

# Differential Elimination and Algebraic Invariants of Polynomial Dynamical Systems

William Simmons<sup>a,b,\*</sup>, André Platzer<sup>b,c</sup>

<sup>a</sup>High Assurance Solutions group, Two Six Technologies, Arlington, USA

<sup>b</sup>Computer Science Department, Carnegie Mellon University, Pittsburgh, USA

<sup>c</sup>Department of Informatics, Karlsruhe Institute of Technology, Karlsruhe, Germany

---

## Abstract

Invariant sets are a key ingredient for verifying safety and other properties of cyber-physical systems that mix discrete and continuous dynamics. We adapt the elimination-theoretic Rosenfeld-Gröbner algorithm to systematically obtain algebraic invariants of polynomial dynamical systems without using Gröbner bases or quantifier elimination. We identify totally real varieties as an important class for efficient invariance checking.

**Keywords:** algebraic invariants, algebraic varieties, elimination theory, differential algebra, polynomial dynamical systems, Rosenfeld-Gröbner algorithm, characteristic set, Gröbner basis, totally real varieties, computational complexity

---

## 1. Introduction

Computers are increasingly hitting the road, taking to the skies, and interacting with people and the physical environment in unprecedented ways. Engineering concerns like realistic models and reliable sensors are critical, but just as important are the complex mathematical problems that lie at the heart of making *cyber-physical systems* (CPS) safe [1, 2]. One of these central problems is computing *invariant sets* [3] of continuous dynamical systems (Section 2.3), where an invariant set is a collection of states from which any trajectory starting in the set will never leave. Given a system of ordinary differential equations (ODEs) and a set of unsafe states, we must identify initial states that will never lead to an unsafe state under the specified dynamics. If an invariant does not intersect the unsafe set, then every state in the invariant set is a safe starting point. Beyond safety [4], invariant reasoning is an important part of other significant properties like stability [5] and liveness [6]. Due to its significance, the problem of invariant generation for ODEs has received substantial interest [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22] and even has a dedicated tool [23], but most methods have nontrivial heuristic search parts.

---

\* Corresponding author

Email addresses: [william.simmons@twosixtech.com](mailto:william.simmons@twosixtech.com) (William Simmons),  
[aplatzer@cs.cmu.edu](mailto:aplatzer@cs.cmu.edu) (André Platzer)

In this article we employ strategies from *elimination theory* [24] to give new algorithms for systematically generating invariants and checking candidates for invariance. Elimination theory draws on algebra, geometry, and logic to give algorithmic procedures for understanding the polynomial systems that arise in many applications. In a narrow sense, elimination is the process of exposing explicit relationships and removing variables. The prototypical example of an elimination method is *Gaussian elimination*, which converts a system of linear equations into a simpler system with the same solutions from which those solutions can be read off easily. However, linear algebraic equations are merely the tip of the iceberg. Crucially, many elimination tools are extremely general. They apply to nonlinear problems of diverse forms, allowing an unusual degree of reuse across theories and applications. In this paper, our problems require methods for symbolically analyzing systems of ODEs that have *real algebraic* [25] constraints; i.e., are defined by polynomial equations over the real numbers (Section 2.3). In recent decades, researchers in *differential algebra* [26] have extended classical algebraic elimination methods to polynomial differential equations (Section 2.4). Broadly speaking, *differential elimination* [27] provides tools for finding all relations implied by a polynomial differential system, regardless of the form. The elimination procedures we develop in Sections 3 and 4 are intrinsically mathematical, but we show that the output corresponds directly to invariants of the input system, giving a novel, complementary view on systematically computing and checking ODE invariants.

As always, there are trade-offs involved. Elimination methods are exact, general and remarkably versatile, but used naively they can have high theoretical and practical costs [28]. We emphasize alternatives within elimination theory that have better computational complexity than standard choices. For example, *characteristic sets* [29] carry less information than the more ubiquitous *Gröbner bases* [30] but they have singly exponential complexity [31] in the number of variables instead of Gröbner bases' doubly exponential growth [32]. We work extensively with *regular systems* (Section 2.6), a weak form of characteristic sets with lower complexity. Similarly, real number solutions are the main goal in applications, but obtaining them is often significantly more expensive than working over the complex numbers [33, 34]. We give a promising workaround that can *equivalently* replace real algebraic computation with more efficient complex<sup>1</sup> alternatives in many situations (Sections 2.2 and 4.4).

Computation is our main motivation for restricting to polynomial differential and algebraic equations. Such equations are general [4], already powerful for applications [35] and undecidability typically ensues when we leave the polynomial setting [36].

*Structure of the Paper.* Section 2 reviews the algebraic geometry and differential algebra used to rigorously justify our results in Sections 3 and 4. If we do not have a reference at hand or the proof is short, we provide a proof without claiming originality.

Most of the material in Section 2 is standard and is self-contained assuming familiarity with basic linear algebra and multivariate calculus. That said, the ideas are nontrivial and, depending on background, readers may need to study most or all of Section 2 in order to fully understand the new results and proofs in Sections 3 and 4.

---

<sup>1</sup> Ironically, computation over complex-valued structures is often less complex than over real-valued structures.

However, skimming Section 2 for notation and definitions should provide a good initial picture even without carefully reading Section 2.

Sections 3 and 4 are the heart of the paper. In Section 3 the main contributions are Theorems 86 and 88. Theorem 86 identifies a novel sufficient condition for a system ( $A = 0, S \neq 0$ ) of polynomial equations and inequations to implicitly determine an invariant. Theorem 88 gives multiple criteria, frequently met in practice, that allow ( $A = 0, S \neq 0$ ) to define the associated invariant more explicitly. A detailed example (Section 3.3) illustrates the necessary computations while postponing a full explanation until Section 4.2.

Section 4.1 introduces  $\text{RGA}_o$ , our new variant of the Rosenfeld-Gröbner algorithm (RGA) of Boulier et al. [37].  $\text{RGA}_o$  takes in a system of ordinary differential equations  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  and polynomial equations  $A = 0$  and systematically extracts a structured, maximal invariant satisfying the equations. In particular, Theorem 98 shows that  $\text{RGA}_o$  produces output that meets the requirements of Theorem 86 for an invariant. Section 4.2 revisits the example of Section 3.3 in the context of RGA. In Section 4.3 we analyze the computational complexity of  $\text{RGA}_o$  and find an explicit upper bound (Theorem 109) on the degrees of polynomials in the output. (Prior works on RGA have either ignored complexity or only found bounds on the order of intermediate differential equations.) Our focus in Section 4.4 is a simple and efficient—compared to standard methods from the literature—test for invariance (Theorem 112) based on *totally real varieties*. These geometric objects provide a bridge that lets us draw conclusions about real number solutions using tools that are naturally suited to the complex numbers with their computational advantages.

Section 5 compares and contrasts  $\text{RGA}_o$  with related approaches for generating and checking invariants. Finally, Section 6 summarizes our contributions and outlines promising future research questions.

## 2. Mathematical Background

### 2.1. Ideals and Varieties

We work extensively with multivariate polynomials over various *fields* [38] like the rational numbers  $\mathbb{Q}$ , the real numbers  $\mathbb{R}$ , and the complex numbers  $\mathbb{C}$ . We often write  $K$  or  $L$  for an unspecified field. (A field is essentially a set equipped with some “addition” and “multiplication” operations that satisfy the usual properties of arithmetic in  $\mathbb{Q}$ ,  $\mathbb{R}$ , or  $\mathbb{C}$ . In particular, we have the ability to divide by nonzero elements.) In Section 2.4 we consider *differential fields*, which are fields having additional structure inspired by calculus. We sometimes restrict to polynomials over the real or complex numbers even when results apply more generally. The fact that  $\mathbb{R}$  has an ordering (given by the usual  $<$  relation) is important, but we try to work algebraically as much as possible (in which case  $\mathbb{C}$  is particularly convenient.) Occasionally we use the Euclidean metric properties of  $\mathbb{R}$  and  $\mathbb{C}$  [39].

Unless indicated otherwise, we use  $n$  for the number of variables and write  $\mathbf{x}$  for the  $n$ -tuple  $(x_1, x_2, \dots, x_n)$ ; then the *polynomial ring*  $K[\mathbf{x}]$  is the set of all polynomials in variables  $x_1, x_2, \dots, x_n$  over field  $K$ . We denote by  $K^n$  the collection of all  $n$ -tuples of elements from  $K$ .

### 2.1.1. Ideals

**Definition 1.** Let  $K$  be a field. If  $I \subseteq K[\mathbf{x}]$ ,  $0 \in I$ , and  $p + q \in I$ ,  $gp \in I$  for all  $p, q \in I$  and  $g \in K[\mathbf{x}]$ , then we say  $I$  is an ideal of  $K[\mathbf{x}]$  and write  $I \trianglelefteq K[\mathbf{x}]$ . If  $I \trianglelefteq K[\mathbf{x}]$  and  $I \neq K[\mathbf{x}]$ , we call  $I$  a proper ideal and write  $I \triangleleft K[\mathbf{x}]$ .

If  $A \subseteq K[\mathbf{x}]$ , then the collection of all finite sums  $\sum_i g_i p_i$ , where  $p_i \in A$  and  $g_i$  is any polynomial in  $K[\mathbf{x}]$ , is the ideal generated by  $A$  in  $K[\mathbf{x}]$ . We write  $(A)_K$  or just  $(A)$  to denote this ideal of  $K[\mathbf{x}]$ .

Our interest in ideals comes from the fact that they correspond to systems of polynomial equations. If  $p \in I$ , we associate  $p$  with the equation  $p = 0$ . The definition of an ideal mirrors the behavior of polynomial equation solutions: given  $\mathbf{a} \in K^n$ , if  $p$  and  $q$  are simultaneously 0 when evaluated at  $\mathbf{a}$ , then  $p(\mathbf{a}) + q(\mathbf{a})$  and  $g(\mathbf{a})p(\mathbf{a})$  are also 0 for any  $g \in K[\mathbf{x}]$ .

Note that  $(A)$  is the minimal ideal of  $K[\mathbf{x}]$  containing  $A$ . Elements of an ideal are linear combinations of generators of the ideal, although the “coefficients” multiplied by the generators are arbitrary polynomials over  $K$ , not necessarily elements of  $K$ .

Even though nonzero ideals in  $K[\mathbf{x}]$  are infinite, they can always be represented in a finite way:

**Theorem 2** (Hilbert’s basis theorem [30, Thm. 4, p. 77]). *Let  $K$  be a field. Every ideal in the multivariate polynomial ring  $K[\mathbf{x}]$  is finitely generated (has a finite generating set).*

We generally rely on context to indicate the polynomial ring of which  $I$  or  $(A)$  is an ideal (namely, the ring mentioned whenever the ideal’s name is introduced), but we use the following notation when changing fields:

**Notation 3.** Let  $K \subseteq L$  be fields and let  $I \trianglelefteq K[\mathbf{x}]$ . We write  $I_L$  for the ideal generated by  $I$  in  $L[\mathbf{x}]$ .

For instance, if  $(A)_K \trianglelefteq K[\mathbf{x}]$ , then  $(A)_L$  is the ideal generated by  $A$  (or equivalently by  $(A)_K$ ) in  $L[\mathbf{x}]$ .

**Lemma 4.** Let  $K \subseteq L$  be fields. If  $p \in K[\mathbf{x}]$  and  $p \in I_L$  for  $I \trianglelefteq K[\mathbf{x}]$ , then  $p \in I$ .

*Proof.* This is immediate from the definition of ideal membership and the linear algebra fact that linear equations with coefficients from a field  $K$  are solvable in  $K$  if and only if they are solvable in the extension  $L$ .  $\square$

Two types of ideals play a particularly fundamental role in relating geometry (specifically, solution sets of polynomial equations) to algebra.

**Definition 5.** A prime ideal  $P \triangleleft K[\mathbf{x}]$  is a proper ideal such that for all  $p, q \in K[\mathbf{x}]$  for which  $pq \in P$ , either  $p \in P$  or  $q \in P$ .

A radical ideal  $I \trianglelefteq K[\mathbf{x}]$  has the property that for all  $p \in K[\mathbf{x}]$  such that  $p^N \in I$  for some natural number  $N$ , already  $p \in I$ . The radical  $\sqrt{I}$  of an arbitrary ideal  $I$  is the intersection of all radical ideals containing  $I$ .

The radical  $\sqrt{I}$  is a radical ideal and consists precisely of those polynomials  $p$  such that  $p^N \in I$  for some  $N$ . Ideal  $I$  is radical if and only if  $I = \sqrt{I}$ . Prime ideals are radical, but not necessarily vice versa (for instance,  $(xy) \subseteq \mathbb{R}[x, y]$  is radical but not prime).

### 2.1.2. Algebraic Varieties and Constructible Sets

Sets definable by polynomial equations, as well as the corresponding ideals, are central players in our work:

**Definition 6.** Let  $K$  be a field,  $A \subseteq K[x]$ , and  $X \subseteq K^n$ . The zero set of  $A$ , denoted  $\mathbf{V}_K(A)$ , is the set of all  $\mathbf{a} \in K^n$  such that  $f(\mathbf{a}) = 0$  for all  $f \in A$ . If  $X = \mathbf{V}_K(B)$  for some  $B \subseteq K[x]$ , we call  $X$  a variety, algebraic set, or Zariski closed set over  $K$ . We refer to subsets of  $X$  that are themselves zero sets of polynomials in  $K[x]$  as subvarieties, algebraic subsets, or Zariski closed subsets over  $K$ .

Even if  $X$  is not algebraic, we define the vanishing ideal of  $X$ , denoted  $\mathbf{I}_K(X)$ , to be the collection of all  $g \in K[x]$  such that  $g(\mathbf{b}) = 0$  for all  $\mathbf{b} \in X$ . (Note that  $\mathbf{I}_K(X)$  is a radical ideal.) If  $K$  is understood from context, we may write  $\mathbf{V}(A)$  or  $\mathbf{I}(X)$  for the zero set and vanishing ideal, respectively. If  $A$  contains only one polynomial  $p$ , we write  $\mathbf{V}(p)$  instead of  $\mathbf{V}(A)$ .

**Example 7.** Trivial examples of algebraic sets are the empty set and all of  $K^n$ . A more interesting example is  $\mathbf{V}_K(\det(\mathbf{x})) \subseteq K^{n^2}$ , where  $\det(\mathbf{a})$  is the determinant of the  $n \times n$  matrix corresponding to  $\mathbf{a} \in K^{n^2}$ . The points of  $\mathbf{V}_K(\det(\mathbf{x}))$  represent singular matrices.

**Lemma 8** ([30, Thm. 15, p. 196]). Let  $K$  be a field and let  $I, J \trianglelefteq K[x]$ . Then  $\mathbf{V}_K(I \cap J) = \mathbf{V}_K(I) \cup \mathbf{V}_K(J)$ .

**Lemma 9** ([30, Thm. 7(ii), p. 183]; Table 1). Let  $K$  be a field and  $A \subseteq K[x]$ . Then  $\mathbf{V}(\mathbf{I}(\mathbf{V}(A))) = \mathbf{V}(A)$ .

**Remark 10.** Lemma 9 suggests an inverse relationship between  $\mathbf{V}$  and  $\mathbf{I}$ . A deeper companion result that fills out this intuition is Hilbert's Nullstellensatz (Theorem 20). We will review several similar results involving various fields ( $\mathbb{R}, \mathbb{C}$ , and differential fields (Section 2.4)), so for convenience we list all of them in Table 1 on p. 6. (The table is referenced prior to the statement of each such theorem.) These theorems are instances of *Galois connections* [40, 41].

Complements of algebraic sets (i.e., points *not* satisfying certain polynomial equations) are also important for our results in Sections 3 and 4.

**Definition 11.** Let  $K$  be a field.  $K$ -constructible sets are Boolean combinations (i.e., complements, finite intersections, and finite unions) of Zariski closed sets over  $K$ . We write constructible sets if  $K$  is understood.

A typical example of a constructible set that might not be an algebraic set is the set difference  $X \setminus Y$  of two algebraic sets  $X, Y$ . However, finite unions and arbitrary intersections of algebraic sets are still algebraic [42, p. 24]. Said differently, *Zariski open sets* (complements of Zariski closed sets) form a *topology* on  $K^n$ .

### 2.1.3. Zariski Closure

Even if a constructible set is not algebraic, it can be augmented to one that is equivalent from the perspective of polynomial equations.

Table 1: Summary of Galois connection theorems

Any field  $K$ :

- (Lemma 9) Let  $A \subseteq K[\mathbf{x}]$ . Then  $\mathbf{V}(\mathbf{I}(\mathbf{V}(A))) = \mathbf{V}(A)$ .
- (Lemma 15) An algebraic variety  $X$  over  $K$  is irreducible if and only if its vanishing ideal  $\mathbf{I}_K(X)$  is a prime ideal.

$\mathbb{C}$  (or any algebraically closed field):

- (Theorem 20, Hilbert's Nullstellensatz) Polynomial  $p \in \mathbb{C}[\mathbf{x}]$  vanishes at every point in the complex zero set of  $I \trianglelefteq \mathbb{C}[\mathbf{x}]$  if and only if  $p \in \sqrt{I}$ .
- (Corollary 25, complex algebra-geometry dictionary) Let  $A, B \subseteq \mathbb{C}[\mathbf{x}]$ . Then  $\mathbf{V}_{\mathbb{C}}(A) \subseteq \mathbf{V}_{\mathbb{C}}(B)$  if and only if  $\sqrt{A} \supseteq \sqrt{B}$ .
- (Theorem 29, Hilbert's Nichtnullstellensatz) Let  $A \subseteq \mathbb{C}[\mathbf{x}]$ , and let  $0 \notin S \subseteq \mathbb{C}[\mathbf{x}]$  be finite. A polynomial  $p \in \mathbb{C}[\mathbf{x}]$  vanishes at every complex solution of  $(A = 0, S \neq 0)$  if and only if  $p \in \sqrt{A} : S^\infty$ .

$\mathbb{R}$  (or any real closed field [25]):

- (Theorem 24, real Nullstellensatz) Polynomial  $p \in \mathbb{R}[\mathbf{x}]$  vanishes at every point in the real zero set of  $I \trianglelefteq \mathbb{R}[\mathbf{x}]$  if and only if  $p \in \sqrt[\mathbb{R}]{I}$ .
- (Corollary 25, real algebra-geometry dictionary) Let  $A, B \subseteq \mathbb{R}[\mathbf{x}]$ . Then  $\mathbf{V}_{\mathbb{R}}(A) \subseteq \mathbf{V}_{\mathbb{R}}(B)$  if and only if  $\sqrt[\mathbb{R}]{A} \supseteq \sqrt[\mathbb{R}]{B}$ .

Any differential field  $K$  (characteristic 0):

- (Theorem 61, differential Nullstellensatz) Given  $A \subseteq K\{\mathbf{x}\}$ , a differential polynomial  $p \in K\{\mathbf{x}\}$  vanishes at every point of  $\mathbf{V}_{K,\delta}(A)$  if and only if  $p \in \sqrt{[A]}$ .
- (Corollary 62, differential algebra-geometry dictionary) Let  $A, B \subseteq K\{\mathbf{x}\}$ . Then  $\mathbf{V}_{K,\delta}(A) \subseteq \mathbf{V}_{K,\delta}(B)$  if and only if  $\sqrt{[A]} \supseteq \sqrt{[B]}$ .
- (Theorem 63, differential Nichtnullstellensatz) Let  $A \subseteq K\{\mathbf{x}\}$ , and let  $0 \notin S \subseteq K\{\mathbf{x}\}$  be finite. A differential polynomial  $p \in K\{\mathbf{x}\}$  vanishes at every solution of  $(A = 0, S \neq 0)$  in every differential extension field of  $K$  if and only if  $p \in \sqrt{[A]} : S^\infty$ .

**Definition 12.** Let  $K$  be a field. Given a set  $X \subseteq K^n$ , the intersection of all Zariski closed sets over  $K$  that contain  $X$  is the Zariski closure of  $X$  over  $K$ . We denote the Zariski closure by  $\overline{X}^K$ , or simply  $\overline{X}$  if  $K$  is understood.

Being an intersection of Zariski closed sets, the Zariski closure is itself a Zariski closed set. As suggested above, the Zariski closure is the best *algebraic* overapprox-

imation (using coefficients from  $K$ ) to the original set. In particular, two sets having the same Zariski closure are indistinguishable using polynomial equations. (For a more precise statement, see Lemma 17.)

Over  $\mathbb{R}$  or  $\mathbb{C}$ , Zariski open sets form a topology that is coarser than the usual Euclidean topology. That is, Zariski open sets are Euclidean open, but not necessarily vice versa (for instance, the open interval  $(0, 1) \subseteq \mathbb{R}^1$  is Euclidean open but not Zariski open because its complement is not the set of roots of a univariate polynomial). However, the following is true:

**Lemma 13.** *Real (respectively, complex) Zariski-closed sets are closed in the real (respectively, complex) Euclidean topology, and the real (respectively, complex) Zariski closure of a real (respectively, complex) constructible set is the real (respectively, complex) Euclidean closure of the set.*

*Proof.* See [43, Cor. 4.20]. The cited proof shows that the complex Euclidean closure of the image of a complex variety under a polynomial map equals the complex Zariski closure of the image, but the constructible set version (real or complex) reduces to that result. (Overview of the idea: Use the identity map. Since the complex Euclidean and Zariski closures are equal by [43, Cor. 4.20], it now suffices to show i) the real Zariski closure is the restriction of the complex Zariski closure to  $\mathbb{R}^n$ , and ii) likewise for the real versus the complex Euclidean topologies. Claim i) is Lemma 19, which is not dependent on the current lemma. Claim ii) is immediate using the Euclidean metric on  $\mathbb{R}^n$  and  $\mathbb{C}^n$ .)  $\square$

To distinguish between the Zariski and the Euclidean closures of a set  $X$  over  $\mathbb{R}$  or  $\mathbb{C}$ , we write  $\overline{X}^{\mathbb{R}\text{-euc}}$  or  $\overline{X}^{\mathbb{C}\text{-euc}}$  for the Euclidean closures.

**Definition 14.** *Let  $K$  be a field and  $X, Y \subseteq K^n$  where  $Y$  is Zariski closed over  $K$ . We say that  $X$  is  $K$ -Zariski dense (or just Zariski dense) in  $Y$  if  $Y = \overline{X}^K$ .*

Here the difference between the Zariski and Euclidean topologies is evident: for instance,  $\mathbb{R}$  is  $\mathbb{C}$ -Zariski dense in  $\mathbb{C}$  (because the only univariate polynomial with infinitely many roots is 0) but  $\mathbb{R}$  is not dense in  $\mathbb{C}$  with respect to the Euclidean topology since points of  $\mathbb{C} \setminus \mathbb{R}$  are not limit points of  $\mathbb{R}$ . This does not violate Lemma 13 because  $\mathbb{R}$  is not a  $\mathbb{C}$ -constructible set.

The next lemma concerns *irreducible* algebraic sets, i.e., algebraic sets over a field  $K$  that are not the union of two smaller algebraic subsets over  $K$ .

**Lemma 15** ([42, p. 35]; Table 1). *An algebraic variety  $X$  over  $K$  is irreducible if and only if its vanishing ideal  $\mathbf{I}_K(X)$  is a prime ideal.*

A typical example is an algebraic set defined by a single polynomial that is irreducible in  $K[x]$ . Some authors require an algebraic set to be irreducible to qualify for the name “variety”, but we do not impose that restriction.

**Lemma 16.** *Let  $K$  be a field and let  $X, Y \subseteq K^n$  be Zariski closed sets. If  $X$  is irreducible over  $K$  and  $X \setminus Y$  is nonempty, then  $\overline{X \setminus Y}^K = X$ .*

*Proof.* If  $\overline{X \setminus Y^K}$  were not all of  $X$ , then  $\overline{X \setminus Y^K} \cup (X \cap Y)$  would be a decomposition of  $X$  that contradicts irreducibility.  $\square$

**Lemma 17.** *Let  $K$  be a field.*

1. *If  $X \subseteq K^n$  and  $p \in K[\mathbf{x}]$ , then  $p$  vanishes at every point of  $X$  if and only if  $p$  vanishes at every point of the Zariski closure  $\overline{X^K}$  of  $X$ ; i.e.,  $\mathbf{I}_K(X) = \mathbf{I}_K(\overline{X^K})$ .*
2. *Given  $X, Y \subseteq K^n$ , we have  $\overline{X^K} = \overline{Y^K}$  if and only  $\mathbf{I}_K(X) = \mathbf{I}_K(Y)$ .*

*Proof.* 1. In both cases  $\mathbf{V}_K(p)$  is a Zariski-closed set containing  $X$ .

2. If  $\overline{X^K} = \overline{Y^K}$ , then  $\mathbf{I}_K(X) = \mathbf{I}_K(\overline{X^K}) = \mathbf{I}_K(\overline{Y^K}) = \mathbf{I}_K(Y)$  by 1. Conversely, suppose  $\mathbf{I}_K(X) = \mathbf{I}_K(Y)$ . Then similarly  $\mathbf{I}_K(\overline{X^K}) = \mathbf{I}_K(\overline{Y^K})$  by 1. Since  $\overline{X^K}, \overline{Y^K}$  are Zariski closed, we have  $\overline{X^K} = \mathbf{V}_K(\mathbf{I}_K(\overline{X^K})) = \mathbf{V}_K(\mathbf{I}_K(\overline{Y^K})) = \overline{Y^K}$  by Lemma 9.  $\square$

**Definition 18.** *Let  $K \subseteq L$  be fields and let  $Y \subseteq L^n$ . We call  $Y \cap K^n$  the  $K$ -points of  $Y$  or the restriction of  $Y$  to  $K^n$ . We denote this set by  $Y(K)$ .*

**Lemma 19.** *Let  $X \subseteq \mathbb{R}^n$ . Then the real Zariski closure  $\overline{X}^{\mathbb{R}}$  equals  $\overline{X}^{\mathbb{C}} \cap \mathbb{R}^n$ , the restriction of the complex Zariski closure to the reals.*

*Proof.*  $\subseteq$ : We must show that  $\overline{X}^{\mathbb{C}} \cap \mathbb{R}^n$  contains  $X$  and is real Zariski closed. Containment of  $X$  is clear. For real Zariski closedness, note that  $\overline{X}^{\mathbb{C}} \cap \mathbb{R}^n$  is the zero set of the real and imaginary parts of the defining polynomials of  $\overline{X}^{\mathbb{C}}$ . (That is, suppose  $\overline{X}^{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(A)$  for some  $A \subseteq \mathbb{C}[\mathbf{x}]$ . For all  $p \in A$ , distribute over the real and imaginary parts of each monomial's coefficient to write  $p = p_1 + ip_2$  where  $p_1, p_2 \in \mathbb{R}[\mathbf{x}]$ . We only care about real solutions  $\mathbf{a} \in \mathbb{R}^n$  here, so  $p(\mathbf{a}) = 0$  if and only if  $p_1(\mathbf{a}) = p_2(\mathbf{a}) = 0$ .)

$\supseteq$ : We must show that  $\overline{X}^{\mathbb{C}} \cap \mathbb{R}^n$  is contained in every real Zariski closed set  $Y$  that contains  $X$ . Observe that  $\mathbf{V}_{\mathbb{C}}(\mathbf{I}_{\mathbb{R}}(Y))$  is a complex Zariski closed set containing  $Y$  and thus  $X$ . Then  $\overline{X}^{\mathbb{C}} \subseteq \mathbf{V}_{\mathbb{C}}(\mathbf{I}_{\mathbb{R}}(Y))$  and so  $\overline{X}^{\mathbb{C}} \cap \mathbb{R}^n \subseteq \mathbf{V}_{\mathbb{C}}(\mathbf{I}_{\mathbb{R}}(Y)) \cap \mathbb{R}^n = \mathbf{V}_{\mathbb{R}}(\mathbf{I}_{\mathbb{R}}(Y)) = Y$ , with the last equality following from Lemma 9.  $\square$

#### 2.1.4. The Nullstellensatz: Connecting geometry and algebra

The following well-known result is fundamental for going back and forth between varieties and ideals over  $\mathbb{C}$ :

**Theorem 20** (Hilbert's Nullstellensatz [30, Thm. 2, p. 179]; Table 1). *Polynomial  $p \in \mathbb{C}[\mathbf{x}]$  vanishes at every point in the complex zero set of  $I \trianglelefteq \mathbb{C}[\mathbf{x}]$  if and only if  $p \in \sqrt{I}$ . Equivalently,  $\mathbf{I}_{\mathbb{C}}(\mathbf{V}_{\mathbb{C}}(I)) = \sqrt{I}$  for  $I \trianglelefteq \mathbb{C}[\mathbf{x}]$ .*

Real algebraic geometry requires a more refined (but computationally less tractable) notion than the radical, the *real radical*:



**Definition 21.** Let  $I \subseteq \mathbb{R}[\mathbf{x}]$ . The real radical  $\sqrt[\mathbb{R}]{I}$  of  $I$  is the set of all polynomials  $p \in \mathbb{R}[\mathbf{x}]$  such that for some natural number  $m$  and polynomials  $g_1, g_2, \dots, g_s \in \mathbb{R}[\mathbf{x}]$ , the sum  $p^{2m} + g_1^2 + g_2^2 + \dots + g_s^2$  belongs to  $I$ .

**Remark 22.** An expression of the form  $g_1^2 + g_2^2 + \dots + g_s^2$  is a *sum-of-squares*. Sums-of-squares are important for real algebraic geometry because  $g(\mathbf{x}) = (g_1(\mathbf{x}))^2 + (g_2(\mathbf{x}))^2 + \dots + (g_s(\mathbf{x}))^2$  is zero at  $\mathbf{a} \in \mathbb{R}^n$  if and only if  $g_i(\mathbf{a}) = 0$  for all  $1 \leq i \leq s$ .

The following straightforward properties follow immediately from the definitions and Remark 22. We may use them without comment but record them here for completeness.

**Proposition 23.**

1. If  $I \subseteq \mathbb{R}[\mathbf{x}]$ , then  $\sqrt[\mathbb{R}]{I}$  is a radical ideal that contains  $\sqrt{I}$  (possibly strictly).
2. If  $I \subseteq \mathbb{C}[\mathbf{x}]$  (respectively,  $\mathbb{R}[\mathbf{x}]$ ), then  $\sqrt{\sqrt[\mathbb{R}]{I}} = \sqrt{I}$  (respectively,  $\sqrt[\mathbb{R}]{\sqrt[\mathbb{R}]{I}} = \sqrt[\mathbb{R}]{I}$  and  $\sqrt[\mathbb{R}]{\sqrt{I}} = \sqrt[\mathbb{R}]{I}$ ).
3. If  $I, J \subseteq \mathbb{C}[\mathbf{x}]$  (respectively,  $\mathbb{R}[\mathbf{x}]$ ) and  $I \subseteq J \subseteq \sqrt{I}$  (respectively,  $\sqrt[\mathbb{R}]{I}$ ), then
  - (a)  $\sqrt{J} = \sqrt{I}$  (respectively,  $\sqrt[\mathbb{R}]{J} = \sqrt[\mathbb{R}]{I}$ ) and
  - (b)  $\mathbf{V}_{\mathbb{C}}(I) = \mathbf{V}_{\mathbb{C}}(J) = \mathbf{V}_{\mathbb{C}}(\sqrt{I})$  (respectively,  $\mathbf{V}_{\mathbb{R}}(I) = \mathbf{V}_{\mathbb{R}}(J) = \mathbf{V}_{\mathbb{R}}(\sqrt[\mathbb{R}]{I})$ ).

A much deeper result known as the *real Nullstellensatz* tells us that  $\sqrt[\mathbb{R}]{I}$  is the largest collection of polynomials over  $\mathbb{R}$  that has the same *real* zero set as  $I$ :

**Theorem 24** (Real Nullstellensatz [25, Cor. 4.1.8]; Table 1). *Polynomial  $p \in \mathbb{R}[\mathbf{x}]$  vanishes at every point in the real zero set of  $I \subseteq \mathbb{R}[\mathbf{x}]$  if and only if  $p \in \sqrt[\mathbb{R}]{I}$ . Equivalently,  $\mathbf{I}_{\mathbb{R}}(\mathbf{V}_{\mathbb{R}}(I)) = \sqrt[\mathbb{R}]{I}$  for  $I \subseteq \mathbb{R}[\mathbf{x}]$ .*

With the Nullstellensatz and real Nullstellensatz, we may give an “algebra-geometry dictionary” connecting ideals and algebraic sets :

**Corollary 25** (Algebra-geometry dictionary [30, Thm. 7, p. 183]; Table 1). *Let  $A, B \subseteq \mathbb{C}[\mathbf{x}]$  (respectively,  $\mathbb{R}[\mathbf{x}]$ ). Then  $\mathbf{V}_{\mathbb{C}}(A) \subseteq \mathbf{V}_{\mathbb{C}}(B)$  (respectively,  $\mathbf{V}_{\mathbb{R}}(A) \subseteq \mathbf{V}_{\mathbb{R}}(B)$ ) if and only if  $\sqrt{(A)} \supseteq \sqrt{(B)}$  (respectively,  $\sqrt[\mathbb{R}]{(A)} \supseteq \sqrt[\mathbb{R}]{(B)}$ ).*

The cited result only deals with the complex case, but the argument is identical given the real Nullstellensatz in place of the Nullstellensatz.

### 2.1.5. Inequations and Saturation

Just as the definition of an ideal corresponds to the behavior of equations, we need an operation on ideals that reflects the presence of *inequations*. Note that  $1 \neq 0$  and if two polynomials  $g, h$  are not 0 at some point, then  $gh$  is not zero at the point either. These simple observations motivate the *saturation* of an ideal by a *multiplicative set*:

**Definition 26.** Let  $K$  be a field. A subset  $S$  of  $K[\mathbf{x}]$  is a *multiplicative set* if  $1 \in S$ ,  $0 \notin S$ , and  $gh \in S$  for all  $g, h \in S$ . If  $I \subseteq K[\mathbf{x}]$ , the *saturation* of  $I$  by multiplicative set  $S$  is the set of all  $p \in K[\mathbf{x}]$  such that for some  $s \in S$  we have  $sp \in I$ . We write  $I : S^{\infty}$  to denote the saturation of  $I$  by  $S$ .

We think of the elements of  $I$  as equations and the elements of  $S$  as inequations; i.e., for all  $p \in I$  and  $g \in S$  we include  $p(\mathbf{x}) = 0, g(\mathbf{x}) \neq 0$  in the system of simultaneous equations and inequations. Lemma 28 (2) makes this interpretation precise. The superscript  $\infty$  in the notation refers to the fact that  $S$  is closed under multiplication and typically the elements of  $S$  are arbitrary products of some finite subset of elements.

Note that the saturation  $I : S^\infty$  is an ideal containing  $I$  and equals the entire polynomial ring if and only if  $S$  contains some element of  $I$ .

Usually the saturation adds to or “saturates”  $I$  with new elements, but sometimes the ideal is unchanged:

**Lemma 27.** *If  $I$  is a prime ideal containing no element of  $S$ , then  $I : S^\infty = I$ .*

*Proof.*  $\subseteq$ : By definition we have  $sp \in I$  for some  $s \in S$  if  $p \in I : S^\infty$ , but for  $I$  prime either  $s$  or  $p$  must then belong to  $I$ . If  $I \cap S = \emptyset$ , then  $p \in I$ .

$\supseteq$ : Immediate. □

We make the convention that if  $0 \notin S \subseteq K[\mathbf{x}]$ , then by  $I : S^\infty$  we mean the saturation of  $I$  by the multiplicative set generated by  $S$  (i.e., the set containing 1 and every finite product of elements from  $S$ ). When we write  $I : S^\infty$  we automatically assume that  $I \trianglelefteq K[\mathbf{x}]$  even if we do not explicitly state this. Note that if  $S = \emptyset$ , then  $I : S^\infty = I : \{1\}^\infty = I$ .

Our main interest is the case where  $S = \{s_1, s_2, \dots, s_m\}$  is finite. In this case it is equivalent to saturate by the single element defined by the product of the  $s_j$ . Let  $\Pi S := \prod_j s_j = s_1 s_2 \cdots s_m$ . We write  $I : (\Pi S)^\infty$  to denote the saturation of  $I$  by the multiplicative set  $\{1, \Pi S, (\Pi S)^2, (\Pi S)^3, \dots\}$  that is generated by the single element  $\Pi S$  (note that  $\Pi S$  is not 0 because  $0 \notin S$ ).

The solution set  $\mathbf{V}(I) \setminus \mathbf{V}(\Pi S)$  (points that make all elements of  $I$ , but *no* elements of  $S$ , vanish) is closely related to  $I : S^\infty$ . The following lemma will help prove our central results in Section 3 by making the connection between saturation ideals, equations, and inequations (and hence constructible sets):

**Lemma 28.** *Let  $I \trianglelefteq \mathbb{C}[\mathbf{x}]$  and let  $0 \notin S \subseteq \mathbb{C}[\mathbf{x}]$  be finite. Then*

1.  $I : S^\infty = I : (\Pi S)^\infty$  and
2.  $\mathbf{V}_{\mathbb{C}}(I : S^\infty) = \mathbf{V}_{\mathbb{C}}(I : (\Pi S)^\infty) = \overline{\mathbf{V}_{\mathbb{C}}(I) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S)}^{\mathbb{C}}$ .

*Proof.* 1.  $\subseteq$ : If  $p \in I : S^\infty$ , then  $(s_1^{k_1} s_2^{k_2} \cdots s_m^{k_m})p \in I$  for some  $s_j \in S$  and  $k_j \geq 0$ . Multiplying by appropriate powers of the  $s_j$  to equalize the exponents, we see that  $(\Pi S)^{\max\{k_1, \dots, k_m\}} p \in I$  (recall that ideals are closed under multiplication by anything). Hence  $p \in I : (\Pi S)^\infty$ .

$\supseteq$ : This direction holds because  $\Pi S$  is in the multiplicative set generated by  $S$ .

2. Part 1 implies the first equality. For the last equality:

$\subseteq$ : Let  $\mathbf{a} \in \mathbf{V}_{\mathbb{C}}(I : (\Pi S)^\infty)$ . By definition of Zariski closure, it suffices to show that  $q(\mathbf{a}) = 0$  for every  $q \in \mathbb{C}[\mathbf{x}]$  that vanishes everywhere on  $\mathbf{V}_{\mathbb{C}}(I) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S)$ .

We claim that  $q \in \sqrt{I : (\Pi S)^\infty}$ . This is equivalent to  $(\Pi S)q \in \sqrt{I}$ . (By definition,  $q \in \sqrt{I : (\Pi S)^\infty}$  means that  $(\Pi S)^M q^N \in I$  for some natural numbers  $M, N$ . Multiplying by appropriate powers of  $\Pi S$  and  $q$  as in the proof of part 1, we have  $((\Pi S)q)^{\max\{M, N\}} \in I$ , whence  $(\Pi S)q \in \sqrt{I}$ .) By the Nullstellensatz (Theorem 20), we must prove that  $(\Pi S)q$  vanishes at every point of  $\mathbf{V}_\mathbb{C}(I)$ . But this is true since  $q$  vanishes everywhere on  $\mathbf{V}_\mathbb{C}(I)$  except possibly at some points of  $\mathbf{V}_\mathbb{C}(\Pi S)$  (where  $\Pi S$  vanishes by definition). Hence  $q \in \sqrt{I : (\Pi S)^\infty}$  and so  $q(\mathbf{a}) = 0$ .

$\supseteq$ : Since  $\mathbf{V}_\mathbb{C}(I : (\Pi S)^\infty)$  is  $\mathbb{C}$ -Zariski closed, it already contains  $\overline{\mathbf{V}_\mathbb{C}(I) \setminus \mathbf{V}_\mathbb{C}(\Pi S)}^\mathbb{C}$  if  $\mathbf{V}_\mathbb{C}(I : (\Pi S)^\infty)$  contains the smaller set  $\mathbf{V}_\mathbb{C}(I) \setminus \mathbf{V}_\mathbb{C}(\Pi S)$ . Hence we only need to show that  $p(\mathbf{b}) = 0$  for every  $p \in I : (\Pi S)^\infty$  and  $\mathbf{b} \in \mathbf{V}_\mathbb{C}(I) \setminus \mathbf{V}_\mathbb{C}(\Pi S)$ . This holds because  $(\Pi S)^M p \in I$  for some  $M$  and so  $((\Pi S)^M p)(\mathbf{b}) = 0$ ; we have  $(\Pi S)(\mathbf{b}) \neq 0$  by assumption, so it must be that  $p(\mathbf{b}) = 0$ .  $\square$

Lemma 28 (1) holds for any field. In Lemma 28 (2) we work over  $\mathbb{C}$  because the proof uses the Nullstellensatz. The algebraic version of Lemma 28 (2) is:

**Theorem 29** (Hilbert's Nichtnullstellensatz; Table 1). *Let  $A \subseteq \mathbb{C}[\mathbf{x}]$ , and let  $0 \notin S \subseteq \mathbb{C}[\mathbf{x}]$  be finite. A polynomial  $p \in \mathbb{C}[\mathbf{x}]$  vanishes at every complex solution of  $(A = 0, S \neq 0)$  if and only if  $p \in \sqrt{(A) : S^\infty}$ .*

*Proof.* The  $(\subseteq)$  case in the proof of Lemma 28 (2) (in particular, the argument there showing  $q \in \sqrt{I : (\Pi S)^\infty}$ ) establishes that vanishing at every complex solution of  $(A = 0, S \neq 0)$  implies membership in  $\sqrt{(A) : S^\infty}$ .

For the other direction, if  $p \in \sqrt{(A) : S^\infty}$ , then  $p^N \in (A) : S^\infty$  for some natural number  $N$ . Substitute this  $p^N$  for the  $p$  that appears in the proof of the  $(\supseteq)$  case in Lemma 28 (2). Follow the argument given there to show that  $p^N$ , and hence  $p$ , vanishes at every complex solution  $\mathbf{b}$  of  $(A = 0, S \neq 0)$ .  $\square$

The next result will help prove correctness (Theorem 93) of an important elimination algorithm in Section 4.

**Theorem 30** (Splitting, algebraic case [44, Cor. 5]). *Let  $A \subseteq \mathbb{C}[\mathbf{x}]$ , and let  $0 \notin S \subseteq \mathbb{C}[\mathbf{x}]$  be finite. If  $h \in \mathbb{C}[\mathbf{x}] \setminus \{0\}$ , then*

$$\sqrt{(A) : S^\infty} = \sqrt{(A, h) : S^\infty} \cap \sqrt{(A) : (S \cup \{h\})^\infty}.$$

*Proof.* The claim follows from Theorem 29 and the fact that every point either makes  $h$  vanish or not.  $\square$

In Section 3 we will need the following fact about zero sets of saturations and extending ideals of  $\mathbb{R}[\mathbf{x}]$  to  $\mathbb{C}[\mathbf{x}]$ :

**Lemma 31.** *For  $I \trianglelefteq \mathbb{R}[\mathbf{x}]$  and multiplicative set  $S \subseteq \mathbb{R}[\mathbf{x}]$ ,  $\mathbf{V}_\mathbb{C}(I_\mathbb{C} : S^\infty) \cap \mathbb{R}^n = \mathbf{V}_\mathbb{C}(I : S^\infty) \cap \mathbb{R}^n$ .*

*Proof.*  $\subseteq$ : Clear because  $I : S^\infty \subseteq I_\mathbb{C} : S^\infty$ .

$\supseteq$ : Assume  $\mathbf{a} \in \mathbf{V}_\mathbb{C}(I : S^\infty) \cap \mathbb{R}^n$  and  $p \in I_\mathbb{C} : S^\infty$ . Note that the real and imaginary parts of  $p$  both belong to  $I : S^\infty$ . Hence both vanish at  $\mathbf{a}$  and  $p(\mathbf{a}) = 0$  as needed.  $\square$

## 2.2. Totally Real Varieties: Keeping complex things real

As suggested earlier, real radicals are usually considered computationally intractable [34, 33]. A recurring theme of our work in Sections 3 and 4 is that we can sometimes circumvent the complications of real algebraic geometry by working over  $\mathbb{C}$ . For instance, we would like to use, without loss of precision, complex radical ideals instead of unwieldy real radical ideals. The following is an important condition that, if satisfied, makes this possible.

**Definition 32.** Let  $X \subseteq \mathbb{C}^n$  be a complex variety that is defined over  $\mathbb{R}$ . (That is,  $X = \mathbf{V}_{\mathbb{C}}(A)$  for some  $A \subseteq \mathbb{R}[\mathbf{x}]$ .) We say  $X$  is *totally real* if the real points of  $X$  are  $\mathbb{C}$ -Zariski dense in  $X$ ; i.e.,  $\overline{X(\mathbb{R})}^{\mathbb{C}} = \overline{X \cap \mathbb{R}^n}^{\mathbb{C}} = X$ .

The key intuition about a totally real variety  $X$  is that it has “enough real points” for the real variety  $X(\mathbb{R})$  to closely resemble  $X$ . More precisely, the real points are not contained in a proper complex subvariety of  $X$  and in that sense are algebraically indistinguishable from the strictly complex points. Proposition 38 below characterizes this phenomenon in terms of dimension. If  $X$  is totally real, we can often transfer simpler proofs or more efficient algorithms for  $X$  to the real variety  $X(\mathbb{R})$  [45].

The following fact illustrates that being totally real allows us to replace real radicals with complex radical ideals:

**Proposition 33** ([46]).  $(A) \trianglelefteq \mathbb{R}[\mathbf{x}]$  is real radical (i.e.,  $\sqrt[\mathbb{R}]{(A)} = (A)$ ) if and only if  $(A)$  is radical and  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real.

We need an alternative characterization that is more amenable to computation. To state it, we require the notions of *irreducible component*, *dimension of a variety*, and *nonsingular point*.

**Definition 34.** Let  $X \subseteq \mathbb{C}^n$  be a complex variety (not necessarily defined over  $\mathbb{R}$ ). An irreducible component  $Y$  of  $X$  is a maximal irreducible complex subvariety of  $X$  (i.e.,  $Y$  is not strictly contained in any irreducible complex subvariety of  $X$ ).

**Example 35.** The complex variety  $\mathbf{V}_{\mathbb{C}}(x^2 + y^2) = \mathbf{V}_{\mathbb{C}}((x + iy)(x - iy))$  is not irreducible, but it has two irreducible components defined by  $x + iy = 0$  and  $x - iy = 0$  (these are lines in  $\mathbb{C}^2$ ).

**Definition 36.** Let  $X \subseteq \mathbb{C}^n$  be a nonempty complex variety, and let  $\mathbf{a} \in X$ . We define the (complex) dimension of  $X$  at  $\mathbf{a}$  (written  $\dim_{\mathbf{a}}(X)$ ) to be  $d$  if i) there are distinct irreducible complex subvarieties  $X_1, \dots, X_d$  of  $X$  such that  $\{\mathbf{a}\} \subsetneq X_1 \subsetneq \dots \subsetneq X_d$  and ii) this is the longest such sequence of subvarieties in  $X$ . If there is no such  $X_1$ , we define  $\dim_{\mathbf{a}}(X)$  to be 0. The dimension of  $X$  is the maximal dimension of  $X$  at any of its points.

By the correspondence between prime ideals and irreducible varieties, this definition is equivalent to the maximal length of a chain of prime ideals in the *coordinate ring* of the variety (the quotient of  $\mathbb{C}[\mathbf{x}]$  by the ideal of all polynomials in  $\mathbb{C}[\mathbf{x}]$  that vanish at every complex point of the variety; this ideal is radical) [42, p. 25]. This version is often referred to as the *Krull dimension*.

**Example 37.** If  $X = \{\mathbf{a}_1, \dots, \mathbf{a}_m\}$  is finite, where  $\mathbf{a}_i \in \mathbb{C}^n$ , then  $\dim_{\mathbf{a}_i}(X) = 0$ . If  $X = \mathbf{V}_{\mathbb{C}}(p)$  for some non-constant polynomial  $p \in \mathbb{C}[\mathbf{x}]$ , then  $\dim_{\mathbf{a}}(X) = n - 1$  at all points of  $X$ . The dimension of  $\mathbb{C}^n$  at any point is  $n$ .

If a variety is reducible, then different components can have different dimensions. For instance,  $X = \mathbf{V}_{\mathbb{C}}(x(y - z), y(y - z)) \subseteq \mathbb{C}^3$  is a union of a line ( $x = y = 0$ , dimension 1) and a plane ( $y - z = 0$ , dimension 2). At the intersection point  $(0, 0, 0)$ ,  $X$  has dimension 2.

The same definitions are used, *mutatis mutandis*, for the *real dimension* of a real variety [25, Def. 2.8.1]; we just replace  $\mathbb{C}^n$  with  $\mathbb{R}^n$  and “complex” with “real” in Definition 36. For the prime ideal/Krull dimension version, we use the *real coordinate ring* (the quotient of  $\mathbb{R}[\mathbf{x}]$  by all polynomials over  $\mathbb{R}$  that vanish at the real points of the variety; this ideal is real radical and not just radical). The real dimension could be smaller than the complex if the variety is not totally real (see Example 42), but not otherwise:

**Proposition 38** ([47, Thm. 12.6.1 (3)][48, Thm. 2.4]). *Let  $X \subseteq \mathbb{C}^n$  be an irreducible complex variety defined over  $\mathbb{R}$ . Then  $X$  is totally real if and only if the real dimension of  $X$  equals the complex dimension.*

Whether or not this happens is determined by *nonsingular points*.

**Definition 39.** Let  $X = \mathbf{V}_{\mathbb{C}}(A)$  where  $A = \{p_1, p_2, \dots, p_s\} \subseteq \mathbb{C}[\mathbf{x}]$  and  $(A)$  is a radical ideal; recall  $|\mathbf{x}| = n$ . The Jacobian matrix corresponding to  $A$  is the  $s \times n$ -matrix  $J_A := \left[ \frac{\partial p_i}{\partial x_j} \right]$  whose  $ij$ -th entry is the formal partial derivative of polynomial  $p_i$  with respect to variable  $x_j$ . We say  $\mathbf{a} \in X$  is a nonsingular point of the variety  $X$  if the matrix  $J_A(\mathbf{a})$  (that is,  $J_A$  with  $\mathbf{a}$  substituted for  $\mathbf{x}$ ) has rank equal to  $n - \dim_{\mathbf{a}}(X)$ . (In other words, there is a maximal choice of  $n - \dim_{\mathbf{a}}(X)$  rows of  $J_A(\mathbf{a})$  that form a linearly independent set of  $\mathbb{C}$ -vectors in  $\mathbb{C}^n$ .) Otherwise we say  $\mathbf{a}$  is a singular point of  $X$ .

If  $X = \mathbf{V}_{\mathbb{C}}(A_1) = \mathbf{V}_{\mathbb{C}}(A_2)$  and both  $(A_1)$  and  $(A_2)$  are radical, then nonsingularity of  $\mathbf{a} \in X$  is independent of the choice of  $A_1$  or  $A_2$  in the sense that  $J_{A_1}(\mathbf{a})$  and  $J_{A_2}(\mathbf{a})$  have the same rank. This follows from the Nullstellensatz (which implies in our case that  $(A_1) = (A_2) = \mathbf{I}_{\mathbb{C}}(X)$ ) and [49, Thm. 5.1, p. 32].

**Example 40.** Suppose  $X = \mathbf{V}_{\mathbb{C}}(p)$  for some square-free (has no repeated factors)  $p \in \mathbb{C}[\mathbf{x}]$ ; then  $(p)$  is radical. Moreover, matrix  $J_{\{p\}}(\mathbf{a})$  has the form  $\left[ \frac{\partial p}{\partial x_1}(\mathbf{a}), \dots, \frac{\partial p}{\partial x_n}(\mathbf{a}) \right]$  and either has rank 0 (if all  $\frac{\partial p}{\partial x_i}$  vanish at  $\mathbf{a}$ ; then  $\mathbf{a}$  is singular) or rank 1 =  $n - (n - 1) = n - \dim_{\mathbf{a}}(X)$  (in which case  $\mathbf{a}$  is a nonsingular point of  $X$ ).

While the definition is technical, the intuitive picture is simpler: at a nonsingular point the variety looks “smooth”, while at a singular point we find cusps/sharp corners, self-intersections, etc. For instance, points in the intersection of two irreducible components are always singular [42, Thm. 2.9]. Importantly, smooth points give us a characterization of totally real varieties that we can calculate with:

**Proposition 41** ([47, Thm. 12.6.1 (4)][50, p. 736]). *Let  $X \subseteq \mathbb{C}^n$  be a complex variety defined over  $\mathbb{R}$ . Then  $X$  is totally real if and only if every irreducible component of  $X$  contains a nonsingular real point of  $X$ .*

In light of Proposition 38, the equivalence given by Proposition 41 is not surprising because the real dimension of a variety (defined over  $\mathbb{R}$ ) at a smooth real point is the same as the complex dimension [51, p. 185].

Decomposition into irreducible components [52] and finding smooth points [48] are both well-studied (albeit computationally intensive) problems in algorithmic algebraic geometry, so we can decide if any given complex variety is totally real.

**Example 42.** *As a simple example, the complex variety defined by  $x^2 + y^2 = 0$  is not totally real because the lone real point  $(0, 0)$  is singular, being the intersection of two complex lines  $x + iy = 0, x - iy = 0$  (the irreducible components of  $\mathbf{V}_{\mathbb{C}}(x^2 + y^2)$ ). Alternatively, the partial derivatives  $2x$  and  $2y$  vanish simultaneously at  $(0, 0)$ ; note that  $x^2 + y^2$  is square-free so  $(x^2 + y^2)$  is radical. Nevertheless, the equations  $x = 0, y = 0$  define the same real points and the corresponding singleton set  $\{(0, 0)\}$  is a totally real complex variety (see Proposition 43). In terms of dimension, all this happens because  $\mathbf{V}_{\mathbb{R}}(x^2 + y^2)$  has real dimension 0 but  $\mathbf{V}_{\mathbb{C}}(x^2 + y^2)$  has complex dimension 1. We give further examples in Section 3.*

*In general, totally real varieties contain non-real points as well; the definition only requires that the complex solutions to the defining equations form the smallest algebraic set containing all the real solutions.*

The next result shows more generally than Example 42 that being totally real depends on the complex variety and not only on the set of real points.

**Proposition 43.** *For any  $A \subseteq \mathbb{R}[x]$ , there exists a finite set  $B \subseteq \mathbb{R}[x]$  such that  $\mathbf{V}_{\mathbb{C}}(B)$  is totally real and  $\mathbf{V}_{\mathbb{R}}(A) = \mathbf{V}_{\mathbb{R}}(B)$ .*

*Proof.* By Hilbert's basis theorem there is a finite generating set  $B$  of  $\sqrt[\mathbb{R}]{(A)}$ , the real radical of the ideal generated by  $A$ . The definition of the real radical implies that  $\mathbf{V}_{\mathbb{R}}(A) = \mathbf{V}_{\mathbb{R}}(\sqrt[\mathbb{R}]{(A)}) = \mathbf{V}_{\mathbb{R}}(B)$ .

To show that  $\mathbf{V}_{\mathbb{C}}(B)$  is totally real, we must establish  $\overline{\mathbf{V}_{\mathbb{R}}(B)}^{\mathbb{C}} = \mathbf{V}_{\mathbb{C}}(B)$ . By Lemma 17 (2) it suffices to show that any  $p \in \mathbb{C}[x]$  that vanishes everywhere on  $\mathbf{V}_{\mathbb{R}}(B)$  also vanishes on  $\mathbf{V}_{\mathbb{C}}(B)$  (i.e.,  $\mathbf{I}_{\mathbb{C}}(\mathbf{V}_{\mathbb{R}}(B)) \subseteq \mathbf{I}_{\mathbb{C}}(\mathbf{V}_{\mathbb{C}}(B))$ ; the reverse containment is immediate). Splitting  $p = p_1 + ip_2$  into real and imaginary parts (see the proof of Lemma 19), it follows from the real Nullstellensatz (Theorem 24) that both  $p_1, p_2$  vanish everywhere on  $\mathbf{V}_{\mathbb{R}}(B)$  and so must belong to  $\sqrt[\mathbb{R}]{(B)} = (B)$  (since  $(B) = \sqrt[\mathbb{R}]{(A)}$  is real radical). Thus  $p_1, p_2$  (and consequently  $p$ ) vanish at each point of  $\mathbf{V}_{\mathbb{C}}(B)$ .  $\square$

Following up on Example 42, an illustration of Proposition 43 is  $A = \{x^2 + y^2\}$  and  $B = \{x, y\}$ .

Proposition 43 shows that any real variety has a representation (i.e., some choice of defining polynomial equations) such that the corresponding complex variety is totally real. Theoretically, this suggests that we can always assume our real varieties are

totally real as complex varieties. Computationally, though, this is a nontrivial assumption because it may require computing generators of the real radical to transform the representation if the original equations have “too many complex solutions”/define a complex variety that is not totally real.

However, in our experience most systems of polynomial equations over  $\mathbb{R}$  that arise from applications already define a totally real variety. Indeed, the only counterexamples we are aware of have the form  $\mathbf{V}_{\mathbb{C}}(p)$  where  $p \in \mathbb{R}[\mathbf{x}]$  and  $p(\mathbf{a}) \geq 0$  for all  $\mathbf{a} \in \mathbb{R}^n$  (for instance, sums of squares like in Example 42). The property of being totally real is common and even appears to be the typical situation. Evidence of this is the following theorem, sometimes called the “sign-changing criterion” in the literature:

**Theorem 44** ([47, Thm. 12.7.1]). *Let  $p \in \mathbb{R}[\mathbf{x}]$  be irreducible. Then  $\mathbf{V}_{\mathbb{C}}(p)$  is totally real if and only if there exist  $\mathbf{a}, \mathbf{b} \in \mathbb{R}^n$  such that  $p(\mathbf{a}) > 0$  and  $p(\mathbf{b}) < 0$ .*

In Section 4.4 we discuss the intriguing relationship between this result and efficiently verifying algebraic invariants (Definition 48) of polynomial dynamical systems.

We extend the notion of totally real varieties to constructible sets. (We are not aware of this definition appearing in the literature, but it is only a minor generalization of the concept for varieties.) This will enable us to use results about saturation ideals over  $\mathbb{C}$  (in particular, Lemma 28 (2)) when handling inequations over  $\mathbb{R}$ .

**Definition 45.** *Let  $A, B \subseteq \mathbb{R}[\mathbf{x}]$ . We say that the constructible set  $\mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)$  is a totally real constructible set if  $\overline{\mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)}^{\mathbb{C}} = \overline{\mathbf{V}_{\mathbb{R}}(A) \setminus \mathbf{V}_{\mathbb{R}}(B)}^{\mathbb{C}}$ ; i.e., the real constructible set  $\mathbf{V}_{\mathbb{R}}(A) \setminus \mathbf{V}_{\mathbb{R}}(B)$  is Zariski dense in  $\overline{\mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)}^{\mathbb{C}}$ .*

The main way to obtain a totally real constructible set is to take the set difference of a totally real variety with an arbitrary variety:

**Lemma 46.** *Let  $A, B \subseteq \mathbb{R}[\mathbf{x}]$ . If  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real, then  $\mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)$  is a totally real constructible set.*

*Proof.* By Lemma 17 (2) it suffices to show that if  $p \in \mathbb{C}[\mathbf{x}]$  vanishes on  $\mathbf{V}_{\mathbb{R}}(A) \setminus \mathbf{V}_{\mathbb{R}}(B)$ , then  $p$  vanishes on  $\mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)$ . Let  $\mathbf{a} \in \mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)$  with the goal of showing  $p(\mathbf{a}) = 0$ . Note that for every  $q \in B$  the product  $pq$  vanishes on all of  $\mathbf{V}_{\mathbb{R}}(A)$  since  $p$  vanishes on  $\mathbf{V}_{\mathbb{R}}(A) \setminus \mathbf{V}_{\mathbb{R}}(B)$  and  $q$  vanishes on  $\mathbf{V}_{\mathbb{R}}(B)$ . It follows by Lemma 17 (1) that  $pq$  vanishes on  $\mathbf{V}_{\mathbb{C}}(A)$  because  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real by assumption and so  $\mathbf{V}_{\mathbb{R}}(A)$  is Zariski dense in  $\mathbf{V}_{\mathbb{C}}(A)$ . Since  $\mathbf{a} \in \mathbf{V}_{\mathbb{C}}(A) \setminus \mathbf{V}_{\mathbb{C}}(B)$ , we have  $\tilde{q}(\mathbf{a}) \neq 0$  for some  $\tilde{q} \in B$ . Thus  $p(\mathbf{a})\tilde{q}(\mathbf{a}) = 0$  and  $p(\mathbf{a}) = 0$  as needed.  $\square$

Totally real constructible sets play an important role in Theorem 88 (Section 3), where they give a simpler characterization of one of our main results (Theorem 86).

### 2.3. Lie Derivatives and Algebraic Invariants of Polynomial Vector Fields

A system of ODEs

$$\mathbf{x}' = (x'_1, \dots, x'_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)) = \mathbf{f}(\mathbf{x})$$

defines a *vector field*  $\mathbf{F} : \mathbb{R}^n \rightarrow \mathbb{R}^n$  [53] that describes the motion of a hypothetical object moving according to the given differential equations. (In particular,  $\mathbf{F}(\mathbf{a}) = \mathbf{f}(\mathbf{a}) = (f_1(\mathbf{a}), \dots, f_n(\mathbf{a}))$  is the velocity vector at  $\mathbf{a} \in \mathbb{R}^n$ .) Abusing terminology, we also refer to the corresponding system  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  as a vector field. In this paper we assume that the  $f_i$  are multivariate polynomials over  $\mathbb{R}$ , so  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  satisfies the **Picard-Lindelöf existence and uniqueness theorem for ODEs** at all points of  $\mathbb{R}^n$  [54, Thm. 10.VI]. We write  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  for the set  $\{x'_1 - f_1(\mathbf{x}), \dots, x'_n - f_n(\mathbf{x})\}$ .

The rate of change of a function  $p : \mathbb{R}^n \rightarrow \mathbb{R}$  **along vector  $\mathbf{F}(\mathbf{x})$**  is given by the **Lie derivative**  $\mathcal{L}_{\mathbf{F}}(p)$  of  $p$  with respect to  $\mathbf{F}$  at  $\mathbf{x}$ :

$$\mathcal{L}_{\mathbf{F}}(p)(\mathbf{x}) := \nabla p \cdot \mathbf{F}(\mathbf{x}) = \sum_{i=1}^n \left( \frac{\partial p}{\partial x_i}(\mathbf{x}) \right) f_i(\mathbf{x}). = \left( \sum f_i \frac{\partial}{\partial x_i} \right) p$$

We repeat the procedure on  $\mathcal{L}_{\mathbf{F}}(p)$  to get **higher-order Lie derivatives**  $\mathcal{L}_{\mathbf{F}}^{(2)}(p), \mathcal{L}_{\mathbf{F}}^{(3)}(p), \dots$  (take  $\mathcal{L}_{\mathbf{F}}^{(0)}(p)$  to be  $p$  and  $\mathcal{L}_{\mathbf{F}}^{(n+1)}(p)$  to be  $\mathcal{L}_{\mathbf{F}}(\mathcal{L}_{\mathbf{F}}^{(n)}(p))$ ).

To emphasize the particular ODEs, we sometimes write  $\mathcal{L}_{\mathbf{x}'=\mathbf{f}(\mathbf{x})}(p)$  instead of  $\mathcal{L}_{\mathbf{F}}(p)$ . If the vector field  $\mathbf{F}$  is understood, we simply write  $\dot{p}$  for the Lie derivative  $\mathcal{L}_{\mathbf{F}}(p)$ . As with  $\mathbf{F}$ , we only consider  $p \in \mathbb{R}[\mathbf{x}]$ .

The following is straightforward:

**Lemma 47.** *Lie derivatives with respect to a vector field  $\mathbf{F}$  obey the sum and product rules:  $\mathcal{L}_{\mathbf{F}}(p + q) = \mathcal{L}_{\mathbf{F}}(p) + \mathcal{L}_{\mathbf{F}}(q)$  and  $\mathcal{L}_{\mathbf{F}}(qp) = \mathcal{L}_{\mathbf{F}}(q)p + q\mathcal{L}_{\mathbf{F}}(p)$ .*

Lie derivatives have a close relationship with *invariant sets* of a vector field  $\mathbf{F}$ .

**Definition 48.** *Let  $\mathbf{F}$  be a vector field on  $\mathbb{R}^n$  defined by a system of ODEs  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ . A subset  $X \subseteq \mathbb{R}^n$  is **invariant** with respect to  $\mathbf{F}$  if for every  $\mathbf{x}_0 \in X$  and solution  $\varphi_{\mathbf{x}_0} : D \rightarrow \mathbb{R}^n$  to the initial value problem ( $\mathbf{x}' = \mathbf{f}(\mathbf{x}), \mathbf{x}(0) = \mathbf{x}_0$ ), we have  $\varphi_{\mathbf{x}_0}(t) \in X$  for all  $t \geq 0$  such that  $\varphi_{\mathbf{x}_0}$  is defined. ( $D$  could be a proper open subset of  $\mathbb{R}$  if  $\varphi_{\mathbf{x}_0}$  does not exist for all time.)*

Intuitively, if  $X$  is invariant, then an object starting at any point of  $X$  will remain in  $X$  as the object follows the dynamics described by  $\mathbf{F}$ . We restrict our focus to invariant sets that are real algebraic varieties. The following well-known result (Theorem 50) characterizes such invariant sets. Its statement uses Lie derivatives of all orders as well as the concept of invariant ideals. An ideal  $I \trianglelefteq \mathbb{R}[\mathbf{x}]$  is an **invariant ideal** with respect to  $\mathbf{F}$  if for all  $p \in I$ , the Lie derivative  $\mathcal{L}_{\mathbf{F}}(p)$  belongs to  $I$  (i.e.,  $I$  is **closed under Lie differentiation**, written  $\mathcal{L}_{\mathbf{F}}(I) = \{\mathcal{L}_{\mathbf{F}}(p) \mid p \in I\} \subseteq I$ ).

**Notation 49.** *Given a subset  $A \subseteq \mathbb{R}[\mathbf{x}]$  and polynomial vector field  $\mathbf{F}$ , we write  $(\mathcal{L}_{\mathbf{F}}^*(A))$  (or simply  $(\mathcal{L}^*(A))$  if the vector field is understood) to denote the ideal  $(\mathcal{L}_{\mathbf{F}}^{(k)}(p) \mid p \in A, k \in \mathbb{N}) \trianglelefteq \mathbb{R}[\mathbf{x}]$  generated by the collection of higher Lie derivatives  $\mathcal{L}_{\mathbf{F}}^{(k)}(p)$  for all  $k \geq 0$  and  $p \in A$ . (Note that  $(\mathcal{L}_{\mathbf{F}}^*(A))$  is distinct from  $\mathcal{L}_{\mathbf{F}}(A)$ , which is the set of first Lie derivatives of the elements of  $A$ .)*

Observe that  $(\mathcal{L}_{\mathbf{F}}^*(A))$  is an invariant ideal of  $\mathbf{F}$  by construction because the generating set is closed under Lie differentiation with respect to  $\mathbf{F}$ .



**Theorem 50** (Characterization of algebraic invariants [33, Lemma 5][55, Lemma 2.1]). *Let  $\mathbf{F}$  be a polynomial vector field and let  $X \subseteq \mathbb{R}^n$ . The following are equivalent:*

1.  $X$  is an algebraic invariant set of  $\mathbf{F}$ .
2. For all  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$  such that  $X = \mathbf{V}_{\mathbb{R}}(p_1, \dots, p_m)$ , we have  $\mathcal{L}_{\mathbf{F}}^{(k)}(p_i)(\mathbf{a}) = 0$  for all  $k \geq 0$ ,  $1 \leq i \leq m$ , and  $\mathbf{a} \in X$ .
3. There exists  $I \trianglelefteq \mathbb{R}[\mathbf{x}]$  such that  $X = \mathbf{V}_{\mathbb{R}}(I)$  and  $I$  is an invariant ideal with respect to  $\mathbf{F}$  (i.e.,  $\mathcal{L}_{\mathbf{F}}(I) \subseteq I$ ).

*Proof.* (1)  $\Rightarrow$  (2): Part (ii) of [55, Lemma 2.1] proves that if  $X = \mathbf{V}_{\mathbb{R}}(p_1, \dots, p_m)$  is invariant with respect to  $\mathbf{F}$ , then  $\mathcal{L}_{\mathbf{F}}(p_i) \in \sqrt{(p_1, \dots, p_m)}$  for  $1 \leq i \leq m$ . Hence  $\mathcal{L}_{\mathbf{F}}(p_i)$  vanishes at every point of  $X$ . Reapply part (ii) of [55, Lemma 2.1] to  $\mathbf{V}_{\mathbb{R}}(p_1, \dots, p_m, \mathcal{L}_{\mathbf{F}}(p_1), \dots, \mathcal{L}_{\mathbf{F}}(p_m))$ , which is still the same invariant  $X$ . This shows that second-order Lie derivatives of the  $p_i$  vanish on  $X$ . Continue the process for any order  $k$ . (See also [56, Thm. 1] for a variant of (1)  $\Leftrightarrow$  (2).)

(2)  $\Rightarrow$  (3): Assuming (2), if  $A = \{p_1, \dots, p_m\}$  then we have  $\mathbf{V}_{\mathbb{R}}(p_1, \dots, p_m) = \mathbf{V}_{\mathbb{R}}((\mathcal{L}_{\mathbf{F}}^*(A)))$ ; as noted above,  $(\mathcal{L}_{\mathbf{F}}^*(A))$  is an invariant ideal.

(1)  $\Leftrightarrow$  (3): This is precisely [33, Lemma 5].  $\square$

**Corollary 51.** *Let  $\mathbf{F}$  be a polynomial vector field and let  $X = \mathbf{V}_{\mathbb{R}}(p_1, \dots, p_m)$ . If  $\mathcal{L}_{\mathbf{F}}(p_i) \in (p_1, \dots, p_m)$  for all  $1 \leq i \leq m$ , then  $X$  is an algebraic invariant set of  $\mathbf{F}$ .*

*Proof.* By the sum and product rules (Lemma 47), for  $I = (p_1, \dots, p_m)$  to be an invariant ideal (and hence satisfy statement 3 of Theorem 50) it suffices that the Lie derivatives of the generators  $p_1, \dots, p_m$  belong to  $I$ .  $\square$

The useful Lemma 52 and Proposition 53 below are probably folklore but we know of no specific references.

**Lemma 52.** *If  $I \trianglelefteq \mathbb{R}[\mathbf{x}]$  is an invariant ideal of  $\mathbf{F}$ , then  $\sqrt[m]{I}$  is also an invariant ideal.*

*Proof.* We use all three equivalent statements in Theorem 50. Since  $I$  is an invariant ideal of  $\mathbf{F}$ , we know  $X := \mathbf{V}_{\mathbb{R}}(I)$  is an invariant set by (3)  $\Rightarrow$  (1) in Theorem 50. We have  $X = \mathbf{V}_{\mathbb{R}}(\sqrt[m]{I})$  by Proposition 23 (3b). By Hilbert's basis theorem (Theorem 2), there exist  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$  that generate  $\sqrt[m]{I}$ . Since  $X$  is invariant and  $X = \mathbf{V}_{\mathbb{R}}(p_1, \dots, p_m)$ , (1)  $\Rightarrow$  (2) implies that  $\mathcal{L}_{\mathbf{F}}^{(k)}(p_i)(\mathbf{a}) = 0$  for all  $k \geq 0$ ,  $1 \leq i \leq m$ , and  $\mathbf{a} \in X$ . By the real Nullstellensatz (Theorem 24), each order of Lie derivative  $\mathcal{L}_{\mathbf{F}}^{(k)}(p_i)$  belongs to  $\sqrt[m]{(p_1, \dots, p_m)} = \sqrt[m]{\sqrt[m]{I}}$  (since the  $p_i$  generate  $\sqrt[m]{I}$ )  $= \sqrt[m]{I}$  (Proposition 23 (2)). Hence  $\mathcal{L}_{\mathbf{F}}(\sqrt[m]{I}) \subseteq \sqrt[m]{I}$  as needed.  $\square$

Finally, we show that  $\mathbf{V}_{\mathbb{R}}(\mathcal{L}_{\mathbf{F}}^*(A))$  is the “largest” invariant contained in  $\mathbf{V}_{\mathbb{R}}(A)$ :

**Proposition 53.** *Let  $A \subseteq \mathbb{R}[\mathbf{x}]$  and let  $\mathbf{F}$  be a polynomial vector field. The real variety  $\mathbf{V}_{\mathbb{R}}(\mathcal{L}_{\mathbf{F}}^*(A))$  is invariant with respect to  $\mathbf{F}$ , is contained in  $\mathbf{V}_{\mathbb{R}}(A)$ , and contains every invariant set  $X$  of  $\mathbf{F}$  such that  $X \subseteq \mathbf{V}_{\mathbb{R}}(A)$ .*

*Proof.* The ideal  $(\mathcal{L}_{\mathbf{F}}^*(A))$  is an invariant ideal, so  $\mathbf{V}_{\mathbb{R}}(\mathcal{L}_{\mathbf{F}}^*(A))$  is an invariant set by Theorem 50. We have  $\mathbf{V}_{\mathbb{R}}(\mathcal{L}_{\mathbf{F}}^*(A)) \subseteq \mathbf{V}_{\mathbb{R}}(A)$  by Corollary 25 because  $A \subseteq \mathcal{L}_{\mathbf{F}}^*(A)$ . For the last claim, by Theorem 50 there is an invariant ideal  $I$  such that  $X = \mathbf{V}_{\mathbb{R}}(I)$ . By Corollary 25,  $\sqrt[\mathbb{R}]{I} \supseteq \sqrt[\mathbb{R}]{(A)}$  since  $\mathbf{V}_{\mathbb{R}}(I) \subseteq \mathbf{V}_{\mathbb{R}}(A)$ . Note that  $\sqrt[\mathbb{R}]{I}$  is invariant by Lemma 52 and that  $\sqrt[\mathbb{R}]{I} \supseteq A$  since  $\sqrt[\mathbb{R}]{(A)} \supseteq A$ . Because  $(\mathcal{L}_{\mathbf{F}}^*(A))$  is contained in every invariant ideal containing  $A$ , we have  $(\mathcal{L}_{\mathbf{F}}^*(A)) \subseteq \sqrt[\mathbb{R}]{I}$  and thus by Corollary 25  $\mathbf{V}_{\mathbb{R}}(\mathcal{L}_{\mathbf{F}}^*(A)) \supseteq \mathbf{V}_{\mathbb{R}}(\sqrt[\mathbb{R}]{I}) = \mathbf{V}_{\mathbb{R}}(I) = X$ .  $\square$

#### 2.4. Differential Polynomial Rings and Differential Ideals

Differential algebra extends commutative algebra and algebraic geometry to settings that involve differentiation. This makes the theory a natural choice for exploring algebraic invariants of polynomial dynamical systems. In particular, differential elimination [27] is the algorithmic engine that powers our main results, Theorem 86 in Section 3 and Theorem 98 in Section 4.

Most of the following definitions and basic lemmas are found in standard references [57, 58].

**Definition 54.** An (ordinary) **differential field** is a field  $K$  equipped with a single derivation operator  $'$  that satisfies  $(a + b)' = a' + b'$  and  $(ab)' = a'b + ab'$  for all  $a, b \in K$ .

Examples are standard fields with the trivial zero derivation, the fraction field  $\mathbb{Q}(x)$  of  $\mathbb{Q}[x]$  with derivation given by the quotient rule, and the field of meromorphic functions (quotients of complex analytic functions) with the usual complex derivative [59]. Many of the definitions and results in Sections 2.4, 2.5, and 2.6 apply to more general differential fields, but in this paper we restrict to ordinary differential fields of characteristic 0 (repeated addition of 1 never yields 0; equivalently, the field contains the rational numbers  $\mathbb{Q}$  as a subfield). Henceforth we simply refer to differential fields, with these restrictions being understood even if not stated explicitly. We generally leave the differential field unspecified and assume that it contains all the solutions that interest us (e.g., real analytic functions solving systems of ODEs with rational number coefficients).

**Definition 55.** Let  $K$  be a differential field and let  $x$  be an indeterminate. The differential polynomial ring  $K\{x\}$  with differential indeterminate  $x$  and coefficients  $K$  is the polynomial ring  $K[x = x^{(0)}, x' = x^{(1)}, \dots, x^{(k)}, \dots]$  having infinitely many algebraic indeterminates (named in a suggestive way). The derivation  $'$  on  $K$  extends to all of  $K\{x\}$  by defining  $(x^{(k)})' = x^{(k+1)}$ ,  $(p + q)' = p' + q'$ , and  $(pq)' = p'q + pq'$  for  $p, q \in K\{x\}$ . We call  $x^{(k)}$  the  $k$ -th derivative of  $x$ . The largest such  $k$  appearing for any variable in a differential polynomial is the order of the polynomial. If  $k \geq 1$  we call  $x^{(k)}$  a proper derivative of  $x$ . For uniformity we call  $x = x^{(0)}$  a derivative (just not a proper one.) Differential polynomial rings having several differential indeterminates  $(x_1, x_2, \dots, x_n) = \mathbf{x}$  are defined analogously and are denoted by  $K\{\mathbf{x}\}$ . If an element  $p \in K\{\mathbf{x}\}$  has no proper derivatives of  $\mathbf{x}$  (i.e.,  $p \in K[\mathbf{x}]$ ), we say  $p$  is a nondifferential polynomial.

Intuitively, differential polynomials are standard polynomials except for the presence of variables representing “derivatives” of the (finitely many) differential indeterminates. For instance,  $x(y')^3 + (x'')^2 - 3$  is an order 2 differential polynomial of total degree 4 (from the term  $x(y')^3$ ) in two differential variables  $x, y$ .

The derivatives are formal and do not necessarily represent limits of difference quotients like in calculus; we only require that they obey the sum and product rules. However, just as we can substitute elements of a field for the variables of a nondifferential polynomial, we can substitute differentiable functions into a differential polynomial and treat  $'$  as the usual analytic derivative. For example,  $p := x'' + x \in \mathbb{C}\{\mathbf{x}\}$  is a differential polynomial and  $\sin : \mathbb{C} \rightarrow \mathbb{C}$  is an element of the differential field of complex meromorphic functions (which contains the elements of  $\mathbb{C}$  considered as constant functions). Substituting  $\sin$  for  $x$  and interpreting  $'$  as the usual complex derivative, we find that  $p(\sin) = \sin'' + \sin = -\sin + \sin = 0$ , the zero function (which is the zero element in this differential field).

Note that  $p'(\sin)$  is also 0:  $p' = x''' + x'$  and  $p'(\sin) = \sin''' + (\sin)' = -\cos + \cos = 0$ . More generally, if  $\mathbf{a} \in K^n$  for differential field  $K$  and  $q \in K\{\mathbf{x}\}$ , then  $q'(\mathbf{a}) = (q(\mathbf{a}))'$ . For instance,  $q(\mathbf{a}) = 0$  implies  $q'(\mathbf{a}) = 0$ . Commutativity of differentiation and substitution is analogous to commutativity of polynomial addition and substitution; e.g.,  $(r + s)(\mathbf{a}) = r(\mathbf{a}) + s(\mathbf{a})$ .

#### 2.4.1. Differential Ideals

Just as ideals give us an algebraic way to approach polynomial equations, *differential ideals* correspond to systems of polynomial differential equations.

**Definition 56.** Let  $K$  be a differential field. A **differential ideal** is an ideal  $I \trianglelefteq K\{\mathbf{x}\}$  that is also closed under differentiation:  $p \in I$  implies  $p' \in I$ . A radical differential ideal is a differential ideal that is also a radical ideal in  $K\{\mathbf{x}\}$ .

Let  $A \subseteq K\{\mathbf{x}\}$ . We write  $[A]_K$  or just  $[A]$  to denote the differential ideal generated by  $A$  in  $K\{\mathbf{x}\}$ : the collection of all finite sums  $\sum_{i,j} g_{i,j} p_i^{(j)}$  where  $p_i \in A$ ,  $p_i^{(j)}$  is the  $j$ -th derivative of  $p_i$ , and  $g_{i,j} \in K\{\mathbf{x}\}$  is any differential polynomial.

We write  $(A)_K$  or  $(A)$  to denote the ideal generated by  $A$  in  $K\{\mathbf{x}\}$  viewed as a polynomial ring. (That is,  $(A)$  consists of sums  $\sum_i g_i p_i$  where  $p_i \in A$  and  $g_i \in K\{\mathbf{x}\}$  is any differential polynomial.) If there is risk of confusion, we specify whether  $(A)$  is the ideal generated by  $A$  in  $K\{\mathbf{x}\}$  or in  $K[\mathbf{x}]$ , but context usually makes it clear (for instance, this could only be an issue if  $A \subseteq K[\mathbf{x}]$ ).

The ideal  $(A)$  is defined similarly to  $[A]$ , except that in forming  $(A)$  we do not allow differentiation of the elements of  $A$ . Hence  $(A) \subseteq [A]$  but generally  $(A) \subsetneq [A]$ . Note that  $[A]$  is the minimal differential ideal containing  $A$ .

We remark that invariant ideals with respect to a polynomial vector field  $\mathbf{F}$  are essentially differential ideals in the sense of Definition 56 (the only difference being that  $\mathbb{R}[\mathbf{x}]$  is a polynomial ring and not a differential polynomial ring). By Lemma 47 (sum and product rule for the Lie derivative), the operator  $\mathcal{L}_{\mathbf{F}} : \mathbb{R}[\mathbf{x}] \rightarrow \mathbb{R}[\mathbf{x}]$  is a derivation on the polynomial ring  $\mathbb{R}[\mathbf{x}]$ . Since  $\mathcal{L}_{\mathbf{F}}(I) \subseteq I$  for an invariant ideal  $I$ , such an ideal is a differential ideal with respect to the derivation  $\mathcal{L}_{\mathbf{F}}$ . See Lemma 66 for the converse relating a given differential ideal to an invariant ideal.

Radical differential ideals are theoretically and practically more tractable than general differential ideals. We need the following straightforward properties:

**Lemma 57.** *Let  $K$  be a differential field and let  $I \trianglelefteq K\{\mathbf{x}\}$  be a differential ideal.*

1. *The radical  $\sqrt{I}$  of differential ideal  $I$  in  $K\{\mathbf{x}\}$  is also a differential ideal.*
2.  *$\sqrt{I \cap K[\mathbf{x}]} = \sqrt{I} \cap K[\mathbf{x}]$  as ideals in  $K[\mathbf{x}]$ .*

*Proof.* 1. [59, Lemma 1.15].

2. Immediate from the definition of the radical of an ideal. Note that  $\sqrt{I \cap K[\mathbf{x}]}$  is the radical of  $I \cap K[\mathbf{x}]$  taken in  $K[\mathbf{x}]$  while the  $\sqrt{I}$  is the radical of  $I$  taken in  $K\{\mathbf{x}\}$ .

□

**Remark 58.** By Lemma 57 (1), the radical ideal  $\sqrt{[A]}$  is a differential ideal and hence the smallest radical differential ideal containing  $A$ . This radical differential ideal is often denoted by  $\{A\}$  in the differential algebra literature. Because we work so often with finite sets containing differential polynomials, we do *not* follow this usage and by  $\{p_1, \dots, p_r\}$  we mean the set of differential polynomials with elements  $p_i$ , not the radical differential ideal  $\sqrt{[p_1, \dots, p_r]}$ .

#### 2.4.2. Differential Nullstellensatz and Differential Saturation Ideals

On the “geometric” side, we are interested in zero sets of collections of differential polynomials. In the differential setting, there is no specific field playing the role of  $\mathbb{C}$  that contains solutions to all polynomial differential equations with coefficients in the field. (*Differentially closed fields* [60], named in analogy to algebraically closed fields like  $\mathbb{C}$ , do exist but we do not explicitly need them in this paper. Moreover, there are no known natural examples.) Instead we use the following terminology and notation.

**Definition 59.** *Let  $K$  be a differential field with  $A, B \subseteq K\{\mathbf{x}\}$ . Let  $L$  be any differential field extending  $K$  and let  $\mathbf{a} \in L^n$  satisfy  $p(\mathbf{a}) = 0$  for all  $p \in A$ . Then we say that  $\mathbf{a}$  is a point (or element) of the differential zero set  $\mathbf{V}_{K,\delta}(A)$ . (We write  $\mathbf{V}_\delta(A)$  if  $K$  is understood.) If every point of  $\mathbf{V}_{K,\delta}(A)$  is also a point of  $\mathbf{V}_{K,\delta}(B)$ , we write  $\mathbf{V}_{K,\delta}(A) \subseteq \mathbf{V}_{K,\delta}(B)$  (i.e., for all differential field extensions  $L$  of  $K$ , all solutions of  $A = 0$  in  $L^n$  are solutions of  $B = 0$ .) If also  $\mathbf{V}_{K,\delta}(B) \subseteq \mathbf{V}_{K,\delta}(A)$ , we write  $\mathbf{V}_{K,\delta}(A) = \mathbf{V}_{K,\delta}(B)$  and say that  $A$  and  $B$  have the same differential zero sets (or the same differential solutions). (See Remark 60 about our use of the term “set” in this context.)*

*We also refer to differential zero sets as differential varieties, differential algebraic sets, or Kolchin closed sets (over  $K$ , when we specify a differential field containing the coefficients of the defining differential polynomials).*

*Analogous definitions hold for differential constructible sets (i.e., Boolean combinations of Kolchin closed sets). See, for instance, Example 71.*

**Remark 60.** We could have defined algebraic varieties in an analogous way, having points in any extension field containing the coefficients of the defining polynomials. In that case Hilbert’s Nullstellensatz (Theorem 20) would read as follows: Let  $K$  be a field and let  $A \subseteq K[\mathbf{x}]$ . Then a polynomial  $f \in K[\mathbf{x}]$  belongs to  $\sqrt{(A)}$  if and only if for all fields  $L$  extending  $K$  and all  $\mathbf{a} \in L^n$  such that  $q(\mathbf{a}) = 0$  for all  $q \in A$ , we have  $f(\mathbf{a}) = 0$ . However,  $\mathbb{C}$  is algebraically closed and thus has the property that a system of polynomial equations over  $\mathbb{C}$  has a solution in some extension field if and only if it has a solution in  $\mathbb{C}$  [61]. Hence there is no need to mention extensions in the algebraic case. We merely do so in the differential case because there is no natural analogue of  $\mathbb{C}$  available.

Strictly speaking, the collection of all points of  $\mathbf{V}_{K,\delta}(A)$  is not a set, but rather a proper class [62] containing the solutions of  $A$  from all differential fields extending  $K$ . However, in this paper we never need to treat it as a single completed object and so do not risk set-theoretic difficulties. We simply use  $\mathbf{V}_{K,\delta}(A)$  as shorthand for universal quantification over differential field extensions. The terms “differential zero set” and “differential algebraic set” are harmless abuses of terminology that we use to mirror the corresponding algebraic concepts. We introduce the notion so that we can conveniently state the *differential Nullstellensatz* without a technical detour into differentially closed fields. Like its algebraic counterpart, the differential Nullstellensatz connects algebra and geometry, giving us a correspondence between radical differential ideals and differential varieties. In this paper, the differential Nullstellensatz is mainly used in the form of Theorems 63 and 64. In turn, these will help prove correctness (Theorem 96) of our main algorithm  $\text{RGA}_o$  in Section 4.

**Theorem 61** (Differential Nullstellensatz [44, Thm. 2]; Table 1). *Let  $K$  be a differential field of characteristic 0. Given  $A \subseteq K\{\mathbf{x}\}$ , a differential polynomial  $p \in K\{\mathbf{x}\}$  vanishes at every point of  $\mathbf{V}_{K,\delta}(A)$  if and only if  $p \in \sqrt{[A]}$ . (Here  $\sqrt{[A]}$  is the radical in  $K\{\mathbf{x}\}$  of the differential ideal generated by  $A$ .)*

Phrased differently,  $\sqrt{[A]}$  consists precisely of those differential polynomials over  $K$  that vanish at all differential solutions of  $A$  in any differential extension field of  $K$ .

The differential Nullstellensatz immediately implies a differential analogue of the algebra-geometry dictionary from Corollary 25:

**Corollary 62** (Differential algebra-geometry dictionary; Table 1). *Let  $A, B \subseteq K\{\mathbf{x}\}$ , where  $K$  is a differential field of characteristic 0. Then  $\mathbf{V}_{K,\delta}(A) \subseteq \mathbf{V}_{K,\delta}(B)$  if and only if  $\sqrt{[A]} \supseteq \sqrt{[B]}$ .*

Given an ideal  $I \trianglelefteq K\{\mathbf{x}\}$  and multiplicative set  $S \subseteq K\{\mathbf{x}\}$ , the saturation ideal  $I : S^\infty$  is defined as before by  $I : S^\infty := \{p \in K\{\mathbf{x}\} \mid sp \in I \text{ for some } s \in S\}$ . We have  $I \subseteq I : S^\infty \subseteq [I] : S^\infty$ . If  $I$  is a differential ideal, then  $[I] : S^\infty = I : S^\infty$  is also a differential ideal (called a *differential saturation ideal*) [59, Lemma 1.3].

Much like algebraic saturation ideals, differential saturation ideals represent systems of polynomial differential equations and inequations. (Example 71 and Lemma 94 show that inequations, and not just equations, are important for differential elimination.) The differential Nichtnullstellensatz makes the following important connection between solutions of differential polynomial (in)equations and radicals of differential saturation ideals. (See Theorem 29 for the algebraic version.)

**Theorem 63** (Differential Nichtnullstellensatz [44, Cor. 3]; Table 1). *Let  $K$  be a differential field of characteristic 0, let  $A \subseteq K\{\mathbf{x}\}$ , and let  $0 \notin S \subseteq K\{\mathbf{x}\}$  be finite. A differential polynomial  $p \in K\{\mathbf{x}\}$  vanishes at every solution of  $(A = 0, S \neq 0)$  in every differential extension field of  $K$  if and only if  $p \in \sqrt{[A] : S^\infty}$ .*

The last result in this subsection is a differential analogue of Theorem 30:

**Theorem 64** (Splitting, differential case [44, Cor. 5]). *Let  $K$  be a differential field of characteristic 0, let  $A \subseteq K\{\mathbf{x}\}$ , and let  $0 \notin S \subseteq K\{\mathbf{x}\}$  be finite. If  $h \in K\{\mathbf{x}\} \setminus \{0\}$ , then*

$$\sqrt{[A] : S^\infty} = \sqrt{[A, h] : S^\infty} \cap \sqrt{[A] : (S \cup \{h\})^\infty}.$$

#### 2.4.3. Explicit Form and Lie Derivatives in Differential Ideals

Since we intend to compute algebraic invariants of polynomial vector fields, we naturally focus on differential polynomials of the following form:

**Definition 65.** *Let  $K$  be a differential field. We say a differential polynomial  $p \in K\{\mathbf{x}\}$  of order 1 is in explicit form (or is explicit) if  $p = x'_i + q$  for some  $1 \leq i \leq n$  and  $q \in K[\mathbf{x}]$ . (In particular, no proper derivative appears in  $q$ .) We also say the corresponding differential equation  $x'_i = -q$  is in explicit form. (Note that explicit form is desirable because it essentially replaces a derivative with a polynomial.)*

In the following lemma and thereafter, if  $I \trianglelefteq \mathbb{R}\{\mathbf{x}\}$  we write  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in I$  as shorthand indicating that each element  $x'_i - f_i(\mathbf{x})$  of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  belongs to  $I$ . This property connects differential ideals to invariant ideals and allows us to use differential algebra to find sets invariant with respect to  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ :

**Lemma 66.** *If  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in I \trianglelefteq \mathbb{R}\{\mathbf{x}\}$  and  $I$  is a differential ideal, then for any  $p \in I \cap \mathbb{R}[\mathbf{x}]$  we have  $\mathcal{L}_{\mathbf{x}' = \mathbf{f}(\mathbf{x})}(p) = \dot{p} \in I \cap \mathbb{R}[\mathbf{x}]$ . (In other words,  $I \cap \mathbb{R}[\mathbf{x}]$  is an invariant ideal with respect to  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .)*

*Proof.* We have  $p' \in I$  because  $I$  is a differential ideal. Since  $p \in \mathbb{R}[\mathbf{x}]$ , all monomials  $m_i$  of  $p'$  have the form  $(k_i)(a)x_1^{k_1} \cdots x_i^{k_i-1} x'_i \cdots x_n^{k_n}$  for some  $a \in \mathbb{R}$  and  $k_1, \dots, k_n \in \mathbb{N}$ . (This is one of the summands produced by the product rule applied to a monomial  $m = ax_1^{k_1} \cdots x_i^{k_i} \cdots x_n^{k_n}$  in  $p$ .) Subtracting  $(k_i)(a)x_1^{k_1} \cdots x_i^{k_i-1} \cdots x_n^{k_n} (x'_i - f_i(\mathbf{x}))$  from  $p'$  produces an element of  $I$  (since  $x'_i - f_i(\mathbf{x}) \in I$  by assumption) that replaces the monomial  $m_i$  with  $(k_i)(a)x_1^{k_1} \cdots x_i^{k_i-1} (f_i(\mathbf{x})) \cdots x_n^{k_n}$ . Doing this for each  $x_i$  in monomial  $m$  and summing the output replaces  $m'$  in  $p'$  with the Lie derivative  $\dot{m}$  of  $m$ . It follows from Lemma 47 that substituting  $\mathbf{f}(\mathbf{x})$  for  $\mathbf{x}'$  in  $p'$  this way yields  $\dot{p} \in I \cap \mathbb{R}[\mathbf{x}]$ . (Recall that  $\dot{p} \in \mathbb{R}[\mathbf{x}]$  by definition.)  $\square$

#### 2.5. Rankings and Reduction

As discussed in the introduction, the central aim of this paper is to use *differential elimination* to algorithmically generate algebraic invariants of polynomial dynamical systems. Elimination identifies the core content of a system of polynomial (or differential polynomial) equations by “reducing” some polynomials with respect to others.

In addition to Gaussian elimination, another classic example is long division of one univariate polynomial by another. If the divisor does not evenly divide the dividend, we are left with a nonzero remainder. One way to extend this to multivariate differential polynomials is to use a *differential ranking* (or ranking, if the context is clear) [63]. Differential rankings identify a “leading derivative” in any differential polynomial (e.g., to determine if  $x'$  or  $y''$  is eliminated first) and ensure termination of algorithms by eliminating “large terms” first. Rankings are analogous to *monomial orderings* in the theory of Gröbner bases [30, Sect. 2.2, Def. 1]. However, rankings only apply to individual variables and their derivatives, whereas monomial orderings concern monomials. Many of the following results do not depend on the choice of ranking (the main exceptions are algorithm  $\text{RGA}_o$  on p. 42 and the proof of Theorem 96) and we do not specify a ranking except when necessary.

**Definition 67.** A differential ranking is a well-founded linear ordering  $<$  of derivatives (i.e., every nonempty subset of derivatives has a least element with respect to  $<$ ) that goes up with differentiation and respects  $'$ :  $x^{(k)} < x^{(k+1)}$  and  $x < y$  implies  $x' < y'$ .

There are different rankings for different purposes. Two prominent classes are *elimination rankings* (sort variables lexicographically irrespective of their order; e.g., if  $x < y$ , then  $x^{(k)} < y$  for any  $k$ ) and *orderly rankings* (the derivative of highest order ranks highest, regardless of the base variable; ties in order are decided according to the ordering on the variables). For instance, if  $x < y$  for an orderly ranking, then  $y^{(l)} < x^{(k)}$  if  $l < k$  and  $x^{(k)} < y^{(l)}$  if  $k \leq l$ .

We identify several important components of a differential polynomial with respect to a ranking. These constituents are useful for specifying the control flow of algorithms involving systems of differential polynomials. (For instance, in Section 4 we split cases by either setting a given separant equal to 0 or not.)

**Definition 68.** Fix a differential ranking. The highest-ranking derivative that appears in a non-constant differential polynomial  $p \in K\{\mathbf{x}\} \setminus K$  is the leader of  $p$  (denoted  $l_p$ ). Note that  $l_p$  is a derivative of a single differential indeterminate and does not involve powers or multiple variables. The initial of  $p$  (denoted  $i_p$ ) is the coefficient (viewing  $p$  as a univariate polynomial in  $l_p$  with coefficients in  $K\{\mathbf{x}\}$  that do not involve  $l_p$ ) of the highest power of  $l_p$ . The separant of  $p$  (denoted  $s_p$ ) is the initial of any derivative  $p^{(k)}$  where  $k \geq 1$  (equivalently, the formal partial derivative  $\frac{\partial p}{\partial l_p}$  of  $p$  with respect to  $l_p$ ). Unlike the initial  $i_p$ , the separant  $s_p$  could contain  $l_p$ , but with a lower degree than  $l_p$  has in  $p$ . We do not define leaders, initials, or separants for constants (i.e., elements of the field  $K$ ).

**Example 69.** Fix any differential ranking such that  $x < y$  and let  $p := x(x+1)(y'')^2 + x'y'' + x^4$ . Then

$$\begin{aligned} p' &= 2x(x+1)(y'')(y''') + (x')(x+1)(y'')^2 + x(x')(y'')^2 + x'y''' + x''y'' + 4x^3x' \\ &= (2x(x+1)y'' + x')(y''') + (2x+1)(x')(y'')^2 + x''y'' + 4x^3x'. \end{aligned}$$

The leader  $l_p$  of  $p$  is  $y''$  (and not  $(y'')^2$ ,  $x(x+1)(y'')^2$ , etc.), the initial  $i_p$  is the coefficient  $x(x+1)$  of  $(y'')^2$ , and the separant  $s_p$  is  $2x(x+1)y'' + x'$ .

**Remark 70.** Rankings induce a well-partial-ordering on differential polynomials ( $q < p$  if the leader of  $p$  is greater than the leader of  $q$  or if they are the same and the degree of the leader is greater in  $p$  than in  $q$ ) and, in turn, on sets of polynomials. See [58, Sect. I.10] and [29, Ch. 5] for exact definitions; also see our remarks about the RGA algorithm at the beginning of Section 4.

Rankings for nondifferential polynomial rings  $K[x]$  are simply linear orderings of the variables. The leader, initial, and separant of a polynomial  $p \in K[x]$  are defined as in the differential case.

### 2.5.1. Differential Pseudodivision

Rankings give us a systematic way of generalizing long division via *differential pseudodivision* (or just pseudodivision; we also say *differential pseudoreduction* or *Ritt reduction*). Here we view multivariate differential polynomials as univariate differential polynomials whose coefficients are differential polynomials in one fewer variable. Differential pseudodivision is like univariate long division except the coefficients are differential polynomials and we usually cannot divide without introducing fractions. We give a concrete example before describing the process more formally.

**Example 71.** Choose any differential ranking with  $x < y$  and let  $p = (x+1)(y'') + x^4$  and  $q = (x^2-1)(y')^2$ . Observe that  $y'$  is the leader  $l_q$  of  $q$  and  $y''$  is the highest derivative of  $y'$  in  $p$ . Pseudodividing/pseudoreducing  $p$  by  $q$  consists of first differentiating  $q$  to match the  $y''$  and then “dividing”  $p$  by  $q'$  (in quotation marks because we must premultiply  $p$  by something in order to divide by  $q'$  without fractions). This eliminates  $y''$ . If the resulting pseudoremainder contains  $(y')^2$ , we “divide” the pseudoremainder by  $q$  to obtain another pseudoremainder. The final reduced pseudoremainder does not contain any proper derivative of  $l_q$  and has degree less than 2 in  $l_q$ .

- Differentiate  $q$  to find  $q' = 2(x^2-1)(y')y'' + (2xx')(y')^2$ . (Note that  $y''$  has degree 1 in  $q'$ .)
- Then premultiply  $p$  by  $(x-1)y'$  because  $x+1$  is the coefficient of  $l_{q'} = y''$  in  $p$  and  $2(x+1)(x-1)y' = 2(x^2-1)y' = i_{q'} = s_q$ .
- Now subtract  $(\frac{1}{2})q'$  from  $(x-1)y'p$  to obtain pseudoremainder  $r = (x-1)(y')(x^4) - xx'(y')^2$ .

Notice that  $p, q'$  vanish precisely when either  $p, q', s_q$  all vanish or  $q', r$  vanish and  $s_q$  does not. Using the notation of Definition 59 we have  $\mathbf{V}_{K,\delta}(p, q') = (\mathbf{V}_{K,\delta}(p, q', s_q)) \cup (\mathbf{V}_{K,\delta}(q', r) \setminus \mathbf{V}_{K,\delta}(s_q))$ . In other words, using splitting and differential pseudodivision to eliminate differential polynomials splits differential varieties into a union of differential constructible sets. The same idea appears in Equations 3,4 on p. 45.

- With one more round of premultiplication and subtraction, we can eliminate  $xx'(y')^2$  in  $r$ . Premultiply  $r$  by  $x^2-1$  (this is the initial  $i_q$  of  $q$  and  $xx'$  doesn't



already contain any factors of  $i_q$ ) and subtract  $-xx'q$  to obtain the final answer  $(x^2 - 1)(x - 1)(y')(x^4)$ . This pseudoremainder has no variables that can be eliminated using  $q$ .

In general, let  $p, q$  be differential polynomials ( $q$  non-constant so that leaders, etc., are well defined; in particular,  $q \neq 0$ ). Pseudodividing  $p$  by  $q$  involves the following steps (see [58, Sect. I.9] and [64, Sect. 2.2] for other versions):

$\text{DiffPseudoDiv}(p, q)$ :

1. If a proper derivative of the leader  $l_q$  of  $q$  appears in  $p$ :
  - Let  $(l_q)^{(k)}$ ,  $k \geq 1$ , be the highest proper derivative of  $l_q$  appearing in  $p$ . Compute  $q^{(k)}$ .
  - Let  $r_k := \text{DiffPseudoDiv}(p, q^{(k)})$ . (Note that the initial of  $q^{(k)}$  is the separant  $s_q$  of  $q$  since  $k \geq 1$ .) Then return  $\text{DiffPseudoDiv}(r_k, q)$ .

(Note that the call  $\text{DiffPseudoDiv}(p, q^{(k)})$  must proceed to step 2 because  $(l_q)^{(k)}$  is the leader of  $q^{(k)}$ . Also note that the degree of  $(l_q)^{(k)}$  in  $q^{(k)}$  is 1.)
2. If  $l_q$  (but no proper derivative thereof) appears in  $p$  and the highest power  $d$  of  $l_q$  that appears in  $p$  is at least the degree  $e$  of  $l_q$  in  $q$ :

- Let  $c \in K\{\mathbf{x}\}$  be the coefficient of  $l_q^d$  in  $p$ . Multiply  $p$  by an appropriate factor  $\alpha$  of the initial  $i_q$  of  $q$  to ensure that  $(\alpha)(c)$  is divisible by  $i_q$ . This is called *premultiplication*. It suffices to premultiply  $p$  by  $\alpha := i_q/g$ , where  $g$  is the GCD of  $i_q$  and  $c$ .
- Now subtract the necessary multiple of  $q$  (namely,  $(c/g)(l_q)^{d-e}q$ ) to eliminate  $(l_q)^d$  from  $p$  and obtain a *pseudoremainder*  $r$  whose highest power of  $l_q$  is less than  $d$ :

$$r := (i_q/g)p - (c/g)(l_q)^{d-e}q.$$

Note that  $i_q/g$  and  $c/g$  are both differential polynomials and not fractions because  $g$  divides both  $i_q$  and  $c$  by definition. Also note that the total degree  $\deg(r)$  of  $r$  is at most the sum of the total degrees  $\deg(p)$ ,  $\deg(q)$  of  $p$  and  $q$ . (This is because degrees of products are additive and the degrees of  $i_q/g$  and  $(c/g)(l_q)^{d-e}$  are at most  $\deg(q) - e$  and  $\deg(p) - d + (d - e) = \deg(p) - e$ , respectively. Hence  $\deg(r) \leq \deg(p) + \deg(q) - e$ , but for simplicity we use the larger bound  $\deg(p) + \deg(q)$ .)

- Return  $\text{DiffPseudoDiv}(r, q)$ .

If  $l_q$  (but no proper derivative thereof) appears in  $p$  and  $d < e$ , return  $p$ .

3. If neither  $l_q$  nor any proper derivative of  $l_q$  appears in  $p$ , return  $p$ .

**Remark 72.** The algorithm  $\text{DiffPseudoDiv}$  terminates because step 1 reduces the order of the highest proper derivative of  $l_q$  that appears in  $p$  and step 2 reduces the degree of  $l_q$  in  $p$  to a value below  $e$ . (In particular,  $(l_q)^{(k)}$  is eliminated by the call  $\text{DiffPseudoDiv}(p, q^{(k)})$  because the degree of  $(l_q)^{(k)}$  in  $q^{(k)}$  is  $e = 1$ .)

The same concepts apply in the nondifferential case (i.e., rankings on variables in  $K[\mathbf{x}]$ ). Algebraic pseudodivision is the same process as  $\text{DiffPseudoDiv}$ , except that step 1 never applies because there are no derivatives.

If  $\text{DiffPseudoDiv}(p, q) = r$ , we say  $r$  is the (differential) pseudoremainder resulting from (differential) pseudodivision of  $p$  by  $q$ . The core component of pseudodivision is a single round of premultiplication and subtraction (the first and second items in step 2 of  $\text{DiffPseudoDiv}$ ). We refer to this as a “single step” of pseudodivision and call the result a pseudoremainder even though it is an intermediate element that may be used for further steps of pseudodivision until the final pseudoremainder is reached. See Remark 91 immediately preceding the description of algorithm `Triangulate`.

The next proposition makes explicit the differential-algebraic relationship between  $p, q$ , and  $r$  when  $\text{DiffPseudoDiv}(p, q) = r$ . (The analogue for division of integer  $a$  by nonzero integer  $b$  is the equation  $a = cb + d$ , where  $c$  is the quotient and  $d$  is the remainder.)

**Proposition 73.** *Let  $\text{DiffPseudoDiv}(p, q) = r$ . Then for some  $\tilde{s}$  a product of factors of  $s_q$ ,  $\tilde{i}$  a product of factors of  $i_q$ , and  $\tilde{q} \in [q]$  we have  $(\tilde{s})(\tilde{i})p - \tilde{q} = r$ . In particular, we have  $p \in [q] : \{s_q, i_q\}^\infty$  if  $r$  is 0.*

*In the nondifferential case (or if  $p$  contains no proper derivatives of the leader  $l_q$  of  $q$ ) we have  $(\tilde{i})p - \tilde{q} = r$ , with  $\tilde{q} \in (q)$  now, and  $p \in (q) : \{i_q\}^\infty$  if  $r$  is 0.*

*Proof.* This follows from the form of operations in  $\text{DiffPseudoDiv}$ . If  $p$  contains a highest proper derivative  $(l_q)^{(k)}$  of the leader of  $q$ , then the first intermediate pseudoremainder (from the call  $\text{DiffPseudoDiv}(p, q^{(k)})$  using step 2 is

$$\tilde{r} := (s_q/g)p - (c/g)((l_q)^{(k)})^{d-1}q^{(k)},$$

where  $s_q$  is the initial of  $q^{(k)}$ ,  $d$  is the highest power of  $(l_q)^{(k)}$  in  $p$ ,  $c$  is the coefficient of  $((l_q)^{(k)})^d$  in  $p$ , and  $g$  is the GCD of  $s_q$  and  $c$ . Note that  $\tilde{r}$  has the claimed property. (Consequently, Proposition 73 also applies to a single step of pseudodivision as defined in Remark 72.) By induction on  $k$  and  $d$  we may assume that  $(s_q^*)(i_q^*)\tilde{r} - q^* = r$  for some  $s_q^*$  a product of factors of  $s_q$ ,  $i_q^*$  a product of factors of  $i_q$ , and  $q^* \in [q]$ . Multiplying  $\tilde{r}$  by  $(s_q^*)(i_q^*)$  and subtracting  $q^*$ , the two preceding equations imply that

$$(s_q^*)(s_q/g)(i_q^*)p - ((s_q^*)(i_q^*)(c/g)((l_q)^{(k)})^{d-1}q^{(k)} + q^*) = r,$$

which has the correct form.

Analogous arguments hold for the case that  $p$  contains no proper derivative of  $l_q$  and the nondifferential case. The assertions for  $r = 0$  follow from the definition of a saturation ideal. (Multiply both sides by appropriate factors of  $s_q, i_q$  so that  $\tilde{s}$  and  $\tilde{i}$  become powers of  $s_q, i_q$  and not just arbitrary products of their factors.)  $\square$

Just as the process in Example 71 eliminated  $y''$  and cut the degree of  $y'$  from 2 to 1, more generally we have the following definition:

**Definition 74.** *Given a differential polynomial ring  $K\{\mathbf{x}\}$ , a differential ranking, and  $p, q \in K\{\mathbf{x}\}$ , we say  $p$  is partially reduced with respect to  $q$  if no proper derivative*

of the leader  $l_q$  of  $q$  appears in  $p$ . (In the nondifferential case there are no derivatives and so partial reducedness holds vacuously.) We say  $p$  is reduced with respect to  $q$  if  $p$  is partially reduced with respect to  $q$  and any instances of  $l_q$  in  $p$  have strictly lower degree than the maximum degree of  $l_q$  in  $q$ . (In particular, it is impossible to pseudodivide  $p$  by  $q$  any further.) We say that a subset  $A \subseteq K\{\mathbf{x}\}$  is partially reduced if all members of  $A$  are pairwise partially reduced. We likewise call  $A$  autoreduced if the elements of  $A$  are pairwise reduced. Similarly, we say  $p \in K\{\mathbf{x}\}$  is (partially) reduced with respect to  $A$  if  $p$  is (partially) reduced with respect to each element of  $A$ .

It follows from Remark 72 that the pseudoremainder  $r$  resulting from pseudodividing  $p$  by  $q$  is reduced with respect to  $q$ . After a “single step” of pseudoreduction as defined in Remark 72, the pseudoremainder is not necessarily reduced yet with respect to  $q$ , but it does have degree in  $l_q$  strictly less than that of  $p$ .

## 2.6. Regular Systems

Systems of polynomial equations and inequations can “hide” their information in the sense that deciding the system’s properties may require substantial computation. We focus on structured collections known as *regular systems* and *regular sets* that are easier to analyze. The basic intuition is that “enough” pseudodivision has been done beforehand so that there is no redundancy left to obscure relations between the system’s elements.

**Definition 75** ([44, Def. 1]). *Let  $K$  be a field, let  $A, S \subseteq K[\mathbf{x}]$  be finite with  $0 \notin S$ , and fix a ranking. The equation/inequation pair  $(A = 0, S \neq 0)$  (or simply  $(A, S)$ ) denoting  $f(\mathbf{x}) = 0$  and  $g(\mathbf{x}) \neq 0$  for each  $f \in A$  and  $g \in S$ , respectively, is a regular algebraic system over  $K$  if*

1. *the elements of  $A$  have distinct leaders and*
2.  *$S$  contains the separant of each element of  $A$ .*

**Definition 76** ([44, Def. 7]). *Let  $K$  be a differential field, let  $A, S \subseteq K\{\mathbf{x}\}$  be finite with  $0 \notin S$ , and fix a differential ranking. The equation/inequation pair  $(A = 0, S \neq 0)$  is a regular differential system over  $K$  if*

1.  *$A$  is partially reduced and the elements of  $A$  have distinct leaders and*
2. *the elements of  $S$  are partially reduced with respect to  $A$ , and  $S$  contains the separant of each element of  $A$ .*

Our statement is simpler than the general definition [44] because we restrict ourselves to a single derivation. The “coherence property” in [44] holds vacuously in the ordinary differential case. Definitions 75 (1), 76 (1) force  $A$  to be finite (since there are only  $n$  indeterminates), so there is no loss of generality in assuming  $A$  is finite to begin with.

We often omit “over  $K$ ” when the field is clear from context. Also, nonzero constant multiples in  $S$  are irrelevant because we interpret the elements of  $S$  as inequations.

Thus, for example, if  $s_f := 2x$  is the separant of  $f \in A$  and  $x \in S$ , we take that as satisfying the requirement that  $S$  contain  $s_f$ . Similarly, we do not explicitly show nonzero scalars when listing the elements of  $S$  even if, like in  $x' - xy$ , the separant is 1.

An equation/inequation pair  $(A = 0, S \neq 0)$  from  $K[\mathbf{x}]$  (respectively,  $K\{\mathbf{x}\}$ ) is an *algebraic system* (respectively, *differential system*) if it is not necessarily regular.

While an arbitrary differential system need not be regular, there always exists a decomposition into one or more regular differential systems (Theorem 90). Our main algorithm  $\text{RGA}_o$  from Section 4 yields such a decomposition if the differential equations have explicit form  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  (Theorem 96).

**Definition 77.** Let  $K$  be a differential field and let  $A, S \subseteq K\{\mathbf{x}\}$ . The restrictions of  $A$  and  $S$ , respectively, to  $K[\mathbf{x}]$  are  $A_{K[\mathbf{x}]} := A \cap K[\mathbf{x}]$  and  $S_{K[\mathbf{x}]} := S \cap K[\mathbf{x}]$ . If  $\mathcal{C} := (A = 0, S \neq 0)$  is a differential system, we call  $\mathcal{C}_{K[\mathbf{x}]} := (A_{K[\mathbf{x}]} = 0, S_{K[\mathbf{x}]} \neq 0)$  the restriction of  $\mathcal{C}$  to  $K[\mathbf{x}]$ .

Every regular differential system naturally contains a regular algebraic system.

**Lemma 78.** Let  $\mathcal{C} := (A = 0, S \neq 0)$  be a regular differential system. Then the restriction  $\mathcal{C}_{K[\mathbf{x}]}$  of  $\mathcal{C}$  to  $K[\mathbf{x}]$  is a regular algebraic system (with respect to the ranking inherited from that of  $\mathcal{C}$ ).

*Proof.* The elements of  $A_{K[\mathbf{x}]} \subseteq A$  have distinct leaders, as do all elements of  $A$ . By definition  $S_{K[\mathbf{x}]} = S \cap K[\mathbf{x}]$ ; this implies that the separants of elements of  $A_{K[\mathbf{x}]}$  belong to  $S_{K[\mathbf{x}]}$  because  $S$  contains the separants of elements of  $A \supseteq A_{K[\mathbf{x}]}$  and the separants of elements of  $A_{K[\mathbf{x}]}$  belong to  $K[\mathbf{x}]$ .  $\square$

For some purposes regular systems are not strong enough. In particular, they do not suffice for testing membership in  $(A) : S^\infty$  or  $[A] : S^\infty$ . For that we need the related notion of a *regular set*. We first give the definition, but the connection to saturation ideal membership is contained in Theorem 81. This in turn plays an important role in the proof of Theorem 97 in Section 3.

**Definition 79** ([65, Def. 2]). Let  $K$  be a field, let  $A = \{p_1, \dots, p_m\} \subseteq K[\mathbf{x}]$ , and fix a ranking. For  $1 \leq j \leq m$  let  $A_j = \{p_1, \dots, p_j\}$  and let  $S_j$  be the multiplicative set generated by the initials  $i_1, \dots, i_j$  of  $p_1, \dots, p_j$ . We say  $A$  is a *regular set* (or *regular chain*) if

1. the elements of  $A$  have distinct leaders and
2. for  $2 \leq j \leq m$ , if  $q \in K[\mathbf{x}]$  and  $q$  does not belong to  $(A_{j-1}) : S_{j-1}^\infty$ , then  $i_j q \notin (A_{j-1}) : S_{j-1}^\infty$ .

In the usual terminology of the area,  $A$  is a *triangular set* (having distinct leaders is suggestive of the triangular shape of an invertible matrix in row echelon form) and for  $2 \leq j \leq m$  the initial  $i_j$  of  $p_j$  is *regular* (i.e., a non-zero-divisor) in the quotient ring  $K[\mathbf{x}]/((A_{j-1}) : S_{j-1}^\infty)$ .

### 2.6.1. Key Results for Regular Systems

To round out the necessary mathematical background, we cite three deeper properties of regular systems and sets that we need in Sections 3 and 4. The first is a technical lemma that, in light of the Nullstellensatz, allows us to go back and forth between zero sets and ideals when dealing with regular algebraic systems.

**Lemma 80** (Lazard’s lemma [44, Thm. 1.1 and Thm. 4]). *Let  $(A = 0, S \neq 0)$  be a regular algebraic system. Then  $(A) : S^\infty$  is a radical ideal; i.e.,  $(A) : S^\infty = \sqrt{(A) : S^\infty}$ . Likewise, if  $(A = 0, S \neq 0)$  is a regular differential system, then  $[A] : S^\infty$  is a radical differential ideal; i.e.,  $[A] : S^\infty = \sqrt{[A] : S^\infty}$ .*

The second gives a decision procedure for membership in saturation ideals determined by regular sets.

**Theorem 81** ([65, Prop. 11][66, Thm. 6.1]). *Let  $A$  be a regular set over field  $K$  and let  $S$  be the multiplicative set generated by the initials of the elements of  $A$ . Then for any  $p \in K[\mathbf{x}]$ , we have  $p \in (A) : S^\infty$  if and only if the pseudoremainder of  $p$  with respect to  $A$  is 0 (i.e., the pseudoremainder after reducing as much as possible with respect to all elements of  $A$ ).*

This is analogous to how Gröbner bases decide membership in arbitrary polynomial ideals [30, Sect. 2.6, Cor. 2]. See Theorem 90 for a differential version of Theorem 81.

The last result provides a link between differential and algebraic ideals. This is critical because computation becomes less complicated when we do not have to keep differentiating. Moreover, theory and tools for symbolic computation are more developed in the algebraic case than the differential.

**Lemma 82** (Rosenfeld’s lemma [44, Thm. 3]). *Let  $(A = 0, S \neq 0)$  be a regular differential system. Then for all differential polynomials  $p \in K\{\mathbf{x}\}$  partially reduced with respect to  $A$ , we have  $p \in [A] : S^\infty$  if and only if  $p \in (A) : S^\infty$ .*

**Remark 83.** Since nondifferential polynomials are (trivially) partially reduced with respect to any set, Rosenfeld’s lemma implies that  $([A] : S^\infty) \cap K[\mathbf{x}] = ((A) : S^\infty) \cap K[\mathbf{x}]$ .

The key lesson of Rosenfeld’s lemma is that, given a regular differential system, a partially reduced polynomial  $p \in [A] : S^\infty$  belongs to the differential saturation for essentially algebraic reasons; we do not have to differentiate  $A$  to prove it.

## 3. Regular Differential Systems and Algebraic Invariants of Polynomial Vector Fields

### 3.1. Explicit Regular Differential Systems

We have now covered the background needed for our new method that uses differential elimination to generate algebraic invariants of polynomial dynamical systems. The principal results of the current section are Theorems 86 and 88. Example 3.3 demonstrates these theorems using the well-known Lorenz system.

To abbreviate theorem statements, we make the following definition that specifies our systems of interest. As stated earlier, we restrict to differential polynomials in explicit form (Definition 65) because we want to apply the theory to finding algebraic invariants of polynomial vector fields. Moreover, this application naturally concerns nondifferential inequations (which we can use, for instance, to indicate “unsafe” locations/states).

**Definition 84.** *Let  $K$  be a differential field and let  $\mathcal{C} := (A = 0, S \neq 0)$  be a differential system over  $K$ . We say  $\mathcal{C}$  is an explicit differential system over  $K$  with nondifferential inequations (or just an explicit system with nondifferential inequations if  $K$  and the differential system are understood) if i) all elements of  $A$  that have a proper derivative are in explicit form and ii) all elements of  $S$  are nondifferential polynomials (in which case  $S = S_{K[\mathbf{x}]} = S \cap K[\mathbf{x}]$ ).*

We prove an important technical lemma that, along with Rosenfeld’s lemma (Lemma 82), implies the central result of this section (Theorem 86).

**Lemma 85.** *Let  $\mathcal{C} := (A = 0, S \neq 0)$  be an explicit regular differential system over  $\mathbb{R}$  with nondifferential inequations. Then  $((A) : S^\infty) \cap \mathbb{R}[\mathbf{x}] = ((A) : S^\infty)_{\mathbb{R}[\mathbf{x}]} = (A_{\mathbb{R}[\mathbf{x}]}) : S^\infty$ .*

*Proof.* The reverse containment  $((A) : S^\infty) \cap \mathbb{R}[\mathbf{x}] \supseteq (A_{\mathbb{R}[\mathbf{x}]}) : S^\infty$  is automatic. For the forward containment, we must show that if  $q \in ((A) : S^\infty) \cap \mathbb{R}[\mathbf{x}]$  is a nondifferential polynomial, then  $q \in (A_{\mathbb{R}[\mathbf{x}]}) : S^\infty$ . Each explicit differential polynomial in  $A$  has the form  $x'_i + g_i$  for some variable  $x_i$  and nondifferential polynomial  $g_i$ . Let  $I \subseteq \{1, \dots, n\}$  be the subset of indices  $i$  for which such an  $x'_i + g_i$  belongs to  $A$ . The remaining elements of  $A$  belong to  $A_{\mathbb{R}[\mathbf{x}]}$ . Since  $q \in (A) : S^\infty$  and  $S = S_{\mathbb{R}[\mathbf{x}]}$ , there exist nondifferential polynomials  $r \in S_{\mathbb{R}[\mathbf{x}]}$  and  $h_j \in A_{\mathbb{R}[\mathbf{x}]}$  as well as differential polynomials  $\alpha_j, \beta_i$  such that  $rq = \sum_j \alpha_j h_j + \sum_{i \in I} \beta_i (x'_i + g_i)$ .

We claim that  $q$  vanishes at all complex solutions of the restriction  $\mathcal{C}_{\mathbb{R}[\mathbf{x}]}$ . (In other words,  $q \in \mathbf{I}_{\mathbb{C}}(\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S))$ . Recall that  $\Pi S$  is the product of the (finitely many) elements of  $S$ .) Let  $\mathbf{a} = (a_1, a_2, \dots, a_n) \in \mathbb{C}^n$  be such that  $h(\mathbf{a}) = 0$  and  $s(\mathbf{a}) \neq 0$  for all  $h \in A_{\mathbb{R}[\mathbf{x}]}$  and  $s \in S_{\mathbb{R}[\mathbf{x}]}$  (in particular, the  $h_j$  and  $r$  from the previous paragraph). By Peano’s existence theorem for (complex-valued) ODEs [54, Thm. X, p. 110], there exists a solution  $\mathbf{x}(t)$  to the initial value problem (IVP)  $x'_i(t) = -g_i(\mathbf{x}(t))$ ,  $x_i(0) = a_i$ ,  $1 \leq i \leq n$ . (If  $i \notin I$ , for the IVP simply let  $x'_i(t) = 0$ ,  $x_i(0) = a_i$ . For such  $i$ , the choice  $x'_i(t) = 0$  does not affect the following argument.)

Substituting  $\mathbf{x}(t)$  into the various differential and nondifferential polynomials, we obtain

$$r(\mathbf{x}(t))q(\mathbf{x}(t)) = \sum_j \alpha_j(\mathbf{x}(t))h_j(\mathbf{x}(t)) + \sum_{i \in I} \beta_i(\mathbf{x}(t))(x'_i(t) + g_i(\mathbf{x}(t))).$$

Evaluating at  $t = 0$ , we find

$$r(\mathbf{a})q(\mathbf{a}) = \sum_j (\alpha_j(\mathbf{x}(t))(0))h_j(\mathbf{a}) + \sum_{i \in I} (\beta_i(\mathbf{x}(t))(0))(x'_i(0) + g_i(\mathbf{a})).$$

(We have written  $\alpha_j(\mathbf{x}(t))(0), \beta_i(\mathbf{x}(t))(0)$  instead of  $\alpha_j(\mathbf{a}), \beta_i(\mathbf{a})$  because  $\alpha_j, \beta_i$  are differential polynomials and the function  $\mathbf{x}(t)$  must be substituted into  $\alpha_j, \beta_i$  and differentiated before evaluating at  $t = 0$ . We similarly write  $x'_i(0)$  instead of  $a'_i$ , which is simply 0.) Since  $r(\mathbf{a}) \neq 0$  and  $h_j(\mathbf{a}) = 0$  (by assumption on  $r, h_j$ , and  $\mathbf{a}$ ) and  $x'_i(0) + g_i(\mathbf{a}) = 0$  (because  $\mathbf{x}(t)$  solves the IVP), this proves that  $q(\mathbf{a}) = 0$  and establishes the claim that  $q \in \mathbf{I}_{\mathbb{C}}(\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S))$ .

Lemma 17 (1) now implies that  $q \in \mathbf{I}_{\mathbb{C}}(\overline{\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S)}^{\mathbb{C}})$ . Lemma 28 (2) converts this to  $q \in \mathbf{I}_{\mathbb{C}}(\mathbf{V}_{\mathbb{C}}((A_{\mathbb{R}[\mathbf{x}]})_{\mathbb{C}} : S^{\infty}))$ , which equals  $\sqrt{(A_{\mathbb{R}[\mathbf{x}]})_{\mathbb{C}} : S^{\infty}}$  by the Nullstellensatz (Theorem 20). It follows from the definitions of radical and saturation ideals that  $(\Pi S)^M q^N \in (A_{\mathbb{R}[\mathbf{x}]})_{\mathbb{C}}$  for some  $M, N$ , so by Lemma 4 we have  $q \in \sqrt{(A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}} \subseteq \mathbb{R}[\mathbf{x}]$ . Lazard's lemma (Lemma 80) gives  $\sqrt{(A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}} = (A_{\mathbb{R}[\mathbf{x}]} : S^{\infty})$  since  $\mathcal{C}_{\mathbb{R}[\mathbf{x}]}$  is a regular algebraic system by Lemma 78. This completes the proof.  $\square$

The proof of Lemma 85 illustrates the theme of proving things about real polynomial systems by first going up to the complex numbers (see Definition 32 and the comments preceding it). This strategy also appears in Theorem 88, Section 3.3, and Section 4.4.

We are ready to give the connection between explicit regular differential systems and algebraic invariants. For convenience going forward, we sometimes refer to this result as the “regular invariant theorem”.

**Theorem 86** (Regular invariant theorem). *Let  $\mathcal{C} := (A = 0, S \neq 0)$  be an explicit regular differential system over  $\mathbb{R}$  with nondifferential inequations.*

*Let  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  be a polynomial vector field such that  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^{\infty}$ . Then  $\mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty})$  is an algebraic invariant set of  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .*

*Proof.* By Lemma 50, it suffices to prove that  $(A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}$  is an invariant ideal. Let  $p \in (A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty} \trianglelefteq \mathbb{R}[\mathbf{x}]$  with the goal of showing  $\dot{p} \in (A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}$  (recall that  $\dot{p}$  is the Lie derivative of  $p$  with respect to  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ ). The saturation  $[A] : S^{\infty} \trianglelefteq \mathbb{R}\{\mathbf{x}\}$  is a differential ideal,  $p \in (A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty} \subseteq [A] : S^{\infty}$ , and by assumption  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^{\infty}$ , so by Lemma 66 we obtain  $\dot{p} \in [A] : S^{\infty}$ . As  $\dot{p}$  is nondifferential and thus partially reduced with respect to  $A$ , Rosenfeld's lemma (Lemma 82) yields  $\dot{p} \in (A) : S^{\infty} \trianglelefteq \mathbb{R}\{\mathbf{x}\}$ . Because  $\dot{p} \in \mathbb{R}[\mathbf{x}]$ , Lemma 85 implies  $\dot{p} \in (A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}$  as desired.  $\square$

While it is not necessary that  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A]$  for the regular invariant theorem to hold (see the example in Section 3.3), the hypothesis that  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^{\infty}$  implies that  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  is a differential-algebraic consequence of  $(A = 0, S \neq 0)$  (by the differential Nichtnullstellensatz, Theorem 63.) How we obtain explicit regular differential systems in the first place is a central topic in Section 4.

### 3.2. Alternate Representations from Additional Hypotheses

As we will see in Section 3.3 and Section 4, Theorem 86 opens the door to novel ways of finding and analyzing algebraic invariants of polynomial vector fields. However, it poses the challenge of finding generators of the saturation ideal  $(A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}$

if we want to explicitly write equations for the invariant. While this is possible using Gröbner bases [30, p. 205], it adds complexity to the process (Remark 114). We would much prefer to read off the invariant directly from  $A_{\mathbb{R}[\mathbf{x}]}$  and  $S$ . To explore this possibility, we start by noting that  $\mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty})$  is sandwiched between two more convenient sets. (The following lemma does not depend on regular systems, so we use generic names in place of  $A_{\mathbb{R}[\mathbf{x}]}$  and  $S$ .)

**Lemma 87.** *If  $B, C \subseteq \mathbb{R}[\mathbf{x}]$ , with  $0 \notin C$  finite, then  $\overline{\mathbf{V}_{\mathbb{R}}(B) \setminus \mathbf{V}_{\mathbb{R}}(\Pi C)}^{\mathbb{R}\text{-euc}} \subseteq \mathbf{V}_{\mathbb{R}}((B) : C^{\infty}) \subseteq \mathbf{V}_{\mathbb{R}}(B)$ .*

*Proof.* We have  $\overline{\mathbf{V}_{\mathbb{R}}(B) \setminus \mathbf{V}_{\mathbb{R}}(\Pi C)}^{\mathbb{R}\text{-euc}} = \overline{\mathbf{V}_{\mathbb{R}}(B) \setminus \mathbf{V}_{\mathbb{R}}(\Pi C)}^{\mathbb{R}}$  by Lemma 13 since  $\mathbf{V}_{\mathbb{R}}(B) \setminus \mathbf{V}_{\mathbb{R}}(\Pi C)$  is a real constructible set. (Recall that  $\overline{X}^{\mathbb{R}\text{-euc}}$  denotes the Euclidean closure of a set  $X \subseteq \mathbb{R}^n$ . Though in this case the closures coincide, we invoke the Euclidean topology because of its visually intuitive nature compared to the Zariski topology.)

The containment  $\overline{\mathbf{V}_{\mathbb{R}}(B) \setminus \mathbf{V}_{\mathbb{R}}(\Pi C)}^{\mathbb{R}} \subseteq \mathbf{V}_{\mathbb{R}}((B) : C^{\infty})$  holds because  $\mathbf{V}_{\mathbb{R}}((B) : C^{\infty})$  is a real Zariski closed set containing  $\mathbf{V}_{\mathbb{R}}(B) \setminus \mathbf{V}_{\mathbb{R}}(\Pi C)$  (this follows quickly from the definition of a saturation ideal; see the  $\supseteq$  case in the proof of Lemma 28 (2)). The last containment holds because  $(B) \subseteq (B) : C^{\infty}$ .  $\square$

It is possible that both  $\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}\text{-euc}}$  and  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$ , in addition to  $\mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty})$ , must be invariant under the hypotheses of the regular invariant theorem. We cannot yet prove or disprove this conjecture. However, we *can* prove invariance of the various sets using additional hypotheses that are commonly satisfied (see also Theorem 112, the discussion following it, and Remark 114):

**Theorem 88** (Alternative criteria for regular invariants). *Let  $\mathcal{C} := (A = 0, S \neq 0)$  be an explicit regular differential system over  $\mathbb{R}$  with nondifferential inequations. Let  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  be a polynomial vector field such that  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^{\infty}$ . Then each of the following conditions is sufficient for the indicated set to be an algebraic invariant set of  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .*

1. *If  $\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S)$  is a totally real constructible set, then  $\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}\text{-euc}} = \mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty})$  is invariant.*
2. *If  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$  is irreducible over  $\mathbb{R}$  and  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)$  is nonempty (i.e.,  $\mathcal{C}_{\mathbb{R}[\mathbf{x}]}$  has a real solution), then  $\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}\text{-euc}} = \mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x]}) : S^{\infty}) = \mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x]})$  is invariant.*
3. *Suppose  $[A] \cap \mathbb{R}[\mathbf{x}] = (A_{\mathbb{R}[\mathbf{x}]})$  and for each  $q \in A_{\mathbb{R}[\mathbf{x}]}$  and monomial  $tx'_i$  in the derivative  $q'$ , we have  $t(x'_i - f_i(\mathbf{x})) \in [A]$ . Then  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$  is invariant. (The first condition strengthens Rosenfeld's lemma (Lemma 82) and the second strengthens the requirement  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^{\infty}$  from Theorem 86.)*

*Proof.* 1. The following chain of equalities establishes the claim:



$$\begin{aligned}
\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}\text{-euc}} &= \overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}} && \text{(Lemma 13)} \\
&= \overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{C}} \cap \mathbb{R}^n && \text{(Lemma 19)} \\
&= \overline{\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S)}^{\mathbb{C}} \cap \mathbb{R}^n && \text{(totally real constructible set)} \\
&= \mathbf{V}_{\mathbb{C}}((A_{\mathbb{R}[\mathbf{x}]})_{\mathbb{C}} : S^{\infty}) \cap \mathbb{R}^n && \text{(Lemma 28 (2))} \\
&= \mathbf{V}_{\mathbb{C}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}) \cap \mathbb{R}^n && \text{(Lemma 31)} \\
&= \mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}),
\end{aligned}$$

which is invariant by the regular invariant theorem.

2. Since  $\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}\text{-euc}} \subseteq \mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}) \subseteq \mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$  by Lemma 87, it suffices by the regular invariant theorem to prove equality of the first and last sets. As in part 1, the real Euclidean closure equals the real Zariski closure. Then  $\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}}$  equals  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$  by Lemma 16 since by hypothesis  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$  is irreducible and  $\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)$  is nonempty.
3. As indicated, the hypotheses are chosen to mimic the proof of the regular invariant theorem using  $(A_{\mathbb{R}[\mathbf{x}]})$  instead of  $(A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty}$ . In particular, let  $p \in A_{\mathbb{R}[\mathbf{x}]}$  with the goal of showing  $\dot{p} \in (A_{\mathbb{R}[\mathbf{x}]})$ . (By Lemma 47 it suffices to consider generators of  $(A_{\mathbb{R}[\mathbf{x}]})$ .) Now  $p' \in [A]$  and it follows from the assumption about monomials in derivatives of elements of  $A_{\mathbb{R}[\mathbf{x}]}$  that  $\dot{p} \in [A]$ . (Replace each  $x'_i$  in  $p'$  with  $x'_i - f_i(\mathbf{x}) + f_i(\mathbf{x})$  and distribute. The assumption about monomials implies that  $p' = \dot{p} + \text{an element of } [A]$ .) Since  $\dot{p}$  is nondifferential and by assumption  $[A] \cap \mathbb{R}[\mathbf{x}] = (A_{\mathbb{R}[\mathbf{x}]})$ , we conclude that  $\dot{p} \in (A_{\mathbb{R}[\mathbf{x}]})$ .

□

**Remark 89.** A common way for  $[A] \cap \mathbb{R}[\mathbf{x}] = (A_{\mathbb{R}[\mathbf{x}]})$  to hold is for  $(A_{\mathbb{R}[\mathbf{x}]}) \trianglelefteq \mathbb{R}[\mathbf{x}]$  to be a prime ideal containing no element of  $S$ . Clearly  $(A_{\mathbb{R}[\mathbf{x}]}) \subseteq [A] \cap \mathbb{R}[\mathbf{x}]$ . For the other containment, note that  $[A] \cap \mathbb{R}[\mathbf{x}] \subseteq ([A] : S^{\infty}) \cap \mathbb{R}[\mathbf{x}]$ , which equals  $((A) : S^{\infty}) \cap \mathbb{R}[\mathbf{x}]$  by Rosenfeld's lemma (see Remark 83). In turn,  $((A) : S^{\infty}) \cap \mathbb{R}[\mathbf{x}] = (A_{\mathbb{R}[\mathbf{x}]}) : S^{\infty} = (A_{\mathbb{R}[\mathbf{x}]})$  by Lemma 85, Lemma 27, and the fact that  $(A_{\mathbb{R}[\mathbf{x}]})$  is prime and has no element of  $S$ .

We illustrate Theorems 86 and 88 with a nontrivial example from the physical sciences. The various hypotheses—in spite of their seemingly technical statements—are all satisfied and readily checked.

### 3.3. Example: Lorenz equations

The ODEs  $x' = \sigma(y - x)$ ,  $y' = \rho x - y - xz$ ,  $z' = xy - \beta z$  comprise the famous *Lorenz equations* [67]. Depending on the parameters, this nonlinear system can display widely varying behavior, including chaotic dynamics [68]. The literature also contains studies of algebraic invariants for the Lorenz system [69, 70]. The benchmark collection from [71] considers the parameters  $\sigma = 1$ ,  $\rho = 2$ ,  $\beta = 1$ , yielding the particular equations  $x' = y - x$ ,  $y' = 2x - y - xz$ ,  $z' = xy - z$  that we abbreviate as  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .

Fix an orderly ranking with  $x > y > z$ . We analyze  $A = \{y' - 2x + y + xz, z' - xy + z, 2x^2 - y^2 - z^2\}$ ,  $S = \{x\}$ . Thus  $A_{\mathbb{R}[\mathbf{x}]} = \{2x^2 - y^2 - z^2\}$ . We discuss how we obtained these sets in Section 4.2; for now we take them as given and confirm the hypotheses of our preceding theorems.

We claim  $\mathcal{C} := (A = 0, S \neq 0)$  satisfies the regular invariant theorem (Theorem 86) and each part of Theorem 88. In particular, the strongest conclusion holds:  $\overline{\mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)}^{\mathbb{R}\text{-euc}} = \mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^\infty) = \mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]})$  is invariant with respect to  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .

(Theorem 86 applies) Clearly,  $\mathcal{C}$  is an explicit regular differential system over  $\mathbb{R}$  with nondifferential inequations. Differential polynomials  $y' - 2x + y + xz$  and  $z' - xy + z$  belong to  $A$ , but the presence of  $p := 2x^2 - y^2 - z^2$  implies that  $x' - y + x$  cannot also be in  $A$  lest  $A$  not be partially reduced. However, we can check  $x' - y + x \in [A] : S^\infty$  with standard computer algebra systems (CAS) by confirming  $x(x' - y + x) \in (y' - 2x + y + xz, z' - xy + z, 2x^2 - y^2 - z^2, 4xx' - 2yy' - 2zz' = (2x^2 - y^2 - z^2)')$ , where  $x', y', z'$  are new algebraic indeterminates. That is, we consider ideal membership in the nondifferential polynomial ring  $\mathbb{R}[x, y, z, x', y', z']$ . This establishes  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^\infty$  and Theorem 86 implies that  $\mathbf{V}_{\mathbb{R}}((A_{\mathbb{R}[\mathbf{x}]}) : S^\infty)$  is an algebraic invariant of  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .

(Theorem 88 applies) To check the additional hypotheses in Theorem 88, we first show that  $p = 2x^2 - y^2 - z^2 \in \mathbb{R}[\mathbf{x}]$  is irreducible over  $\mathbb{C}$ . (The weaker condition of irreducibility over  $\mathbb{R}$  suffices for parts 2 and 3 of Theorem 88, but we prefer to prove the stronger result that is helpful for part 1.) In this case it is simple to work directly: reducibility would imply that  $p = (a_1x + b_1y + c_1z)(a_2x + b_2y + c_2z)$  for some  $a_i, b_i, c_i \in \mathbb{C}$ . But distributing and comparing to the coefficients of  $2x^2 - y^2 - z^2$  gives an inconsistent system:  $a_1a_2 = 2, b_1b_2 = c_1c_2 = -1, a_1b_2 + a_2b_1 = a_1c_2 + a_2c_1 = b_1c_2 + b_2c_1 = 0$ . (Inconsistency is conveniently shown by using a CAS to conclude  $1 \in (a_1a_2 - 2, b_1b_2 + 1, c_1c_2 + 1, a_1b_2 + a_2b_1, a_1c_2 + a_2c_1, b_1c_2 + b_2c_1)$ ). Thus the polynomial  $p$  and the variety  $\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]})$  are irreducible over  $\mathbb{C}$ .

1. (Part 1) Since  $\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]})$  only has one irreducible component, we just need to find one real smooth point to prove that  $\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]})$  (and hence  $\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S)$ , by Lemma 46) is totally real. An obvious choice is  $(1, 1, 1) \in \mathbb{R}^3$ , which is smooth because  $(p) = (A_{\mathbb{R}[\mathbf{x}]})$  is prime (and hence radical) and  $(\frac{\partial p}{\partial x}, \frac{\partial p}{\partial y}, \frac{\partial p}{\partial z})$  evaluated at  $(1, 1, 1)$  is  $(4, -2, -2) \neq \mathbf{0}$ . Alternatively,  $\mathbf{V}_{\mathbb{C}}(A_{\mathbb{R}[\mathbf{x}]})$  is totally real by Theorem 44 since  $p$  is irreducible,  $p(1, 0, 0) > 0$ , and  $p(0, 1, 0) < 0$ . It follows that  $\mathcal{C}$  satisfies Theorem 88 (1).
2. (Part 2) Irreducibility over  $\mathbb{C}$  implies irreducibility over  $\mathbb{R}$  and  $(1, 1, 1) \in \mathbf{V}_{\mathbb{R}}(A_{\mathbb{R}[\mathbf{x}]}) \setminus \mathbf{V}_{\mathbb{R}}(\Pi S)$ , so  $\mathcal{C}$  satisfies part 2.
3. (Part 3) Ideal  $(A_{\mathbb{R}[\mathbf{x}]})$  is prime and  $(A_{\mathbb{R}[\mathbf{x}]}) \cap S$  is empty since  $2x^2 - y^2 - z^2$  does not divide  $x$ . Remark 89 thus implies that  $[A] \cap \mathbb{R}[\mathbf{x}] = (A_{\mathbb{R}[\mathbf{x}]})$ .

Lastly, since  $(2x^2 - y^2 - z^2)' = 4xx' - 2yy' - 2zz'$ , we must show that  $4x(x' - y + x), -2y(y' - 2x + y + xz)$ , and  $-2z(z' - xy + z)$  belong to  $[A]$ . This was done above in our proof of  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^\infty$ .

#### 4. The Rosenfeld-Gröbner Algorithm for Algebraic Invariants

A modified version of the Rosenfeld-Gröbner algorithm (RGA) of Boulier et al. [44, 37] is our main tool for differential elimination. We explain the basic ideas behind RGA and then formulate  $\text{RGA}_o$ , our handcrafted version that produces explicit regular differential systems with nondifferential inequations (and hence invariants by the regular invariant theorem). The subscript  $o$  stands for “ordinary” because our setting involves ODEs of a special form.

##### 4.1. $\text{RGA}_o$ for Explicit Systems

Unlike Gröbner basis techniques that output generators of an ideal, RGA uses a differential generalization of *characteristic sets*. Given a ranking, a characteristic set  $C$  of ideal  $I$  is by definition a minimal-rank autoreduced subset of  $I$  (Remark 70). Such a  $C$  is not necessarily unique and might not be a generating set of  $I$ , but  $C$  is nonempty, finite, and pseudoreduces every element of  $I$  to zero [29, p. 175]. The same definition and properties hold for *differential characteristic sets* if we use *differential* rankings, *differential* ideals, and *differential* pseudoreduction. Given a differential ranking and a system of polynomial differential equations and inequations, RGA outputs a finite collection of special differential characteristic sets called *regular differential chains* [72] or simply *chains*; see parts 2, 3 of Theorem 90. (Recall Definition 79 and Theorem 81 for the nondifferential version.) Multiple chains in the output come from case splits over the vanishing of initials and separants. For this reason, RGA typically outputs a “generic” chain (obtained by placing initials and separants with the inequations as much as possible while maintaining consistency) and several more specific ones; see [73] for precise definitions and Section 4.2 for an example that continues the one in Section 3.3.

Regular differential chains contain important “geometric” information. Take an input differential system  $(A = 0, S \neq 0)$  of equations and inequations and perform RGA. Then a differential polynomial  $p$  is zero at all points that satisfy  $(A = 0, S \neq 0)$  if and only if  $p$  is differentially pseudoreduced to zero by each chain that RGA returns given input  $(A = 0, S \neq 0)$  [44, Cor. 3 and Thm. 9]. By the differential Nichtnullstellensatz (Theorem 63), this gives an algorithm for testing *radical* differential saturation ideal membership. This is especially noteworthy because, unlike the algebraic case, general differential ideal membership is undecidable (even for finitely generated differential ideals) [74].

We cite the important properties guaranteed by RGA. Compare Theorem 90 below to Theorems 96 and 98, our main results in this section:

**Theorem 90** ([44, Thm. 9]). *Let  $K$  be a differential field of characteristic 0, let  $A, S \subseteq K\{\mathbf{x}\}$  be finite with  $0 \notin S$ , and fix a differential ranking.*

*Then RGA applied to  $(A, S)$  returns differential systems  $(A_1, S_1), \dots, (A_r, S_r)$  such that*

1.  $\sqrt{[A] : S^\infty} = ([A_1] : S_1^\infty) \cap \dots \cap ([A_r] : S_r^\infty)$ ,
2. *each  $(A_i, S_i)$  is a regular differential system (together with item 3, this makes each  $A_i$  a regular differential chain), and*

3. for all  $p \in K\{\mathbf{x}\}$  and  $1 \leq i \leq r$ , we have  $p \in [A_i] : S_i^\infty$  if and only if the differential pseudoremainder of  $p$  with respect to  $A_i$  is 0.

Strictly speaking, for differential elimination results to be computationally meaningful we must be able to algorithmically add, multiply, divide, differentiate, and check equality with 0. We always tacitly assume this about the finitely many differential field elements that appear during a computation. (Our inputs are finite sets of differential polynomials and so there are only finitely many coefficients; all intermediate elements result from these via arithmetic operations or differentiation.) The assumption is mild because in practice coefficients typically belong to  $\mathbb{Q}$ .

The original authors of RGA gave two versions of the algorithm [37, pp. 162-3] [44, p. 111]. RGA has been implemented in the Maple computer algebra system, where it forms the heart of the `DifferentialAlgebra` package [75]. While this tool is convenient (for example, we use it in the example from Section 4.2), the proprietary nature of Maple impedes a full analysis of the implementation and its performance. As an alternative, Boulier makes freely available the C libraries on which the Maple implementation is based [76]. RGA has proven its versatility by admitting refinements and extensions over the past two decades [77, 78, 44, 79, 80, 81].

Published applications of RGA include parameter estimation for continuous dynamical systems [82, 83] and preprocessing of systems for later numerical solution [84]. The literature contains various case studies from control theory [85], medicine [86], and mathematical biology [64].

We give a modified version of RGA that we call  $\text{RGA}_o$  and that is well-suited for analyzing systems in explicit form. In some ways our algorithm is simpler than those in the literature. In particular, we produce regular differential systems but do not guarantee that they are regular differential chains. This helps us control the form of the output and more easily obtain explicit bounds. Our application to algebraic invariants (culminating in Theorem 98) does not require radical differential ideal membership testing, so regular differential systems suffice for our use case.

First we describe a purely algebraic algorithm, `Triangulate`, that we use as a subroutine in  $\text{RGA}_o$ . The general structure of `Triangulate` mirrors that of  $\text{RGA}_o$  but does not have to deal with derivatives. After presenting both algorithms, proving them correct, and interpreting the output, we analyze their complexity.

Intuitively, `Triangulate` is a recursive divide-and-conquer algorithm that decomposes the radical of a saturation ideal into an intersection of radical ideals determined by regular algebraic systems. (The same high-level description also applies to  $\text{RGA}_o$ , but in that case using *differential* polynomial rings and ideals.) Case splits are based on assigning initials and separants either to the set of equations or inequations.

**Remark 91.** To facilitate the complexity analysis in Section 4.3 (e.g., Theorem 101), we use the following convention in describing `Triangulate` and  $\text{RGA}_o$ : unless stated otherwise, “pseudodivision” refers to a single step of pseudodivision as discussed in Remark 72.

**Triangulate:**

- Choose the ranking  $x_n > x_{n-1} > \cdots > x_1$ . (The particular choice is not essential; we specify a ranking for concreteness.)

- Input: a finite set of polynomials  $A = \{p_1, p_2, \dots, p_m\} \subseteq \mathbb{R}[\mathbf{x}]$  that determines the equations  $p_1 = 0, \dots, p_m = 0$ . Let  $S$  be a finite set of polynomials in  $\mathbb{R}[\mathbf{x}] \setminus \{0\}$  corresponding to inequations. (That is, the input is the algebraic system  $(A = 0, S \neq 0)$ ). We abuse terminology slightly by calling  $A$  itself a set of equations and  $S$  itself a set of inequations.
- Output: Pairs  $(A_1, S_1), \dots, (A_r, S_r)$  such that  $A_1, \dots, A_r \subseteq \mathbb{R}[\mathbf{x}]$ ,  $S_1, \dots, S_r \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$  are finite sets of polynomials and

$$\sqrt{(A) : S^\infty} = ((A_1) : S_1^\infty) \cap \dots \cap ((A_r) : S_r^\infty),$$

where  $(A_i = 0, S_i \neq 0)$  is a regular algebraic system (i.e.,  $A_i$  is triangular and  $S_i$  contains at least the separants of  $A_i$ ).

1. If  $A$  is already triangular and separant  $s_q$  belongs to  $S$  for every  $q \in A$ , then return  $(A, S)$ .

Otherwise, choose the highest-ranking leader  $x$  that either appears in multiple elements of  $A$  or appears in only one  $q \in A$  but  $s_q \notin S$ . We call  $x$  the *target variable* for the pair  $(A, S)$ . Choose some  $q \in A$  that has minimal degree in  $x$  among all elements of  $A$  having leader  $x$ ; if there are multiple such polynomials, pick one that has least total degree among those with minimal degree in  $x$  (again there might be several).

We define two auxiliary sets that we need in steps 2 and 3.

- Let  $\tilde{A} := (A \cup \{i_q, q - i_q x^{\deg_x(q)}\}) \setminus \{q\}$ , where  $q - i_q x^{\deg_x(q)}$  is the *tail* of  $q$  (i.e., what is left of  $q$  if we substitute zero for the initial of  $q$ ).

The notation  $\deg_x(q)$  represents the degree of variable  $x$  in polynomial  $q$ . The set  $\tilde{A}$  is finite; the parentheses around  $A \cup \{i_q, \dots\}$  separate the union from the set difference and do not indicate an ideal. Note that the solutions of  $(\tilde{A} = 0, S \neq 0)$  are the same as those of  $(A \cup \{i_q\} = 0, S \neq 0)$ . This replacement is not technically pseudodivision, but it behaves similarly and in Theorem 93 (correctness of `Triangulate`) and Lemma 94 we analyze this case together with the pseudodivision steps.

Note that  $x$  does not appear in  $i_q$  and  $\deg_x(q - i_q x^{\deg_x(q)}) < \deg_x(q)$ . Also note that the target variable of  $(\tilde{A}, S)$  could still be  $x$  or might have strictly lower rank, but cannot have higher rank than  $x$ .

- Let  $\hat{S} := S \cup \{i_q\}$ . (Note that  $i_q$  is not 0.)

2. If  $x$  appears in multiple elements of  $A$ , choose some  $p \neq q$  that has maximal degree in  $x$  among all elements of  $A$  having leader  $x$ . If there are multiple such polynomials, pick any one that has greatest total degree among those with maximal degree in  $x$  (again there might be several). Now pseudodivide  $p$  by  $q$  and let  $r$  be the resulting pseudoremainder. Update the equations by omitting  $p$  and including  $r$ ; let  $\hat{A} := (A \cup \{r\}) \setminus \{p\}$ .

Note that  $\deg_x(r) < \deg_x(p)$  and  $\deg_x(q) \leq \deg_x(p)$ , but we do not guarantee  $\deg_x(r) < \deg_x(q)$  because we use a single step of pseudodivision (Remark 91) and  $r$  is not necessarily reduced with respect to  $q$ .

Return the union  $\text{Triangulate}(\tilde{A}, S) \cup \text{Triangulate}(\hat{A} \cup \{s_q\}, \hat{S}) \cup \text{Triangulate}(\hat{A}, \hat{S} \cup \{s_q\})$ .

(Note: It is convenient to describe these recursive calls in terms of splitting the computation into different branches. Here in step 2 we have split twice. On one branch we included  $i_q$  with the equations, left the inequations  $S$  unchanged, and called  $\text{Triangulate}$  on the updated system  $(\tilde{A}, S)$ . On the other branch we included  $i_q$  with the inequations, pseudodivided  $p$  by  $q$ , and then split again over including  $s_q$  with the equations or the inequations. This led to  $\text{Triangulate}(\hat{A} \cup \{s_q\}, \hat{S})$  and  $\text{Triangulate}(\hat{A}, \hat{S} \cup \{s_q\})$ , respectively.)

3. If  $q$  is the lone element of  $A$  with leader  $x$ , then we consider two cases:

- (a) If  $s_q \in \hat{S}$ , return the union  $\text{Triangulate}(\tilde{A}, S) \cup \text{Triangulate}(A, \hat{S})$ .
- (b) If  $s_q \notin \hat{S}$ , then  $0 < \deg_x(s_q) < \deg_x(q)$  because if  $x$  does not appear in  $s_q$ , then  $\deg_x(q) = 1$  and  $s_q = i_q \in \hat{S}$ . Pseudodivide  $q$  by  $s_q$  and let  $r$  be the resulting pseudoremainder; note that  $\deg_x(r) < \deg_x(q)$ .

Return the union  $\text{Triangulate}(\tilde{A}, S) \cup \text{Triangulate}((A \cup \{s_q, r\}) \setminus \{q\}, \hat{S}) \cup \text{Triangulate}(A, \hat{S} \cup \{s_q\})$ .

(Note: As in step 2, we say that we have split over including  $i_q$  with the equations or inequations, and then likewise over  $s_q$ .)

**Remark 92.** Though not necessary for correctness of  $\text{Triangulate}$ , in practice it is essential to trim inconsistent branches (i.e., pairs  $(A = 0, S \neq 0)$  that have no solution in the reals) as the algorithm progresses. Discarding such branches does not lose any solutions. Analogously, state-of-the-art versions of Buchberger's algorithm for Gröbner bases avoid redundant  $S$ -polynomial calculations by finding an appropriate subset of the possibilities [30, Sect. 2.10]. A simple optimization of  $\text{Triangulate}$  would be to omit branches that add a nonzero constant to the equations or 0 to the inequations. Likewise, we can spot inconsistency by inspection if a nonzero constant multiple of a polynomial in the equations shows up in the inequations or vice versa. In general, though, it may be necessary to compute a regular chain (see Theorem 81) or a Gröbner basis of  $(B) : S_B^\infty$  to determine if  $(B = 0, S_B \neq 0)$  is solvable in  $\mathbb{C}$  (in  $\mathbb{R}$  would require even more, such as real quantifier elimination [25, Prop. 5.2.2]). These calculations can be expensive, so good judgment is required to pick a strategy for efficiently detecting most of the inconsistent branches. In any case, the worst-case complexity (Theorem 101) is not affected by the lack of consistency checking in  $\text{Triangulate}$  since we must always take into account the possibility of splitting.

We now prove termination and correctness of  $\text{Triangulate}$ . The termination argument is somewhat delicate because many different cases can emerge during a run of the algorithm. To ensure termination we desire a well ordering that strictly decreases in all cases we could encounter. This demands multiple criteria for ranking sets of equations

and inequations and requires a cleverly crafted ordering of the list at the beginning of Theorem 93's proof.

**Theorem 93** (Termination and correctness of `Triangulate`). *Given finite sets of polynomials  $A \subseteq \mathbb{R}[\mathbf{x}]$ ,  $S \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$ , algorithm `Triangulate` terminates and the output  $(A_1, S_1), \dots, (A_r, S_r)$  satisfies*

$$\sqrt{(A) : S^\infty} = ((A_1) : S_1^\infty) \cap \dots \cap ((A_r) : S_r^\infty),$$

where  $A_1, \dots, A_r \subseteq \mathbb{R}[\mathbf{x}]$ ,  $S_1, \dots, S_r \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$ , and  $(A_i = 0, S_i \neq 0)$  is a regular algebraic system (i.e.,  $A_i$  is triangular and  $S_i$  contains at least the separants of  $A_i$ ).

*Proof.* We first prove termination. This follows from a partial well ordering on pairs  $(B, S_B)$  where  $B, S_B \subseteq \mathbb{R}[\mathbf{x}]$  are finite sets of polynomials. Given such pairs  $(B_1, S_{B_1})$ ,  $(B_2, S_{B_2})$ , we say that  $(B_2, S_{B_2})$  has higher rank than  $(B_1, S_{B_1})$  and write  $(B_1, S_{B_1}) < (B_2, S_{B_2})$  if one of the following conditions holds. (Recall that the target variable of pair  $(B, S_B)$  is the variable  $x$  of highest rank such that either  $B$  contains multiple elements having leader  $x$  or  $B$  has only one element  $p$  with leader  $x$  and the separant  $s_p$  of  $p$  does not belong to  $S_B$ .)

1. The target variable  $x$  of  $(B_2, S_{B_2})$  has higher rank than the target variable  $y$  of  $(B_1, S_{B_1})$ .
2. The two pairs have the same target variable  $x$ , but  $x$  appears with strictly larger degree in  $B_2$ .
3. The target variable and maximal degree in the target are the same for both pairs, but  $B_2$  has strictly more elements with maximal degree in the target.
4. All the previous quantities are the same for both pairs, but  $B_2$  has strictly more elements whose leader is the target.
5. All the previous quantities are the same for both pairs, but an element of  $B_2$  with minimal nonzero degree in the target variable  $x$  has strictly higher degree in  $x$  than the corresponding element of  $B_1$ .

More formally, we are using  $\{1, 2, \dots, n\} \times \mathbb{N}^4$  ordered lexicographically with the standard orders on  $\{1, 2, \dots, n\}$  and  $\mathbb{N}$ . The subscript of the target variable belongs to  $\{1, 2, \dots, n\}$  and the four copies of  $\mathbb{N}$  represent the highest degree in the target variable, the number of elements with the highest degree in the target, the number of elements having the target as their leader, and the minimal degree in the target, respectively.

`Triangulate` recursively transforms the input pair  $(A, S)$  into more refined pairs via finitely many splitting and pseudodivision operations. Thus to show termination it suffices to show that each recursive call in the body of `Triangulate` acts on a pair of strictly lower rank than that of  $(A, S)$ .

We first note that in all cases the target variable can only remain the same or decrease. This is because we never remove anything from the inequations and the only variables that can appear in the elements added to the equations are the original target variable or variables of lower rank. If the target variable remains the same, then the

maximal degree in the target must remain the same or decrease because anything we add to the equations has degree in the target that is strictly less than the original maximal degree in that variable. Hence we must show that one of the remaining quantities decreases if the quantities that lexicographically precede it stay the same.

- Step 2 of **Triangulate** deals with the case that  $A$  has multiple elements with leader  $x$ . First we produce the pair  $(\tilde{A}, S)$ , where  $\tilde{A} := (A \cup \{i_q, q - i_q x^{\deg_x(q)}\}) \setminus \{q\}$ ,  $x$  is the target variable of  $(A, S)$ , and  $q$  is an element of  $A$  having leader  $x$  and minimal degree in  $x$ . To see that  $(\tilde{A}, S) < (A, S)$ , we observe that
  - If  $\deg_x(q)$  is maximal as well as minimal, then the number of elements of maximal degree in  $x$  decreases because we removed  $q$ , the initial  $i_q$  does not contain  $x$  and  $\deg_x(q - i_q x^{\deg_x(q)}) < \deg_x(q)$ .
  - If  $\deg_x(q)$  is not maximal, then the number of elements of maximal degree in  $x$  stays the same. If  $x$  does not appear in  $q - i_q x^{\deg_x(q)}$ , then the number of elements with  $x$  as the leader decreases (we replaced  $q$  with  $q - i_q x^{\deg_x(q)}$  and  $x$  does not appear in  $i_q$ ). If  $x$  does appear in  $q - i_q x^{\deg_x(q)}$ , then the number of elements with  $x$  as the leader stays the same, but the minimal degree in  $x$  decreases (because  $\deg_x(q - i_q x^{\deg_x(q)}) < \deg_x(q)$ ).

Step 2 also produces the pairs  $(\hat{A} \cup \{s_q\}, \hat{S})$  and  $(\hat{A}, \hat{S} \cup \{s_q\})$ , where  $\hat{S} := S \cup \{i_q\}$  and  $\hat{A} := (A \cup \{r\}) \setminus \{p\}$  for  $p \neq q$  having maximal degree in  $x$  and  $r$  the pseudoremainder upon pseudodividing  $p$  by  $q$ . The number of elements having maximal degree in  $x$  decreases because  $r$  and  $s_q$  have strictly lower degree in  $x$  than  $p$  and we remove  $p$ .

- Step 3 of **Triangulate** deals with the case that  $q$  is the lone element of  $A$  with leader  $x$ .
  - If  $s_q \in \hat{S}$ , then step 3 produces the pair  $(A, \hat{S})$ . (We already have shown that  $(\tilde{A}, S) < (A, S)$ , so here we just look at  $(A, \hat{S})$ ). In this situation the target variable must decrease because  $q$  is the only element of  $A$  with leader  $x$  and now  $s_q$  belongs to the inequations (so by definition  $x$  is no longer a target variable).
  - If  $s_q \notin \hat{S}$ , then step 3 produces the pairs  $((A \cup \{s_q, r\}) \setminus \{q\}, \hat{S})$  and  $(A, \hat{S} \cup \{s_q\})$ , where  $x$  appears in  $s_q$  and  $r$  is the pseudoremainder upon pseudodividing  $q$  by  $s_q$ . In the first instance,  $((A \cup \{s_q, r\}) \setminus \{q\}, \hat{S}) < (A, S)$  because either the target variable decreases or it remains the same and the maximal degree in  $x$  decreases (since  $\deg_x(r) < \deg_x(q)$ ,  $\deg_x(s_q) < \deg_x(q)$ , and  $q$  was the lone element of  $A$  with leader  $x$ ). In the second,  $(A, \hat{S} \cup \{s_q\}) < (A, S)$  because the target variable must decrease ( $q$  was the only element of  $A$  with leader  $x$  and now  $s_q$  belongs to the inequations).

This proves termination. We now establish the properties of the output systems  $(A_i = 0, S_i \neq 0)$ .

Each  $A_i$  is triangular and  $S_i$  contains the separants of all elements of  $A_i$  (i.e.,  $(A_i = 0, S_i \neq 0)$  is a regular algebraic system) because this is the base case that



returns an explicit answer instead of a recursive call. (Note that  $0 \notin S_i$  because we only ever add  $i_q$  or  $s_q$  to the inequations, and these are never the zero polynomial.)

Lastly, we show that the ideals  $(A_i) : S_i^\infty$  decompose  $\sqrt{(A) : S^\infty}$  as claimed. Observe that  $\sqrt{(A_1) : S_1^\infty} \cap \cdots \cap \sqrt{(A_r) : S_r^\infty} = ((A_1) : S_1^\infty) \cap \cdots \cap ((A_r) : S_r^\infty)$  because each  $(A_i) : H_i^\infty$  is radical by Lazard's lemma (Lemma 80). Each operation during a run of `Triangulate` converts a system  $(B = 0, S_B \neq 0)$  into another system  $(B_1 = 0, S_{B_1} = 0)$  or two systems  $(B_1 = 0, S_{B_1} = 0), (B_2 = 0, S_{B_2} = 0)$ . By induction on the number of splitting and pseudodivision operations during a run of `Triangulate`, it suffices to confirm at each step that  $\sqrt{(B) : S_B^\infty} = \sqrt{(B_1) : S_{B_1}^\infty}$  or  $\sqrt{(B) : S_B^\infty} = \sqrt{(B_1) : S_{B_1}^\infty} \cap \sqrt{(B_2) : S_{B_2}^\infty}$ .

1. (Splitting over an initial or separant) Steps 2 and 3 both split the computation into branches, one where the initial  $i_q$  or separant  $s_q$  of a chosen polynomial  $q \in B$  is included with the equations  $B$  and one where it is included with the inequations  $S_B$ . Thus by Theorem 30, we have, respectively,

$$\sqrt{(B) : S^\infty} = \sqrt{(B, i_q) : S^\infty} \cap \sqrt{(B) : (S_B \cup \{i_q\})^\infty}$$

or

$$\sqrt{(B) : S^\infty} = \sqrt{(B, s_q) : S^\infty} \cap \sqrt{(B) : (S_B \cup \{s_q\})^\infty}.$$

2. (Pseudodivision) Steps 2 and 3b of `Triangulate` replace some  $g \in B$  with its pseudoremainder  $r_g$  upon pseudodividing by some  $h$ , where  $h \in B$  and the initial  $i_h \in S_B$ . (In step 2,  $g$  is  $p$  and  $h$  is  $q$  while in step 3b,  $g$  is  $q$  and  $h$  is  $s_q$ . In the latter case, the initial  $i_{s_q}$  of  $s_q$  is a nonzero constant multiple of  $i_q$  (which *does* belong to the inequations  $\hat{S}$ ) because separants are partial derivatives with respect to the leader.)

We must show

$$\sqrt{(B) : S_B^\infty} = \sqrt{((B \cup \{r_g\}) \setminus \{g\}) : S_B^\infty}. \quad (1)$$

By Proposition 73 (which makes explicit the relationship between a pseudoremainder and the original polynomials) there exist  $\alpha \in \mathbb{R}[\mathbf{x}]$  and a product  $\tilde{i}$  of factors of  $i_h$  such that  $(\tilde{i})g - \alpha h = r_g$ . Thus for any point  $\mathbf{a} \in \mathbb{C}^n$  we see that  $\mathbf{a}$  causes both  $g$  and  $h$  to vanish but not  $i_h$  if and only if  $\mathbf{a}$  causes  $h$  and  $r_g$  to vanish but not  $i_h$ . (If  $i_h(\mathbf{a}) \neq 0$ , then  $\tilde{i}(\mathbf{a}) \neq 0$  because  $\tilde{i}$  is a product of factors of  $i_h$ .) Symbolically,

$$\mathbf{V}_{\mathbb{C}}(B) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S_B) = \mathbf{V}_{\mathbb{C}}(B \cup \{r_g\} \setminus \{g\}) \setminus \mathbf{V}_{\mathbb{C}}(\Pi S_B). \quad (2)$$

(Similar reasoning applies to Equation 4 in the proof of Theorem 94.) Then Equation 1 follows by Theorem 29 (Hilbert's Nichtnullstellensatz, which links

radicals of saturation ideals to solutions of systems of equations and inequations).

Technically we don't perform pseudodivision when converting  $(A \cup \{i_q\}, S)$  to  $(\tilde{A}, S)$ , but the outcome is analogous. (As noted in step 1 on p. 37, the solutions of  $(\tilde{A} = 0, S \neq 0)$  are the same as those of  $(A \cup \{i_q\} = 0, S \neq 0)$ . See also the proof of Lemma 94 on p. 45.) Hence

$$\sqrt{(A \cup \{i_q\}) : S^\infty} = \sqrt{((A \cup \{i_q, q - i_q x^{\deg_x(q)}\}) \setminus \{q\}) : S^\infty} = \sqrt{(\tilde{A}) : S^\infty}.$$

This proves the claimed properties of `Triangulate`.  $\square$

We can now describe the full  $\text{RGA}_o$  algorithm.  $\text{RGA}_o$  eliminates ODEs in explicit form using differential pseudodivision; moreover, no new ODEs are introduced. Between pseudodivision steps, we apply `Triangulate` to the nondifferential elements of the current system. The computation recursively splits into multiple branches that yield different parts of the desired differential radical decomposition.

Importantly, the eliminated ODEs still belong to all differential saturation ideals that appear during the computation. This is ensured by a technical assumption on  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  that is given in the input description below. (The correctness proof for  $\text{RGA}_o$ , Theorem 96, shows how the assumption accomplishes this.) Without the assumption, the operations of  $\text{RGA}_o$  could produce differential saturation ideals that do not satisfy the hypotheses of the regular invariant theorem (Theorem 86). In turn, that would break the connection between  $\text{RGA}_o$  and algebraic invariants that we establish in Theorem 98.

$\text{RGA}_o$ :

- Choose the *orderly* differential ranking such that  $x_n > x_{n-1} > \dots > x_1$ . (We will use the fact that the ranking is orderly to prove correctness, but the particular sequence of variables is not essential.)
- Input: Let  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  be a polynomial vector field. Let  $A = \{\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}), p_1, p_2, \dots, p_m\}$  be a finite set where  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  is a subset of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  and the  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$  are nondifferential polynomials. Also, we have a finite set of nondifferential polynomials  $S \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$ . As in `Triangulate`, the elements of  $A$  correspond to equations and the elements of  $S$  to inequations. Lastly, the “technical assumption” mentioned above: we assume that for each member  $x' - f(\mathbf{x})$  of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  we either have  $x' - f(\mathbf{x}) \in A$  (equivalently,  $x' - f(\mathbf{x}) \in \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ ) or

$$s(x' - f(\mathbf{x})) = \beta(\mathbf{x}) + \sum_j \gamma_j(\mathbf{x})(x'_j - f_j(\mathbf{x}))$$

for some  $s \in S, \beta(\mathbf{x}) \in [A \cap \mathbb{R}[\mathbf{x}]] \subseteq \mathbb{R}\{\mathbf{x}\}, \gamma_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}], x_j < x$ , and  $x'_j - f_j(\mathbf{x}) \in A$ . (This is a specific case of  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A] : S^\infty$ . The key point is that for all  $x' - f(\mathbf{x}) \in \mathbf{x}' - \mathbf{f}(\mathbf{x})$ , either  $x' - f(\mathbf{x})$  explicitly belongs to the equations  $A$  or  $x' = f(\mathbf{x})$  is implied by  $A$  and the inequations  $S$ .)

- Output: Pairs  $(A_1, S_1), \dots, (A_r, S_r)$  such that  $A_1, \dots, A_r \subseteq \mathbb{R}\{\mathbf{x}\}$ ,  $S_1, \dots, S_r \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$  are finite sets and

$$\sqrt{[A] : S^\infty} = ([A_1] : S_1^\infty) \cap \dots \cap ([A_r] : S_r^\infty),$$

where each  $(A_i = 0, S_i \neq 0)$  is a regular differential system. That is,  $A_i$  is partially reduced (no element contains a proper derivative of the leader of another element) and triangular (no two elements have the same leader), and  $S_i$  is partially reduced with respect to  $A_i$  and contains at least the separants of  $A_i$ . Moreover, the elements of  $A_i$  containing proper derivatives form a subset of  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ , and for each  $x' - f(\mathbf{x}) \in \mathbf{x}' - \mathbf{f}(\mathbf{x})$  and  $1 \leq i \leq r$  we either have  $x' - f(\mathbf{x}) \in A_i$  or

$$\hat{s}(x' - f(\mathbf{x})) = \hat{\beta}(\mathbf{x}) + \sum_j \hat{\gamma}_j(\mathbf{x})(x'_j - f_j(\mathbf{x}))$$

for some  $\hat{s} \in S_i$ ,  $\hat{\beta}(\mathbf{x}) \in [A_i \cap \mathbb{R}[\mathbf{x}]] \leq \mathbb{R}\{\mathbf{x}\}$ ,  $\hat{\gamma}_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ ,  $x_j < x$ , and  $x'_j - f_j(\mathbf{x}) \in A_i$ . (The proof of Theorem 96 shows that the technical assumption on  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  at the start is preserved by each operation of  $\text{RGA}_o$ , and hence holds of the output.)

1. If  $A$  is already partially reduced and triangular, and separant  $s_q$  belongs to  $S$  for every  $q \in A$ , then return  $(A, S)$ .
2. If  $A$  is not triangular or separant  $s_q \notin S$  for some nondifferential  $q \in A$ , compute  $\text{Triangulate}(A \cap \mathbb{R}[\mathbf{x}], S) = \text{Triangulate}(\{p_1, \dots, p_m\}, S)$ . (Recall the  $p_i$  are the nondifferential elements of  $A$ . Also, an element of the form  $x'_j - f_j(\mathbf{x})$  has separant 1, so as usual we assume such a separant belongs to the inequations  $S$ .) This yields a finite collection of regular algebraic systems involving only nondifferential polynomials. Return the union  $\bigcup_{(B, S_B)} \text{RGA}_o(B \cup \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}), S_B)$  over all  $(B, S_B)$  returned by  $\text{Triangulate}(\{p_1, \dots, p_m\}, S)$ . (That is, for each such  $(B, S_B)$ , re-include with the equations  $B$  the elements of  $A$  that contain proper derivatives and call  $\text{RGA}_o$  on the resulting system. This produces a finite collection of differential systems; take the union of all these collections.)
3. If  $A$  is triangular and  $s_q \in S$  for all  $q \in A$  but  $A$  is not partially reduced, choose the highest-ranking leader  $x_j$  such that  $x'_j - f_j(\mathbf{x}) \in A$  and there exists  $q \in A \cap \mathbb{R}[\mathbf{x}]$  having leader  $x_j$ . (Such  $x'_j - f_j(\mathbf{x})$  and  $q$  exist because  $A$  is not partially reduced. Because  $A$  is triangular and  $x_j$  is the highest-ranking variable with the desired property,  $x'_j - f_j(\mathbf{x})$  and  $q$  are unique.) For concision we write  $x'_j - f_j(\mathbf{x})$  as  $x' - f(\mathbf{x})$ .

Recalling that  $s_q \in S$  by assumption in the current case, differentiate  $q$  and pseudodivide  $x' - f(\mathbf{x})$  by  $q'$ . Let  $\tilde{r}$  be the resulting pseudoremainder; note that  $x'$  is not present in  $\tilde{r}$  because the degree of  $x'$  is 1 in  $x' - f(\mathbf{x})$  and  $q'$ . (In this case, the pseudoremainder is reduced with respect to  $q'$  after a single step of pseudodivision.) However, derivatives of other variables in  $q$  may be present. Let  $y$  be such a variable; there is some  $g(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$  such that  $y' - g(\mathbf{x})$  is a

member of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$ . Replace every instance of  $y'$  in  $\tilde{r}$  with  $g(\mathbf{x})$ . (We justify this move in Theorem 96, the correctness proof for  $\text{RGA}_o$ .) Doing so for each proper derivative present in  $\tilde{r}$  produces a nondifferential polynomial  $r$ . (Abusing terminology, we also refer to  $r$  as a pseudoremainder.) Update the equations by omitting  $x' - f(\mathbf{x})$  and including  $r$ ; let  $\hat{A} := (A \cup \{r\}) \setminus \{x' - f(\mathbf{x})\}$ . Note that the elements of  $\hat{A}$  having proper derivatives form the set  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}) \setminus \{x' - f(\mathbf{x})\}$  because  $r$  is nondifferential.

Now compute  $\text{Triangulate}(\hat{A} \cap \mathbb{R}[\mathbf{x}], S)$ . Return the union  $\bigcup_{(B, S_B)} \text{RGA}_o(B \cup (\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}) \setminus \{x' - f(\mathbf{x})\}), S_B)$  over all  $(B, S_B)$  returned by  $\text{Triangulate}(\hat{A} \cap \mathbb{R}[\mathbf{x}], S)$ .

The next result is an important ingredient of the correctness proof for  $\text{RGA}_o$  (Theorem 96). The lemma performs the critical job of uniting the algebraic part (calls to  $\text{Triangulate}$ ) and differential part (differential saturation ideals) of  $\text{RGA}_o$ .

**Lemma 94.** *Let  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  be a polynomial vector field. Let  $A = \{\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}), p_1, p_2, \dots, p_m\}$  be a finite set where  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  is a subset of the differential polynomials  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  and the  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$  are nondifferential polynomials. Let  $S \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$  be a finite set of nondifferential polynomials. Let  $(B_1, S_1), \dots, (B_N, S_N)$  be the output of  $\text{Triangulate}(A \cap \mathbb{R}[\mathbf{x}], S)$ ; by correctness of  $\text{Triangulate}$  (Theorem 93) we know that*

$$\sqrt{(A \cap \mathbb{R}[\mathbf{x}]) : S^\infty} = \sqrt{(B_1) : S_1^\infty} \cap \dots \cap \sqrt{(B_N) : S_N^\infty} = ((B_1) : S_1^\infty) \cap \dots \cap ((B_N) : S_N^\infty).$$

Then we have

$$\begin{aligned} \sqrt{[A] : S^\infty} &= \sqrt{[A \cap \mathbb{R}[\mathbf{x}], \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S^\infty} = \sqrt{[B_1, \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S_1^\infty} \cap \dots \\ &\quad \cap \sqrt{[B_N, \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S_N^\infty}. \end{aligned}$$

*Proof.* The key observation is that the two operations of  $\text{Triangulate}$  (namely, splitting and nondifferential pseudodivision) preserve the differential solutions of the augmented system that includes the ODEs with the equations. (See Remark 95 for a meta-mathematical issue concerning this approach.) Moreover, these operations only involve nondifferential polynomials. For instance, if  $q \in A \cap \mathbb{R}[\mathbf{x}]$  we have

$$\sqrt{(A \cap \mathbb{R}[\mathbf{x}]) : S^\infty} = \sqrt{(A \cap \mathbb{R}[\mathbf{x}], i_q) : S^\infty} \cap \sqrt{(A \cap \mathbb{R}[\mathbf{x}]) : (S \cup \{i_q\})^\infty}$$

after a splitting step because the solutions of  $(A \cap \mathbb{R}[\mathbf{x}] = 0, S \neq 0)$  in  $\mathbb{C}$  are the union of the solutions of  $(A \cap \mathbb{R}[\mathbf{x}] = 0, i_q = 0, S \neq 0)$  and  $(A \cap \mathbb{R}[\mathbf{x}] = 0, S \cup \{i_q\} \neq 0)$  in  $\mathbb{C}$  (see Theorem 30). The analogous differential decomposition holds if we include the ODEs and consider *differential* solutions in any differential extension field. By

definition of  $A$  and by Theorem 64 we have

$$\begin{aligned}\sqrt{[A] : S^\infty} &= \sqrt{[A \cap \mathbb{R}[\mathbf{x}], \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S^\infty} \\ &= \sqrt{[A \cap \mathbb{R}[\mathbf{x}], i_q, \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S^\infty} \cap \\ &\quad \cap \sqrt{[A \cap \mathbb{R}[\mathbf{x}], \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : (S \cup \{i_q\})^\infty}.\end{aligned}\tag{3}$$

If  $g \in A \cap \mathbb{R}[\mathbf{x}]$  and  $r_g$  is the pseudoremainder from pseudodividing  $g$  by some other element of  $A \cap \mathbb{R}[\mathbf{x}]$  whose initial belongs to  $S$ , then much like Equation 2 in the proof of Theorem 93 we have

$$\begin{aligned}\mathbf{V}_\delta(A) \setminus \mathbf{V}_\delta(\Pi S) &= \mathbf{V}_\delta((A \cap \mathbb{R}[\mathbf{x}]) \cup \{\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})\}) \setminus \mathbf{V}_\delta(\Pi S) \\ &= \mathbf{V}_\delta(((A \cap \mathbb{R}[\mathbf{x}]) \cup \{r_g\}) \setminus \{g\}) \cup \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}) \setminus \mathbf{V}_\delta(\Pi S).\end{aligned}\tag{4}$$

Theorem 63 then gives

$$\sqrt{[A] : S^\infty} = \sqrt{[(((A \cap \mathbb{R}[\mathbf{x}]) \cup \{r_g\}) \setminus \{g\}), \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S^\infty}.$$

Similarly, for  $q \in A \cap \mathbb{R}[\mathbf{x}]$  we have

$$\sqrt{[A \cup \{i_q\}] : S^\infty} = \sqrt{[(((A \cap \mathbb{R}[\mathbf{x}]) \cup \{i_q, q - i_q x^{\deg_x(q)}\}) \setminus \{q\}), \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S^\infty}.$$

(See the final part of the proof of Theorem 93, p. 42.)

Thus re-inserting the ODEs  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  after a single splitting or pseudodivision step preserves the differential decomposition. The full decomposition follows by induction on the number of splitting and pseudodivision operations during a run of **Triangulate**. (In other words, since the ODEs  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  are not involved in the operations of **Triangulate**, it is equivalent to perform the entire run of **Triangulate** on the nondifferential elements and then re-introduce the  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ .)  $\square$

The system  $(B_i = 0, S_i \neq 0)$  is a regular algebraic system and so  $\sqrt{(B_i) : S_i^\infty} = (B_i) : S_i^\infty$  by Lazard's lemma (Lemma 80). However,  $(B_i = 0, \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}) = 0, S_i \neq 0)$  might not be partially reduced so we need the radicals in the differential decomposition given by Lemma 94.

**Remark 95.** Though the proof of Lemma 94 is straightforward, a subtle issue lurks nearby. We initially hoped to use more efficient radical ideal decomposition methods (e.g., that of Szántó [87, 88], which we discuss in Section 4.3, p. 60) in place of **Triangulate**. This provides an algebraic decomposition of the desired form

$$\begin{aligned}\sqrt{(A \cap \mathbb{R}[\mathbf{x}]) : S^\infty} &= \sqrt{(B_1) : S_1^\infty} \cap \cdots \cap \sqrt{(B_N) : S_N^\infty} \\ &= ((B_1) : S_1^\infty) \cap \cdots \cap ((B_N) : S_N^\infty),\end{aligned}\tag{5}$$

but requires methods beyond simple splitting and (nondifferential) pseudodivision. We were unable to prove Lemma 94 using only the algebraic decomposition in Equation 5

without the fact that splitting and pseudodivision preserve differential solutions. This illustrates a major challenge of differential algebra: even when differential polynomials have a simple form, drawing conclusions about differential ideals from restrictions to algebraic ideals is nontrivial. It also explains why we stopped with regular differential systems in  $\text{RGA}_o$  instead of continuing with the calculations needed to get regular differential chains.

Other published versions of RGA [37, pp. 162-3] [79, p. 587] [44, p. 111] use analogues of `Triangulate` (i.e., they are based on recursive splitting and pseudoreduction), so they must have nonelementary [89, pp. 419-23] worst-case complexity like we find for  $\text{RGA}_o$  (Theorems 107,109). The *Wu-Ritt process*, a close relative of `Triangulate`, has nonelementary complexity [90, p. 121] similar to what we show in Theorem 106.

**Theorem 96** (Termination and correctness of  $\text{RGA}_o$ ). *Let  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  be a polynomial vector field. Let  $A = \{\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}), p_1, p_2, \dots, p_m\}$  be a finite set where  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  is a subset of the differential polynomials  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  and the  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$  are nondifferential polynomials. Let  $S \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$  be a finite set of nondifferential polynomials. Lastly, assume that for each member  $x' - f(\mathbf{x})$  of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  we either have  $x' - f(\mathbf{x}) \in A$  (equivalently,  $x' - f(\mathbf{x}) \in \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ ) or*

$$s(x' - f(\mathbf{x})) = \beta(\mathbf{x}) + \sum_j \gamma_j(\mathbf{x})(x'_j - f_j(\mathbf{x}))$$

for some  $s \in S$ ,  $\beta(\mathbf{x}) \in [A \cap \mathbb{R}[\mathbf{x}]] \trianglelefteq \mathbb{R}\{\mathbf{x}\}$ ,  $\gamma_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ ,  $x_j < x$ , and  $x'_j - f_j(\mathbf{x}) \in A$ .

Then the algorithm  $\text{RGA}_o$  terminates on input  $(A, S)$  and the output  $(A_1, S_1), \dots, (A_r, S_r)$  satisfies

$$\sqrt{[A] : S^\infty} = ([A_1] : S_1^\infty) \cap \dots \cap ([A_r] : S_r^\infty),$$

where  $A_1, \dots, A_r \subseteq \mathbb{R}\{\mathbf{x}\}$ ,  $S_1, \dots, S_r \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$  are finite sets such that each  $(A_i = 0, S_i \neq 0)$  is a regular differential system. Moreover, the elements of  $A_i$  containing proper derivatives form a subset of  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ , and for each  $x' - f(\mathbf{x}) \in \mathbf{x}' - \mathbf{f}(\mathbf{x})$  and  $1 \leq i \leq r$  we either have  $x' - f(\mathbf{x}) \in A_i$  or

$$\hat{s}(x' - f(\mathbf{x})) = \hat{\beta}(\mathbf{x}) + \sum_j \hat{\gamma}_j(\mathbf{x})(x'_j - f_j(\mathbf{x}))$$

for some  $\hat{s} \in S_i$ ,  $\hat{\beta}(\mathbf{x}) \in [A_i \cap \mathbb{R}[\mathbf{x}]] \trianglelefteq \mathbb{R}\{\mathbf{x}\}$ ,  $\hat{\gamma}_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ ,  $x_j < x$ , and  $x'_j - f_j(\mathbf{x}) \in A_i$ . (That is, the “technical assumption” on  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  that we made of the input also holds of the output.)

*Proof.* We first argue that  $\text{RGA}_o$  terminates. On any branch of the computation, once the input  $(A, S)$  has the property that  $A$  is triangular and  $s_q \in S$  for all  $q \in A$ , this property continues to hold for each new call to  $\text{RGA}_o$  along that branch. This is so because the property activates step 3 and step 3 calls `Triangulate` (which terminates by Theorem 93) right before recursively calling  $\text{RGA}_o$ . Hence every subsequent call to  $\text{RGA}_o$  either terminates immediately or proceeds to step 3 and eliminates one of the

ODEs  $x' - f(\mathbf{x})$ . Note that at most  $n$  of the original equations contain proper derivatives and no eliminated proper derivatives are ever re-introduced to the set of equations (**Triangulate** only involves nondifferential polynomials and the pseudoremainder  $r$  introduced by step 3 of  $\text{RGA}_o$  is nondifferential). It follows that, at most, a branch of  $\text{RGA}_o$  calls **Triangulate** and  $\text{RGA}_o$   $n + 1$  times (the first time in step 2 to make the equations triangular and put separants in the inequations; thereafter only step 3 applies) before terminating.

We justify the decomposition by showing that after each intermediate step we have a decomposition with the claimed form and properties, except possibly partial reducedness and being radical. However, these will both hold of the final output; see the final paragraph of the proof. During a run of  $\text{RGA}_o$ , new differential systems are produced either by calling **Triangulate** on the nondifferential equations (followed by re-inserting the ODEs) or performing differential pseudodivision. By Lemma 94, a call to **Triangulate**, followed by re-inserting the ODEs, decomposes  $\sqrt{[A] : S^\infty}$  into a finite intersection of radicals of differential ideals of the right form (except possibly for partial reducedness)

$$\sqrt{[A] : S^\infty} = \sqrt{[B_1, \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S_1^\infty} \cap \cdots \cap \sqrt{[B_N, \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})] : S_N^\infty},$$

where  $(B_1, S_1), \dots, (B_N, S_N)$  is the output of **Triangulate** $(A \cap \mathbb{R}[\mathbf{x}], S)$ . In particular, the equations with proper derivatives are exactly  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ . We must confirm that each  $(B_l \cup \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}), S_l)$  preserves the technical assumption on the elements of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$ . If  $x' - f(\mathbf{x}) \in \mathbf{x}' - \mathbf{f}(\mathbf{x})$  belongs to  $A$ , then  $x' - f(\mathbf{x})$  remains in  $B_l \cup \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  because the proper derivatives are unchanged. Otherwise, we have

$$s(x' - f(\mathbf{x})) = \beta(\mathbf{x}) + \sum_j \gamma_j(\mathbf{x})(x'_j - f_j(\mathbf{x})) \quad (6)$$

for some  $s \in S, \beta(\mathbf{x}) \in [A \cap \mathbb{R}[\mathbf{x}]] = [p_1, \dots, p_m], \gamma_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}], x_j < x$ , and  $x'_j - f_j(\mathbf{x}) \in A$ . These same  $x'_j - f_j(\mathbf{x})$  are now in  $B_l \cup \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ . By the algebraic decomposition

$$\sqrt{(A \cap \mathbb{R}[\mathbf{x}]) : S^\infty} = ((B_1) : S_1^\infty) \cap \cdots \cap ((B_N) : S_N^\infty)$$

guaranteed by correctness of **Triangulate** (Theorem 93), we know that each  $p_i \in A \cap \mathbb{R}[\mathbf{x}]$  belongs to each  $(B_l) : S_l^\infty \subseteq \mathbb{R}[\mathbf{x}]$ . It follows that  $p_i^{(k)} \in [B_l] : S_l^\infty \subseteq \mathbb{R}\{\mathbf{x}\}$  for all  $k \in \mathbb{N}$  and hence  $[p_1, \dots, p_m] \subseteq [B_l] : S_l^\infty$ .

Multiplying both sides of equation 6 by an appropriate element of  $S_l$ , we thus obtain

$$\hat{s}(x' - f(\mathbf{x})) = \hat{\beta}(\mathbf{x}) + \sum_j \hat{\gamma}_j(\mathbf{x})(x'_j - f_j(\mathbf{x})) \quad (7)$$

for some  $\hat{s} \in S_l$  (recall that  $S \subseteq S_l$  because on a given branch no inequations are ever removed),  $\hat{\beta}(\mathbf{x}) \in [B_l]$ , and  $\hat{\gamma}_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$ . This shows that  $(B_l \cup \tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x}), S_l)$  preserves the technical assumption on the elements of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$ .

We now check the differential pseudodivision from step 3 of  $\text{RGA}_o$ . Step 3 of  $\text{RGA}_o$  produces a pseudoremainder  $\tilde{r}$  by pseudodividing some  $x' - f(\mathbf{x}) \in A$  by  $q'$ , where the separant  $s_q \in S$  and  $q \in A \cap \mathbb{R}[\mathbf{x}]$  has leader  $x$ . Recall that  $s_q$  is the initial of  $q'$  and belongs to  $\mathbb{R}[\mathbf{x}]$ . Because the initial of  $x' - f(\mathbf{x})$  is 1 and the degree of  $x'$  is 1 in both  $x' - f(\mathbf{x})$  and  $q'$ , we have  $s_q(x' - f(\mathbf{x})) - q' = \tilde{r}$ . (This is an instance of Proposition 73.) Step 3 of  $\text{RGA}_o$  goes on to substitute nondifferential polynomials (using the relations  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ ) for the remaining proper derivatives (which necessarily have lesser rank than  $x'$ ) in  $\tilde{r}$ . This produces  $r \in \mathbb{R}[\mathbf{x}]$  such that  $\tilde{r} = \sum_l \zeta_l(\mathbf{x})(x'_l - f_l(\mathbf{x})) + r$  for some  $\zeta_l(\mathbf{x}) \in \mathbb{R}[\mathbf{x}]$  and  $x_l < x$ . (As in the proof of Lemma 66, we replace  $x'_l$  in  $\tilde{r}$  with  $(x'_l - f_l(\mathbf{x})) + f_l(\mathbf{x})$ . Then distribute to get an equation of the claimed form for  $\tilde{r}$ .) Hence  $s_q(x' - f(\mathbf{x})) = q' + \sum_l \zeta_l(\mathbf{x})(x'_l - f_l(\mathbf{x})) + r$ . Let  $\hat{A} := (A \cup \{r\}) \setminus \{x' - f(\mathbf{x})\}$ ; note that  $\hat{A}$  contains all nondifferential polynomials of  $A$  and of the others only omits  $x' - f(\mathbf{x})$ . Step 3 of  $\text{RGA}_o$  then proceeds using the system  $(\hat{A}, S)$ . If  $\hat{A}$  is no longer triangular or  $S$  does not contain  $s_r$ , the next call to `Triangulate` will restore those properties.

We show that  $(\hat{A}, S)$  preserves the technical assumption on the elements of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$  and that  $[A] : S^\infty = [\hat{A}] : S^\infty$ . Though  $x' - f(\mathbf{x}) \in A$ , by definition  $x' - f(\mathbf{x}) \notin \hat{A}$ . However, by assumption each  $x'_l - f_l(\mathbf{x})$  in the equation

$$s_q(x' - f(\mathbf{x})) = q' + \sum_l \zeta_l(\mathbf{x})(x'_l - f_l(\mathbf{x})) + r \quad (8)$$

either belongs to  $A$  (and hence to  $\hat{A}$  since  $x'_l - f_l(\mathbf{x}) \neq x' - f(\mathbf{x})$ ) or can be written as

$$s_l(x'_l - f_l(\mathbf{x})) = \beta_l(\mathbf{x}) + \sum_j \gamma_{j,l}(\mathbf{x})(x'_j - f_j(\mathbf{x})) \quad (9)$$

for some  $s_l \in S, \beta_l(\mathbf{x}) \in [A \cap \mathbb{R}[\mathbf{x}]] \subseteq [\hat{A} \cap \mathbb{R}[\mathbf{x}]], \gamma_{j,l}(\mathbf{x}) \in \mathbb{R}[\mathbf{x}], x_j < x_l$ , and  $x'_j - f_j(\mathbf{x}) \in A$ . Since  $x_j < x_l < x$ , we have  $x'_j - f_j(\mathbf{x}) \neq x' - f(\mathbf{x})$  and so  $x'_j - f_j(\mathbf{x}) \in \hat{A}$ . Multiplying both sides of 8 by appropriate elements of  $S$ , using 9, and using the fact that  $q, r$  belong to  $\hat{A} \cap \mathbb{R}[\mathbf{x}]$ , we see that the technical assumption holds of  $x' - f(\mathbf{x})$  with respect to  $(\hat{A}, S)$ . We now consider all  $y' - g(\mathbf{x}) \in \mathbf{x}' - \mathbf{f}(\mathbf{x})$  such that  $y' - g(\mathbf{x}) \neq x' - f(\mathbf{x})$ . If  $y' - g(\mathbf{x}) \in A$ , then  $y' - g(\mathbf{x})$  still belongs to  $\hat{A}$ . If  $y' - g(\mathbf{x}) \notin A$ , by assumption

$$s(y' - g(\mathbf{x})) = \beta(\mathbf{x}) + \sum_j \gamma_j(\mathbf{x})(x'_j - f_j(\mathbf{x})) \quad (10)$$

for some  $s \in S, \beta(\mathbf{x}) \in [A \cap \mathbb{R}[\mathbf{x}]], \gamma_j(\mathbf{x}) \in \mathbb{R}[\mathbf{x}], x_j < y$ , and  $x'_j - f_j(\mathbf{x}) \in A$ . Here one of the  $x'_j - f_j(\mathbf{x})$  might be  $x' - f(\mathbf{x})$ , but we showed above that  $x' - f(\mathbf{x})$  has the right form with respect to  $(\hat{A}, S)$ . Hence we can multiply both sides of 10 by appropriate elements of  $S$ , substitute for  $x' - f(\mathbf{x})$ , and conclude that  $y' - g(\mathbf{x}) \in [\hat{A}] : S^\infty$  has the form required by the technical assumption.

To prove that  $[A] : S^\infty = [\hat{A}] : S^\infty$ , it suffices to show that  $x' - f(\mathbf{x}) \in [\hat{A}] : S^\infty$  and  $r \in [A] : S^\infty$ . Both memberships follow from equations 8 and 9 (recall  $q \in A \cap \mathbb{R}[\mathbf{x}], r \in \hat{A} \cap \mathbb{R}[\mathbf{x}]$ , and  $x' - f(\mathbf{x}) \in A$ ). Thus differential pseudodivision replaces



a system with an equivalent one whose corresponding differential saturation ideal is the same (in particular, the decomposition does not change).

Lastly, we explain why each output  $(A_i = 0, S_i \neq 0)$  is a regular differential system. (Each  $[A_i] : H_i^\infty$  is then radical by Lazard's lemma (Lemma 80), which is why  $\sqrt{[A_1] : S_1^\infty} \cap \dots \cap \sqrt{[A_r] : S_r^\infty} = ([A_1] : S_1^\infty) \cap \dots \cap ([A_r] : S_r^\infty)$ .) Both  $A_i$  and  $S_i$  are finite because only finitely many elements can enter at any step. Initials and separants are never identically zero, so 0 was not added to the inequations during the computation (i.e.,  $0 \notin S_i$ ). Termination only occurs when  $A_i$  is partially reduced, so that property is assured. The nondifferential polynomials in  $A_i$  form a triangular set by the action of **Triangulate**. The remaining differential polynomials form a subset of  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$ . The orderly ranking ensures that an element  $x'_j - f_j(\mathbf{x})$  of  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  has leader  $x'_j$ , so the entire set  $A_i$  (i.e., the union of the nondifferential elements of  $A_i$  and a subset of the original ODEs) remains triangular. The separant of any element of  $\tilde{\mathbf{x}}' - \tilde{\mathbf{f}}(\mathbf{x})$  is 1 and the separants of nondifferential elements of  $A_i$  belong to  $S_i$  by **Triangulate**. Since  $S_i \subseteq \mathbb{R}[\mathbf{x}]$  has no proper derivatives, it is partially reduced with respect to  $A_i$ . Thus  $(A_i = 0, S_i \neq 0)$  is a regular differential system. This completes the proof.  $\square$

We need the following theorem to interpret the output of  $\text{RGA}_o$ . The result is intuitively natural but slightly fussy to prove. It connects differential ideals to invariant ideals of polynomial vector fields: in particular, in the presence of an explicit system  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$ , the nondifferential polynomials in a differential ideal form the smallest invariant ideal containing the nondifferential polynomials in the original set that generated the differential ideal.

**Theorem 97.** *Let  $A = \{\mathbf{x}' - \mathbf{f}(\mathbf{x}), p_1, p_2, \dots, p_m\}$  with  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$ . Then  $(\mathcal{L}_{\mathbf{F}}^*(A \cap \mathbb{R}[\mathbf{x}])) = (\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x}]})) = (\mathcal{L}_{\mathbf{F}}^*(p_1, \dots, p_m)) = [A] \cap \mathbb{R}[\mathbf{x}]$ , where  $\mathbf{F}$  is the polynomial vector field  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ .*

*Proof.*  $(\subseteq)$ : Immediate from Lemma 66.

$(\supseteq)$  Let  $q \in [A] \cap \mathbb{R}[\mathbf{x}]$ . Then for some  $l \geq 1$ , we have a representation

$$q = \sum_{1 \leq i \leq n, 1 \leq k \leq l} g_{i,k}(\mathbf{x})(x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})) + \sum_{1 \leq j \leq m, 1 \leq k \leq l} h_{j,k}(\mathbf{x})p_j^{(k)} + \sum_{1 \leq j \leq m} h_j(\mathbf{x})p_j,$$

where  $g_{i,k}, h_{j,k}, h_j \in \mathbb{R}\{\mathbf{x}\}$ . Proceeding as in the proof of Lemma 66 (i.e., replacing  $x'_i$  with  $x'_i - f_i(\mathbf{x}) + f_i(\mathbf{x})$ ), for  $k \geq 1$  we may replace  $p_j^{(k)}$  with  $\mathcal{L}_{\mathbf{F}}^{(k)}(p_j)$  plus a sum of multiples of the various  $x'_i - f_i(\mathbf{x}), \dots, x_i^{(k)}(\mathbf{x}) - f_i^{(k-1)}(\mathbf{x})$ . Regrouping and renaming the coefficient polynomials  $g_{i,k}$ , etc., as necessary, we may thus assume  $q$  has the form

$$q = \sum_{1 \leq i \leq n, 1 \leq k \leq l} g_{i,k}(\mathbf{x})(x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})) + \sum_{1 \leq j \leq m, 1 \leq k \leq l} h_{j,k}(\mathbf{x})\mathcal{L}_{\mathbf{F}}^{(k)}(p_j) + \sum_{1 \leq j \leq m} h_j(\mathbf{x})p_j.$$

Because  $q$  and the various  $f_i(\mathbf{x}), \mathcal{L}_{\mathbf{F}}^{(k)}(p_j)$ , and  $p_j$  belong to  $\mathbb{R}[\mathbf{x}]$ , we may assume that no derivative of order greater than  $l$  appears on the right-hand side (i.e.,  $g_{i,k}, h_{j,k}, h_j \in \mathbb{R}[x_1, \dots, x_n, \dots, x_1^{(l)}, \dots, x_n^{(l)}]$ ). Finally, we may assume that  $h_{j,k}, h_j \in \mathbb{R}[\mathbf{x}]$  and that each  $g_{i,k}$  has order no greater than  $k$ . To see this, note that any  $x_i^{(r)}$  in  $g_{i,k}, h_{j,k}, h_j$  ( $l \geq r > k$  in the case of  $g_{i,k}$  and  $l \geq r > 0$  for  $h_{j,k}, h_j$ ) may be replaced with  $x_i^{(r)} - f_i^{(r-1)}(\mathbf{x}) + f_i^{(r-1)}(\mathbf{x})$  where  $f_i^{(r-1)}(\mathbf{x})$  has order less than  $r$ . The general form of the representation of  $q$  is preserved but the resulting replacements for  $g_{i,k}, h_{j,k}, h_j$  contain fewer derivatives of order  $r$  (and no higher ones were introduced), so the claim follows by induction.

We now have a form that is conducive to proving  $q \in (\mathcal{L}_{\mathbf{F}}^*(p_1, \dots, p_m))$ . We induct on the maximum order  $l$  of the  $x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})$  (in particular, for the inductive hypothesis we do not need the order of the Lie derivatives of  $p_j$  to match  $l$ ; we just require the assumptions that  $h_{j,k}, h_j \in \mathbb{R}[\mathbf{x}]$  and that  $g_{i,k}$  has order no greater than  $k$ ). Subtracting from both sides, we obtain

$$\begin{aligned} q - \left( \sum_{1 \leq i \leq n, 1 \leq k < l} g_{i,k}(\mathbf{x})(x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})) + \sum_{1 \leq j \leq m, 1 \leq k \leq l} h_{j,k}(\mathbf{x})\mathcal{L}_{\mathbf{F}}^{(k)}(p_j) + \right. \\ \left. + \sum_{1 \leq j \leq m} h_j(\mathbf{x})p_j \right) = \sum_{1 \leq i \leq n} g_{i,l}(\mathbf{x})(x_i^{(l)} - f_i^{(l-1)}(\mathbf{x})). \end{aligned} \quad (11)$$

Denote the left-hand side of equation 11 by  $\tilde{q}$  and choose an orderly ranking on  $x_1, \dots, x_n$  (so all derivatives of order  $l$  are greater than any derivative of lower order). Observe that  $A_0 := \{x_1^{(l)} - f_1^{(l-1)}(\mathbf{x}), \dots, x_n^{(l)} - f_n^{(l-1)}(\mathbf{x})\}$  is a regular set when we consider the entries as elements of  $\mathbb{R}[x_1, \dots, x_n, \dots, x_1^{(l)}, \dots, x_n^{(l)}]$ : each entry in  $A_0$  has a distinct leader  $x_i^{(l)}$  and every initial is 1 (whence Definition 79 (2) trivially holds). Moreover,  $\tilde{q}$  is reduced with respect to  $A_0$  (by our assumptions, none of the leaders  $x_i^{(l)}$  appears in  $\tilde{q}$ ). Equation 11 witnesses that  $\tilde{q} \in (A_0) = (A_0) : S^\infty$  (since the multiplicative set  $S$  generated by the initials of  $A_0$  is simply  $\{1\}$ ). However, by Theorem 81,  $\tilde{q} \in (A_0) : S^\infty$  if and only if  $A_0$  pseudoreduces  $\tilde{q}$  to zero. Since  $\tilde{q}$  is already reduced with respect to  $A_0$ , this implies that both  $\tilde{q}$  and the right-hand side  $\sum_{1 \leq i \leq n} g_{i,l}(\mathbf{x})(x_i^{(l)} - f_i^{(l-1)}(\mathbf{x}))$  are identically zero. Hence

$$q = \sum_{1 \leq i \leq n, 1 \leq k < l} g_{i,k}(\mathbf{x})(x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})) + \sum_{1 \leq j \leq m, 1 \leq k \leq l} h_{j,k}(\mathbf{x})\mathcal{L}_{\mathbf{F}}^{(k)}(p_j) + \sum_{1 \leq j \leq m} h_j(\mathbf{x})p_j,$$

which has lower maximum order of the  $x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})$  but the same overall form and preserves our assumptions on  $g_{i,k}, h_{j,k}, h_j$ . By induction we may eliminate all the  $x_i^{(k)} - f_i^{(k-1)}(\mathbf{x})$ , leaving

$$q = \sum_{1 \leq j \leq m, 1 \leq k \leq l} h_{j,k}(\mathbf{x})\mathcal{L}_{\mathbf{F}}^{(k)}(p_j) + \sum_{1 \leq j \leq m} h_j(\mathbf{x})p_j.$$

This proves that  $q \in (\mathcal{L}_{\mathbf{F}}^*(p_1, \dots, p_m))$ . □

Our work on  $\text{RGA}_o$  culminates with Theorem 98, which interprets the output as a canonical algebraic invariant of a polynomial vector field  $\mathbf{F}$ . In particular, parts 1 and 3 connect differential ideals and the maximal invariant contained in  $\mathbf{V}_{\mathbb{R}}(A \cap \mathbb{R}[\mathbf{x}])$ . Part 3 also indicates the structure of this invariant in terms of smaller invariant sets. These are the major contributions of Theorem 98. Part 2 is implicit in [91] because there the authors obtain  $(\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x}]}))$ , from which membership in the radical can be tested. (See our remarks on [91] in Section 5.1. We discuss radical ideal membership in Section 4.4 and the two paragraphs preceding it.) However, our mechanism is different (regular differential systems instead of Gröbner bases) and shows that to test membership in  $\sqrt{(\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x]}))}$  it is unnecessary to first find generators of  $(\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x]}}))$ .

**Theorem 98.** *Let  $A = \{\mathbf{x}' - \mathbf{f}(\mathbf{x}), p_1, p_2, \dots, p_m\}$  with  $p_1, \dots, p_m \in \mathbb{R}[\mathbf{x}]$  and let  $\mathbf{F}$  be the polynomial vector field  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ . If  $(A_1, S_1), \dots, (A_r, S_r)$  are the regular differential systems returned by  $\text{RGA}_o$  given  $(A, \emptyset)$  as input, then*

1.

$$\begin{aligned} \sqrt{(\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x]}))} &= \sqrt{[A]} \cap \mathbb{R}[\mathbf{x}] \\ &= ((A_1 \cap \mathbb{R}[\mathbf{x}]) : S_1^\infty) \cap \dots \cap ((A_r \cap \mathbb{R}[\mathbf{x}]) : S_r^\infty). \end{aligned}$$

2. Membership in  $\sqrt{(\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x]}))}$  is decidable.

3.  $\mathbf{V}_{\mathbb{R}}([A] \cap \mathbb{R}[\mathbf{x}])$  is the largest invariant with respect to  $\mathbf{F}$  that is contained in  $\mathbf{V}_{\mathbb{R}}(A \cap \mathbb{R}[\mathbf{x}])$ . Moreover,  $\mathbf{V}_{\mathbb{R}}([A] \cap \mathbb{R}[\mathbf{x}])$  is a finite union of invariants of the form  $\mathbf{V}_{\mathbb{R}}((A_i \cap \mathbb{R}[\mathbf{x}]) : S_i^\infty)$ .

*Proof.* 1. The first equation follows from Theorem 97 and Lemma 57 (2). For the second, we have

$$\begin{aligned} \sqrt{[A]} \cap \mathbb{R}[\mathbf{x}] &= (([A_1] : S_1^\infty) \cap \dots \cap ([A_r] : S_r^\infty)) \cap \mathbb{R}[\mathbf{x}] && \text{(Theorem 96)} \\ &= (([A_1] : S_1^\infty) \cap \mathbb{R}[\mathbf{x}]) \cap \dots \cap (([A_r] : S_r^\infty) \cap \mathbb{R}[\mathbf{x}]) \\ &= (((A_1) : S_1^\infty) \cap \mathbb{R}[\mathbf{x}]) \cap \dots \cap (((A_r) : S_r^\infty) \cap \mathbb{R}[\mathbf{x}]) && \text{(Theorem 82)} \\ &= ((A_1 \cap \mathbb{R}[\mathbf{x}]) : S_1^\infty) \cap \dots \cap ((A_r \cap \mathbb{R}[\mathbf{x}]) : S_r^\infty). && \text{(Lemma 85)} \end{aligned}$$

Theorem 96, correctness of  $\text{RGA}_o$ , applies because  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in A$ . Lemma 85 applies because the  $(A_i, S_i)$  are explicit regular differential systems by Theorem 96.

2.  $\text{RGA}_o$  computes the regular differential systems  $(A_i, S_i)$ . Membership in  $(A_i \cap \mathbb{R}[\mathbf{x}]) : S_i^\infty$  is decidable using Gröbner bases or regular chains (Section 2.6.1). Membership in a finite intersection of ideals is decidable using Gröbner bases [30, p. 194].

3. By part 1 of this theorem, Lemma 8, and part 3b of Proposition 23 we have

$$\begin{aligned} \mathbf{V}_{\mathbb{R}}(\mathcal{L}_{\mathbf{F}}^*(A_{\mathbb{R}[\mathbf{x}]})) &= \mathbf{V}_{\mathbb{R}}([A] \cap \mathbb{R}[\mathbf{x}]) \\ &= \mathbf{V}_{\mathbb{R}}((A_1 \cap \mathbb{R}[\mathbf{x}]) : S_1^\infty) \cup \cdots \cup \mathbf{V}_{\mathbb{R}}((A_r \cap \mathbb{R}[\mathbf{x}]) : S_r^\infty) \end{aligned}$$

The claims then follow from Lemma 53 and Theorem 86. (Theorem 86 applies because Theorem 96 implies that  $\mathbf{x}' - \mathbf{f}(\mathbf{x}) \in [A_i] : S_i^\infty$  and  $(A_i, S_i)$  is an explicit regular differential system.)

□

Note that our Theorems 96,98 have more specialized hypotheses than the RGA theorem of Boulier et al. (Theorem 90) and do not guarantee that all elements of  $[A_i] : S_i^\infty$  are differentially pseudoreduced to 0 by  $A_i$ . However, Theorem 90 does not identify the dynamical meaning of the nondifferential polynomials in the output. Moreover, our Theorem 98 still allows for testing membership in  $\sqrt{[A]} \cap \mathbb{R}[\mathbf{x}]$ . The greater specificity of Theorem 98 may also lead to better computational complexity; see Remark 114.

#### 4.2. Algebraic Invariants from RGA Using Parameters

We now explain how we obtained the Lorenz system invariant in Section 3.3. Recall that the ODEs in question are  $x' = y - x, y' = 2x - y - xz, z' = xy - z$ . Our goal is to identify at least one nontrivial algebraic invariant of this system using the algorithms and theorems from Section 4.1. Consider the parameterized polynomial constraint  $g(x, y, z) = ax^2 + by^2 + cz^2 = 0$ , where  $a, b, c$  are unknown constants. (We call  $g$  a *template*.) To settle on this choice, we first restricted to polynomials of degree 2 and looked at possibilities containing  $g$  but also having additional monomials. By trial-and-error we found that other parameters seem to be 0 for interesting invariants, so here we only present  $g$ . The input system is  $A := (x' - y + x, y' - 2x + y + xz, z' - xy + z, g, a', b', c')$ , where we interpret the polynomials as equations; the inequation set is empty. The terms  $a', b', c'$  express that  $a, b, c$  are constant and do not depend on time like  $x, y, z$ . Computing RGA in Maple (using the `RosenfeldGroebner` command) on the system  $A$  with an orderly ranking  $x > y > z > a > b > c$  yields five regular differential chains:

1.  $x' + x - y, xz - 2x + y + y', -xy + z + z', a, b, c,$
2.  $xz - 2x + y + y', -xy + z + z', c', 2x^2 - y^2 - z^2, a + 2c, b - c,$
3.  $z' + z, a', b', x, y, c,$
4.  $b', c', x - y, y^2 - 1, z - 1, a + b + c,$
5.  $a', b', c', x, y, z.$

Even though we used a black-box commercial version of RGA for the calculation, Section 3.3 shows that the hypotheses of Theorems 86 and 88 hold of the output. (Specifically, chain 2; the others give invariants by inspection. See the next paragraph.) By default, Maple suppresses the inequations associated to each chain; however, the user can print them with the `Inequations` command. When implemented,  $\text{RGA}_o$  should give equivalent output (but explicitly showing the inequations).

In the output we interpret  $a, b, c$  as parameters and the invariants as algebraic sets in  $\mathbb{R}^3$  defined by polynomials in  $\mathbb{R}[x, y, z]$ . Chain 1 defines the trivial invariant set  $\mathbb{R}^3$  because  $a = b = c = 0$  causes  $g$  to vanish at every point in  $\mathbb{R}^3$ . Chain 2 requires  $a = -2c$  and  $b = c$ , which is the relationship of coefficients in  $g_{a=2, b=-1, c=-1} = 2x^2 - y^2 - z^2$ . In other words, chain 2 defines the two-dimensional surface  $2x^2 - y^2 - z^2 = 0$ , the invariant we confirmed in Section 3.3. (Any nonzero scalar multiple of  $(2, -1, -1)$ , or equivalently any nonzero solution of  $a = -2c, b = c$ , would define the same surface.) This appears to be the “most generic chain” or “general solution” produced by RGA (p. 35; roughly, no additional equations hold beyond those implied by the input). Chain 3 requires  $x, y$  to constantly be zero; the final term of  $g$  vanishes because  $c = 0$ . Thus chain 3 defines the  $z$ -axis, a one-dimensional curve. Chain 4 is even simpler, defining the (zero-dimensional) points  $(1, 1, 1)$  and  $(-1, -1, 1)$ . Lastly, chain 5 defines the origin,  $(0, 0, 0)$ .

Theorem 98 implies that the union of these sets contains *every* algebraic invariant of the form  $ax^2 + by^2 + cz^2 = 0$  in  $\mathbb{R}^3$  for the vector field  $x' = y - x, y' = 2x - y - xz, z' = xy - z$ . (Moreover, invariants that are proper subsets of  $\mathbb{R}^3$  are contained in the union of the invariants given by the final four chains.) This is essentially a completeness result describing the sense in which  $\text{RGA}_o$  finds *all* invariants having a given parameterized form. Moreover, the output invariant is structured, being comprised of smaller invariants of various dimensions. The example suggests that a generic chain corresponds to an invariant that has maximal dimension among the proper invariants.

#### 4.3. Bounds on $\text{RGA}_o$

We now find upper bounds (Theorems 107, 109) on the complexity of  $\text{RGA}_o$ . The maximal degree of polynomials in the output is a common measure of complexity for algorithms that operate on polynomials; in this paper we use the term *degree complexity*. Like many authors we consider degree complexity as a function of the maximal degree  $d$  of the input polynomials and the number of variables  $n$ . Algorithms involving polynomial ideals frequently have degree complexity that is singly or doubly exponential in  $n$  and polynomial in  $d$  (e.g.,  $O(d^{2^n})$ ) [92]. Thus it is reasonable to ignore matters like time complexity of addition and multiplication, the number of polynomials in the input, etc., that affect the output in only polynomial or singly exponential fashion.

We start by analyzing `Triangulate`. This involves a recursively defined function  $T(d, n)$  that bounds the degree complexity. It is not surprising that the *Fibonacci numbers* appear in the definition of  $T(d, n)$  because a single step of pseudodivision produces a pseudoremainder whose degree is at most the sum of the degrees of the dividend and divisor (see step 2 of `DiffPseudoDiv` on p. 25).

**Notation 99.** We write  $F_j$  for the  $j$ -th Fibonacci number, defined recursively by  $F_0 := 0, F_1 := 1, F_j := F_{j-1} + F_{j-2}$  for  $2 \leq j$ .

**Proposition 100** (Binet’s formula [93, p. 92]).

$$F_j = \frac{\phi_1^j - \phi_2^j}{\sqrt{5}},$$

where  $\phi_1 := \frac{1+\sqrt{5}}{2}$  and  $\phi_2 := \frac{1-\sqrt{5}}{2}$ .

It is somewhat tricky to pin down the degree complexity of `Triangulate` for the same reason that termination (Theorem 93) was delicate to establish: depending on the inputs, `Triangulate` must accommodate many different patterns of degrees throughout the computation. This includes the difficulty that multiple intermediate polynomials can have the same degree, so the degree of a given output is not necessarily tied to how many pseudodivision steps the calculation required. To handle this, we induct on the number of times that the minimal and maximal degrees in the target variable change.

**Theorem 101** (Degree complexity of `Triangulate`). *Given finite sets of polynomials  $A \subseteq \mathbb{R}[\mathbf{x}]$ ,  $S \subseteq \mathbb{R}[\mathbf{x}] \setminus \{0\}$  in  $n = |\mathbf{x}|$  variables such that each polynomial has total degree at most  $d$ , algorithm `Triangulate` returns polynomials that have total degree at most  $T(d, n)$ , where  $T(d, k)$  is defined recursively by  $T(d, 0) := d$ ,  $T(d, k) := (F_{2 \cdot T(d, k-1)+1}) \cdot T(d, k-1)$  for  $1 \leq k$ .*

*Proof.* Throughout a run of `Triangulate`, the inequations are updated with initials and separants of updated equations. Hence it suffices to bound the total degrees of the equations. Equations result from including initials or separants, which doesn’t increase the degree, or from a single pseudodivision step. Hence to find an upper bound we may assume that each new equation results from pseudodivision and adds the degrees of the two polynomials involved.

For  $0 \leq k \leq n$  we claim that  $T(d, k)$  is a bound on the total degree of any equation after eliminating  $k$  target variables, which implies the theorem statement. (That is,  $T(d, k)$  is a bound after `Triangulate` ensures that each of those  $k$  target variables is the leader in at most one equation and the separant the corresponding polynomial belongs to the inequations.) Initially, total degrees are at most  $T(d, 0) = d$  because we haven’t done anything yet (no variables eliminated). We prove that  $T(d, 1) = F_{2d+1}d$  is a bound on the total degree after eliminating one target variable. This is sufficient because the process is identical going from  $k-1$  to  $k$ . In particular, if  $T(d, k-1)$  bounds total degrees after we have eliminated  $k-1$  variables, the same argument (just replacing  $d$  with  $T(d, k-1)$ ) shows that  $T(T(d, k-1), 1) = (F_{2 \cdot T(d, k-1)+1}) \cdot T(d, k-1)$  is a bound after eliminating  $k$  variables. The latter expression is  $T(d, k)$  by definition.

We now show that  $T(d, 1) = F_{2d+1}d$  is a bound on the total degree after eliminating one target variable. Let  $x$  be the first target variable. We introduce the following terminology to assist with the proof. We refer to the polynomial  $q$  chosen in step 1 of `Triangulate` as the *minimal pseudodivisor* for the next pseudodivision step. (Recall that by definition  $q$  has minimal degree in  $x$  among the equations with leader  $x$  and also has minimal total degree among equations with that minimal degree in  $x$ .) We refer to the polynomial  $p$  chosen in step 2 of `Triangulate` as the *maximal pseudodividend* ( $p$

has maximal total degree among all equations of maximal degree in  $x$ ). Suppose we have performed  $i$  pseudodivision steps so far. The key values are the current minimal nonzero degree in  $x$  of any equation (call it  $x_{\min,i}$ ) and the current maximal degree in  $x$  of any equation (call it  $x_{\max,i}$ ). Then the current minimal pseudodivisor has degree  $x_{\min,i}$  in  $x$  and the maximal pseudodivisor has degree  $x_{\max,i}$  in  $x$ . Let  $t_{\max,i}$  be the current maximal total degree of any equation (not necessarily having  $x$  as its leader). For instance,  $x_{\min,0} \leq x_{\max,0} \leq t_{\max,0} \leq d$  (the initial bound before any pseudodivisions).

As long as elements of degree  $x_{\min,0}$  in  $x$  are used to pseudodivide elements of degree  $x_{\max,0}$  in  $x$ , we get pseudoremainders of total degree at most  $2d$ . (In other words, as long as  $x_{\min}$  and  $x_{\max}$  do not change.) This is because any polynomials not present initially are pseudoremainders that have degree in  $x$  strictly less than  $x_{\max,0}$ . Hence they have not been used as pseudodivisors yet. Also, any polynomial with degree  $x_{\min,0}$  in  $x$  that becomes the minimal pseudodivisor in place of the original must have total degree no greater than that of the original minimal pseudodivisor (which was at most  $d$ ). Otherwise it would not be minimal. Hence as soon as  $x_{\min,i+1} < x_{\min,i}$  or  $x_{\max,i+1} < x_{\max,i}$  for the first time, we still have  $t_{\max,i+1} \leq 2d$ . Note that  $2d = 1d + 1d = F_1d + F_2d = (F_1 + F_2)d = F_3d$ . Note also that if exactly one of  $x_{\min,i+1} < x_{\min,i}$  or  $x_{\max,i+1} < x_{\max,i}$  occurs, then at least one of the subsequent minimal pseudodivisor and maximal pseudodivisor still has total degree at most  $d = 1d = F_2d$ . This is because the subsequent minimal pseudodivisor has total degree at most  $d$  if  $x_{\min,i+1} = x_{\min,i}$ . If  $x_{\max,i+1} = x_{\max,i}$ , then one of the original equations of maximal degree in  $x$  is still present and the subsequent maximal pseudodivisor has total degree at most  $d$ . If both  $x_{\min,i+1} < x_{\min,i}$  and  $x_{\max,i+1} < x_{\max,i}$  occur, then both the new minimal pseudodivisor and maximal pseudodivisor have degree at most  $2d = F_3d$ . From now on we omit the numerical subscripts from  $x_{\min,i}$ ,  $x_{\max,i}$ , and  $t_{\max,i}$  because the important quantity is *how many times  $t_{\max}$  can increase*, not how many pseudodivision steps are performed in all. The amount that  $t_{\max}$  can change in any individual step is bounded (e.g., earlier in this paragraph we saw that  $t_{\max}$  is at most  $2d$  after the first change in  $x_{\min}$  or  $x_{\max}$ ), so bounding the *number* of changes allows us to bound the final value of  $t_{\max}$ .

In particular, the crucial observation is that  $t_{\max}$  cannot increase more times than the combined number of decreases in  $x_{\min}$  and  $x_{\max}$ , plus 1. Each of  $x_{\min}$ ,  $x_{\max}$  can decrease at most  $d - 1$  times and keep a nonzero value. So after decreasing a combined number of  $2d - 2$  times, at most  $x_{\min} = x_{\max} = 1$ . Then each subsequent pseudodivision eliminates  $x$ , so the pseudoremainders are not used as long as  $x$  is still the target variable. Hence at this stage there can be no more changes to  $x_{\min}$  and  $x_{\max}$  (they will both still be 1 when only one polynomial with leader  $x$  remains) and  $t_{\max}$  can only increase one more time (due to pseudodivision involving elements having degree 1 in  $x$ ), making for  $2d - 1$  increases at most.

As alluded to immediately before the theorem statement, we induct on the combined number of decreases in  $x_{\min}$  and  $x_{\max}$  to show that  $t_{\max}$  never exceeds  $F_{2d+1}d = T(d, 1)$ . In particular, we assert that after  $j$  total decreases in  $x_{\min}$  and  $x_{\max}$  (with  $1 \leq j \leq 2d - 2$ ), we satisfy two conditions: 1. we have  $t_{\max} \leq F_{j+2}d$  and 2. at least one of the current minimal pseudodivisor and maximal pseudodivisor has total degree at most  $F_{j+1}d$ . The paragraph before last establishes the base case  $j = 1$ . The

reasoning is analogous for the inductive case: suppose after  $j - 1$  decreases we have  $t_{\max} \leq F_{(j-1)+2}d = F_{j+1}d$  and at least one of the current minimal pseudodivisor and maximal pseudodividend has total degree at most  $F_{(j-1)+1}d = F_jd$ . As in the base case, we perform pseudodivision until we decrease either one or both of  $x_{\min}$  and  $x_{\max}$  for a total of  $j$  or  $j + 1$  decreases. Since by assumption either the pseudodivisor or pseudodividend has total degree at most  $F_jd$  and neither has total degree greater than  $F_{j+1}d$ , the pseudoremainder has total degree at most  $F_jd + F_{j+1}d = F_{j+2}d < F_{(j+1)+2}d$ . This proves the assertion about  $t_{\max}$ . If  $x_{\min}$  stays the same, then the subsequent minimal pseudodivisor has total degree at most  $F_{j+1}d$ . If  $x_{\max}$  stays the same, then the subsequent maximal pseudodivisor has total degree at most  $F_{j+1}d$ . If both  $x_{\min}$  and  $x_{\max}$  decrease, the condition on minimal pseudodivisors and maximal pseudodividends continues to hold: we now have  $j + 1$  decreases and both the new minimal pseudodivisor and new maximal pseudodividend have total degree at most  $F_{j+2}d = F_{(j+1)+1}d$ . This proves the inductive case.

Hence when  $j = 2d - 2$  (necessarily forcing  $x_{\min} = x_{\max} = 1$ ), we have a current minimal pseudodivisor of total degree at most  $F_{2d-2+1}d = F_{2d-1}d$  and current maximal pseudodividend of total degree at most  $F_{2d-2+2}d = F_{2d}d$ . The final pseudodivision steps at most add  $F_{2d-1}d$  and  $F_{2d}d$  to yield the claimed value  $F_{2d+1}d = T(d, 1)$ . This completes the proof.  $\square$

We now find an explicit function that bounds the recursively defined function  $T(d, n)$ . We start with a couple of straightforward inequalities.

**Lemma 102.** *For all  $j \in \mathbb{N}$ , the  $j$ -th Fibonacci number  $F_j$  satisfies  $F_j < 2^j$ .*

*Proof.*

$$\begin{aligned} F_j &= \frac{\phi_1^j - \phi_2^j}{\sqrt{5}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^j - \left(\frac{1-\sqrt{5}}{2}\right)^j}{\sqrt{5}} && \text{(Binet's formula, Proposition 100)} \\ &< \frac{2^j + 1}{\sqrt{5}} && (\phi_1 < 2, |\phi_2| < 1) \\ &< 2^j. && (\sqrt{5} > 2, 1 \leq 2^j) \end{aligned}$$

$\square$

**Lemma 103.** *Let  $M, N \in \mathbb{R}$  with  $M > 2$ . Then  $N \cdot (2^M) + 2M < (N + 1) \cdot (2^M)$ .*

*Proof.* Note that  $N \cdot (2^M) + 2M < (N + 1) \cdot (2^M)$  if and only if  $2M < 2^M$ . This holds by calculus:  $2M = 2^M$  for  $M = 2$  and the derivatives satisfy  $(2M)' = 2 < \ln 2 \cdot (2^M)' = (2^M)'$  when  $M \geq 2$ .  $\square$

**Notation 104.** *For natural numbers  $d \geq 1$  and  $n = 1$  we define*

$$\text{Tower}(d, 1) := 2^{3d+1}.$$

*For  $d \geq 1$  and  $n > 1$  we define*

$$\text{Tower}(d, n) := 2^{2^{\cdot^{\cdot^{\cdot^{3d+n+1}}}}},$$



where the right-hand side is an exponent tower of height  $n + 1$  (i.e., the tower consists of nested exponents with  $n$  copies of 2 followed by a final exponent  $3d + n + 1$ ).

**Lemma 105.** All natural numbers  $d, n \geq 1$  satisfy  $2^{4 \cdot \text{Tower}(d, n)} \leq \text{Tower}(d, n + 1)$ .

*Proof.* First let  $n = 1$ . Then

$$2^{4 \cdot \text{Tower}(d, 1)} = 2^{4 \cdot 2^{3d+1}} = 2^{2^{3d+1+2}} = 2^{2^{3d+3}} = \text{Tower}(d, 2).$$

Now let  $n > 1$ . We find

$$\begin{aligned} 2^{4 \cdot \text{Tower}(d, n)} &= 2^{4 \cdot 2^{2^{\cdot^{3d+n+1}}}}} \\ &= 2^2 \left( 2^{\cdot^{3d+n+1}} + 2 \right) \\ &\leq 2^2 \left( 2 \cdot 2^{\cdot^{3d+n+1}} \right). \end{aligned}$$

The net effect is to add 1 to the exponent of the third 2 from the bottom of the tower. Repeat the cycle of “adding 1 to an exponent is less than multiplying the exponent by 2, which adds 1 to the next exponent up” as long as the exponent is 2. This propagates addition of 1 up the tower to the final exponent, whence

$$2^{4 \cdot \text{Tower}(d, n)} \leq 2^{2^{2^{\cdot^{3d+n+2}}}}} = \text{Tower}(d, n + 1).$$

□

**Theorem 106** (Explicit bounds on degree complexity of `Triangulate`). Let  $T(d, n)$  be the recursive function from Theorem 101 that bounds the degree complexity of the output of `Triangulate`. The following inequality holds for natural numbers  $d, n \geq 1$ :

$$T(d, n) < \text{Tower}(d, n).$$

(See Notation 104 for the definition of  $\text{Tower}(d, n)$ .)

*Proof.* We induct on  $n$ , starting with  $n = 1$ . By definition,  $T(d, 1) = (F_{2 \cdot T(d, 0) + 1}) \cdot T(d, 0) = F_{2d+1}d$ . We observe the following:

$$\begin{aligned} F_{2d+1}d &< 2^{2d+1}d && \text{(Lemma 102)} \\ &< 2^{2d+1}2^d = 2^{3d+1} = \text{Tower}(d, 1). \end{aligned}$$

This proves the base case. Now suppose the inequality holds for  $n = k$ ; i.e.,  $T(d, k) < \text{Tower}(d, k)$ . The inductive case is similar but we now have an additional power of 2,

allowing us to use Lemma 103. By definition,  $T(d, k+1) = (F_{2 \cdot T(d,k)+1}) \cdot T(d, k)$ . We obtain the following:

$$\begin{aligned}
(F_{2 \cdot T(d,k)+1}) \cdot T(d, k) &< 2^{(2 \cdot \text{Tower}(d,k)+1)} \cdot 2^{\log_2 \text{Tower}(d,k)} && \text{(Lemma 102 and inductive hypothesis)} \\
&= 2^{(2 \cdot \text{Tower}(d,k)+1+\log_2 \text{Tower}(d,k))} \\
&< 2^{(2 \cdot 2^{\log_2 \text{Tower}(d,k)}+2 \log_2 \text{Tower}(d,k))} && (\log_2 \text{Tower}(d, k) > 2) \\
&< 2^{(3 \cdot 2^{\log_2 \text{Tower}(d,k)})} && \text{(Lemma 103)} \\
&= 2^{(3 \cdot \text{Tower}(d,k))} \\
&< \text{Tower}(d, k+1). && \text{(Lemma 105)}
\end{aligned}$$

This completes the proof.  $\square$

**Theorem 107** (Degree complexity of  $\text{RGA}_o$ ). *Let  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$ ,  $A, S$  satisfy the hypotheses of Theorem 96, the termination and correctness result for  $\text{RGA}_o$ . Suppose further that each element of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$ ,  $A, S$  has degree at most  $d$ . Then every nondifferential polynomial returned by  $\text{RGA}_o(A, S)$  has degree at most  $R(d, n)$ , defined recursively by  $R(d, n)_0 := T(d, n)$ ,  $R(d, n)_{k+1} := T(d + R(d, n)_k, n)$  for  $0 \leq k < n$ , and  $R(d, n) := R(d, n)_n$ . (The values  $R(d, n)_k$  give bounds on intermediate polynomials' degrees after  $\text{RGA}_o$  has recursively called itself  $k$  times out of the maximum possible  $n$ . The outputs containing a proper derivative form a subset of  $\mathbf{x}' - \mathbf{f}(\mathbf{x})$ , so their degree is bounded by  $d$ .)*

*Proof.* As noted in the correctness proof (Theorem 96),  $\text{RGA}_o$  alternates between calls to **Triangulate** and to itself. The first possible call is to **Triangulate**, producing nondifferential polynomials of degree at most  $T(d, n) = R(d, n)_0$ . Then in step 3 an ODE  $x' - f(\mathbf{x})$  may be pseudodivided by the derivative of a nondifferential polynomial  $q$ ; this at most adds the degrees of the dividend and divisor, yielding  $d + T(d, n)$ . (Recall that  $s_q(x' - f(\mathbf{x})) - q' = \tilde{r}$ , where  $\tilde{r}$  is the pseudoremainder. The total degree of  $s_q(x' - f(\mathbf{x}))$  is at most  $d + T(d, n)$ . In fact,  $d + T(d, n) - 1$  is a strict upper bound because the degree of the separant actually goes down, but we ignore this. The proper derivatives in  $\tilde{r}$  all come from  $q'$ , which has total degree at most  $T(d, n)$ . After replacing the proper derivatives using the relations  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  and obtaining  $r$ , the total degree in the transformed version of  $q'$  is also at most  $d + T(d, n)$ .)

Another call to **Triangulate** yields  $T(d + T(d, n), n) = R(d, n)_1$  and restarts the process (beginning with pseudodivision in step 3 since the equations are now triangular and have their separants in the set of inequations). After  $k$  iterations have eliminated  $k$  ODEs, the degree is at most  $R(d, n)_k$ , whence pseudodivision and another call to **Triangulate** yield  $R(d, n)_{k+1} = T(d + R(d, n)_k, n)$ .  $\square$

**Notation 108.** For natural numbers  $d, n \geq 1$  and  $0 \leq k \leq n$  we define

$$RTower(d, n)_k := 2^{\cdot^{\cdot^{\cdot^{\text{Tower}(d, n+k)}}}},$$

where the right-hand side is an exponent tower of height  $k(n - 1) + 1$  (i.e., the tower consists of nested exponents with  $k(n - 1)$  copies of 2 followed by a final exponent  $\text{Tower}(d, n + k)$ ).

We also define

$$\text{RTower}(d, n) := \text{RTower}(d, n)_n = 2^{\dots^{\text{Tower}(d, 2n)}}$$

where the right-hand side is an exponent tower of height  $n(n - 1) + 1$ .

**Theorem 109** (Explicit bounds on degree complexity of  $\text{RGA}_o$ ). *Let  $R(d, n)$  be the recursive function from Theorem 107 that bounds the degree complexity of the output of  $\text{RGA}_o$ . The following inequality holds for natural numbers  $d, n \geq 1$ :*

$$\underline{R(d, n)} < \text{RTower}(d, n).$$

(See Notation 108 for the definition of  $\text{RTower}(d, n)$ .)

*Proof.* We use induction on  $k$  for  $0 \leq k \leq n$  to bound  $R(d, n)_k$  (recall that  $R(d, n) := R(d, n)_n$ ). For  $k = 0$  we have  $R(d, n)_0 := T(d, n) < \text{Tower}(d, n)$  by Theorem 106; this equals  $\text{RTower}(d, n)_0$ , which is a tower with  $0 = 0(n - 1)$  copies of 2 followed by exponent  $\text{Tower}(d, n + 0)$ .

Now let  $0 \leq k < n$  and suppose  $R(d, n)_k < \text{RTower}(d, n)_k$ . We show that  $R(d, n)_{k+1} < \text{RTower}(d, n)_{k+1}$ .

$$\begin{aligned} R(d, n)_{k+1} &= T(d + R(d, n)_k, n) \\ &< \text{Tower}(d + R(d, n)_k, n) && \text{(Theorem 106)} \\ &< \text{Tower}(d + \text{RTower}(d, n)_k, n) && \text{(inductive hypothesis; Tower is an increasing function of both inputs)} \\ &= 2^{\dots^{3(d + \text{RTower}(d, n)_k) + \alpha}} && \text{(n copies of 2 (hence at least one); } \alpha := 1 \text{ if } n = 1 \text{ and } \alpha := n + 1 \text{ if } n > 1\text{)} \\ &= 2^{\dots^{3 \cdot \text{RTower}(d, n)_k + 3d + \alpha}} \\ &< 2^{\dots^{4 \cdot \text{RTower}(d, n)_k}} && \text{(unfold the definitions to see that } \text{RTower}(d, n)_k > 3d + \alpha\text{)} \\ &= 2^{\dots^{4 \cdot \left( 2^{\dots^{\text{Tower}(d, n+k)}} \right)}} && \text{(where the tower replacing } \text{RTower}(d, n)_k \text{ has } k(n - 1) \text{ copies of 2 followed by final exponent } \text{Tower}(d, n + k)\text{)} \\ &\leq 2^{\dots^{\left( 2^{\dots^{4 \cdot \text{Tower}(d, n+k)}} \right)}} \\ &\leq 2^{\dots^{\text{Tower}(d, n+k+1)}} && \text{(clear since } \text{Tower}(d, n+k) > 1\text{)} \end{aligned}$$

(Lemma 105 applies because the lower tower has at least one copy of 2; this reduces the copies of 2 by one and leaves  $n - 1 + k(n - 1) = (k + 1)(n - 1)$  copies)

$$= \text{RTower}(d, n)_{k+1}.$$

□

After expanding the top exponent  $\text{Tower}(d, 2n)$  of  $\text{RTower}(d, n)$ , the bound on  $\text{RGA}_o$  becomes an exponent tower with  $n(n-1) + 2n = n^2 + n$  copies of 2 followed by a final exponent  $3d + 2n + 1$ .

While the nonelementary bounds in Theorem 109 are enormous from a practical perspective, there are important compensating factors. As noted in Remark 95, other published versions of RGA use the same mechanism of recursive splitting and pseudodivision that blows up the bounds on `Triangulate` and hence on  $\text{RGA}_o$ . In spite of RGA's apparently high worst-case complexity, it has nonetheless been used profitably in applications (p. 36). Likewise, our experience (e.g., Sections 3.3, 4.2) shows that RGA has potential for studying algebraic invariants due to its systematic nature and universal results.

More theoretically, the problem of getting a differential radical decomposition of an explicit system with nondifferential inequations is close in spirit to the *non*-differential radical ideal membership problem. The *effective Nullstellensatz* [94] shows that radical ideal membership in polynomial rings over fields is strictly easier than general ideal membership in those rings. This opens the door for specialized approaches to radical ideal membership that outperform general Gröbner basis methods in terms of asymptotic complexity. (Möller and Mora [95] adapted a previous example [32] to prove doubly exponential lower bounds for Gröbner bases. In particular, they demonstrated ideals with generators of degree  $d$  in  $n$  variables such that *all* Gröbner bases using certain monomial orderings must have an element of degree doubly exponential in  $n$  and polynomial in  $d$ .) Szántó [87, 88] developed a characteristic set method of singly exponential complexity (in  $n$ , polynomial in  $d$ ) [96] for radical ideal membership. (See also [97, 98, 66, 99].) Szántó's method reduces radical ideal membership testing to checking whether polynomials pseudoreduce to zero modulo certain characteristic sets. (In fact, the theory is closely related to that of RGA.)

It may be possible to generalize this to the differential case and prove Lemma 94 while replacing `Triangulate` with a method of singly exponential complexity. The results of [100] and [91] imply that the invariant yielded by  $\text{RGA}_o$  can be obtained by other techniques with doubly exponential complexity (Section 5.2). This further supports the idea that some modification of `Triangulate` might dispense with the nonelementary bounds. Lastly, Theorem 112 and the resulting analysis in Section 4.4 suggest that the closely related problem of *checking* invariance has a very rare worst case and that singly exponential complexity is actually the norm.

#### 4.4. Invariance Checking, Totally Real Varieties, and Complexity

In this section we connect totally real varieties to invariance checking. Theorem 112 below and the subsequent commentary are also relevant to complexity and bounds.

**Proposition 110.** *Let  $A = \{p_1, \dots, p_m\} \subseteq \mathbb{R}[\mathbf{x}]$ , let  $\mathbf{F}$  be a polynomial vector field, and let  $\mathbf{V}_{\mathbb{R}}(A)$  be an invariant set with respect to  $\mathbf{F}$ . Then  $\sqrt[A]{A}$  is an invariant ideal. If in addition  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real, then  $\sqrt[A]{A}$  is an invariant ideal.*

*Proof.* By the real Nullstellensatz (Theorem 24) and statement 2 of Theorem 50, the ideal  $(\mathcal{L}_{\mathbf{F}}^*(A)) \subseteq \sqrt[\mathbb{R}]{(A)}$ . Since  $(A) \subseteq (\mathcal{L}_{\mathbf{F}}^*(A)) \subseteq \sqrt[\mathbb{R}]{(A)}$ , Proposition 23 (3a) shows that  $\sqrt[\mathbb{R}]{(\mathcal{L}_{\mathbf{F}}^*(A))} = \sqrt[\mathbb{R}]{(A)}$ . The ideal  $(\mathcal{L}_{\mathbf{F}}^*(A))$  is closed under Lie differentiation and hence is invariant; it follows by Lemma 52 that  $\sqrt[\mathbb{R}]{(A)}$  is invariant.

If  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real, then by Proposition 23 (2),(3b) and Proposition 33 we have  $\sqrt{(A)} = \sqrt[\mathbb{R}]{(A)}$ , which is invariant by the preceding paragraph.  $\square$

**Proposition 111.** *Let  $A = \{p_1, \dots, p_m\} \subseteq \mathbb{R}[\mathbf{x}]$  and let  $\mathbf{F}$  be a polynomial vector field. If  $\mathcal{L}_{\mathbf{F}}(p_j) \notin \sqrt[\mathbb{R}]{(A)}$  for some  $1 \leq j \leq m$ , then  $\mathbf{V}_{\mathbb{R}}(A)$  is not an invariant set with respect to  $\mathbf{F}$ . If  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real and  $\mathcal{L}_{\mathbf{F}}(p_j) \notin \sqrt{(A)}$  for some  $1 \leq j \leq m$ , then  $\mathbf{V}_{\mathbb{R}}(A)$  is not invariant.*

*Proof.* Immediate from Proposition 110 because the hypotheses of Proposition 111 imply that  $\sqrt[\mathbb{R}]{(A)}$  and  $\sqrt{(A)}$ , respectively, are not invariant ideals.  $\square$

The next theorem generalizes to multiple polynomials Lie's criterion for invariance of smooth algebraic manifolds [91, Fig. 1][101, Thm. 2.8]: let  $h \in \mathbb{R}[\mathbf{x}]$  and assume that the real variety  $\mathbf{V}_{\mathbb{R}}(h)$  has no singular points. Lie's criterion then implies that  $\mathbf{V}_{\mathbb{R}}(h)$  is invariant with respect to polynomial vector field  $\mathbf{F}$  if the first Lie derivative  $\mathcal{L}_{\mathbf{F}}(h)$  vanishes everywhere on  $\mathbf{V}_{\mathbb{R}}(h)$ .

**Theorem 112.** *Let  $A = \{p_1, \dots, p_m\} \subseteq \mathbb{R}[\mathbf{x}]$  and let  $\mathbf{F}$  be a polynomial vector field. If  $(A)$  is real radical (i.e.,  $(A) = \sqrt[\mathbb{R}]{(A)}$ ), then  $\mathbf{V}_{\mathbb{R}}(A)$  is an invariant set with respect to  $\mathbf{F}$  if and only if  $\mathcal{L}_{\mathbf{F}}(p_j) \in (A)$  for all  $1 \leq j \leq m$ . Equivalently, if  $\mathbf{V}_{\mathbb{C}}(A)$  is totally real and  $(A)$  is radical (i.e.,  $(A) = \sqrt{(A)}$ ), then  $\mathbf{V}_{\mathbb{R}}(A)$  is an invariant set with respect to  $\mathbf{F}$  if and only if  $\mathcal{L}_{\mathbf{F}}(p_j) \in (A)$  for all  $1 \leq j \leq m$ .*

*Proof.* Immediate from Corollary 51 and Proposition 111.  $\square$

Theorem 112 raises some important questions. How common is it for  $\mathbf{V}_{\mathbb{C}}(A)$  to be totally real and  $(A)$  to be radical, and can we check those properties efficiently? Regarding the prevalence of totally real varieties, we make the following observations about Theorem 44, which states that the complex variety corresponding to an irreducible real algebraic variety defined by a single polynomial  $p \in \mathbb{R}[\mathbf{x}]$  is totally real if and only if  $p$  assumes both positive and negative values as  $\mathbf{x}$  varies over  $\mathbb{R}^n$ .

Fix the degree  $d$ . Blekherman ([102, Thm. 1.1]) has given an asymptotic, probabilistic result showing that for large  $n = |\mathbf{x}|$ , a randomly chosen polynomial almost certainly attains both positive and negative values. (More precisely, [102] puts a probability measure on the space of polynomials and shows that as  $n \rightarrow \infty$ , the ratio of the measure of the set of nonnegative polynomials and the measure of the set of all polynomials goes to 0. See the first inequality in Theorem 1.1 of [102], which gives an upper bound  $c_2 n^{-1/2}$  on this ratio for some constant  $c_2$ .) Also, if  $n \geq 2$  the space of reducible polynomials of at most a given bounded degree has strictly lower dimension than the space of all polynomials with that bound on the degree (see Example 113 below). Hence for large  $n$  a randomly chosen polynomial  $p \in \mathbb{R}[\mathbf{x}]$  will almost certainly define a totally real complex variety by Theorem 44 because  $p$  will almost certainly be irreducible and take on both positive and negative values. We suspect that a similar

result holds for varieties that are defined by multiple, possibly reducible, polynomials (i.e., the generic situation should be that a complex variety defined over  $\mathbb{R}$  is totally real).

We are not aware of specific results on the prevalence of radical ideals among all ideals, but we expect that a “typical” ideal (with respect to some reasonable probability distribution) is radical. Consequently, we hypothesize that for almost all (in a precise sense that would require additional work to specify) complex varieties defined over the reals, checking invariance with respect to a polynomial vector field reduces by Theorem 112 to checking membership of the first Lie derivatives in the ideal generated by the defining polynomials of the variety.

This leads to an interesting situation with regard to the computational complexity of checking for invariance. Given  $A \subseteq \mathbb{R}[x]$ , if  $V_{\mathbb{C}}(A)$  is totally real and  $(A)$  is radical, then we can check invariance of  $V_{\mathbb{R}}(A)$  with complexity singly exponential in the number of variables. (This requires a singly exponential test for radical ideal membership like Szántó’s [87, 88].) As explained in the preceding paragraph, we have reason to believe that this is possible for almost all choices of  $A$ .

However, we are left with the “measure zero” cases where  $V_{\mathbb{C}}(A)$  is not totally real or  $(A)$  is not radical. Determining whether a given candidate  $A$  has these properties appears, in the worst case, to be doubly exponential in the number of variables. For instance, decomposing a variety into irreducible components (which seems unavoidable for determining if the variety is totally real) has doubly exponential lower bounds in  $n$  [103, Thm. 1]. (In particular, Chistov shows that for sufficiently large  $n, d$  there are polynomials in  $n$  variables of degree less than  $d$  defining a reducible variety with a component whose corresponding prime ideal has no set of generators with all elements having degree less than a certain doubly exponential bound.) Likewise, checking if a variety is radical is closely related to *primary ideal decomposition* [30, Sect. 4.8], which has doubly exponential complexity (following again from [103, Thm. 1]).

In summary, then, we suspect that with singly exponential complexity we can almost always correctly guess whether a given  $A$  is invariant, but *proving* that we have the correct answer may require doubly exponential complexity. (This is similar, but not identical, to the hypothesis—also possibly true—that proving invariance of an algebraic set has singly exponential average-case complexity but doubly exponential worst-case complexity.) However, we cannot discard the possibility that the worst case is also singly exponential; settling the matter appears difficult.

**Example 113.** *As part of the preceding analysis we claimed that the set of reducible polynomials of at most a given bounded degree has smaller dimension than the set of all such polynomials, and hence there is a precise sense in which almost all polynomials are irreducible. If  $n = 1$ , then over  $\mathbb{C}$  every polynomial of degree  $d > 1$  is reducible, so we only care about the case  $n \geq 2$ . Rather than prove a formal theorem with full details, we illustrate with a simple case that mirrors the general result (the example is based on an argument from [104]).*

*Let  $K$  be an algebraically closed field and consider  $P_{2,d \leq 2} \setminus \{0\} \subseteq K[x, y]$ , where  $P_{2,d \leq 2} \setminus \{0\}$  is the set of all nonzero polynomials over  $K$  in two variables having degree at most 2. An arbitrary element of  $P_{2,d \leq 2} \setminus \{0\}$  has the form  $p = a_1 + a_2x + a_3y + a_4x^2 + a_5xy + a_6y^2$ , with not all  $a_i$  being zero. We can thus identify  $p$  with the 6-tuple*

$(a_1, \dots, a_6) \in K^6 \setminus \{0\}$ . Irreducibility is not affected by nonzero scalar multiples, so it is natural to view  $p$  as a point  $(a_1 : \dots : a_6)$  in  $\mathbb{P}^5(K)$ , the five-dimensional projective space over  $K$  [30, Sect. 8.2]. By definition,  $\mathbb{P}^5(K)$  is the quotient of  $K^6 \setminus \{0\}$  by the equivalence relation  $\sim$  such that  $\mathbf{a} \sim \mathbf{b}$  if and only if there exists  $0 \neq \alpha \in K$  such that  $\alpha \mathbf{a} = \mathbf{b}$ . (Going forward we omit the  $K$  in  $\mathbb{P}^5(K)$ .) For instance, both  $1 + 2x^2 - 3xy$  and  $-2 - 4x^2 + 6xy$  correspond to  $(1 : 0 : 0 : 2 : -3 : 0) \in \mathbb{P}^5$ .

Points of  $\mathbb{P}^5$  that correspond to reducible polynomials in  $K[x, y]$  are contained in the image of the map  $f : \mathbb{P}^2 \times \mathbb{P}^2 \rightarrow \mathbb{P}^5$  defined by

$$f((b_1 : b_2 : b_3), (c_1 : c_2 : c_3)) = (b_1 c_1 : b_1 c_2 + b_2 c_1 : b_1 c_3 + b_3 c_1 : b_2 c_2 : b_2 c_3 + b_3 c_2 : b_3 c_3).$$

This point represents the factorization  $p = qr$ , where  $q = b_1 + b_2 x + b_3 y$  and  $r = c_1 + c_2 x + c_3 y$ . The image of  $f$  has dimension at most  $4 = 2 + 2 = \dim(\mathbb{P}^2) + \dim(\mathbb{P}^2) = \dim(\mathbb{P}^2 \times \mathbb{P}^2) < \dim(\mathbb{P}^5) = 5$ . These values are justified by Examples 1.30, 1.33 (p. 67) and Theorem 1.25 (p. 75) of [42]. Hence every polynomial corresponding to a point in the “large” set  $\mathbb{P}^5 \setminus f(\mathbb{P}^2 \times \mathbb{P}^2)$  (the complement of a lower-dimensional set) is irreducible.

**Remark 114.** We note that the prevalence of totally real and/or irreducible varieties is also relevant to the complexity of generating *equations* for algebraic invariants. In particular, Theorem 88 implies that these and other conditions make it easier to interpret the output of  $\text{RGA}_o$ . For instance, suppose  $\text{RGA}_o$  returns a collection of regular differential systems  $(A_1, S_1), \dots, (A_r, S_r)$  and each  $(A_i, S_i)$  satisfies the hypotheses of Theorem 88 (2). Then we may ignore the (doubly exponential) complication of finding generators of the saturation ideals  $(A_i \cap \mathbb{R}[\mathbf{x}]) : S_i^\infty$  because the invariant is simply  $\bigcup_{i=1}^r \mathbf{V}_{\mathbb{R}}(A_i \cap \mathbb{R}[\mathbf{x}])$  and the inequations are superfluous. (Compare to Theorem 98 (3).)

## 5. Related work

### 5.1. Invariant Generation and Checking

Several recent algebraic algorithms for generating invariants are close in spirit to our use of  $\text{RGA}_o$ . In particular, all are *template methods* that find invariants having the form of a parameterized polynomial input (see the example in Section 4.2). However,  $\text{RGA}_o$ ’s basic elimination method (namely, differential pseudodivision) is unique in the class. This leads to a major advantage of our approach:  $\text{RGA}_o$  avoids both Gröbner bases and real quantifier elimination. In particular, we obtain the largest possible invariant that is consistent with the input system without having to test ideal membership or the vanishing of Lie derivatives.

Liu, Zhan, and Zhao [105] proved that invariance of semialgebraic sets (i.e., defined by polynomial equations and inequalities over the real numbers) with respect to a polynomial vector field is decidable and gave an algorithm—referred to here as the **LZZ** algorithm—for the problem of checking invariance. By enforcing an invariance criterion on a template, the algorithm gives a way of generating invariants of a given form. The chief downside of LZZ is that it uses two expensive tools, Gröbner bases and real quantifier elimination. (The generation version only uses real quantifier elimination, but the template might need to be large to find a nontrivial invariant.)

Ghorbal and Platzer [56] contributed a procedure that here we refer to as DRI (“differential radical invariant”). Given a homogeneous template polynomial  $h$  with parameter coefficients, assume an order  $N$  and write a symbolic matrix representing membership of the  $N$ -th Lie derivative of  $h$  in the ideal generated by  $h$  and the preceding  $N - 1$  Lie derivatives. DRI seeks an invariant of maximal dimension with this form by minimizing the rank of the symbolic matrix.

One virtue of DRI is completeness: any algebraic invariant that exists can be produced by choosing  $N$  and the degree of  $h$  to be sufficiently large [56, Cor. 1]. Another is its reliance on linear algebra (similar to [106, 107], which DRI partly generalizes), an area with many efficient computational tools. DRI does not use Gröbner bases, but nonlinear real arithmetic/quantifier elimination is generally required to find parameter values that minimize the rank. DRI has considerable power, as demonstrated by a number of nontrivial case studies from the aerospace domain [56, Sect. 6]. Nonetheless, it is significantly slower than the following two algorithms [33, Sect. 6].

Kong et al. [108] use a similar idea for invariant generation, though they restrict themselves to the case of invariants  $p$  that are *Darboux polynomials*. This means that the Lie derivative  $\dot{p} = ap$  for some polynomial  $a$  (i.e.,  $p$  divides its own Lie derivative with respect to the vector field in question). This prevents completeness, but also contributes to better empirical performance when it applies [108, Table 1]. However, the implementation still uses Gröbner bases and nonlinear real arithmetic [108, Remark 3].

Recent work of Boreale [33] has strong ties to both DRI [56] and [108]. The POST algorithm [33, p. 9] builds on the same theory as [56] but focuses on invariants containing a given initial set. Moreover, POST uses Gröbner bases and an iterative process involving descending chains of vector spaces and ascending chains of ideals. In some sense, Boreale’s work is intermediate between that of [56] and [108]: POST offers completeness guarantees missing from [108] but in general is slower than [108] and faster than DRI. Boreale also uses POST and a generic point of the initial set to study the semialgebraic case.

In [91] Ghorbal, Sogokon, and Platzer give an invariant checking algorithm that is related to LZZ but is restricted to algebraic sets and improves efficiency in that case. Like LZZ, the method in [91] uses Gröbner bases and nonlinear real arithmetic. The algorithm computes successive Lie derivatives of the input  $A \subseteq \mathbb{R}[\mathbf{x}]$  and checks ideal membership (where Gröbner bases come in) until the first-order Lie derivatives of all preceding elements belong to the ideal generated by those elements. This will eventually happen by Hilbert’s basis theorem (Theorem 2), so  $A$  and the subsequent Lie derivatives computed up to that stage generate  $(\mathcal{L}_{\mathbf{F}}^*(A))$  (see our comments immediately preceding Theorem 98). Real arithmetic checks that each Lie derivative computed vanishes on all of  $\mathbf{V}_{\mathbb{R}}(A)$ . This holds if and only if  $\mathbf{V}_{\mathbb{R}}(A)$  is invariant with respect to  $\mathbf{F}$  (Corollary 51).

The recent ESE invariant checking algorithm of [109] refines and extends both LZZ and [91]. ESE again uses Gröbner bases and real arithmetic, but it structures quantifier elimination subproblems more efficiently than does LZZ and, unlike [91], applies to semialgebraic sets. Based on the topological notion of *exit sets* [110] (which concern vector field trajectories exiting the boundary of a set in  $\mathbb{R}^n$ ), the ESE algorithm can verify or disprove invariance of a candidate semialgebraic set. ESE is often much faster than an enhanced version of LZZ that is also described in [109].



We lastly mention a new approach of Wang et al. [111] for generating *invariant barrier certificates* (a concept closely tied to invariants; see [111, Thm. 4]). The method employs Gröbner bases to find a sufficient number of Lie derivatives and uses them to satisfy conditions [111, Def. 4] that guarantee a template is an invariant barrier certificate. However, [111] then translates the criterion into a numerical optimization problem. Experiments show promising performance, but the method’s reliance on local extrema occasionally results in erroneous output [111, Table 1]. (Wang et al. provide the option of searching for global extrema using a branch-and-bound technique, but this can increase the complexity substantially.) This contrasts with the trade-offs made by fully symbolic methods like  $\text{RGA}_o$  for generating or checking invariants.

## 5.2. Complexity

As indicated in Section 5.1, the **order of Lie derivatives needed to check invariants** is an important factor in the complexity of the algorithms from [105, 91, 33, 111, 109]. The best upper bound known is **doubly exponential in the number of variables** [100, Thm. 4], but both [109] and [100] suggest this is overly conservative. This intuition is consistent with our discussion in Section 4.4, where Theorem 112 collapses invariance checking to a single round of radical ideal membership testing (assuming a radical ideal that defines a totally real variety; we argued that this should almost always hold). Whether or not the worst-case complexity is greater than singly exponential, it is necessarily considerable since generating algebraic invariant sets is NP-hard [56, p. 289].)

In another direction, Section 4.3 demonstrates that the complexity of  $\text{RGA}$  is non-trivial to analyze. While degree bounds for  $\text{RGA}$  have not previously appeared, upper bounds on the *order* of intermediate and output differential polynomials have been worked out [79, 112]. The order bounds on  $\text{RGA}$  from [79] amount to  $n!$  for ODEs of the form  $\mathbf{x}' = \mathbf{f}(\mathbf{x})$  in  $n$  variables. However, this result is excessive for  $\text{RGA}_o$  because we differentiate at most  $n$  times. Moreover, in  $\text{RGA}_o$  we only handle differential polynomials of order at most 1 since we use the explicit form to substitute nondifferential polynomials for proper derivatives.

Degree bounds for differential characteristic sets appear in [113, Thm. 5.48], but these are again excessive for our situation.

## 6. Conclusion

In this paper we have adapted the Rosenfeld-Gröbner algorithm to generate algebraic invariants of polynomial differential systems. Finding invariants is a crucial and computationally difficult task that our method tackles with a new and systematic approach using tools from algebraic geometry, differential algebra, and the theory of regular systems. Our algorithm  $\text{RGA}_o$  provides an alternative to the traditional Gröbner bases and real quantifier elimination while giving a novel representation of the largest algebraic invariant contained in an input algebraic set. We have also highlighted the prevalence and importance of totally real varieties for reducing the computational complexity of both generating and checking invariants of differential equations.

The unique aspects of  $\text{RGA}_o$  provide multiple directions for future work. One important goal is modifying the subroutine `Triangulate` to preserve differential solutions

while obtaining a regular algebraic decomposition with singly exponential complexity. Beyond theoretical complexity improvements, our framework would greatly benefit from effective heuristics (e.g., for detecting totally real varieties) and optimizations like pruning superfluous branches in `Triangulate`. Some rankings are much easier to compute than others [114], so translating from one differential ranking to another could be an important strategy. Partial runs of `RGAo` are another interesting possibility. In our experience, the final iterations of the algorithm tend to be drastically more expensive than the early ones while yielding less additional information (e.g., giving relatively trivial, low-dimensional chains when we already know the generic chain). The example in 4.2 demonstrates this; we are most interested in the generic Chain 2 and would like the option of only computing it.

The treatment of parameters is also a critical matter. Our example used auxiliary variables with constant derivative, but this is suboptimal. Fakouri et al. [77] describe a modified version of RGA designed to more efficiently identify all possible regular chains corresponding to different values of parameters. Adapting this algorithm to our problems could be important for a more scalable `RGAo`.

While purely algebraic invariants are important for continuous dynamical systems and enjoy strong decidability properties [4], many polynomial vector fields have no such invariants that are nontrivial (not isolated points, coordinate axes, etc.). The Van der Pol oscillator is an example that nonetheless has interesting semialgebraic invariants [115, 116]. In the literature there are several encodings of inequalities as equations using auxiliary variables (e.g., [117, 118]). Our initial investigation suggests that this idea, together with RGA, can yield insights into semialgebraic invariants of nonlinear systems with non-obvious dynamics.

In light of these prospects, we view our results in this paper as laying the groundwork for an enhanced method that produces easily verified invariants, combines optimal theoretical complexity with strong practical performance, and is broadly applicable. Progress on these fronts could lead to inclusion in practical tools for CPS verification such as the theorem prover `KeYmaera X` [119] with its automatic invariant-generating utility, `Pegasus` [71].

*Acknowledgements.* We are grateful to François Boulier, Khalil Ghorbal, and Yong Kiam Tan for helpful exchanges. This work was supported by the AFOSR under grants FA9550-18-1-0120 and FA9550-16-1-0288.

## References

- [1] A. Platzer, *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*, Springer, Heidelberg, 2010. doi:10.1007/978-3-642-14509-4.
- [2] A. Platzer, *Logical Foundations of Cyber-Physical Systems*, Springer, 2018. doi:10.1007/978-3-319-63588-0. URL <https://doi.org/10.1007/978-3-319-63588-0>
- [3] A. Goriely, *Integrability and nonintegrability of dynamical systems*, Vol. 19, World Scientific, 2001.

- [4] A. Platzer, Y. K. Tan, Differential equation invariance axiomatization, *J. ACM* 67 (1) (2020) 6:1–6:66. doi:10.1145/3380825.
- [5] Y. K. Tan, A. Platzer, Deductive stability proofs for ordinary differential equations, in: *TACAS* (2), Vol. 12652 of *Lecture Notes in Computer Science*, Springer, 2021, pp. 181–199.
- [6] Y. K. Tan, A. Platzer, An axiomatic approach to existence and liveness for differential equations, *Formal Aspects of Computing* (2021) 1–58.
- [7] E. Rodríguez-Carbonell, A. Tiwari, Generating polynomial invariants for hybrid systems, in: M. Morari, L. Thiele (Eds.), *HSCC*, Vol. 3414 of *LNCS*, Springer, 2005, pp. 590–605.
- [8] S. Sankaranarayanan, H. B. Sipma, Z. Manna, Constructing invariants for hybrid systems, *Form. Methods Syst. Des.* 32 (1) (2008) 25–55. doi:10.1007/s10703-007-0046-1.
- [9] A. Tiwari, Generating box invariants, in: M. Egerstedt, B. Mishra (Eds.), *HSCC*, Vol. 4981 of *LNCS*, Springer, 2008, pp. 658–661.
- [10] A. Platzer, E. M. Clarke, Computing differential invariants of hybrid systems as fixedpoints, *Form. Methods Syst. Des.* 35 (1) (2009) 98–120. doi:10.1007/s10703-009-0079-8.
- [11] S. Sankaranarayanan, Automatic invariant generation for hybrid systems using ideal fixed points, in: K. H. Johansson, W. Yi (Eds.), *HSCC*, ACM, 2010, pp. 221–230. doi:10.1145/1755952.1755984.
- [12] S. Sankaranarayanan, A. Tiwari, Relational abstractions for continuous and hybrid systems, in: G. Gopalakrishnan, S. Qadeer (Eds.), *CAV*, Vol. 6806 of *LNCS*, Springer, Berlin, 2011, pp. 686–702. doi:10.1007/978-3-642-22110-1\_56.
- [13] A. Taly, S. Gulwani, A. Tiwari, Synthesizing switching logic using constraint solving, *STTT* 13 (6) (2011) 519–535. doi:10.1007/s10009-010-0172-8.
- [14] A. Platzer, A differential operator approach to equational differential invariants, in: L. Beringer, A. Felty (Eds.), *ITP*, Vol. 7406 of *LNCS*, Springer, 2012, pp. 28–48.
- [15] B. Wu, X. Zou, Computing invariants for hybrid systems, in: *Electronic System-Integration Technology Conference (ESTC)*, 2012 4th, 2012, pp. 203–206. doi:10.1109/ESTC.2012.6485572.
- [16] K. Ghorbal, A. Platzer, Characterizing algebraic invariants by differential radical invariants, in: E. Ábrahám, K. Havelund (Eds.), *TACAS*, Vol. 8413 of *LNCS*, Springer, 2014, pp. 279–294. doi:10.1007/978-3-642-54862-8\_19.

- [17] A. Sogokon, K. Ghorbal, P. B. Jackson, A. Platzer, A method for invariant generation for polynomial continuous systems, in: B. Jobstmann, K. R. M. Leino (Eds.), *Verification, Model Checking, and Abstract Interpretation - 17th International Conference, VMCAI 2016, St. Petersburg, FL, USA, January 17-19, 2016. Proceedings*, Vol. 9583 of *Lecture Notes in Computer Science*, Springer, 2016, pp. 268–288. doi:10.1007/978-3-662-49122-5\_13. URL [https://doi.org/10.1007/978-3-662-49122-5\\_13](https://doi.org/10.1007/978-3-662-49122-5_13)
- [18] P. Roux, Y. Voronin, S. Sankaranarayanan, Validating numerical semidefinite programming solvers for polynomial invariants, in: X. Rival (Ed.), *Static Analysis - 23rd International Symposium, SAS 2016, Edinburgh, UK, September 8-10, 2016. Proceedings*, Vol. 9837 of *LNCS*, Springer, 2016, pp. 424–446. doi:10.1007/978-3-662-53413-7\_21.
- [19] S. Sankaranarayanan, Change-of-bases abstractions for non-linear hybrid systems, *Nonlinear Analysis: Hybrid Systems 19 (2016)* 107 – 133.
- [20] H. Kong, S. Bogomolov, C. Schilling, Y. Jiang, T. A. Henzinger, Safety verification of nonlinear hybrid systems based on invariant clusters, in: G. Frehse, S. Mitra (Eds.), *Proceedings of the 20th International Conference on Hybrid Systems: Computation and Control, HSCC 2017, Pittsburgh, PA, USA, April 18-20, 2017, ACM, 2017*, pp. 163–172.
- [21] M. Boreale, Complete algorithms for algebraic strongest postconditions and weakest preconditions in polynomial ode’s, in: A. M. Tjoa, L. Bellatreche, S. Biffl, J. van Leeuwen, J. Wiedermann (Eds.), *SOFSEM 2018: Theory and Practice of Computer Science - 44th International Conference on Current Trends in Theory and Practice of Computer Science, Krems, Austria, January 29 - February 2, 2018. Proceedings*, Vol. 10706 of *LNCS*, Springer, 2018, pp. 442–455.
- [22] K. Ghorbal, A. Sogokon, Characterizing positively invariant sets: Inductive and topological methods, *J. Symb. Comput.* 113 (2022) 1–28. doi:10.1016/j.jsc.2022.01.004. URL <https://doi.org/10.1016/j.jsc.2022.01.004>
- [23] A. Sogokon, S. Mitsch, Y. K. Tan, K. Cordwell, A. Platzer, Pegasus: Sound continuous invariant generation, *Form. Methods Syst. Des.* 58 (1) (2022) 5–41, special issue for selected papers from FM’19. doi:10.1007/s10703-020-00355-z.
- [24] D. Wang, *Elimination Methods, Texts & Monographs in Symbolic Computation*, Springer, 2001. doi:10.1007/978-3-7091-6202-6. URL <https://doi.org/10.1007/978-3-7091-6202-6>
- [25] J. Bochnak, M. Coste, M.-F. Roy, *Real algebraic geometry*, Vol. 36 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Springer, 1998.

- [26] E. R. Kolchin, Differential algebra and algebraic groups, Pure and Applied Mathematics, Vol. 54, Academic Press, New York-London, 1973.
- [27] W. Li, C. Yuan, Elimination theory in differential and difference algebra, *J. Syst. Sci. Complex.* 32 (1) (2019) 287–316.  
doi:10.1007/s11424-019-8367-x.  
URL <https://doi.org/10.1007/s11424-019-8367-x>
- [28] L. M. Pardo, How lower and upper complexity bounds meet in elimination theory, in: *AAECC*, Vol. 948 of Lecture Notes in Computer Science, Springer, 1995, pp. 33–69.
- [29] B. Mishra, Algorithmic algebra, Texts and Monographs in Computer Science, Springer-Verlag, New York, 1993.
- [30] D. Cox, J. Little, D. O’Shea, Ideals, varieties, and algorithms, 4th Edition, Undergraduate Texts in Mathematics, Springer, 2015.
- [31] G. Gallo, B. Mishra, Efficient algorithms and bounds for Wu-Ritt characteristic sets, in: *Effective methods in algebraic geometry*, Springer, 1991, pp. 119–142.
- [32] E. W. Mayr, A. R. Meyer, The complexity of the word problems for commutative semigroups and polynomial ideals, *Advances in Mathematics* 46 (3) (1982) 305–329.
- [33] M. Boreale, Complete algorithms for algebraic strongest postconditions and weakest preconditions in polynomial  
*Sci. Comput. Program.* 193 (2020) 102441.  
doi:10.1016/j.scico.2020.102441.  
URL <https://doi.org/10.1016/j.scico.2020.102441>
- [34] E. Becker, R. Neuhaus, Computation of real radicals of polynomial ideals, in: *Computational algebraic geometry*, Springer, 1993, pp. 1–20.
- [35] L. Menini, C. Possieri, A. Tornambè, Algebraic Geometry for Robotics and Control Theory, World Scientific, 2021.
- [36] D. Richardson, Some undecidable problems involving elementary functions of a real variable, *The Journal of Symbolic Logic* 33 (4) (1969) 514–520.
- [37] F. Boulier, D. Lazard, F. Ollivier, M. Petitot, Representation for the radical of a finitely generated differential ideal, in: *ISSAC*, ACM, 1995, pp. 158–166.
- [38] S. Lang, Algebra, 3rd Edition, Vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, 2002.
- [39] W. Rudin, Real and Complex Analysis, 3rd Ed., McGraw-Hill, Inc., USA, 1987.
- [40] S. Mac Lane, Categories for the working mathematician, 2nd Edition, Vol. 5 of Graduate Texts in Mathematics, Springer Science & Business Media, 2013.

- [41] O. Ore, Galois connexions, *Transactions of the American Mathematical Society* 55 (3) (1944) 493–513.
- [42] I. R. Shafarevich, *Basic algebraic geometry 1*, 3rd Edition, Springer-Verlag, Berlin Heidelberg, 2013, translated from the 2007 Russian edition by Miles Reid. doi:<https://doi.org/10.1007/978-3-642-37956-7>.
- [43] M. Michałek, B. Sturmfels, *Invitation to nonlinear algebra*, Vol. 211 of Graduate Studies in Mathematics, American Mathematical Soc., 2021.
- [44] F. Boulier, F. Ollivier, D. Lazard, M. Petitot, Computing representations for radicals of finitely generated differential ideals, *Appl. Algebra Engrg. Comput.* 20 (1) (2009) 73–121. doi:[10.1007/s00200-009-0091-7](https://doi.org/10.1007/s00200-009-0091-7). URL <http://dx.doi.org/10.1007/s00200-009-0091-7>
- [45] F. Sottile, Real algebraic geometry for geometric constraints, in: M. Sitharam, A. S. John, J. Sidman (Eds.), *Handbook of geometric constraint systems principles*, CRC Press, 2019, pp. 273–286.
- [46] T. Sander, *Aspects of algebraic geometry over non algebraically closed fields*, Technical report, International Comp. Sci. Institute (1996).
- [47] M. Marshall, Positive polynomials and sums of squares, no. 146, American Mathematical Soc., 2008.
- [48] K. Harris, J. D. Hauenstein, Á. Szántó, Smooth points on semi-algebraic sets, *ACM Commun. Comput. Algebra* 54 (3) (2020) 105–108.
- [49] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics 52. Springer-Verlag, 1977.
- [50] G. Blekherman, R. Sinn, G. G. Smith, M. Velasco, Sums of squares: A real projective story, *Notices of the American Mathematical Society* 68 (5) (2021).
- [51] P. Conti, C. Traverso, A case of automatic theorem proving in euclidean geometry: the Maclane  $8_3$  theorem, in: *AAECC*, Vol. 948 of Lecture Notes in Computer Science, Springer, 1995, pp. 183–193.
- [52] D. Wang, Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases, *Comput. Aided Geom. Des.* 9 (6) (1992) 471–484.
- [53] J. H. Hubbard, B. B. Hubbard, *Vector calculus, linear algebra, and differential forms: a unified approach*, Matrix Editions, 2015.
- [54] W. Walter, *Ordinary Differential Equations*, 1st Edition, Graduate Texts in Mathematics, 182, Springer New York, 1998.
- [55] C. Christopher, J. Llibre, C. Pantazi, S. Walcher, Inverse problems for multiple invariant curves, *Proceedings of the Royal Society of Edinburgh Section A: Mathematics* 137 (6) (2007) 1197–1226.

- [56] K. Ghorbal, A. Platzer, Characterizing algebraic invariants by differential radical invariants, in: TACAS, Vol. 8413 of Lecture Notes in Computer Science, Springer, 2014, pp. 279–294.
- [57] J. F. Ritt, Differential Algebra, Dover Publications, New York, 1950.
- [58] E. R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1976.
- [59] D. Marker, Model theory of differential fields, Model Theory of Fields, eds. D. Marker, M. Messmer, & A. Pillay 5 (2005) 41–109.
- [60] A. Robinson, On the concept of a differentially closed field, Office of Scientific Research, US Air Force, 1959.
- [61] D. Marker, Introduction to the model theory of fields, Model Theory of Fields, eds. D. Marker, M. Messmer, & A. Pillay 5 (2005) 1–37.
- [62] H. B. Enderton, Elements of set theory, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1977.
- [63] W. Y. Sit, The Ritt–Kolchin theory for differential polynomials, in: W. Y. Sit (Ed.), Differential algebra and related topics, World Scientific, 2002, pp. 1–70.
- [64] F. Boulier, Differential elimination and biological modelling, in: Workshop D2.2 of the Special Semester on Gröbner Bases and Related Methods, Vol. 2, de Gruyter, 2006, pp. 111–139.
- [65] F. Boulier, F. Lemaire, M. M. Maza, A. Poteaux, A short contribution to the theory of regular chains, Math. Comput. Sci. 15 (2) (2021) 177–188.
- [66] P. Aubry, D. Lazard, M. M. Maza, On the theories of triangular sets, J. Symb. Comput. 28 (1-2) (1999) 105–124.
- [67] E. N. Lorenz, Deterministic nonperiodic flow, Journal of atmospheric sciences 20 (2) (1963) 130–141.
- [68] C. Sparrow, The Lorenz equations: bifurcations, chaos, and strange attractors, Vol. 41, Springer Science & Business Media, 2012.
- [69] J. Llibre, X. Zhang, Invariant algebraic surfaces of the Lorenz system, Journal of Mathematical Physics 43 (3) (2002) 1622–1645.
- [70] S. P. Swinnerton-Dyer, The invariant algebraic surfaces of the Lorenz system, in: Mathematical Proceedings of the Cambridge Philosophical Society, Vol. 132, Cambridge University Press, 2002, pp. 385–393.
- [71] A. Sogokon, S. Mitsch, Y. K. Tan, K. Cordwell, A. Platzer, Pegasus: sound continuous invariant generation, Formal Methods Syst. Des. 58 (1-2) (2021) 5–41.

- [72] F. Boulier, F. Lemaire, A normal form algorithm for regular differential chains, *Math. Comput. Sci.* 4 (2-3) (2010) 185–201.
- [73] E. Hubert, Essential components of an algebraic differential equation, *J. Symb. Comput.* 28 (4-5) (1999) 657–680.
- [74] U. Umirbaev, Algorithmic problems for differential polynomial algebras, *Journal of Algebra* 455 (2016) 77–92.
- [75] M. (Waterloo Maple Inc.), Overview of the DifferentialAlgebra package (online documentation), <https://www.maplesoft.com/support/help/maple/view.aspx?path=DifferentialAlgebra>, Accessed: 2021-09-01.
- [76] F. Boulier, BLAD software package, <https://www.lifl.fr/%7Eboulier/pmwiki/pmwiki.php?n=>, Accessed: 2021-09-01.
- [77] S. Fakouri, S. Rahmany, A. Basiri, A new algorithm for computing regular representations for radicals of parametric differential ideals, *Cogent Mathematics & Statistics* 5 (1) (2018) 1507131.
- [78] A. Hashemi, Z. Touraji, An improvement of Rosenfeld-Gröbner algorithm, in: *ICMS, Vol. 8592 of Lecture Notes in Computer Science*, Springer, 2014, pp. 466–471.
- [79] O. Golubitsky, M. V. Kondratieva, M. M. Maza, A. Ovchinnikov, A bound for the Rosenfeld-Gröbner algorithm, *J. Symb. Comput.* 43 (8) (2008) 582–610.
- [80] D. Bouziane, A. Kandri-Rody, H. Maarouf, Unmixed-dimensional decomposition of a finitely generated perfect differential ideal, *J. Symb. Comput.* 31 (6) (2001) 631–649.
- [81] E. Hubert, Factorization-free decomposition algorithms in differential algebra, *J. Symb. Comput.* 29 (4-5) (2000) 641–662.
- [82] R. Ushirobira, D. V. Efimov, P. Blirnan, Estimating the infection rate of a SIR epidemic model via differential elimination, in: *ECC, IEEE*, 2019, pp. 1170–1175.
- [83] N. Verdière, S. Zhu, L. Denis-Vidal, A distribution input-output polynomial approach for estimating parameters in nonlinear models: application to a chikungunya model, *J. Comput. Appl. Math.* 331 (2018) 104–118.
- [84] F. Boulier, F. Lemaire, Differential algebra and system modeling in cellular biology, *Algebraic Biology* (2008) 22–39.
- [85] H. A. Harrington, K. L. Ho, N. Meshkat, A parameter-free model comparison test using differential algebra, *Complex.* 2019 (2019) 6041981:1–6041981:15.



- [86] J.-Y. Hong, K. Hara, J.-W. Kim, E. F. Sato, E. B. Shim, K.-H. Cho, Minimal systems analysis of mitochondria-dependent apoptosis induced by cisplatin, *The Korean Journal of Physiology & Pharmacology* 20 (4) (2016) 367–378.
- [87] Á. Szántó, Complexity of the Wu-Ritt decomposition, in: *PASCO*, ACM, 1997, pp. 139–149.
- [88] A. Szántó, Computation with polynomial systems, PhD dissertation, Cornell University, 1999.
- [89] A. V. Aho, J. E. Hopcroft, J. D. Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley, 1974.
- [90] G. Gallo, B. Mishra, Wu-Ritt characteristic sets and their complexity, in: *Discrete and Computational Geometry*, Vol. 6 of DIMACS Series in Discrete Mathematics and Theoretical Computer Science, DIMACS/AMS, 1990, pp. 111–136.
- [91] K. Ghorbal, A. Sogokon, A. Platzer, Invariance of conjunctions of polynomial equalities for algebraic differential equations, in: *SAS*, Vol. 8723 of Lecture Notes in Computer Science, Springer, 2014, pp. 151–167.
- [92] A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa, The membership problem for unmixed polynomial ideals is solvable in single exponential time, *Discret. Appl. Math.* 33 (1-3) (1991) 73–94.
- [93] W. D. Wallis, J. C. George, *Introduction to combinatorics*, Chapman and Hall/CRC, 2010.
- [94] W. D. Brownawell, Bounds for the degrees in the Nullstellensatz, *Annals of Mathematics* 126 (3) (1987) 577–591.
- [95] H. M. Möller, F. Mora, Upper and lower bounds for the degree of Groebner bases, in: *EUROSAM*, Vol. 174 of Lecture Notes in Computer Science, Springer, 1984, pp. 172–183.
- [96] E. Amzallag, M. Sun, G. Pogudin, T. N. Vo, Complexity of triangular representations of algebraic sets, *Journal of Algebra* 523 (2019) 342–364.
- [97] P. Bürgisser, P. Scheiblechner, On the complexity of counting components of algebraic varieties, *J. Symb. Comput.* 44 (9) (2009) 1114–1136.
- [98] F. Boulier, F. Lemaire, M. M. Maza, Well known theorems on triangular systems and the D5 principle, in: *Transgressive Computing 2006*, J.-G. Dumas, Université Joseph Fourier, Grenoble, France, 2006, pp. 79–91.
- [99] M. Kalkbrener, Prime decompositions of radicals in polynomial rings, *J. Symb. Comput.* 18 (4) (1994) 365–372.
- [100] D. Novikov, S. Yakovenko, Trajectories of polynomial vector fields and ascending chains of polynomial ideals, in: *Annales de l’institut Fourier*, Vol. 49, 1999, pp. 563–609.

- [101] P. J. Olver, Applications of Lie groups to differential equations, 2nd Edition, Vol. 107 of Graduate Texts in Mathematics, Springer, 2000.
- [102] G. Blekherman, There are significantly more nonnegative polynomials than sums of squares, *Israel Journal of Mathematics* 153 (1) (2006) 355–380.
- [103] A. Chistov, Double-exponential lower bound for the degree of any system of generators of a polynomial prime ideal, *St. Petersburg Mathematical Journal* 20 (6) (2009) 983–1001.
- [104] Q. Yuan, Are most polynomials reducible or irreducible?, *Mathematics Stack Exchange*, <https://math.stackexchange.com/q/459881> (version: 2013-08-05, accessed 2022-05-30).
- [105] J. Liu, N. Zhan, H. Zhao, Computing semi-algebraic invariants for polynomial dynamical systems, in: EMSOFT, ACM, 2011, pp. 97–106.
- [106] R. Rebiha, A. V. Moura, N. Matringe, Generating invariants for non-linear hybrid systems, *Theor. Comput. Sci.* 594 (2015) 180–200.
- [107] N. Matringe, A. V. Moura, R. Rebiha, Generating invariants for non-linear hybrid systems by linear algebraic methods, in: SAS, Vol. 6337 of Lecture Notes in Computer Science, Springer, 2010, pp. 373–389.
- [108] H. Kong, S. Bogomolov, C. Schilling, Y. Jiang, T. A. Henzinger, Safety verification of nonlinear hybrid systems based on invariant clusters, in: HSCC, ACM, 2017, pp. 163–172.
- [109] K. Ghorbal, A. Sogokon, Characterizing positively invariant sets: Inductive and topological methods, *J. Symb. Comput.* 113 (2022) 1–28.
- [110] C. C. Conley, Isolated invariant sets and the Morse index, no. 38, American Mathematical Soc., 1978.
- [111] Q. Wang, M. Chen, B. Xue, N. Zhan, J. Katoen, Synthesizing invariant barrier certificates via difference-of-convex programming, in: CAV (1), Vol. 12759 of Lecture Notes in Computer Science, Springer, 2021, pp. 443–466.
- [112] R. Gustavson, A. Ovchinnikov, G. Pogudin, New order bounds in differential elimination algorithms, *J. Symb. Comput.* 85 (2018) 128–147.
- [113] W. Simmons, H. Towsner, Proof mining and effective bounds in differential polynomial rings, *Advances in Mathematics* 343 (2019) 567–623.
- [114] F. Boulier, Efficient computation of regular differential systems by change of rankings using kähler differentials, in: MEGA 2000, 2000.
- [115] M. Jones, M. M. Peet, Using SOS for optimal semialgebraic representation of sets: Finding minimal representations of limit cycles, chaotic attractors and unions, in: ACC, IEEE, 2019, pp. 2084–2091.

- [116] K. Odani, The limit cycle of the van der Pol equation is not algebraic, *Journal of Differential Equations* 115 (1) (1995) 146–152.
- [117] A. Platzer, J. Quesel, P. Rümmer, Real world verification, in: *CADE*, Vol. 5663 of *Lecture Notes in Computer Science*, Springer, 2009, pp. 485–501.
- [118] B. D. O. Anderson, R. W. Scott, Output feedback stabilization—solution by algebraic geometry methods, *Proceedings of the IEEE* 65 (6) (1977) 849–861.
- [119] N. Fulton, S. Mitsch, J. Quesel, M. Völz, A. Platzer, Keymaera X: an axiomatic tactical theorem prover for hybrid systems, in: *CADE*, Vol. 9195 of *Lecture Notes in Computer Science*, Springer, 2015, pp. 527–538.