Characterizing Algebraic Invariants by Differential Radical Invariants[*]

Khalil Ghorbal and André Platzer

Carnegie Mellon University, Pittsburgh, PA, 15213, USA
{kghorbal,aplatzer}@cs.cmu.edu

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.

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

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 [15], abstraction [21,27], or approximation [10]. 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 [18]. We focus on this core problem in this paper. We study the case of *algebraic*

[*] 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 Agency under contract no. DARPA FA8750-12-2-0291.

E. Ábrahám and K. Havelund (Eds.): TACAS 2014, LNCS 8413, pp. 279–294, 2014.

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 [19,17], 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. The proofs of all presented results are available in [5].

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. 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 $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, 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.

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

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), 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 $\{\dot{x} = x^2, x(t_\iota) = x_\iota \neq 0\}$ 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* (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 $\mathbb{R}^n$.

Definition 3 (Orbit). *The reachable set, or orbit, of the solution of Eq.* (1)*, $\boldsymbol{x}(t)$ is defined as $\mathcal{O}(\boldsymbol{x}_\iota) \overset{def}{=} \{\boldsymbol{x}(t) \mid t \in U_t\} \subseteq \mathbb{R}^n$.*

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 [10] for the verification of hybrid systems). In this work, we introduce a sound abstraction of the orbit, $\mathcal{O}(\boldsymbol{x}_\iota)$, using (affine) varieties[2]. 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

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

geometry called the *Zariski closure* ([6, 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):

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

By Def. 4, the set $\langle h_1, \ldots, h_r \rangle$ is an ideal. More interestingly, by Hilbert's Basis Theorem [7], any ideal I of the Noetherian ring $\mathbb{R}[\boldsymbol{x}]$ can be *finitely generated* by, say $\{h_1, \ldots, h_r\}$, so that $I = \langle h_1, \ldots, h_r \rangle$.

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,

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

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 $\boldsymbol{x} \in S$:

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

The Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ of the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ is defined as the variety of the vanishing ideal of $\mathcal{O}(\boldsymbol{x}_\iota)$:

$$\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \overset{\text{def}}{=} V(I(\mathcal{O}(\boldsymbol{x}_\iota))) . \tag{3}$$

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

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 1 corresponds to the reflexivity property of the Zariski closure: for any subset S of $\mathbb{R}^n$, $S \subseteq V(I(S))$. Besides, 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 $\mathcal{O}(\boldsymbol{x}_\iota)$.

[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 $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$.

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 fails to be informative. 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. 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 $\mathbb{R}$ are in fact exactly the real radical ideals [1, Section 4.1]. In real algebraic geometry, real radical ideals are notoriously hard[4] to compute. 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 is defined as follows.

Definition 5 (Lie Derivative). *The Lie derivative of $h \in \mathbb{R}[\boldsymbol{x}]$ along the vector field $\boldsymbol{p} = (p_1, \ldots, p_n)$ is defined by:*

$$\mathfrak{L}_{\boldsymbol{p}}(h) \overset{\text{def}}{=} \sum_{i=1}^{n} \frac{\partial h}{\partial x_i} p_i \ . \tag{4}$$

Higher-order Lie derivatives are defined recursively: $\mathfrak{L}_{\boldsymbol{p}}^{(k+1)}(h) \overset{\text{def}}{=} \mathfrak{L}_{\boldsymbol{p}}(\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h))$, with $\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h) \overset{\text{def}}{=} h$.

We state an important property of the ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Similar result is known under different formulations ([23, Theorem 3.1] and [16, Lemma 3.7]).

Proposition 2. *$I(\mathcal{O}(\boldsymbol{x}_\iota))$ 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 $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, $\mathfrak{L}_{\boldsymbol{p}}(h) \in I(\mathcal{O}(\boldsymbol{x}_\iota))$.*

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 this section, we study the algebraic properties of the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ defined in the previous section. We then define and characterize invariant algebraic sets of polynomial vector fields.

[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 $2^{O(n^2)}$ [14, Theorem 5.9].

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

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

Since the ring $\mathbb{R}[\boldsymbol{x}]$ is Noetherian, the chain above has necessarily a finite length: the maximal ideal (in the sense of inclusion), so-called the *differential radical ideal*[5] of h, will be denoted by $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$. Its *order* is the smallest N such that:

$$\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) \in \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h), \dots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h) \rangle \ . \tag{5}$$

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*

$$\bigwedge_{0 \le i \le N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)(\boldsymbol{x}_\iota) = 0 \ . \tag{6}$$

The statement of Theorem 1 is general and assumes nothing about $\boldsymbol{x}_\iota \in \mathbb{R}^n$. A natural question to ask is how differential radical characterization can 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. In particular, we focus on invariant algebraic sets where S is variety.

Definition 6 (Invariant Variety). *The variety S is an invariant variety for the vector field* $\mathbf{p}$ *if and only if $\forall \boldsymbol{x}_\iota \in S, \mathcal{O}(\boldsymbol{x}_\iota) \subseteq S$.*

Dual to the geometrical point of view in Def. 6, 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 7 (Algebraic Invariant Equation (Vector Field)). *The expression $h = 0$ is an algebraic invariant equation for the vector field $\mathbf{p}$ if and only if $V(\langle h \rangle)$ is an invariant variety for $\mathbf{p}$.*

Unlike Def. 2, Def. 7, or its geometrical counterpart, Def. 6, corresponds to the typical object of studies in hybrid system verification 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).

We will say that the polynomial h is a *differential radical invariant* (for $\boldsymbol{p}$) if and only if $V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}\right)$ is an invariant variety for $\boldsymbol{p}$.

[5] The construction of $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$ is very similar to the construction of the radical of an ideal except with higher-order Lie derivatives in place of higher powers of polynomials.

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 $\boldsymbol{p}$. Theorem 2 solves the problem.

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 $\mathbf{p}$ (or equivalently $h = 0$ is an algebraic invariant equation for $\mathbf{p}$) if and only if*

$$h = 0 \rightarrow \bigwedge_{1 \leq i \leq N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0 \ . \tag{7}$$

Corollary 1 (Decidability). *It is decidable whether the expression $h = 0$ is an algebraic invariant equation for the vector field $\mathbf{p}$ assuming real algebraic coefficients for h and $\boldsymbol{p}$.*

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

$$(\mathrm{DRI})\, \frac{h = 0 \rightarrow \bigwedge_{1 \leq i \leq N-1} \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) = 0}{(h = 0) \rightarrow [\dot{\boldsymbol{x}} = \boldsymbol{p}](h = 0)} \ . \tag{8}$$

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.

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 $\mathbf{p}$ 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 $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h \rangle}$):*

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

Observe how Theorem 3 proves, from the differential radical characterization point of view, the well-known fact about invariant polynomial functions [17, Theorem 3]: if $\mathfrak{L}_{\boldsymbol{p}}(h(\boldsymbol{x})) = 0$, then, for any $c \in \mathbb{R}$, $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h(\boldsymbol{x}) - c\rangle} = \langle h(\boldsymbol{x}) - c\rangle$, and so $s = v(\langle h(\boldsymbol{x}) - c\rangle)$ is an invariant variety for $\boldsymbol{p}$.

An algebraic invariant equation for $\boldsymbol{p}$ is defined semantically (Def. 7) 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. By Theorem 3, both coincide.

The explicit formulation of Eq. (5), namely

$$\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h), \tag{10}$$

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. Section 4 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. (10), 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 have to satisfy.

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[6]. When the degrees of all nonzero monomials of a polynomial h are equal, we say that h is *homogeneous*, or a *form*, of degree d.

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 form in $\mathbb{R}[x_0][\boldsymbol{x}]$. The additional variable x_0 is considered as a time-independent function: its time derivative is zero ($\dot{x}_0 = p_0 = 0$). "De-homogenizing" the vector field corresponds to instantiating x_0 with 1, which gives back the original vector field. 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 original variety in the projective plane [3, Chapter 8].

From a computational prospective, working in the projective plane offers a more symmetric representation: all monomials of a form have the same degree. The arithmetic of degrees over forms is also simplified: the degree of a product is the sum of the degrees of the operands. In the reminder of this section, we only consider forms of $\mathbb{R}[x_0, \ldots, x_n]$. The symbol $\boldsymbol{x}$ will denote the vector of all involved variables.

[6] The degree of the zero polynomial (0) is undefined. We assume in this work that all finite degrees are acceptable for the zero polynomial.

If h denotes a form of degree d, and d' the maximum degree among the degrees of p_i, then the degree of the polynomial $\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h)$ is given by:

$$\deg(\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h)) = d + k(-1 + d') \ . \tag{11}$$

Recall that a form of degree d in $\mathbb{R}[x_0, \ldots, x_n]$ has

$$m_d \overset{\text{def}}{=} \tbinom{n+d}{d} \tag{12}$$

monomials (the binomial coefficient of $n+d$ and d). A parametrized form $h_{\boldsymbol{\alpha}}$ of degree d can therefore be represented by its symbolic coefficients' vector $\boldsymbol{\alpha} : \mathbb{R}^{m_d}$. For this representation to be canonical, one needs to fix an order over monomials of the same degree. We will use the usual lexicographical order, except for x_0: $x_1 > x_2 > \cdots > x_n > x_0$. 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 $h_{\boldsymbol{\alpha}}$ of degree $d = 1$ is equal to $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$. Its related coefficients' vector is $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$.

Let $h_{\boldsymbol{\alpha}}$ be a parametrized 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. Since all polynomials in Eq. (10) are forms in projective coordinates, the degree of each term $g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_{\boldsymbol{\alpha}})$ matches exactly the degree of $\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h_{\boldsymbol{\alpha}})$. Hence, by Eq. (11): $\deg(g_i) = (N - i)(-1 + d')$. The coefficients' vector of each form g_i is then a vector, $\boldsymbol{\beta}_i$, of size $m_{(N-i)(-1+d')}$ (see Eq. (12)). So that we obtain $m_{d+N(-1+d')}$ biaffine equations: linear in $\boldsymbol{\alpha}_i$, $1 \le i \le m_d$, and affine $\boldsymbol{\beta}_{i,j}$, $0 \le i \le N-1$, $1 \le j \le m_{(N-i)(-1+d')}$. A concrete example is as 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 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:

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

As suggested in Example 1, for a given d and N, and if we concatenate all vectors $\boldsymbol{\beta}_i$ into one vector $\boldsymbol{\beta}$, the equational constraints can be rewritten as a symbolic linear algebra problem of the following form:

$$M_{d,N}(\boldsymbol{\beta})\boldsymbol{\alpha} = 0, \tag{13}$$

where $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are decoupled. The matrix $M_{d,N}(\boldsymbol{\beta})$ is called the *matrix representation* of the ideal membership problem $\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h_{\boldsymbol{\alpha}}) \in ?\langle h_{\boldsymbol{\alpha}}, \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_\alpha)\rangle$.

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 $0 \in \mathbb{R}^c$:

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

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 $h_{\boldsymbol{\alpha}} = 0$: the only differential radical ideal generated by a form of degree d is the trivial ideal $\langle 0 \rangle$. If, however, $s \geq 1$, 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, which prevents the de-homogenization (see Example 2). Otherwise, we recover an invariant (affine) variety for the original vector field. This is formally stated in the following theorem.

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

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 $V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}} \rangle}\right)$ is a *family* of invariant varieties of $\boldsymbol{p}$ (parametrized with $\boldsymbol{\gamma}$).

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 $\boldsymbol{x}_\iota$, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h(\boldsymbol{x}) - h(\boldsymbol{x}_\iota) \rangle}\right) = V(\langle h(\boldsymbol{x}) - h(\boldsymbol{x}_\iota) \rangle)$.

For a generic $\boldsymbol{x}_\iota \in \mathbb{R}^n$, if $\boldsymbol{x}_\iota$ satisfies Eq. (6), then, by Theorem 1, $h_{\boldsymbol{\alpha}} \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, and $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq V\left(\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_{\boldsymbol{\alpha}} \rangle}\right)$ ([5, Corollary 1]). However, for $\boldsymbol{x}_\iota$ to satisfy Eq. (6), $\boldsymbol{\alpha}$ must be in the intersection of N hyperplanes, $H_0, \ldots, H_{N-1}$, each defined explicitly by the condition $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_{\boldsymbol{\alpha}})(\boldsymbol{x}_\iota) = 0$:

$$H_i \overset{\text{def}}{=} \left\{\boldsymbol{\alpha} \in \mathbb{R}^{m_d} \mid \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_{\boldsymbol{\alpha}})(\boldsymbol{x}_\iota) = 0\right\} . \tag{14}$$

Proposition 3 (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.* (10). *Let $H_i \subseteq \mathbb{R}^{m_d}$, $0 \leq i \leq N-1$, be the hyperplanes defined in Eq.* (14). *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:*

$$\dim(\ker(M_{d,N}(\boldsymbol{\beta}))) > m_d - \dim\left(\bigcap_{i=0}^{N-1} H_i\right) . \tag{15}$$

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 $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_s) : \mathbb{R}^s$. By Theorem 4, we want to find an instance, $\boldsymbol{\beta}^*$, of $\boldsymbol{\beta}$ that maximizes $\dim \ker(M_{d,N}(\boldsymbol{\beta}))$, where all the elements of $M_{d,N}(\boldsymbol{\beta})$ are affine in $\boldsymbol{\beta}$. At each iteration, our algorithm [5, Algorithm 1] 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. A set, $\mathcal{M}$, gathers all the instantiations of $M_{d,N}(\boldsymbol{\beta})$. The procedure ends when no further assignment can be done. The algorithm is in fact a typical MapReduce procedure which can be parallelized. A naive approach would be to first extract a basis for the matrix $M_{d,N}(\boldsymbol{\beta})$ (which requires symbolic computation capabilities for linear algebra), then, solves for $\boldsymbol{\beta}$s that zero the determinant. In practice, however, row-reducing speeds up the computation: we row-reduce $M_{d,n}(\boldsymbol{\beta})$, and record any divisions by the pivot element: we then branch with any $\boldsymbol{\beta}$ that zero the denominator.

Example 2. We apply the algorithm sketched above 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 kernel of $M_{1,1}(0)$, of dimension 1, is generated by $(0, 0, 1)$. The only candidates in this case are $h_{\boldsymbol{\alpha}}(\boldsymbol{x}) = \gamma x_0$, $\gamma \in \mathbb{R}$. If we de-homogenize (set x_0 to 1), then, $\gamma = 0$ and we find the trivial invariant variety, $\mathbb{R}^n$.

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 $\delta \overset{\text{def}}{=} (a_1 - b_2)^2 + 4a_2b_1$. If $\delta \geq 0$, and $a_2 \neq 0$, then the kernel of $M_{1,1}(\beta)$ is generated by the vector $\big(a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0\big)$ (which is an eigenvector of the matrix $M_{1,1}(\beta)$). By Theorem 4, we have an invariant variety given by: $\big(a_1 - b_2 \pm \sqrt{\delta}\big)x_1 + 2a_2x_2 = 0$. This is also expected for linear systems as eigenvectors span stable subspaces.

Complexity. By Theorem 4, the generation of invariant varieties is equivalent to maximizing the dimension of the kernel of the matrix $M_{d,N}(\boldsymbol{\beta})$ over unconstrained $\boldsymbol{\beta}$, which is in turn equivalent to the following unconstrained minimal rank problem:

$$\min_{\boldsymbol{\beta}} \operatorname{rank}(M_{d,N}(\boldsymbol{\beta})), \tag{16}$$

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 (16) is in PSPACE [2, Corollary 20] over the field of real numbers[7], and is at least NP-hard (see [2, Corollary 12] and [8, 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. (13). 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 [8, Theorems 3.7 and 3.8].

5 Related Work and Contributions

The contribution of this work is fourfold.

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

Sound and Precise Algebraic Abstraction of Reachable Sets (Section 2). Unlike previous work [28,23,12,11], we start by studying algebraic initial value problems. We propose a sound abstraction (Proposition 1) 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 [28,12,17], which are sound but can only prove a restrictive class of invariants. From Theorem 2, we derive a sound and complete proof rule (Eq. (8)) and prove that the problem is decidable (Corollary 1) 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. (9)). It naturally generalizes [9,26] where linear vector fields are handled and [24,12] where only a restrictive class of invariant varieties is considered.

Effective Generation of Invariant Varieties (Section 4). Unlike [28,23,11,22], 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 3). In both cases, the problem requires maximizing the dimension of the kernel of a symbolic matrix. The complexity is shown to be NP-hard, but in PSPACE, for polynomial vector fields without parameters. We also generalize the previous related work on polynomial-consecution. In particular, Theorems 2 and 4 in [12] are special cases of, respectively, Theorem 4 and Proposition 3, 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: $p_1 = -x_2$, $p_2 = x_1$, $p_3 = x_4^2$, $p_4 = x_3 x_4$.

It 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 3 is satisfied and, for any $\boldsymbol{x}_\iota$, we find the following algebraic invariant equations for the corresponding initial value problem:

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

In particular, 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. By Theorem 4, 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 $\boldsymbol{p}$:

$$-1 + x_1x_4 = 0 \wedge -x_2x_4 + x_3 = 0 \wedge -1 - x_3^2 + x_4^2 = 0 \ . \tag{17}$$

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. (17) 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. (17) 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. (17) 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, any decoupling breaks an essential link between all involved variables: time.

We proceed to discuss collision avoidance of two airplanes (Section 6.1) and then the use of invariant varieties to tightly capture the vertical motion of an airplane (Section 6.2).

6.1 Collision Avoidance

We revisit the linear vector field encoding Dubin's vehicle model for aircrafts [4]. Although the system was discussed in many recent papers [20,23,11], 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 an arbitrarily $(\gamma_1, \ldots, \gamma_4) \in \mathbb{R}^4$. We have $\sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_1 \rangle} = \sqrt[\mathfrak{L}_{\boldsymbol{p}}]{\langle h_2 \rangle} = \langle h_1, h_2 \rangle$. Observe also that $V(\langle h_1 \rangle)$ and $V(\langle h_2 \rangle)$ are not invariant varieties for $\boldsymbol{p}$.

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 [25]. 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 [25, Chapter 5] (u: axial velocity, w: vertical velocity, x: range, z: altitude, q: pitch rate, θ: pitch angle):

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

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. Unlike [23], 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 three invariant functions:

$$\frac{Mz}{I_{yy}} + g\theta + \left(\frac{X}{m} - qw\right)\cos(\theta) + \left(\frac{Z}{m} + qu\right)\sin(\theta),$$
$$\frac{Mx}{I_{yy}} - \left(\frac{Z}{m} + qu\right)\cos(\theta) + \left(\frac{X}{m} - qw\right)\sin(\theta), \quad -q^2 + \frac{2M\theta}{I_{yy}} \; .$$

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 polynomial 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. Bochnak, J., Coste, M., Roy, M.F.: Real Algebraic Geometry. A series of modern surveys in mathematics. Springer (2010)
2. Buss, J.F., Frandsen, G.S., Shallit, J.: The computational complexity of some problems of linear algebra. J. Comput. Syst. Sci. 58(3), 572–596 (1999)
3. Cox, D.A., Little, J., O'Shea, D.: Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer (2007)
4. Dubins, L.E.: 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)

5. Ghorbal, K., Platzer, A.: Characterizing algebraic invariants by differential radical invariants. Tech. Rep. CMU-CS-13-129, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 15213 (November 2013), `http://reports-archive.adm.cs.cmu.edu/anon/2013/abstracts/13-129.html`
6. Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics. Springer (1977)
7. Hilbert, D.: Über die Theorie der algebraischen Formen. Mathematische Annalen 36(4), 473–534 (1890)
8. Hillar, C.J., Lim, L.H.: Most tensor problems are NP-hard. J. ACM 60(6), 45 (2013)
9. Lafferriere, G., Pappas, G.J., Yovine, S.: Symbolic reachability computation for families of linear vector fields. J. Symb. Comput. 32(3), 231–253 (2001)
10. Lanotte, R., Tini, S.: Taylor approximation for hybrid systems. In: Morari, Thiele (eds.) [13], pp. 402–416
11. Liu, J., Zhan, N., Zhao, H.: Computing semi-algebraic invariants for polynomial dynamical systems. In: Chakraborty, S., Jerraya, A., Baruah, S.K., Fischmeister, S. (eds.) EMSOFT, pp. 97–106. ACM (2011)
12. Matringe, N., Moura, A.V., Rebiha, R.: Generating invariants for non-linear hybrid systems by linear algebraic methods. In: Cousot, R., Martel, M. (eds.) SAS 2010. LNCS, vol. 6337, pp. 373–389. Springer, Heidelberg (2010)
13. Morari, M., Thiele, L. (eds.): HSCC 2005. LNCS, vol. 3414. Springer, Heidelberg (2005)
14. Neuhaus, R.: Computation of real radicals of polynomial ideals II. Journal of Pure and Applied Algebra 124(13), 261–280 (1998)
15. Platzer, A.: Differential dynamic logic for hybrid systems. J. Autom. Reasoning 41(2), 143–189 (2008)
16. Platzer, A.: Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics. Springer, Heidelberg (2010)
17. Platzer, A.: A differential operator approach to equational differential invariants - (invited paper). In: Beringer, L., Felty, A.P. (eds.) ITP. LNCS, vol. 7406, pp. 28–48. Springer (2012)
18. Platzer, A.: Logics of dynamical systems. In: LICS, pp. 13–24. IEEE (2012)
19. Platzer, A.: The structure of differential invariants and differential cut elimination. Logical Methods in Computer Science 8(4), 1–38 (2012)
20. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: Gupta, A., Malik, S. (eds.) CAV 2008. LNCS, vol. 5123, pp. 176–189. Springer, Heidelberg (2008)
21. Rodríguez-Carbonell, E., Kapur, D.: An abstract interpretation approach for automatic generation of polynomial invariants. In: Giacobazzi, R. (ed.) SAS 2004. LNCS, vol. 3148, pp. 280–295. Springer, Heidelberg (2004)
22. Rodríguez-Carbonell, E., Tiwari, A.: Generating polynomial invariants for hybrid systems. In: Morari, Thiele (eds.) [13], pp. 590–605
23. Sankaranarayanan, S.: Automatic invariant generation for hybrid systems using ideal fixed points. In: Johansson, K.H., Yi, W. (eds.) HSCC, pp. 221–230. ACM (2010)
24. Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Constructing invariants for hybrid systems. Formal Methods in System Design 32(1), 25–55 (2008)
25. Stengel, R.F.: Flight Dynamics. Princeton University Press (2004)
26. Tiwari, A.: Approximate reachability for linear systems. In: Maler, O., Pnueli, A. (eds.) HSCC 2003. LNCS, vol. 2623, pp. 514–525. Springer, Heidelberg (2003)
27. Tiwari, A.: Abstractions for hybrid systems. Formal Methods in System Design 32(1), 57–83 (2008)
28. Tiwari, A., Khanna, G.: Nonlinear systems: Approximating reach sets. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 600–614. Springer, Heidelberg (2004)