Characterizing Algebraic Invariants by Differential Radical Invariants

Khalil Ghorbal* **André Platzer***

November 2013
CMU-CS-13-129

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

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. 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: algebraic invariant, differential ideals, high-order Lie derivation, differential equation, automated generation, row reduction, abstraction, continuous dynamics, formal verification, hybrid system

Abstract

We give a necessary and sufficient characterization of algebraic invariants of algebraic differential equations by a differential radical invariance criterion, i.e. an explicit equation on higher-order Lie derivatives. Differential radical invariants are computationally easy to check using polynomial arithmetic on higher-order Lie derivatives. The characterization makes it possible to generate invariants by solving for the coefficients in a parametrization by comparing coefficients. We investigate symbolic linear algebra tools based on Gaussian elimination to efficiently automate the generation of algebraic invariants. The approach can, e.g., generate non-trivial algebraic invariants capturing the exact airplane behavior during take-off or landing in longitudinal motion.

1 Introduction

Reasoning about the solutions of differential equations by means of their first integrals (conserved functions and expressions) is ubiquitous all over science studying dynamical processes. It is even crucial in many scientific domains. For instance, many physical experiments require a guarantee that the behavior of the system will remain within a certain predictable range. In computer science, the interest of the automated generation of algebraic 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 [10], abstraction [20, 27], or approximation [5]. Fundamentally, however, the study of safety of hybrid systems can be shown to reduce constructively to the problem of generating invariants for their differential equations [13]. We focus on this core problem in this paper and study the case of algebraic invariants, i.e. invariants described by a polynomial equation $h(\boldsymbol{x}) = 0$ for algebraic differential equations, i.e. systems of differential equations in (vectorial) explicit form $\frac{d\boldsymbol{x}}{dt} = \boldsymbol{p}(\boldsymbol{x})$ with a polynomial right-hand side. The class is far from restrictive and many analytic non-algebraic functions such as the square root, the inverse, the exponential or trigonometric functions can be exactly modeled as solutions of differential equations with polynomial vector field (a concrete example will be given in Section Section 6.2). Once suitable invariants of a system have been found, they can be used in proofs [11], as abstractions for reachable sets [28], or as a way of handling differential equations in abstract interpretation [20].

While algebraic invariant equations are often not the only invariants of interest for hybrid systems [14, 17], they are still related intimately to more general classes of invariants such as semi-algebraic invariants. We, thus, believe the characterization of algebraic invariants that we achieve in this paper to be an important step forward in understanding the invariance problem of hybrid systems.

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

Contributions. The primary contribution of this paper is that we identify a *necessary and sufficient* characterization of algebraic invariants of algebraic differential equations. This characterization yields a semi-decision procedure for polynomial equational invariants. It is computationally attractive, because checking invariants reduces to simple polynomial arithmetic on higher-order Lie derivatives of polynomials. As a second contribution, we identify an efficient way of using the characterization for generating invariants using symbolic linear algebra. The resulting approach is shown to scale to interesting case studies.

2 Soundness by Zariski Closure

We study the autonomous[1] ordinary differential equation system given below (1). 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. Let $\boldsymbol{x} \stackrel{\text{def}}{=} (x_1, \ldots, x_n) \in \mathbb{R}^n$, and $\boldsymbol{x}(t) \stackrel{\text{def}}{=} (x_1(t), \ldots, x_n(t))$, where $x_i : \mathbb{R} \to \mathbb{R}; t \mapsto x_i(t)$. The initial value of the system will be denoted by $\boldsymbol{x}_\iota \stackrel{\text{def}}{=} \boldsymbol{x}(t_\iota) = (x_1(t_\iota), \ldots, x_n(t_\iota)) \in \mathbb{R}^n$ for some $t_\iota \in \mathbb{R}$. As we focus on characterizing the continuous part, we do not consider any additional constraint on the dynamics, that is the evolution domain corresponds to the domain of definition. The abstraction and invariants found here can be used to help finding a *global* fixpoint for the whole hybrid-system, where any additional constraint, on the evolution domain or initial values, needs to be considered.

Definition 1 (Algebraic Differential Equation)**.** *Let p_i be multivariate polynomials of the polynomial ring $\mathbb{R}[\boldsymbol{x}]$. An algebraic differential equation with initial value $\boldsymbol{x}_\iota \in \mathbb{R}^n$ is the system:*

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

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 open set $U_t \subseteq \mathbb{R}$. A global solution defined for all $t \in \mathbb{R}$ may not exist in general (unless, e.g. the system is globally Lipschitz). 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 $\mathbb{R} \setminus \{t_\iota + \frac{1}{x_\iota}\}$. Nevertheless, for the considered class of ordinary differential equation systems, local solutions always exist.

Definition 2 (Algebraic Invariant Expression)**.** *An algebraic invariant expression 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 $\boldsymbol{x}(t)$, $t \in U_t$, is the maximal solution of* (1)*.*

The function $h(\boldsymbol{x}(t))$, and hence the polynomial $h(\boldsymbol{x})$, depend on the initial value $\boldsymbol{x}_\iota$. We implicitly assume this dependency for a clearer notation. We stress the fact that algebraic invariant expressions generalize algebraic invariant functions, that is, functions that remain constant while the system evolves (see [17] for a detailed discussion).

Observe also that $h(\boldsymbol{x}(t)) \in \mathbb{R}$, as a real function of time t, is only defined over the open set $U_t \subseteq \mathbb{R}$ as 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 $\mathbb{R}^n$.

Given an algebraic differential system, we search for a polynomial $h(\boldsymbol{x})$ such that $h(\boldsymbol{x}(t)) = 0$ for all $t \in U_t$. 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*, ot simply a variety. In the sequel, we formalize how varieties can be used to soundly overapproximate the reachable set $\{\boldsymbol{x}(t) \mid t \in U_t\}$. We first give a formal definition of the reachable set as the orbit of the differential equation system.

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

Definition 3 (Orbit)**.** *The orbit of* (1) *through the initial state* $\boldsymbol{x}_\iota \in \mathbb{R}^n$ *is defined as*

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

where $\boldsymbol{x}(t)$ *is the solution of* (1) *w.r.t. the initial value* $\boldsymbol{x}_\iota$*.*

The complete characterization of the orbit requires the exact solution of the original system. Very few systems admit an analytic solution, although a local approximation can be always given using Taylor series approximations (such approximation is for instance used in [5]). In this work, we discuss a sound overapproximation of the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ using (affine) varieties. The idea is to embed the orbit (which is not a variety in general) in a variety to be defined. The embedding (or topological closure) we will be using is a well-known closure operation in algebraic geometry called Zariski closure (see [2, Chapter 4] for an introduction). Varieties, which are sets of points, can be represented and computed efficiently using their algebraic counterpart: ideals of polynomials. Therefore, we first recall two useful definitions: an ideal I of the ring $\mathbb{R}[\boldsymbol{x}]$ and the variety $V(I)$ corresponding to an ideal I.

Definition 4 (Ideal)**.** *An ideal* I *of* $\mathbb{R}[\boldsymbol{x}]$ *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 for all* $q \in \mathbb{R}[\boldsymbol{x}]$*,* $qh \in I$*.*

We use $\langle h_1, \ldots, h_r \rangle$, for a finite natural number r, to denote the set 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 definition, the set $\langle h_1, \ldots, h_r \rangle$ is an ideal. More interestingly, by Hilbert's Basis Theorem [3], any ideal I of $\mathbb{R}[\boldsymbol{x}]$ can be *finitely generated* by, say, $\{h_1, \ldots, h_r\}$, so that $I = \langle h_1, \ldots, h_r \rangle$.

Definition 5 (Variety of an ideal)**.** *Given an ideal* I *of* $\mathbb{R}[\boldsymbol{x}]$*, the variety* $V(I)$ *is a subset of* $\mathbb{R}^n$ *defined by the common roots of all polynomials in* I*. That is,*

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

By Def. 5, $V(.)$ can be thought of as an operator that maps ideals to subsets of $\mathbb{R}^n$. In general, the map $V(.)$ is not injective: two distinct ideals 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 incomparable: the polynomial $x_1 \in I_1$ is not in I_2 but $x_2 \in I_2$ is not in I_1.

We are now ready to formally define the closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ of the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ by first defining the *vanishing ideal* $I(\mathcal{O}(\boldsymbol{x}_\iota))$ of the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ as the set of polynomials that evaluates to zero for all $\boldsymbol{x} \in \mathcal{O}(\boldsymbol{x}_\iota)$:

$$I(\mathcal{O}(\boldsymbol{x}_\iota)) \stackrel{\text{def}}{=} \{h \in \mathbb{R}[\boldsymbol{x}] \mid \forall \boldsymbol{x} \in \mathcal{O}(\boldsymbol{x}_\iota), h(\boldsymbol{x}) = 0\} \ . \tag{2}$$

By definition, the set $I(\mathcal{O}(\boldsymbol{x}_\iota)) \subseteq \mathbb{R}[\boldsymbol{x}]$ is an ideal as it satisfies the requirements of Def. 4. Observe that, very much like $V(.)$, we can think of $I(.)$, in (2), as an (non injective) operator that acts on subsets of $\mathbb{R}^n$. The *Zariski closure*, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$, of $\mathcal{O}(\boldsymbol{x}_\iota)$ is defined as the variety of the vanishing ideal of $\mathcal{O}(\boldsymbol{x}_\iota)$:

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

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 $\mathcal{O}(\boldsymbol{x}_\iota)$ of (1), including necessarily the initial value $\boldsymbol{x}_\iota$:

Proposition 1 (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 $I(\mathcal{O}(\boldsymbol{x}_\iota))$ (by definition of the vanishing ideal, see equation (2)), and all roots of all polynomials in $I(\mathcal{O}(\boldsymbol{x}_\iota))$ are in $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ (by definition of the variety of an ideal, see definition 5). Hence, $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq V(I(\mathcal{O}(\boldsymbol{x}_\iota))) = \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. □

Hence, all safety properties that hold true for $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$, are also true for $\mathcal{O}(\boldsymbol{x}_\iota)$. Soundness (Proposition 1) corresponds to the reflexivity property $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq \bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ of the Zariski closure. The algebraic geometrical fact that the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is the smallest [2] 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 $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) = \mathbb{R}^n$ is the whole space, and the Zariski closure operation fails to be informative. Since the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is the most precise variety containing the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$, the uselessness of the closure we define in this work happens exactly when there are no polynomial equations in $\boldsymbol{x}$ which set of roots contain $\mathcal{O}(\boldsymbol{x}_\iota)$ other than the trivial equation $0 = 0$. For instance, for (non-degenerated) one dimensional systems ($n = 1$) that evolve over time, the only univariate polynomial that has infinitely many roots is the zero polynomial.

Therefore, the accuracy of our subsequent computation inherits from the geometrical precision 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 systems. 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 evolves without saying anything about where the system will be at what time (which is what a solution would describe and which exactly what the abstraction we are defining here tries to get rid off). In particular, $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is independent of whether the system evolves forward or backward in time.

By Proposition 1, the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ provides sound and precise equational invariants for the behavior of system (1). Its definition, however, depends on the solution of the system (1), which is in general intractable, if at all computable. The key step in getting a computational handle

[2] w.r.t. to the usual geometrical sense, that is any other variety that contains the operand contains also its closure.

on $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ is the use of Lie derivatives [3]. The Lie derivative of a polynomial along a vector field [4] h will be denoted by $\mathfrak{L}_{\boldsymbol{p}}(h)$ and is defined as follows.

Definition 6 (Lie derivative along a vector field)**.** *For $h \in \mathbb{R}[\boldsymbol{x}]$ and $\boldsymbol{p} \stackrel{\text{def}}{=} (p_1, \ldots, p_n)$ from* (1)*, the Lie-derivative of h along the vector field $\boldsymbol{p}$ is defined by:*

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

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

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

We are now able to state a useful and well known (see for instance [22, Theorem 3.1] and [12, Lemma 3.7]) property of the ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$.

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

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 (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 $\boldsymbol{x}(t)$. This means that $\boldsymbol{x}(t)$ is a zero of the Lie derivative of h, $\mathfrak{L}_{\boldsymbol{p}}(h)$, 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 a polynomial h to be an algebraic invariant.

3 Characterization of Algebraic Invariants

In the previous section, the closure operation was used to embed the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$ into the smallest variety containing it, namely $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$. Given a variety, as a purely geometrical object, it is not easy in general to compute an algebraic representation for it. A variety $V(I)$ generated by an ideal I of polynomials, however, can be represented easily through the ideal I which is in turn represented by a finite set of polynomials that generate it.

In this section, we give an explicit characterization of the elements of the vanishing ideal, $I(\mathcal{O}(\boldsymbol{x}_\iota))$, that defines the Zariski closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ (see Def. 3 and (3)). We further explain how this characterization can be used to both check and generate algebraic invariant candidates of a given algebraic differential system. The following theorem, main contribution of this work, states a new necessary and sufficient condition for a polynomial h to be in $I(\mathcal{O}(\boldsymbol{x}_\iota))$.

[3] The relationship of Lie derivatives to solutions can be made precise by the derivation lemma [17, Lemma 2]

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

Theorem 1. *A polynomial $h \in \mathbb{R}[\boldsymbol{x}]$ is in the ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$, if and only if, there exists a finite positive integer N, such that*

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

$$\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h)(\boldsymbol{x}_\iota) = 0, \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h)(\boldsymbol{x}_\iota) = 0 \ . \tag{$\imath\imath$}$$

Proof. Necessary condition. Let h be a polynomial in the ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Then, the ideal $\langle h \rangle \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$ (ideals are stable under exterior multiplication Def. 4). By Proposition 2, $\mathfrak{L}_{\boldsymbol{p}}(h)$ is also in $I(\mathcal{O}(\boldsymbol{x}_\iota))$. Therefore, we recursively construct an ascending chain of ideals using the Lie derivative as an operator, we get:

$$\langle h \rangle = \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h) \rangle \subset \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h), \mathfrak{L}_{\boldsymbol{p}}^{(1)}(h) \rangle \subset \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h), \mathfrak{L}_{\boldsymbol{p}}^{(1)}(h), \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h) \rangle \cdots \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota)) \ .$$

The property $\imath$) follows from the ascending chain condition on ideals of the (Notherian) ring of polynomials: every ascending chain on ideals admits a maximal element. Since the chain above is ascending, it necessarily reaches a maximal element after finitely many N steps. The condition $\imath\imath$) 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 ($\imath$) and ($\imath\imath$) are 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 $I(\mathcal{O}(\boldsymbol{x}_\iota))$ (see equation (2)). 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: $f(t) \stackrel{\text{def}}{=} h(\boldsymbol{x}(t))$. We want to prove that the function f is identically zero on U_t. By equation ($\imath$), there exists a set of polynomials $g_i(\boldsymbol{x})$ such that

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

Let $\alpha_i : U_t \to \mathbb{R}$; $t \mapsto g_i(\boldsymbol{x}(t))$.The equality (7), together with the initial value condition given by equation ($\imath\imath$), can be transformed into the following homogeneous higher-order linear differential equation

$$f^{(N)}(t) - \sum_{i=0}^{N-1} \alpha_i(t) f^{(i)}(t) = 0 \tag{5}$$

$$f^{(0)}(t_\iota) = f^{(1)}(t_\iota) = \cdots = f^{(N-1)}(t_\iota) = 0 \tag{6}$$

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 original differential equation system. We know, however, that they are all continuous functions which is enough for this proof. By (global) Cauchy-Lipschitz theorem, applied to the newly defined system (which is the N dimensional linear non-autonomous —α_i are time dependent— system using the encoding $\boldsymbol{f} = (f^{(0)}, \ldots, f^{(N-1)})$), there exists a unique solution $\boldsymbol{f}(t)$ defined on the entire interval U_t, that satisfies the initial condition $\boldsymbol{f}_\iota = 0$. However, the null function, $\boldsymbol{f}(t) = 0$ is an obvious solution to the system. Hence, $\boldsymbol{f}(t)$ is identically zero on all U_t. By definition of $\boldsymbol{f}(t)$, and for all, $0 \leq i \leq N-1$, $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)(\boldsymbol{x}(t)) = 0$ for all $\boldsymbol{x}(t)$, i.e. the polynomial h as well as all its Lie derivatives are members of $I(\mathcal{O}(\boldsymbol{x}_\iota))$. □

The explicit version of ($\imath$), used in the proof of Theorem 1, namely

$$\exists\, g_i \in \mathbb{R}[\boldsymbol{x}], 0 \leq i \leq N-1 : \mathfrak{L}_{\boldsymbol{p}}^{(N)}(h) = \sum_{i=0}^{N-1} g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h) \ . \tag{7}$$

Equation (7) in Theorem 1 is an explicit version of ($\imath$) that is computationally easy to check by polynomial arithmetic on higher-order Lie derivatives of h with respect to the dynamics (1).

The construction of the ideal in equation ($\imath$) is very similar to the construction of the radical of an ideal [5], except with higher-order Lie derivatives, $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)$, in place of higher powers of polynomials h^i. We, therefore, call a polynomial equation $h = 0$ a *differential-radical invariant* for the system (1) if $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, or equivalently, h satisfies equations ($\imath$) and ($\imath\imath$).

Algebraic invariants (Def. 2) are defined semantically as the polynomials that evaluate to zero all along the solutions of (1). Differential-radical invariants are, on the other hand, defined by computationally "well-behaved" higher-order Lie derivatives. Both coincide:

Corollary 1 (Differential-radical characterization)**.** *The algebraic invariants of* (1) *are exactly the differential-radical invariants of* (1)*.*

Proof. On one hand, $I(\mathcal{O}(\boldsymbol{x}_\iota))$, by definition, contains all algebraic invariants, i.e., all polynomials that vanish along the solution of (1). On the other hand, by Theorem 1, elements of $I(\mathcal{O}(\boldsymbol{x}_\iota))$ are exactly the differential-radical invariants. □

Furthermore, the characterization given in Theorem 1 is of great importance when it comes to checking whether a given candidate is an algebraic invariant for a given system in the form of (1).

Corollary 2 (Decidability of invariant expressions)**.** *It is decidable whether a polynomial h with real algebraic coefficients is an algebraic invariant of an algebraic differential system with real algebraic coefficients and real algebraic initial values.*

Proof. If the candidate satisfies conditions ($\imath$) and ($\imath\imath$), then it is an algebraic invariant. Otherwise, the candidate is not an invariant, as all algebraic invariants have to satisfy these conditions. □

Going one step further, differential-radical invariants give an insight about the algebraic structure of the vanishing ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$. The higher-order Lie derivatives of a differential-radical invariant h_j play a major role in Theorem 1 as they span a differential ideal that underapproximates $I(\mathcal{O}(\boldsymbol{x}_\iota))$. The differential ideal related to h_j in condition ($\imath$):

$$J_j \stackrel{\text{def}}{=} \langle \mathfrak{L}_{\boldsymbol{p}}^{(0)}(h_j), \ldots, \mathfrak{L}_{\boldsymbol{p}}^{(N-1)}(h_j) \rangle, \tag{8}$$

for some finite N (dependent on h_j), underapproximates $I(\mathcal{O}(\boldsymbol{x}_\iota))$: $J_j \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$. Observe that $I(\mathcal{O}(\boldsymbol{x}_\iota))$ is a proper [6] ideal, and consequently, J_j is itself proper. Goemetrically, the closure $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ can never be the empty variety (but could be the whole space) as it always contains at least one

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

[6] a proper ideal is an ideal distinct from the whole ring $\mathbb{R}[\boldsymbol{x}]$.

point: $\boldsymbol{x}_\iota$. By the (weak) Nullstellensatz, its vanishing ideal does not contain 1 and is hence proper. The fact that J_j is proper is enforced in Theorem 1 by equation $(\imath\imath)$ which literally says that the system of polynomial equations $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h_j) = 0$, $0 \leq i \leq N-1$, has at least $\boldsymbol{x}_\iota$ as a common root.

Henceforth, $I(\mathcal{O}(\boldsymbol{x}_\iota))$ can be underapproximated by successive computation of its elements h_j and, more importantly, their related differential proper ideals:

$$\bigoplus_{j \in \Im} J_j = I(\mathcal{O}(\boldsymbol{x}_\iota)) \ .$$

The sum of two ideals, denoted by $\oplus$, is the ideal generated by concatenating the list of generators of the operands. Again, by the ascending chain condition, the set of indices $\Im$ has to be finite.

Theorem 2 (Structure of The Invariants Ideal)**.** *The vanishing ideal $I(\mathcal{O}(\boldsymbol{x}_\iota))$ is a finite sum of proper differential ideals.*

Although, we know, by the celebrated Hilbert Basis Theorem, that $I(\mathcal{O}(\boldsymbol{x}_\iota))$ is finitely generated, like any other ideal of $\mathbb{R}[\boldsymbol{x}]$, computing all its generators may be intractible. Vanishing ideals in real algebraic geometry are notoriously hard to compute. In fact, by the real Nullstellensatz, vanishing ideals are exactely the real radical ideals [1, Section 4]. Fortunately, by Theorem 2, differential-radical invariants allow for a sound and precise overapproximation of the close $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ and hence the orbit $\mathcal{O}(\boldsymbol{x}_\iota)$.

Proposition 3 (Soundness of Differential-Radical Invariants)**.** *Differential-radical invariants are sound, that is, for a differential-radical invariant h, and its related differential ideal J (as defined in* (8)*), $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq V(J)$.*

Proof. This is the geometrical counterpart of $J \subseteq I(\mathcal{O}(\boldsymbol{x}_\iota))$. Recall that $\bar{\mathcal{O}}(\boldsymbol{x}_\iota) = V(I(\mathcal{O}(\boldsymbol{x}_\iota)))$ and that the $V(.)$ operator, defined (Def. 5) on ideals of $\mathbb{R}[\boldsymbol{x}]$, inverts the inclusion, that is for two ideals I_1 and I_2, $I_1 \subseteq I_2$ implies $V(I_1) \supseteq V(I_2)$. □

As a corollary of Proposition 3, the overapproximation of $\bar{\mathcal{O}}(\boldsymbol{x}_\iota)$ can be refined at a cost of computing additional differential-radical invariants.

Corollary 3. *Let $h_1, \ldots, h_r$ denote a family of differential-radical invariants, and let $J_1, \ldots, J_r$ denote their respective ideals, then*

$$\bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq \bigcap_{1 \leq i \leq r} V(J_i) \ . \tag{9}$$

Proof. It is sufficient to apply Proposition 3 for each h_i, $1 \leq i \leq r$, individually. □

The next section shows how Theorem 1 can be used in practice to automatically generate differential-radical invariants.

4 Effective Generation of Algebraic Invariants

We explain in this section how we automatically construct differential-radical invariants given the system (1). Using the condition ($\imath$) of Theorem 1 we derive a set of constraints that the coefficients of a radical-differential invariant (of a certain degree d) have to satisfy. We then solve these constraints and discuss the different interpretations of the condition ($\imath\imath$) of Theorem 1.

As seen earlier, the condition ($\imath$) of Theorem 1 has an explicit formulation, given in equation (7) in term of polynomial arithmetics. This equation is the key ingredient for the automated generation of radical-differential invariant. 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 non-negative integers ($d_i \geq 0$). By convention, $x_i^0 = 1$ for any x_i. If the coefficient α is non-zero, the monomial degree is defined by

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

A polynomial can be written in a canonical form as a finite sum of monomials with non-zero 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 degree d of all non-zero 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 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 with a suitable power of x_0, any polynomial of $\mathbb{R}[\boldsymbol{x}]$ can be homogenized to a (homogeneous) polynomial in $\mathbb{R}[x_0][\boldsymbol{x}]$.[7] The system given in (1) 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:

$$d' \stackrel{\text{def}}{=} \max_i(\deg(p_i)) \ . \tag{10}$$

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 at least one of the $p_i \neq 0$, as otherwise $\bar{\mathcal{O}}(\boldsymbol{x}_\imath) = \{\boldsymbol{x}_\imath\}$ and $I(\mathcal{O}(\boldsymbol{x}_\imath)) = \langle x_0 - \boldsymbol{x}_{\imath 0}, \ldots, x_n - \boldsymbol{x}_{\imath n}\rangle$, and nothing else needs to be done. So, d' is always defined.

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

The homogenization of polynomials presented here is very similar to the idea of homogeneous (or projective) varieties in projective geometry, where the homogenized polynomial is the representative of the original polynomial in the projective plane [9, Chapter 1]. From a computational

[7] 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.

prospective, working in the projective plane offers a more symmetric representation of polynomials: the constant terms can be regarded to as simple monomials. The arithmetic of degrees is also simplified as all monomials are saturated to the same degree. Hence, we benefit from the graded structure of the polynomial ring.

We now use the differential-radical criterion (7), in the projective system, to explicitely derive the constraints on the coefficients of a parametric form of a given degree. If h denotes a form of degree d, and d' is as defined in equation (10), then the degree of the polynomial $\mathfrak{L}_{\boldsymbol{p}}^{(k)}(h)$ is given by:.

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

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 arbitrarely 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.

In the reminder of this section, the original system given in (1) is lifted to $\mathbb{R}[x_0][x_1, \ldots, x_n]$. Therefore, we only consider forms of $\mathbb{R}[x_0][x_1, \ldots, x_n]$. 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: $x_0, \ldots, x_n$. Theorem 1 can now be applied to characterize forms of $I(\mathcal{O}(\boldsymbol{x}_\iota)) \subseteq \mathbb{R}[x_0, \ldots, x_n]$.

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

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

monomials (the binomial coefficient indexed by $n + d$ 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 the monomials of a form h, that is 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 compare the degrees of x_1 first, and if equal we compare the degrees of x_2 and so one till reaching x_n and then x_0. For instance, for $n = 2$, a parametrized form h of degree $d = 1$ is equal to $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$.

Let h be a form of degree d and let $\boldsymbol{\alpha} \stackrel{\text{def}}{=} (\alpha_1, \ldots, \alpha_{m_d})$ denote the coefficients' vector with respect to the monomial order defined above. Let $\boldsymbol{\beta}_i$, $0 \leq i \leq N - 1$, denote the coefficients' vector of the parametrized form g_i (see equation (7)). Exploiting the graded algebra structure of $\mathbb{R}[x_0, \ldots, x_n]$, the degree of each term $g_i \mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)$ should match the degree of $\mathfrak{L}_{\boldsymbol{p}}^{(N)}(h)$ for a fixed positive integer N. Hence, by equation (11):

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

The coefficients' vector of each form g_i is then a vector, $\boldsymbol{\beta}_i$, of size $m_{(N-i)(-1+d')}$ (see equation (12)). In addition, equation (7) gives $m_{d+N(-1+d')}$ bilinear equations involving $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}_i$. Example 1 gives a concrete example for $N = 1$.

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 form h is equal to $\alpha_1 x_1 + \alpha_2 x_2 + \alpha_3 x_0$. Its first-order Lie derivative form $\mathfrak{L}_{\boldsymbol{p}}(h)$ has the same*

degree, 1*, and is equal to* $\alpha_1(a_1x_1 + a_2x_2) + \alpha_2(b_1x_1 + b_2x_2)$*. 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:*

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

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 $M_{d,N}(\beta)$ is called the *matrix representation* of the condition $(\imath)$ of Theorem 1 and is formally introduced by Lemma 1.

Lemma 1 (Matrix Representation)**.** *Let* $d > 0$ *and* $N > 0$ *be two non-negative integers. Let* $\boldsymbol{\alpha} \in \mathbb{R}^{m_d}$ *be the coefficients of the parametrized form* h *of degree* d*. Similarly, let* $\boldsymbol{\beta}_i \in \mathbb{R}^{m_{(N-i)(-1+d')}}$*,* $0 \leq i \leq N-1$*, denote the coefficients of the parametrized forms* g_i *of respective degrees* $(N-i)(-1+d')$*. Finally, let* $\boldsymbol{\beta}$ *denote the concatenation of all* $\boldsymbol{\beta}_i$*. The polynomial* h *satisfies the condition* $(\imath)$ *of Theorem 1 if and only if there exists a matrix* $M_{d,N}(\boldsymbol{\beta})$ *such that* $M_{d,N}(\boldsymbol{\beta})\boldsymbol{\alpha} = 0$*. The matrix* $M_{d,N}(\boldsymbol{\beta})$ *has* $m_{d+N(-1+d')}$ *rows and* m_d *columns. Its elements are linear in the coefficients of* $\boldsymbol{\beta}$*.*

Proof. The system of constraints derived from equation (7) is bilinear in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Therefore, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ can be decoupled and the system can be equivalently rewritten as a symbolic linear algebra problem of the form $M_{d,N}(\boldsymbol{\beta})\boldsymbol{\alpha} = 0$. □

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 pre-image of the vector $0 \in \mathbb{R}^c$:

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

Let $s \stackrel{\text{def}}{=} \dim(\ker(M_{d,N}(\boldsymbol{\beta}))) \leq m_d$. If $s = 0$, or equivalently the kernel is reduced to $\{0\}$. Then, $\boldsymbol{\alpha} = 0$ and, for the chosen N, the only ideal generated by a form of degree d is the trivial ideal $\langle 0\rangle$. In such cases, one can either increase N or the degree d for the dimension of the kernel of $M_{d,N}(\boldsymbol{\beta})$ to be strictly positive. If, however, $s > 0$, then by condition $(\imath\imath)$ of Theorem 1 we obtain an *invariant (projective) variety* for the given algebraic system (1): whenever the system starts in this variety, it will never leave it.

Theorem 3 (Local Invariant (Projective) Varieties)**.** *If there exist nonnegative integers,* $d > 0$ *and* $N > 0$*, and a vector* $\boldsymbol{\beta}$ *such that* $\dim(\ker(M_{d,N}(\boldsymbol{\beta}))) > 0$*, then for any non-zero vector,* $\boldsymbol{\alpha}$ *of* $\ker(M_{d,N}(\boldsymbol{\beta}))$*, the projective variety* $V(J_{\boldsymbol{\alpha}})$ *is invariant for the system:* $J_{\boldsymbol{\alpha}}$ *(see equation* (8)*) denotes the ideal related to the differential-radical invariant* $h_{\boldsymbol{\alpha}}$*, itself obtained by instantiating the parametrized form* h *(of degre* d*) with the vector* $\boldsymbol{\alpha}$*. (By setting the variable* x_0 *to* 1*, we recover an invariant variety of the original system before homogenization.)*

Proof. By choosing $\boldsymbol{\alpha}$ in the kernel of $M_{d,N}(\boldsymbol{\beta})$, we ensure that condition $(\imath)$ of Theorem 1 is satisfied for N. Furthermore, by forcing the system to start somewhere in the variety $V(J_{\boldsymbol{\alpha}})$, we chose exactely the initial values $\boldsymbol{x}_\iota$ that satisfy condition $(\imath\imath)$ of Theorem 1. Hence, for those intial values, $h_{\boldsymbol{\alpha}}$ is a differential-radical invariants and $\mathcal{O}(\boldsymbol{x}_\iota) \subseteq \bar{\mathcal{O}}(\boldsymbol{x}_\iota) \subseteq V(J_{\boldsymbol{\alpha}})$. □

Theorem 3 is a direct consequence of Theorem 1. It is stated in a way particularly suitable for the automated generation of invariant varieties as the requirements are phrazed using symbolic linear algebra formulation. More importantly, it exhibits an important characteristic of differential-radical invariants, namely their ability to generate invariants as a conjunction of polynomials, where none of the involved polynomials alone is an invariant (see the first case study in Section 6 for a concrete example).

Following the same reasoning, we discuss in the sequel under which conditions the initial value $\boldsymbol{x}_\iota$ is unconstrained. That is, we want to generate, if exists, an invariant variety, parametrized by the intial value $\boldsymbol{x}_\iota$, that holds for any given initial condition $\boldsymbol{x}_\iota$. Such invariants are very useful and of particular interest as they partition the (whole) space into invariant disjoint regions. For instance, the energy function of a conservative Hamiltonian system (such as the perfect pendulum) partitions the space into disjoint enery level sets: depending on the intial enery of the system, the total enery will always remain constant. We will see that the energy functions are in fact a special case of the differential-radical invariants.

For conveninence to the reader, we first state some abstract geometrical facts that we will need later on.

Lemma 2. *Let $n > 1$. Let L be a linear subspace of $\mathbb{R}^n$, such that $\dim(L) > 0$ (i.e. L non reduced to the origin). Let S be a subspace of $\mathbb{R}^n$ such that $n - \dim(L) < \dim(S) \leq n$. The intersection of S and L is necessarily non-empty, i.e. there exists a vector v of S that is included in L.*

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

The condition $(\imath\imath)$ of Theorem 1 requires the vector $\boldsymbol{\alpha}$ to be in an intersection of N hyperplanes, $H_0, \ldots, H_{N-1}$, each defined explicitly by the condition $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)(\boldsymbol{x}_\iota) = 0$:

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

To give a concrete example, going back to Example 1, for $N = 2$, the two normal vectors that define the two hyperplanes, H_0 and H_1, are respectively: $\boldsymbol{x}_\iota = (x_1(t_\iota), x_2(t_\iota), 1)$ (related to $\mathfrak{L}_{\boldsymbol{p}}^{(0)}(h)(\boldsymbol{x}_\iota) = 0$) and $(a_1 x_1(t_\iota) + a_2 x_2(t_\iota), b_1 x_1(t_\iota) + b_2 x_2(t_\iota), 1)$ (related to $\mathfrak{L}_{\boldsymbol{p}}^{(1)}(h)(\boldsymbol{x}_\iota) = 0$).

In fact, for the homogenized system, all the hyperplanes H_i pass through the origin: the vector $0 \in \mathbb{R}^{m_d}$ is a trivial solution for the condition $(\imath\imath)$, where $\boldsymbol{\alpha} \in \mathbb{R}^{m_d}$ is the unknown. Using Lemma 2, we derive the required condition:

Theorem 4 (Global Invariant (Projective) Varieties)**.** *Let $d > 0$ and $N > 0$ be two natural numbers. Let h denote a parametrized form of degree d, and $M_{d,N}(\boldsymbol{\beta})$ the matrix representation of*

equation ($\imath\imath$) *according to Lemma 1. Let* $H_i \subseteq \mathbb{R}^{m_d}$, $0 \leq i \leq N-1$, *be the hyperplane defined by* $\mathfrak{L}_{\boldsymbol{p}}^{(i)}(h)(\boldsymbol{x}_\iota) = 0$. *Then,* $h \in I(\mathcal{O}(\boldsymbol{x}_\iota))$, *if and only if, there exists* $N > 0$, *and* $\boldsymbol{\beta}$ *such that*

$$\dim(\ker(M_{d,N}(\boldsymbol{\beta}))) > m_d - \dim\left(\bigcap_{0\leq i\leq N-1} H_i\right) \quad . \tag{14}$$

The matrix $M_{d,N}(\boldsymbol{\beta})$ *has* $m_{d+N(-1+d')}$ *rows and* m_d *columns. All its elements are linear in (the elements of)* $\boldsymbol{\beta}$.

Proof. According to Lemma 1, condition ($\imath$) of Theorem 1 is equivalent to having $\boldsymbol{\alpha} \in \ker(M_{d,N}(\boldsymbol{\beta}))$. By Lemma 2, for condition ($\imath\imath$) to be satisfied, equation (14) has to hold. □

Theorem 4 is new and it generalizes previous work by Matringe et al.. In fact, Theorem ... in [] is a particular case ($N = 1$) of Theorem 4. The requirement of Theorem 4 to ensure global invariance of a variety is clearly stronger than its local counterpart given in Theorem 3. Both tell us that, for a given $d > 0$ and $N > 0$, maximizing $\dim(\ker(M_{d,N}(\boldsymbol{\beta})))$ is a crucial step to generate either local or global invariants. We discuss the computation of $\ker(M_{d,N}(\boldsymbol{\beta}))$ is covered in the following sections.

Gaussian Elimination Let $\boldsymbol{\beta} \stackrel{\text{def}}{=} (\beta_1, \ldots, \beta_s) \in \mathbb{R}^s$.Given a symbolic matrix M with r rows and c columns, $c \leq r$, we want to find an instance $\boldsymbol{\beta}^*$ for $\boldsymbol{\beta}$ such that $\dim\ker(M(\boldsymbol{\beta})) > 1$, assuming that all the elements of M are linear 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 $M(\boldsymbol{\beta})$ to maximize the dimension of its kernel. The set $\mathcal{M}$ gathers all the instantiations of $M(\boldsymbol{\beta})$. 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, computing and solving the determinant (lines 2 and 3) are expensive. Instead, we row reduce the square matrix and record any divisions by the pivot element: we then branch with any $\boldsymbol{\beta}$ assignment that zero the denominator.

Example 2. *We apply Algorithm 1 to Example 1. The determinant of the matrix* $M(\beta)$ *is* $\beta(\beta^2 - (a_1 + b_2)\beta - a_2b_1 + a_1b_2)$. *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* $\beta = 0$ *which therefore leads to the following set* $\mathcal{M}$*:*

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

The kernel of the above matrix is generated by $(0, 0, 1)$, *its dimension is therefore* 1. *The only invariant in this case is therefore* $h(\boldsymbol{x}) = \alpha_3 x_0$. *Applying condition* ($\imath\imath$) *of Theorem 1, we obtain* $\alpha_3 = 0$ *and hence the trivial invariant* $0 = 0$, *as stated by Theorem 4. We conclude that we either need to increase* N *or look for invariants of high degrees, i.e. increase* d.

Algorithm 1: Find $\boldsymbol{\beta}^*$, s.t. (14).

Data: M: r rows, c columns, elements linear in elements of $\boldsymbol{\beta}$.
Result: A set of $M(\boldsymbol{\beta}^*)$, s.t. (14).
$\mathcal{M} \leftarrow \{M(\boldsymbol{\beta})\}$
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 $det_{\boldsymbol{\beta}} \leftarrow \det(M(l_{i_1}, \ldots, l_{i_q}))$
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
$\mathcal{M} \leftarrow \mathcal{M}'$

It is interesting to notice from Example 2 that the method triggers naturally a discussion on the parameters for the system to have a linear invariant. Let $\delta \stackrel{\text{def}}{=} (a_1 - b_2)^2 + 4a_2b_1$. If $\delta \geq 0$, the set $\mathcal{M}$ contains three matrices, namely $M(\beta)$, for $\beta \in \{0, \frac{1}{2}(a_1 + b_2 + \sqrt{\delta}), \frac{1}{2}(a_1 + b_2 - \sqrt{\delta})\}$. The case $\beta = 0$ leads to the same conclusion as above. When $\beta = \frac{1}{2}(a_1 + b_2 \pm \sqrt{\delta}) \neq 0$, and $a_2 \neq 0$, the kernel of $M(\beta)$ is generated by the vector $(a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0)$. For the condition $(\imath\imath)$ of Theorem 1 to hold, the following condition on the initial values $(x_1(t_\imath), x_2(t_\imath))$ have to hold:

$$\left(a_1 - b_2 \pm \sqrt{\delta}\right) x_1(t_\imath) + 2a_2 x_2(t_\imath) = 0 \ .$$

This implies that whenever the initial state lies in the hyperplane defined above, and under the assumption $\delta \geq 0$, the system is trapped in that same hyperplane. In fact, if $a_2 \neq 0$, the vector $\left(a_1 - b_2 \pm \sqrt{\delta}, 2a_2, 0\right)$ is nothing but the eigenvector of the matrix $M(\beta)$ related to the eigenvalue β. If $a_2 = 0$, then the determinant of the matrix $M(\beta)$ is $\beta(-a_1 + \beta)(-b_2 + \beta)$ and the three different new cases can be discussed similarly.

5 Related Work

Tremendous progress has been achieved over the past ten years to automate the generation of algebraic and semi-algebraic invariants. The initial focus was on approximation of the reachable sets at a given time for linear differential systems. In [4, 26] techniques from the spectral theory are used. The system is solved (which is always possible for linear differential systems) and the reachable set phrased as a quantifier elimination problem. In [26], the authors used different simplification techniques observing that special patterns of the eigenvalues can be translated in a straightforward manner to equational invariants based on results on o-minimal hybrid systems [4]. In [21], 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 [21]. In [28], Tiwari and Khanna started investigating nonlinear systems by adapting linear techniques. 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 (polynomial functions essentially) and may therefore miss others. The authors also used Gröbner Basis algorithm. The use of Syzygies has been generalized in [22], Sankaranarayanan characterized the invariant ideal of algebraic invariants as an ideal fixpoint of a monotonic operator (introduced in [24] and essentially applied for linear systems). The operator encodes the stability under Lie derivation and forces the invariant to hold true for any initial condition. Gröbner basis are also heavily used to compute the successive iteration of the operator. The convergence is ensured by iterating over pseudo-ideals [22]. In the same year, Matringe et al. [8] handled a special case of algebraic invariants, where the first-order Lie derivative of a polynomial is in the ideal generated by the polynomial itself (called P-consecution). The problem is phrased in term of maximization of the null-space of a linear (symbolic) matrix which is much more efficient than the two techniques used so far, namely, Gröbner basis and quantifier elimination. The same authors tried an extension to generate invariants spanned by formal

power series [19]. More recently, higher-order Lie derivatives were used by Liu et al. to derive semi-algebraic invariants [6] and Lyapunov functions [7] for nonlinear systems. They essentially extended the Barrier certificate [18] formulation to constrain a higher-order (instead of first-order) Lie derivative to be strictly negative whenever the trajectory touches the boundary of the certificate. Quantifier elimination is used to generate the semi-algebraic invariants, which is rather expensive and inefficient in practice given the degrees of the involved polynomials.

Characterization of Algebraic Invariants. Unlike previous work [28, 22, 19, 8], we start by overapproximating the reachable set (orbit) using its topological closure over (affine) varieties, 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 for its elements.

The work presented here can be thought of as dual to [22] where the (real radical) ideal of algebraic invariants is characterized as the *greatest* fixpoint of a monotonic refinement operator over the lattice of ideals: the fixpoint is approximated from above leading to a transfinite descending chain of ideals. This elegant theoretical characterization suffers from three drawbacks in practice: $1)$ the intermediate steps of the downward Tarski iterations are unsound (they overapproximate the invariants ideal, and therefore underapproximate the reachable set—orbit), the only sound result is either the fixpoint or any post fixpoint. $2)$ Each iteration is computationally intensive and requires the computation of a basis of syzygies module as well as an intersection of ideals which also requires a Gröbner basis computation. $3)$ Widening forces the iterations to be performed over pseudo-ideals[8], which forces the termination but may give a pessimistic post fixpoint. In fact, it is hard to measure the accuracy of the approximation and no "narrowing" operator was proposed.

We present a dual approach that does not have the above issues, by approaching the ideal of algebraic invariants from below (underapproximation). $1)$ We give a necessary and sufficient condition for a polynomial to be an algebraic invariant. To each invariant h corresponds a (differential) ideal, generated by the higher-order Lie derivatives of h, that underapproximates the ideal of algebraic invariants. $2)$ The computation (generation and checking) of the invariant h relies on the ascending chain condition and requires finitely, yet unbounded, many steps. It is furthermore translated into a symbolic linear algebra problem which reduces tremendously the computational complexity underlying algebraic invariants generation.

This novel approach allows to go one step further toward the automated generation and syntactic checking of algebraic invariants. The latter point is of great importance: if we want to check whether a given polynomial is an invariant of a given system a characterization of an invariant is required (unless we have the solutions of the system). Already existing necessary conditions are incomplete as they only use the first-order Lie derivative. This is partially addressed in [17] but requires a more restrictive extra condition. Theorem 1 gives a necessary and sufficient condition that only requires the computation of higher-order Lie derivative of the polynomial itself. It is worth noting that [28, 8] and [17, Theorem 3] are special cases of Theorem 1 where only the first-order Lie derivative is considered. The theorem is powerful enough to completely generate all algebraic invariants for linear systems (which is not the case of [22] unless the refinement operator is iterated over the ideals —not the pseudo-ideals— lattice). It hence gives a unifying framework

[8]This limits the computation to a bound degree to ensure a descending chain condition.

for [4, 26, 20] and includes equational differential invariants [17] as a special case.

Underlying Computation Techniques. We have developed and generalized the use of symbolic linear algebra tools to effectively generate algebraic invariants. The use of linear algebra was independently investigated by Matringe et al. [8]. In fact, [8, Theorems 1 and 2] are special cases of Theorem 1 and Theorem 4 where only the first-order Lie derivative is considered.

6 Case Studies

The following challenging example comes up as a subsystem of a study of aircraft dynamics:

$$p_1 = \dot{x_1} = -x_2,\ p_2 = \dot{x_2} = x_1,\ \dot{x_3} = x_4^2,\ \dot{x_4} = x_3 x_4,\ \boldsymbol{x}_\iota = (1, 0, 0, 1) \tag{15}$$

Such subsystems appear frequently whenever Euler angles and the three dimensional rotational matrix is used to describe the dynamics of rigid body motion. System (15) is an algebraic encoding of trigonometric functions with the unique solution $x_1(t) = \cos(t)$, $x_2(t) = \sin(t)$, $x_3(t) = \tan(t)$, $x_4(t) = \sec(t)$.

Using Theorem 1 it is easy to prove the following algebraic invariants of (15), which are associated with trigonometric identities as indicated:

$$\begin{aligned}
h_1 &= x_1^2 + x_2^2 - 1 && (\cos(t)^2 + \sin(t)^2 = 1)\\
h_2 &= x_1 x_4 - 1 && (\cos(t)\sec(t) = 1)\\
h_3 &= x_3 - x_2 x_4 && (\tan(t) = \sin(t)\sec(t))\\
h_4 &= x_4^2 - x_3^2 - 1 && (\sec(t)^2 = 1 + \tan(t)^2)
\end{aligned}$$

All these invariants can be generated easily using the algorithm in Section 4. The invariant h_1 is easy to find: its first-order Lie derivative vanishes. The other three invariants are more challenging and show why the higher derivatives in Theorem 1 are crucial. In fact, h_2, h_3 and h_4 generate the differential ideal $\langle h_i, \mathfrak{L}_{\boldsymbol{p}}(h_i), \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h_i)\rangle$ for any $i \in \{2, 3, 4\}$. Notice also that although p_1 and p_2 can be decoupled from the rest of the system, they are crucial to identify the other invariants. This example shows that in practice, decoupling the system should be avoided when possible as it may hide global invariants of the original system (although decoupling for the purpose of solving is always desired). 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 algebraic invariants to tightly capture the vertical motion of an airplane.

6.1 Collision Avoidance

We revisit the differential equation system encoding Dubin's vehicle model for aircrafts [29]. Although the system was discussed in many recent papers [22, 23, 6], they all missed one important invariant (actually two, but both are related as detailed in the sequel) that links both airplanes. It

turns out that the invariant helps proving a complete flyable collision avoidance maneuver for both aircrafts. This result builds on top of the improvements already done in [16, 11]. The differential equation system is given by:

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

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). In this case, apart from the already known invariants, we discovered the fact that the following algebraic invariants hold when ω_1 and ω_2 are arbitrarily instantiated to either 0 or ω:

$$h_1 = -e_2^0 d_1 - e_1^0 d_2 + d_2^0 e_1 + d_1^0 e_2 = 0,$$
$$h_2 = -e_1^0 d_1 + e_2^0 d_2 + d_1^0 e_1 - d_2^0 e_2 = 0 \ .$$

It is easy to check $h_1(\boldsymbol{x}_\iota) = h_2(\boldsymbol{x}_\iota) = 0$, $h_2 = \omega \mathfrak{L}_{\boldsymbol{p}}(h_1)$, $h_1 = -\omega \mathfrak{L}_{\boldsymbol{p}}(h_2)$ and:

$$\mathfrak{L}_{\boldsymbol{p}}^{(2)}(h_1) \in \langle h_1, \mathfrak{L}_{\boldsymbol{p}}(h_1)\rangle = \langle h_1, h_2\rangle = \langle h_2, \mathfrak{L}_{\boldsymbol{p}}(h_2)\rangle \ni \mathfrak{L}_{\boldsymbol{p}}^{(2)}(h_2) \ .$$

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 equation then discuss the non-trivial algebraic invariants 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] (u:axial velocity, w:vertical velocity, x:range, z:altitude, q:pitch rate, θ:pitch angle):

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

We encode the trigonometric functions following [15]. Our technique, as stated earlier, handles parametrized systems. Moreover, it is important to note that, unlike [22], we do not augment our set of variables with the parameters and state that these do not evolve over time. They are carried along the symbolic row-reduction computation as parameters. In fact, our algorithm makes it possible to infer some constraints on the parameters of the system to enforce an invariant without overhead: this can be used for instance to "synthesize" systems that must respect a given invariant. The same reasoning holds for the initial value, our algorithm assumes initially nothing about the initial values and is able to compute which initial conditions eventually trap the system into a variety. For the longitudinal mode, we were able to automatically find the following three non-trivial conserved quantities.

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

We substituted the intermediate variables that encode $\sin$ and $\cos$ back to emphasize the fact that algebraic invariants and algebraic differential systems are well suitable to encode many real complex dynamical systems.

7 Conclusion

The reachable set of solutions of algebraic differential system is soundly abstracted by the smallest (affine) variety that contains it using a geometrical closure operator. The variety is then represented using the ideal of algebraic invariants. We state a necessary and sufficient condition for a polynomial to be an algebraic invariant of an algebraic differential system. Our characterization permits effective computation (generation and checking) of algebraic invariants using linear symbolic computation. Our focus will be in bounding the number of iterations required to generate an algebraic invariant. We plan to investigate further the cases where the closure operator fails to give accurate approximation (as sketched for the 1-dimensional case).

References

[1] J. Bochnak, M. Coste, and M.F. Roy. *Real Algebraic Geometry*. A series of modern surveys in mathematics. Springer, 2010.

[2] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, 2007.

[3] David Hilbert. Über die theorie der algebraischen formen. *Mathematische Annalen*, 36(4):473–534, 1890.

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

[5] Ruggero Lanotte and Simone Tini. Taylor approximation for hybrid systems. In *HSCC*, pages 402–416, 2005.

[6] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Computing semi-algebraic invariants for polynomial dynamical systems. In *Proceedings of the ninth ACM international conference on Embedded software*, EMSOFT '11, pages 97–106, New York, NY, USA, 2011. ACM.

[7] Jiang Liu, Naijun Zhan, and Hengjun Zhao. Automatically discovering relaxed lyapunov functions for polynomial dynamical systems. *Math. Comp. Sci.*, 6(4):395–408, 2012.

[8] Nadir Matringe, ArnaldoVieira Moura, and Rachid Rebiha. Generating invariants for non-linear hybrid systems by linear algebraic methods. In Radhia Cousot and Matthieu Martel, editors, *Static Analysis*, volume 6337 of *LNCS*, pages 373–389. Springer Berlin Heidelberg, 2011.

[9] R. Miranda. *Algebraic Curves and Riemann Surfaces*. Dimacs Series in Discrete Mathematics and Theoretical Comput. American Mathematical Society, 1995.

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

[11] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010.

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

[13] André Platzer. The complete proof theory of hybrid systems. In *LICS*, pages 541–550, 2012.

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

[15] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008.

[16] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. *Form. Methods Syst. Des.*, 35(1):98–120, 2009.

[17] Andr Platzer. A differential operator approach to equational differential invariants. In Lennart Beringer and Amy Felty, editors, *Interactive Theorem Proving*, volume 7406 of *LNCS*, pages 28–48. Springer Berlin Heidelberg, 2012.

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

[19] Rachid Rebiha, Nadir Matringe, and Arnaldo Vieira Moura. Transcendental inductive invariants generation for non-linear differential and hybrid systems. In *HSCC*, pages 25–34, New York, NY, USA, 2012. ACM.

[20] Enric Rodríguez-Carbonell and Deepak Kapur. An abstract interpretation approach for automatic generation of polynomial invariants. In Roberto Giacobazzi, editor, *Static Analysis*, volume 3148 of *LNCS*, pages 280–295. Springer Berlin Heidelberg, 2004.

[21] Enric Rodríguez-Carbonell and Ashish Tiwari. Generating polynomial invariants for hybrid systems. In Manfred Morari and Lothar Thiele, editors, *HSCC*, volume 3414 of *LNCS*, pages 590–605. Springer Berlin Heidelberg, 2005.

[22] Sriram Sankaranarayanan. Automatic invariant generation for hybrid systems using ideal fixed points. In *HSCC*, pages 221–230, New York, NY, USA, 2010. ACM.

[23] Sriram Sankaranarayanan. Automatic abstraction of non-linear systems using change of bases transformations. In *HSCC*, pages 143–152. ACM, 2011.

[24] Sriram Sankaranarayanan, HennyB. Sipma, and Zohar Manna. Fixed point iteration for computing the time elapse operator. In JooP. Hespanha and Ashish Tiwari, editors, *HSCC*, volume 3927 of *LNCS*, pages 537–551. Springer Berlin Heidelberg, 2006.

[25] R.F. Stengel. *Flight Dynamics*. Princeton University Press, 2004.

[26] Ashish Tiwari. Approximate reachability for linear systems. In Oded Maler and Amir Pnueli, editors, *HSCC*, volume 2623 of *LNCS*, pages 514–525. Springer Berlin Heidelberg, 2003.

[27] Ashish Tiwari. Abstractions for hybrid systems. *Form. Methods Syst. Des.*, 32(1):57–83, 2008.

[28] Ashish Tiwari and Gaurav Khanna. Nonlinear systems: Approximating reach sets. In Rajeev Alur and GeorgeJ. Pappas, editors, *HSCC*, volume 2993 of *LNCS*, pages 600–614. Springer, 2004.

[29] Claire Tomlin, George J. Pappas, and Shankar Sastry. Conflict resolution for air traffic management. *IEEE T. Automat. Contr.*, 43(4):509–521, 1998.