = \dim G$ and some integer $k < r$. Moreover, from the proof of Theorem 2.17, we know that there are no differential invariants of order strictly greater than k and strictly less than r.

Assume first that $\tilde{\mathcal{I}}$ is a classifying set. Then for $r = \dim G$ and some integer $k < r$, we have $\operatorname{ord}(\tilde{K}_2) = r$ and $\operatorname{ord}(\tilde{K}_1) = k$ and $\mathbb{C}(J^k)^G = \mathbb{C}(\tilde{K}_1)$ and $\mathbb{C}(J^r)^G = \mathbb{C}(\tilde{K}_1, \tilde{K}_2)$. Now we have two sets of generators for each of the fields $\mathbb{C}(J^k)^G$ and $\mathbb{C}(J^r)^G$ and so there exist invertible rational functions $\Phi \in \mathbb{C}(\kappa_1)$ and $\Psi \in \mathbb{C}(\kappa_1, \kappa_2)$ such that $\tilde{K}_1 = \Phi(K_1)$ and $\tilde{K}_2 = \Psi(K_1, K_2)$. The function Φ induces an automorphism of $\mathbb{C}(J^k)^G$ fixing $\mathbb{C}$. It is known (see, for instance, [29, Exercise 6, Sec. V.2]) that the only automorphisms of a rational field $\mathbb{K}(z)$ fixing the ground field $\mathbb{K}$ are given by linear fractional maps over $\mathbb{K}$. The first formula in (5) follows with $\mathbb{K} = \mathbb{C}$. Similarly Ψ induces an automorphism of $\mathbb{C}(J^r)^G = \mathbb{C}(J^k)^G(K_2)$ fixing $\mathbb{C}(J^k)^G = \mathbb{C}(K_1)$. By the same argument, with $\mathbb{K} = \mathbb{C}(K_1)$, the second formula in (5) follows.

Now assume that $\tilde{K}_1$ and $\tilde{K}_2$ are given by (5). Then since these formulas are invertible, $\operatorname{ord}(\tilde{K}_1) = k$, $\operatorname{ord}(\tilde{K}_2) = r$, and $\mathbb{C}(J^k)^G = \mathbb{C}(\tilde{K}_1)$, while $\mathbb{C}(J^r)^G = \mathbb{C}(\tilde{K}_1, \tilde{K}_2)$. By Theorem 2.20, $\tilde{\mathcal{I}} = \{\tilde{K}_1, \tilde{K}_2\}$ is a classifying set. □

2.4 Restriction to algebraic curves

To evaluate differential functions on an affine curve, we lift the curve into the jet space as follows. Let $F(x, y) \in \mathbb{C}[x, y]$ be irreducible and $X = V(F) \subset \mathbb{C}^2$. For any point $p = (p_1, p_2) \in X$ with $F_y(p) \neq 0$ the curve X agrees in some neighborhood of p with the graph of an analytic function $y = f(x)$. Then for a positive integer n, we can define $y_X^{(n)}(p) = f^{(n)}(p_1)$ to be the n-th derivative of $f(x)$ at $x = p_1$. One can show that for each $n \in \mathbb{Z}_+$, $y_X^{(n)}$ is a rational function on X that, using the implicit differentiation, can be written as a rational function of partial derivatives of F. For example,

$$y_X^{(1)} = \frac{-F_x}{F_y} \quad \text{and} \quad y_X^{(2)} = \frac{-F_{xx}F_y^2 + 2F_{xy}F_xF_y - F_{yy}F_x^2}{F_y^3}. \tag{6}$$

Definition 2.22. The *n-th jet* of a curve $X \subset \mathbb{C}^2$, denoted $X^{(n)}$, is the algebraic closure of the image of X under the rational map $j_X^n : X \dashrightarrow J^n$, where for $p \in X$,

$$j_X^n(p) = (x(p), y(p), y_X^{(1)}(p), \ldots, y_X^{(n)}(p)).$$

Note that the prolongation of the action of G to J^n (Definition 2.13) is defined so that the following fundamental property holds:

$$j^n_{g\cdot X}(g\cdot p) \;=\; g\cdot j^n_X(p) \;\text{ for all } g\in G \text{ and } p\in X \text{ where } g\cdot p \text{ is defined.} \tag{7}$$

In particular, the n-th jet of the image of X under the action of $g\in G$ coincides with the image of the n-th jet of X under the prolonged action of g:

$$\overline{g\cdot X^{(n)}} = \overline{(g\cdot X)^{(n)}}. \tag{8}$$

Definition 2.23. For a curve X, the *restriction* of a differential function K to X is denoted $K|_X$ and defined by the composition, $K|_X = K\circ j^n_X$.

If K is a *rational* differential function on J^n, then $K|_X$ is a rational function on X, and we can obtain the explicit formula for $K|_X$ as a rational function of x and y by substituting the expressions $y^{(1)}_X,\dots,y^{(n)}_X$ in (6) for coordinates $y^{(1)},\dots,y^{(n)}$.

Definition 2.24. Let $\mathcal{I}=\{K_1,K_2\}$ be a classifying set of rational differential invariants for a group G of dimension r. Let $\operatorname{ord}(K_1)=k$ and let $W_1\subset J^k$ be a maximal domain of separation for $\{K_1\}$ and $W_2\subset J^r$ be a maximal domain of separation for $\mathcal{I}$. Then, for $X\subset\mathbb{C}^2$, a point $p\in X$ is called *$\mathcal{I}$-regular* if

(a) $j^r_X(p)$ is defined;

(b) $j^k_X(p)\in W_1$ and $j^r_X(p)\in W_2$;

(c) $\frac{\partial K_1}{\partial y^k}\big|_{j^k_X(p)}\neq 0$ if K_1 is constant on X, and $\frac{\partial K_2}{\partial y^{(r)}}\big|_{j^r_X(p)}\neq 0$ otherwise.

The condition that $j^r_X(p)$ is defined can equivalently be stated as $F_y(p)\neq 0$ where $F(x,y)$ is the polynomial whose zero set equals X. Thus singular points of X are not $\mathcal{I}$-regular.

Definition 2.25. A complex algebraic curve $X\subset\mathbb{C}^2$ is called *non-exceptional* with respect to a classifying set of differential invariants, $\mathcal{I}$, if all but a finite number of its points are $\mathcal{I}$-regular.

We will need the following lemma to show that generic curves are non-exceptional.

Lemma 2.26. Let d,n be positive integers satisfying $n\leq\binom{d+2}{2}-2$. For a generic point $a=(a_0,\dots,a_n)\in\mathbb{C}^{n+1}$, there exists an algebraic curve $X\subset\mathbb{C}^2$ of degree d for which $(0,a_0)\in X$ and $j^{(n)}_X(0,a_0) \;=\; (0,a_0,\dots,a_n)$.

Proof. Consider the subset $\mathcal{Y}$ of $\mathbb{P}(\mathbb{C}[x,y]_{\leq d})\times\mathbb{C}^{n+1}$ consisting of pairs $([F],a)$ for which F is irreducible of degree d, $F(0,a_0)=0$, $F_y(0,a_0)\neq 0$, and $j^{(n)}_{V(F)}(0,a_0)=(0,a_0,\dots,a_n)$. Since $j^{(n)}_{V(F)}$ is a rational function of both the points of $V(F)$ and the coefficients of F, as seen in (6), this is a quasi-projective variety. The conditions $F(0,a_0)=0$ and $a_k=y^{(k)}_X(0,a_0)$ are algebraically independent, since each involves a new variable, a_k. From this, it follows that $\mathcal{Y}$ has codimension $n+1$ in $\mathbb{P}(\mathbb{C}[x,y]_{\leq d})\times\mathbb{C}^{n+1}$ and thus dimension $\binom{d+2}{2}-1$. The projection of $\mathcal{Y}$ onto $\mathbb{C}^{n+1}$ is therefore a quasi-affine variety. It either contains a nonempty Zariski-open set or is contained in a hypersurface in $\mathbb{C}^{n+1}$. We need to rule out the latter when $n\leq\binom{d+2}{2}-2$.

Suppose for the sake of contradiction that for some $n\leq\binom{d+2}{2}-2$, there is a polynomial relation $P(y,y^{(1)},\dots,y^{(n)})=0$ that holds for every point on the image of $X\cap V(x)$ under $j^{(n)}_X$ for every irreducible curve X of degree d. Without loss of generality, we can assume that n is the minimal integer for which this holds and that the polynomial P is irreducible. Then, by Bertini's theorem, for generic $a_0,\dots,a_{n-1}\in\mathbb{C}$, $P(a_0,\dots,a_{n-1},y^{(n)})$ is a non-zero polynomial in $y^{(n)}$ with simple roots, around which $y^{(n)}$ is an analytic function of $a_0,\dots,a_{n-1}$. Due to the uniqueness theorem for the solutions of complex ODEs [30], for any such $a_0,\dots,a_{n-1}$ and a_n with $P(a_0,\dots,a_n)=0$, there exists a unique solution $y=f(x)$ to the differential equation $P(y,y^{(1)},\dots,y^{(n)})=0$ satisfying the initial conditions $x=0$, $f(0)=a_0$, and $f^{(k)}(0)=a_k$ for $k=1,\dots,n$.

If there exists an irreducible polynomial $F \in \mathbb{C}[x,y]$ of degree d for which $F(x,f(x))$ is identically zero, then F is unique up to scaling. This means that every point in the projection of $\mathcal{Y}$ onto $\mathbb{C}^{n+1}$ has at most one preimage. Since the projection has dimension $\leq n$, this implies that the dimension of $\mathcal{Y}$ is also at most n, which contradicts the calculation that $\dim(\mathcal{Y})$ equals $\binom{d+2}{2} - 1 > n$. Therefore the projection of $\mathcal{Y}$ onto $\mathbb{C}^{n+1}$ must be Zariski-dense. □

Theorem 2.27. Let $\mathcal{I}$ be a G-classifying set of rational differential invariants for the action of a group G. Then for $d \in \mathbb{Z}_+$ with $\binom{d+2}{2} - 2 \geq \dim G$, a generic plane curve of degree d is non-exceptional with respect to $\mathcal{I}$.

Proof. For an irreducible curve X, the $\mathcal{I}$-regular points form a Zariski-open subset of X, as seen in Definition 2.24. Either this is all but finitely-many points of X, in which case X is non-exceptional, or empty, meaning that no points of X are $\mathcal{I}$-regular. In particular, if all intersection points of X with $V(x)$ are $\mathcal{I}$-regular, then X is non-exceptional.

Indeed, the condition that a point p is $\mathcal{I}$-regular on X is equivalent to the jet $j_X^{(r)}(p)$ belonging to a Zariski-open subset $\mathcal{U}$ of $J^r \cong \mathbb{C}^{r+2}$, where $r = \dim(G)$. Consider the quasi-projective variety $\mathcal{Y}$ defined in the proof of Lemma 2.26 with $n = r$. Its intersection with $\mathbb{P}(\mathbb{C}[x,y]_{\leq d}) \times \mathcal{U}$ is an open subset of $\mathcal{Y}$, which is nonempty by Lemma 2.26.

Furthermore, the projection of $\mathcal{Y}$ onto $\mathbb{P}(\mathbb{C}[x,y]_{\leq d})$ is dominant (i.e. the image in Zariski-dense). Specifically, consider the open dense set of irreducible polynomials $F \in \mathbb{C}[x,y]_{\leq d}$ for which $F(0,y)$ has a simple root $y = a_0$ at which $F_y(0,a_0)$ is nonzero. For any such F, $([F],a)$ belongs to $\mathcal{Y}$, where $j^{(r)}_{V(F)}(0,a_0) = (0,a)$. It follows that the projection of the set $\mathcal{Y} \cap (\mathbb{P}(\mathbb{C}[x,y]_{\leq d}) \times \mathcal{U})$ onto $\mathbb{P}(\mathbb{C}[x,y]_{\leq d})$ is also dominant. Therefore, for a generic plane curve of degree d, the points $X \cap V(x)$ are $\mathcal{I}$-regular in X, and thus X is non-exceptional. □

We will also make use of the G-invariance of the set of non-exceptional curves.

Lemma 2.28. If X is non-exceptional then so is $Y = \overline{g \cdot X}$ for all $g \in G$.

Proof. We check that if conditions (a) – (c) in Definition 2.24 are satisfied by all but finitely many points on X, then the same is true for Y.

(a) Assume that there are at most finitely many points $p \in X$, such that $j^r_X(p)$ is undefined (equivalently $F_y(p) = 0$, where F is a defining polynomial of X). This is, in fact, true for any irreducible curve of degree greater than 1. Since the action of G preserves these properties, there are at most finitely many points $p \in Y$, such that $j^r_Y(p)$ is undefined.

(b) Assume that there are at most finitely many points $p \in X$, such that $j^k_X(p) \notin W_1$ and $j^r_X(p) \notin W_2$. From the G-invariance of W_1 and W_2 and (7), combined with the fact that $Y \backslash (g \cdot X)$ is a finite set, it follows that there are at most finitely many points $p \in Y$ such that $j^k_Y(p) \notin W_1$ and $j^r_Y(p) \notin W_2$.

(c) We start by showing that if K is a differential invariant of order n, then the set of points $p^{(n)} \in J^n$ where $\frac{\partial K}{\partial y^{(n)}}(p^{(n)}) \neq 0$ is G-invariant. Since K is invariant, $K(p^{(n)}) = K(g \cdot p^{(n)})$, whenever both sides are defined, and the differentiation with respect $y^{(n)}$using the chain rule yields:

$$\begin{aligned}
&\frac{\partial K}{\partial y^{(n)}}\left(p^{(n)}\right) \\
&= \frac{\partial K}{\partial \overline{x}}\left(g \cdot p^{(n)}\right) \frac{\partial \overline{x}}{\partial y^{(n)}}\left(p^{(n)}\right) + \frac{\partial K}{\partial \overline{y}}\left(g \cdot p^{(n)}\right) \frac{\partial \overline{y}}{\partial y^{(n)}}\left(p^{(n)}\right) + \ldots + \frac{\partial K}{\partial \overline{y}^{(n)}}\left(g \cdot p^{(n)}\right) \frac{\partial \overline{y}^{(n)}}{\partial y^{(n)}}\left(p^{(n)}\right) \\
&= \frac{\partial K}{\partial \overline{y}^{(n)}}\left(g \cdot p^{(n)}\right) \frac{\partial \overline{y}^{(n)}}{\partial y^{(n)}}\left(p^{(n)}\right).
\end{aligned}$$

The last equality follows from the fact that the functions $\overline{x}, \overline{y}$, and $\overline{y}^{(i)}$, given in Definition 2.13, do not depend on $y^{(n)}$ for $i = 1, \ldots, n-1$. Thus if $\frac{\partial K}{\partial y^{(n)}}(p^{(n)}) \neq 0$, so does every point in the orbit of $p^{(n)}$.

Condition (c) states that, if K_1 is constant on X, then for all but finitely many $p \in X$, $\frac{\partial K_1}{\partial y^k}|_{j^k_X(p)} \neq 0$, otherwise for all but finitely many $p \in X$, $\frac{\partial K_2}{\partial y^r}|_{j^r_X(p)} \neq 0$, where $k = \mathrm{ord}(K_1)$ and $r = \mathrm{ord}(K_2)$. Due to (7), and G-invariance property showed above, the same is true for Y. □

2.5 Differential signatures of algebraic curves

In this section, we define the signature map and signature curve and show that signatures characterize the equivalence classes of generic algebraic curves. Throughout this section, we assume G is an algebraic group with $\dim(G) = r$ and that $\{K_1, K_2\}$ are a classifying set of differential invariants with $\mathrm{ord}(K_1) = k < r = \mathrm{ord}(K_2)$, as described above.

Definition 2.29. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let $X \subset \mathbb{C}^2$ be a non-exceptional curve. Then the rational map $\sigma_X : X \dashrightarrow \mathbb{C}^2$ with coordinates $(K_1|_X, K_2|_X)$ is called the *signature map*. The image of $\mathcal{S}_X = \sigma_X(X)$ is called the *signature* of X.

Note that since X is irreducible, the closure $\overline{\mathcal{S}_X}$ is also an irreducible variety of dimension 0 or 1. If $\dim(\overline{\mathcal{S}_X}) = 0$, then it is a single point and, therefore, σ_X is a constant map. If $\dim(\overline{\mathcal{S}_X}) = 1$, then it is an irreducible planar curve, which we call the *signature curve* of X. An irreducible polynomial vanishing on $\overline{\mathcal{S}_X}$ is called a *signature polynomial* and is denoted by S_X and it is unique up to scaling by a non-zero constant.

Proposition 2.30. Assume that $X, Y \subset \mathbb{C}^2$ are G-equivalent and non-exceptional with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$. Then $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$.

Proof. If X and Y are G-equivalent, then there exists $g \in G$ such that $Y = \overline{g \cdot X}$. Due to the fundamental property of prolongation (7), we have $j^r_Y(q) = g \cdot j^r_X(p)$, for any $p \in X$ where $q = g \cdot p$ is defined. Since K_1 and K_2 are invariant, we have

$$K_1(j^r_X(p)) = K_1(j^r_Y(q)) \text{ and } K_2(j^r_X(p)) = K_2(j^r_Y(q)).$$

This implies $\sigma_X(p) = \sigma_Y(q)$. Since $g \cdot p$ is defined for all but finitely many points in X and $g \cdot X$ is dense in Y, this implies that $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$. □

We will gradually work towards proving the converse of the above statement, and thus show that the signature polynomials characterize the equivalence classes of curves. We will also show the relationship between the cardinality of the preimage of a generic point under a signature map and the cardinality of the symmetry group. For both of these results we need several lemmas.

Lemma 2.31. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let $X, Z \subset \mathbb{C}^2$ be two non-exceptional curves, such that the restrictions of K_1 to both curves equal to the same constant function:

$$K_1|_X = K_1|_Z = c.$$

If there exists $p \in X \cap Z$ such that

1. $j^k_X(p) = j^k_Z(p)$, where $k = \mathrm{ord}(K_1)$,
2. p is not exceptional for X,

then $X = Z$.

Proof. Since p is non-singular for both X and Z, in some neighborhood of p, curves X and Z coincide with the graphs of analytic functions $y = f(x)$ and $y = g(x)$, respectively. Both $y = f(x)$ and $y = g(x)$ are solutions of the differential equation

$$K_1(x, y, y^{(1)}, \ldots, y^{(k)}) = c, \tag{9}$$

with the same initial condition described by the point $j^k_X(p) = j^k_Z(p)$. Since p is non-exceptional, $\frac{\partial K_1}{\partial y^k}|_{j^k_X(p)} \neq 0$, and so using the implicit function theorem, (9) can be rewritten as $y^{(k)} = H(x, y, y^{(1)}, \dots, y^{(k-1)})$ in a neighborhood of $j^k_X(p)$, where H is an analytic function of the jet coordinates. We can now invoke the uniqueness theorem for the solutions of complex ODEs [30] to conclude that $f(x) = g(x)$. Therefore X and Z coincide on a positive dimensional subset. Since they are irreducible $X = Z$. □

Lemma 2.32. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let $X, Z \subset \mathbb{C}^2$ be two non-exceptional curves with the same signature curves, $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$. If there exists $p \in X \cap Z$ such that

1. $j^r_X(p) = j^r_Z(p)$,
2. p is not exceptional for X
3. if $\dim \mathcal{S}_X > 0$ and $S_X(\kappa_1, \kappa_2)$ is a signature polynomial, then $\frac{\partial S}{\partial \kappa_2}|_{\sigma_X(p)} \neq 0$,

then $X = Z$.

Proof. If σ_X (and, therefore, σ_Z) is a constant map, then there exists $c \in \mathbb{C}$, such that $K_1|_X = c$ and $K_1|_Z = c$. Then we are in the situation of Lemma 2.31 and the conclusion follows. Otherwise, σ_X and, σ_Z define the same signature polynomial $S_X(\kappa_1, \kappa_2) = S_Z(\kappa_1, \kappa_2) := S(\kappa_1, \kappa_2)$. Since p is non-singular for both X and Z, in some neighborhood of p, curves X and Z coincide with the graphs of analytic functions $y = f(x)$ and $y = g(x)$, respectively. Both $y = f(x)$ and $y = g(x)$ are solutions of the differential equation

$$S\left(K_1(x, y, y^{(1)}, \dots, y^{(k)}), K_2(x, y, y^{(1)}, \dots, y^{(r)})\right) = 0 \tag{10}$$

with the same initial condition described by the point $j^r_X(p) = j^r_Z(p)$. By assumption, $\frac{\partial S}{\partial \kappa_2}|_{\sigma_X(p)}$ and $\frac{\partial K_2}{\partial y^{(r)}}|_{j^r_X(p)}$ are both nonzero. Then using the implicit function theorem, (10) can be rewritten as $y^{(r)} = H(x, y, y^{(1)}, \dots, y^{(r-1)})$ in a neighborhood of $j^r_X(p)$, where H is an analytic function of the jet coordinates. As in the previous lemma, we invoke the uniqueness theorem for the solutions of ODEs, to conclude $X = Z$. □

Lemma 2.33. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let X be a non-exceptional curve. Let $p, q \in X$ be two non-exceptional points, such that

1. $\sigma_X(p) = \sigma_X(q)$
2. if $\dim \mathcal{S}_X > 0$ and $S_X(\kappa_1, \kappa_2)$ is the signature polynomial, then $\frac{\partial S}{\partial \kappa_2}|_{\sigma_X(p)} \neq 0$.

Then there exists $g \in \mathrm{Sym}(X, G)$, such that $q = gp$.

Proof. Since, $\sigma_X(p) = \sigma_X(q)$ we have

$$K_1(j^r_X(p)) = K_1(j^r_X(q)) \text{ and } K_2(j^r_X(p)) = K_2(j^r_X(q)).$$

Since $\mathcal{I}$ is a separating set, and p and q are non-exceptional, there exists $g \in G$, such that $j^r_X(p) = g \cdot j^r_X(q)$. Consider a curve $Z = \overline{g \cdot X}$. By Lemma 2.28, Z is non-exceptional. Condition $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$ holds due to Proposition 2.30. Due to the fundamental property of prolongation (7) we have $j^r_Z(p) = g \cdot j^r_X(q)$. This implies $p = g \cdot q \in Z$ and $j^r_Z(p) = j^r_X(p)$. We verified that X and Z satisfy all conditions of Lemma 2.32. Then $X = Z = \overline{g \cdot X}$ and, therefore $g \in \mathrm{Sym}(X, G)$. □

Lemma 2.34. Suppose that X is a non-exceptional curve with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$. Then the following are equivalent:

(1) $K_1|_X$ is a constant function on X,

(2) $H = \mathrm{Sym}(X, G)$ is infinite,

(3) the signature $\mathcal{S}_X$ consists of a single point.

Proof. (1) $\Rightarrow$ (2) Assume $K_1|_X = c$ is a constant function on X. Fix a non-exceptional point p. We will show that any non-exceptional point on X belongs to the orbit Hp. Since non-exceptional points are dense in X, the conclusion would follow from Proposition 2.10.

Let q be a non-exceptional point on X. Then $K_1(j^k_X(p)) = K_1(j^k_X(q)) = c$ where k equals $\mathrm{ord}(K_1)$. Since K_1 is separating on J^k, there exists $g \in G$, such that $j^k_X(p) = g \cdot j^k_X(q)$. Consider a curve $Z = \overline{g \cdot X}$. By Lemma 2.28, Z is non-exceptional. Condition $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$ holds due to Proposition 2.30. Therefore $K_1|_Z$ is the same constant function as $K_1|_X$. Due to the fundamental property of prolongation (7) we have $j^r_Z(p) = g \cdot j^r_X(q)$. This implies $p = g \cdot q \in Z$ and $j^r_Z(p) = j^r_X(p)$. We verified that X and Z satisfy all conditions of Lemma 2.31. Then $X = Z = \overline{g \cdot X}$ and, therefore $g \in H$ and so $q \in Hp$.

(2) $\Rightarrow$ (3) Let p be a non-exceptional point. For any $q \in Hp$, there exists $g \in H$, such that $p = g \cdot q$ and $X = g \cdot X$. If q is non-exceptional, it follows from (7) that $j^k_X(p) = g \cdot j^k_X(q)$. Since K_1 is a differential invariant, $K_1|_X(g \cdot j^k_X(q)) = K_1|_X(j^k_X(q))$. Then

$$K_1|_X(j^k_X(p)) = K_1|_X(j^k_X(q)) \text{ for all non-exceptional } q \in H_p.$$

Since H is infinite, from Proposition 2.10, it follows the orbit Hp is dense in X. The set of non-exceptional points is also dense in X. Thus $K_1|_X$ is a constant rational function on a dense subset of X and, therefore, is constant on X.

(3) $\Rightarrow$ (1) Obvious from the definition of $\mathcal{S}_X$. □

We are now ready to prove the converse of the Proposition 2.30.

Proposition 2.35. If algebraic curves $X, Y \subset \mathbb{C}^2$ are non-exceptional with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$ under an action of G on $\mathbb{C}^2$ and their signature curves are equal, $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$, then X and Y are G-equivalent.

Proof. Then $\mathcal{S} := \overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$ is an irreducible curve, and let $S(\kappa_1, \kappa_2)$ be its defining polynomial. If $\frac{\partial S}{\partial \kappa_2}$ were identically zero, then $K_1|_X$ would be constant and Lemma 2.34 would imply that $\mathcal{S}$ is a single point. Therefore $\frac{\partial S}{\partial \kappa_2}|_s$ is nonzero for all but finitely many points $s \in \mathcal{S}$. Moreover, since X and Y are non-exceptional, for all but finitely many such points $s \in \mathcal{S}$, none of the points in the preimage $\sigma_X^{-1}(s)$ are exceptional in X and none of the points in the preimage $\sigma_Y^{-1}(s)$ are exceptional in Y. By Chevalley's Theorem (see e.g. [20, Thm. 3.16]), the images $\mathcal{S}_X$ and $\mathcal{S}_Y$ are constructible sets and thus all but at most finitely many points of their Zariski closure $\mathcal{S}$. We fix a point $s \in \mathcal{S}$ with these desired properties, a point $p \in \sigma_X^{-1}(s)$ and a point $q \in \sigma_Y^{-1}(s)$. Otherwise $\overline{\mathcal{S}_X}$ (and, therefore, $\overline{\mathcal{S}_Y}$) is a single point, and we let p and q be any non-exceptional points on X and Y, respectively.

In both cases, $\sigma_X(p) = \sigma_Y(q)$, meaning that

$$K_1(j^r_X(p)) = K_1(j^r_Y(q)) \quad \text{and} \quad K_2(j^r_X(p)) = K_2(j^r_Y(q)).$$

Since $\mathcal{I}$ is separating and p and q are non-exceptional, there exists a group element $g \in G$ for which $j^r_X(p)$ equals $g \cdot j^r_Y(q)$.

Consider a curve $Z = \overline{g \cdot Y}$. By Lemma 2.28, Z is non-exceptional. Condition $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$ holds due to Proposition 2.30. Due to the fundamental property of prolongation (7), we have $j^r_Z(p) = g \cdot j^r_X(q)$. Therefore, $p = g \cdot q \in Z$ and $j^r_Z(p) = j^r_X(p)$. We verified that X and Z satisfy all conditions of Lemma 2.32. Then $X = Z = \overline{g \cdot Y}$. □

Combining Lemma 2.34 with Propositions 2.30 and 2.35 we get the following corollary.

Corollary 2.36. If X and Y have a finite symmetry group, then X and Y are G-equivalent if and only if their signature polynomials S_X, S_Y are equal up to a non-zero constant factor.

We are finally ready to state the first main result of the paper about the existence of a pair of classifying invariants characterizing the equivalence classes of generic irreducible algebraic curves:

Theorem 2.37. Let an r-dimensional group $G \subset \mathcal{PGL}(3)$ act on $\mathbb{C}^2$. Then there exists a pair of differential invariants $\mathcal{I} = \{K_1, K_2\}$ of differential order at most r, such that for all integers d, where $\binom{d+2}{2} - 2 \geq r$, there exists a Zariski open subset $\mathcal{P}_d \subset \mathbb{C}[x,y]_{\leq d}$ such that any curves X, Y whose defining polynomials lie in $\mathcal{P}_d$ satisfy:

$$X \underset{G}{\cong} Y \quad \Longleftrightarrow \quad \overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}, \tag{11}$$

where $\mathcal{S}_X$ and $\mathcal{S}_Y$ are signatures of X and Y based on invariants $\mathcal{I}$, as given by Definition 2.29.

Proof. From Theorem 2.20 we know that there exists a classifying set $\mathcal{I}$ of rational differential invariants of order at most r. By Propositions 2.30 and 2.35, the statement (11) is valid for all $\mathcal{I}$-non-exceptional curves. By Theorem 2.27, for any d, such that $\binom{d+2}{2} - 2 \geq r$, there exists a Zariski open subset $\mathcal{P}_d \subset \mathbb{C}[x,y]_{\leq d}$, such that all curves whose defining polynomials lie in $\mathcal{P}_d$ are non-exceptional. □

The next theorem establishes an important relationship between the size of the symmetry group of an algebraic curve and some properties of its signature map. This result plays a crucial role in our degree formula derived in the next sections.

Theorem 2.38. Suppose that X is a non-exceptional curve with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$ for action G. Then $|\operatorname{Sym}(X, G)| = n$ if and only if the map σ_X is generically $n : 1$.

Proof. ($\Rightarrow$) We need to show that there exists a dense subset $\mathcal{S}_0 \subset \overline{\mathcal{S}_X}$, such that $|\sigma_X^{-1}(s)| = n$ for all $s \in \mathcal{S}_0$. Denote $H := \operatorname{Sym}(X, G)$. Since H is finite, from Lemma 2.34, it follows that $\overline{\mathcal{S}_X}$ is an irreducible curve and its defining polynomial $S(\kappa_1, \kappa_2)$ depends non-trivially on κ_2. Therefore the set $\mathcal{S}_1 = \left\{ s \in \mathcal{S}_X \;\middle|\; \left.\frac{\partial S}{\partial \kappa_2}\right|_s \neq 0 \right\}$ is dense in $\overline{\mathcal{S}_X}$. Due to Proposition 2.11 for all but maybe finitely many points $p \in X$, the orbit Hp consists of exactly n distinct points. Moreover, since X has only finitely many exceptional points, the set of points

$$X_0 = \{p \in X \,|\, Hp \text{ consists of exactly } n \text{ non-exceptional points}\}$$

is dense in X. Then its image $\mathcal{S}_2 = \sigma_X(X_0)$ is dense in $\overline{\mathcal{S}_X}$. It follows that the intersection $\mathcal{S}_0 := \mathcal{S}_1 \cap \mathcal{S}_2$ is dense in $\overline{\mathcal{S}_X}$. For any $s \in \mathcal{S}_0$, let $p \in \sigma_X^{-1}(s)$. By Lemma 2.33, $\sigma_X^{-1}(s) = Hp$ and so $|\sigma_X^{-1}(s)| = n$.

($\Leftarrow$) Suppose that the map σ_X is generically $n : 1$. Then, by Lemma 2.34, $\operatorname{Sym}(X, G)$ is finite. By the forward implication, $n = \operatorname{Sym}(X, G)$. □

Example 2.39. Consider the special Euclidean group $\mathcal{SE}(2)$ of complex translations and rotations of $\mathbb{C}^2$. The action of $\mathcal{SE}(2)$ is given by $g \cdot (x, y) = (\overline{x}, \overline{y}) = (cx + sy + a, -sx + cy + b)$, where $c^2 + s^2 = 1$ and $c, s, a, b \in \mathbb{C}$ (see Definition 4.3). From this, using the recursive formula in Definition 2.13, one can compute the prolonged action of $\mathcal{SE}(2)$ on J^2. For instance, $\overline{y}^{(1)}$ is given by

$$\overline{y}^{(1)} = \frac{\frac{d}{dx}(-sx + cy + b)}{\frac{d}{dx}(cx + sy + a)} = \frac{-s + cy^{(1)}}{c + sy^{(1)}}$$

and the full prolonged action on J^2 is

$$g \cdot \left(x, y, y^{(1)}, y^{(2)}\right) = \left(cx + sy + a, -sx + cy + b, \frac{-s + cy^{(1)}}{c + sy^{(1)}}, \frac{y^{(2)}}{(sy^{(1)} + c)^3}\right).$$

The set $\mathcal{I}^{\mathcal{SE}} = \{K_1, K_2\}$, where $K_1 = \kappa^2$, the square of Euclidean curvature, and $K_2 = \kappa_s$ its derivative with respect to Euclidean arc-length, explicitly given in (20) is classifying. Indeed, one can check directly that $\mathcal{I}^{\mathcal{SE}}$ separates orbits on the $\mathcal{SE}$-invariant open subset

$$W_3 = \left\{ \left(x, y, y^{(1)}, y^{(2)}, y^{(3)}\right) \mid \left(y^{(1)}\right)^2 + 1 \neq 0 \right\}$$

and K_1 separates orbits on an open set $W_2 = \pi(W_3) \subset J^2$ under the standard projection $\pi\colon J^3 \to J^2$. Thus the conditions of Definition (2.19) are satisfied. According to Theorem 2.20 we conclude that

$$\mathbb{C}(J^3)^{\mathcal{SE}(2)} = \mathbb{C}(K_1, K_2) \quad \text{and} \quad \mathbb{C}(J^2)^{\mathcal{SE}(2)} = \mathbb{C}(K_1).$$

By Theorem 2.27, a generic curve of degree ≥ 2 is non-exceptional with respect to $\mathcal{I}^{\mathcal{SE}}$. In fact, a careful consideration of the conditions in Definition 2.24 shows that there are *no* irreducible curves of degree greater than one that are $\mathcal{I}^{\mathcal{SE}}$-exceptional.

We will now compute the signature polynomial for the ellipse X defined by the zero set of

$$F(x, y) = x^2 + y^2 + xy - 1.$$

The signature map $\sigma_X = (K_1|_X, K_2|_X) : X \to \mathbb{C}^2$ is explicitly defined by

$$K_1|_X(x, y) = 36\frac{(x^2 + xy + y^2)^2}{(5x^2 + 8xy + 5y^2)^3} \quad \text{and} \quad K_2|_X(x, y) = 54\frac{(y^4 - x^4 + xy^3 - x^3y)}{(5x^2 + 8xy + 5y^2)^3}.$$

Under the $\mathcal{SE}(2)$-action the ellipse has a symmetry group of cardinality two generated by the 180°-degree rotation. We observe that in agreement with Theorem 2.38, σ_X is generically a $2\colon 1$ map on X. One can use a Gröbner basis elimination algorithm to compute a signature polynomial of X, that is an irreducible polynomial vanishing on the image of the rational map σ_X:

$$S_X(\kappa_1, \kappa_2) = 2916\kappa_1^6 + 972\kappa_1^4\kappa_2^2 + 108\kappa_1^2\kappa_2^4 + 4\kappa_2^6 - 13608\kappa_1^5 + 1944\kappa_1^3\kappa_2^2 + 2187\kappa_1^4.$$

Any curve $\mathcal{SE}(2)$-equivalent to X will have the same signature polynomial. For most degree three algebraic curves, it takes much longer to compute their signature polynomials under $\mathcal{SE}(2)$ actions, and for higher degree curves it is rarely possible in practice. For this reason, it is of interest to determine properties, such as the degree, of signature polynomials for curves without their explicit computation.

3 The degree of the signature of algebraic curves

This section is devoted to the degree formula for the signature polynomial. In Section 3.1 we give the necessary algebraic geometry background. In Section 3.2 we give a formula for the degree of the signature polynomial for a non-exceptional curve with finite symmetry group. (Theorem 3.8) and some easily computable bounds for this degree (Corollary 3.9).

3.1 Multiplicity, plane curves, and rational maps

Here we review and establish some fundamental properties of plane curves, their intersections, and their images under rational maps. See, for example, [14] or [45] for more background.

Definition 3.1. Given a point $p \in \mathbb{C}^2$, the *local ring* of $\mathbb{C}^2$ at p, denoted $\mathcal{O}_p$, is the ring of rational functions in $\mathbb{C}(x, y)$ that are defined at p. A polynomial ideal $I \subset \mathbb{C}[x, y]$ defines an ideal $I \cdot \mathcal{O}_p$ of the local ring, and the *multiplicity of I at p* is defined to be the dimension (as a $\mathbb{C}$-vector space) of the quotient:

$$m_p(I) \quad = \quad \dim_{\mathbb{C}} (\mathcal{O}_p / I \cdot \mathcal{O}_p)$$

In particular, $m_p(I)$ is positive if and only if p belongs to the variety $V(I)$. For a homogeneous ideal $J \subset \mathbb{C}[x_0, x_1, x_2]$ and a point $\mathbf{p} = [p_0 : p_1 : p_2] \in \mathbb{CP}^2$ with $p_i \neq 0$ for some $i = 0, 1, 2$, we define the multiplicity of J at $\mathbf{p}$, denoted $m_{\mathbf{p}}(J)$, to be $m_p(I)$, where $p \in \mathbb{C}^2$ and I are obtained from $\mathbf{p}$ and J by restricting p_i and x_i to equal 1, respectively. On can check that this definition is independent of the choice of non-zero coordinate p_i.

In an important special case when the ideal I is generated by two polynomials, $I = \langle F, G\rangle$, we call $m_p(I) = m_p(F, G)$ the *intersection multiplicity* of F, G at p. In this case, $m_p(F, G) = 1$ if and only if $p \in V(F, G)$ and $\nabla_p F$ and $\nabla_p G$ are linearly independent.

An equivalent definition of multiplicity uses power series. After a change of coordinates, we can take $p = (0, 0)$. Then $m_p(I)$ equals the dimension as a $\mathbb{C}$-vector space of the quotient of the power series ring $\mathbb{C}[[x, y]]$ by the image of I in this ring:

$$m_p(I) \quad = \quad \dim_{\mathbb{C}} \ (\mathbb{C}[[x, y]]/I \cdot \mathbb{C}[[x, y]]) \, .$$

To precisely compute intersection multiplicities at a non-singular point p, one can parametrize a neighborhood of p in $V(F)$ using *Laurent series*, $\mathbb{C}((t))$. The ring of Laurent series consists of formal sums $\sum_{j=k}^{\infty} a_j t^j$ for some integer $k \in \mathbb{Z}$. The series we consider will converge for $t \in \mathbb{C}^*$ of sufficiently small modulus. We define the *valuation*, denoted $\mathrm{val}(\mathbf{a})$, of a Laurent series $\mathbf{a} = \sum_{j=k}^{\infty} a_j t^j$ to be the smallest power of t with nonzero coefficient. Since p is non-singular, $\frac{\partial F}{\partial x}(p) \neq 0$ or $\frac{\partial F}{\partial y}(p) \neq 0$. Assume $\frac{\partial F}{\partial y}(p) \neq 0$, then in a neighborhood of p, $V(F)$ can be parametrized by $\alpha(t) = (p_1 + t, a(t))$, otherwise it can be parametrized by $\alpha(t) = (a(t), p_2 + t)$, where in both cases $a(t)$ is some Maclaurin series. Then according to [13, §8.4]:

$$m_p(F, G) = \mathrm{val}(G(\alpha)). \tag{12}$$

We now establish some basic facts and notation about rational maps on $\mathbb{CP}^2$. A vector $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$, whose entries $\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2 \in \mathbb{C}[x_0, x_1, x_2]$ are homogeneous polynomials of the same degree d, defines a rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ (denoted by the same symbol). For any non-zero homogeneous polynomial $h \in \mathbb{C}[x_0, x_1, x_2]$, a polynomial vector $h\boldsymbol{\phi} = [h\boldsymbol{\phi}_0, h\boldsymbol{\phi}_1, h\boldsymbol{\phi}_2]$ defines an equivalent rational map, i.e. the values of the maps ϕ and $h\phi$ are equal, whenever both are defined. In what follows we *do not* assume that $\gcd(\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2) = 1$ and the following definition clearly depends on the choice of a polynomial vector.

Definition 3.2. A vector $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$ whose entries $\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2 \in \mathbb{C}[x_0, x_1, x_2]$ are homogeneous polynomials of the same degree d, is called a *homogeneous vector of degree* d and the notation $\deg(\boldsymbol{\phi}) = d$ is used. The *base locus* of $\boldsymbol{\phi}$ is the set of points at which all its components are zero

$$Bl(\boldsymbol{\phi}) = V(\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2).$$

We say that $\boldsymbol{\phi}$ is *defined on an algebraic curve* X if X is not contained in $Bl(\boldsymbol{\phi})$. We say that $\boldsymbol{\phi}$ is *non-constant on an algebraic curve* X, if the corresponding rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ is non-constant when restricted to X.

Proposition 3.3. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ be irreducible and homogeneous, and let $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$ be a homogeneous vector that is both defined and non-constant on $V(\mathbf{F})$. For $\mathbf{a} = [a_0, a_1, a_2] \in \mathbb{CP}^2$, consider an equivalence class (up to scaling by a constant) of a linear form $\mathbf{L_a} = a_0 y_0 + a_1 y_1 + a_2 y_2 \in \mathbb{C}[y_0, y_1, y_2]$ and its pullback $\boldsymbol{\phi}^* \mathbf{L_a} = a_0 \boldsymbol{\phi}_0 + a_1 \boldsymbol{\phi}_1 + a_2 \boldsymbol{\phi}_2 \in \mathbb{C}[x_0, x_1, x_2]$. Then for all $\mathbf{a} \in \mathbb{CP}^2$:

(a) $V(\boldsymbol{\phi}^* \mathbf{L_a}) = \boldsymbol{\phi}^{-1}(V(\mathbf{L_a})) \cup Bl(\boldsymbol{\phi})$.

In addition, if $\mathbf{a} \in \mathbb{CP}^2$ is generic:

(b) $\mathbf{F}$ and $\boldsymbol{\phi}^* \mathbf{L_a}$ have no common factors,

(c) if $\mathbf{p} \in V(\mathbf{F}) \cap V(\boldsymbol{\phi}^* \mathbf{L_a})$ with $\mathbf{p} \notin Bl(\boldsymbol{\phi})$, then $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^* \mathbf{L_a}) = 1$.

Proof. (a) If $\mathbf{p} \notin Bl(\boldsymbol{\phi})$, then $\boldsymbol{\phi}$ is defined at $\mathbf{p}$. Then $\boldsymbol{\phi}(\mathbf{p})$ belongs to $V(\mathbf{L_a})$ if and only if $\mathbf{p}$ belongs to $V(\boldsymbol{\phi}^* \mathbf{L_a})$. If $\mathbf{p}$ belongs to $Bl(\boldsymbol{\phi})$, then it clearly also belongs to $V(\boldsymbol{\phi}^* \mathbf{L_a})$.

(b) Since $\mathbf{F}$ is irreducible, $\boldsymbol{\phi}^* \mathbf{L_a}$ and $\mathbf{F}$ have a common factor if and only if $\mathbf{F}$ divides $\boldsymbol{\phi}^* \mathbf{L_a}$, if and only if $\boldsymbol{\phi}^* \mathbf{L_a}$ is identically zero on $V(\mathbf{F})$. Consider a map $\Psi \colon \mathbb{CP}^2 \times V(\mathbf{F}) \to \mathbb{C}$, defined by $\Psi(\mathbf{a}, \mathbf{p}) = a_0 \boldsymbol{\phi}_0(\mathbf{p}) + a_1 \boldsymbol{\phi}_1(\mathbf{p}) + a_2 \boldsymbol{\phi}_2(\mathbf{p})$. Since $\boldsymbol{\phi}$ is defined on $V(\mathbf{F})$, there exists $\hat{\mathbf{a}} \in \mathbb{CP}^2$ such that $\hat{a}_0 \boldsymbol{\phi}_0 + \hat{a}_1 \boldsymbol{\phi}_1 + \hat{a}_2 \boldsymbol{\phi}_2$ is not identically zero on $V(\mathbf{F})$ (otherwise with an appropriate choice of $\mathbf{a}$'s we can show that $\phi_j \equiv 0$ on $V(\mathbf{F})$ for $j = 0, 1, 2$). Then $\Psi(\hat{\mathbf{a}}, \hat{\mathbf{p}}) \neq 0$ for some

$\hat{\mathbf{p}} \in V(\mathbf{F})$. By continuity, $\Psi(\mathbf{a}, \mathbf{p}) \neq 0$ in some open neighborhood of $(\hat{\mathbf{a}}, \hat{\mathbf{p}})$ in $\Psi \colon \mathbb{CP}^2$. Thus $\boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}$ is non-zero l on $V(\mathbf{F})$ for all $\mathbf{a}$ in some open subset of $\mathbb{CP}^2$.

(c) It is sufficient to show that $\nabla \mathbf{F}|_\mathbf{p}$ and $\nabla_x \boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}|_{(\mathbf{p},\mathbf{a})}$ are linearly dependent, for a generic $\mathbf{a} \in \mathbb{C}^3$ and $\mathbf{p} \in V(\mathbf{F})$ such that $\mathbf{p} \notin Bl(\boldsymbol{\phi})$, where, for a moment, we consider $V(\mathbf{F})$, $Bl(\boldsymbol{\phi})$ to be varieties in $\mathbb{C}^3$. Consider

$$\mathcal{Y} \;=\; \left\{ (\mathbf{p}, \mathbf{a}) \in \mathbb{C}^6 \,|\, \mathbf{p} \in V(\mathbf{F}, \boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}), \quad \mathbf{p} \notin Bl(\boldsymbol{\phi}) \cup V(\mathbf{F})_{sing} \right\}$$

where $V(\mathbf{F})_{sing}$ denotes the variety $V(\frac{\partial \mathbf{F}}{\partial x_0}, \frac{\partial \mathbf{F}}{\partial x_1}, \frac{\partial \mathbf{F}}{\partial x_2})$. Let $\pi : \mathcal{Y} \to \mathbb{C}^3$ denote the regular map defined by projection $\pi(\mathbf{p}, \mathbf{a}) = \mathbf{a}$. Note that restricting to $\mathbf{p} \notin Bl(\boldsymbol{\phi}) \cup V(\mathbf{F})_{sing}$ makes $\mathcal{Y}$ nonsingular.

Bertini's generic smoothness theorem [45, Ch. 2, Sec. 6, Thm 2.27][9] then guarantees the existences of a nonempty Zariski-open set $U \subset \mathbb{C}^3$ so that for all $\mathbf{a} \in U$ and all preimages $(\mathbf{p}, \mathbf{a}) \in \pi^{-1}(\mathbf{a})$, the induced map on tangent spaces $d_{(\mathbf{p},\mathbf{a})}\pi : T_{\mathcal{Y},(\mathbf{p},\mathbf{a})} \to T_{\mathbb{C}^3,\mathbf{a}}$ is surjective.

For $(\mathbf{p}, \mathbf{a}) \in \mathcal{Y}$,

$$T_{\mathcal{Y},(\mathbf{p},\mathbf{a})} = \ker \begin{bmatrix} \nabla \mathbf{F}|_\mathbf{p} & 0 & 0 & 0 \\ \nabla_x \boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}|_{(\mathbf{p},\mathbf{a})} & \phi_0(\mathbf{p}) & \phi_1(\mathbf{p}) & \phi_2(\mathbf{p}) \end{bmatrix}.$$

The map $d_{(\mathbf{p},\mathbf{a})}$ maps $(u_0, u_1, u_2, w_0, w_1, w_2)^T \in T_{\mathcal{Y},(\mathbf{p},\mathbf{a})}$ to $(w_0, w_1, w_2)^T \in T_{\mathbb{C}^3,\mathbf{a}} = \mathbb{C}^3$. If $\nabla \mathbf{F}|_\mathbf{p}$ and $\nabla_x \boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}|_{(\mathbf{p},\mathbf{a})}$ are linearly dependent as vectors in $\mathbb{C}^3$, then $(u_0, u_1, u_2, w_0, w_1, w_2)^T$ belongs to $T_{\mathcal{Y},(\mathbf{p},\mathbf{a})}$ if and only if $(u_0, u_1, u_3)^T \in \ker \nabla \mathbf{F}|_\mathbf{p}$ and $a_0 w_0 + a_1 w_1 + a_2 w_2 = 0$. The latter gives a non-trivial linear condition on the vectors in the image of $d_{(\mathbf{p},\mathbf{a})}\pi$ and, therefore, if $\nabla \mathbf{F}|_\mathbf{p}$ and $\nabla_x \boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}|_{(\mathbf{p},\mathbf{a})}$ are linearly dependent, $d_{(\mathbf{p},\mathbf{a})}\pi$ is not surjective.

Combining the results of the previous two paragraphs, we conclude that for $\mathbf{a} \in U$ and $\mathbf{p} \in V(\mathbf{F}) \cap V(\boldsymbol{\phi}^* \mathbf{L}_\mathbf{a})$, such that $\mathbf{p} \notin Bl(\boldsymbol{\phi}) \cup V(\mathbf{F})_{sing}$, $\nabla \mathbf{F}|_\mathbf{p}$ and $\nabla_x \boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}|_{(\mathbf{p},\mathbf{a})}$ are linearly independent. Observing that for a generic $\mathbf{a}$, $V(\boldsymbol{\phi}^* \mathbf{L}_\mathbf{a}) \cap V(\mathbf{F})_{sing} = \emptyset$, we finish the proof. □

Lemma 3.4. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ be homogeneous and irreducible, and let $\boldsymbol{\phi}$ be a homogeneous vector. For $\mathbf{p} \in V(\mathbf{F}) \cap Bl(\boldsymbol{\phi})$, the minimum of $m_\mathbf{p}(\mathbf{F}, a_0\boldsymbol{\phi}_0 + a_1\boldsymbol{\phi}_1 + a_2\boldsymbol{\phi}_2)$ over all $\mathbf{a} \in \mathbb{CP}^2$ is achieved generically.

Proof. If $\mathbf{p}$ is a non-singular point of $V(\mathbf{F})$, then for any $j \in \mathbb{Z}_{\geq 0}$ the collection of $\mathbf{G}$ for which $m_\mathbf{p}(\mathbf{F}, \mathbf{G}) \geq j$ is linear subspace of $\mathbb{C}[x_0, x_1, x_2]_D$, where $D = \deg(\mathbf{G})$ (This claim easily follows from (12). See also [14, Prob. 3.20]). It follows that $m_\mathbf{p}(\mathbf{F}, a_0\boldsymbol{\phi}_0 + a_1\boldsymbol{\phi}_1 + a_2\boldsymbol{\phi}_2) \geq j$ is a linear condition on $\mathbf{a} \in \mathbb{CP}^2$.

Now suppose $\mathbf{p}$ is a singular point of $\mathbf{X} = V(\mathbf{F})$ and consider a non-singular model $\mathbf{Y}$ of this curve with birational morphism $f : \mathbf{Y} \to \mathbf{X}$ (see [14, Ch. 7]). This induces an embedding of the fields of rational functions $f^* \colon \mathbb{C}(\mathbf{X}) \hookrightarrow \mathbb{C}(\mathbf{Y})$. Choose some linear form $\ell \in \mathbb{C}[x_0, x_1, x_2]_1$ with $\ell(\mathbf{p}) \neq 0$. Let $\mathbf{G}' = \mathbf{G}/\ell^{\deg(\mathbf{G})}$ in $\mathbb{C}(\mathbf{X})$. Using [14, Ch. 7, Prop. 2]:

$$m_\mathbf{p}(\mathbf{F}, \mathbf{G}) = \sum_{\mathbf{q} \in f^{-1}(\mathbf{p})} m_\mathbf{q}(\mathbf{Y}, \mathbf{G}'),$$

where $m_\mathbf{q}(\mathbf{Y}, \mathbf{G}')$ is the order of vanishing of $\mathbf{G}'$ at the smooth point $\mathbf{q} \in \mathbf{Y}$.

This reduces to the non-singular case. □

The minimum multiplicity in Lemma 3.4 will reappear frequently and we denote it by

$$\text{mult}_\mathbf{p}(\mathbf{F}, \boldsymbol{\phi}) \;=\; \min_{\mathbf{a} \in \mathbb{CP}^2} m_\mathbf{p}(\mathbf{F}, a_0\boldsymbol{\phi}_0 + a_1\boldsymbol{\phi}_1 + a_2\boldsymbol{\phi}_2). \tag{13}$$

The following bounds can be useful for computing this multiplicity:

[9] Bertini's generic smoothness theorem is an algebraic analogue of Sard's theorem in differential geometry.

Proposition 3.5. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ be an irreducible homogeneous polynomial and $\boldsymbol{\phi}$ be a homogeneous vector defined on $V(\mathbf{F})$. For $\mathbf{p} \in Bl(\boldsymbol{\phi})$ and for any $\mathbf{a} = [a_0 : a_1 : a_2] \in \mathbb{CP}^2$,

$$m_{\mathbf{p}}(\langle \mathbf{F}, \boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2 \rangle) \;\leq\; \text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}) \;\leq\; m_{\mathbf{p}}(\mathbf{F}, a_0\boldsymbol{\phi}_0 + a_1\boldsymbol{\phi}_1 + a_2\boldsymbol{\phi}_2),$$

where the right inequality is tight for generic $\mathbf{a} \in \mathbb{CP}^2$.

Proof. For the first inequality, note that for any $\mathbf{a} \in \mathbb{CP}^2$, $\boldsymbol{\phi}^*\mathbf{L_a} = a_0\boldsymbol{\phi}_0 + a_1\boldsymbol{\phi}_1 + a_2\boldsymbol{\phi}_2$ belongs to the ideal $\langle \boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2 \rangle$. It follows immediately from Definition 3.1 that for any pair of nested homogeneous ideals $I \subset J \subset \mathbb{C}[x_0, x_1, x_2]$ and any point $\mathbf{p} \in \mathbb{CP}^2$, we have that $m_{\mathbf{p}}(I) \geq m_{\mathbf{p}}(J)$. Therefore, for every point $\mathbf{p} \in \mathbb{CP}^2$, $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L}) \geq m_{\mathbf{p}}(\langle \mathbf{F}, \boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2 \rangle)$. The inequality then follows from a generic choice of $\mathbf{a} \in \mathbb{CP}^2$ and equation (14).

The second inequality follows directly from the definition of $\text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi})$, and tightness follows from Lemma 3.4. □

Theorem 3.6. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ be irreducible and homogeneous and $\boldsymbol{\phi}$ be a homogeneous vector, such that the rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ is defined and generically $n : 1$ on $V(\mathbf{F})$. Let $\mathbf{P} \in \mathbb{C}[y_0, y_1, y_2]$ denote the minimal polynomial vanishing on the image $\boldsymbol{\phi}(V(\mathbf{F}))$. Then

$$n \cdot \deg(\mathbf{P}) \;=\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\phi}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\phi})} \text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}) \tag{14}$$

Proof. For a linear form $\mathbf{L_a} = a_0y_0 + a_1y_1 + a_2y_2 \in \mathbb{C}[y_0, y_1, y_2]$, by Bezout's Theorem ([14, §5.3]) and Proposition 3.3(a) give that

$$\deg(\mathbf{F}) \cdot \deg(\boldsymbol{\phi}^*\mathbf{L_a}) = \sum_{\mathbf{p}} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L_a}) = \sum_{\mathbf{p} \in \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L_a}) + \sum_{\mathbf{p} \in Bl(\boldsymbol{\phi})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L_a}).$$

By Lemma 3.4, $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L_a}) = \text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi})$ for a generic $\mathbf{a} \in \mathbb{CP}^2$ and every $\mathbf{p}$. Also, for a generic $\mathbf{a}$, $\boldsymbol{\phi}^*\mathbf{L_a}$ is nonzero and its degree equals $\deg(\boldsymbol{\phi})$. By Proposition 3.3(c), for each point $\mathbf{p} \in V(\mathbf{F}) \cap \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))$, the intersection multiplicity $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L_a})$ equals one. Since $\boldsymbol{\phi}$ is generically $n : 1$, there are at most finitely many points $\mathbf{p} \in V(\mathbf{F})$ for which $|\boldsymbol{\phi}^{-1}(\boldsymbol{\phi}(\mathbf{p})) \cap V(\mathbf{F})| \neq n$, implying that for a generic $\mathbf{a}$, the line $V(\mathbf{L_a})$ does not contain the image $\boldsymbol{\phi}(\mathbf{p})$ of any of these points. Therefore, for every point $\mathbf{p} \in \boldsymbol{\phi}^{-1}(\mathbf{L_a}) \cap V(\mathbf{F})$, there are exactly n points of $V(\mathbf{F})$ in the set $\boldsymbol{\phi}^{-1}(\boldsymbol{\phi}(\mathbf{p}))$. Putting this all together gives that

$$\sum_{\mathbf{p} \in \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L_a}) \;=\; |V(\mathbf{F}) \cap \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))| \;=\; n \cdot |\boldsymbol{\phi}(V(\mathbf{F})) \cap V(\mathbf{L_a})|.$$

By Chevalley's Theorem (see e.g. [20, Thm. 3.16]), the image $\boldsymbol{\phi}(V(\mathbf{F}))$ is all but finitely many points of its Zariski closure $V(\mathbf{P})$. For a generic $\mathbf{a}$, every point in $V(\mathbf{L_a}) \cap V(\mathbf{P})$ belongs to $V(\mathbf{L_a}) \cap \boldsymbol{\phi}(V(\mathbf{F}))$ and that the number of these points equals to $\deg(\mathbf{P})$. This proves equality in (14). □

3.2 The degree of the signature polynomial

Definition 3.7. Let $X \subset \mathbb{C}^2$ be an algebraic plane curve and let $\psi : X \dashrightarrow \mathbb{C}^2$ be a rational map. We say that a rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ is a *projective extension* of ψ if

$$\psi(p) \;=\; \left(\frac{\boldsymbol{\phi}_1(1, p)}{\boldsymbol{\phi}_0(1, p)}, \frac{\boldsymbol{\phi}_2(1, p)}{\boldsymbol{\phi}_0(1, p)} \right)$$

for a Zariski-dense set of points $p \in X$ at which ψ is defined and $\boldsymbol{\phi}_0(1, p) \neq 0$.

Recall from Section 2.5, that a classifying set of rational differential invariants of the action of a group G on $\mathbb{C}^2$ define a *signature map* σ_X on a non-exceptional, irreducible curve $X \subset \mathbb{C}^2$. As in Definition 2.29, we fix a classifying set of rational differential invariants $\mathcal{I}$ with respect to the action G and suppose that the signature map $\sigma_X : X \dashrightarrow \mathbb{C}^2$ is non-constant on X. We will consider a projective extension $\boldsymbol{\sigma} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$. Note that while we will drop X from the notation, the map $\boldsymbol{\sigma}$ still heavily depends on the original curve X.

Theorem 3.8. Let $X \subset \mathbb{C}^2$ be a non-exceptional algebraic curve defined by an irreducible polynomial F, and let $n = |\operatorname{Sym}(X, G)|$. Then for any homogeneous vector $\boldsymbol{\sigma}$, defining a projective extension $\boldsymbol{\sigma} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ of the signature map σ_X, the degree of the signature polynomial S_X satisfies

$$n \cdot \deg(S_X) \quad = \quad \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}). \tag{15}$$

Here $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ denotes the homogenization of F.

Proof. From Theorem 2.38 we know that $\sigma_X : X \dashrightarrow \mathbb{C}^2$ is generically $n : 1$ map. Then $\boldsymbol{\sigma}$ is defined and generically $n : 1$ on $V(\mathbf{F})$, which is the Zariski-closure of X in $\mathbb{CP}^2$. Since F, and thus $\mathbf{F}$, are irreducible, the minimal polynomial $\mathbf{P}$ vanishing on the image $\boldsymbol{\sigma}(V(\mathbf{F}))$ is also irreducible. Its dehomogenezation is exactly the signature polynomial S_X. The result then follows from Theorem 3.6. □

At first glance the last term in the degree formula (15) appears to be difficult to obtain as we recall from (13), $\operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi})$ is defined as the minimal multiplicity over $\mathbf{a} \in \mathbb{CP}^2$. The following corollary shows that a generic choice of $\mathbf{a} \in \mathbb{CP}^2$ gives the desired minimal multiplicity, and thus the degree of the signature can be computed by randomized algorithms. It also establishes the degree bounds, that can also help in determining the degree of a signature curve.

Corollary 3.9. Under the hypotheses of Theorem 3.8, for any $\mathbf{a} \in \mathbb{CP}^2$, we have

$$n \cdot \deg(S_X) \;\geq\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, a_0\boldsymbol{\sigma}_0 + a_1\boldsymbol{\sigma}_1 + a_2\boldsymbol{\sigma}_2), \tag{16}$$

with equality holding for a generic $\mathbf{a}$. In addition:

$$n \cdot \deg(S_X) \;\leq\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2), \tag{17}$$

Proof. This is a direct corollary of Proposition 3.5 and Theorem 3.8. □

In the following example we show how one can use the bounds in Corollary 3.9 to predict the degree of the signature polynomial and what problems can arise.

Example 3.10. We will illustrate Theorem 3.8 and Corollary 3.9 by studying the signature of the curve X defined by the zero set of the irreducible cubic

$$F(x, y) = x^2y + y^2 + y + \frac{64}{121}$$

for the action of the affine group $\mathcal{A}(2)$ consisting of linear transformations and translations on $\mathbb{C}^2$. We will use classifying invariants (21) introduced in Section 4.1 below. If we restrict these invariants to X and cancel common factors, then we can construct a projective extension $\boldsymbol{\sigma}$ of σ_X where $\deg(\boldsymbol{\sigma}) = 26$.

In Figure 1 in red, on the left, the real affine points of X are shown, while on the right, the real affine points of its signature curve $\overline{\mathcal{S}_X}$. In blue, on the right, is the line $V(\mathbf{L_a})$ defined by $\mathbf{a} = [5 : 1 : 1]$ and on the left its pullback $V(\boldsymbol{\sigma}^*\mathbf{L_a})$. Under the action of the affine group of transformations on the plane, X has a symmetry group of size two. Then by Theorem 2.38, the map $\boldsymbol{\sigma}$ is generically $2\colon 1$ on X.

A direct computation of the rightmost terms in (16) and (17) give that

$$\sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, 5\boldsymbol{\sigma}_0 + \boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_2) = \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2) = 30$$

This allows us to conclude that $\sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}) = 30$. Thus by Theorem 3.8 the degree of the signature curve equals $\deg(S_X) = (3 \cdot 26 - 30)/2 = 24$.

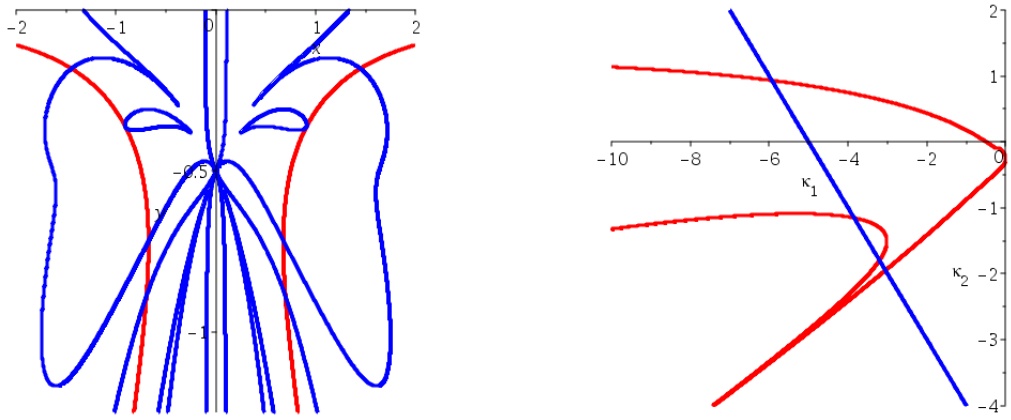

Figure 1: X and $\overline{\mathcal{S}_X}$ intersected with $V(\boldsymbol{\sigma}^*\mathbf{L_a})$ and $V(\mathbf{L_a})$ respectively.

We now show that a line $\mathbf{L}_{\tilde{\mathbf{a}}}$ defined by $\tilde{\mathbf{a}} = [1 : -6 : 1]$ does not provide us with exact degree count (the corresponding pictures are given by Figure 2). For this choice of line, $\sum_{\mathbf{p}\in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}_0 - 6\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_2) = 32$ and Corollary 3.9 tells us only that $23 \leq \deg(S_X) \leq 24$ and that $\tilde{\mathbf{a}}$ is non-generic. Indeed, $V(\mathbf{L}_{\tilde{\mathbf{a}}})$ intersects $\overline{\mathcal{S}_X}$ at the point $[0 : 6 : 1]$ which is not in $\mathcal{S}_X$, a property that must be avoided by generic lines.

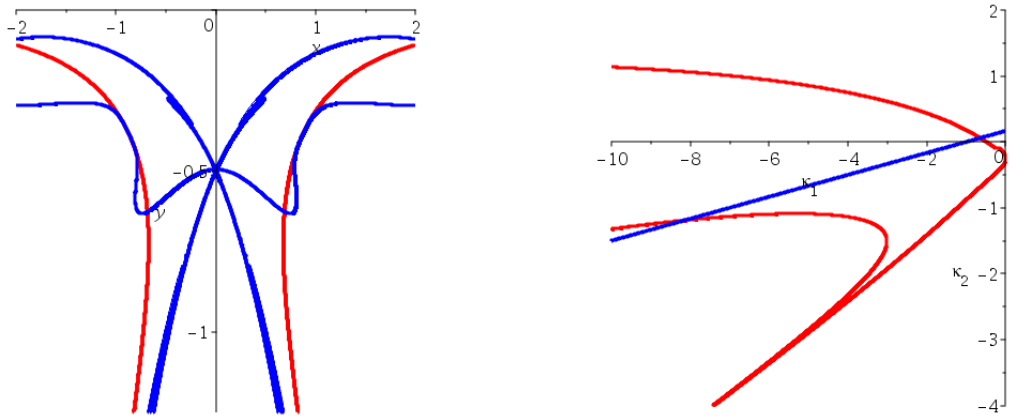

Figure 2: X and $\overline{\mathcal{S}_X}$ intersected with with $V(\boldsymbol{\sigma}^*\mathbf{L}_{\tilde{\mathbf{a}}})$ and $V(\mathbf{L}_{\tilde{\mathbf{a}}})$ respectively.

3.3 Super signature and the generic degree

Let $F_{\mathbf{c}} = \sum_{0\leq i,j\leq d} c_{ij}x^iy^j$ be a polynomial of degree $\leq d$ with unspecialized coefficients $c_{ij} \in \mathbb{C}$, where $0 \leq i, j \leq d$ and $\mathbf{c} = (c_{00} : c_{10} : \ldots : c_{0d})$. It is natural to ask if we could compute a signature polynomial $S_{\mathbf{c}}(\kappa_1, \kappa_2)$ for a curve defined by a polynomial with unspecified coefficients $\mathbf{c}$ and what information it encodes. In theory, such *super-signature* polynomial can be defined in the same way as signature polynomials for specific curves were defined in Section 2.5 and computed by elimination. In practice, the explicit computation seems to only be feasible for small groups and small d, such as, for instance, quadratics under the special Euclidean action. We also know that specialization does not always commute with elimination and, therefore, we can not expect that substitution of a specific value $\mathbf{c} = \mathbf{c}_0$ into the super-signature polynomial will produce a signature of an algebraic curve $X_{\mathbf{c}_0}$ defined by $F_{\mathbf{c}_0}$ even if $X_{\mathbf{c}_0}$ happens to be an irreducible, non-exceptional curve. However, we can show that this is the case generically.

To give a rigorous definition of the super-signature polynomial, we view

$$F(\mathbf{c}, x, y) = \sum_{0 \le i,j \le d} c_{ij} x^i y^j$$

as a polynomial of degree $d+1$ in $\mathbb{C}[\mathbf{c}, x, y]$, while $F_{\mathbf{c}} \in \mathbb{C}[x,y]_{\le d}$ denotes its specialization. Then $\mathcal{Y} = V(F)$ is a variety in $\mathbb{C}^N \times \mathbb{C}^2$, where $N = \binom{d+2}{2}$.

$$\mathcal{Y} = \{(\mathbf{c}, x, y) \,|\, \mathbf{c} \in \mathbb{C}^N, (x,y) \in V(F_{\mathbf{c}})\}. \tag{18}$$

Let $j^n(F) : \mathcal{Y} \dashrightarrow \mathbb{C}^{n+2}$ be the rational map defined by the rational functions of the partials of $F_{\mathbf{c}}(x,y)$ as in (6), with $\mathbf{c}$ treated as parameters. For a differential function K, let

$$K|_F = K \circ j^n(F) : \mathcal{Y} \dashrightarrow \mathbb{C}.$$

For a classifying pair of invariants $\mathcal{I} = \{K_1, K_2\}$, consider the rational map $\sigma : \mathcal{Y} \dashrightarrow \mathbb{C}^N \times \mathbb{C}^2$ defined by

$$\sigma(\mathbf{c}, x, y) = \left(\mathbf{c}, K_1|_F(\mathbf{c}, x, y), K_2|_F(\mathbf{c}, x, y)\right). \tag{19}$$

Denote the minimal polynomial vanishing on the image $\sigma(\mathcal{Y})$ as $S(\mathbf{c}, \kappa_1, \kappa_2) \in \mathbb{C}[\mathbf{c}, \kappa_1, \kappa_2]$ and let $\mathfrak{S} = V(S) \subset \mathbb{C}^N \times \mathbb{C}^2$ be its variety. We call S a *super-signature polynomial* and $\mathfrak{S}$ the *super-signature variety*.

The following theorem asserts that for a generic curve $X = V(F)$ of degree fixed d, one can substitute the coefficients of F into the super signature polynomial S to obtain S_X of X.

Theorem 3.11. Let $S(\mathbf{c}, \kappa_1, \kappa_2)$ be the *super-signature polynomial* for polynomials of a degree d, sufficiently large so that non-exceptional curves are generic[10], under the action of a group G with a chosen set of classifying invariants $\mathcal{I} = \{K_1, K_2\}$. For $\mathbf{c} \in \mathbb{C}^N$, let $X_{\mathbf{c}} = V(F_{\mathbf{c}})$ be the corresponding algebraic curve in $\mathbb{C}^2$. For a generic point $\mathbf{c} \in \mathbb{C}^N$,

$$\left\{\mathbf{c} \in \mathbb{C}^N \,|\, S(\mathbf{c}, \kappa_1, \kappa_2) = S_{X_{\mathbf{c}}}(\kappa_1, \kappa_2)\right\},$$

where $S_{X_{\mathbf{c}}}$ is a signature polynomial of the curve $X_{\mathbf{c}}$.[11]

Proof. The variety $\mathcal{Y}$ defined by (18) is irreducible and so is its image $\sigma(\mathcal{Y})$ under the rational map (19). Thus the super-signature polynomial $S(\mathbf{c}, \kappa_1, \kappa_2) \in \mathbb{C}[x, y, \mathbf{c}]$, which is a minimal polynomial vanishing on $\sigma(\mathcal{Y})$, is irreducible. The variety $\mathfrak{S} = V(S)$ is the Zariski-closure of $\sigma(\mathcal{Y})$ and, by Chevalley's Theorem, there is some subvariety $\mathcal{H} \subset \mathfrak{S}$ of codimenision ≥ 1 so that $\mathfrak{S} \backslash \mathcal{H} \subseteq \sigma(\mathcal{Y}) \subseteq \mathfrak{S}$. Note that $\dim \mathfrak{S} = N+1$ and so $\dim \mathcal{H} \le N$.

Consider a regular map $\pi : \mathfrak{S} \to \mathbb{C}^N$ given by $\pi(\mathbf{c}, \kappa_1, \kappa_2) = \mathbf{c}$. From the definition of $\mathfrak{S}$, it is clear that π is surjective. We claim that, for a generic $\mathbf{c} \in \mathbb{C}^N$, the set $\pi^{-1}(\mathbf{c}) \cap \mathcal{H}$ is either empty or finite. Indeed, if $\overline{\pi(\mathcal{H})} \neq \mathbb{C}^N$, then for a generic $\mathbf{c}$ lying in the Zariski open non-empty subset $\mathbb{C}^N \backslash \overline{\pi(\mathcal{H})}$, the set $\pi^{-1}(\mathbf{c}) \cap \mathcal{H}$ is empty. If $\overline{\pi(\mathcal{H})} = \mathbb{C}^N$, then, for a generic choice of $\mathbf{c}$, the dimension of $\pi^{-1}(\mathbf{c}) \cap \mathcal{H}$ is given by $\dim \mathcal{H} - N = 0$ [45, Ch. 1, Sec. 5, Theorem 1.25], implying that $\pi^{-1}(\mathbf{c}) \cap \mathcal{H}$ is either empty or finite.

By our assumption on d, for a generic point $\mathbf{c} \in \mathbb{C}^N$, the curve $X_{\mathbf{c}}$ is irreducible and non-exceptional (reducible curves have codimension $d-1$). Let us fix such generic $\mathbf{c}_0$ that also satisfies the generic condition in the previous paragraph and for which the restriction $S(\mathbf{c}_0, \kappa_1, \kappa_2) \in \mathbb{C}[\kappa_1, \kappa_2]$ is irreducible. As before, let $\sigma_{X_{\mathbf{c}_0}} : X_{\mathbf{c}_0} \dashrightarrow \mathbb{C}^2$ denote the signature map of $X_{\mathbf{c}_0}$, as given in Definition 2.29, and let $\mathcal{S}_{X_{\mathbf{c}_0}}$ denote the image of this map. Consider the intersection $\mathcal{Y}_{\mathbf{c}_0}$ of the varieties $\mathcal{Y}$ with the linear space give by $\mathbf{c} = \mathbf{c}_0$. This equals $\{\mathbf{c}_0\} \times X_{\mathbf{c}_0}$. Its image under the map σ agrees with $\{\mathbf{c}_0\} \times \mathcal{S}_{X_{\mathbf{c}_0}}$. Note that the signature polynomial $S_{X_{\mathbf{c}_0}}$ is the unique minimal polynomial in $\mathbb{C}[\kappa_1, \kappa_2]$ that vanished on this set $\sigma(\mathcal{Y}_{\mathbf{c}_0})$.

[10] Theorem 2.27 guarantees that for a sufficiently large d a generic curve is non-exceptional.

[11] Recall that for an irreducible curve the signature polynomial is uniquely defined up to multiplication by a non-zero constant.

This set is contained in the intersection of the super signature variety $\mathfrak{S}$ and and the linear space given by $\mathbf{c} = \mathbf{c}_0$, which we denote $\mathfrak{S}_{\mathbf{c}_0}$. The minimal polynomial in $\mathbb{C}[\kappa_1, \kappa_2]$ vanishing on this set is the restriction of the super polynomial $S(\mathbf{c}_0, \kappa_1, \kappa_2)$ and is irreducible by our genericity assumption on $\mathbf{c}_0$.

Recall that the set of points in $\mathfrak{S}$ that are not in $\sigma(\mathcal{Y})$ belong to a hypersurface $\mathcal{H}$, and so the set of points in $\sigma(\mathcal{Y}_{\mathbf{c}_0})$ that are not in $\mathfrak{S}_{\mathbf{c}_0}$ is a subset of $\pi^{-1}(\mathbf{c}_0) \cap \mathcal{H}$. To summarize,

$$\sigma(\mathcal{Y}_{\mathbf{c}_0}) \subseteq \mathfrak{S}_{\mathbf{c}_0} \quad \text{and} \quad \mathfrak{S}_{\mathbf{c}_0} \backslash \sigma(\mathcal{Y}_{\mathbf{c}_0}) \subseteq \pi^{-1}(\mathbf{c}_0) \cap \mathcal{H}.$$

By the argument above, $\pi^{-1}(\mathbf{c}_0) \cap \mathcal{H}$ is either empty or finite. This implies that the Zariski-closure of $\sigma(\mathcal{Y}_{\mathbf{c}_0})$ equals $\mathfrak{S}_{\mathbf{c}_0}$. Therefore the minimal polynomials in $\mathbb{C}[\kappa_1, \kappa_2]$ vanishing on these sets, $S_{X_{\mathbf{c}_0}}$ and $S(\mathbf{c}_0, \kappa_1, \kappa_2)$, must be equal. □

An immediate corollary of the above theorem is that the signature polynomials of generic curves of fixed degree d share the same monomial support in κ_1, κ_2, and hence have the same degree. Since signature polynomials (up to overall scaling) characterize equivalence classes of generic curves of degree d, it follows that if we consider the super-signature polynomial as an element of $\mathbb{C}(\mathbf{c})[\kappa_1, \kappa_2]$ and divide it by one of its non-zero coefficients $h(\mathbf{c}) \in \mathbb{C}[\mathbf{c}]$, the coefficients of the resulting polynomial generate the ring of rational invariants for the action of G on the space of polynomials $\mathbb{C}[x, y]_{\leq d}$.

Since explicit computation of such generating sets is known to be a very challenging problem, it is not surprising that computing super-signature polynomials is also very challenging. Conics under $\mathcal{SE}(2)$ is one of the few examples where the super-signature polynomial can be computed explicitly.

Example 3.12. Consider an arbitrary quadratic curve

$$F_{\mathbf{c}} = c_{00} + c_{10}x + c_{01}y + c_{20}x^2 + c_{11}xy + c_{02}y^2.$$

Let $\Upsilon_1 = c_{02}+c_{20}$, $\Upsilon_2 = 4c_{20}c_{02}-c_{11}^2$, and $\Upsilon_3 = 4\,c_{00}c_{01}c_{20}-c_{00}{c_{11}}^2-{c_{01}}^2c_{20}+c_{01}c_{10}c_{11}-c_{01}{c_{10}}^2$. These are known polynomial invariants for conics under the $\mathcal{SE}(2)$-action. For the action of the special Euclidean group $\mathcal{SE}(2)$, using the classifying pair of invariants (21) introduced in Section 4.1, the super-signature for conics computed by an elimination algorithm is:

$$\begin{aligned} S(\mathbf{c}, \kappa_1, \kappa_2) = {} & 2916\,(\Upsilon_3)^2\,\kappa_1^6 + 2916\left(\Upsilon_3\Upsilon_1\left(4\,(\Upsilon_1)^2 - 3\Upsilon_2\right)\right)\kappa_1^5 + 972\,(\Upsilon_3)^2\,\kappa_1^4\kappa_2^2 \\ & + 729\,(\Upsilon_2)^3\,\kappa_1^4 - 972\,(\Upsilon_3\Upsilon_2\Upsilon_1)\,\kappa_1^3\kappa_2^2 + 108\,(\Upsilon_3)^2\,\kappa_1^2\kappa_2^4 + 4\,(\Upsilon_3)^2\,\kappa_2^6. \end{aligned}$$

Dividing through by $(\Upsilon_3)^2$ produces three distinct non-constant coefficients listed below with constant multiples omitted:

$$A_1 = \frac{\Upsilon_1\left(4\,(\Upsilon_1)^2 - 3\Upsilon_2\right)}{\Upsilon_3}, \quad A_2 = \frac{(\Upsilon_2)^3}{(\Upsilon_3)^2}, \quad A_3 = \frac{\Upsilon_1\,\Upsilon_2}{\Upsilon_3}.$$

This is a generating set for the field of rational invariants for the action of $\mathcal{SE}(2)$ on the space of quadratic polynomials, but it is not a minimal generating set since $A_1 = 4\frac{(A_3)^3}{A_2} - 3\,A_3$.

Although computing a super-signature is very challenging, we can use super-signatures to establish theoretical results. Below we use Theorem 3.11 to show that the generic degree is the sharp upper bound for the degrees of signature polynomial. Discussion and further implications of Theorem 3.11 are explored in [42].

Theorem 3.13. Under the assumptions of Theorem 3.11, for a generic curve of degree d, the degree of its signature polynomial equals to the (κ_1, κ_2)-degree D of the super-signature polynomial. Moreover, for any non-exceptional curve X of degree less then or equal to d, the degree of its signature polynomial is less than or equal to D.

Proof. For a generic point $\mathbf{c}_0 \in \mathbb{C}^N$, the restriction of the super signature polynomial $S(\mathbf{c}_0, \kappa_1, \kappa_2)$ has degree D and, by Theorem 3.11, equals the signature polynomial of the curve $X_{\mathbf{c}_0}$. Thus for a generic curve the degree of its signature polynomial equals to D.

Now let X_0 be an arbitrary non-exceptional curve of degree $\leq d$, with defining equation $F(\mathbf{c}_0, x, y)$ corresponding to $\mathbf{c}_0 \in \mathbb{C}^N$. It will be helpful to consider a pencil of curves containing X_0. Let $\mathbf{c}_1 \in \mathbb{C}^N$ be a point satisfying the genericity conditions above, so that the signature of the curve X_1 defined by $F(\mathbf{c}_1, x, y)$ equals the restriction of $S(\mathbf{c}_1, \kappa_1, \kappa_2)$ of the super signature polynomial and has degree D. Then the open, dense set of points $\mathbf{c}$ for which the signature polynomial of the curve defined by $F(\mathbf{c}, x, y)$ is the restriction of the super signature polynomial $S(\mathbf{c}, \kappa_1, \kappa_2)$ has nontrivial intersection with the line joining $\mathbf{c}_0$ and $\mathbf{c}_1$. Thus, for a generic $\lambda \in \mathbb{C}$, the signature polynomial of the curve defined by $F((1-\lambda)\mathbf{c}_0 + \lambda\mathbf{c}_1, x, y)$ will equal the restriction of the super signature polynomial to $\mathbf{c} = (1-\lambda)\mathbf{c}_0 + \lambda\mathbf{c}_1$.

Analogously to the proof of Theorem 3.11, consider the polynomial

$$P(t, x, y) = F((1-t)\mathbf{c}_0 + t\mathbf{c}_1, x, y) = (1-t)F(\mathbf{c}_0, x, y) + tF(\mathbf{c}_1, x, y) \in \mathbb{C}[t, x, y].$$

Since X_0 and X_1 are irreducible, so are their defining equations. From this, it follows that P is irreducible in $\mathbb{C}[t, x, y]$. Let $\mathcal{Z} = V(P) \subset \mathbb{C} \times \mathbb{C}^2$ be the irreducible variety it defines. Let $j^n(P) : \mathcal{Z} \dashrightarrow \mathbb{C}^{n+2}$ be the rational map defined by the rational functions of the partials of $P(t, x, y)$ as in (6), with t treated as a parameter. For a differential function K, we can define $K|_P = K \circ j^n(P) \colon \mathcal{Z} \dashrightarrow \mathbb{C}$

Similarly to the definition of a super-signature, for a classifying pair of invariants $\mathcal{I} = \{K_1, K_2\}$, we define a rational map $\tau : \mathcal{Z} \dashrightarrow \mathbb{C} \times \mathbb{C}^2$ by

$$\tau(t, x, y) = \left(t, K_1|_P(t, x, y), K_2|_P(t, x, y)\right).$$

Denote the minimal polynomial vanishing on the image $\tau(\mathcal{Z})$ as $Q(t, \kappa_1, \kappa_2) \in \mathbb{C}[t, \kappa_1, \kappa_2]$. Since $\tau(\mathcal{Z})$ is the image of an irreducible variety under a rational map, $Q(t, \kappa_1, \kappa_2)$ is irreducible. For $\lambda \in \mathbb{C}$, let $\mathcal{Z}_\lambda$ denote the intersection of $\mathcal{Z}$ with the plane $t = \lambda$. This equals $\{\lambda\} \times X_\lambda$ where $X_\lambda \subset \mathbb{C}^2$ is the curve defined by $P(\lambda, x, y) = 0$. The image of $\mathcal{Z}_\lambda$ equals $\{\lambda\} \times \mathcal{S}_{X_\lambda}$.

It follows that the variety of Q in $\mathbb{C} \times \mathbb{C}^2$ is irreducible of dimension 2 and contains $\{\lambda\} \times \mathcal{S}_{X_\lambda}$ for every $\lambda \in \mathbb{C}$. Using the same argument as in the the proof of Theorem 3.11, one can show that for generic $\lambda \in \mathbb{C}$, the signature polynomial of X_λ equals the restriction of $Q(\lambda, \kappa_1, \kappa_2)$. It also equals the restriction of the super signature polynomial to $\mathbf{c} = (1-\lambda)\mathbf{c}_0 + \lambda\mathbf{c}_1$. Therefore Q has degree D in (κ_1, κ_2). Since the variety of Q is irreducible, has dimension 2, and contains points with $t = \lambda$ for every $\lambda \in \mathbb{C}$, the specialized polynomial $Q(\lambda, \kappa_1, \kappa_2)$ is non-zero for every $\lambda \in \mathbb{C}$. In particular, $Q(0, \kappa_1, \kappa_2)$ is non-zero and vanishes on $\mathcal{S}_{X_0}$. The signature polynomial S_{X_0} must divide $Q(0, \kappa_1, \kappa_2)$, giving

$$\deg S_{X_0} \leq \deg Q(0, \kappa_1, \kappa_2) \leq \deg_{(\kappa_1, \kappa_2)} Q = D.$$

□

4 Classical subgroups of the projective groups

In this section, we apply our general results to the actions of the full projective group and its affine, special affine, and special Euclidean subgroups. In Section 4.1 we explicitly list classifying pairs and exceptional curves for each of these groups. In Section 4.2, we derive the degree formula for signatures of generic curves under these actions as a function of the degree of the original curve (Theorem 4.13), observe that this dependence is quadratic and show that these generic degrees are sharp upper bounds. Finally, in Section 4.3, we use Fermat curves to illustrate that non-generic curves, in particular curves with a large symmetry group, may have much lower degree than generic curves. For arbitrary degree curves in this family, we give formulas of their projective and affine signature polynomials and observe that the degrees of these signatures do not depend on the degrees of the original curves.

4.1 Classifying invariants

Here we introduce rational classifying pairs of invariants for the actions of $\mathcal{PGL}(3)$ and some of its of well-known subgroups: the affine group $\mathcal{A}(2)$, the special affine group $\mathcal{SA}(2)$, and the special Euclidean group $\mathcal{SE}(2)$. For the treatment of the full Euclidean and the similarity groups see [42].

As we discussed at the beginning of Section 2.2, $\mathcal{PGL}(3)$ is the group of automorphisms of $\mathbb{CP}^2$ and is isomorphic to the quotient group $\mathcal{GL}(3)/\{\lambda I\}$, where $\mathcal{GL}(3)$ denotes the group of 3×3 non-singular matrices, $\lambda \in \mathbb{C}$ is non-zero and I is the identity matrix. The actions of $\mathcal{PGL}(3)$ and its subgroups on $\mathbb{CP}^2$ and $\mathbb{C}^2$ are given by (1) and (2).

Definition 4.1. The *affine group*, denoted $\mathcal{A}(2)$, is the subgroup of $\mathcal{PGL}(3)$ that fixes the line of points $[x_0 : x_1 : x_2]$ with $x_0 = 0$.

The affine group is isomorphic to a subgroup of $\mathcal{GL}(3)$ of matrices with the first row equal to $[1, 0, 0]$. It is a group of linear transformations and translations on $\mathbb{C}^2$.

Definition 4.2. The *special affine group*, denoted $\mathcal{SA}(2)$, is the subgroup of $\mathcal{A}(2)$ that preserves area under the action (2).

The special affine group is isomorphic to a subgroup of $\mathcal{GL}(3)$ of matrices with the first row equal to $[1, 0, 0]$ and the determinant equal to 1.

Definition 4.3. The *special Euclidean group*, denoted $\mathcal{SE}(2)$, is the subgroup of $\mathcal{PGL}(3)$ isomorphic to the group of matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ a & c & s \\ b & -s & c \end{bmatrix}, \qquad \text{with } c^2 + s^2 = 1.$$

The real subset of $\mathcal{SE}(2)$ is the well-known special Euclidean group of rotations and translations on $\mathbb{R}^2$.

In [5], the authors used classical non-rational differential invariants to build two lowest order rational invariants for the projective and affine groups and directly proved that they satisfy the Definition 2.19 of classifying invariants over $\mathbb{R}$ (see Theorem 4 in [5]). Using the same line of argument, we can show that these invariants are classifying over $\mathbb{C}$, and also produce classifying pairs for the actions of the special affine and the special Euclidean groups over $\mathbb{C}$. The following inductive expressions [10, 32] for classical differential invariants are useful for expressing these pairs in a concise manner. We start with the classical Euclidean curvature and arc-length:

$$\kappa = \frac{y^{(2)}}{(1 + [y^{(1)}]^2)^{3/2}}, \quad ds = \sqrt{1 + [y^{(1)}]^2}\,dx. \tag{20}$$

Restriction of κ to a curve given as a graph $y = u(x)$ produces its Euclidean curvature, while restrictions of ds to such curve produces a differential one-form, whose integration along a curve equals to its Euclidean length. As a differential form on the jet space, ds is contact-invariant under prolonged Euclidean transformations. There are well known counterparts of the lowest order differential invariants (curvatures) and the lowest order contact-invariant one-forms (arc-length forms) for other classical group actions. The special affine curvature and arc-length can be expressed in terms of the Euclidean invariants:

$$\mu = \frac{3\kappa(\kappa_{ss} + 3\kappa^3) - 5\kappa_s^2}{9\kappa^{8/3}}, \qquad d\alpha = \kappa^{1/3} ds,$$

where $\frac{d}{ds} = \frac{1}{\sqrt{1+[y^{(1)}]^2}} \frac{d}{dx}$, $\kappa_s = \frac{d\kappa}{ds}$ etc, and the action of operator $\frac{d}{dx}$ on differential functions is described after Definition 2.13. In a similar manner, the projective curvature and arc-length are

$$\eta = \frac{6\mu_{\alpha\alpha\alpha}\mu_\alpha - 7\mu_{\alpha\alpha}^2 - 9\mu_\alpha^2\mu}{6\mu_\alpha^{8/3}}, \qquad d\rho = \mu_\alpha^{1/3} d\alpha.$$

$$\Theta_1 = u_1^2 + 1 \qquad \Theta_2 = u_2 \qquad \Theta_3 = u_3\Theta_1 - 3u_1\Theta_2^2$$
$$\Theta_4 = 3u_4u_2 - 5u_3^2 \qquad \Theta_5 = 9u_5u_2^2 - 45u_4u_3u_2 + 40u_3^3$$
$$\Theta_6 = 9u_6u_2^3 - 63u_5u_3u_2^2 - 45u_4^2u_2^2 + 255u_4u_3^2u_2 - 160u_3^4$$
$$\begin{aligned}\Theta_7 = (9/2)\big[&18u_7u_2^4(\Theta_5) - 189u_6^2u_2^6 + 126u_6u_2^4(9u_5u_3u_2 + 15u_4^2u_2 - 25u_4u_3^2)\\ &- 189u_5^2u_2^4(4u_3^2 + 15u_2u_4) + 210u_5u_3u_2^2(63u_4^2u_2^2 - 60u_4u_3^2u_2 + 32u_3^4)\\ &-525u_4u_2(9u_4^3u_2^3 + 15u_4^2u_3^2u_2^2 - 60u_4u_3^4u_2 + 64u_3^6) + 11200u_3^8\big]\end{aligned}$$
$$\begin{aligned}\Theta_8 = (243/2)(u_2^4)\big[&2u_8u_2(\Theta_5)^2 - 8u_7(\Theta_5)(9u_6u_2^3 - 36u_5u_3u_2^2 - 45u_4^2u_2^2\\ &+ 120u_4u_3^2u_2 - 40u_3^4) + 504u_6^3u_2^5 - 504u_6^2u_2^3(9u_5u_3u_2 + 15u_4^2u_2 - 25u_4u_3^2)\\ &+ 28u_6(432u_5^2u_3^2u_2^3 + 243u_5^2u_4u_2^4 - 1800u_5u_4u_3^3u_2^2 - 240u_5u_3^5u_2 + 540u_5u_4^2u_3u_2^3\\ &+ 6600u_4^2u_3^4u_2 - 2000u_4u_3^6 - 5175u_4^3u_3^2u_2^2 + 1350u_4^4u_2^3) - 2835u_5^4u_2^4\\ &+ 252u_5^3u_3u_2^2(9u_4u_2 - 136u_3^2) - 35840u_5^2u_3^6 - 630u_5^2u_4u_2(69u_4^2u_2^2 - 160u_3^4 - 153u_4u_3^2u_2)\\ &+2100u_5u_4^2u_3(72u_3^4 + 63u_4^2u_2^2 - 193u_4u_3^2u_2) - 7875u_4^4(8u_4^2u_2^2 - 22u_4u_3^2u_2 + 9u_3^4)\big]\end{aligned}$$

Table 1: Differential functions used in (21). Here u_k denotes $y^{(k)}$.

Theorem 4.4. The following are pairs of classifying invariants for the actions of $\mathcal{SE}(2)$, $\mathcal{SA}(2)$, $\mathcal{A}(2)$, and $\mathcal{PGL}(3)$ on $\mathbb{C}^2$:

Group	$\mathcal{SE}(2)$	$\mathcal{SA}(2)$	$\mathcal{A}(2)$	$\mathcal{PGL}(3)$
K_1	$\kappa^2 = \dfrac{(\Theta_2)^2}{(\Theta_1)^3}$	$\mu^3 = \dfrac{(\Theta_4)^3}{(\Theta_2)^8}$	$\dfrac{\mu_\alpha^2}{\mu^3} = \dfrac{(\Theta_5)^2}{(\Theta_4)^3}$	$\eta^3 = \dfrac{(\Theta_7)^3}{(\Theta_5)^8}$
K_2	$\kappa_s = \dfrac{\Theta_3}{(\Theta_1)^3}$	$\mu_\alpha = \dfrac{\Theta_5}{(\Theta_2)^4}$	$\dfrac{\mu_{\alpha\alpha}}{\mu^2} = \dfrac{\Theta_6}{(\Theta_4)^2}$	$\eta_\rho = \dfrac{\Theta_8}{(\Theta_5)^4}$

(21)

The explicit formulas for Θ's in terms of jet coordinates are given in Table 1.

We use $\mathcal{I}^{\mathcal{SE}}$, $\mathcal{I}^{\mathcal{SA}}$, $\mathcal{I}^{\mathcal{A}}$, and $\mathcal{I}^{\mathcal{P}}$ to denote the respective pairs of classifying invariants in (21).

Proof. In [5, Theorem 4], $\mathcal{I}^{\mathcal{A}}$, and $\mathcal{I}^{\mathcal{P}}$ are shown to be classifying in the real case. The proof for the complex case follows similarly and an analogous argument can be applied to $\mathcal{I}^{\mathcal{SE}}$ and $\mathcal{I}^{\mathcal{SA}}$. See [33] for details. □

Proposition 4.5. The exceptional curves with respect to $\mathcal{I}^{\mathcal{P}}$, $\mathcal{I}^{\mathcal{A}}$, and $\mathcal{I}^{\mathcal{SA}}$ are lines and conics. The $\mathcal{I}^{\mathcal{SE}}$-exceptional curves are lines. In particular, if $X = V(F)$ is a curve exceptional with respect to the classifying invariants in (21) then F has degree at most two.

Proof. Propositions 2 and 3 from Section 4.3 in [5] show that $\mathcal{I}^{\mathcal{A}}$- and $\mathcal{I}^{\mathcal{P}}$-exceptional curves are lines and conics and an analogous argument shows that this is the case for $\mathcal{I}^{\mathcal{SA}}$-exceptional curves as well. A curve $X = V(F)$ being $\mathcal{I}^{\mathcal{SE}}$-exceptional is equivalent to the curve satisfying either $F_y \equiv 0$, $\Theta_1 \equiv 0$, or $\Theta_2 \equiv 0$, all of which imply X is degree one or two. □

4.2 The generic signature degree

We derive formulas for the degrees of signatures of generic[12] curves for the four actions discussed in Section 4.1 with signature maps based on the classifying sets $\mathcal{I}^{\mathcal{SE}}, \mathcal{I}^{\mathcal{SA}}, \mathcal{I}^{\mathcal{A}}, \mathcal{I}^{\mathcal{P}}$

[12] As stated in the introduction, we say that a property holds for a generic curve of degree d, if there exists a nonempty Zariski-open subset $\mathcal{P}_d$ of $\mathbb{C}[x,y]_{\leq d}$, such that for all $F \in \mathcal{P}_d$ the property holds for $V(F)$.

given in (21). To do so we analyze each term in the degree formula (15) of Theorem 3.8. We start by taking a closer look at the rational functions defining invariants (21).

Lemma 4.6. For a generic polynomial $F \in \mathbb{C}[x,y]$ of degree $d \geq 3$, the restrictions of the differential functions Θ_i to the curve $V(F)$ are equal to rational functions of the form $T_i(x,y)/(F_y)^{d_i}$ with $\deg(T_i) \leq \tau_i$ where τ_i, d_i are given as follows:

i	1	2	3	4	5	6	7	8
τ_i	$2d-2$	$3d-4$	$6d-8$	$8d-12$	$12d-18$	$16d-24$	$32d-48$	$48d-72$
d_i	2	3	6	8	12	16	32	48

Proof. One can check that each derivative function restricted to $X = V(F)$ can be written

$$y^{(n)}|_X = \frac{P_n(x,y)}{(F_y)^{2n-1}} \quad \text{where } P_n \in \mathbb{Q}\left[\frac{\partial^{i+j}F}{\partial x^i \partial y^j} \ : \ i+j \leq n\right]$$

and $P_n(x,y)$ is a polynomial of degree $(2n-1)d-(3n-2)$. One can evaluate the formulas for $\Theta_1, \ldots, \Theta_8$ given in Table 1. For example, plugging in the rational expressions for $y^{(n)}|_X$ to the differential formula for Θ_4 gives $\Theta_4 = \left(3P_4P_2 - 5(P_3)^2\right)/F_y^{10}$. See [33] for explicit computations. The numerator has degree $10d-14$, but it is also divisible by F_y^2. This gives an expression $\Theta_4 = T_4(x,y)/(F_y)^8$ where T_i has degree less than or equal to $8d-12$. The arguments for the other differential functions follow similarly. □

Explicit formulas for the polynomials T_i are quite long. A code to compute them can be found in [33]. Note that for each of the classifying invariants, the partial derivative function F_y cancels out and leaves each invariant as a rational function of the polynomials $T_1, \ldots, T_8$. In the following lemma, we use homogenizations of $T_1, \ldots, T_8$ to write down projective extensions $\boldsymbol{\sigma}$ of the signature maps for each pair of invariants (21).

Lemma 4.7. Fix an irreducible polynomial $F \in \mathbb{C}[x,y]$ of degree $d \geq 3$ and let $X = V(F)$. For $G = \mathcal{SE}, \mathcal{SA}, \mathcal{A}, \mathcal{P}$, let σ_X^G denote the signature map given by the invariants $\mathcal{I}^G$ in (21). Then

$$\begin{aligned} \boldsymbol{\sigma}^{\mathcal{SE}} &= [\mathbf{T}_1{}^3 : x_0^2\mathbf{T}_2{}^2 : x_0^2\mathbf{T}_3], & \boldsymbol{\sigma}^{\mathcal{SA}} &= [\mathbf{T}_2{}^8 : x_0^4\mathbf{T}_4{}^3 : x_0^2\mathbf{T}_2{}^4\mathbf{T}_5], \\ \boldsymbol{\sigma}^{\mathcal{A}} &= [\mathbf{T}_4{}^3 : \mathbf{T}_5{}^2 : \mathbf{T}_4\mathbf{T}_6], \quad \text{and} & \boldsymbol{\sigma}^{\mathcal{P}} &= [\mathbf{T}_5{}^8 : \mathbf{T}_7{}^3 : \mathbf{T}_8\mathbf{T}_5{}^4] \end{aligned} \tag{22}$$

are projective extensions of the maps $\sigma_X^{\mathcal{SE}}$, $\sigma_X^{\mathcal{SA}}$, $\sigma_X^{\mathcal{A}}$, and $\sigma_X^{\mathcal{P}}$, respectively, where for each i, $\mathbf{T}_i$ equals the homogenization, $x_0^{\tau_i}T_i(\frac{x_1}{x_0}, \frac{x_2}{x_0}) \in \mathbb{C}[x_0,x_1,x_2]$, of the polynomial T_i from Lemma 4.6. Moreover,

$$\deg(\boldsymbol{\sigma}^{\mathcal{SE}}) = 6d-6, \ \deg(\boldsymbol{\sigma}^{\mathcal{SA}}) = 24d-32, \ \deg(\boldsymbol{\sigma}^{\mathcal{A}}) = 24d-36, \ \text{ and } \ \deg(\boldsymbol{\sigma}^{\mathcal{P}}) = 96d-144.$$

Proof. First, we note that by Lemma 4.6, the coordinates of $\boldsymbol{\sigma}^G$ are homogeneous of the stated degrees and that by Proposition 4.5, X is non-exceptional with respect to each of the classifying sets of invariants in (21). Moreover, with $G = \mathcal{A}$, for a point $p \in X$ we see that,

$$\sigma_X^{\mathcal{A}}(p) \ = \ \left(\frac{\Theta_5(p)^2}{\Theta_4(p)^3}, \frac{\Theta_6(p)}{\Theta_4(p)^2}\right) \ = \ \left(\frac{T_5(p)^2}{T_4(p)^3}, \frac{T_6(p)}{T_4(p)^2}\right) \ = \ \left(\frac{\boldsymbol{\sigma}_1^{\mathcal{A}}(1,p)}{\boldsymbol{\sigma}_0^{\mathcal{A}}(1,p)}, \frac{\boldsymbol{\sigma}_2^{\mathcal{A}}(1,p)}{\boldsymbol{\sigma}_0^{\mathcal{A}}(1,p)}\right).$$

Here the middle equality follows from the fact that the factors of F_y given by the degrees d_i in Lemma 4.6 all cancel out in the above expressions. If $\boldsymbol{\sigma}^{\mathcal{A}}(p)$ is not defined then $\Theta_4(p) = 0$, meaning p is not $\mathcal{I}$-regular. Thus $\boldsymbol{\sigma}^{\mathcal{A}}(p)$ is defined at all but finitely many points of X. Analogous arguments show that $\boldsymbol{\sigma}^{\mathcal{SE}}$, $\boldsymbol{\sigma}^{\mathcal{SA}}$, and $\boldsymbol{\sigma}^{\mathcal{P}}$ are projective extensions of $\sigma_X^{\mathcal{SE}}$, $\sigma_X^{\mathcal{SA}}$, and $\sigma_X^{\mathcal{P}}$. □

We are now ready to analyze the last term in the degree formula (15) where the sum of multiplicities is taken over the base locus of a projective extension $\boldsymbol{\sigma}$ of the signature map. We first show that, for our choices of projective extensions, all base locus points belonging to a generic curve are "at infinity."

Lemma 4.8. For a generic polynomial $F \in \mathbb{C}[x,y]_{\leq d}$, $d \geq 4$, the base locii of the maps $\boldsymbol{\sigma}^{\mathcal{SE}}$, $\boldsymbol{\sigma}^{\mathcal{SA}}$, $\boldsymbol{\sigma}^{\mathcal{A}}$ and $\boldsymbol{\sigma}^{\mathcal{P}}$ in (22) contain no points of the form $[1:p] \in \mathbb{CP}^2$ where $F(p) = 0$.

Proof. We will provide a detailed proof for the affine group and then show how this argument can be adapted to other groups. For any point $p \in \mathbb{C}^2$, consider the set

$$\mathcal{V}_p^{\mathcal{A}} \;=\; \left\{F \in \mathbb{C}[x,y]_{\leq d} \,|\, F(p) = 0 \text{ and } [1:p] \text{ belongs to the base locus of } \boldsymbol{\sigma}^{\mathcal{A}}\right\}.$$

Our goal is to show that the set

$$\mathcal{V}^{\mathcal{A}} = \bigcup_{p \in \mathbb{C}^2} \mathcal{V}_p^{\mathcal{A}}$$

has codimension at least 1 in the linear space of polynomials $\mathbb{C}[x,y]_{\leq d}$.

For a polynomial $F \in \mathbb{C}[x,y]_{\leq d}$, a point $[1:p]$ belongs to the base locus of the map $\boldsymbol{\sigma}^{\mathcal{A}}$ if and only if $T_4(p) = T_5(p) = 0$. Polynomials T_i were introduced in Lemma 4.6, and they can be expressed as polynomials function of the partial derivatives of F. Therefore, for $F(x,y) = \sum_{i+j\leq d} c_{ij} x^i y^j$ with undetermined coefficients and a fixed point p, expressions $T_4(p)$ and $T_5(p)$ can be viewed as polynomials in the coefficients c_{ij}. This allows us to express $\mathcal{V}_p^{\mathcal{A}}$ as the variety of three polynomial expressions $F(p)$, $T_4(p)$, and $T_5(p)$ in the coefficients c_{ij} where $i + j \leq d$.

For $p = (0,0)$, we can use computational algebra techniques to find the codimension of this set. The condition $F(0,0) = 0$ is equivalent to $c_{0,0} = 0$. The highest order partial derivative appearing in the expressions for T_4 and T_5 is 5. Therefore $T_4(0,0)$ and $T_5(0,0)$ can be written as polynomials of c_{ij} where $i+j \leq 5$. Moreover, for $d \geq 5$, these polynomials are independent of d. For $d = 4$, all monomials involving $c_{ij}, i+j = 5$ will disappear. For $d \geq 4$, one can check (see [33]) that three polynomials $c_{0,0}$, $T_4(0,0)$ and $T_5(0,0)$ impose algebraically independent conditions, implying that $\mathcal{V}_{(0,0)}^{\mathcal{A}}$ has codimension 3 in $\mathbb{C}[x,y]_{\leq d}$ (the case $d = 4$ has to be checked separately).

Now we claim that for any point $p \in \mathbb{C}^2$, a polynomial F belongs to $\mathcal{V}_p^{\mathcal{A}}$ if and only if its image under translation $\overline{F}(x,y) = F(x+p_1, y+p_2)$ belongs to $\mathcal{V}_{(0,0)}^{\mathcal{A}}$. Note that the partial derivatives of F are invariant under translations: $\frac{\partial^{i+j}\overline{F}}{\partial x^i y^j}(x,y) = \frac{\partial^{i+j}F}{\partial x^i y^j}(x+p_1, y+p_2)$ for all i, j. Let $\overline{T_4}, \overline{T_5}$ denote the polynomials obtained from Lemma 4.6 from $\overline{F}$. Since these are functions of the partial derivatives of $\overline{F}$, they are also invariant under translations: $\overline{T}_i(x,y) = T_i(x+p_1, y+p_2)$. Then F belongs to $\mathcal{V}_p^{\mathcal{A}}$ if and only if $F(p) = \overline{F}(0,0) = 0$, $T_4(p) = \overline{T_4}(0,0) = 0$, and $T_5(p) = \overline{T_5}(0,0) = 0$, which occurs if and only if $\overline{F} \in \mathcal{V}_{(0,0)}^{\mathcal{A}}$. This shows that the set of polynomials not satisfying the condition in the statement of Lemma 4.8 can be written as

$$\mathcal{V}^{\mathcal{A}} \;=\; \left\{F \in \mathbb{C}[x,y]_{\leq d} \,|\, F(x+p_1, y+p_2) \in \mathcal{V}_{(0,0)}^{\mathcal{A}}\right\}.$$

Then the dimension of $\mathcal{V}^{\mathcal{A}}$ is at most $\dim(\mathcal{V}_{(0,0)}^{\mathcal{A}}) + 2$. Since $\mathcal{V}_{(0,0)}^{\mathcal{A}}$ has codimension 3 in the space of polynomials $\mathbb{C}[x,y]_{\leq d}$, this means that $\mathcal{V}^{\mathcal{A}}$ has codimension ≥ 1.

A similar argument, based on translation of an affine point p to the origin, goes through for other groups, and the proof of the lemma boils down to showing that

$$\mathcal{V}_{(0,0)}^{G} \;=\; \left\{F \in \mathbb{C}[x,y]_{\leq d} \,|\, F(p) = 0 \text{ and } [1:p] \text{ belongs to the base locus of } \boldsymbol{\sigma}^{G}\right\},$$

where $\boldsymbol{\sigma}^G$ is the projective extension of the signature map for an appropriate group G, has a codimension of at least 3 in $\mathbb{C}[x,y]_{\leq d}$.

In the $\mathcal{SE}(2)$ case and $d \geq 2$, the variety $\mathcal{V}_{(0,0)}^{\mathcal{SE}}$ is defined by four polynomials $c_{0,0}$, $T_1(0,0) = (c_{01})^2 + (c_{10})^2$, $T_2(0,0) = -2c_{20}(c_{01})^2 + 2c_{11}c_{10}c_{01} - 2(c_{10})^2 c_{02}$ and $T_3(0,0)$ in $\mathbb{C}[c_{ij} : i+j \leq 3]$. Clearly, $T_1(0,0)$, $T_2(0,0)$ and c_{00} impose algebraically independent conditions on $\mathbb{C}[x,y]_{\leq d}$. Thus, by the above argument, $\mathcal{V}_{(0,0)}^{\mathcal{SE}}$ must be of codimension at least 3 in $\mathbb{C}[x,y]_{\leq d}$ for all $d \geq 2$.

In the $\mathcal{SA}(2)$ case, the variety $\mathcal{V}_{(0,0)}^{\mathcal{SA}}$ is defined by three polynomials $c_{0,0}$, $T_2(0,0)$ and $T_4(0,0)$ in $\mathbb{C}[c_{ij} : i + j \leq 4]$, where for $d \geq 4$, $T_2(0,0)$ and $T_4(0,0)$ are independent of d. Algebraic independence of these polynomials is checked in [33]. Finally, for the full projective group

$\mathcal{PGL}(3)$, the variety $\mathcal{V}^{\mathcal{SA}}_{(0,0)}$ is defined by three polynomials $c_{0,0}$, $T_5(0,0)$ and $T_7(0,0)$ in $\mathbb{C}[c_{ij} : i+j \leq 7]$, where $T_5(0,0)$ and $T_7(0,0)$ are independent of d for $d \geq 7$. The algebraic independence of these three polynomials is checked in [33]. When $d = 4, 5$, or 6 some monomials disappear and so algebraic independence has to be checked separately. □

As a side remark, we point out that under the $\mathcal{SE}(2)$-action, a generic curves does not have any base locus points (even at infinity) as shown in Lemma 4.12 below.

Lemma 4.9. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ be a generic homogeneous polynomial of degree d satisfying two generic conditions:

(i) $\mathbf{F}(0, 0, 1) \neq 0$,

(ii) the discriminant of the univariate polynomial $F(0, 1, x_2)$ is nonzero.

Then neighborhood of any point $\mathbf{p} = [0 : p_1 : p_2]$ in $V(\mathbf{F})$ can be parametrized by $t \mapsto [\alpha(t)]$ where

$$\alpha(t) \;=\; \left(t, 1, \sum_{j=0}^{\infty} a_j t^j\right) \;\in\; \mathbb{C}[[t]]^3. \tag{23}$$

Moreover, for any homogeneous polynomial $\mathbf{G} \in \mathbb{C}[x_0, x_1, x_2]$, the intersection multiplicity of $\mathbf{F}$ and $\mathbf{G}$ at $\mathbf{p}$ is given by $\mathrm{val}(\mathbf{G}(\alpha))$.

Proof. Consider a point $\mathbf{p} = [0 : p_1 : p_2]$ in $V(\mathbf{F})$. From the first assumption it follows that $p_1 \neq 0$ and thus we can take $p_1 = 1$. From the second assumption it follows the restriction $H = \mathbf{F}(v, 1, w) \in \mathbb{C}[v, w]$ satisfies $H_w(0, p_2) = \frac{\partial \mathbf{F}}{\partial x_2}(\mathbf{p}) \neq 0$. Therefore, in some neighborhood of $(0, p_2)$, the curve $V(H) \subset \mathbb{C}^2$ agrees with the graph $w = f(v)$ of an analytic function f. We obtain α as a power series expansion of this function with $a_j = \frac{f^{(j)}(0)}{j!}$. For the claim that the intersection multiplicity of $\mathbf{F}$ and $\mathbf{G}$ is given by $\mathrm{val}(\mathbf{G}(\alpha))$, see [13, §8.4]. □

Lemma 4.10. For $d \geq 3$, a generic point $(a_0, \ldots, a_8) \in \mathbb{C}^9$ can be extended to the coefficients of the parametrization (23) for some $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ satisfying conditions of Lemma 4.9.

Proof. Note that $n = 8$ and $d \geq 3$ satisfy the assumptions of Lemma 2.26, implying that for a generic point $a \in \mathbb{C}^9$, there exists an irreducible algebraic curve $X \subset \mathbb{C}^2$ of degree d, such that $(0, a_0) \in X$ and $j^{(8)}_X(0, a_0) \;=\; (0,\, a_0, 1!\, a_1 \ldots, 8!\, a_8)$. Let $F(x, y) \in \mathbb{C}[x, y]$ be an irreducible polynomial of degree d whose variety is X. It is easy to check that for the homogenization $\mathbf{F}(x_0, x_1, x_2) = x_1^d F\left(\frac{x_0}{x_1}, \frac{x_2}{x_1}\right)$, the projective curve $V(\mathbf{F})$ has the desired parametrization (23) in a neighborhood of $[0 : 1 : a_0]$. □

Lemma 4.11. Let $F \in \mathbb{C}[x, y]_{\leq d}$ be a generic polynomial with degree $d \geq 3$ and let $\alpha = (\alpha_0, \alpha_1, \alpha_2)$ denote the parametrization given by Lemma 4.9 for its homogenization $\mathbf{F}$. For sufficiently small $t \in \mathbb{C}^*$, the Laurent series

$$\beta(t) = t^{-1}(\alpha_1(t), \alpha_2(t)) = \left(t^{-1}, \sum_{j=-1}^{\infty} a_{j+1} t^j\right)$$

parametrizes the curve $V(F)$. The differential functions Θ_i along this parametrization satisfy:

i	1	2	3	4	5	6	7	8
$\mathrm{val}(\Theta_i(\beta))$	0	3	4	8	15	19	40	60

Proof. First let us calculate the image of β in the jet space. For $(x(t), y(t)) = (t^{-1}, t^j)$ with $j \geq 1$, the derivative of y with respect to x equals $-jt^{j+1}$. Repeated applications of $\frac{\partial}{\partial x}$ then yields that $y^{(k)}(x)$ equals $(-1)^k t^{j+k} \prod_{i=0}^{k-1}(i+j)$. Then for $(x(t), y(t)) = \beta(t)$ and $k \geq 2$,

$$y^{(k)}(x) \quad = \quad (-1)^k \cdot \sum_{j=1}^{\infty} a_{j+1} t^{j+k} \cdot \prod_{i=0}^{k-1}(i+j).$$

We can then evaluate the differential functions $\Theta_1, \ldots, \Theta_8$ on truncations of these formulas, where a_j are indeterminates. (See [33].) For example, evaluating Θ_4 and Θ_5 give

$$\begin{aligned} \Theta_4(\beta) &= -36 \cdot a_2 \cdot t^8 + \text{higher order terms}, \quad \text{and} \\ \Theta_5(\beta) &= -4320 \cdot (2a_3^3 - 3a_2 a_3 a_4 + a_2^2 a_5) \cdot t^{15} + \text{higher order terms}. \end{aligned}$$

In each case, the leading coefficients are polynomials of $a_0, \ldots, a_8$. Therefore, by Lemma 4.10 and the genericity of F, we may assume that these leading coefficients do not vanish. □

Lemma 4.12. For a generic homogeneous polynomial $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ with $d \geq 3$ and a point $\mathbf{p} = [0 : p_1 : p_2]$ in $V(\mathbf{F})$, we have

$$\operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SE}}) = 0, \quad \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SA}}) = 16, \quad \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{A}}) = 12, \quad \text{and} \quad \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{P}}) = 72,$$

where $\boldsymbol{\sigma}^{\mathcal{SE}}$, $\boldsymbol{\sigma}^{\mathcal{SA}}$, $\boldsymbol{\sigma}^{\mathcal{A}}$ and $\boldsymbol{\sigma}^{\mathcal{P}}$ are the polynomial vectors given by Lemma 4.7 for $F = \mathbf{F}(1, x, y)$ and the corresponding multiplicities are defined by (13).

Proof. Let $\alpha \in \mathbb{C}[[t]]^3$ be the local parametrization of $V(\mathbf{F})$ guaranteed by Lemma 4.9. For each index $i = 1, \ldots, 8$, let v_i denote the valuation of $\mathbf{T}_i(\alpha)$. By the same lemma and the formulas in Lemma 4.7, the desired multiplicities are

$$\begin{aligned} \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SE}}) = \min\{3v_1, 2 + 2v_2, 2 + v_3\}, \quad \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SA}}) = \min\{8v_2, 4 + 3v_4, 2 + 4v_2 + v_5\}, \\ \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{A}}) = \min\{3v_4, 2v_5, v_4 + v_6\}, \text{ and } \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{P}}) = \min\{8v_5, 3v_7, 4v_5 + v_8\}. \quad (24) \end{aligned}$$

Let $\beta \in \mathbb{C}((t))^2$ be the tuple of Laurent series given by Lemma 4.11. Since $\mathbf{T}_i$ is homogeneous of degree τ_i and $\alpha = t \cdot (1, \beta)$, we see that

$$\mathbf{T}_i(\alpha) = \mathbf{T}_i(t, t\beta) = t^{\tau_i} \mathbf{T}_i(1, \beta) = t^{\tau_i} T_i(\beta).$$

By genericity, the coefficient of x^{d-1} in F_y is nonzero, meaning that the valuation of $F_y(\beta)$ is $-(d-1)$. This and the formulas $T_i = \Theta_i \cdot (F_y)^{d_i}$ from Lemma 4.6 give that

$$\begin{aligned} v_i = \operatorname{val}(\mathbf{T}_i(\alpha)) = \tau_i + \operatorname{val}(T_i(\beta)) &= \tau_i + \operatorname{val}(\Theta_i(\beta)) + d_i \operatorname{val}(F_y(\beta)) \\ &= \tau_i + \operatorname{val}(\Theta_i(\beta)) - d_i(d-1). \end{aligned}$$

Then combining the data from Lemmas 4.6 and 4.11 gives that

$$v_1 = 0, \quad v_2 = 2, \quad v_3 = 2, \quad v_4 = 4, \quad v_5 = 9, \quad v_6 = 11, \quad v_7 = 24, \quad \text{and} \quad v_8 = 36.$$

Substitution of this value in (24) finishes the proof. □

Theorem 4.13. Fix an irreducible polynomial $F \in \mathbb{C}[x, y]_{\leq d}$ of degree $d \geq 4$ and let $X = V(F)$. Let $S_X^{\mathcal{SE}}$, $S_X^{\mathcal{A}}$, $S_X^{\mathcal{SA}}$, and $S_X^{\mathcal{P}}$ denote the signature polynomials defined by the invariants in (21). Then, when the symmetry group of X is finite,

$$\deg(S_X^{\mathcal{SE}}) \leq 6d^2 - 6d, \quad \deg(S_X^{\mathcal{SA}}), \deg(S_X^{\mathcal{A}}) \leq 24d^2 - 48d, \quad \text{and} \quad \deg(S_X^{\mathcal{P}}) \leq 96d^2 - 216d.$$

Furthermore, these bounds are tight for generic $F \in \mathbb{C}[x, y]_{\leq d}$.

Proof. First we show that the bounds above are achieved for generic $F \in \mathbb{C}[x,y]_{\leq d}$. By Proposition 4.5, the curve X is non-exceptional for $\mathcal{I}^{\mathcal{SE}}$, $\mathcal{I}^{\mathcal{A}}$, $\mathcal{I}^{\mathcal{SA}}$, and $\mathcal{I}^{\mathcal{P}}$ and we can apply Theorem 3.8. Since X is a general curve of degree ≥ 4, its symmetry group is trivial and so $n = 1$ [47]. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ denote the homogenization of F and $\boldsymbol{X} = V(\mathbf{F}) \in \mathbb{CP}^2$. Then by Theorem 3.8, for a projective extension of a signature map $\boldsymbol{\sigma}$,

$$\deg(S_X) \;=\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}).$$

For a generic $\mathbf{F}$, the variety $V(\mathbf{F})$ contains exactly d points with $x_0 = 0$. The multiplicities at each of these points is given by Lemma 4.12 for every group under consideration. By Lemma 4.8, these are the only points of $V(\mathbf{F})$ in the base locii of the projective extensions $\boldsymbol{\sigma}^{\mathcal{SE}}$, $\boldsymbol{\sigma}^{\mathcal{A}}$, $\boldsymbol{\sigma}^{\mathcal{SA}}$, and $\boldsymbol{\sigma}^{\mathcal{P}}$. All together, this gives

$$\begin{aligned}
\deg(S_X^{\mathcal{SE}}) &= d \cdot (6d-6) - d \cdot (0) \;=\; 6d^2 - 6d, \\
\deg(S_X^{\mathcal{SA}}) &= d \cdot (24d-32) - d \cdot (16) \;=\; 24d^2 - 48d, \\
\deg(S_X^{\mathcal{A}}) &= d \cdot (24d-36) - d \cdot (12) \;=\; 24d^2 - 48d, \text{ and} \\
\deg(S_X^{\mathcal{P}}) &= d \cdot (96d-144) - d \cdot (72) \;=\; 96d^2 - 216d.
\end{aligned}$$

From Theorem 3.13, these degrees are upper bounds. □

We note that for all groups we consider, for generic curves, the degree of the signature curve has a quadratic dependence on the degree of the original curve. The symmetry group of a generic curve is trivial, but many interesting and important curves have non-trivial symmetry groups. In accordance with the degree formula (15), these curves have lower degree signature. The next subsection is devoted to the Fermat curves family. For this family, in the case of the projective and affine action, the growth of the signature curve degree is completely suppressed by the increase in the symmetry group size.

4.3 The Fermat curves

The d-th degree Fermat curve, denoted in this section by X_d, is the zero set over $\mathbb{C}^2$ of the polynomial $F_d(x,y) = x^d + y^d + 1$, whose homogenization is $\mathbf{F}_d(x_0, x_1, x_2) = x_0^d + x_1^d + x_2^d$.

Theorem 4.14. The symmetry group of the d-th degree Fermat curve with respect to full projective, affine and special Euclidean groups are:

- $\mathrm{Sym}(X_d, \mathcal{PGL}(3)) = S_3 \rtimes (\mathbb{Z}_d \times \mathbb{Z}_d)$ of cardinality $6d^2$,
- $\mathrm{Sym}(X_d, \mathcal{A}(2)) = S_2 \rtimes (\mathbb{Z}_d \times \mathbb{Z}_d)$ of cardinality $2d^2$, and
- $\mathrm{Sym}(X_d, \mathcal{SE}(2)) = \begin{cases} \mathbb{Z}_1 & \text{of cardinality 1, when } d \text{ is odd} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{of cardinality 4, when } d \text{ is even.} \end{cases}$

Here S_k is the permutation group over k-elements and $\mathbb{Z}_k$ is the cyclic groups of k-elements.

Proof. In [49] it has been shown that $\mathrm{Sym}(X_d, \mathcal{PGL}(3))$ consists of compositions of permutations of the homogeneous coordinates $[x_0 : x_1 : x_2]$ and transformations scaling the coordinates by d-th roots of unity, *i.e.* $[x_0 : x_1 : x_2] \to [x_0 : \omega_1 x_1 : \omega_2 x_2]$, where ω_1 and ω_2 are d-th roots of 1. This shows the first result. Since $\mathrm{Sym}(X_d, \mathcal{A}(2))$ is the subgroup of $\mathrm{Sym}(X_d, \mathcal{PGL}(3))$ that fixes the homogenous coordinate x_0, in the second result S_3 must be replaced with S_2. Finally, in the case of the special Euclidean group for odd d there are no non-trivial symmetries, while for even d the symmetry group is generated by two independent elements, each of order two, namely $[x_0 : x_1 : x_2] \to [x_0 : -x_2 : x_1]$ and $[x_0 : x_1 : x_2] \to [x_0 : -x_1 : -x_2]$. □

For the projective and for the affine groups, the cardinality of the symmetry groups depend quadratically on d. At the same time Theorem 4.13 shows that the degrees of generic signature curves depend quadratically on d. In fact, these quadratic dependencies cancel, and the degrees of signatures of the Fermat curves for these actions are independent of d.

Theorem 4.15. The signature of the Fermat curve $V(x^d + y^d + 1) \subset \mathbb{C}^2$ has

- degree four for all $d \geq 3$ for the $\mathcal{PGL}(3)$-action.
- degree two for $d = 3$ and degree three for all $d \geq 4$ for the $\mathcal{A}(2)$-action.

We remind the reader that the signatures of lines and conics are undefined under the projective and affine actions. The above result can be proven by computing all quantities involved in (15) (see [33] for details) or by explicit computation of signature polynomials. We present here the explicit formulas for signatures polynomials and observe that their coefficients (but not their degrees) depend on d. For the projective group the signature polynomial of the Fermat curve of degree $d > 2$ is:

$$\begin{aligned}
S^{\mathcal{P}}_{X_d}(\kappa_1, \kappa_2) \;=\; & 49392(d-2)^4 d^3 (d+1)^4 (2d-1)^4 \kappa_2^4 + 602112(d-2)^4 d^3 (d+1)^4 (2d-1)^4 \kappa_1 \kappa_2^2 \\
& + 10584(d-2)^3 d^2 (d+1)^3 (2d-1)^3 \left(10d^2 - 3d + 3\right) \left(34d^2 - 27d + 27\right) \kappa_2^3 \\
& + 1835008(d-2)^4 d^3 (d+1)^4 (2d-1)^4 \kappa_1^2 - 9289728(d-2)^3 d^2 (d+1)^3 (2d-1)^3 \left(d^2 - d + 1\right)^2 \kappa_1 \kappa_2 \\
& + 61236(d-2)^2 d (d+1)^2 (2d-1)^2 \left(d^2 - d + 1\right) \left(10d^2 - 3d + 3\right)^2 \left(16d^2 - 9d + 9\right) \kappa_2^2 \\
& - 23328(d-2)^2 d (d+1)^2 (2d-1)^2 \left(11792d^8 - 17376d^7 + 28152d^6 - 24424d^5 + 19473d^4 - 8940d^3 \right. \\
& \left. + 3358d^2 - 324d + 81\right) \kappa_1 + 118098(d-2)(d+1)(2d-1) \left(d^2 - d + 1\right)^2 \left(10d^2 - 3d + 3\right)^4 \kappa_2 \\
& + 531441 d \left(d^2 - d + 1\right)^3 \left(10d^2 - 3d + 3\right)^4 .
\end{aligned}$$

The signature polynomial of the Fermat curve of degree $d > 2$ under the affine action is:

$$\begin{aligned}
S^{\mathcal{A}}_{X_d}(\kappa_1, \kappa_2) \;=\; & (d-3)^2 (d-2) d^2 (d+1) (2d-1)^3 \kappa_2^3 - (d-5)^3 d (2d-1)^2 \kappa_1^2 \\
& + 3(d-5)(d-2) d (d+1) (2d-1)^2 (5d-11) \kappa_1 \kappa_2 + 6(d-2)^2 d (d+1)^2 (2d-1)^2 \left(d^2 - 4d + 6\right) \kappa_2^2 \\
& + 2(d-2)^2 (d+1)^2 (2d-1) \left(15d^2 - 10d + 18\right) \kappa_1 + 12(d-2)^3 (d+1)^3 (2d-1) \left(d^2 - 2d + 3\right) \kappa_2 \\
& + 8(d-2)^4 d (d+1)^4 .
\end{aligned}$$

For $d = 3$, the coefficient of κ_2^3 vanishes and the degree of the signature polynomial drops to two.

5 Discussion and future directions

The problem of equivalence and symmetry of algebraic curves under the action of the projective group and its subgroups is intimately related to the problem of the equivalence and symmetries of ternary forms under the action of the general linear group and its subgroups. Such problems and their generalizations were at the heart of classical 19th century invariant theory. Linear changes of variables induce linear transformations of the coefficients of polynomials. The latter serve as coordinates on the $\binom{d+2}{2}$-dimensional vector space $\mathbb{C}[x_0, x_1, x_2]_d$. The classical problem was to find generators of the rings of polynomial invariants and generators of the fields of rational invariants under such actions. Actions on the product space $\mathbb{C}[x_0, x_1, x_2]_d \times \mathbb{C}^3$ were also considered, and the invariants with respect to these actions were called covariants in the classical literature. An overview of the classical methods for constructing invariants and covariants as well their application to the classification of polynomials can be found in [15], [19], [39]. Due to Hilbert's finite basis theorem, the generating sets for such actions are finite [1], but their cardinality and the complexity of the invariants grow dramatically with the degree. In fact, the complete set of the generators remains unknown except for the ternary forms of low degrees.

Applications of differential invariants to the problems in classical invariant theory was first proposed by Sophus Lie [35]. One of the main advantages of using differential invariants in comparison with classical algebraic invariants and covariants is that the same set of invariants can

be used for all ternary forms independently of their degrees. Differential signature constructions for homogeneous polynomials in two variables (binary forms) were first introduced by Olver [39] and applied to their symmetry groups computation in [3]. For the case of ternary forms, a fundamental set of differential invariants was first computed in [31] and it has been shown in [18] that the differential algebra of invariants can be generated by a single differential invariant and two invariant differential operators. In his thesis, Wears [51], considered differential signatures of polynomials in an arbitrary number of variables. In the above literature, one extends the action to the jets of the graphs of homogeneous polynomials $u = \mathbf{F}(x_0, x_1, x_2)$ or in-homogeneous polynomials $u = F(x, y)$, computes the set of fundamental invariants of a sufficiently high order, and uses these invariants to construct signatures. In contrast to the signatures developed in this paper, the signatures of these graphs are surfaces rather than curves.

Gaining an understanding of the relationship between signatures surfaces of the defining polynomials, considered in the above literature, and signatures curves of their zero sets, considered in this paper, is an interesting problem for future research. In particular, signature surfaces of the graphs of the Fermat polynomials with respect to the projective groups computed in [31] can be compared with the signatures of Fermat curves obtained here.

Proposition 2.21, provides a simple relationship between pairs of classifying invariants for a given group. *The signatures curves and their degrees depend on a choice of classifying invariants, but a careful study of this dependence is outside of the scope of the current paper.*

Since explicit computation of signature polynomials is challenging, it is helpful to identify their properties that can be computed a priori. In this paper we derived the degree formula of signature polynomials. One natural step is to *determine their Newton polytope, which gives a more detailed information about the monomials of the signature polynomial.*

It is immediate that the signatures curves of rational curves are rational. However, the signatures of non-rational curves may be also rational, as happens for instance in the case of all Fermat curves under the affine and the projective actions. It is an interesting problem *to identify classes of curves with rational signatures and, more generally, to understand if we can predict the genus of a signature curve.*

References

[1] M. Ackerman and R. Hermann, *Hilbert's Invariant Theory Papers*, Math Sci Press, Brookline, Mass., 8 (1978).

[2] D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler, *Numerically solving polynomial systems with Bertini*, vol. 25 of Software, Environments, and Tools, Society for Industrial and Applied Mathematics, Philadelphia, PA, 2013.

[3] I. A. Berchenko (Kogan) and P. J. Olver, *Symmetries of polynomials*, Journal of Symbolic Computations, 29 (2000), pp. 485–514.

[4] M. Boutin, *Numerically invariant signature curves*, Int. J. Computer vision, 40 (2000), pp. 235–248.

[5] J. M. Burdis, I. A. Kogan, and H. Hong, *Object-image correspondence for algebraic curves under projections*, SIGMA Symmetry Integrability Geom. Methods Appl., 9 (2013), pp. Paper 023, 31.

[6] E. Calabi, P. J. Olver, C. Shakiban, A. Tannenbaum, and S. Haker, *Differential and numerically invariant signatures curves applied to object recognition*, Int. J. Computer vision, 26 (1998), pp. Paper 107,135.

[7] E. Cartan, *La méthode du repère mobile, la théorie des groupes continus, et les espaces généralisés*, vol. 5 of Exposés de Géométrie, Hermann, Paris, 1935.

[8] E. Cartan, *Les problèmes d'équivalence*, Oeuvres completes, Part II, volume 2, pp. 1311-1334, Gauthier-Villars, Paris, 1953.

[9] H. Derksen and G. Kemper, *Computational invariant theory*, vol. 130 of Encyclopaedia of Mathematical Sciences, Springer, Heidelberg, enlarged ed., 2015. With two appendices by Vladimir L. Popov, and an addendum by Norbert A'Campo and Popov, Invariant Theory and Algebraic Transformation Groups, VIII.

[10] O. Faugeras, *Cartan's moving frame method and its application to the geometry and evolution of curves in the Euclidean, affine and projective planes*, Application of Invariance in Computer Vision, J.L Mundy, A. Zisserman, D. Forsyth (eds.) Springer-Verlag Lecture Notes in Computer Science, 825 (1994), pp. 11–46.

[11] O. Faugeras, Q.T. Luong, *The geometry of multiple images. The laws that govern the formation of multiple images of a scene and some of their applications*, MIT Press, Cambridge, MA, 2001.

[12] M. Fels and P. J. Olver, *Moving Coframes. II. Regularization and Theoretical Foundations*, Acta Appl. Math., 55 (1999), pp. 127–208.

[13] G. Fischer, *Plane algebraic curves*, vol. 15 of Student Mathematical Library, American Mathematical Society, Providence, RI, 2001. Translated from the 1994 German original by Leslie Kay.

[14] W. Fulton, *Algebraic curves*, Advanced Book Classics, Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[15] J. H. Grace and A. Young, *The Algebra of Invariants*, Cambridge Univ. Press, Cambridge, 1903.

[16] A. Grim and C. Shakiban, *Applications of signature curves to characterize melanomas and moles*, in Applications of computer algebra, vol. 198 of Springer Proc. Math. Stat., Springer, Cham, 2017, pp. 171–189.

[17] A. Grim, T. O'Connor, P. J. Olver, C. Shakiban, R. Slechta, and R. Thompson, *Automatic Reassembly of Three-Dimensional Jigsaw Puzzles*, in Int. J. of Image and Graphics, vol. 16, 2016, no. 2

[18] G. Gün Polat and P. J. Olver, *Joint differential invariants of binary and ternary forms*, Portugaliae Math., (2019), to appear, `http://www-users.math.umn.edu/~olver/a_/ternary.pdf`.

[19] G. Gurevich, *Foundations of the theory of algebraic invariants*, Noordhoff, 1964.

[20] J. Harris, *Algebraic geometry*, vol. 133 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[21] J. Harris and I. Morrison, *Moduli of Curves*, Springer Verlag (1998).

[22] R. Hartley R. and A. Zisserman, *Multiple view geometry in computer vision*, Cambridge University Press, Cambridge, 2001.

[23] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[24] M. S. Hickman, *Euclidean signature curves*, J. Math. Imaging Vision, 43 (2012), pp. 206–213.

[25] D. J. Hoff and P. J. Olver, *Extensions of invariant signatures for object recognition*, J. Math. Imaging Vision, 45 (2013), pp. 176–185.

[26] D. J. Hoff and P. J. Olver, *Automatic solution of jigsaw puzzles*, J. Math. Imaging Vision, 49 (2014), pp. 234–250.

[27] E. Hubert and I. A. Kogan, *Rational invariants of an algebraic group action: Construction and rewriting*, Journal of Symbolic Computations, 42 (2007), pp. 203–217.

[28] E. Hubert and I. A. Kogan, *Smooth and algebraic invariants of a group action: local and global construction.*, Foundation of Computational Math. J., 7:4 (2007), pp. 345–383.

[29] T. W. Hungerford, *Algbera*, vol. 73 of Graduate Texts in Mathematics, Springer-Verlang, New York-Berlin, 1980.

[30] E. L. Ince, *Ordinary Differential Equations*, Dover Publications, New York, 1944.

[31] I. A. Kogan, *Inductive Approach to Cartan's Moving Frames Method with Applications to Classical Invariant Theory*, PhD thesis, University of Minnesota, 2000, `https://iakogan.math.ncsu.edu/papers/thesisKogan.pdf`.

[32] I. A. Kogan, *Two algorithms for a moving frame construction*, Canad. J. Math., 55 (2003), pp. 266–291.

[33] I. A. Kogan, M. G. Ruddy, and C. Vinzant, *Supplementary materials for "Differential Signature of Algebraic Curves" paper*. `https://mgruddy.wixsite.com/home/dsag-supplementarymaterials`, 2019.

[34] B. Kruglikov and V. Lychagin, *Global Lie–Tresse theorem*, Selecta Mathematica, 22:3 (2016), pp. 1357–1411.

[35] S. Lie, *Vorlesungen über continuierliche Gruppen mit Geometrischen und anderen Anwendungen*, Chelsea Publishing Co., Bronx, N.Y., 1971. Bearbeitet und herausgegeben von Georg Scheffers, Nachdruck der Auflage des Jahres 1893.

[36] E. Musso and L. Nicolodi, *Invariant signatures of closed planar curves*, J. Math. Imaging Vision, 35 (2009), pp. 68–85.

[37] P. J. Olver, *Applications of Lie groups to differential equations*, Springer, second-ed., 1993.

[38] P. J. Olver, *Equivalence, invariants and Symmetry*, Cambridge University Press, 1995.

[39] P. J. Olver, *Classical invariant theory*, vol. 44 of London Mathematical Society Student Texts, Cambridge University Press, Cambridge, 1999.

[40] P. J. Olver, *Moving frames and singularities of prolonged group actions*, Selecta Math. (N.S.), 6 (2000), pp. 41–77.

[41] L. V. Ovsiannikov, *Group analysis of differential equations*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1982. Translated from the Russian by Y. Chapovsky, Translation edited by William F. Ames.

[42] M. Ruddy, *The Equivalence Problem and Signatures of Algebraic Curves*, PhD thesis, North Carolina State University, 2019, `http://www.lib.ncsu.edu/resolver/1840.20/36673`.

[43] A. N. Parshin and I. R. Shafarevich, eds., *Algebraic geometry. IV*, vol. 55 of Encyclopaedia of Mathematical Sciences, Springer-Verlag, Berlin, 1994.

[44] I. R. Shafarevich, eds., *Algebraic geometry. I*, vol. 23 of Encyclopaedia of Mathematical Sciences, Springer-Verlag, Berlin, 1994.

[45] I. R. Shafarevich, *Basic algebraic geometry. 1*, Springer, Heidelberg, third ed., 2013. Varieties in projective space.

[46] M. Shin, L. Tsap, and D. Goldgof, *Gesture recognition using Bezier curves for visualization navigation from registered 3-D data*, Pattern Recognition, 37 (2004), pp. 1011–1024.

[47] V. V. Shokurov, *Riemann surfaces and algebraic curves*, in Shafarevich [44], pp. 1–166.

[48] T. A. Springer, *Linear algebraic groups*, in Parshin and Shafarevich [43], pp. 1–121.

[49] P. Tzermias, *The group of automorphisms of the Fermat curve*, J. Number Theory, 53 (1995), pp. 173–178.

[50] V. L. Popov and E. B. Vinberg, *Invariant theory*, in Parshin and Shafarevich [43], pp. 122–278.

[51] T. Wears, *Signature Varieties of Polynomial Functions.*, PhD thesis, North Carolina State University, 2011, `http://www.lib.ncsu.edu/resolver/1840.16/7336`.