Characterizing Algebraic Invariants by Differential Radical Invariants

Khalil Ghorbal **André Platzer**
{kghorbal|aplatzer}@cs.cmu.edu

January 2014
CMU-CS-13-129

Publisher:
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA, 15213

To appear [6] in the
Proceedings of the 20th International Conference on
Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2014),
5-14 April 2014, Grenoble, France.

This material is based upon work supported by the National Science Foundation by NSF CAREER Award CNS-1054246, NSF EXPEDITION CNS-0926181 and grant no. CNS-0931985. This research is also partially supported by the Defense Advanced Research Projects Agency under contract no. DARPA FA8750-12-2-0291. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of any sponsoring institution or government.

Keywords: invariant algebraic sets, polynomial vector fields, real algebraic geometry, Zariski topology, higher-order Lie derivation, automated generation and checking, symbolic linear algebra, rank minimization, formal verification, hybrid systems

Abstract

We prove that any invariant algebraic set of a given polynomial vector field can be algebraically represented by one polynomial and a finite set of its successive Lie derivatives. This so-called *differential radical characterization* relies on a sound abstraction of the reachable set of solutions by the smallest variety that contains it. The characterization leads to a differential radical invariant proof rule that is sound and complete, which implies that invariance of algebraic equations over real-closed fields is decidable. Furthermore, the problem of generating invariant varieties is shown to be as hard as minimizing the rank of a symbolic matrix, and is therefore NP-hard. We investigate symbolic linear algebra tools based on Gaussian elimination to efficiently automate the generation. The approach can, e.g., generate nontrivial algebraic invariant equations capturing the airplane behavior during take-off or landing in longitudinal motion.

1 Introduction

Reasoning about the solutions of differential equations by means of their conserved functions and expressions is ubiquitous all over science studying dynamical processes. It is even crucial in many scientific fields (e.g. control theory or experimental physics), where a guarantee that the behavior of the system will remain within a certain predictable region is required. In computer science, the interest of the automated generation of these conserved expressions, so-called *invariants*, was essentially driven and motivated by the formal verification of different aspects of hybrid systems, i.e. systems combining discrete dynamics with differential equations for the continuous dynamics.

The verification of hybrid systems requires ways of handling both the discrete and continuous dynamics, e.g., by proofs [20], abstraction [27, 35], or approximation [13]. Fundamentally, however, the study of the safety of hybrid systems can be shown to reduce constructively to the problem of generating invariants for their differential equations [23]. We focus on this core problem in this paper. We study the case of *algebraic invariant equation*, i.e. invariants described by a polynomial equation of the form $h = 0$ for a polynomial h. We also only consider algebraic differential equations (or algebraic vector fields), i.e. systems of ordinary differential equations in (vectorial) explicit form $\frac{d\boldsymbol{x}}{dt} = \boldsymbol{p}(\boldsymbol{x})$, with a polynomial right-hand side, $\boldsymbol{p}$. The class of algebraic vector fields is far from restrictive and many analytic nonalgebraic functions, such as the square root, the inverse, the exponential or trigonometric functions, can be exactly modeled as solutions of ordinary differential equations with a polynomial vector field (a concrete example will be given in Section 6.2).

While algebraic invariant equations are not the only invariants of interest for hybrid systems [24, 22], they are still intimately related to all other algebraic invariants, such as semialgebraic invariants. We, thus, believe that the characterization we achieve in this paper to be an important step forward in understanding the invariance problem of polynomial vector fields, and hence the hybrid systems with polynomial vector fields.

Our results indicate that algebraic geometry is well suited to reason about and effectively compute algebraic invariant equations. Relevant concepts and results from algebraic geometry will be introduced and discussed as needed.

Content In Section 2, we introduce a precise algebraic abstraction of the reachable set of the solution of a generic algebraic initial value problem. This abstraction is used to give a necessary and sufficient condition for a polynomial h to have the reachable set of the solution as a subset of the set of its roots. Section 3 builds on top of this characterization to, firstly, check the invariance of a variety candidate (Section 3.1) and, secondly, give an algebraic characterization for a variety to be an invariant for a polynomial vector field (Section 3.2). The characterization of invariant varieties is exploited in Section 4 where the generation of invariant varieties is reduced to symbolic linear algebra computation. The contributions of this work are summarized in Section 5 right after discussing the related work. Finally, Section 6 presents three case studies to highlight the importance of our approach through concrete and rather challenging examples.

2 Sound and Precise Algebraic Abstraction by Zariski Closure

We consider autonomous[1] algebraic initial value problems (see Def. 1 below). A nonautonomous system with polynomial time dependency can be reformulated as an autonomous system by adding a clock variable that reflects the progress of time. In this section, we investigate algebraic invariant equations for the considered initial value problems. This study is novel and will turn out to be fruitful from both the theoretical and practical points of view. The usual approach which assumes the initial value to be in a region of the space, often an algebraic set, will be discussed in Section 3.

Let $\boldsymbol{x} = (x_1, \ldots, x_n) : \mathbb{R}^n$, and $\boldsymbol{x}(t) = (x_1(t), \ldots, x_n(t))$, where $x_i : \mathbb{R} \to \mathbb{R}$, $t \mapsto x_i(t)$. The initial value $\boldsymbol{x}(t_\iota) = (x_1(t_\iota), \ldots, x_n(t_\iota)) \in \mathbb{R}^n$, for some $t_\iota \in \mathbb{R}$, will be denoted by $\boldsymbol{x}_\iota$. We do not consider any additional constraint on the dynamics, that is the evolution domain corresponds to the domain of definition.

Definition 1 (Algebraic Initial Value Problem)**.** *Let p_i, $1 \leq i \leq n$, be multivariate polynomials of the polynomial ring $\mathbb{R}[\boldsymbol{x}]$. An* algebraic initial value problem *is a pair of an explicit algebraic ordinary differential equations system (or polynomial vector field), $\boldsymbol{p}$, and an initial value, $\boldsymbol{x}_\iota \in \mathbb{R}^n$:*

$$\frac{dx_i}{dt} = \dot{x}_i = p_i(\boldsymbol{x}), 1 \leq i \leq n,\ \boldsymbol{x}(t_\iota) = \boldsymbol{x}_\iota \ . \tag{1}$$

Since polynomial functions are smooth (C^∞, i.e. they have derivatives of any order), they are locally Lipschitz-continuous. By Cauchy-Lipschitz theorem (a.k.a. Picard-Lindelöf theorem) [14], there exists a unique maximal solution to the initial value problem (1) defined on some nonempty open set $U_t \subseteq \mathbb{R}$. A global solution defined for all $t \in \mathbb{R}$ may not exist in general. For instance, the maximal solution $x(t)$ of the 1-dimensional system $\left\{\dot{x} = x^2, x(t_\iota) = x_\iota \neq 0\right\}$ is defined on $\mathbb{R} \setminus \{t_\iota + x_\iota^{-1}\}$.

Algebraic invariant equations for initial value problems are defined as follows.

Definition 2 (Algebraic Invariant Equation (Initial Value Problem))**.** *An* algebraic invariant equation *for the initial value problem* (1) *is an expression of the form $h(\boldsymbol{x}(t)) = 0$ that holds true for all $t \in U_t$, where $h \in \mathbb{R}[\boldsymbol{x}]$ and $\boldsymbol{x} : U_t \to \mathbb{R}^n$, is the (unique) maximal solution of Eq.* (1)*.*

Notice that any (finite) disjunction of conjunctions of algebraic invariant equations over the reals is also an algebraic invariant equation (w.r.t. Def. 2) using the following equivalence ($\mathbb{R}[\boldsymbol{x}]$ is an integral domain):

$$\bigvee_i \bigwedge_j f_{i,j} = 0 \longleftrightarrow \prod_i \sum_j f_{i,j}^2 = 0 \ . \tag{2}$$

In Def. 2, the function $h(\boldsymbol{x}(t))$, and hence the polynomial $h(\boldsymbol{x})$, depend on the fixed but unknown initial value $\boldsymbol{x}_\iota$. We implicitly assume this dependency for a clearer notation and will emphasize it whenever needed. Also, observe that $h(\boldsymbol{x}(t))$, seen as a real valued function of time t, is only defined over the open set $U_t \subseteq \mathbb{R}$ since the solution $\boldsymbol{x}(t)$ is itself only defined over U_t. The polynomial function $h : \mathbb{R}^n \to \mathbb{R}; \boldsymbol{x} \mapsto h(\boldsymbol{x})$ is, however, defined for all $\mathbb{R}^n$.

[1] Autonomous means that the rate of change of the system over time depends only on the system's state, not on time.

Geometrically, the equation $h(\boldsymbol{x}) = 0$ is represented by the set of its roots which is a subset of $\mathbb{R}^n$. Such a set is called an *affine variety*, or simply a variety[2]. We introduce and formalize the use of varieties as a sound abstraction of the reachable set of the solution of Eq. (1).

Definition 3 (Orbit)**.** *The* orbit*, or reachable set, of the solution of Eq.* (1)*,* $\boldsymbol{x}(t)$ *is defined as*

$$\mathcal{O}(\boldsymbol{x}_\iota) \stackrel{\text{def}}{=} \{\boldsymbol{x}(t) \mid t \in U_t\} \subseteq \mathbb{R}^n \ .$$

The complete geometrical characterization of the orbit requires the exact solution of Eq. (1). Very few initial value problems admit an analytic solution, although a local approximation can be always given using Taylor series approximations (such approximation is for instance used in [13] for the verification of hybrid systems). In this work, we introduce a sound abstraction of the orbit, $\mathcal{O}(\boldsymbol{x}_\iota)$, using varieties. The idea is to embed the orbit (which is not a variety in general) in a variety to be defined. The embedding we will be using is a well-known topological closure operation in algebraic geometry called the *Zariski closure* ([9, Chapter 1]). Varieties, which are sets of points, can be represented and computed efficiently using their algebraic counterpart: ideals of polynomials. Therefore, we first recall three useful definitions: an ideal of the ring $\mathbb{R}[\boldsymbol{x}]$, the variety of a subset of $\mathbb{R}[\boldsymbol{x}]$, and finally the vanishing ideal of a subset of $\mathbb{R}^n$.

Definition 4 (Ideal)**.** *An* ideal I *is a subset of* $\mathbb{R}[\boldsymbol{x}]$ *that contains the polynomial zero (*0*), is stable under addition, and external multiplication. That is, for all* $h_1, h_2 \in I$*, the sum* $h_1 + h_2 \in I$*; and if* $h \in I$*, then,* $qh \in I$*, for all* $q \in \mathbb{R}[\boldsymbol{x}]$*.*

For a finite natural number r, we denote by $\langle h_1, \ldots, h_r \rangle$ the subset of $\mathbb{R}[\boldsymbol{x}]$ generated by the polynomials $\{h_1, \ldots, h_r\}$, i.e. the set of linear combinations of the polynomials h_i (where the coefficients are themselves polynomials):

$$\langle h_1, \ldots, h_r \rangle \stackrel{\text{def}}{=} \left\{ \sum_{i=1}^{r} g_i h_i \mid g_1, \ldots, g_r \in \mathbb{R}[\boldsymbol{x}] \right\} \ .$$

By Def. 4, the set $\langle h_1, \ldots, h_r \rangle$ is an ideal. More interestingly, by Hilbert's Basis Theorem [10], any ideal I of the Noetherian ring $\mathbb{R}[\boldsymbol{x}]$ can be *finitely generated* by, say $\{h_1, \ldots, h_r\}$, so that $I = \langle h_1, \ldots, h_r \rangle$.

Definition 5 (Variety or Algebraic Set or Zeros Set)**.** *Given* $Y \subseteq \mathbb{R}[\boldsymbol{x}]$*, the* variety *(over the reals),* $V(Y)$*, is a subset of* $\mathbb{R}^n$ *defined by the common roots of all polynomials in* Y*. That is,*

$$V(Y) \stackrel{\text{def}}{=} \left\{ \boldsymbol{x} \in \mathbb{R}^n \mid \forall h \in Y, h(\boldsymbol{x}) = 0 \right\} \ .$$

$V(\cdot)$ can be thought of as an operator that maps subsets of $\mathbb{R}[\boldsymbol{x}]$ to subsets of $\mathbb{R}^n$. In general, the map $V(\cdot)$ is not injective even when applied to ideals: two distinct subsets of $\mathbb{R}[\boldsymbol{x}]$ can be mapped to the exact same variety. For instance, in $\mathbb{R}[x_1, x_2]$, the ideals $I_1 = \langle x_1, x_2^2 \rangle$ and $I_2 = \langle x_1^2, x_2 \rangle$, are mapped to the point $(x_1, x_2) = (0, 0)$ (which is a variety). The ideals I_1 and I_2 are distinct and incomparable: the polynomial $x_1 \in I_1$ is not in I_2 but $x_2 \in I_2$ is not in I_1.

[2]Some authors use the terminology algebraic sets so that varieties is reserved for irreducible algebraic sets. Here we will use both terms equally.

Definition 6 (Vanishing Ideal)**.** *The* vanishing ideal *(over the reals), $I(S)$, of $S \subseteq \mathbb{R}^n$ is the set of all polynomials that evaluates to zero for all $\boldsymbol{x} \in S$:*

$$I(S) \stackrel{\text{def}}{=} \left\{h \in \mathbb{R}[\boldsymbol{x}] \mid \forall \boldsymbol{x} \in S, h(\boldsymbol{x}) = 0\right\} \ . \tag{3}$$

The set $I(S) \subseteq \mathbb{R}[\boldsymbol{x}]$ is an ideal as it satisfies the requirements of Def. 4. Likewise, we can think of $I(\cdot)$ (Def. 6) as a non-injective operator that acts on subsets of $\mathbb{R}^n$. For instance, the two intervals $[1, 2]$ and $[-2, -1]$ are subsets of $\mathbb{R}$ mapped to the same ideal, namely $\langle 0 \rangle$. However, when restricted to varieties, the operator $I(\cdot)$ is injective.

We state the following well-known result (see, e.g. [4, Chapter 4, Theorem 7]) for convenience as it permits to switch back and forth between varieties of $\mathbb{R}^n$ and ideals of $\mathbb{R}[\boldsymbol{x}]$.

Proposition 1 (Ideal-Variety Correspondence)**.** *For any ideals I_1 and I_2 of $\mathbb{R}[\boldsymbol{x}]$, if $I_1 \subseteq I_2$, then $V(I_1) \supseteq V(I_2)$. Likewise, for any varieties V_1 and V_2 of $\mathbb{R}^n$, if $V_1 \subseteq V_2$, then $I(V_1) \supseteq I(V_2)$. Furthermore, for any variety S, we have $V(I(S)) = S$ and for any ideal Y, we have $Y \subseteq I(V(Y))$.*

We are now ready to formally define the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ of the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ as the variety of the vanishing ideal of $\mathcal{O}(\boldsymbol{x}_\iota)$:

$$\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \stackrel{\text{def}}{=} V(I(\mathcal{O}(\boldsymbol{x}_\iota))) \ . \tag{4}$$

That is, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is defined as the set of all points that are common roots of all polynomials that are zero everywhere on the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$. The variety $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ soundly overapproximates all reachable states $\boldsymbol{x}(t)$ in the orbit of $\mathcal{O}(\boldsymbol{x}_\iota)$, including, the initial value $\boldsymbol{x}_\iota$:

Proposition 2 (Soundness of Zariski Closure)**.** $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$.

Proof. All points of $\mathcal{O}(\boldsymbol{x}_\iota)$ are roots of some polynomial in its vanishing ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$ (Def. 6), and all roots of all polynomials in $I(\mathcal{O}(\boldsymbol{x}_\iota))$ are in $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ (Def. 5). Thus, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V(I(\mathcal{O}(\boldsymbol{x}_\iota))) = \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. □

Therefore, all safety properties that hold true for $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$, are also true for $\mathcal{O}(\boldsymbol{x}_\iota)$. The soundness in Proposition 2 corresponds to the reflexivity property of the Zariski closure: for any subset S of $\mathbb{R}^n$, $S \subseteq V(I(S))$. The algebraic geometrical fact that the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is the *smallest*[3] variety containing $\mathcal{O}(\boldsymbol{x}_\iota)$ corresponds to the fact that $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is the most precise algebraic abstraction of $\mathcal{O}(\boldsymbol{x}_\iota)$.

Observe that if the set of generators of $I(\mathcal{O}(\boldsymbol{x}_\iota))$ is only the zero polynomial, $I(\mathcal{O}(\boldsymbol{x}_\iota)) = \langle 0 \rangle$, then $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) = \mathbb{R}^n$ (the whole space) and the Zariski closure operation fails to be informative. The uselessness of the closure we use in this work happens exactly when there are no polynomials (in $\boldsymbol{x}$) which set of roots contain $\mathcal{O}(\boldsymbol{x}_\iota)$ other than the zero polynomial 0. For instance, for (non-degenerated) one dimensional vector fields ($n = 1$) that evolve over time, the only univariate polynomial that has infinitely many roots is the zero polynomial.

[3]Smallest here is to be understood w.r.t. to the usual geometrical sense, that is, any other variety containing $\mathcal{O}(\boldsymbol{x}_\iota)$, contains also its closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$.

Therefore, the accuracy of our subsequent computation inherits from the geometrical precision (sparsity of the closed sets in the Zariski topology) offered by the use of varieties as abstraction. If the orbit is precisely approximated by a variety, then we will be able to represent it precisely, otherwise, the abstraction will give rather pessimistic (still sound) approximations as seen for the one dimensional case. This points out the limitation of the closure operation used in this work and raises interesting question about how to deal with such cases. This will be left as future work.

The closure operation abstracts time. This means that $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ defines a subset of $\mathbb{R}^n$ within which the solution always evolves without saying anything about where the system will be at what time (which is what a solution would describe and which is exactly what the abstraction we are defining here gets rid off). In particular, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is independent of whether the system evolves forward or backward in time.

Although, we know that $I(\mathcal{O}(\boldsymbol{x}_\iota))$ is finitely generated, computing all its generators may be intractable. By the real Nullstellensatz, vanishing ideals over the reals are in fact exactly the real-radical ideals [1, Section 4.1]. In real algebraic geometry, real-radical ideals are notoriously hard to compute[4]. However, we shall see in the sequel that *Lie derivation* will give us a powerful computational handle that permits to tightly approximate (and even compute in some cases) $I(\mathcal{O}(\boldsymbol{x}_\iota))$. The Lie derivative of a polynomial along a vector field[5] is defined as follows.

Definition 7 (Lie Derivative)**.** *The* Lie derivative *of $h \in \mathbb{R}[\boldsymbol{x}]$, $\mathfrak{L}_{\boldsymbol{p}}(h)$, along the vector field $\boldsymbol{p} = (p_1, \ldots, p_n)$ is defined by:*

$$\mathfrak{L}_{\boldsymbol{p}}(h) \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial h}{\partial x_i} p_i \ . \tag{5}$$

Higher-order Lie derivatives are defined recursively: $\mathfrak{L}^{(0)}_{\boldsymbol{p}}(h) \stackrel{\text{def}}{=} h$ and

$$\mathfrak{L}^{(k+1)}_{\boldsymbol{p}}(h) \stackrel{\text{def}}{=} \mathfrak{L}_{\boldsymbol{p}}(\mathfrak{L}^{(k)}_{\boldsymbol{p}}(h)) \ .$$

Lie derivatives are closely related to time derivatives. In fact, they are equal.

Lemma 1 (Derivation)**.** *Let $h \in \mathbb{R}[\boldsymbol{x}]$. Then,*

$$\mathfrak{L}_{\boldsymbol{p}}(h) = \dot{h} \ .$$

Proof. The lemma follows from the chain rule: the polynomial h is seen as a function of $\boldsymbol{x}$ which is in turn a function of t (when $\boldsymbol{x}(t)$ is the solution of the initial value problem (see Def. 1). Thus,

$$\dot{h} = \frac{d}{dt} h(\boldsymbol{x}(t)) = \sum \frac{\partial h}{\partial x_i} \dot{x_i}(t) = \mathfrak{L}_{\boldsymbol{p}}(h) \ .$$

□

[4]Given an ideal $I \subseteq \mathbb{R}[\boldsymbol{x}]$, the degree of the polynomials that generate its real radical is bounded by the degree of polynomials that generate I to the power of $2^{O(n^2)}$ [19, Theorem 5.9].

[5]Lie derivatives can be defined on any sufficiently smooth function. In this work, we focus on polynomials.

The time derivation gives an analytic point of view, whereas the Lie derivative is purely algebraic and makes explicit the link to the vector field, which is hidden for $\dot{h}$. Therefore, although time is abstracted, we can still compute the time derivatives using Lie derivation.

We end this section by stating an important property of the vanishing ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Similar result is known under different formulations ([29, Theorem 3.1] and [21, Lemma 3.7] where algebraic invariant equations for a vector field are considered instead of algebraic invariant equations for an initial value problem as defined Def. 2).

Proposition 3. *$I(\mathcal{O}(\boldsymbol{x}_\iota))$ is a differential ideal for $\mathfrak{L}_{\boldsymbol{p}}$, i.e. it is stable under the action of the $\mathfrak{L}_{\boldsymbol{p}}$ operator. That is, for all $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, $\mathfrak{L}_{\boldsymbol{p}}(h) \in I(\mathcal{O}(\boldsymbol{x}_\iota))$.*

Proof. For the proof, we need to inject time into our reasoning. Let I denote $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Given $h \in I$, we prove that $\mathfrak{L}_{\boldsymbol{p}}(h) \in I$. If h is in I, then for all time $t \in U_t$, the vector $\boldsymbol{x}(t)$, solution of Eq. (1), is a zero of the polynomial $h(\boldsymbol{x})$. This means that the time function $h(\boldsymbol{x}(t))$, obtained by substituting $\boldsymbol{x}$ in h by the solution $\boldsymbol{x}(t)$, is a constant function and is actually equal to zero. Its time derivative is therefore also zero for all $\boldsymbol{x}(t)$. Since the time derivative of $h(\boldsymbol{x}(t))$ corresponds exactly to the Lie derivative of h, $\mathfrak{L}_{\boldsymbol{p}}(h)$, this means that $\boldsymbol{x}(t)$ is a zero of $\mathfrak{L}_{\boldsymbol{p}}(h)$, seen as a polynomial of $\mathbb{R}[\boldsymbol{x}]$. Therefore, $\mathfrak{L}_{\boldsymbol{p}}(h) \in I$, by definition of I. □

In the next section, we give a necessary and sufficient condition for a polynomial h to be in $I(\mathcal{O}(\boldsymbol{x}_\iota))$, that is for the expression $h = 0$ to be an algebraic invariant equation for the initial value problem (1), i.e. h evaluates to 0 all along the orbit of $\boldsymbol{x}_\iota$.

3 Differential Radical Characterization

In the previous section, the Zariski closure was used to embed the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ into the smallest variety containing it, namely $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. A variety $V(I)$, generated by the ideal I, can be represented using the ideal I, or approximated by any subset of I. In this section, we give an explicit characterization of the elements of the vanishing ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$ (see Def. 6).

For $h \in \mathbb{R}[\boldsymbol{x}]$, we recursively construct an ascending chain of ideals of $\mathbb{R}[\boldsymbol{x}]$ by appending higher-order Lie derivatives of h to the list of generators:

$$\langle h\rangle \subset \langle h, \mathfrak{L}_{\boldsymbol{p}}^{(1)}(h)\rangle \subset \cdots \subset \langle h, \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h)\rangle = \langle h, \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h)\rangle \ .$$

Since the ring $\mathbb{R}[\boldsymbol{x}]$ is Noetherian, the chain above has necessarily a finite length. The construction of the ascending chain above is very similar to the construction of the radical of an ideal[6], except with higher-order Lie derivatives, $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)$, in place of higher powers of polynomials, h^i. This motivates the following definition.

Definition 8 (Differential Radical Ideal)**.** *For $h \in \mathbb{R}[\boldsymbol{x}]$, let $1 \leq N < \infty$ be the smallest natural number such that:*

$$\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) \in \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h), \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h)\rangle \ . \tag{6}$$

[6]For a principal ideal, $\langle h\rangle$, the construction of its radical ideal, $\sqrt{\langle h\rangle}$ consists of augmenting $\langle h\rangle$ by all high powers h^i of the generating element h.

We call the ideal

$$\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle} \stackrel{\text{def}}{=} \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h), \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h) \rangle, \tag{7}$$

the differential radical ideal *of* h*.* N *will be referred to as the* order *of* $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$.

The following theorem, an important contribution of this work, states a necessary and sufficient condition for a polynomial h to be in $I(\mathcal{O}(\boldsymbol{x}_\iota))$.

Theorem 1 (Differential Radical Characterization)**.** *Let* $h \in \mathbb{R}[\boldsymbol{x}]$*, and let* N *denote the order of* $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$*. Then,* $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$ *if and only if*

$$\bigwedge_{0 \leq i \leq N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)(\boldsymbol{x}_\iota) = 0 \ . \tag{8}$$

Proof. Necessary condition. Let h be a polynomial in the ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Then, $\langle h \rangle \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$ (ideals are stable under exterior multiplication, see Def. 4). By Proposition 3, all higher-order Lie derivatives of h are also in $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Eq. (8) follows from the fact that all polynomials of $I(\mathcal{O}(\boldsymbol{x}_\iota))$ vanish on all point of $\mathcal{O}(\boldsymbol{x}_\iota)$, in particular for $\boldsymbol{x}_\iota$, since $\boldsymbol{x}_\iota \in \mathcal{O}(\boldsymbol{x}_\iota)$.

Sufficient condition. We prove that if Eq. (8) is satisfied then $h(\boldsymbol{x}(t)) = 0$ for all $\boldsymbol{x}(t) \in \mathcal{O}(\boldsymbol{x}_\iota)$, which implies the ideal membership by definition of $I(\mathcal{O}(\boldsymbol{x}_\iota))$ (Def. 6). Recall that U_t is the domain of definition (some open interval of $\mathbb{R}$) for t of the solution $\boldsymbol{x}(t)$. We define the real function $f : U_t \to \mathbb{R}$ by: $f(t) = h(\boldsymbol{x}(t))$. We want to prove that the function f is identically zero on U_t. Since N is the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$, by Eq. (6) (Def. 8), there exists a set of polynomials $g_i(\boldsymbol{x})$ such that

$$\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) - \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0 \ . \tag{9}$$

Let $\alpha_i : U_t \to \mathbb{R}$; $t \mapsto g_i(\boldsymbol{x}(t))$.The equality of Eq. (9), together with the initial value condition given by Eq. (8), can be transformed into the following homogeneous higher-order linear differential equation (recall from Lemma 1 that $\mathfrak{L}_{\boldsymbol{p}}(h) = \dot{h}$).

$$\begin{aligned} &f^{(N)}(t) - \sum_{i=0}^{N-1} \alpha_i(t) f^{(i)}(t) = 0, \\ &f^{(0)}(t_\iota) = f^{(1)}(t_\iota) = \cdots = f^{(N-1)}(t_\iota) = 0, \end{aligned} \tag{10}$$

where t_ι denotes the initial time. Notice that the function f, its higher-order time derivatives $f^{(i)}$, and the functions α_i are not necessarily polynomials as they depend on the solution $\boldsymbol{x}(t)$ of the initial value problem. We know, however, that they are all continuous functions which is enough for this proof.

The newly defined system in Eq. (10) can be seen as an N dimensional linear nonautonomous ($\alpha_i(t)$ are time dependent) system using the encoding $\boldsymbol{f} = \left(f^{(0)}, \ldots, f^{(N-1)}\right)$:

$$\dot{\boldsymbol{f}} - A(t)\boldsymbol{f} = \boldsymbol{0}, \tag{11}$$

where,

$$A(t) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ \alpha_0(t) & \alpha_1(t) & \cdots & \alpha_{N-2}(t) & \alpha_{N-1}(t) \end{pmatrix} .$$

In the newly defined linear system of Eq. (11), $A(t)\boldsymbol{f}$ is globally Lipschitz continuous, w.r.t. $\boldsymbol{f}$. That is, there exists a global Lipschitz constant, namely $\|A(t)\|$, the induced norm of $\mathbb{R}^N$ on the $\mathbb{R}^{N\times N}$ space, such that, for all t:

$$\forall \boldsymbol{f}_1, \boldsymbol{f}_2 \in \mathbb{R}^N, \quad \|A(t)\boldsymbol{f}_1 - A(t)\boldsymbol{f}_2\| \leq \|A(t)\|\|\boldsymbol{f}_1 - \boldsymbol{f}_2\| \ .$$

By Cauchy-Lipschitz theorem [14] (see [37, Chapter 14, Theorem VI] for the multi-linear case), there exists a unique solution $\boldsymbol{f}(t)$ defined on the entire interval U_t ($\alpha_i(t)$, and hence $A(t)$, are not defined outside U_t since both depend on the solution $\boldsymbol{x}(t)$), that satisfies the initial condition $\boldsymbol{f}_\iota = 0$. However, the null function, $\boldsymbol{f}(t) = \mathbf{0}$ is an obvious solution to Eq. (11), which satisfies $\boldsymbol{f}(t_\iota) = \mathbf{0}$. Hence, $\boldsymbol{f}(t)$ is identically zero for all $t \in U_t$. Since $\boldsymbol{f}(t) = \left(f^{(0)}, \ldots, f^{(N-1)}\right)$, by Lemma 1, for all, i, $0 \leq i \leq N-1$, $\mathfrak{L}^{(i)}_{\boldsymbol{p}}(h)(\boldsymbol{x}(t)) = 0$ for all $\boldsymbol{x}(t)$. Therefore, the polynomial h as well as all its Lie derivatives vanish on the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ and are hence members of $I(\mathcal{O}(\boldsymbol{x}_\iota))$. □

Going one step further, the differential radical characterization gives an insight about the algebraic structure of the vanishing ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$. In fact, if $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, then, by Proposition 3, $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h\rangle} \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$.

We will say that $h_1, h_2 \in I(\mathcal{O}(\boldsymbol{x}_\iota))$ are *distinct* if $h_1 \notin \sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_2\rangle}$ and $h_2 \notin \sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_1\rangle}$, so that their respective differential radical ideals are incomparable (in the sense of inclusion). Henceforth, $I(\mathcal{O}(\boldsymbol{x}_\iota))$ can be underapproximated by successive computation of its distinct elements h_j and, more importantly, their related differential radical ideals:

$$\bigoplus_{j\in\Im} \sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_j\rangle} \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota)) \ . \tag{12}$$

The sum of two ideals, denoted by $\oplus$, is the ideal generated by concatenating the list of generators of the operands. The finiteness of $\Im$ is assured by two facts: h_i are distinct (by hypothesis) and $I(\mathcal{O}(\boldsymbol{x}_\iota))$ has finitely many generators (by Hilbert's Basis Theorem).

As a consequence, the overapproximation of $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ can be refined at a cost of computing additional distinct elements of $I(\mathcal{O}(\boldsymbol{x}_\iota))$

Corollary 1. *Let $h_1, \ldots, h_r$ denote a set of distinct elements of $I(\mathcal{O}(\boldsymbol{x}_\iota))$, then*

$$\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq \bigcap_{1\leq i\leq r} V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_i\rangle}\right) \ . \tag{13}$$

Proof. For each h_i, $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_i\rangle} \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$ (Eq. (12)). Hence, $V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_i\rangle}\right) \supseteq V(I(\mathcal{O}(\boldsymbol{x}_\iota)))$ (Proposition 1), and $V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_i\rangle}\right) \supseteq \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ by definition of $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. □

So far, the initial value $\boldsymbol{x}_\iota \in \mathbb{R}^n$ was considered fixed, but *unconstrained*. The statement of Theorem 1 is general and assumes nothing about $\boldsymbol{x}_\iota$. A natural question to ask is how can differential radical characterization be used to reason about *invariant regions* of a given polynomial vector field ? By invariant (or stable) regions, we mean, regions $S \subset \mathbb{R}^n$ from which the trajectory of the solution of the initial value problem (1), with $\boldsymbol{x}_\iota \in S$, can never escape.

Definition 9 (Invariant Regions)**.** *The region $S \subseteq \mathbb{R}^n$ is invariant for the vector field $\boldsymbol{p}$ if and only if*

$$\forall \boldsymbol{x}_\iota \in S, \mathcal{O}(\boldsymbol{x}_\iota) \subseteq S \ .$$

In particular, we focus on invariant algebraic sets, that is, where S is variety. This choice is essentially motivated by the interesting algebraic properties of varieties. As a matter of fact, when S is a variety, the (intractable) orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ in Def. 9 can be equivalently substituted by its closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ allowing a powerful algebraic handle for invariant varieties.

Lemma 2. *The variety S is an invariant variety for the vector field $\boldsymbol{p}$ if and only if*

$$\forall \boldsymbol{x}_\iota \in S, \bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq S \ .$$

Proof. If S is an invariant variety then, for all $\boldsymbol{x}_\iota \in S$, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq S$ (Def. 9). However, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is the smallest variety containing $\mathcal{O}(\boldsymbol{x}_\iota)$. Therefore, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq S$.

On the other hand, since $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ (Proposition 2), then $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq S$ implies $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq S$. □

We highlight two interesting special cases of invariant varieties.

Equilibria. When S is reduced to exactly one fixed point in the space[7] the solution starts in $\boldsymbol{x}_\iota$ and remains in $\boldsymbol{x}_\iota$ forever.

Families of Invariant Varieties. When the invariant variety S is itself parametrized, we obtain a family of invariant varieties. For instance, for the 2-dimensional vector field $(p_1 = x_1, p_2 = x_2)$, the variety $S_\gamma = V(\langle \gamma_1 x_1 + \gamma_2 x_2 \rangle)$ is a family of invariant variety. Another well-known example consists of the class of polynomials that remain constant (for any chosen real constant) while the system evolves (see [22] for a detailed discussion). This class corresponds to invariant varieties of the form $S_c = V(\langle h(\boldsymbol{x}) - c \rangle)$, where $\mathfrak{L}_{\boldsymbol{p}}(h)$ is the polynomial 0.

Dual to the geometrical point of view in Lemma 2, the algebraic point of view is given by extending the definition of algebraic invariant equation for initial value problems (Def. 2), to algebraic invariant equation for polynomial vector fields.

Definition 10 (Algebraic Invariant Equation (Vector Field))**.** *The expression $h = 0$ is an algebraic invariant equation for the vector field $\boldsymbol{p}$ if and only if $V(\langle h \rangle)$ is an invariant variety for $\boldsymbol{p}$.*

Unlike Def. 2, Def. 10, corresponds to the typical object of study that one may find in the literature of algebraic invariant generation. Indeed, in hybrid system verification, they play an important role as they permit the abstraction of the continuous part by means of algebraic equations. In the two following sections, we show how differential radical characterization (Theorem 1) can be used to address two particular questions: *checking* the invariance of a variety candidate (Section 3.1) and *characterizing* invariant varieties (Section 3.2).

[7] An invariant region can never be empty as it contains at least $\boldsymbol{x}_\iota$ by definition.

3.1 Checking Invariant Varieties by Differential Radical Invariants

The problem we solve in this section is as follows: given a polynomial vector field $\boldsymbol{p}$, can we decide whether the equation $h = 0$ is an algebraic invariant equation for the vector field $\boldsymbol{p}$? Dually, we want to check whether the variety $V(\langle h \rangle)$ is invariant for $\boldsymbol{p}$. Using Theorem 1, we detail in the sequel how we solve this problem.

Before stating the theorem, for convenience, we recall the definition of a *real* ideal and announce the real Nullstellensatz following [1].

Definition 11 (Real Ideal [1, Definition 4.1.3])**.** *An ideal I of $\mathbb{R}[\boldsymbol{x}]$ is said to be* real *if and only if for every sequence $q_1, \ldots, q_r$ of elements of $\mathbb{R}[\boldsymbol{x}]$, we have*

$$q_1^2 + \cdots + q_r^2 \in I \longrightarrow q_i \in I, \text{ for } i = 1, \ldots, r \ .$$

In particular, all vanishing ideals are real ideals.

Lemma 3. *The vanishing ideal $I(S)$ of any $S \subseteq \mathbb{R}^n$ is a real ideal.*

Proof. If the polynomial $q_1^2 + \cdots + q_r^2$ is in $I(S)$, for some $q_1, \ldots, q_r \in \mathbb{R}[\boldsymbol{x}]$, then its set of roots contain S (Def. 6). However, we have the following equivalence over the reals

$$q_1^2 + \cdots + q_r^2 = 0 \leftrightarrow q_i = 0, \text{ for } i = 1, \ldots, r \ .$$

Thus, a root of the polynomial $q_1^2 + \cdots + q_r^2$ is also a root of the polynomials q_i, for $i = 1, \ldots, r$. This means that $q_i \in I(S)$ for $i = 1, \ldots, r$. By Def. 11, $I(S)$ is a real ideal. □

In $\mathbb{R}[\boldsymbol{x}]$, real ideals have an important property, they are fixed under the mapping $I(V(\cdot))$ (see Def. 6 and Def. 5).

Proposition 4 (Real Nullstellensatz [1, Theorem 4.1.4])**.** *Let Y be an ideal of $\mathbb{R}[\boldsymbol{x}]$. Then, $Y = I(V(Y))$ if and only if Y is real.*

The following new theorem gives a necessary and sufficient condition for a polynomial equation of the form $h = 0$ to be an algebraic invariant equation for the vector field $\boldsymbol{p}$.

Theorem 2. *Let $h \in \mathbb{R}[\boldsymbol{x}]$, and let N denote the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$. Then, $V(\langle h \rangle)$ is an invariant variety for the vector field $\boldsymbol{p}$ (or equivalently $h = 0$ is an algebraic invariant equation for $\boldsymbol{p}$) if and only if*

$$h = 0 \rightarrow \bigwedge_{1 \leq i \leq N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0 \ . \tag{14}$$

Proof. Necessary Condition. Let $\boldsymbol{x}_\iota$ be a root of h ($\boldsymbol{x}_\iota \in V(\langle h \rangle)$). If $V(\langle h \rangle)$ is an invariant variety, then $V(I(\mathcal{O}(\boldsymbol{x}_\iota))) = \bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq V(\langle h \rangle)$ (Lemma 2) and therefore $I(V(I(\mathcal{O}(\boldsymbol{x}_\iota)))) \supseteq I(V(\langle h \rangle))$ (Proposition 1). We know that $I(V(\langle h \rangle)) \supseteq \langle h \rangle$ and that $I(V(I(\mathcal{O}(\boldsymbol{x}_\iota)))) = I(\mathcal{O}(\boldsymbol{x}_\iota))$ (from Lemma 3, $I(\mathcal{O}(\boldsymbol{x}_\iota))$ is a real ideal, the equality follows from the real Nullstellensatz stated in Proposition 4), hence $I(\mathcal{O}(\boldsymbol{x}_\iota)) \supseteq \langle h \rangle$. This means that $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$ and Eq. (8) of Theorem 1 holds.

Sufficient Condition. Let $\boldsymbol{x}_\iota \in V(\langle h \rangle)$, by hypothesis, $h = 0 \rightarrow \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0$, where N is the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$. Hence, Eq. (8) of Theorem 1 is satisfied, and $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$. But then $\langle h \rangle \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$, and by Proposition 1, $V(\langle h \rangle) \supseteq V(I(\mathcal{O}(\boldsymbol{x}_\iota))) = \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. By Lemma 2, $V(\langle h \rangle$ is an invariant variety. □

Corollary 2 (Decidability of Algebraic Invariants Equations)**.** *It is decidable whether the expression $h = 0$ is an algebraic invariant equation for the vector field $\boldsymbol{p}$ assuming real algebraic coefficients for h and $\boldsymbol{p}$.*

Proof. By Theorem 2, it is necessary and sufficient to check that Eq. (14) is satisfied where N denotes the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$. Eq. (6) gives a constructive way to check whether a given natural number N is the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$: one starts with $N = 1$, then check for the ideal membership, if $Eq.$ (6) holds, then N is the order, otherwise N is incremented by one. This procedure ends necessarily after finitely many steps since the existence and finiteness of N is ensured by the ascending chain condition. Using the universal closure, Eq. (8) is a formula (with quantifiers) of the first-order theory over the real algebraic numbers, which admits an effective quantifier elimination procedure. □

The *sound* and *complete* related proof rule from Theorem 2 can be written as follows (N denotes the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$):

$$(\text{DRI}) \ \frac{h = 0 \rightarrow \bigwedge_{i=0}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0}{(h = 0) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0)} \ . \tag{15}$$

Using the naive trick in Eq. (2), theoretically, the proof rule can be easily extended to check for the invariance of any finite disjunction of conjunctions of algebraic invariant equations for $\boldsymbol{p}$. This means that we can check for the invariance of any variety for $\boldsymbol{p}$, given its algebraic representation. However, in practice, other techniques, outside the scope of this paper, should be considered to try to keep the degree of the involved polynomials as low as possible. Bounding the order N is also of great importance and will be left as future work.

3.2 Differential Radical Characterization of Invariant Varieties

In the previous section, we were given a variety candidate of the form $V(\langle h \rangle)$ and asked whether we can decide for its invariance. In this section, we characterize all invariant varieties of a vector field $\boldsymbol{p}$ using a differential radical criterion. The following theorem fully characterizes invariant varieties of polynomial vector fields.

Theorem 3 (Characterization of Invariant Varieties)**.** *A variety S is an invariant variety for the vector field $\boldsymbol{p}$ if and only if there exists a polynomial h such that $S = V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\right)$. As a consequence, every invariant variety corresponds to an algebraic invariant equation involving a polynomial and its higher-order Lie derivatives (N denotes the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$):*

$$\bigwedge_{0 \leq i \leq N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0 \ . \tag{16}$$

Proof. Necessary Condition. Let S be an invariant variety for $\boldsymbol{p}$. Let $I(S) = \langle h_1, \ldots, h_r \rangle$ denote the vanishing ideal of S, and the polynomials h_i its generators. Our candidate will be the sum of squares $h = \sum_{i=1}^{r} h_i^2$. We prove that $S = V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\big)$. Over the field of reals, by definition of h, we have $h = 0$ if and only if $\bigwedge_{i=1}^{r} h_i = 0$. Hence, $V(\langle h \rangle) = V(I(S))$ (Def. 5), and $V(I(S)) = S$ (Proposition 1). But S is an invariant variety, then $V(\langle h \rangle)$ is also an invariant variety for $\boldsymbol{p}$. By Theorem 2, $h = 0 \longrightarrow \bigwedge_{i=1}^{N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0$, where N denotes the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$. This means that $V(\langle h \rangle) = V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\big) = S$ and the necessary condition is proved.

Sufficient Condition. If $S = V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\big)$, then for all $\boldsymbol{x}_\iota \in S$, (8) of Theorem 1 is satisfied. Since N is the order of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$ by hypothesis, $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, which means that $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle} \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$ and $S = V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\big) \supseteq V(I(\mathcal{O}(\boldsymbol{x}_\iota))) = \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. So that $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq S$, for all $\boldsymbol{x}_\iota \in S$. By Lemma 2, S is an invariant variety. □

It is interesting to notice that Theorem 3 proves, from the differential radical characterization point of view, the well-known fact discussed right after Lemma 2 about invariant polynomial functions: If $\mathfrak{L}_{\boldsymbol{p}}(h(\boldsymbol{x})) = 0$, then $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h(\boldsymbol{x}) - c \rangle} = \langle h(\boldsymbol{x}) - c \rangle$, and so $S_c = V(\langle h(\boldsymbol{x}) - c \rangle)$ is a family of invariant varieties. Besides, it is clear now why the family $S_\gamma = V(\langle \gamma_1 x_1 + \gamma_2 x_2 \rangle)$ is invariant under the action of the vector field $(p_1, p_2) = (x_1, x_2)$: $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle \gamma_1 x_1 + \gamma_2 x_2 \rangle} = \langle \gamma_1 x_1 + \gamma_2 x_2 \rangle$.

We say that the polynomial h is a *differential radical invariant* (for the vector field $\boldsymbol{p}$) if and only if $V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\big)$ is an invariant variety for $\boldsymbol{p}$. An algebraic invariant equation for $\boldsymbol{p}$ is defined semantically (Def. 10) as a polynomial that evaluates to zero if it is zero initially (admits $\boldsymbol{x}_\iota$ as a root). Differential-radical invariants are, on the other hand, defined as a structured, syntactically computable, conjunction of polynomial equations involving one polynomial and its successive Lie derivatives. Both coincide.

Corollary 3. *Invariant varieties for $\boldsymbol{p}$ are exactly differential radical invariants for $\boldsymbol{p}$.*

Corollary 3 will be crucial to generate differential radical invariants (see Section 4). The condition $\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) \in \sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$ and, more precisely, its explicit formulation:

$$\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h), \tag{17}$$

for some $g_i \in \mathbb{R}[\boldsymbol{x}]$, is computationally attractive as it only involves polynomial arithmetic on higher-order Lie derivatives of one polynomial, h, which in turn can be computed automatically by symbolic differentiation. The next section exploits this fact to automatically generate differential radical invariants and consequently invariant varieties.

4 Effective Generation of Invariant Varieties

In the previous section, we have seen (Theorem 3) that differential radical ideals characterize invariant varieties. Based on Eq. (17), we explain in this section how we automatically construct differential radical ideals given a polynomial vector field $\boldsymbol{p}$ by deriving a set of constraints that the coefficients of a parametrized polynomial (of a certain degree d) have to satisfy.

We first recall some well-known definitions for the sake of clarity. A *monomial* of $\mathbb{R}[\boldsymbol{x}]$ is a term of the form $\alpha\Pi_{i=1}^{n} x_i^{d_i}$, where α is a real number and the d_i are nonnegative integers ($d_i \geq 0$). By convention, $x_i^0 = 1$ for any x_i. If the coefficient α is nonzero, the degree of a monomial is defined by

$$\deg\left(\alpha\Pi_{i=1}^{n} x_i^{d_i}\right) \stackrel{\text{def}}{=} \sum_{i=1}^{n} d_i \ .$$

A polynomial can be written in a canonical form as a finite sum of monomials with nonzero coefficient, or simply monomials. The degree of a polynomial in $\mathbb{R}[\boldsymbol{x}]$ is defined as the maximum degree among the (finite) set of degrees of its monomials. When the degrees of all nonzero monomials of a polynomial h are equal, we say that h is *homogeneous* of degree d, or that h is a *form* of degree d. The degree of the zero polynomial (0) is undefined. We assume in this work that all finite degrees are acceptable for the zero polynomial.

By introducing an extra variable x_0 and multiplying all monomials by a suitable power of x_0, any polynomial of $\mathbb{R}[\boldsymbol{x}]$ can be homogenized to a (homogeneous) polynomial in $\mathbb{R}[x_0][\boldsymbol{x}]$[8]. Any polynomial vector field $\boldsymbol{p}$ can be, therefore, homogenized and all polynomials p_i can be seen as having the same degree d', defined as the maximum degree among all degrees of the original polynomials:

$$d' \stackrel{\text{def}}{=} \max_i(\deg(p_i)) \ . \tag{18}$$

The additional variable x_0 is considered as a time-independent function: its time derivative is zero ($\dot{x}_0 = p_0 = 0$). In the sequel, we should always consider that there is at least one i, $1 \leq i \leq n$, such that $p_i \neq 0$. Otherwise, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) = \{\boldsymbol{x}_\iota\}$ and $I(\mathcal{O}(\boldsymbol{x}_\iota)) = \langle x_0 - \boldsymbol{x}_{\iota 0}, \ldots, x_n - \boldsymbol{x}_{\iota n}\rangle$, and nothing else needs to be done (any point of $\mathbb{R}^n$ is an equilibrium). Under this fair assumption, d' is always defined.

"De-homogenizing" a homogenized polynomial corresponds to instantiating x_0 with 1, which gives back the original polynomial. Therefore, any vector field can be lifted to a homogeneous vector field involving only forms of the ring $\mathbb{R}[x_0, \ldots, x_n]$.

Geometrically, the homogenization of polynomials corresponds to the notion of projective varieties in projective geometry, where the homogenized polynomial is the algebraic representative of the variety related to the original polynomial in the projective plane [4, Chapter 8]. From a computational prospective, working in the projective plane offers a more symmetric representation where all monomials of any given polynomial have the same degree. The arithmetic of degrees is also simplified: the degree of a product is the sum of the degrees of the operands. Hence, we benefit from the graded structure of the polynomial ring.

In the reminder of this section, we only consider forms of $\mathbb{R}[x_0, \ldots, x_n]$. To ease the readability, the symbol $\boldsymbol{x}$ will now denote the vector of all involved variables, that is, $x_0, \ldots, x_n$. Likewise, the symbol $\boldsymbol{x}_\iota$ will be overloaded to denote the initial value of all involved variables (while keeping in mind that $\boldsymbol{x}_{\iota 0} = 1$).

[8]The nested polynomial ring $\mathbb{R}[x_0][\boldsymbol{x}]$ is isomorphic to the multivariate polynomial ring $\mathbb{R}[x_0, x_1, \ldots, x_n]$. The former notation emphasizes the lifting we are doing and emphasizes that the homogenization coordinate x_0 is different from the other variables. The latter notation treats x_0 as a regular variable. We will switch whenever necessary between these two notations to better emphasize the use of x_0.

If h denotes a form of degree d, and d' is as defined in Eq. (18), then the degree of the form $\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h)$ is given by:

$$\deg(\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h)) = d + k(-1+d') \ . \tag{19}$$

This assertion can be proved recursively on the order k using the following two facts. On one hand, the partial derivative of a form with respect to one of its variables either gives the zero polynomial (to which we can assign any arbitrarily finite degree) or decreases the degree by 1. On the other hand, the degree of the product of two forms is equal to the sum of their respective degrees.

Recall that a form of degree d in $\mathbb{R}[\boldsymbol{x}]$ has

$$m_d \stackrel{\text{def}}{=} \binom{n+d}{d} \tag{20}$$

monomials (the binomial coefficient of $n+d$ and d). A parametrized form h of degree d can therefore be represented by its symbolic coefficients' vector $\boldsymbol{\alpha} \in \mathbb{R}^{m_d}$. For this representation to be canonical, we fix an order over monomials of the same degree. We will use the usual lexicographical order, except for x_0: $x_1 > x_2 > \cdots > x_n > x_0$. That is, we first compare the degrees of x_1, if equal, we compare the degrees of x_2 and so on till reaching x_n and then x_0. For instance, for $n = 2$, a parametrized form h of degree $d = 1$ is equal to $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$. Its related coefficients' vector is $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$. The last position of the homogenizing variable x_0 in the above monomial order makes high powers of x_0 ineffective compared to the degrees of other variables, for instance $x_1^2 x_0 > x_1 x_0^{10}$. When de-homogenizing, x_0 is set to 1, and appending a high power of 1 to any monomial will not alter the monomial itself[9]. This property is reflected in the monomials ordering introduced above.

Let h be a form of degree d and let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{m_d})$ denote the coefficients' vector with respect to the monomial order defined above. From Eq. (17), the degree of each term $g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)$ have to match the degree of $\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h)$. Hence, by Eq. (19):

$$\deg(g_i) = \deg(\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h)) - \deg(\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)) = (d+N(-1+d')) - (d+i(-1+d')) = (N-i)(-1+d') \ .$$

The coefficients' vector of each form g_i, $\boldsymbol{\beta}_i$, is then a vector of size $m_{(N-i)(-1+d')}$ (see Eq. (20)).

The polynomial equation Eq. (17) can be rewritten as $m_{d+N(-1+d')}$ biaffine equations, i.e. linear in $\boldsymbol{\alpha}_i$, $1 \leq i \leq m_d$, and affine $\boldsymbol{\beta}_{i,j}$, $0 \leq i \leq N-1$, $1 \leq j \leq m_{(N-i)(-1+d')}$. A concrete example follows.

Example 1. *Suppose we have $n = 2$, $d' = 1$, $p_1 = a_1 x_1 + a_2 x_2$ and $p_2 = b_1 x_1 + b_2 x_2$. For $d = 1$, the parametrized form $h_{\boldsymbol{\alpha}}$ is equal to $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$. Let $N = 1$. The first-order Lie derivative, $\mathfrak{L}_{\boldsymbol{p}}(h_{\boldsymbol{\alpha}})$, has the same degree, 1, and is equal to $\alpha_1(a_1 x_1 + a_2 x_2) + \alpha_2(b_1 x_1 + b_2 x_2)$. In this case, g_0 is a form of degree 0, that is a real number. So it has one coefficient $\beta \in \mathbb{R}$. We, therefore, obtain $m_1 = \binom{3}{1} = 3$ constraints:*

$$\begin{array}{lll} (-a_1+\beta)\alpha_1 + (-b_1)\alpha_2 & = 0 & \\ (-a_2)\alpha_1 + (-b_2+\beta)\alpha_2 & = 0 & \leftrightarrow \begin{pmatrix} -a_1+\beta & -b_1 & 0 \\ -a_2 & -b_2+\beta & 0 \\ 0 & 0 & \beta \end{pmatrix} . \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = 0 \ . \\ (\beta)\alpha_3 & = 0 & \end{array}$$

[9] In fact, the lexicographical order defined here over monomials of $\mathbb{R}[x_0, \ldots, x_n]$ corresponds exactly to the well-known graded lexicographical order [4, Chapter 2] over monomials of $\mathbb{R}[x_1, \ldots .x_n]$ after de-homogenizing.

As suggested in Example 1, if we concatenate all vectors $\boldsymbol{\beta}_i$ into one vector $\boldsymbol{\beta}$, the equational constraints on the coefficients of the involved polynomials in Eq. (17) can be rewritten as a symbolic linear algebra problem of the following form:

$$M_{d,N}(\boldsymbol{\beta})\boldsymbol{\alpha} = 0, \tag{21}$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are decoupled. We call the matrix $M_{d,N}(\boldsymbol{\beta})$ the *matrix representation* of Eq. (17). The matrix has $m_{d+N(-1+d')}$ rows and m_d columns (d' is defined as in Eq. (18)). The size of $\boldsymbol{\beta}$ is computed as the sum of the sizes of all $\boldsymbol{\beta}_i$:

$$|\boldsymbol{\beta}| = \sum_{i=0}^{N-1} m_{(N-i)(-1+d')} \ .$$

Recall that the *kernel* (or null-space) of a matrix $M \in \mathbb{R}^{r\times c}$, with r rows and c columns is the subspace of $\mathbb{R}^c$ defined as the preimage of the vector $0 \in \mathbb{R}^c$:

$$\ker(M) \stackrel{\text{def}}{=} \{x \in \mathbb{R}^c \mid Mx = 0\} \ .$$

Let $s = \dim(\ker(M_{d,N}(\boldsymbol{\beta}))) \leq m_d$. If, for all $\boldsymbol{\beta}$, $s = 0$, then the kernel is $\{0\}$. Hence, $\boldsymbol{\alpha} = 0$ and, for the chosen N, we have $0 = \mathfrak{L}_{\boldsymbol{p}}^{(N)} \in \sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h\rangle} = \langle 0\rangle$: the only differential radical ideal generated by a form of degree d is the trivial ideal $\langle 0\rangle$. If, however, $s > 0$, then, by Theorem 3, we generate an invariant (projective) variety for $\boldsymbol{p}$. In this case, de-homogenizing is not always possible. In fact, the constraint on the initial value could involve x_0, for instance $(x_0 = 0)$ which prevents the de-homogenization (see Example 2 below for a concrete example). Otherwise, we recover an invariant (affine) variety for the original vector field. This is formally stated in the following proposition.

Theorem 4 (Effective Generation of Projective Invariant Varieties)**.** *Let $h_{\boldsymbol{\alpha}}$ denote a parametrized form of degree d. There exists a $\boldsymbol{\beta}$ such that $\dim(\ker(M_{d,N}(\boldsymbol{\beta}))) \geq 1$ if and only if for $\boldsymbol{\alpha} \in \ker(M_{d,N}(\boldsymbol{\beta}))$, $V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}}\rangle}\big) \subset \mathbb{R}^{n+1}$ is a projective invariant variety for the homogenized vector field $\boldsymbol{p}$.*

Proof. The proposition is a projective formulation of Theorem 3. The condition on the dimension of the kernel of $\ker(M_{d,N}(\boldsymbol{\beta}))$ avoids the trivial case where $h_{\boldsymbol{\alpha}}$ is the form zero. □

When $s = \dim(\ker(M_{d,N}(\boldsymbol{\beta}))) \geq 1$, the subspace $\ker(M_{d,N}(\boldsymbol{\beta}))$ is spanned by s vectors, $e_1, \ldots, e_s \in \mathbb{R}^{m_d}$, and for $\boldsymbol{\alpha} = \gamma_1 e_1 + \cdots + \gamma_s e_s$, for arbitrarily $(\gamma_1, \ldots, \gamma_s) \in \mathbb{R}^s$, the variety $V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}}\rangle}\big)$ is a *family* of invariant varieties of $\boldsymbol{p}$.

In the sequel, we give a sufficient condition, so that, for any given initial value, one gets a variety (different from the trivial whole space) that embeds the reachable set of the trajectory, $\mathcal{O}(\boldsymbol{x}_\iota)$. For instance, for conservative Hamiltonian system, if the total energy function, h, is polynomial (such as the energy function of the perfect pendulum), then, for any initial value $\boldsymbol{x}_\iota$, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h(\boldsymbol{x}) - h(\boldsymbol{x}_\iota)\rangle}\big) = V(\langle h(\boldsymbol{x}) - h(\boldsymbol{x}_\iota)\rangle)$.

For a generic $\boldsymbol{x}_\iota \in \mathbb{R}^{n+1}$, if $\boldsymbol{x}_\iota$ satisfies Eq. (8), then, by Theorem 1, $h_{\boldsymbol{\alpha}} \in I(\mathcal{O}(\boldsymbol{x}_\iota))$ and $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq V\big(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}}\rangle}\big)$ (Corollary 1). However, for $\boldsymbol{x}_\iota$ to satisfy Eq. (8), $\boldsymbol{\alpha}$ must be in the intersection of N hyperplanes, $H_0, \ldots, H_{N-1}$, each defined explicitly by the condition $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_{\boldsymbol{\alpha}})(\boldsymbol{x}_\iota) = 0$:

$$H_i \stackrel{\text{def}}{=} \big\{\boldsymbol{\alpha} \in \mathbb{R}^{m_d} \mid \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_{\boldsymbol{\alpha}})(\boldsymbol{x}_\iota) = 0\big\} \ . \tag{22}$$

For instance, going back to Example 1, for $N = 2$, the two normal vectors that define the two hyperplanes, H_0 and H_1, are respectively: $(\boldsymbol{x}_{\iota 1}, \boldsymbol{x}_{\iota 2}, 1)$ (related to $h_{\boldsymbol{\alpha}}(\boldsymbol{x}_\iota) = 0$) and $(a_1\boldsymbol{x}_{\iota 1} + a_2\boldsymbol{x}_{\iota 2}, b_1\boldsymbol{x}_{\iota 1} + b_2\boldsymbol{x}_{\iota 2}, 1)$ (related to $\mathfrak{L}_{\boldsymbol{p}}(h_{\boldsymbol{\alpha}})(\boldsymbol{x}_\iota) = 0$).

The following abstract geometrical fact will be needed.

Lemma 4. *Let $r > 1$. Let L be a linear subspace of $\mathbb{R}^r$, such that $\dim(L) > 0$ (i.e. L non reduced to the origin). Let S be a subspace of $\mathbb{R}^r$ such that $r - \dim(L) < \dim(S) \leq r$ (i.e. the dimension of S is strictly greater than the codimension of L). The intersection of S and L is necessarily nonempty, i.e. there exists a vector $v \neq 0$ of S that is included in L.*

Proof. If $L \cap S = \{0\}$, then $\dim(L + S) = \dim(L) + \dim(S) > r$ which contradicts the fact that $\dim(L + S) \leq r$ since $L + S \subseteq \mathbb{R}^r$. Therefore, $\dim(L \cap S) > 0$ and the lemma follows. □

Using Lemma 4, we derive the required condition on $\boldsymbol{\alpha}$ for $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_\alpha \rangle}\right)$.

Proposition 5 (Effective Sound Approximation of $\mathcal{O}(\boldsymbol{x}_\iota)$)**.** *Let $h_{\boldsymbol{\alpha}}$ be a parametrized form of degree d, and $M_{d,N}(\boldsymbol{\beta})$ the matrix representation of Eq.* (17)*. Let $H_i \subseteq \mathbb{R}^{m_d}$, $0 \leq i \leq N-1$, be the hyperplanes defined in Eq.* (22)*. Then, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}} \rangle}\right)$, if there exists $\boldsymbol{\beta}$ such that:*

$$\dim(\ker(M_{d,N}(\boldsymbol{\beta}))) > m_d - \dim\left(\bigcap_{i=0}^{N-1} H_i\right) \quad . \tag{23}$$

Proof. Apply Lemma 4 for $r = m_d$, $S = \ker(M_{d,N}(\boldsymbol{\beta}))$, $L = \bigcap_{i=0}^{N-1} H_i$. If L is non-reduced to $\{0\}$, then there exists $\boldsymbol{\alpha} \neq 0$ in $S \cap L$. Since $\boldsymbol{\alpha} \in S$, then N is greater than or equal to the order of the differential radical ideal $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}} \rangle}$. Besides, $\boldsymbol{\alpha} \in L$, for any $\boldsymbol{x}_\iota \in \mathbb{R}^{n+1}$, then the hypothesis of Theorem 1 hold and $h_{\boldsymbol{\alpha}} \in I(\mathcal{O}(\boldsymbol{x}_\iota))$. By Corollary 1, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}} \rangle}\right)$. □

The remainder of this section discusses our approach to maximize the dimension of the kernel of $M_{d,N}(h)$, as well as the complexity of the underlying computation.

Gaussian Elimination Let $\boldsymbol{\beta} \stackrel{\text{def}}{=} (\beta_1, \ldots, \beta_s) : \mathbb{R}^s$. Let $d > 0$ and $N > 0$ be fixed nonnegative integers.We want to find an instance, $\boldsymbol{\beta}^*$, of $\boldsymbol{\beta}$ that maximizes $\dim \ker(M_{d,N}(\boldsymbol{\beta}))$, assuming that all the elements of $M_{d,N}(\boldsymbol{\beta})$ are affine in $\boldsymbol{\beta}$. The general scheme of the algorithm is sketched in algorithm 1. At each iteration, the algorithm assigns new values to the remaining coefficients in $\boldsymbol{\beta}$ for the matrix $M_{d,N}(\boldsymbol{\beta})$ to maximize the dimension of its kernel. The set $\mathcal{M}$ gathers all the instantiations of $M_{d,N}(\boldsymbol{\beta})$ that have been considered so far. The procedure ends when no further assignment can be done. Observe that the algorithm (line 1) is a typical `MapReduce` procedure which can be parallelized. In line 1, extracting a basis $(l_{i_1}, \ldots, l_{i_q})$ requires symbolic computation capabilities for linear algebra, which we refer to as *Symbolic Linear Programming*. In practice, the naive approach which computes and solves the determinant (lines 2 and 3) is expensive. Instead, row-reducing speeds up the computation in average: we row-reduce $M_{d,n}(\boldsymbol{\beta})$, and record any divisions by the pivot element: we then branch with any $\boldsymbol{\beta}$ assignment that zero the denominator.

Algorithm 1: Find $\boldsymbol{\beta}^*$, s.t. $\dim(\ker(M_{d,N}(\boldsymbol{\beta}^*)))$ is maximized.

Data: $M_{d,N}(\boldsymbol{\beta})$: $m_{d+N(-1+d')}$ rows, m_d columns, elements linear in elements of $\boldsymbol{\beta}$.
Result: A set of $M(\boldsymbol{\beta}^*)$, s.t. $\dim(\ker(M_{d,N}(\boldsymbol{\beta}^*)))$ is maximized.
$\mathcal{M} \leftarrow \{M_{d,N}(\boldsymbol{\beta})\}$
while *true* **do**
1 **foreach** $K \in \mathcal{M}$ **do**
$(l_1, \ldots, l_r) \leftarrow$ rows of K
Find $(l_{i_1}, \ldots, l_{i_q})$ basis of $(l_1, \ldots, l_r)$ `// Symbolic Linear Programming`
if $q = c$ **then**
2 $det_{\boldsymbol{\beta}} \leftarrow \det(M_{d,N}(l_{i_1}, \ldots, l_{i_q}))$
3 $S \leftarrow$ roots of $det_{\boldsymbol{\beta}} = 0$
$\mathcal{M}' \leftarrow \mathcal{M} \setminus K$ `// Prune`
if $S \neq \emptyset$ **then**
$\mathcal{M}' \leftarrow \bigcup_{s \in S} K(s)$ `// Branch`
if $\mathcal{M}' = \mathcal{M}$ **then**
Return $\mathcal{M}$
else
$\mathcal{M} \leftarrow \mathcal{M}'$

Example 2. *We apply Algorithm 1 to Example 1. The determinant of the matrix* $M_{1,1}(\beta)$ *is* $\beta\big(\beta^2 - (a_1+b_2)\beta - a_2b_1 + a_1b_2\big)$. *Since we do not have any constraints on the parameters* a_1, a_2, b_1, b_2*, the only generic solution for the determinant is* $\beta = 0$*. The algorithm terminates with* $\mathcal{M}$ *containing one matrix,* $M_{1,1}(0)$*:*

$$\begin{pmatrix} -a_1 & -b_1 & 0 \\ -a_2 & -b_2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \ .$$

The kernel of the above matrix is generated by $(0, 0, 1)$*, its dimension is therefore* 1*. Hence,* $\boldsymbol{\alpha} = (0, 0, \gamma)$*, and the* $h_{\boldsymbol{\alpha}} = \gamma x_0$*, for some* $\gamma \in \mathbb{R}$*. If we de-homogenize, we find the trivial algebraic invariant equation* $0 = 0$*. Enforcing* x_0 *to be* 0 *would lead to a projective invariant variety.*

The result of Example 2 is expected as it studies a generic linear vector field without any a priori constraints on the parameters. This triggers, naturally, an interesting feature of the differential radical characterization: its ability to synthesize vector fields to enforce an invariant variety. For instance, in Example 2, let $\delta \stackrel{\text{def}}{=} (a_1 - b_2)^2 + 4a_2b_1$. If $\delta \geq 0$, the set $\mathcal{M}$ contains three matrices (instead of only one earlier), namely $M_{1,1}(\beta)$, for $\beta \in \{0, \frac{1}{2}\big(a_1 + b_2 + \sqrt{\delta}\big), \frac{1}{2}\big(a_1 + b_2 - \sqrt{\delta}\big)\}$. The case $\beta = 0$ was already discussed. When $\beta = \frac{1}{2}\big(a_1 + b_2 \pm \sqrt{\delta}\big) \neq 0$, and $a_2 \neq 0$, the kernel of $M_{1,1}(\beta)$ is generated by the vector $\big(a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0\big)$. By Theorem 4, we have an invariant variety given by:

$$\Big(a_1 - b_2 \pm \sqrt{\delta}\Big)x_1 + 2a_2x_2 = 0 \ .$$

In fact, when $a_2 \neq 0$, the vector $\big(a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0\big)$ is nothing but the eigenvector of the matrix $M_{1,1}(\beta)$ related to the eigenvalue β. This is also expected for linear systems as eigenvectors span stable subspaces.

Complexity We fix $N > 0$ and $d > 0$. Maximizing the dimension of the kernel of the matrix $M_{d,N}(\boldsymbol{\beta})$ over unconstrained $\boldsymbol{\beta}$ is equivalent to the following unconstrained minimal rank problem:

$$\min_{\boldsymbol{\beta}} \operatorname{rank}(M_{d,N}(\boldsymbol{\beta})), \tag{24}$$

where the elements of the vector $\boldsymbol{\beta}$ are in $\mathbb{R}$. If the vector field $\boldsymbol{p}$ has no parameters, then the entries of the matrix $M_{d,N}(\boldsymbol{\beta})$ are either elements of $\boldsymbol{\beta}$ or real numbers. Under these assumptions, the problem in Eq. (24) is in PSPACE [2, Corollary 20] over the field of real numbers[10], and is at least NP-hard (see [2, Corollary 12] and [11, Theorem 8.2]) independently from the underlying field. In fact, deciding whether the rank of $M_{d,N}(\boldsymbol{\beta})$ is less than or equal to a given fixed bound is no harder than deciding the corresponding existential first-order theory.

On the other hand, there is an NP-hard lower bound for the feasibility of the original set of (biaffine) equations in $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}$ given in Eq. (21). In the simpler bilinear case and, assuming, as above, that the vector field has no parameters, finding a nontrivial solution ($\boldsymbol{\alpha} = 0$ is trivial) is also NP-hard [11, Theorems 3.7 and 3.8].

[10]The complexity class depends on the underlying field and is worse for fields with nonzero characteristic.

5 Related Work and Contributions

Tremendous progress has been achieved over the past ten years to automate checking and generating algebraic invariants (both algebraic and semialgebraic sets). The initial focus was on approximations of the reachable sets at a given time of the solution of linear initial value problems. In [12, 34] techniques from the spectral theory were used. The initial value problem is solved (which is always possible for linear vector fields) and the reachable set phrased as a quantifier elimination problem. In [34], the authors used different simplification techniques observing that special patterns of the eigenvalues can be translated in a straightforward manner to invariant equations (for the studied linear vector field) based on results on o-minimal hybrid systems [12]. In [28], this idea is formalized in an algebraic setting using Gröbner Bases, which have been experimentally shown to be more efficient on average than quantifier elimination for small systems with low degrees. In [36], TIWARI and KHANNA started investigating nonlinear polynomial vector field by adapting linear techniques. Gröbner Bases algorithm were used. Syzygies replaced eigenvectors and special cases are discussed: for instance, exact syzygies correspond to invariant polynomial functions. The method is not "complete" in the sense that it only generates a special kind of invariants (namely invariant polynomial functions) and may therefore miss others. The use of Syzygies is generalized in [29]: Assuming an initial given variety, SANKARANARAYANAN characterized the invariant ideal of invariant varieties as an ideal fixpoint of a monotonic operator (introduced in [31] and essentially applied for hybrid systems with linear vector fields therein). Gröbner basis are also heavily used to compute the successive iteration of the operator. The convergence is ensured by iterating over pseudo-ideals [3]. MATRINGE et al. [17] handled a special case of invariant varieties, therein called "constant-scale" and "polynomial-scale" consecutions, where the first-order Lie derivative of a polynomial is in the ideal generated by the polynomial itself. In the literature, such polynomials are known as *Darboux polynomials*. They are intimately related to rational first integrals of the system [8, Chapter 2], which in reality correspond exactly to the invariants studied in [36, 32, 17]. The problem of generating Darboux polynomials is phrased in term of maximization of the null-space of a linear (symbolic) matrix which is more efficient than the two techniques used so far, namely, Gröbner basis and quantifier elimination. The same authors tried in [26] an extension to generate invariant equation involving formal power series. More recently, higher-order Lie derivatives were used by LIU et al. to compute invariant semialgebraic sets [15] and generate Lyapunov functions [16] for (nonlinear) polynomial vector fields. They essentially extended the Barrier certificate [25] formulation (which only involves first-order Lie derivative) to constrain a higher-order Lie derivative to be strictly negative whenever the trajectory touches the boundary of the certificate. Quantifier elimination is heavily used, which seems to be rather expensive and inefficient in practice.

The contribution of this work is fourfold.

Sound and Precise Algebraic Abstraction of Reachable Sets (Section 2) Unlike previous work [36, 29, 17, 15], we start by studying algebraic initial value problems. We propose a sound abstraction (Proposition 2) to embed (overapproximate) the reachable set. Our abstraction relies on the Zariski closure operator over affine varieties (closed sets of the Zariski topology), which allows

a clean and sound geometrical abstraction. From there, we define the vanishing ideal of the closure, and give a necessary and sufficient condition (Theorem 1) for a polynomial equation to be an invariant for algebraic initial value problems.

Checking Invariant Varieties by Differential Radical Invariants (Section 3.1) The differential radical characterization allows to check for and falsify the invariance of a variety candidate. Unlike already existing proof rules [36, 17, 22], which are sound but can only prove a restrictive class of invariants. From Theorem 2, we derive a sound and complete proof rule (Eq. (15)) and prove that the problem is decidable (Corollary 2) over the real-closed algebraic fields.

Differential Radical Characterization of Invariant Varieties (Section 3.2) The differential radical criterion completely characterizes all invariant varieties of polynomial vector fields. This new characterization (Theorem 3) permits to relate invariant varieties to a purely algebraic, well-behaved, conjunction of polynomial equations involving one polynomial and its successive Lie derivatives (Eq. (16)). It naturally generalizes [12, 34] where linear vector fields are handled and [32, 17] where only a restrictive class of invariant varieties is considered.

Effective Generation of Invariant Varieties (Section 4) Unlike [36, 29, 15, 28], we do not use quantifier elimination procedures nor Gröbner Bases algorithms for the generation of invariant varieties. We have developed and generalized the use of symbolic linear algebra tools to effectively generate families of invariant varieties (Theorem 4) and to soundly overapproximate reachable sets (Proposition 5). In both cases, the problem requires maximizing the dimension of the kernel of a symbolic matrix. The complexity is shown to be NP-hard for polynomial vector fields without parameters. We give further a necessary and sufficient condition for a differential radical invariant to generate a family of projective invariant varieties (Proposition 5). We also generalize the previous related work on polynomial-consecution. In particular, Theorems 2 and 4 in [17] are special cases of, respectively, Theorem 4 and Proposition 5, when the order of differential radical ideals is exactly 1.

6 Case Studies

The following challenging example comes up as a subsystem we encountered when studying aircraft dynamics:

$$p_1 = -x_2,\ p_2 = x_1,\ p_3 = x_4^2,\ p_4 = x_3 x_4 \quad . \tag{25}$$

The above vector field $\boldsymbol{p}$ appears frequently whenever Euler angles and the three dimensional rotational matrix is used to describe the dynamics of rigid body motions. For some chosen initial value, such as $\boldsymbol{x}_\iota = (1, 0, 0, 1)$, it is an exact algebraic encoding of the trigonometric functions : $x_1(t) = \cos(t)$, $x_2(t) = \sin(t)$, $x_3(t) = \tan(t)$, $x_4(t) = \sec(t)$. When $d = 2$ and $N = 1$, the matrix $M_{2,1}(\boldsymbol{\beta})$ is 35×15, with 90 (out of 525) nonzero elements, and $|\boldsymbol{\beta}| = 5$. The maximum dimension of $\ker(M_{2,1}(\boldsymbol{\beta}))$ is 3 attained for $\boldsymbol{\beta} = \mathbf{0}$. The condition of Proposition 5 is satisfied and,

for any $\boldsymbol{x}_\iota$, we find the following algebraic invariant equations for the corresponding initial value problem:

$$h_1 = x_1^2 + x_2^2 - \boldsymbol{x}_{\iota 1}^{\,2} - \boldsymbol{x}_{\iota 2}^{\,2} = 0 \tag{26}$$
$$h_2 = -x_3^2 + x_4^2 + \boldsymbol{x}_{\iota 3}^{\,2} - \boldsymbol{x}_{\iota 4}^{\,2} = 0 \tag{27}$$

For the initial value $\boldsymbol{x}_\iota = (1, 0, 0, 1)$, one recovers two trigonometric identities, namely $\cos(t)^2 + \sin(t)^2 - 1 = 0$ for h_1 and $-\tan(t)^2 + \sec(t)^2 - 1 = 0$ for h_2.

For $N = 3$, the matrix $M_{2,3}(\boldsymbol{\beta})$ is 126×15, with 693 (out of 1890) nonzero elements, and $|\boldsymbol{\beta}| = 55$. We found a $\boldsymbol{\beta}$ for which the dimension of $\ker(M_{2,3}(\boldsymbol{\beta}))$ is 5. Therefore, we have a family of invariant varieties for $\boldsymbol{p}$ encoded by the following differential radical invariant:

$$h = \gamma_1 - x_3^2\gamma_2 + x_4^2\gamma_2 + x_2x_4\gamma_3 + x_1^2\gamma_4 + x_2^2\gamma_4 + x_1x_4\gamma_5,$$

where γ_i, $1 \leq i \leq 5$, are real numbers. In particular, when $(\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5) = (1, 0, 0, 0, 1)$, we have the following algebraic invariant equation for $\boldsymbol{p}$:

$$-1 + x_1x_4 = 0 \wedge (-x_2 + x_1x_3)x_4 = 0 \wedge x_4\big(-2x_2x_3 + x_1\big(-1 + x_3^2 + x_4^2\big)\big) = 0,$$

or, equivalently (after simplification):

$$-1 + x_1x_4 = 0 \wedge -x_2x_4 + x_3 = 0 \wedge -1 - x_3^2 + x_4^2 = 0 \ . \tag{28}$$

Interestingly, since $\boldsymbol{x}_\iota = (1, 0, 0, 1)$ satisfies the above equations, we recover, respectively, the following trigonometric identities:

$$-1 + \cos(t)\sec(t) = 0 \wedge -\sin(t)\sec(t) + \tan(t) = 0 \wedge -1 - \tan(t)^2 + \sec(t)^2 = 0 \ .$$

We stress the fact that Eq. (28) is *one* algebraic invariant equation for $\boldsymbol{p}$. In fact, any conjunct alone, a part from $-1 - x_3^2 + x_4^2 = 0$, of Eq. (28) is not an algebraic invariant equation for $\boldsymbol{p}$. Indeed, we can falsify the candidate $-1 + x_1x_4 = 0$ using Theorem 2: the implication $-1 + x_1x_4 = 0 \longrightarrow -x_2x_4 + x_3 = 0$ is obviously false in general.

Notice that h_1 and h_2 can be found separately by splitting the original vector field into two separate vector fields since the pairs (p_1, p_2) and (p_3, p_4) can be decoupled. However, by decoupling, algebraic invariant equation such as Eq. (28) cannot be found. This clearly shows that in practice, splitting the vector field into independent ones should be done carefully when it comes to generating invariant varieties. This is somehow counter-intuitive as decoupling for the purpose of solving is always desirable. In fact, the decoupling breaks an essential link between all involved variables: time.

We proceed to discuss collision avoidance of two airplanes and then the use of invariant varieties to tightly capture the vertical motion of an airplane.

6.1 Collision Avoidance

We revisit the linear vector field encoding Dubin's vehicle model for aircrafts [5]. Although the system was discussed in many recent papers [29, 30, 15], we want to highlight an additional algebraic invariant equation that *links* both airplanes when turning with the same angular velocity. The differential equation system is given by:

$$\begin{array}{llll} p_1 = \dot{x}_1 = d_1, & p_2 = \dot{x}_2 = d_2, & p_3 = \dot{d}_1 = -\omega_1 d_2, & p_4 = \dot{d}_2 = \omega_1 d_1, \\ p_5 = \dot{y}_1 = e_1, & p_6 = \dot{y}_2 = e_2, & p_7 = \dot{e}_1 = -\omega_2 e_2, & p_8 = \dot{e}_2 = \omega_2 e_1 \ . \end{array}$$

The angular velocities ω_1 and ω_2 can be either zero (straight line flight) or equal to a constant ω which denotes the standard rate turn (typically $180^\circ/2mn$ for usual commercial airplanes). When the two airplanes are manoeuvring with the same standard rate turn ω, apart from the already known invariants, we discovered the following differential radical invariant (which corresponds to a family of invariant varieties):

$$h_1 = \gamma_1 d_1 + \gamma_2 d_2 + \gamma_3 e_1 + \gamma_4 e_2 = 0 \wedge h_2 = \gamma_2 d_1 - \gamma_1 d_2 + \gamma_4 e_1 - \gamma_3 e_2 = 0,$$

for some arbitrarily vector $(\gamma_1, \ldots, \gamma_4) \in \mathbb{R}^4$. We have $\sqrt[\mathfrak{o}_{\boldsymbol{p}}]{\langle h_1 \rangle} = \sqrt[\mathfrak{o}_{\boldsymbol{p}}]{\langle h_2 \rangle} = \langle h_1, h_2 \rangle$. Observe also that $V(\langle h_1 \rangle)$ and $V(\langle h_2 \rangle)$ are not invariant varieties of the vector field $\boldsymbol{p}$.

6.2 Longitudinal Motion of an Airplane

The full dynamics of an aircraft are often separated (decoupled) into different modes where the differential equations take a simpler form by either fixing or neglecting the rate of change of some configuration variables [33]. The first standard separation used in stability analysis gives two main modes: longitudinal and lateral-directional. We study the 6th order longitudinal equations of motion as it captures the vertical motion (climbing, descending) of an airplane. We believe that a better understanding of the envelope that soundly contains the trajectories of the aircraft will help tightening the surrounding safety envelope and hence help trajectory management systems to safely allow more dense traffic around airports. The current safety envelope is essentially a rough cylinder that doesn't account for the real capabilities allowed by the dynamics of the airplane. We use our automated invariant generation techniques to characterize such an envelope. The theoretical improvement and the effective underlying computation techniques described earlier in this work allow us to push further the limits of automated invariant generation. We first describe the differential equations (vector field) then show the nontrivial energy functions (invariant functions for the considered vector field) we were able to generate. Let g denote the gravity acceleration, m the total mass of an airplane, M the aerodynamic and thrust moment w.r.t. the y axis, (X, Z) the aerodynamics and thrust forces w.r.t. axis x and z, and I_{yy} the second diagonal element of its inertia matrix. The restriction of the nominal flight path of an aircraft to the vertical plane reduces the full dynamics to the following 6 differential equations [33, Chapter 5] (u:axial velocity, w:vertical

velocity, x:range, z:altitude, q:pitch rate, θ:pitch angle):

$$\begin{aligned}
\dot{u} &= \frac{X}{m} - g\sin(\theta) - qw & \dot{z} &= -\sin(\theta)u + \cos(\theta)w \\
\dot{w} &= \frac{Z}{m} + g\cos(\theta) + qu & \dot{q} &= \frac{M}{I_{yy}} \\
\dot{x} &= \cos(\theta)u + \sin(\theta)w & \dot{\theta} &= q
\end{aligned}$$

We encode the trigonometric functions using two additional variables for $\cos(\theta)$ and $\sin(\theta)$, making the total number of variables equal to 8. The parameters are considered unconstrained (they appear as additional symbols in the matrix $M_{d,N}(\boldsymbol{\beta})$). Unlike [29], we do not consider them as new time independent variables. So that the total number of state variables (n) and hence the degree of the vector field are unchanged. Instead, they are carried along the symbolic row-reduction computation as symbols in $M_{d,N}(\boldsymbol{\beta})$. For the algebraic encoding of the above vector field ($n = 8$), the matrix $M_{3,1}(\boldsymbol{\beta})$ is 495×165, with 2115 (out of 81675) nonzero elements, and $|\boldsymbol{\beta}| = 9$. We were able to automatically generate the following invariant functions (families of invariant varieties):

$$\begin{aligned}
&\frac{Mz}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw\right)\cos(\theta) + \left(\frac{Z}{m} + qu\right)\sin(\theta) \\
&\frac{Mx}{I_{yy}} - \left(\frac{Z}{m} + qu\right)\cos(\theta) + \left(\frac{X}{m} - qw\right)\sin(\theta) \\
&-q^2 + \frac{2M\theta}{I_{yy}}
\end{aligned}$$

We substituted the intermediate variables that encode $\sin$ and $\cos$ back to emphasize the fact that algebraic invariants and algebraic differential systems are suitable to encode many real complex dynamical systems. Using our Mathematica implementation, the computation took 1 hour on a recent laptop with 4GB and 1.7GHz Intel Core i5.

Acknowledgments

We thank the anonymous reviewers for their careful reading and detailed comments. We also would like to very much thank JEAN-BAPTISTE JEANNIN and ANDREW SOGOKON for the multiple questions, various comments and fruitful objections they both had on an early version of this work. We are finally grateful to ERIC GOUBAULT and SYLVIE PUTOT for the relevant references they pointed out to us on the integrability theory of nonlinear systems.

7 Conclusion

For algebraic vector fields, we give an algebraic characterization of invariant varieties. This so-called differential radical characterization makes it possible to decide for the invariance of a given

variety candidate. It is, in addition, computationally attractive: generating invariant varieties requires minimizing the rank of a symbolic matrix and is hence at least NP-hard. The case studies show how the technique applies successfully to rather complex systems. We also revisited some known problems in the literature to exemplify the benefits of having a necessary and sufficient condition: all other known sound approaches generate a special class of invariant varieties (i.e. miss others).

In the future, we plan to investigate upper bounds for the order of the differential radical ideal of a given polynomial. Also, invariant varieties are not the only invariant of interest for polynomial vector fields, we want to consider semialgebraic sets as they play a prominent role in both hybrid systems and control theory. Finally, the effective use of algebraic invariants in general in the context of hybrid systems is still a challenging problem that we want to explore in more depth.

References

[1] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real Algebraic Geometry*. A series of modern surveys in mathematics. Springer, 2010.

[2] Jonathan F. Buss, Gudmund Skovbjerg Frandsen, and Jeffrey Shallit. The computational complexity of some problems of linear algebra. *J. Comput. Syst. Sci.*, 58(3):572–596, 1999.

[3] Michael Colón. Approximating the algebraic relational semantics of imperative programs. In Giacobazzi [7], pages 296–311.

[4] David A. Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2007.

[5] Lester Eli Dubins. On curves of minimal length with a constraint on average curvature, and with prescribed initial and terminal positions and tangents. *American Journal of Mathematics*, 79(3):497–516, 1957.

[6] Khalil Ghorbal and André Platzer. Characterizing algebraic invariants by differential radical invariants. In Erika Ábrahám and Klaus Havelund, editors, *TACAS*. Springer, 2014.

[7] Roberto Giacobazzi, editor. *Static Analysis, 11th International Symposium, SAS 2004, Verona, Italy, August 26-28, 2004, Proceedings*, volume 3148 of *Lecture Notes in Computer Science*. Springer, 2004.

[8] Alain Goriely. *Integrability and Nonintegrability of Dynamical Systems*. Advanced series in nonlinear dynamics. World Scientific, 2001.

[9] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977.

[10] David Hilbert. Über die Theorie der algebraischen Formen. *Mathematische Annalen*, 36(4):473–534, 1890.

[11] Christopher J. Hillar and Lek-Heng Lim. Most tensor problems are NP-hard. *J. ACM*, 60(6):45, 2013.

[12] Gerardo Lafferriere, George J. Pappas, and Sergio Yovine. Symbolic reachability computation for families of linear vector fields. *J. Symb. Comput.*, 32(3):231–253, 2001.

[13] Ruggero Lanotte and Simone Tini. Taylor approximation for hybrid systems. In Morari and Thiele [18], pages 402–416.

[14] Ernest Lindelöf. Sur l'application de la méthode des approximations successives aux équations différentielles ordinaires du premier ordre. *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 116:454–458, 1894.

[15] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Computing semi-algebraic invariants for polynomial dynamical systems. In Samarjit Chakraborty, Ahmed Jerraya, Sanjoy K. Baruah, and Sebastian Fischmeister, editors, *EMSOFT*, pages 97–106. ACM, 2011.

[16] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Automatically discovering relaxed Lyapunov functions for polynomial dynamical systems. *Mathematics in Computer Science*, 6(4):395–408, 2012.

[17] Nadir Matringe, Arnaldo Vieira Moura, and Rachid Rebiha. Generating invariants for non-linear hybrid systems by linear algebraic methods. In Radhia Cousot and Matthieu Martel, editors, *SAS*, volume 6337 of *Lecture Notes in Computer Science*, pages 373–389. Springer, 2010.

[18] Manfred Morari and Lothar Thiele, editors. *Hybrid Systems: Computation and Control, 8th International Workshop, HSCC 2005, Zurich, Switzerland, March 9-11, 2005, Proceedings*, volume 3414 of *Lecture Notes in Computer Science*. Springer, 2005.

[19] Rolf Neuhaus. Computation of real radicals of polynomial ideals II. *Journal of Pure and Applied Algebra*, 124(13):261 – 280, 1998.

[20] André Platzer. Differential dynamic logic for hybrid systems. *J. Autom. Reasoning*, 41(2):143–189, 2008.

[21] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010.

[22] André Platzer. A differential operator approach to equational differential invariants - (invited paper). In Lennart Beringer and Amy P. Felty, editors, *ITP*, volume 7406 of *Lecture Notes in Computer Science*, pages 28–48. Springer, 2012.

[23] André Platzer. Logics of dynamical systems. In *LICS*, pages 13–24. IEEE, 2012.

[24] André Platzer. The structure of differential invariants and differential cut elimination. *Logical Methods in Computer Science*, 8(4):1–38, 2012.

[25] Stephen Prajna. Barrier certificates for nonlinear model validation. *Automatica*, 42(1):117–126, 2006.

[26] Rachid Rebiha, Nadir Matringe, and Arnaldo Vieira Moura. Transcendental inductive invariants generation for non-linear differential and hybrid systems. In Thao Dang and Ian M. Mitchell, editors, *HSCC*, pages 25–34. ACM, 2012.

[27] Enric Rodríguez-Carbonell and Deepak Kapur. An abstract interpretation approach for automatic generation of polynomial invariants. In Giacobazzi [7], pages 280–295.

[28] Enric Rodríguez-Carbonell and Ashish Tiwari. Generating polynomial invariants for hybrid systems. In Morari and Thiele [18], pages 590–605.

[29] Sriram Sankaranarayanan. Automatic invariant generation for hybrid systems using ideal fixed points. In Karl Henrik Johansson and Wang Yi, editors, *HSCC*, pages 221–230. ACM, 2010.

[30] Sriram Sankaranarayanan. Automatic abstraction of non-linear systems using change of bases transformations. In Marco Caccamo, Emilio Frazzoli, and Radu Grosu, editors, *HSCC*, pages 143–152. ACM, 2011.

[31] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. Fixed point iteration for computing the time elapse operator. In João P. Hespanha and Ashish Tiwari, editors, *HSCC*, volume 3927 of *Lecture Notes in Computer Science*, pages 537–551. Springer, 2006.

[32] Sriram Sankaranarayanan, Henny B. Sipma, and Zohar Manna. Constructing invariants for hybrid systems. *Formal Methods in System Design*, 32(1):25–55, 2008.

[33] Robert F. Stengel. *Flight Dynamics*. Princeton University Press, 2004.

[34] Ashish Tiwari. Approximate reachability for linear systems. In Oded Maler and Amir Pnueli, editors, *HSCC*, volume 2623 of *Lecture Notes in Computer Science*, pages 514–525. Springer, 2003.

[35] Ashish Tiwari. Abstractions for hybrid systems. *Formal Methods in System Design*, 32(1):57–83, 2008.

[36] Ashish Tiwari and Gaurav Khanna. Nonlinear systems: Approximating reach sets. In Rajeev Alur and George J. Pappas, editors, *HSCC*, volume 2993 of *Lecture Notes in Computer Science*, pages 600–614. Springer, 2004.

[37] Wolfgang Walter. *Ordinary Differential Equations*. Graduate Texts in Mathematics. Springer, 1998.