Numerical equality tests for rational maps and signatures of curves

Tim Duff
tduff3@gatech.edu
School of Mathematics, Georgia Tech
Atlanta, Georgia, USA

Michael Ruddy
michael.ruddy@mis.mpg.de
Max Planck Institute for Mathematics in the Sciences
Leipzig, Germany

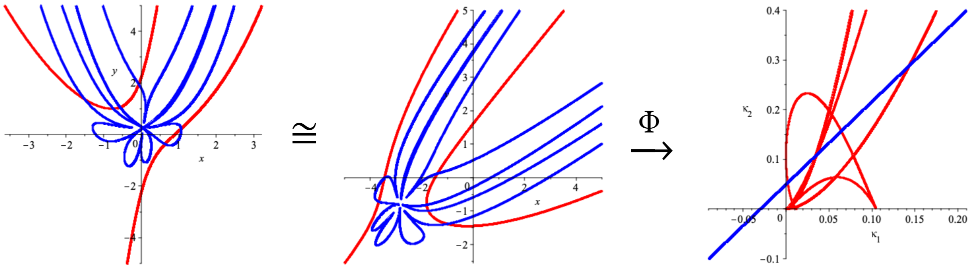

Figure 1: Two curves and their signature in red. A line and its pullback in blue. Made with Maple [33].

ABSTRACT

We apply numerical algebraic geometry to the invariant-theoretic problem of detecting symmetries between two plane algebraic curves. We describe an efficient equality test which determines, with "probability-one", whether or not two rational maps have the same image up to Zariski closure. The application to invariant theory is based on the construction of suitable signature maps associated to a group acting linearly on the respective curves. We consider two versions of this construction: differential and joint signature maps. In our examples and computational experiments, we focus on the complex Euclidean group, and introduce an algebraic joint signature that we prove determines equivalence of curves under this action. We demonstrate that the test is efficient and use it to empirically compare the sensitivity of differential and joint signatures to noise.

KEYWORDS

differential invariants, invariant theory, numerical algebraic geometry, polynomial systems, Euclidean group, computer algebra, homotopy continuation

ACM Reference Format:

Tim Duff and Michael Ruddy. 2020. Numerical equality tests for rational maps and signatures of curves. In *Proceedings of ISSAC '20: ACM International Symposium on Symbolic and Algebraic Computation (ISSAC '20)*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/1122445.1122456

ISSAC '20, July 20–23, 2020, Kalamata, Greece
© 2020 Association for Computing Machinery.
ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

This paper studies two related problems.

Problem 1. Given two irreducible algebraic varieties, $X_0 \subset \mathbb{C}^{n_0}$ and $X_1 \subset \mathbb{C}^{n_1}$, and two rational maps, $\Phi_0 : X_0 \dashrightarrow \mathbb{C}^m$ and $\Phi_1 : X_1 \dashrightarrow \mathbb{C}^m$, decide if $\overline{\operatorname{im}\Phi_0} = \overline{\operatorname{im}\Phi_1}$.

Problem 2. Given an infinite algebraic group $G \subset \mathcal{PGL}_3(\mathbb{C})$ acting linearly on $\mathbb{C}^2$ and two plane algebraic curves $C_0, C_1 \subset \mathbb{C}^2$, decide if there exists $g \in G$ such that $C_0 = \overline{g \cdot C_1}$.

In the context of *differential invariant theory*, we can reduce Problem 2 to Problem 1 by constructing a suitable *signature map* for the action of G on the curves C_1, C_2. For Problem 1, the field of *numerical algebraic geometry* furnishes a suite of "probability-one" tests. In this article, we explain the aforementioned approaches to these problems in detail and demonstrate that they yield practical *equality tests* for both problems.

In Problem 1, $\overline{\operatorname{im}\Phi_i}$ denotes the Zariski closure of the image of Φ_i. We do not address the more delicate problem of deciding equality of the constructible sets $\operatorname{im}\Phi_i$, which may be addressed by either of the symbolic methods considered in [10, 19].

A formally correct algorithmic solution to Problem 1 clearly depends on how the input is "given" to us and what type of guarantee we seek. A natural route via symbolic computation is to compute the ideal of implicit equations for each map and check if these ideals are equal. This is a standard application of Gröbner bases [7, 13]. Resultants and more specialized techniques may provide useful alternatives [9, 12, 27, 42].

Our approach to Problem 1 via numerical algebraic geometry is in the same spirit as previous works [11, 23, 24], where the cost of implicitization is replaced by the cost of computing certain *witness sets*. A key feature of our approach is that it requires a pre-computed witness set for only one of the maps, say Φ_1. This feature is motivated mainly by our interest in Problem 2. We view computing a witness set for Φ_1 as an *offline* cost. The *online* cost of testing equality via Algorithm 1 is typically negligible by comparison. This is advantageous in a scenario where we wish to test Φ_1 against many different choices of Φ_0.

To reduce Problem 2 to Problem 1, one may use the maps obtained by restricting a pair of independent, rational differential invariants for G to C_0 and C_1 [28], which can be explicitly constructed via the Fels-Olver moving frame method [16] or its algebraic formulation [26]. The image of an algebraic curve C under this map is the curve's *differential signature.* In greater generality, differential signatures may be constructed for smooth submanifolds of some ambient space equipped with a Lie group action. The differential signature locally characterizes the manifold's equivalence class under the action, meaning that manifolds with the same signature are locally equivalent under the Lie group [16]. For an algebraic group acting on $\mathbb{C}^2$ and a plane curve $C \subset \mathbb{C}^2$, such a construction yields a rational map $\Phi : \mathbb{C}^2 \dashrightarrow \mathbb{C}^2$, referred to as the curve's differential signature map. In this special case, local equivalence implies global equivalence.

Example 1.1. In Figure 1, the red curve on left depicts real points (x, y) such that $8x^3 - 20xy + 2y^2 + 5x - 10 = 0$. Applying a real rotation and translation yields the curve in the middle. Thus these curves are equivalent under the linear action of the complex Euclidean group $\mathcal{E}_2(\mathbb{C})$. The closed image of their respective differential signature maps is the red curve of degree 48 depicted on the right.

Differential signatures of curves have been successfully applied to object recognition under noise, with applications ranging from jigsaw puzzle reconstruction [25] to medical imaging [18]. Differential signatures have also been used to solve classical invariant theory problems such as determining equivalence of binary and ternary forms [4, 29, 38]. The setting of algebraic curves is a useful testing ground for algorithms in this subject. In [8] the notion of a signature polynomial was introduced to determine equivalence of plane algebraic curves via implicitization methods. In [28] it is shown that this reduction to implicitization can always be done for any group acting as in Problem 2.

In this paper we show that the numerical algorithm for Problem 1 yields an effective way for solving Problem 2 using differential signatures, even when implicitization is not practically feasible. We also consider *joint signatures*, which are obtained by constructing rational maps using joint invariants of the induced action of G on the product $\mathbb{C}^2 \times \ldots \times \mathbb{C}^2$ [39]. While we focus on plane curves, in principle the numerical equality test can be used to determine equivalence of higher dimensional varieties through differential or joint signatures, provided one can find a suitable set of *rational* differential or joint invariants.

In Section 2, we review notions from numerical algebraic geometry and describe a general solution to Problem 1 (Algorithm 1.) Section 3 considers the signature approach to Problem 2. In 3.1 we follow the construction in [8, 28] to describe a differential signature for plane algebraic curves using a *classifying pair* of differential invariants. In 3.2 we describe how joint signatures can be used to determine equivalence of plane curves using lower order differential invariant functions, with a detailed analysis in the case of the complex Euclidean group $\mathcal{E}_2(\mathbb{C})$. In Section 4, we describe an implementation in Macaulay2 [17], which has been successful for studying both classes of maps on curves of degree up to 10. Our (reproducible) experiments show that offline witness computation for plane curves of various degrees is feasible, that the online equality test gives a fast alternative to symbolic methods, and that the numerical approach is robust in a certain regime of noise.[1]

2 NUMERICAL EQUALITY

2.1 Background

In this subsection we fix notation and terminology related to algebraic varieties and witness sets. A more comprehensive overview of numerical algebraic geometry may be found in the survey [44] or books [3, 45]. A general system of polynomial equations is denoted by a c-tuple $f = (f_1, \ldots, f_c)$ for $f_1, \ldots, f_c \in \mathbb{C}[x_1, \ldots, x_n]$. Where convenient, we may identify f with a map $\mathbb{C}^n \to \mathbb{C}^c$. The vanishing locus $V(f) := \{x \in \mathbb{C}^n \mid f_1(x) = \cdots = f_c(x) = 0\}$ is a closed subvariety of $\mathbb{C}^n$. If c is the codimension of $V(f)$, then f is said to be a *regular sequence* and the variety $V(f)$ is a *complete intersection.* For polynomial systems $f = (f_1, \ldots, f_k)$ and $g = (g_1, \ldots, g_{k'})$ we write $(f \mid g) := (f_1, \ldots, f_k, g_1, \ldots, g_{k'})$, yielding a polynomial system whose vanishing locus is $V(f) \cap V(g)$. We let $\mathcal{I}_X$ denote the radical ideal of polynomials vanishing on a closed subvariety $X \subset \mathbb{C}^n$. A property is said to hold generically on an irreducible variety X if it holds on some Zariski-open $U \subset X$.

Part of the input to Algorithm 1 is an irreducible variety X, represented via an unspecified sampling oracle and equations f defining a complete intersection $V(f) \supset X$ such that X and $V(f)$ both have codimension c. Since this description is essentially set-theoretic, we should treat the possibility that $\langle f_1, \ldots, f_c \rangle \subsetneq \mathcal{I}_{V(f)}$ with some care. We say that f is *generically reduced* along X if there exists a point $x \in X$ such that the tangent space $T_x(f) = \ker\left(df_i/dx_j\right)$ has dimension $n - c$.

The main data structures in numerical algebraic geometry are variations on the notion of a *witness set.* The overarching idea is to represent an irreducible variety $X \subset \mathbb{C}^n$ by its intersection with a generic affine linear subspace of complimentary dimension. The number of points in such an intersection is the degree $\deg X$, i.e. the degree of the projective closure of X under the usual embedding $\mathbb{C}^n \ni (x_1, \ldots, x_n) \mapsto [x_1 : \cdots : x_n : 1] \in \mathbb{P}(\mathbb{C}^{n+1})$.

We define a c-slice in $\mathbb{C}^n$ to be a polynomial system consisting of c affine hyperplanes, $L = (l_1, \ldots, l_c)$ with $l_i \in \mathbb{C}[x_1, \ldots, x_n]_{\le 1}$. For convenience we write L in place of $V(L(x))$ and also use the notation L^c. For X an irreducible variety of codimension c and a generic slice L^c, the intersection $X \cap L^c$ is *transverse*, consisting of $\deg X$ isolated, nonsingular points [36, Thm 5.1].

The standard definition of a witness set for a variety assumes that defining equations for the variety of interest are known. A more flexible notion is that of a *pseudo-witness set* for a rational map. This was first studied for linear projections in [23]. Our Definition 2.1 differs from that used in [3, 23, 24]; to distinguish our setup, we provisionally use the term *weak pseudowitness set.*

Definition 2.1. Let $V(f) \subset \mathbb{C}^n$ be a variety, $X \subset V(f)$ be one of its irreducible components, and $\Phi : X \dashrightarrow \mathbb{C}^m$ be a rational map. Set $c = \operatorname{codim} V(f)$, $d = \dim \overline{\operatorname{im} \Phi}$. A weak pseudowitness set for Φ is a quadruple $(f, \Phi, (L|L'), \{w_1, \ldots, w_e\})$, where L is a generic affine

[1] Obtain the code at https://github.com/timduff35/NumericalSignatures.

$(m-d)$-slice of $\overline{\operatorname{im}\Phi}$, L' is a generic affine $(c-m+d)$-slice of X, and such that $w_1,\dots,w_e$ are points in $X\cap L'$ where Φ is defined such that $\overline{\operatorname{im}\Phi}\cap L=\{\Phi(w_1),\dots,\Phi(w_e)\}$ and $e=\deg\overline{\operatorname{im}\Phi}$.

"Weak" means $\{w_1,\dots,w_e\}\subset L'\cap\Phi^{-1}\left(\overline{\operatorname{im}\Phi}\cap L\right)$ may be a proper containment, i.e. when Φ has degree greater than 1. This is preferable for us since fewer points need to be stored. The data in Definition 2.1 are already sufficient for testing queries of the form $y\in\overline{\operatorname{im}\Phi}$, as noted in [23, Remark 2] and related applications [6, 11]. For a membership tests of the form $y\in\operatorname{im}\Phi$ and other applications, the stronger notion is required [24].

In our context, equations defining $\overline{\operatorname{im}\Phi}$ are seldom known, so in what follows we may informally refer to the objects of Definition 2.1 and their multiprojective counterparts in Definition 2.2 as "witness sets" without ambiguity. In practice, we can at best hope that our numerical approximations to points $w_1,\dots,w_e$ lie sufficiently close to $\overline{\operatorname{im}\Phi}\cap L$: to clearly distinguish practice from theory, we occasionally use the term *numerical (weak / pseudo) witness set.*

Witness sets for an irreducible $X\subset\mathbb{C}^n$ reflect the algebraic geometry of the projective closure $\overline{X}\subset\mathbb{P}(\mathbb{C}^{n+1})$. It is also interesting to consider instead the closure of X embedded in some product of projective spaces [21, 22, 32]. To do so, we fix $(n_1,\dots,n_k)$, an integer partition of n, and consider X in the affine space $\mathbb{C}^{n_1}\times\cdots\times\mathbb{C}^{n_k}$. We consider slices $L^{\boldsymbol{e}}=L^{e_1}|\cdots|L^{e_k}$, where $\boldsymbol{e}=(e_1,\dots,e_k)\in\mathbb{N}^k$ is an integral vector such that $e_1+\cdots e_k=\dim X$, and L^{e_j} is a e_j-slice consisting of e_j affine hyperplanes in the coordinates of $\mathbb{C}^{n_j}$. We say that $\boldsymbol{e}$ is a *multidimension* of X if for generic $L^{\boldsymbol{e}}$ the intersection $X\cap L^{\boldsymbol{e}}$ is a finite set of nonsingular points; the number of points for such $L^{\boldsymbol{e}}$ is a constant called the $\boldsymbol{e}$*-multidegree* $\deg_{\boldsymbol{e}}X$. These definitions reflect the geometry of the *multiprojective closure* of X under the map

$$X\ni(x_1,\dots,x_n)\mapsto\Big([x_1:\cdots:x_{n_1}:1],\dots.$$

$$[x_{n-n_k+1}:\cdots:x_n:1]\Big)\in\mathbb{P}(\mathbb{C}^{n_1+1})\times\cdots\times\mathbb{P}(\mathbb{C}^{n_k+1}),$$

Following [22], we give a multiprojective generalization of Definition 2.1.

Definition 2.2. Let f,X,c,L',Φ be as in 2.1, and $\boldsymbol{e}$ be a multidimension of $\overline{\operatorname{im}\Phi}$ corresponding to some partition of n. An $\boldsymbol{e}$-weak pseudowitness set for Φ consists of $\left(f,\Phi,(L^{\boldsymbol{e}}|L'),\{w_1,\dots,w_e\}\right)$, such that $\overline{\operatorname{im}\Phi}\cap L^{\boldsymbol{e}}=\{\Phi(w_1),\dots,\Phi(w_e)\}$ and $e=\deg_{\boldsymbol{e}}\overline{\operatorname{im}\Phi}$.

The general membership test for multiprojective varieties proposed in [22] uses the stronger notion of a witness collection. This is required since for an arbitrary point $x\in X$ there may not exist transverse slices $L^{\boldsymbol{e}}\ni x$ for $\boldsymbol{e}$ ranging over all multidimensions of X—see [22, Example 3.1]. This subtlety is not encountered for generic $x\in X$; we record this basic fact in Proposition 2.3.

Proposition 2.3. *Fix irreducible* $X\subset\mathbb{C}^{n_1}\times\cdots\times\cdots\mathbb{C}^{n_k}$ *and* $\boldsymbol{e}$ *some multi-dimension of* X*. For* $x=(x_1,\cdots,x_k)\in X$ *generic, there exists an* $\boldsymbol{e}$*-slice* $L^{\boldsymbol{e}}\ni x$ *such that* $\dim(X\cap L^{\boldsymbol{e}})=0$*. Moreover, for* $x\notin X_{sing}$*, we also have that* $x\notin(X\cap L^{\boldsymbol{e}})_{sing}$ *for generic* $L^{\boldsymbol{e}}$*.*

Proof. For generic x_1 in the image of $\pi_1:X\to\mathbb{C}^{n_1}$ we have that the fiber $\pi_1^{-1}(x_1)$ has dimension $\dim X-\dim\pi_1(X)$. Choose such an x_1 and let $L^{e_1}\ni x_1$ be generic so that $\pi_1(X)\cap L^{e_1}$ has dimension $\dim\pi_1(X)-e_1$. It follows that $\dim(X\cap L^{e_1})$ has dimension $\dim X-e_1$. This construction holds for all x_1 on some Zariski open $U_1\subset\pi_1(X)$. Repeating this construction for the remaining factors yields $U_2,\dots,U_k$ such that the first part holds for all $x\in U_1\times\cdots\times U_k$. The second part follows from the appropriate Bertini theorem, cf. [20, Thm 17.16] □

2.2 A general equality test

Now let $\Phi_0:X_0\dashrightarrow\mathbb{C}^m$ and $\Phi_1:X_1\dashrightarrow\mathbb{C}^m$ denote two rational maps with each $X_i\subset\mathbb{C}^{n_i}$ of codimension c_i. Problem 1 from the introduction asks us to decide whether or not their images are equal up to Zariski closure. A probabilistic procedure is given in Algorithm 1. This equality test refines general membership and equality tests from numerical algebraic geometry, which are summarized in [45, Ch. 13, 15] and [3, Ch. 8,16]. Our setup is motivated by an efficient solution to Problem 2. Following the standard terminology, our test correctly decides equality with "probability-one" in an idealized model of computation. This is the content of Theorem 2.1. Standard disclaimers apply, since any implementation must rely on numerical approximations in floating-point. The actual success rate depends on the typical conditioning of various subproblems, the amount of precision used, implementation-specific evaluation and approximation schemes, and many other factors.

Algorithm 1 assumes different representations for the two maps. The map Φ_1 is represented by a witness set in the sense the sense of Definition 2.1, say $(f_1,\Phi_1,(L_1|L_1'),\{w_1,\dots,w_e\})$. In fact, the only data needed by Algorithm 1 are the map itself Φ_1, the slice L_1, and the points $w_1,\dots,w_e$. For the map Φ_0, we need a sampling oracle and generically reduced equations vanishing on its domain. Despite being technical, these assumptions may be relevant in situations where we can sample from X_0 (eg. via a parametrization) but the ideal $\mathcal{I}_{X_0}$ is unknown. We sketch the multiprojective generalization of Algorithm 1 at the end of the section.

Suppose $\dim\overline{\operatorname{im}\Phi_0}=\dim\overline{\operatorname{im}\Phi_1}=d$. There is a probabilistic membership test for queries of the form $\Phi_0(x_0)\in\overline{\operatorname{im}\Phi_1}$ based on homotopy continuation. The relevant homotopy depends parametrically on L_1, a $(m-d)$-slice $L_0\ni\Phi_0(x_0)$, a (c_0-m+d)-slice $L_0'\ni x_0$, and a regular sequence $f_0=(f_{0,1},\dots,f_{0,c_0})$ which is generically reduced with respect to X_0. The homotopy H is defined as

$$H(x;t)=\Big(f_0\,\Big|L_0'\Big|\,t\,L_1\circ\Phi_0+(1-t)\,L_0\circ\Phi_0\Big)(x).\tag{1}$$

In simple terms, H moves a slice through $\Phi_0(x_0)$ to the slice witnessing $\overline{\operatorname{im}\Phi_1}$ as t goes from 0 to 1. A solution curve associated to (1) is a smooth map $x:[0,1]\to\mathbb{C}^n$ such that $H(x(t),t)=0$ for all t. For generic parameters L_0,L_1,L_0' the Jacobian $H_x(x,t)$ is invertible for all $t\in[0,1]$, solution curves satisfy the ODE

$$x'(t)=-H_x(x,t)^{-1}H_t(x,t),$$

and each of the points $w_1,\dots,w_e$ is the endpoint of some solution curve x with $x(0)\in X\cap L_0'$. These statements follow from more general results on *coefficient-parameter homotopy*, as presented in [35] or [45, Thm 7.1.1]. We assume a subroutine TRACK(H,x_0) which returns $x(1)$ for the solution curve based at x_0. In practice, the curve $x(t)$ is approximated by numerical predictor/corrector methods [1, 34]. We allow our TRACK routine to fail; this will occur, for instance, when $\Phi_0(x_0)$ is a singular point on $\overline{\operatorname{im}\Phi_0}$. However, it

Algorithm 1. Probability-1 equality test

Input: Let $X_0 \subset \mathbb{C}^{n_0}, X_1 \subset \mathbb{C}^{n_1}$ be irreducible algebraic varieties, and $\Phi_0 : X_0 \to \mathbb{C}^m$, $\Phi_1 : X_1 \to \mathbb{C}^m$ be rational maps, represented via the following ingredients:

1) $(L_1, \{w_1, \dots, w_e\})$ with $\overline{\operatorname{im}\Phi_1} \cap L_1 = \{\Phi_1(w_1), \dots, \Phi_e(w_e)\}$ and $e = \deg \overline{\operatorname{im}\Phi_1}$ (cf. Definition 2.1),
2) $f_{0,1}, \dots, f_{0,c_0} \in \mathbb{C}[x_1, \dots, x_{n_0}]$: a generically reduced regular sequence such that $\operatorname{codim}(X_0) = c_0$ and $X_0 \subset V(f_1, \dots, f_{c_0})$,
3) an oracle for sampling a point $x_0 \in X_0$, and
4) explicit rational functions representing each map Φ_i.

Output: YES if $\overline{\operatorname{im}\Phi_0} = \overline{\operatorname{im}\Phi_1}$ and NO if $\overline{\operatorname{im}\Phi_0} \neq \overline{\operatorname{im}\Phi_1}$.

```
1: sample $x_0 \in X_0$
2: $T_{x_0}(f) \leftarrow \ker (D f)_{x_0}$
3: $d \leftarrow \operatorname{rank} (D \Phi_0)_{x_0}\big|_{T_{x_0}(f)}$
4: if $d \neq \dim \overline{\operatorname{im}\Phi_1}$ then return NO
5: $H(x; t) \leftarrow$ the homotopy from equation 1
6: $x_1 \leftarrow$ TRACK $(H, x_0)$
7: if $\Phi_0(x_1) \in \{\Phi_1(w_1), \dots, \Phi_1(w_e)\}$ return YES
       else return NO
```

will succeed for generic (and hence *almost all*) choices of parameters and $x_0 \in \mathbb{C}^{n_0}$. Algorithm 1 exploits this fact.

Theorem 2.1. *For generic x_0, L_0, L_0', L_1, Algorithm 1 correctly decides if $\overline{\operatorname{im}\Phi_0} = \overline{\operatorname{im}\Phi_1}$.*

Remark 2.4. To apply the coefficient-parameter theory to the homotopy H, the set of "nongeneric" L_1 must depend on Φ_0 as well as Φ_1; for fixed (Φ_1, L_1), a malicious adversary could cook up Φ_0 with $\dim \overline{\operatorname{im}\Phi_0} = \dim \overline{\operatorname{im}\Phi_1}$ and $\dim(\overline{\operatorname{im}\Phi_0} \cap L_1) > 0$. In this case, we assume Algorithm 1 fails at line 6. We could also use a homotopy similar to H to compute a new witness set for Φ_1 beforehand.

Proof. Since x_0 is generic and f_0 is generically reduced, we may assume that that $d = \dim \overline{\operatorname{im}\Phi_0}$. Noting line 4, we are done unless $d = \dim \overline{\operatorname{im}\Phi_1}$. In this case, since the $\overline{\operatorname{im}\Phi_i}$ are irreducible,

$$\dim\left(\overline{\operatorname{im}\Phi_0} \cap \overline{\operatorname{im}\Phi_1}\right) = d \quad \Leftrightarrow \quad \overline{\operatorname{im}\Phi_0} = \overline{\operatorname{im}\Phi_1}. \tag{2}$$

As previously mentioned, generic slices give that the solution curve $x(t)$ associated to 1 with initial value x_0 exists and satisfies $x(t) \in V(f) \setminus V(f)_{\text{sing}}$ for all $t \in [0, 1]$. The endpoint x_1 is, *a priori*, a point of $V(f)$. Since $X_0 \setminus (X_0)_{\text{sing}}$ is a connected component of $V(f) \setminus V(f)_{\text{sing}}$ in the complex topology [43, Ch. 7, Sec. 2, Thm 2] and $x_0 \in X_0$, so also must $x_1 \in X_0$. Hence $\Phi_0(x_1) \in \overline{\operatorname{im}\Phi_0} \cap L_1$. Now if $\overline{\operatorname{im}\Phi_0} = \overline{\operatorname{im}\Phi_1}$, then clearly we must have

$$\Phi_0(x_1) \in \overline{\operatorname{im}\Phi_1} \cap L_1 = \{\Phi_1(w_1), \dots, \Phi_1(w_e)\}, \tag{3}$$

as is tested on line 7. Conversely, if (3) holds, then

$$\dim(\overline{\operatorname{im}\Phi_0} \cap \overline{\operatorname{im}\Phi_1} \cap L_1) \geq 0,$$

which by (2) and the genericity of L_1 implies $\overline{\operatorname{im}\Phi_0} = \overline{\operatorname{im}\Phi_1}$. □

We close by explaining how to extend Algorithm 1 to the case where Φ_1 is represented by a multiprojective witness set in multidimension $\boldsymbol{e}$ (cf. Definition 2.2.) We keep the same notation, defining the homotopy H in terms of the appropriate slices. If the $\overline{\operatorname{im}\Phi_i}$ are equal then $\boldsymbol{e}$ is also a multidimension of Φ_0. By proposition 2.3 and genericity of $\Phi_0(x_0)$, it suffices to check that $H_x(x_0, 0)$ is invertible. The rest of the argument is the same as for Theorem 2.1.

3 SIGNATURES OF CURVES

3.1 Differential signatures

In what follows, all plane curves are complex algebraic, irreducible, and of degree greater than one. Let $G \subset \mathcal{PGL}_3(\mathbb{C})$ be an infinite algebraic group acting linearly on $\mathbb{C}^2$ with action $g \cdot (x, y) = (\overline{x}, \overline{y})$.

Definition 3.1. Two curves C_0, C_1 are said to be *G-equivalent*, denoted $C_0 \cong_G C_1$, if there exists a $g \in G$ such that $C_0 = \overline{g \cdot C_1}$.

A differential signature that determines G-equivalence of curves can be constructed from a set of classifying invariants (Definition 3.6.) We let J^n denote the nth order jet space, a complex vector space of dimension $(n + 2)$ with coordinates $(x, y, y^{(1)}, \dots, y^{(n)})$. Letting $\Omega(J^n)$ denote the set of complex-differentiable functions from J^n to $\mathbb{C}$, the *total derivative operator* $\frac{d}{dx} : \Omega(J^n) \to \Omega(J^{n+1})$ is the unique $\mathbb{C}$-linear map satisfying the product rule and the relations $\frac{d}{dx}(x) = 1$, $\frac{d}{dx}(y^{(k)}) = y^{(k+1)}$ for $k \geq 0$ (cf. [37, Ch. 7].)

The *prolonged* action of G on J^n is given by

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

where

$$\overline{y}^{(1)} = \frac{\frac{d}{dx}\left[\overline{y}(g, x, y)\right]}{\frac{d}{dx}\left[\overline{x}(g, x, y)\right]},$$

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

Definition 3.2. A *differential invariant* for the action of G is a function on J^n that is invariant under the prolonged action of G on J^n. The *order* of a differential invariant is the maximum k such that the function depends explicitly on $y^{(k)}$.

Definition 3.3. The *n-th jet* of an algebraic curve C is the image of the map $j_C^n : C \dashrightarrow J^n$ given (where defined) by

$$(x, y) \mapsto (x, y, y_C^{(1)}(x, y), y_C^{(2)}(x, y), \dots, y_C^{(n)}(x, y)),$$

where $y_C^{(k)}(x, y)$ is the k-th derivative of y with respect to x at the point $(x, y) \in C$.

The prolonged action of G is defined such that

$$g \cdot j_C^n(C) = j_{g \cdot C}^n(g \cdot C).$$

Definition 3.4. The *restriction* of a differential invariant K of order n to a curve C is the map $K|_C : C \dashrightarrow \mathbb{C}^2$ given by $K|_C = K \circ j_C^n$.

The coordinates of the n-th jet map j_n^C are rational functions of x and y that can be computed via implicit differentiation. For example, letting $\mathcal{I}_C = \langle F \rangle$, we have

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

Thus if K is a *rational* differential invariant of order n, meaning it is a rational function in the coordinates of J^n, then $K|_C$ is a rational function in x and y.

Definition 3.5. We say that a set of differential invariants $\mathcal{I}$ *separates orbits* for the prolonged action on a nonempty Zariski-open $W \subset J^n$ if, for all $p, q, \in W$,

$$K(p) = K(q) \ \forall K \in \mathcal{I} \quad \Leftrightarrow \quad \exists g \in G \text{ such that } p = g \cdot q.$$

Definition 3.6. Let an r-dimensional algebraic group G act on $\mathbb{C}^2$. A pair of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$ is said to be *classifying* if K_1 separates orbits on $U_k \subset J^k$ for some $k < r$ and $\mathcal{I}$ separates orbits on $U_r \subset J^r$.

For a particular action of G, such a pair of classifying invariants always exists, and one can explicitly construct a pair by computing generators for the field of rational invariants for the prolonged action of G [28, Thm 2.20], using algorithms such as those found in [14] and [26]. It should be noted that $\mathcal{I}$ is not unique, and different choices can lead to different differential signatures.

Definition 3.7. For a pair of classifying invariants $\mathcal{I} = \{K_1, K_2\}$, an algebraic curve C is said to be *non-exceptional* if all but finitely many points on $p \in C$ satisfy

$$j^k_C(p) \in U_k, \ j^r_C(p) \in U_r, \ \text{ and } \frac{\partial K_1}{\partial y^k}, \frac{\partial K_2}{\partial y^r} \neq 0 \text{ at } j^r_C(p).$$

A generic curve of degree d where $\binom{d+2}{2} - 2 \geq r$ is non-exceptional with respect to a given classifying set [28, Thm 2.27].

Definition 3.8. Let $\mathcal{I} = \{K_1, K_2\}$ be a pair of classifying invariants for the action of G on $\mathbb{C}^2$ and C a non-exceptional algebraic curve with respect to $\mathcal{I}$. Then the image of C under the map

$$(K_1|_C, K_2|_C) : C \dashrightarrow \mathbb{C}^2$$

is the *differential signature* of C and is denoted $\mathcal{S}_C$.

The following appears as Theorem 2.37 in [28].

Theorem 3.9. *If algebraic curves C_0, C_1 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 $\mathbb{C}^2$ then*

$$C_0 \cong_G C_1 \quad \Leftrightarrow \quad \overline{\mathcal{S}_{C_0}} = \overline{\mathcal{S}_{C_1}}.$$

Example 3.10. Consider the action of the Euclidean group $\mathcal{E}_2$ of complex translations, rotations, and reflections on $\mathbb{C}^2$ where the action of $g \in \mathcal{E}_2(\mathbb{C})$ is given by

$$g \cdot (x, y) = (cx+sy+a, -sx+cy+b) \text{ or } g \cdot (x, y) = (-cx+sy+a, sx+cy+b),$$

where $c^2 + s^2 = 1$ and $c, s, a, b \in \mathbb{C}$. The pair $\mathcal{I} = \{K_1, K_2\}$ defined below is derived from classical Euclidean curvature and is classifying for the action of $\mathcal{E}_2$.

$$K_1 = \frac{\left(y^{(2)}\right)^2}{\left(1 + \left(y^{(1)}\right)^2\right)^3} \tag{4}$$

$$K_2 = \frac{\left(y^{(3)}\left(1 + \left(y^{(1)}\right)^2\right) - 3y^{(1)}\left(y^{(2)}\right)^2\right)^2}{\left(1 + \left(y^{(1)}\right)^2\right)^6} \tag{5}$$

Moreover, there are no $\mathcal{I}$-exceptional algebraic curves—for details see [41]. By Theorem 3.9, the equivalence class of an algebraic curve C under $\mathcal{E}_2(\mathbb{C})$ is determined by $\mathcal{S}_C$.

3.2 Joint signatures

In [39], the author considers the use of *joint* differential signatures to determine equivalence. As an example, for the action of G on $\mathbb{C}^2$ given by $g \cdot (x, y) = (\overline{x}, \overline{y})$, consider the induced action on the Cartesian product space $(\mathbb{C}^2)^n = \mathbb{C}^2 \times \mathbb{C}^2 \times \ldots \times \mathbb{C}^2$ given by

$$g \cdot (x_1, y_1, x_2, y_2, \ldots, x_n, y_n) = (\overline{x}_1, \overline{y}_1, \overline{x}_2, \overline{y}_2, \ldots, \overline{x}_n, \overline{y}_n)$$

where $\overline{x}_i = \overline{x}|_{x=x_i, y=y_i}$ and $\overline{y}_i = \overline{y}|_{x=x_i, y=y_i}$. For a curve $C \subset \mathbb{C}^2$ denote the Cartesian product by $C^n = C \times C \times \ldots \times C \subset (\mathbb{C}^2)^n$. Then we can see that two curves C_0 and C_1 are G-equivalent if and only if their Cartesian products C_0^n, C_1^n are G-equivalent under the induced action on $(\mathbb{C}^2)^n$.

The advantage of considering G-equivalence of products of the curve C is that the order of the differential invariants needed to define a differential signature on this space can be reduced. Though the number of invariants required may increase, the lower order of the differentials can result in a more noise-resistant differential signature. In fact, for a large enough product space, it is often possible to construct a differential signature from '0-th order' differential invariants, or *joint invariants*, which we refer to as a *joint signature*. For more on joint signatures see [39].

Consider the action of $\mathcal{E}_2(\mathbb{C})$ on $\mathbb{C}^2$ as defined in Example 3.10. This induces an action on the product space $(\mathbb{C}^2)^n$. Joint invariants for this action are given by the squared inter-point distance functions

$$d_{jk}(x_j, y_j, x_k, y_k) = (x_j - x_k)^2 + (y_j - y_k)^2,$$

where $j < k$ and $j, k \in \{1, \ldots, n\}$. Let the map $d_n : C^n \longrightarrow \mathbb{C}^{n(n-1)/2}$ be the map which takes an n-tuple of points on C and outputs all the inter-point distances, i.e.

$$(x_1, y_1, \ldots, x_n, y_n) \mapsto (d_{12}, d_{13}, \ldots, d_{1n}, \ldots, d_{(n-1)n}). \tag{6}$$

To define a joint signature for curves under $\mathcal{E}_2(\mathbb{C})$, we take $n = 4$ and follow a similar construction as the joint signature of smooth curves in $\mathbb{R}^2$ under the action of $\mathcal{E}_2(\mathbb{R})$ (see [39, Ex. 8.2]).

Definition 3.1. The *Euclidean joint signature* of an algebraic curve $C \subset \mathbb{C}^2$ under the action of $\mathcal{E}_2(\mathbb{C})$, which we denote $\mathcal{J}_X$, is the image of the polynomial map $d_4 : C^4 \longrightarrow \mathbb{C}^6$ defined as in (6).

To prove that the Euclidean joint signature can determine equivalence of algebraic curves under $\mathcal{E}_2(\mathbb{C})$, we first show that these six invariant functions characterize almost all orbits of the action of $\mathcal{E}_2(\mathbb{C})$ on $(\mathbb{C}^2)^4$.

Proposition 3.2. *The polynomial invariants $\mathcal{I}_3 = \{d_{12}, d_{13}, d_{23}\}$ separates orbits for the induced action of $\mathcal{E}_2$ on $(\mathbb{C}^2)^3$ and the set*

$$\mathcal{I}_4 = \{d_{12}, d_{13}, d_{23}, d_{14}, d_{24}, d_{34}\}$$

separates orbits for the induced action of $\mathcal{E}_2(\mathbb{C})$ on $(\mathbb{C}^2)^4$.

Proof. Consider two triples of points $p = (p_i)_{i=1}^3$ and $q = (q_i)_{i=1}^3 \in (\mathbb{C}^2)^3$, where $p_i = (x_i^p, y_i^p)$ and q_i is denoted similarly, that take the same values on $\mathcal{I}_3$ and lie in the Zariski-open subset given by

$$W_3 = \{p \in (\mathbb{C}^2)^{\times 3} \,|\, d_{12}, d_{13}, d_{23} \neq 0\}.$$

Note that W_3 excludes triples of collinear points as well as isotropic triples such as $(0,0), (1,i), (1,-i)$. We will show that both triples of points necessarily lie in the same orbit. Since $d_{12} \neq 0$ we can choose a representative from the orbit of p under $\mathcal{E}_2$ such that $p_1 = (0,0)$ and $p_2 = (0, y_2^p)$ by applying the transformation in $\mathcal{E}_2(\mathbb{C})$ given by

$$c = \frac{y_2^p - y_1^p}{\sqrt{d_{12}}},\ s = \frac{x_2^p - x_1^p}{\sqrt{d_{12}}},\ a = -x_1^p,\ b = -y_1^p, \tag{7}$$

and similarly we can assume for q that $q_1 = (0,0)$ and $q_2 = (0, y_2^q)$. Since $p, q \in W_3$, $y_2^p, y_2^q \neq 0$. Thus $d_{12}(p) = d_{12}(q)$ gives that $(y_2^p)^2 = (y_2^q)^2$ meaning $y_2^p = \pm y_2^q$. Therefore, by reflecting about x-axis if necessary, we can assume $y_2^p = y_2^q$. The equations $d_{13}(p) = d_{13}(q)$ and $d_{23}(p) = d_{23}(q)$ give

$$(x_3^p)^2 + (y_3^p)^2 = (x_3^q)^2 + (y_3^q)^2$$
$$(x_3^p)^2 + (y_2^p - y_3^p)^2 = (x_3^q)^2 + (y_2^q - y_3^q)^2.$$

Subtracting these yields $(y_2^p)^2 - 2y_2^p y_3^p = (y_2^q)^2 - 2y_2^q y_3^q$ which implies $y_3^p = y_3^q$. Thus, from $d_{13}(p) = d_{13}(q)$, we have $(x_3^p)^2 = (x_3^q)^2$. From this we conclude, reflecting about the y-axis if necessary, that $x_3^p = x_3^q$. We have now shown that p and q must lie in the same orbit.

Suppose we have two 4-tuples of points $p = (p_i)_{i=1}^4$ and $q = (q_i)_{i=1}^4 \in (\mathbb{C}^2)^3$ that take the same values on $\mathcal{I}_4$ and lie in the Zariski-open subset given by

$$W_3 = \{p \in (\mathbb{C}^2)^{\times 3} \,|\, d_{12}, d_{13}, d_{23}, d_{14}, d_{24}, d_{34} \neq 0\}.$$

By the previous argument we can assume that p_1, p_2 have the same form as above and that $p_i = q_i$ for $i = 1, 2, 3$. As before the equations $d_{14}(p) = d_{14}(q)$ and $d_{24}(p) = d_{24}(q)$ imply that and $y_4^q = y_4^p$ and $x_4^p = \pm x_4^q$. If $x_4^p = -x_4^q$ and $x_3^p, x_3^q = 0$, then a reflection about the y-axis preserves the other values in q and sends x_4^q to $-x_4^q$. Otherwise subtracting the equations $d_{14}(p) = d_{14}(q)$ and $d_{34}(p) = d_{34}(q)$ yields $-2x_3^p x_4^p = -2x_3^p x_4^p$, which implies that $x_4^p = x_4^q$. Thus p and q must lie in the same orbit. □

Lemma 3.3. *For an algebraic curve $C \subset \mathbb{C}^2$, a generic n-tuple of points on C^n lies inside W_n. Additionally for any fixed $(n-1)$-tuple of points in $(p_1, \dots, p_{n-1}) \in W_{n-1} \cap X^{n-1}$ and a generic point $p_n \in C$, the n-tuple $(p_1, \dots, p_n)$ lies in W_n.*

Proof. For any n-tuple $p \in (\mathbb{C}^2)^n$, the condition that $d_{jk}(p) = 0$ means that p lies in one of the two planes defined by

$$x_j - x_k + y_j - y_k = 0 \quad \text{or} \quad x_j - x_k - iy_j + iy_k = 0.$$

Note that since $\deg(C) > 1$ and X is irreducible, $\deg(C^n) > 1$ and C^n is irreducible, and hence C^n cannot be contained in one of the planes. Thus a generic n-tuple $p \in C^n$ lies in W_n.

Similarly for a fixed $(n-1)$-tuple in $W_{n-1} \cap X^{n-1}$ and any $p_n \in C$, the n-tuple $p = (p_1, \dots, p_n)$ lies in W_n if and only if $d_{jn}(p) = 0$ for some $j \in 1, \dots, n-1$. However, since $\deg(C) > 1$, a generic point $p_n \in C$ lies outside of the planes defined by $d_{jn}(p) = 0$. Thus $p \in W_n$. □

Proposition 3.4. *The stabilizer of a point $p \in (\mathbb{C}^2)^2$ such that $d_{12}(p) \neq 0$ under the action of $\mathcal{E}_2(\mathbb{C})$ is a discrete subgroup of size two. Additionally the action of $\mathcal{E}_2(\mathbb{C})$ is free on the subset of $(\mathbb{C}^2)^3$ consisting of distinct, non-collinear points.*

Proof. The stabilizer of a point $p \in (\mathbb{C}^2)^2$ is the subgroup of $\mathcal{E}_2(\mathbb{C})$ given by

$$\mathcal{E}_2(\mathbb{C})_p = \{g \in \mathcal{E}_2(\mathbb{C}) \,|\, g \cdot p = p\}.$$

The size of the stabilizer of a point is preserved by the action of the group. Since $d_{12}(p) \neq 0$, by applying the transformation in (7), we can assume p has the form $p = (p_1, p_2) = (0, 0, 0, y_2)$ where $y_2 \neq 0$. Given the parameterization of $\mathcal{E}_2(\mathbb{C})$ in Example 3.10, $g \cdot p = p$ immediately implies that $a = b = 0$ and that $sy_2 = 0$ Thus $\mathcal{E}_2(\mathbb{C})_p$ consists of either the identity transformation or a reflection about the y-axis.

By the same argument, if $p = (p_1, p_2, p_3) \in (\mathbb{C}^2)^3$ where p_1, p_2 and p_3 are distinct, then $\mathcal{E}_2(\mathbb{C})$ consists of only the identity transformation if p_3 lies outside of the line defined by p_1, p_2. Thus $\mathcal{E}_2(\mathbb{C})$ is free on this subset of $(\mathbb{C}^2)^3$. □

Lemma 3.5. *For plane curves C_0, C_1, suppose that there exists $p = (p_1, p_2) \in C_0^2, C_1^2$ such that $d_{12}(p) \neq 0$ and*

$$d_3(p_1 \times p_2 \times C_0) = d_3(p_1 \times p_2 \times C_1).$$

Then $g \cdot C_0 = C_1$ where $g \in \mathcal{E}_2(\mathbb{C})_{(p_1, p_2)}$.

Proof. By Lemma 3.3, for a generic point $q \in C_0$, the 3-tuple $(p_1, p_2, q) \in W_3$. Since both curves have the same image under d_3, there exists a point $r \in C_1$ such that $r \in d_3^{-1}(p_1, p_2, q)$. By Proposition 3.2, both triples (p_1, p_2, q) and (p_1, p_2, r) lie in the same orbit under $\mathcal{E}_2(\mathbb{C})$, and hence there exists $g \in \mathcal{E}_2(\mathbb{C})$ such that $g \cdot (p_1, p_2, q) = (p_1, p_2, r)$. However, this implies that $g \in \mathcal{E}_2(\mathbb{C})_{(p_1, p_2)}$. By Proposition 3.4, $\mathcal{E}_2(\mathbb{C})_{(p_1, p_2)} = \{e, h\}$ where $h \in \mathcal{E}_2(\mathbb{C})$ is a reflection about the line containing p_1 and p_2. Therefore $q = r$ or $\cdot q = r$, implying that C_1 shares infinitely many points with C_0 or $h \cdot C_0$, proving the lemma. □

Lemma 3.6. *For plane curves C_0, C_1, suppose that there exists a 3-tuple $(p_1, p_2, p_3) \in C_0^3, C_1^3$ such that p_1, p_2, p_3 are distinct, non-collinear, and*

$$d_4(p_1 \times p_2 \times p_3 \times C_0) = d_4(p_1 \times p_2 \times p_3 \times C_1).$$

Then $C_0 = C_1$.

Proof. The proof follows similarly as in Lemma 3.5 by applying Propositions 3.2 and 3.4. □

Proposition 3.7. *Two plane curves $C_0, C_1 \subset \mathbb{C}^2$ of degree $d > 2$ are $\mathcal{E}_2(\mathbb{C})$-equivalent if and only if $\overline{\mathcal{J}_{C_0}} = \overline{\mathcal{J}_{C_1}}$.*

Proof. Since the map $d_4 : C^4 \to \mathbb{C}^6$ is defined by $\mathcal{E}_2(\mathbb{C})$-invariants the forward direction is clear. For the remainder of the proof assume that $\overline{\mathcal{J}_{C_0}} = \overline{\mathcal{J}_{C_1}} := \mathcal{J}$. We deal with two cases. Either the image of the map $d_3 : C_0^3 \to \mathbb{C}^3$ lies in a Zariski-closed subset of dimension ≤ 2 or is Zariski-dense in $\mathbb{C}^3$.

First suppose that $d_3(C_0^3)$ (and hence $d_3(C_1^3)$) is Zariski-dense in $\mathbb{C}^3$. This implies $\dim(\mathcal{J})$ equals 3 or 4. Consider the projection $\pi_{12} : \mathcal{J} \to \mathbb{C}$ of $\mathcal{J}$ onto the first coordinate d_{12}. Let $\mathcal{H}_{12} = \pi_{12}^{(-1)}(r)$ be the pullback of a generic point so that $\dim(\mathcal{H}_{12} \cap \mathcal{J})$ equals 2 or

3. Appealing to Bertini's Theorem as in Proposition 2.3, the singular points of $H_{12} \cap \mathcal{J}$ are also singular points of $\mathcal{J}$. For similarly defined $\mathcal{H}_{13}$ and $\mathcal{H}_{23}$ let $\mathcal{Y} = \mathcal{H}_{12} \cap \mathcal{H}_{13} \cap \mathcal{H}_{23} \cap \mathcal{J}$. Then $\dim(\mathcal{Y})$ equals 0 or 1, and the singular points of $\mathcal{Y}$ are singular points of $\mathcal{J}$.

Consider a generic 4-tuple of points $p = (p_1, p_2, p_3, p_4) \in C_0^4$., Since the $d_4(C_i)$ agree on a dense set, we may assume $d_4(p) \in d_4(C_0) \cap d_4(C_1)$. Taking generic $\mathcal{H}_{12} \cap \mathcal{H}_{13} \cap \mathcal{H}_{23}$ through $d_3(p)$, the previous paragraph gives that $d_3(p)$ is a non-singular point of $\mathcal{Y}$. Let $q = (q_1, q_2, q_3, q_4)$ be a point on C_1^4 in the inverse image $d_4^{-1}(d_4(p))$. By Proposition 3.2 and Lemma 3.3, there exists some $g \in \mathcal{E}_2(\mathbb{C})$ such that $g \cdot q = p$. Let $C_2 = g \cdot C_1$.

Both curves C_0 and C_2 contain the points $p_1, \ldots, p_4$, and hence both $d_4(p_1 \times p_2 \times p_3 \times C_0)$ and $d_4(p_1 \times p_2 \times p_3 \times C_2)$ are dense in irreducible components of $\mathcal{Y}$. If $\dim(d_4(p_1 \times p_2 \times p_3 \times C_0) = 0$ then the invariant functions d_{12}, d_{13}, d_{23} take a single value on C_0^4. Adapting the argument of 3.3 shows this cannot be the case. Hence $\dim(d_4(p_1 \times p_2 \times p_3 \times C_0) = 1$, which implies that $\dim(\mathcal{Y}) = 1$. Since $d_4(p)$ is a non-singular point of $\mathcal{Y}$, it is necessarily contained in exactly one irreducible component of $\mathcal{Y}$. Therefore

$$d_4(p_1 \times p_2 \times p_3 \times C_0) = d_4(p_1 \times p_2 \times p_3 \times C_2).$$

By Lemma 3.6, $C_0 = C_2 = g \cdot C_1$, completing the proof for the case where $d_3(C_0^3) \subset \mathbb{C}^3$ is Zariski dense. The remaining case follows analagously (take $\mathcal{Y} = \mathcal{H}_{12} \cap d_3(C_0^3)$ and apply Lemma 3.5.) □

4 IMPLEMENTATION, EXAMPLES, AND EXPERIMENTS

Our implementation of Algorithm 1 treats only the special case where the domain of each rational map is some Cartesian product of irreducible plane curves, say $X_i = C_i^k$ for some integer k. Our results showcase features of the `NumericalAlgebraicGeometry` ecosystem in Macaulay2 (aka `NAG4M2`, see [30, 31] for an overview.) We rely extensively on the core path-tracker and the packages `SLPexpressions` and `MonodromySolver`. All of our examples and experiments deal with differential and joint signatures for the Euclidean group. However, the current functionality should make it easy to study other group actions and variations on the signature construction in the future.

For the purpose of our implementation, the various ingredients for the input to Algorithm 1 are easily provided. Suppose $\mathcal{I}_{C_i} = \langle f_i \rangle$ for $i = 0, 1$. Then the reduced regular sequence we need is given by $(f_0(x_1, y_1), \ldots, f_0(x_k, y_k))$. Sampling from X_0 amounts to sampling k times from C_0; we sample the curve C_0 using homotopy continuation from a linear-product start system [45, 8.4.3]. Finally, a witness set for the image of the signature map Φ_1 can be computed using methods of numerical algebraic geometry. Heuristics based on *monodromy* allow us to make this offline computation relatively efficient; `MonodromySolver` implements a general framework described in [5, 15]. We also observe that a witness set for the signature of a particular curve may be computed if we have already computed a witness set for the corresponding signature of some *generic* curve of the same degree. This is yet another application of coefficient parameter homotopy. [35] The efficiency of these two methods is compared in Example 4.1.

d	$\deg \mathcal{S}$	time (s)	$\deg_{(1,0)} \mathcal{S}$	time (s)
2	6	0.3	3	0.1
3	72	2	36	0.5
4	144	9	72	2
5	240	21	120	4
6	360	55	180	7

Figure 2: Degrees and monodromy timings for differential signatures.

d	$\deg \mathcal{J}$	time (s)	$\deg_{\boldsymbol{e}_1} \mathcal{J}$	time (s)	$\deg_{\boldsymbol{e}_2} \mathcal{J}$	time (s)
2	42	4	24	2	26	2
3	936	33	576	17	696	16
4	3024	139	1920	57	2448	87
5	7440	463	4800	206	6320	276
6	15480	1315	10080	748	13560	791

Figure 3: Degrees and monodromy timings for joint signatures (see Conjecture 4.1.)

We explain some aspects of our implementation that appear to give reasonable numerical stability. A key feature is that polynomials and rational maps are given by straight-line programs as opposed to their coefficient representations. This is especially crucial in the case of differential signatures, where expanding the rational expressions derived from equations (4) and (5) involves many terms and does not suggest a natural evaluation scheme. We also homogenize the equations of our plane curves and work in a random affine chart. Finally, in our sampling procedure we discard samples which map too close to the origin in the codomain of our maps, as these tend to produce nearly-singular points on the image.

Example 4.1. The code below computes a witness set for the differential signature of a "generic" quartic (whose coefficients are random complex numbers of modulus 1.)

```
(d, k) = (4, 1);
dom = domain(d, k);
Map = diffEuclideanSigMap dom;
H = witnessHomotopy(dom, Map);
W = runMonodromy H;
```

To compute a witness set for the differential signature of the Fermat quartic $V(x^4 + y^4 + z^4) \subset \mathbb{P}(\mathbb{C}^3)$, we use the previous computation.

```
R = QQ[x,y,z];
f=x^4+y^4+z^4;
Wf = witnessCollect(f, W)
```

The output resulting from the last line reads

```
witness data w/ 18 image points (144 preimage points)
```

indicating that the differential signature map is generically 8 to 1, which is equivalent to the Fermat curve having eight Euclidean symmetries [28, Thm 2.38]. We timed these witness set computations at 5 and 0.5 seconds, respectively. For joint signatures, the analagous computations were timed at 95 and 17 seconds.

Figures 2 and 3 give degrees and single-run timings for monodromy computations on curves up to degree 6. We also considered multiprojective witness sets for $\mathcal{S} \subset \mathbb{C}^1 \times \mathbb{C}^1$ and $\mathcal{J} \subset (\mathbb{C}^1)^6$, where

d	track time (ms)	lookup time (ms)	track K_1	lookup K_1
2	191	0.35	127	0.25
3	177	0.37	121	0.31
4	276	0.42	145	0.36
5	472	0.39	203	0.43
6	597	0.40	284	0.37

Figure 4: Equality test timings for differential signatures S_d.

d	track time (ms)	lookup time (ms)	track $\boldsymbol{e}_1$	lookup $\boldsymbol{e}_1$
2	230	0.36	208	0.34
3	283	0.38	213	0.35
4	335	0.39	288	0.40
5	409	0.32	357	0.32
6	507	0.32	462	0.33

Figure 5: Equality test timings for joint signatures $\mathcal{J}_d$.

fewer witness points are needed. For the differential signatures, we considered $(1,0)$-slices which fix the value of K_1 in equation (4). For joint signatures, there are two combinatorially distinct classes of $(\mathbb{C}^1)^6$ witness sets determined by which $d_{i,j}$ are fixed; the undirected graph of fixed distances must either be the 3-pan (a 3-cycle with pendant edge) or the 4-cycle. We fix corresponding multidimensions $\boldsymbol{e}_1 = (1,1,1,1,0,0)$ and $\boldsymbol{e}_2 = (0,1,1,1,1,0)$.

The timings in figures 2 and 3 are not optimal for a number of reasons. For instance, some multiprojective witness sets have an *imprimitive* monodromy action, meaning that additional symmetries can be exploited [2]. We successfully ran monodromy (with less conservative settings) for both signature maps on curves of degree up to 10. These computations suggested formulas for the degrees. For the joint signature, we state these formulas in the form of a conjecture. For the case of differential signatures, see [28]; degrees for $d = 2$ are corrected by a factor of 4 (counting the isometries of a generic plane conic.)

Conjecture 4.1. *Let $\mathcal{J}_d$ denote the joint signature for a generic plane curve of degree d. For $d \geq 3$:*

$$\deg \overline{\mathcal{J}_d} = 12d(d^3-1)$$
$$\deg_{\boldsymbol{e}_1} \mathcal{J}_d = 8d^2(d^2-1)$$
$$\deg_{\boldsymbol{e}_2} \mathcal{J}_d = 4d(d-1)(3d^2+d-1).$$

To assess the speed and robustness of the online equality test, we conducted an experiment where, for degrees $d = 2, \ldots, 6$, curves $C_1, \ldots, C_{10}$ were generated with coefficients drawn uniformly from the unit sphere in $\mathbb{R}^{(d+2)(d+1)/2}$. For each C_i, we computed a witness set via parameter homotopy from a generic d-ic. We then applied 20 random transformations from $\mathcal{E}_2(\mathbb{R})$ to the C_i and perturbed the resulting coefficients by random real $\vec{\epsilon}$ with $\|\vec{\epsilon}\|_2 \in \{0, 10^{-7}, 10^{-6}, \ldots, 10^{-3}\}$, thus obtaining curves $\widetilde{C_{i,1,\epsilon}}, \ldots, \widetilde{C_{i,20,\epsilon}}$. With all numerical tolerances fixed, we ran the equality test for each $\widetilde{C_{i,j,\epsilon}}$ against each C_i.

Figures 4 and 5 summarize the timings for the equality tests in this experiment. Overall, these tests run on the order of sub-seconds. Most of the time is spent on path-tracking. The tracking times reported give the total time spent on lines 1 and 5 of Algorithm 1. The only other possible bottleneck is the lookup on line 7. This is negligible, even for large witness set sizes, if an appropriate data structure is used. The runtimes for all cases considered seem comparable, although using differential signatures and multiprojective slices appear to give a slight edge over the respective alternatives.

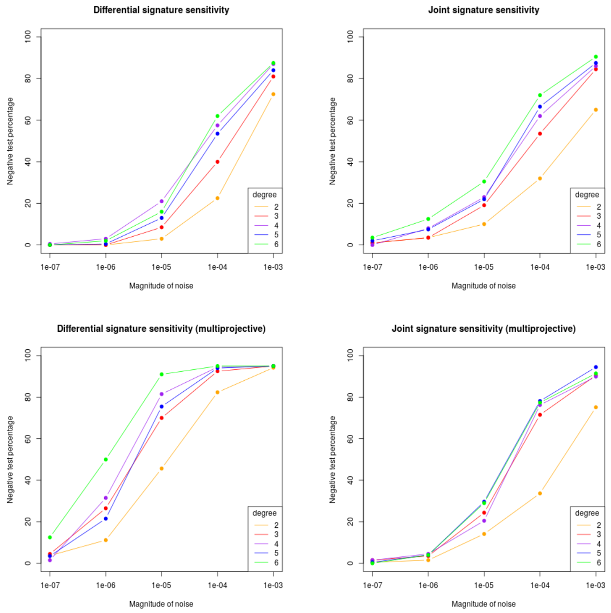

Figure 6: Sensitivity of the equality test to noise.

The plots in Figure 6 (made with R [40]) illustrate the results of our sensitivity analysis. The respective axes are the magnitude of the noise ϵ and the percentage of $\widetilde{C_{i,j,\epsilon}}$ deemed to be not equivalent to C_i. Note that the horizontal axis is given on a log scale, and excludes the noiseless case $\epsilon = 0$; here, one false negative was reported for the differential signatures with $d = 6$. We include a trend line to make the plots more readable. In general, we observe a threshold phenomenon, where most tests are positive for sufficiently low noise and are negative for sufficiently high noise.

The threshold regions in Figure 6 clearly depend on the numerical tolerances used (for this experiment, defaults provided by NAG4M2), the type of map, and the type of witness set. Besides the multiprojective differential signature (depicted in the bottom-left), we observe a similar stability profile for this type of random perturbation. The similar profiles on the right illustrate an apparent robustness for the joint signature maps. We speculate that similar analyses, based on more geometrically meaningful perturbations, may highlight further differences between the joint and differential signatures.

ACKNOWLEDGMENTS

Research of T. Duff is supported in part by NSF DMS-1719968, a fellowship from the Algorithms and Randomness Center at Georgia Tech, and by the Max Planck Institute for Mathematics in the Sciences in Leipzig, where this work was completed.

REFERENCES

[1] E. L. Allgower and K. Georg. 2012. *Numerical continuation methods: an introduction*. Vol. 13. Springer Science & Business Media.

[2] C. Améndola and J. I. Rodriguez. 2016. Solving parameterized polynomial systems with decomposable projections. *arXiv preprint arXiv:1612.08807* (2016).

[3] D. J. Bates, , A. J. Hauenstein, Jonathan D Sommese, and C. W. Wampler. 2013. *Numerically solving polynomial systems with Bertini*. SIAM.

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

[5] N. Bliss, T. Duff, A. Leykin, and J. Sommars. 2018. Monodromy solver: sequential and parallel. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation*. 87–94.

[6] T. Brysiewicz. 2018. Numerical Software to Compute Newton Polytopes. In *International Congress on Mathematical Software*. Springer, 80–88.

[7] B. Buchberger and F. Winkler. 1998. *Gröbner bases and applications*. Vol. 17. Cambridge University Press Cambridge.

[8] J. M. Burdis, I. A. Kogan, and H. Hong. 2013. Object-image correspondence for algebraic curves under projections. *SIGMA Symmetry Integrability Geom. Methods Appl.* 9 (2013), Paper 023, 31. https://doi.org/10.3842/SIGMA.2013.023

[9] L. Busé, D. Cox, and C. d'Andrea. 2003. Implicitization of surfaces in $\mathbb{P}_3$ in the presence of base points. *Journal of Algebra and its Applications* 2, 02 (2003), 189–214.

[10] C. Chen, O. Golubitsky, F. Lemaire, M. M. Maza, and W. Pan. 2007. Comprehensive triangular decomposition. In *International Workshop on Computer Algebra in Scientific Computing*. Springer, 73–101.

[11] J. Chen and J. Kileel. 2019. Numerical implicitization for Macaulay2. *Journal of Software for Algebra and Geometry* 9 (2019), 55–65.

[12] R. M. Corless, M. W. Giesbrecht, I. S. Kotsireas, and S. M. Watt. 2000. Numerical implicitization of parametric hypersurfaces with linear algebra. In *International Conference on Artificial Intelligence and Symbolic Computation*. Springer, 174–183.

[13] D. Cox, J. Little, and D. OShea. 2013. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media.

[14] H. Derksen and G. Kemper. 2015. *Computational invariant theory* (enlarged ed.). Encyclopaedia of Mathematical Sciences, Vol. 130. Springer, Heidelberg. xxii+366 pages. https://doi.org/10.1007/978-3-662-48422-7 With two appendices by Vladimir L. Popov, and an addendum by Norbert A'Campo and Popov, Invariant Theory and Algebraic Transformation Groups, VIII.

[15] T. Duff, C. Hill, A. Jensen, K. Lee, A. Leykin, and J. Sommars. 2019. Solving polynomial systems via homotopy continuation and monodromy. *IMA J. Numer. Anal.* 39, 3 (2019), 1421–1446.

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

[17] D. Grayson and M. Stillman. 1997. Macaulay 2–a system for computation in algebraic geometry and commutative algebra.

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

[19] C. Harris, M. Michałek, and E. C. Sertöz. 2019. Computing images of polynomial maps. *Advances in Computational Mathematics* 45, 5-6 (2019), 2845–2865.

[20] J. Harris. 2013. *Algebraic geometry: a first course*. Vol. 133. Springer Science & Business Media.

[21] J. D. Hauenstein, A. Leykin, J. I. Rodriguez, and F. Sottile. 2019. A numerical toolkit for multiprojective varieties. *arXiv preprint arXiv:1908.00899* (2019).

[22] J. D. Hauenstein and J. I. Rodriguez. 2015. Multiprojective witness sets and a trace test. *To appear in Advances in Geometry. arXiv preprint arXiv:1507.07069,* (2015).

[23] J. D. Hauenstein and A. J. Sommese. 2010. Witness sets of projections. *Appl. Math. Comput.* 217, 7 (2010), 3349–3354.

[24] J. D. Hauenstein and A. J. Sommese. 2013. Membership tests for images of algebraic sets by linear projections. *Appl. Math. Comput.* 219, 12 (2013), 6809–6818.

[25] D. J. Hoff and P. J. Olver. 2014. Automatic solution of jigsaw puzzles. *J. Math. Imaging Vision* 49, 1 (2014), 234–250. https://doi.org/10.1007/s10851-013-0454-3

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

[27] D. Kapur, T. Saxena, and L. Yang. 1994. Algebraic and geometric reasoning using Dixon resultants. In *Proceedings of the international symposium on Symbolic and algebraic computation*. ACM, 99–107.

[28] I. Kogan, M. Ruddy, and C. Vinzant. 2018. Differential Signatures of Algebraic Curves. *To appear in SIAM Journal on Applied Algebra and Geometry. arXiv:1812.11388* (2018).

[29] I. A. Kogan and M. Moreno Maza. 2002. Computation of canonical forms for ternary cubics. In *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*. ACM, New York, 151–160. https://doi.org/10.1145/780506.780526

[30] A. Leykin. 2011. Numerical algebraic geometry. *Journal of Software for Algebra and Geometry* 3, 1 (2011), 5–10.

[31] A. Leykin. 2018. Homotopy Continuation in Macaulay2. In *International Congress on Mathematical Software*. Springer, 328–334.

[32] A. Leykin, J. I. Rodriguez, and F. Sottile. 2018. Trace test. *Arnold Mathematical Journal* 4, 1 (2018), 113–125.

[33] W. O. Maplesoft, a division of Waterloo Maple Inc. [n. d.]. Maple 2019.0.

[34] A. Morgan. 2009. *Solving polynomial systems using continuation for engineering and scientific problems*. Vol. 57. SIAM.

[35] A. P. Morgan and A. J. Sommese. 1989. Coefficient-parameter polynomial continuation. *Appl. Math. Comput.* 29, 2 (1989), 123–160.

[36] D. Mumford. 1995. *Algebraic geometry I: complex projective varieties*. Springer Science & Business Media.

[37] P. J. Olver. 1995. *Equivalence, invariants and symmetry*. Cambridge University Press.

[38] P. J. Olver. 1999. *Classical invariant theory*. London Mathematical Society Student Texts, Vol. 44. Cambridge University Press, Cambridge. xxii+280 pages. https://doi.org/10.1017/CBO9780511623660

[39] P. J. Olver. 2001. Joint invariant signatures. *Found. Comput. Math.* 1, 1 (2001), 3–67. https://doi.org/10.1007/s10208001001

[40] R Core Team. 2018. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

[41] M. Ruddy. 2019. *The Equivalence Problem and Signatures of Algebraic Curves*. Ph.D. Dissertation. North Carolina State University.

[42] T. W. Sederberg and F. Chen. 1995. Implicitization using moving curves and surfaces. In *Siggraph*, Vol. 95. 301–308.

[43] I. Shafarevich. 1994. *Basic algebraic geometry* (2 ed.). Vol. 1. Springer.

[44] A. J. Sommese, J. Verschelde, and C. W. Wampler. 2005. Introduction to numerical algebraic geometry. In *Solving polynomial equations*. Springer, 301–337.

[45] I. C. W. Wampler et al. 2005. *The Numerical solution of systems of polynomials arising in engineering and science*. World Scientific.