Heavy use of Lie derivatives

Science of Computer Programming 193 (2020) 102441

Contents lists available at ScienceDirect

Science of Computer Programming

www.elsevier.com/locate/scico

Complete algorithms for algebraic strongest postconditions and weakest preconditions in polynomial ODEs

Michele Boreale [1]

Università di Firenze, Dipartimento di Statistica, Informatica, Applicazioni (DiSIA) "G. Parenti", Italy

ARTICLE INFO

Article history:
Received 1 August 2019
Received in revised form 5 March 2020
Accepted 6 March 2020
Available online 13 March 2020

Keywords:
Ordinary differential equations
Postconditions
Preconditions
Invariants
Gröbner bases

ABSTRACT

A system of polynomial ordinary differential equations (ODEs) is specified via a vector of multivariate polynomials, or vector field, F. A safety assertion $\psi \longrightarrow [F]\phi$ means that the trajectory of the system will lie in a subset ϕ (the postcondition) of the state-space, whenever the initial state belongs to a subset ψ (the precondition). We consider the case when ϕ and ψ are *algebraic varieties*, that is, zero sets of polynomials. In particular, polynomials specifying the postcondition can be seen as a system's conservation laws implied by ψ. Checking the validity of algebraic safety assertions is a fundamental problem in, for instance, hybrid systems. We consider a generalized version of this problem, and offer an algorithm that, given a user specified polynomial set P and an algebraic precondition ψ, finds the largest subset of polynomials in P implied by ψ (relativized strongest postcondition). Under certain assumptions on ϕ, this algorithm can also be used to find the largest algebraic invariant included in ϕ and the weakest algebraic precondition for ϕ. Applications to continuous semialgebraic systems are also considered. The effectiveness of the proposed algorithm is demonstrated on several case studies from the literature.

1. Introduction

In recent years, there has been a renewed interest in computational models based on ordinary differential equations (ODEs), in such diverse fields as System Biology [2] and stochastic systems [40]. In particular, starting from [33], the field of hybrid systems has witnessed the emergence of a novel class of formal methods based on concepts from Algebraic Geometry – see e.g. [39,34,15] and references therein.

A system of ODEs can be seen as specifying the evolution over time, or *trajectory*, of certain variables of interest $x_1, \ldots, x_N$, describing for instance physical quantities. A fundamental problem in many fields is being able to prove or to disprove assertions of the following type. For each initial state in a given set $\psi \subseteq \mathbb{R}^N$ (the precondition), the resulting system's trajectory will lie in a given set $\phi \subseteq \mathbb{R}^N$ (the postcondition). This is a *safety assertion* that, using a notation akin to Platzer's Dynamic Logic, we can write as $\boxed{\psi \longrightarrow [F]\phi}$ where F is the vector field specifying the system. Evidently, safety assertions can be considered as a continuous counterpart of Hoare's triples in imperative programs — see [27].

Here we are primarily interested in the case where both ψ and ϕ are algebraic varieties, that is they are specified as zeros of (multivariate) polynomial sets, and the drifts f_i in $F = (f_1, \ldots, f_N)$ are polynomials themselves. Although (sets of) trajectories can rarely be represented *exactly* as algebraic varieties, these provide overapproximations that may be useful

E-mail address: michele.boreale@unifi.it.

[1] Università di Firenze, Dipartimento di Statistica, Informatica, Applicazioni (DiSIA) "G. Parenti", Viale Morgagni 65, I-50134 Firenze, Italy.

https://doi.org/10.1016/j.scico.2020.102441
0167-6423/© 2020 Elsevier B.V. All rights reserved.

in practice. In a valid safety assertion, the polynomials specifying the postcondition ϕ can be seen as system's *conservation laws* (for instance energy or mass conservation[2]) that are implied by the precondition ψ. Driven by the analogy with Hoare's triples, we find it natural to generalize the problem of checking the assertion $\psi \longrightarrow [F]\phi$ in two distinct ways. (1) Strongest postcondition: given a precondition ψ, find the smallest ϕ such that the assertion is valid; (2) weakest precondition: given a postcondition ϕ, find the largest ψ such that the assertion is valid. Problem (1) amounts to characterizing I_ψ, the set of *all* polynomial~~s~~ invariants (conservation laws) implied by ψ. The difficulty of (1) motivates the introduction of a relativized version of this problem: for a user specified polynomial set P, compute $P \cap I_\psi$. We call this a relativized strongest postcondition. Depending on P, computing this can be a lot easier than computing the whole I_ψ.

We offer a complete algorithm, called POST, that computes relativized strongest postconditions. In particular, this problem will be considered in the case where the set P is specified via a polynomial template. This way, for example, one can find at once all polynomial conservation laws of the system up to a given degree. As a byproduct of the POST algorithm, we also get the weakest algebraic invariant that implies all laws in $P \cap I_\psi$. The POST algorithm is based on building ascending chains of polynomial ideals: these represent, basically, more and more refined overapproximations of the (relativized) strongest postcondition. The proof of correctness and termination relies on a few concepts from Algebraic Geometry, notably Gröbner bases [10]. We will demonstrate the effectiveness of POST reporting the outcomes of a few experiments we have conducted on nontrivial systems taken from the literature, based on a Sagemath/Python implementation. Wherever possible, we will compare our results with those obtained by other authors.

Focusing on algebraic sets, as we do, does not necessarily imply that one is limited to algebraic safety properties: in fact, by considering a family of varieties depending on a set of parameters, one can often get a good approximation of a *semialgebraic* set of interest. In our case, the parameters will basically correspond to possible initial conditions of the system. In this way, we will show that safety verification of continuous systems with semialgebraic initial and unsafe sets is possible. Formally, this will require embedding the original system into a larger space, with the introduction of auxiliary variables, and relating these new variables to the original ones using a suitable precondition.

The present paper builds on our previous work [6], which deals with simple initial values problems, where the precondition ψ always consists of a singleton. This restriction prevents one from dealing with the most interesting continuous systems, such as semialgebraic systems. In particular, the concept of weakest precondition is absent from [6]. In the concluding section, we will discuss relations with this work, as well as with recent contributions from other authors, dealing with invariant generation for polynomial ODEs in the context of continuous and hybrid systems, notably [15] and [17].

Structure of the paper The rest of the paper is organized as follows. The necessary mathematical preliminaries, including polynomial differential equations and a few facts from Algebraic Geometry, are introduced in Section 2, while Section 3 introduces algebraic safety assertions and invariants. In Section 4, the main technical results are presented: the POST algorithm and the proof of (relative) completeness. A more algorithmic presentation of POST and computational issues connected with real radicals are discussed in Section 5. A few experiments on systems drawn from the literature are described in Section 6. An application to semialgebraic systems, together with further examples, is the subject of Section 7. We round off the technical development so far with a discussion in Section 8. Related works are reviewed in Section 9. For the sake of readability, a few technical proofs and some additional technical material have been confined to four separate Appendices (A, B, C and D).

2. Preliminaries

We review a few preliminary notions about ODEs, polynomials, Lie derivatives and Algebraic Geometry.

Polynomial ODEs Let us fix an integer $N \geq 1$ and a set of N distinct variables $x_1, \ldots, x_N$. We will denote by $\mathbf{x}$ the vector $(x_1, \ldots, x_N)$. We let $\mathbb{R}[\mathbf{x}]$ denote the set of multivariate polynomials in the variables $x_1, \ldots, x_N$ with coefficients in $\mathbb{R}$, and let p, q range over it. Here we regard polynomials as syntactic objects. Given an integer $d \geq 0$, by $\mathbb{R}_d[\mathbf{x}]$ we denote the set of polynomials of degree $\leq d$. As an example, $p = 2xy^2 + (1/5)wz + yz + 1$ is a polynomial of degree $\deg(p) = 3$, that is $p \in \mathbb{R}_3[x, y, z, w]$, with monomials xy^2, wz, yz and 1. Depending on the context, with a slight abuse of notation it may be convenient to let a polynomial denote the induced function $\mathbb{R}^N \to \mathbb{R}$, defined as expected: for $v \in \mathbb{R}^N$, $p(v) \in \mathbb{R}$ denotes the value obtained by evaluating p at v. In particular, x_i can be seen as denoting the projection on the i-th coordinate.

A (polynomial) *vector field* is a vector of N polynomials, $F = (f_1, \ldots, f_N)$, seen as a function $F : \mathbb{R}^N \to \mathbb{R}^N$. Throughout the paper, all definitions and statements refer to an arbitrarily fixed polynomial vector field F over a N-vector $\mathbf{x}$. The vector field F and an initial condition $v_0 \in \mathbb{R}^N$ together define an *initial value problem* $\mathbf{\Phi} = (F, v_0)$, often written in the following form

$$\mathbf{\Phi} : \begin{cases} \dot{\mathbf{x}}(t) = F(\mathbf{x}(t)) \\ \mathbf{x}(0) = v_0 \,. \end{cases} \tag{1}$$

[2] More precisely, when the precondition is $\psi = \mathbb{R}^N$, conservation laws in our sense coincide with what are known in Physics as *first integrals of motion*, up to an additive constant.

The functions f_i in F are called *drifts* in this context. A *solution* to this problem is a differentiable function $\mathbf{x}(t) : D \to \mathbb{R}^N$, for some nonempty open interval $D \subseteq \mathbb{R}$ containing 0, which fulfills the above two equations, that is: $\frac{d}{dt}\mathbf{x}(t) = F(\mathbf{x}(t))$ for each $t \in D$ and $\mathbf{x}(0) = v_0$. By the Picard-Lindelöf theorem [1], there exists a nonempty open interval D containing 0, over which there is a *unique* solution, say $\mathbf{x}(t) = (x_1(t), ..., x_N(t))$, to the problem. In our case, as F is infinitely differentiable, the solution is seen to be *analytic* in D: each $x_i(t)$ admits a Taylor series expansion in a neighborhood of 0. For definiteness, we will take the domain of definition D of $\mathbf{x}(t)$ to be the largest open interval where the Taylor expansion from 0 of each of the $x_i(t)$ converges (possibly $D = \mathbb{R}$). The resulting vector function of t, denoted $\mathbf{x}(t)$, is called the *time trajectory* of the system. Note that both the time trajectory and its domain of definition do depend in general on the initial v_0. We shall write them as $\mathbf{x}(t; v_0)$ and D_{v_0}, respectively, whenever we want to make this dependence explicit in the notation.

For any polynomial $p \in \mathbb{R}[\mathbf{x}]$, the function $p(\mathbf{x}(t)) : D \to \mathbb{R}$, obtained by composing p as a function with the time trajectory $\mathbf{x}(t)$, is analytic: we let $p(t)$ denote the extension of this function over the largest open interval of convergence (possibly coinciding with $\mathbb{R}$) of its Taylor expansion from 0. We will call $p(t)$ the *polynomial behavior induced by p and by* the initial value problem (1). Again, fixing $N, \mathbf{x}$ and F once and for all, we shall write $p(t; v_0)$ when we want to emphasize the dependence of this function on the initial value v_0.

Lie derivatives Given a differentiable function $g : E \to \mathbb{R}$, for some open set $E \subseteq \mathbb{R}^N$, the *Lie derivative of g along F* is the function $E \to \mathbb{R}$ defined as: $\mathcal{L}_F(g) \stackrel{\triangle}{=} \langle \nabla g, F \rangle = \sum_{i=1}^{N}(\frac{\partial g}{\partial x_i} \cdot f_i)$. The Lie derivative of the sum $h+g$ and product $h \cdot g$ functions obey the familiar rules

it's a derivation

$$\mathcal{L}_F(h+g) = \mathcal{L}_F(h) + \mathcal{L}_F(g) \tag{2}$$

$$\mathcal{L}_F(h \cdot g) = h \cdot \mathcal{L}_F(g) + \mathcal{L}_F(h) \cdot g. \tag{3}$$

in fact L_F is the unique derivation s.t. $L_F(x_i) = f_i$

Note that $\mathcal{L}_F(x_i) = f_i$. Moreover if $p \in \mathbb{R}_d[\mathbf{x}]$ then $\mathcal{L}_F(p) \in \mathbb{R}_{d+d'}[\mathbf{x}]$, for some integer $d' \geq 0$ that depends on d and on F. This allows us to view the Lie derivative of polynomials along a polynomial field F as a purely syntactic mechanism, that is as a function $\mathcal{L}_F : \mathbb{R}[\mathbf{x}] \to \mathbb{R}[\mathbf{x}]$ that does not assume anything about the solution of (1). Informally, we can view p as a program, and taking the Lie derivative of p can be interpreted as unfolding the definition of each variable x_i, according to the equations in (1) and to the formal rules for product and sum differentiation, (2) and (3). More generally, we can define inductively $\mathcal{L}_F^{(0)}(p) \stackrel{\triangle}{=} p$ and $\mathcal{L}_F^{(j+1)}(p) \stackrel{\triangle}{=} \mathcal{L}_F(\mathcal{L}_F^{j}(p))$.

Example 1. The following system, borrowed from [17], will be used as a running example. Consider $N = 2$, $\mathbf{x} = (x, y)$ and the vector field $F = (y^2, xy)$. Let $p = x - y$. Examples of Lie derivatives are $\mathcal{L}_F(p) = y^2 - xy$ and $\mathcal{L}_F^{(2)}(p) = 2xy^2 - x^2y - y^3$.

In what follows, for any $v_0 \in \mathbb{R}^N$ we let $p(v_0)$ denote the real number obtained by evaluating p at v_0; recall that $p(t; v_0)$ denotes the function $p(\mathbf{x}(t; v_0))$, defined for t in a suitable neighborhood of the origin. We shall often abbreviate the syntactic Lie derivative $\mathcal{L}_F^{(j)}(p)$ as $p^{(j)}$, and shall omit the subscript $_F$ from $\mathcal{L}_F$ when clear from the context. The connection between Lie derivatives of p along F and the initial value problem (1) is given by the equations below, which can be readily checked.

$$p(t; v_0)_{|t=0} = p(v_0) \tag{4}$$
$$\frac{d}{dt}p(t; v_0) = \left(p^{(1)}\right)(t; v_0)\,.$$

More generally, we have the following equation for the j-th derivative of $p(t; v_0)$ $(j = 0, 1, ...)$:

$$\frac{d^j}{dt^j}p(t; v_0) = \left(p^{(j)}\right)(t; v_0)\,. \tag{5}$$

Algebraic geometry preliminaries We quickly review a few notions from Algebraic Geometry that will be used throughout the paper. A comprehensive treatment of these concepts can be found for instance in Cox et al.'s excellent textbook [10]. A set of polynomials $I \subseteq \mathbb{R}[\mathbf{x}]$ is an *ideal* if: (1) $0 \in I$ and (2) $p_1, ..., p_m \in I$ and $h_1, ..., h_m \in \mathbb{R}[\mathbf{x}]$ implies $\sum_{i=1}^{m} h_i p_i \in I$. The ideal generated by a set $P \subseteq \mathbb{R}[\mathbf{x}]$ is defined as

$$\langle\, P \,\rangle \stackrel{\triangle}{=} \left\{ \sum_{i=1}^{m} h_i p_i \;:\; m \geq 0 \text{ and } h_i \in \mathbb{R}[\mathbf{x}],\; p_i \in P \text{ for } i = 1, ..., m \right\}.$$

This is the smallest ideal containing P and as a consequence $\langle\, \langle\, P \,\rangle \,\rangle = \langle\, P \,\rangle$. Given an ideal I, a set P such that $I = \langle\, P \,\rangle$ is said to be a set of *generators* for I. Hilbert's basis theorem implies that: (a) any ideal $I \subseteq \mathbb{R}[\mathbf{x}]$ has a finite set of generators; (b) any infinite ascending chain of ideals $I_0 \subseteq I_1 \subseteq \cdots$ stabilizes in a finite number of steps (*ascending chain condition*). Once a total *monomial order* (e.g. lexicographic; see also Appendix B) is fixed, a multivariate version of polynomial division naturally arises — see [10] for the precise definition. A *Gröbner basis* of an ideal I (w.r.t. a fixed monomial order) is a finite set of generators G of I such that for any polynomial $p \in \mathbb{R}[\mathbf{x}]$ the *remainder* of the division of p by G, $r = p \bmod G$, enjoys following property: $p \in I$ iff $r = 0$. An alternative definition is that the leading monomial (greatest in the monomial order) of each $p \in I$ is divisible by the leading monomial of some $g \in G$. Given a Gröbner basis G of I, the *ideal membership* problem $p \in I$ can be decided[3] by just checking if $p \bmod G = 0$. Ideal inclusion $I \subseteq J$ can be decided similarly. There are algorithms that, given a finite P and a monomial order, compute a Gröbner basis G such that $\langle G \rangle = \langle P \rangle$: e.g. Buchberger's [9] and Faugeres' F4 and F5 algorithms [13,14]. The worst-case time complexity of these algorithms is exponential in the number of variables, so this computation is potentially expensive.

The geometric counterpart of polynomial sets are algebraic varieties. Given a set of polynomials $P \subseteq \mathbb{R}[\mathbf{x}]$, the set of points in $\mathbb{R}^N$ which are roots of all polynomials in P

$$\mathbf{V}(P) \stackrel{\triangle}{=} \{v \in \mathbb{R}^N : p(v) = 0 \text{ for each } p \in P\}$$

is the *algebraic*[4] *variety* represented by P. Ideals and algebraic varieties are connected as follows. For any set $A \subseteq \mathbb{R}^N$, the set of polynomials that vanish on A

$$\mathbf{I}(A) \stackrel{\triangle}{=} \{p \in \mathbb{R}[\mathbf{x}] \,:\, p(v) = 0 \text{ for each } v \in A\}$$

is the ideal induced by A. Note that both $\mathbf{V}$ and $\mathbf{I}$ are inclusion reversing: $P \subseteq Q$ implies $\mathbf{V}(P) \supseteq \mathbf{V}(Q)$, and $A \subseteq B$ implies $\mathbf{I}(A) \supseteq \mathbf{I}(B)$. For A an algebraic variety and J an ideal, it is easy to see that $\mathbf{V}(\mathbf{I}(A)) = A$ and that $\mathbf{I}(\mathbf{V}(J)) \supseteq J$; if the equality $\mathbf{I}(\mathbf{V}(J)) = J$ holds, J is said to be a *real radical*. We will have in general more than one ideal J representing A, that is such that $\mathbf{V}(J) = A$.

3. Algebraic safety assertions and invariants

We will be interested in *safety assertions* of the following type, where $\psi, \phi \subseteq \mathbb{R}^N$ are user specified algebraic varieties, which we call the *pre* and *postcondition*, respectively. Each of them is specified by a set of polynomials, that is, we will have $\phi = \mathbf{V}(P_1)$ and $\psi = \mathbf{V}(P_2)$ for some $P_1, P_1 \subseteq \mathbb{R}[\mathbf{x}]$.

$$\text{Whenever } v_0 \in \psi \text{ then for each } t \in D_{v_0}, \mathbf{x}(t; v_0) \in \phi. \tag{6}$$

The above assertion means that every trajectory starting in the precondition ψ will stay in the postcondition ϕ; hence necessarily $\psi \subseteq \phi$ for the assertion to hold. Using a notation akin to Platzer's Dynamic Logic's [27], the safety assertion (6) will be abbreviated as

$$\psi \longrightarrow [F]\,\phi\,. \tag{7}$$

A common technique for proving (7) is finding an algebraic variety χ such that $\psi \subseteq \chi \subseteq \phi$ and χ is an *algebraic invariant* for the vector field F, that is it satisfies $\chi \longrightarrow [F]\,\chi$. The invariance condition means that all trajectories starting in χ must remain in χ.

Let us now introduce two distinct generalizations of the problem of checking the safety assertion (7). These are the problems we will actually try to solve. In what follows, "finding" an algebraic variety means building a finite set of polynomials representing it. Also note that, for varieties, "smallest" means "strongest", and "largest" means "weakest".

Problem 1 *(strongest postcondition). Given an algebraic variety ψ, find ϕ_ψ, the smallest algebraic variety ϕ_ψ such that (7) is true when $\phi = \phi_\psi$.*

Note that ϕ_ψ always exists and is the intersection of all the varieties ϕ such that $\psi \longrightarrow [F]\phi$. Finding ϕ_ψ amounts to building (a basis of) an appropriate ideal I such that $\mathbf{V}(I) = \phi_\psi$. One such ideal is

$$I_\psi \stackrel{\triangle}{=} \mathbf{I}(\phi_\psi)\,. \tag{8}$$

Currently, we do not know how to compute I_ψ, or any other polynomial representation of ψ. This motivates the introduction of a relaxed, or relativized, version of the previous problem. In this version, a user specified set of polynomials P is used to tune the strength, hence precision, of the postcondition.

Problem 2 *(strongest postcondition, relativized). Given a polynomial set $P \subseteq \mathbb{R}[\mathbf{x}]$ and an algebraic variety ψ, find a finite representation of $P \cap I_\psi$.*

[3] Provided the involved coefficients can be finitely represented, for instance are rational.

[4] Some authors use *affine*.

Of course, we have that $\mathbf{V}(P \cap I_\psi) \supseteq \mathbf{V}(I_\psi) = \phi_\psi$, which implies that $\psi \longrightarrow [F]\mathbf{V}(P \cap I_\psi)$. In other words, $P \cap I_\psi$ represents an overapproximation of the strongest postcondition. There is another meaningful way of generalizing the problem of checking (7).

Problem 3 *(weakest precondition). Given an algebraic variety ϕ, find ψ_ϕ, the largest algebraic variety such that (7) is true when $\psi = \psi_\phi$.*

Union of all $\psi : \psi \to [F]\phi$

Let us now comment briefly on the relations existing between the above introduced problems. It is not difficult to see that being able to solve either of Problem 1 or Problem 3 implies one is able to check (7) for *given ψ and ϕ*, based on the fact that one knows how to check inclusion between two varieties (see Section 2). Indeed, wanting to check the assertion $\psi \longrightarrow [F]\,\phi$, one may either check that $\phi \supseteq \phi_\psi$ or that $\psi \subseteq \psi_\phi$. The relativized Problem 2 too is more general than checking (7). Indeed, wanting to check $\psi \longrightarrow [F]\,\phi$, one may let $P = Q$ in Problem 2 and then check if P is included in the computed $P \cap I_\psi$, that is if $P \subseteq I_\psi$.

Example 2. Let us reconsider the vector field F of Example 1. The variety $\psi = \mathbf{V}(\{p\}) = \mathbf{V}(\{x - y\})$ is the line $x = y$. Consider $\phi = \mathbf{V}(\{q\})$ where $q = x^2 - xy$. Let P be the set of all polynomials of degree ≤ 2. We can consider the following problems. (a) Decide whether $\psi \longrightarrow [F]\phi$; (b) find a finite representation of $P \cap I_\psi$, that is all the conservation laws of degree at ≤ 2 that are satisfied, for each initial state in the line $x = y$ (relativized strongest postcondition); (c) find a finite representation of the largest algebraic variety ψ_ϕ such that $\psi_\phi \longrightarrow [F]\,\phi$ (weakest precondition). Note that solving (b) also yields a solution of (a).

Concerning the weakest precondition Problem 3, we note that a simple algorithm consists in collecting all algebraic conditions ensuring that the derivatives at any order of the polynomials specifying ϕ vanish. Specifically, assuming $\phi = \mathbf{V}(P)$ for a user defined, finite set $P \subseteq \mathbb{R}[\mathbf{x}]$, one considers the chain of sets $P_0 \stackrel{\triangle}{=} P$, $P_{j+1} = P_j \cup \mathcal{L}_F(P_j) = P_j \cup \{\mathcal{L}_F(p) : p \in P_j\}$, until the least m such that $\langle\, P_{m+1} \,\rangle = \langle\, P_m \,\rangle$, where the last equality can be checked via Gröbner bases computation. Then one has $\psi_\phi = \mathbf{V}(P_m)$. Termination and correctness of this algorithm can be easily derived from the results presented, for example, in [21,15] (see also [24]). Novikov&Yakovenko For the sake of completeness, we report a proof in Appendix A. In our experience, though, this simple algorithm tends to scale badly as the number of variables grows, so alternatives are worthwhile to consider.

In the following sections, we shall focus on Problem 2. In particular, we shall give a method, called POST, that works quite well in the case when the polynomial set P is specified by a polynomial template. Moreover, as a byproduct of this method, we will also get the weakest algebraic precondition for (and largest algebraic invariant included in) $\mathbf{V}(P \cap I_\psi)$, which can be used to address Problem 3 as well. Finally, POST will also give us a handle on the more general and difficult Problem 1.

4. The POST algorithm

Recall from (8) that I_ψ is the ideal that induces the strongest algebraic postcondition of the system at hand, for a user specified variety (precondition) ψ. Our goal is to give a method to effectively compute $P \cap I_\psi$, for a polynomial set P which is itself user-specified. Following a well-established tradition in the field of continuous and hybrid systems, we shall consider the case when the user specifies P via a polynomial *template*, which we review in the next paragraph.

Polynomial templates Fix a tuple of $n \geq 1$ of distinct *template parameters*, say $\mathbf{a} = (a_1, \ldots, a_n)$, disjoint from $\mathbf{x}$. Let $\mathbb{L}(\mathbf{a})$, ranged over by ℓ, be the set of *linear expressions* with coefficients in $\mathbb{R}$ and variables in $\mathbf{a}$; e.g. $\ell = 5a_1 + 42a_2 - 3a_3$ is one such expression.[5] A *template* [33] is a polynomial π in $\mathbb{L}(\mathbf{a})[\mathbf{x}]$, that is, a polynomial with linear expressions as coefficients. For example, the following is a template: $\pi = (5a_1 + (3/4)a_3)xy^2 + (7a_1 + (1/5)a_2)xz + (a_2 + 42a_3)$. Note that $\mathbb{L}(\mathbf{a})[\mathbf{x}] \subseteq \mathbb{R}[\mathbf{a}, \mathbf{x}]$, so, whenever convenient, we can consider a template as a polynomial in this larger ring. A *template parameters valuation* is a vector

$$\lambda = (\mu_1, \ldots, \mu_n) \in \mathbb{R}^n \,.$$

Given such a λ, we will let $\ell[\lambda] \in \mathbb{R}$ denote the result of replacing each template parameter a_i with μ_i, and evaluating the resulting expression; we will let $\pi[\lambda] \in \mathbb{R}[\mathbf{x}]$ denote the polynomial obtained by replacing each ℓ with $\ell[\lambda]$ in π. Given a set $S \subseteq \mathbb{R}^n$, we let $\pi[S]$ denote the set $\{\pi[\lambda] : \lambda \in S\} \subseteq \mathbb{R}[\mathbf{x}]$. The (formal) Lie derivative of π is defined as expected, once linear expressions are treated as constants; note that $\mathcal{L}(\pi)$ is still a template. It is easy to see that the following property is true, as a consequence of the fact that $a_1, \ldots, a_n$ are treated as symbolic constants during differentiation: for each π and λ, one has $\mathcal{L}(\pi[\lambda]) = \mathcal{L}(\pi)[\lambda]$. This property extends as expected to the j-th Lie derivative ($j \geq 0$):

$$\mathcal{L}^{(j)}(\pi[\lambda]) = \mathcal{L}^{(j)}(\pi)[\lambda] \,. \tag{9}$$

[5] Note that linear expressions with a constant term, such as $2 + 5a_1 + 42a_2 - 3a_3$ are not allowed.

The algorithm Given a user specified algebraic variety ψ (the precondition) and a polynomial template π, describing $P = \pi[\mathbb{R}^n]$, our objective is to compute the relativized strongest postcondition $P \cap I_\psi$; recall that I_ψ represents the strongest algebraic postcondition. The following one is an important concept.

Definition 1 *(polynomial invariant).* Let us call $p \in \mathbb{R}[\mathbf{x}]$ a *polynomial invariant for* F *and* v_0 if the function $p(t; v_0)$ is identically 0.

A polynomial invariant expresses a law which is satisfied by the solution of the initial value problem (F, v_0), that is a conservation law. We will rely on the following two lemmas. The first one is just a reformulation of the definition of $I_\psi = \mathbf{I}(\phi_\psi)$. The easy proof of the second lemma is reported in Appendix B.

Lemma 1. *$I_\psi = \{p : p$ is a polynomial invariant for F and each $v_0 \in \psi\}$.*

Lemma 2. *Let $p \in \mathbb{R}[\mathbf{x}]$. Then p is a polynomial invariant for F and v_0 if and only if for each $j \geq 0$, $p^{(j)}(v_0) = 0$.*

The above two lemmas suggest the following strategy to compute the set $\pi[\mathbb{R}^n] \cap I_\psi$. We should identify those template parameter valuations $\lambda \in \mathbb{R}^n$, such that $\pi[\lambda]$ is a polynomial invariant for each $v_0 \in \psi$ (Lemma 1). That is, those λ's such that for each $j \geq 0$ and for each $v_0 \in \psi$, $\pi^{(j)}[\lambda](v_0) = 0$ (Lemma 2). Or, equivalently, $\pi^{(j)}[\lambda] \in \mathbf{I}(\psi)$ for each $j \geq 0$. For each $j \geq 0$, the last condition imposes certain constraints on λ, that is on the parameters of the template $\pi^{(j)}$. In order to make these constraints explicit, we shall rely on the following key lemma. In the sequel we shall assume, over the polynomial ring $\mathbb{R}[\mathbf{a}, \mathbf{x}]$, a lexicographic monomial order[6] such that $a_i > x_j$ for each i, j. A proof of the lemma is reported in Appendix B.

Lemma 3. *Let $G \subseteq \mathbb{R}[\mathbf{x}]$ be a Gröbner basis. Let π be a polynomial template and $r = \pi \bmod G$. Then r is linear in the template parameters $a_1, \ldots, a_n$. Moreover, for each $\lambda \in \mathbb{R}^n$, $\pi[\lambda] \bmod G = r[\lambda]$.*

Fix a Gröbner basis G of $\mathbf{I}(\psi)$. By the above lemma, for a fixed j, $\pi^{(j)}[\lambda] \in \mathbf{I}(\psi)$ exactly when $r_j[\lambda] = 0$, where $r_j = \pi^{(j)} \bmod G$. By seeing r_j as a polynomial in $\mathbb{L}(\mathbf{a})[\mathbf{x}]$, the condition on λ

$$r_j[\lambda] = 0 \tag{10}$$

can be represented as a set of *linear* constraints on the template parameters $\mathbf{a}$: indeed, a polynomial is zero exactly when all of its coefficients — in the present case, linear expressions in $\mathbf{a}$ — are zero.[7] This discussion leads to the method described below. We first give a purely mathematical description of the method, deferring the discussion of its computational aspects to Section 5.

The method can be seen as a generalization of the double chain algorithm of [6] to algebraic safety assertions; see the concluding section for a discussion on the differences between the two algorithms. The basic idea here is gradually refining the space of template parameter valuations, seen as a subset of $\mathbb{R}^n$. More precisely, the algorithm builds two chains of sets: a descending chain of vector spaces V_i, representing spaces of template parameter valuations for which all the derivatives of π up to order i vanish on the points in ψ; and an (eventually) ascending chain of ideals J_i, induced by the polynomials obtained from those parameter valuations. This ideal chain is used in the algorithm to detect the stabilization of the sequence, as discussed below. In order to state the correctness of the result in the most general form, let us fix an arbitrary ideal $I_0 \subseteq \mathbf{I}(\psi)$ and a Gröbner basis G of I_0. Note that by admitting a I_0 smaller than $\mathbf{I}(\psi)$ we actually allow for a weakening of the precondition. For each $j \geq 0$, let $r_j \stackrel{\triangle}{=} \pi^{(j)} \bmod G$. For each $i \geq 0$, consider the sets

$$V_i \stackrel{\triangle}{=} \{\lambda \in \mathbb{R}^n : r_j[\lambda] \text{ is the 0 polynomial, for } j = 0, \ldots, i\} \tag{11}$$

$$J_i \stackrel{\triangle}{=} \left\langle \bigcup_{j=0}^{i} \pi^{(j)}[V_i] \right\rangle . \tag{12}$$

It is easy to check that each $V_i \subseteq \mathbb{R}^n$ is a vector space over $\mathbb{R}$ of dimension $\leq n$: this stems from the linearity in $\mathbf{a}$ of the r_j terms. Now let $m \geq 0$ be the least integer such that the following conditions are *both* true:

$$V_{m+1} = V_m \tag{13}$$

$$J_{m+1} = J_m . \tag{14}$$

[6] This guarantees that, for any finite set $G \subseteq \mathbb{R}[\mathbf{x}]$, G is a Gröbner basis in $\mathbb{R}[\mathbf{a}, \mathbf{x}]$ if and only if it is in $\mathbb{R}[\mathbf{x}]$; see [10, Ch.3,§1,Th.2]. Any *elimination* ordering for the template parameters a_i could as well be considered.

[7] For instance, if $\pi = (a_1 + a_2)x_1 + a_3x_2$ then $\pi[\lambda] = 0$ corresponds to the constraints $a_1 = -a_2$ and $a_3 = 0$.

The algorithm returns (V_m, J_m), written $\textsc{post}_F(\psi,\pi) = (V_m, J_m)$; we shall omit the subscript $_F$ when the vector field F is clear from the context. Note that the integer m is well defined: indeed, $V_0 \supseteq V_1 \supseteq \cdots$ forms an infinite descending chain of finite-dimensional vector spaces, which must stabilize in finitely many steps. In other words, we can consider the least m' such that $V_{m'} = V_{m'+k}$ for each $k \geq 1$. Then $J_{m'} \subseteq J_{m'+1} \subseteq \cdots$ forms an infinite ascending chain of ideals, which must stabilize at some $m \geq m'$. Therefore there must be some index m such that (13) and (14) are both satisfied, and we choose the least such m.

Results We start with an important concept, which is needed to state and prove the correctness and completeness of $\textsc{post}$.

Definition 2 *(invariant ideal).* A set of polynomials $J \subseteq \mathbb{R}[\mathbf{x}]$ is an *invariant ideal* for the vector field F if it is an ideal and $\mathcal{L}_F(J) \stackrel{\triangle}{=} \{\mathcal{L}_F(p) : p \in J\} \subseteq J$.

The next theorem states the correctness and relative completeness of $\textsc{post}$. Informally, the algorithm outputs a space V such that $\pi[V] \subseteq I_\psi$, which is the largest such space if $I_0 = \mathbf{I}(\psi)$, and the smallest invariant ideal J including $\pi[V]$. This invariant ideal also conveys important information about the system, as discussed later on in the section. In order to prove the main theorem, we need a technical lemma, whose proof is reported in the Appendix B.

Lemma 4. *Let V_m, J_m be the sets returned by the $\textsc{post}$ algorithm. Then for each $j \geq 1$, one has $V_m = V_{m+j}$ and $J_m = J_{m+j}$.*

Theorem 1 *(correctness and relative completeness of $\textsc{post}_F$). Let ψ be an algebraic variety, let $I_0 \subseteq I_\psi$ be an ideal and G be a Gröbner basis of I_0. For any polynomial template π, let $\textsc{post}_F(\psi,\pi) = (V, J)$. Then*

(a) *$\pi[V] \subseteq \pi[\mathbb{R}^n] \cap I_\psi$. In particular, $\pi[V] = \pi[\mathbb{R}^n] \cap I_\psi$ if $I_0 = \mathbf{I}(\psi)$;*
(b) *J is the smallest invariant ideal such that $J \supseteq \pi[V]$. Moreover, $J \subseteq I_\psi$.*

Proof. Let $(V, J) = (V_m, J_m)$ for some $m \geq 0$. Concerning part (a), we first note that, by virtue of Lemma 1 and Lemma 2, $\pi[\lambda] \in \pi[\mathbb{R}^n] \cap I_\psi$ if and only if for each $j \geq 0$, $(\pi[\lambda])^{(j)} = \pi^{(j)}[\lambda] \in \mathbf{I}(\psi)$ (here we have used property (9)). If $\lambda \in V_m = V_{m+1} = V_{m+2} = \cdots$ (here we are using Lemma 4), then by definition, for each $j \geq 0$, $r_j[\lambda] = (\pi^{(j)})[\lambda] \bmod G = (\pi[\lambda])^{(j)} \bmod G = 0$ (here we have used again property (9) and Lemma 3). That is, for each $j \geq 0$, $(\pi[\lambda])^{(j)} \in I_0 \subseteq \mathbf{I}(\psi)$. This implies (again by Lemmas 1 and 2) that $\pi[\lambda] \in I_\psi$. Assume now that $I_0 = \mathbf{I}(\psi)$ and let λ such that $\pi[\lambda] \in \pi[\mathbb{R}^n] \cap I_\psi$, that is if for each $j \geq 0$, $(\pi[\lambda])^{(j)} = \pi^{(j)}[\lambda] \in \mathbf{I}(\psi)$. That is, being G a Gröbner basis of $\mathbf{I}(\psi)$, $\pi^{(j)}[\lambda] \bmod G = r_j[\lambda] = 0$ (the first equality here follows from Lemma 3), for each $j \geq 0$. This assertion, by definition, means that $\lambda \in V_j$ for each $j \geq 0$, hence in particular $\lambda \in V_m$.

Concerning part (b), to prove that J_m is the smallest invariant ideal including $\pi[V_m]$, it is enough to prove the following: (1) J_m is an invariant ideal, (2) $J_m \supseteq \pi[\mathbb{R}^n] \cap I_\psi$, and (3) for any invariant ideal I such that $\pi[\mathbb{R}^n] \cap I_\psi \subseteq I$, we have that $J_m \subseteq I$. We first prove (1), that J_m is an invariant ideal. Indeed, for each $\lambda \in V_m$ and each $j = 0, \ldots, m-1$, we have $\mathcal{L}(\pi^{(j)}[\lambda]) = \pi^{(j+1)}[\lambda] \in J_m$ by definition, while for $j = m$, since $\lambda \in V_m = V_{m+1}$, we have $\mathcal{L}(\pi^{(m)}[\lambda]) = \pi^{(m+1)}[\lambda] \in J_{m+1} = J_m$ (note that in both cases we have used property (9)). Concerning (2), note that $J_m \supseteq \pi[V_m] = \pi[\mathbb{R}^n] \cap I_\psi$, by virtue of part (a). Concerning (3), consider any invariant ideal $I \supseteq \pi[\mathbb{R}^n] \cap I_\psi$. We show by induction on $j = 0, 1, \ldots$ that for each $\lambda \in V_m$, $\pi^{(j)}[\lambda] \in I$; this will imply the wanted statement. Indeed, $\pi^{(0)}[V] = \pi[V] \in I_\psi \cap \pi[\mathbb{R}^n]$, as $\pi[V_m] \subseteq I_\psi$ by (a). Assuming now that $\pi^{(j)}[\lambda] \in I$, by invariance of I we have $\pi^{(j+1)}[\lambda] = \mathcal{L}(\pi^{(j)}[\lambda]) \in I$ (again, we have used here property (9)).

Finally, $J_m \subseteq I_\psi$ follows from the last statement and from the fact that I_ψ, as clearly seen from Lemmas 1 and 2, is an invariant ideal. □

Example 3. We reconsider the vector field F of Example 1. Let us consider $\psi = \mathbf{V}(\{x - y\})$. A Gröbner basis of $\mathbf{I}(\psi)$ is just $G = \{x - y\}$. We let π be the complete template of degree 2 (described below). Running $\textsc{post}_F(\psi,\pi)$ means building the chain of sets V_i, J_i, for $i = 0, 1, \ldots$. Below, $\lambda = (\mu_1, \ldots, \mu_6) \in \mathbb{R}^6$ denotes a generic template parameters valuation, while $e_j \in \mathbb{R}^n$ denotes the j-th basis vector in $\mathbb{R}^n$, for $j = 1, \ldots, 6$. With the help of the computer algebra system (e.g. SageMath [32]), we consider the successive Lie derivatives of π and their remainders mod G, as follows:

- $\pi = a_6xy + a_5y^2 + a_4x^2 + a_3y + a_2x + a_1$ and $r_0 = \pi \bmod G = (a_4 + a_5 + a_6)y^2 + (a_2 + a_3)y + a_1$. Thus $V_0 = \{\lambda \in \mathbb{R}^6 : \mu_4 + \mu_5 + \mu_6 = 0,\ \mu_2 + \mu_3 = 0,\ \mu_1 = 0\}$. A parametric representation of the elements of V_0 is $(0, -\mu_3, \mu_3, -\mu_5 - \mu_6, \mu_5, \mu_6)$, from which a basis is obtained as $B_0 = \{-e_2 + e_3, -e_4 + e_5, -e_4 + e_6\}$. We let $J_0 = \langle\, \pi[V_0]\, \rangle = \langle\, \pi[B_0]\, \rangle$;
- $\pi^{(1)} = a_6x^2y + 2(a_4 + a_5)xy^2 + a_6y^3 + a_3xy + a_2y^2$ and $r_1 = \pi^{(1)} \bmod G = 2(a_4 + a_5 + a_6)y^3 + (a_2 + a_3)y^2$: the last equation can be checked directly by equating x and y, which is what $\pi^{(1)} \bmod \{x - y\}$ means. We see that $r_1 = 0$ does not induce new constraints on the template parameters, that is $V_1 = V_0$. Next, we compute a basis for $\pi^{(1)}[V_1] = \pi^{(1)}[V_0]$ as $\pi^{(1)}[B_0] = \{xy - y^2, 0, x^2y - 2xy^2 + y^3\}$; we can check (again, equating x and y) that the last set is $\subseteq J_0$, which implies $\pi^{(1)}[V_1] \subseteq J_0$. This in turn implies $J_1 = \langle\, \pi[V_1] \cup \pi^{(1)}[V_1]\, \rangle = J_0$: therefore also the ideal chain has stabilized.

Therefore both chains stabilize already at $m = 0$ and $\textsc{post}(\psi, \pi) = (V_0, J_0)$. A Gröbner basis of J_0 is $G_0 = G$.

Remark 1 *(result template).* Given a template π and $\lambda \in \mathbb{R}^n$, checking if $\pi[\lambda] \in \pi[V]$ is equivalent to checking if $\lambda \in V$: this can be effectively done knowing a basis B of the vector space V (see Section 5). In practice, it is computationally more convenient to represent the whole set $\pi[V]$ returned by $\textsc{post}$ compactly in terms of a *new* n'-parameters ($n' \leq n$) result template π' such that $\pi'[\mathbb{R}^{n'}] = \pi[V]$. For instance, in the previous example, the result template $\pi' = a_1(y^2 - x^2) + a_2(xy - x^2) + a_3(y - x)$ represents $\pi[V_0]$, in the precise sense that $\pi[V_0] = \pi'[\mathbb{R}^3]$. The result template π' can in fact be built directly from π, by propagating the linear constraints on $\mathbf{a}$ (10) as they are generated. This will be explicitly described when discussing the algorithmic presentation in Section 5.

Note that, while typically the user will be interested in $\pi[V]$, the ideal J as well may contain useful information, such as higher order, nonlinear conservation laws. The theorem below is about the meaning of J as an invariant and as a precondition. The theorem relies on Theorem 1 and on the following lemma, stating that invariant ideals, on the polynomial side, precisely correspond to algebraic invariants. The proofs of both the lemma and the theorem are reported in the Appendix B.

Lemma 5. *Consider a set $\chi \subseteq \mathbb{R}^N$. Then χ is an algebraic invariant for the vector field F if and only if there is an invariant ideal J for F such that $\chi = \mathbf{V}(J)$.*

Theorem 2 *(weakest algebraic invariant and precondition). For an algebraic variety ψ and a polynomial template π, let $\textsc{post}_F(\psi, \pi) = (V, J)$ and $\phi = \mathbf{V}(\pi[V])$. Then*

(a) *$\mathbf{V}(J)$ is the largest algebraic invariant included in ϕ; and*
(b) *$\mathbf{V}(J)$ is the weakest precondition of ϕ.*

We stress that Theorem 2(b) provides a means to solve Problem 3 (weakest precondition) via the $\textsc{post}$ algorithm. In fact, given ϕ, it suffices to consider *any* precondition ψ and template π such that $\textsc{post}(\psi, \pi) = (V, J)$ and $\mathbf{V}(\pi[V]) = \phi$: then $\mathbf{V}(J)$ is ϕ's weakest precondition. In particular, ψ may consist of a singleton. Also note that the theorem does not require the equality $I_0 = \mathbf{I}(\psi)$. An example of application of this technique is given below. Other examples will be discussed in Section 6 (see in particular the Kepler laws example).

Example 4. We reconsider the vector field F of Example 1. Let $\phi = \mathbf{V}(\{q\})$ be given, where $q = x^2 - xy$. We want to compute the weakest precondition ψ_ϕ via $\textsc{post}$. We choose the trivial precondition $\psi = \{(0,0)\} = \mathbf{V}(\{x, y\})$: both $x(t;\ (0,0))$ and $y(t;\ (0,0))$ are identically 0, making $\psi \to [F]\phi$ a valid assertion. Now choosing $\pi = a_1 \cdot q$ and running $\textsc{post}$, we obtain $\textsc{post}(\psi, \pi) = (V, J)$, where $V = \mathbb{R}$ and necessarily $\mathbf{V}(\pi[V]) = \phi$, and $J = \left\langle \{xy^2 - y^3, x^2 - xy\} \right\rangle$. By Theorem 2(b), $\psi_\phi = \mathbf{V}(J) = \mathbf{V}(\{x - y\})$.

Finally, the following result of theoretical interest, shows that the whole ideal I_ψ as well can be characterized in terms of the $\textsc{post}$ algorithm. For any $k \geq 0$, the *complete polynomial template* of degree k over a set of variables X is $\pi \stackrel{\triangle}{=} \sum_\alpha a_\alpha \alpha$, where α ranges over all monomials of degree $\leq k$ on the variables in X, and a_α ranges over distinct template parameters.

Corollary 1 *(characterization of I_ψ). Let ψ be an algebraic variety. Let $k \geq 0$, π_k be the complete template of degree k over the variables in $\mathbf{x}$ and $(V, J) = \textsc{post}(\psi, \pi_k)$. For k large enough, $J = I_\psi$.*

Proof. By Hilbert's basis theorem, there is a finite set of polynomials P such that $I_\psi = \left\langle P \right\rangle$. Therefore I_ψ is the smallest ideal containing P, and is also an invariant ideal. Now let k be the maximum degree of polynomials in P, let π_k be the complete template of degree k over all variables, and n the number of template parameters in π_k. As $P \subseteq \pi_k[\mathbb{R}^n]$ and $P \subseteq I_\psi$, we have $\pi_k[\mathbb{R}^n] \cap I_\psi \supseteq P$. Now let $(V, J) = \textsc{post}(\psi, \pi_k)$. By Theorem 1(b), $J \supseteq \pi_k[V] = \pi_k[\mathbb{R}^n] \cap I_\psi \supseteq P$, hence $J \supseteq I_\psi$. On the other hand, again by Theorem 1(b), $J \subseteq I_\psi$. Therefore $J = I_\psi$. □

We leave open the problem of computing a lower bound on the degree k that is needed to recover I_ψ. We end the section with a remark on the expressive power of algebraic varieties.

Remark 2 *(expressive power).* Algebraic varieties can in general provide only overapproximations of sets of initial states and trajectories. However, the expressive power of algebraic varieties can often be significantly enhanced by introducing auxiliary, or *ghost* variables, in the terminology of Platzer [28]. These variables are used to express properties of interest. We have found particularly interesting the case when ghost variables are used to encode *generic* initial values of the system: apparently, keeping track of such values allows for more expressive polynomial invariants. This is illustrated by the example below. We will put this technique into use in Section 6 and, in a more systematic way, in Section 7, where we shall deal with semialgebraic systems.

Algorithm 1 POST.

```
Input: $F$ a vector field, $\pi$ a $n$-parameters template, $G \subseteq \mathbf{I}(\psi)$ a Gröbner basis for $I_0$
Output: $\pi'$ a $n'$-parameters template, $J$ an invariant ideal (s.t. $\text{POST}_F(\psi, \pi) = (V, J)$ and $\pi'[\mathbb{R}^{n'}] = \pi[V]$)
$S := [\,]$
while true do
    $r := \pi$ mod $G$
    $\gamma :=$ solve$(r = 0)$
    if $\gamma = \emptyset$ then                          // Check if $V_{i+1} = V_i$; equivalently if $r = 0$
        $GS :=$ instantiate$(S)$
        $J := \langle\, GS \,\rangle$
        if instantiate$(\{\pi\}) \subseteq J$ then        // Check if $J_{i+1} = J_i$; if yes, we have stabilization
            return (first$(S)$, $J$)
    else                                                  // $V_{i+1} \neq V_i$; vector spaces chain not stabilized
        $\pi := \gamma(\pi)$                              // Propagate constraints $\gamma$
        $S := \gamma(S)$
    $S :=$ append$(S, \pi)$
    $\pi := \mathcal{L}_F(\pi)$
```

Example 5. Consider again the system of Example 1. With no constraints on the initial states, that is with $\psi = \mathbb{R}^2$, the strongest postcondition is quite easily seen to be the trivial $\phi = \mathbb{R}^2$, that is $I_\psi = \{0\}$. We build now a new system by introducing two new variables x_0, y_0, together with the corresponding equations $\dot{x}_0 = 0$ and $\dot{y}_0 = 0$: this means they represent (generic) constants — in effect, parameters. We consider the precondition $\psi = \mathbf{V}(\{x - x_0, y - y_0\})$, meaning that x_0 and y_0 represent the (generic) initial values of x and y, respectively. Using a complete template π of degree 2, we now get the nontrivial result $\text{POST}(\psi, \pi) = (V, J)$ with $J = \langle\, \{x_0^2 - y_0^2 - x^2 + y^2\} \,\rangle$ and $\pi[V] = \pi'[\mathbb{R}]$, where $\pi' = a_1(x^2 - x_0^2 - y^2 + y_0^2)$. Here J represents a valid nontrivial invariant for every instantiation of x_0, y_0.

5. Computational aspects of POST

We consider here some important computational aspects of the POST algorithm. We will first derive a more algorithmic presentation of the abstract procedure introduced in Section 4; then discuss issues related to selecting an appropriate ideal $I_0 \subseteq \mathbf{I}(\psi)$ and a Gröbner G basis for it.

5.1. Algorithmic presentation

When it comes to the effective implementation of POST, the first aspect to consider is how to finitely represent the sets V_i, J_i. Each subspace V_i is spanned by a finite basis B_i, which can in principle be computed explicitly from the linear constraints on the template parameters $a_1, \ldots, a_n$ imposed by (11). From (12) it is then easy to check that $\bigcup_{j=0}^{i} \pi^{(j)}[B_i]$ is a basis of J_i. The termination conditions $V_i = V_{i+1}$ and $J_i = J_{i+1}$ can also be checked effectively. In particular, checking $J_i = J_{i+1}$ involves computing a Gröbner basis of J_i, a potentially expensive operation, and checking if $\pi^{(i+1)}[B] \subseteq J_i$. Fortunately, this need not be done at each step, but only if actually $V_i = V_{i+1}$, the latter a relatively inexpensive check.

Rather than building the V_i's explicitly, computationally it is more convenient to represent them implicitly, via symbolic linear constraints on the template parameters $a_1, \ldots, a_n$. At each step $i \geq 0$, such constraints are generated from the condition $r_i = 0$ on the remainder (see (10)), and are represented by a substitution γ that eliminates a few template parameters. The constraints γ are propagated to all templates $\pi^{(j)}$ $(0 \leq j \leq i)$ generated so far. This discussion leads to Algorithm 1. Note that program blocks are defined by indentation. We make use of a few auxiliary variables and functions, as detailed below:

1. S is an initially empty list of polynomial templates, used to collect the successive Lie derivatives of π. The functions first$(\cdot)$ and append$(\cdot)$, defined on lists, have the usual interpretation: first(S) returns the first element of S, with the proviso that first$([\,]) \overset{\triangle}{=} 0$, the zero polynomial template, while append(S, π) returns the list obtained by appending π to S as a last element.
2. γ is a substitution, encoding linear constraints existing among the template parameters. Formally, a substitution γ is a finite partial map from $\{a_1, \ldots, a_n\}$ (template parameters) to $\mathbb{L}[\mathbf{a}]$ (linear expressions), such that no parameter in dom(γ) occurs in any $\ell \in$ range(γ). We write $\gamma(c)$ for the result of applying σ to every parameter occurring in (the expression, set,...) c.
3. solve$(r = 0)$ returns a (minimal) substitution γ such that $\gamma(r) = 0$, the zero polynomial. We insist that $|\text{dom}(\gamma)|$ be minimal, that is eliminated as few template parameters as possible. In linear algebraic terms, let $\ell_1, \ldots, \ell_K \in \mathbb{L}(\mathbf{a})$ be the distinct coefficients of r, where $\ell_i = \sum_{j=1}^{n} c_{ij} a_j$. Let C be the $K \times n$ real coefficients matrix of the c_{ij}'s. A template parameter valuation $\lambda \in \mathbb{R}^n$ makes $r[\lambda]$ the null polynomial if and only if λ^T is a solution of the linear system in the variables $\mathbf{a}$, $C\mathbf{a}^T = 0$. We insist that γ describe the whole space $U \subseteq \mathbb{R}^n$ of solutions of this system. As U has dimension $n - \text{rk}(C)$, this is equivalent to saying that $\gamma(r) = 0$ and $|\text{dom}(\gamma)| = \text{rk}(C)$.

4. instantiate$(L) \subseteq \mathbb{R}[\mathbf{x}]$, for L a list or set of templates, returns a finite generating set of the vector space spanned by $\cup_{\pi' \in L} \pi'[\mathbb{R}^n]$ in $\mathbb{R}[\mathbf{x}]$. Specifically, letting $e_j \in \mathbb{R}^n$ denote the j-th canonical basis vector ($1 \le j \le n$), seen as a parameter valuation, we have (below 0 denotes the zero polynomial):

$$\text{instantiate}(L) \stackrel{\triangle}{=} \{\pi'[e_j] : \pi' \in L,\ \ j = 1, \ldots, n\} \setminus \{0\}\,.$$

   As an example, if $n = 4$ and $\pi = (2a_2 - a_3)xy + a_3$ then instantiate$(\{\pi\}) = \{\pi[e_1], \pi[e_2], \pi[e_3], \pi[e_4]\} \setminus \{0\} = \{2xy, -xy + 1\}$.

The exact theoretical complexity of this algorithm is difficult to characterize, even assuming, as we do here, that the basis G s.t. $\langle\, G\,\rangle = I_0 \subseteq \mathbf{I}(\psi)$ has been precomputed. But one can at least work out some very conservative bounds, as follows. Let us denote by d the sum of the degree of π and of the maximal degree of polynomials in F, and by N the number of variables. We note that: (a) each step potentially involves the computation of a Gröbner basis, for which known algorithms have an exponential worst case time complexity upper bounded approximately by $O(D^{2^N})$, where D is the maximum degree in the input polynomial set (see [10]); (b) the maximum degree D of the derivatives $\pi^{(j)}$'s occurring in S, for $0 \le j \le m+1$, is bounded by $(m+1)d$. Overall, this gives a worst case time complexity of approximately $O(m^{2^N+1} d^{2^N})$. Finally, according to a result in [24], the number of steps m before stabilization of an ascending chain of ideals generated by successive Lie derivatives is upper bounded by $d^{N^{O(N^2)}}$. One should stress that these are very conservative bounds. A SageMath/Python [32] implementation strictly adhering to Algorithm 1 is available[8] that works reasonably well in a number of cases of practical interest; see Section 6. SageMath directly provides an efficient implementation in exact rational arithmetic of the most important auxiliary functions, such as linear constraints and Gröbner bases generation.

Novikov &
Yakovenko

5.2. *The choice of I_0 and the real radical problem*

A crucial aspect in the POST algorithm is the choice of the ideal $I_0 \subseteq \mathbf{I}(\psi)$ and the computation of a Gröbner basis G for it. In the following discussion, we fix the following notation and terminology:

- $\psi = \mathbf{V}(Q)$, the variety generated by a finite (user specified) set $Q \subseteq \mathbb{R}[\mathbf{x}]$;
- $I = \langle\, Q\,\rangle$, the ideal generated by Q;
- $\mathbf{I}(\psi) = \{p : p(v) = 0 \text{ for each } v \in \psi\} \supseteq I$, the *real radical* of I.

In the statement of Theorem 1(a), equality, hence completeness, is guaranteed if $I_0 = \mathbf{I}(\psi)$ is the real radical of I; otherwise only soundness holds in general. Unfortunately, at present computing a set of generators G for a real radical appears to be, in the general case, computationally infeasible. Below, we shall briefly discuss the state of the art concerning this problem, then a special case where this computation is feasible, and what are the alternatives in cases where it is not.

A classical algorithm for computing real radicals is due to Neuhaus [23]. This is also implemented as part of Singular's `realrad` library [11, Sect.D.4.16], accessible via SageMath [32]. The worst case asymptotic complexity of this algorithm is very high: $D^{2^{O(N^2)}}$ (exact) arithmetic operations, where D is the maximum total degree of the polynomials in the set Q. Over the years there have been improvements: let us just mention the algorithm by Lasserre et al., based on semi-definite relaxations but limited to ideals with zero dimensional varieties [20]; and the recent probabilistic method by El Din et al. [12], which lowers the asymptotic complexity to $|Q|^{O(1)}(ND)^{O(Nr2^r)}$, where r is the dimension of the variety ψ. Despite these advances, the resulting algorithms appear to be still totally impractical but for very simple instances: [12] mentions an example with $N = 9$ variables and maximum total degree $D = 3$ which is beyond Singular's capabilities and requires 800 s with their implementation.

Next, we consider a simple special case of practical interest, where it is trivial to build the real radical. This case is relevant to the auxiliary variables method mentioned in Remark 2, and will be put into systematic use when dealing with semialgebraic systems (Section 7). The general idea is that ψ, as a precondition, equates each system variable to a generic constant, or polynomial expression thereof, which are the g_i s in the statement. This permits a quite uniform and general treatment of initial conditions.

Proposition 1. *Let $\mathbf{x} = (x_1, \ldots, x_N)$, let $1 \le m < N$ and assume $Q = \{x_i - g_i : i = 1, \ldots, m\}$, where $g_i \in \mathbb{R}[x_{m+1}, \ldots, x_N]$. Then, for $\psi = \mathbf{V}(Q)$, we have $\mathbf{I}(\psi) = \langle\, Q\,\rangle$.*

Proof. Fix a lexicographic monomial order such that $x_i > x_j$ whenever $i \le m$ and $j \ge m+1$. W.r.t. this order, Q is a Gröbner basis for $I = \langle\, Q\,\rangle$: indeed, take any $0 \ne p \in I$ and assume by contradiction that LM(p) (the leading monomial of p) is not divisible by any leading monomial x_i in Q; that is, LM(p) does not contain any x_i with $i \le m$. This would imply, by definition of lex order, that p does not contain any such x_i, that is $p \in \mathbb{R}[x_{m+1}, \ldots, x_N]$. Then for each $v = (\mu_{m+1}, \ldots, \mu_N)$,

[8] https://github.com/micheleatunifi/postconditions/blob/master/Post.py.

we can consider $w = (g_1(v), \ldots, g_m(v), \mu_{m+1}, \ldots., \mu_N) \in \psi = \mathbf{V}(Q)$, implying $p(w) = p(v) = 0$. In conclusion, as $p(v) = 0$ for each v, p is the zero polynomial, contradicting the assumption.

Now let us check that $\mathbf{I}(\psi) = \langle\, Q \,\rangle = I$. Clearly $\mathbf{I}(\psi) \supseteq \langle\, Q \,\rangle$. On the other hand, consider any $p \in \mathbf{I}(\psi)$ and let $p = q + r$, where $r = p \bmod Q$ and $q \in I$. By the above assumptions on Q and by definition of remainder, no variable x_i with $i \le m$ can occur in r, that is $r \in \mathbb{R}[x_{m+1}, \ldots, x_N]$. Now assume by contradiction $r \neq 0$, so there is $v = (\mu_{m+1}, \ldots, \mu_N)$ such that $r(v) = a \neq 0$. Then $w = (g_1(v), \ldots, g_m(v), \mu_{m+1}, \ldots., \mu_N) \in \psi$, hence $p(w) = 0$; yet $p(w) = q(w) + r(v) = 0 + a \neq 0$, which is a contradiction. □

When computing $\mathbf{I}(\psi)$ is not feasible, there is little alternative to replacing it with some easy to compute ideal $I_0 \subseteq \mathbf{I}(\psi)$: as discussed above, this preserves soundness of the approach, although completeness is lost in general. A practical choice might be considering $\sqrt{I}$, the *complex* radical ideal of I

$$\sqrt{I} \overset{\triangle}{=} \{p \in \mathbb{C}[\mathbf{x}] \,:\, p^m \in I \text{ for some } m > 0\}$$

where $\mathbb{C}$ denotes the complex field. By Hilbert's strong Nullstellensatz [10, Ch.4,§1.2,Th.6], in $\mathbb{C}[\mathbf{x}]$ we have

$$\sqrt{I} = \mathbf{I}(\mathbf{V}_{\mathbb{C}}(I))$$

where $\mathbf{V}_{\mathbb{C}}(I) = \{v \in \mathbb{C}^N \,:\, p(v) = 0 \text{ for each } p \in I\}$ is the complex algebraic variety induced by I. As $\mathbf{V}_{\mathbb{C}}(I) \supseteq \mathbf{V}(I)$, one has

$$\sqrt{I} \cap \mathbb{R}[\mathbf{x}] \subseteq \mathbf{I}(\psi)\,. \tag{15}$$

Therefore, we can set $I_0 = \sqrt{I} \cap \mathbb{R}[\mathbf{x}]$ and take as G any Gröbner basis of $\sqrt{I}$; note that, as $I \subseteq \mathbb{R}[\mathbf{x}]$, necessarily $G \subseteq \mathbb{R}[\mathbf{x}]$. The inclusion (15) is in general strict. As an example, consider $Q = \{x^2 + 1\}$, hence $\mathbf{V}(Q) = \emptyset$: then trivially $\mathbf{I}(\psi) = \mathbb{R}[\mathbf{x}]$. On the other hand, $\mathbf{V}_{\mathbb{C}}(\{x^2 + 1\}) = \{\iota, -\iota\}$ hence $\sqrt{I} \cap \mathbb{R}[\mathbf{x}] \neq \mathbb{R}[\mathbf{x}]$; for example $x \notin \sqrt{I}$.

The problem of computing a set of generators for the complex radical of I is well understood, and there exist well-known algorithms to this purpose: in particular, those by Krick and Logar [18] and by Laplagne [19]. Although the worst-case complexity of these methods is doubly exponential in the number of variables, they often work reasonably well and a number of implementations are offered in computer algebra systems, including those in Singular's `radical` library [11, Sect.D.4.14.7]. We rely on this library in our implementation.

6. Experiments

We report below the outcomes of three experiments we have conducted, applying the POST algorithm to challenging systems taken from the literature. The execution times reported below are for an implementation in Python under SageMath [32], running on a Core i5 machine.[9] Wherever possible, we compare our results with those obtained by other authors.

Collision avoidance We consider the two-aircraft dynamics used to study collision avoidance, discussed in many papers on hybrid systems [34,21,15]. The model is described by the equations below, where the variables have the following meaning: (x_1, x_2) and (y_1, y_2) represent the Cartesian coordinates of aircraft 1 and 2, respectively; (d_1, d_2) and (e_1, e_2) their velocities; applying the technique discussed in Remark 2, we also introduce the auxiliary variables (parameters, hence 0 derivative) ω_1 and ω_2, representing the angular velocities of the two aircrafts, and $x_{10}, x_{20}, y_{10}, y_{20}, d_{10}, d_{20}, e_{10}, e_{20}$, representing generic initial values of the corresponding variables. Overall, the system's vector field F_1 consists of 18 polynomials over as many variables (including the auxiliary ones).

$$\begin{array}{llll} \dot{x}_1 = d_1 & \dot{y}_1 = e_1 & \dot{d}_1 = -\omega_1 d_2 & \dot{e}_1 = -\omega_2 e_2 \\ \dot{x}_2 = d_2 & \dot{y}_2 = e_2 & \dot{d}_2 = -\omega_1 d_1 & \dot{e}_2 = -\omega_2 e_1\,. \end{array}$$

We consider the precondition ψ that assigns to each non constant variable the parameter corresponding to its (generic) initial value: $\psi = \mathbf{V}(\{x_1 - x_{10}, x_2 - x_{20}, \ldots\})$. Note that $G = \{x_1 - x_{10}, x_2 - x_{20}, \ldots\}$ is a set of generators for $\mathbf{I}(\psi)$, and in fact a Gröbner basis w.r.t. the lexicographic order (Proposition 1). We then consider a complete template π of degree 2 over all the system's variables: π is a linear combination of $n = 190$ monomials that uses as many template parameters. We then run POST(ψ, π), which returns, after $m = 3$ iterations and about 16 s, a pair (V, J). The vector space V corresponds to a result template with 10 parameters, $\pi' = \sum_{i=1}^{10} a_i \cdot p_i$. The instances of π' are therefore all and only the system's polynomial invariants of degree ≤ 2, starting from a fully generic precondition (Theorem 1(a)). These include all the polynomial invariants mentioned in [34,21], and several new ones, like the following

$$-x_{10}d_{10} - x_{20}d_{20} + d_{10}x_1 + d_{20}x_2 + x_{10}d_1 - x_1 d_1 + x_{20}d_2 - x_2 d_2\,.$$

[9] Code and examples available at https://github.com/micheleatunifi/postconditions/blob/master/Post.py.

Let $\phi \overset{\triangle}{=} \mathbf{V}(\pi'[\mathbb{R}^n])$ be the variety defined by the result template π'. The invariant ideal J returned by the algorithm represents the weakest algebraic precondition $\chi \overset{\triangle}{=} \mathbf{V}(J)$ such that $\chi \longrightarrow [F_1]\phi$: in other words, the largest algebraic precondition for which all instances of π' are polynomial invariants (Theorem 2(b)). Moreover, χ is also the weakest algebraic invariant included in ϕ (Theorem 2(a)). A Gröbner basis of J consists of 12 polynomials that represent as many conservation laws of the system (see Appendix C).

Airplanes vertical motion We consider the 6-th order longitudinal equations that capture the vertical motion (climbing, descending) of an airplane [37, Chapter 5]. The system is given by the equations below, where the variables have the following meaning: u = axial velocity, w = vertical velocity, x = range, z = altitude, q = pitch rate, θ = pitch angle. We also have two equations encoding $\cos\theta$ and $\sin\theta$: note that, in the equations, these two are just variable names, not transcendental functions themselves. Applying the technique discussed in Remark 2, we also introduce the following auxiliary variables (parameters, hence 0 derivative): g = gravity acceleration; X/m, Z/m and M/I_{yy}, where m is the mass of the airplane, M the aerodynamic and thrust moment w.r.t. the y axis, (X, Z) are the aerodynamics and thrust forces w.r.t. axis x and z, and I_{yy} is the second diagonal element of its inertia matrix (see also [37,15,17]); and u_0, w_0, x_0, z_0, q_0, standing for the generic initial values of the corresponding variables. Overall, the system's vector field F_2 consists of 17 polynomials over as many variables.

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

In order to discover interesting polynomial invariants, we consider a complete template π of degree 2 over all the original system's variables plus two auxiliary variables, the latter representing the monomials qu and qw.[10] π is a linear combination of $n = 207$ monomials that uses as many template parameters. We apply the approach underpinned by Theorem 2(b): we first pick up a precondition that requires $\theta = 0$ and assign (generic) initial values to the remaining variables, $\psi_0 \overset{\triangle}{=} \mathbf{V}(\{\theta, \sin\theta, \cos\theta - 1, u - u_0, w - w_0, x - x_0, z - z_0, q - q_0\})$. Note that $G = \{\theta, \sin\theta, ...\}$ is a set of generators for $\mathbf{I}(\psi)$, and in fact a Gröbner basis w.r.t. the lexicographic order (Proposition 1). We then run $\textsc{post}(\psi_0, \pi)$, which returns, after $m = 8$ iterations and about 26 s, a pair (V, J). The vector space V corresponds to the following result template:

$$\begin{aligned}
\pi' \;=\; \sum_{i=1}^{4} a_i \cdot p_i = a_1 \cdot \left(\cos^2\theta + \sin^2\theta - 1\right) \quad + \quad & a_2 \cdot \left(-\frac{1}{2}q^2 + \theta\frac{M}{I_{yy}} + \frac{1}{2}q_0^2\right) + \\
& a_3 \cdot \left(uq\cos\theta + wq\sin\theta - \frac{X}{m}\sin\theta + \frac{Z}{m}\cos\theta - x\frac{M}{I_{yy}} - -\frac{M}{I_{yy}}x_0 + u_0q_0 + \frac{Z}{m}\right) + \\
& a_4 \cdot \left(wq\cos\theta - uq\sin\theta - \theta g - \frac{X}{m}\cos\theta - \frac{Z}{m}\sin\theta - z\frac{M}{I_{yy}} - \frac{M}{I_{yy}}z_0 + w_0q_0 + \frac{X}{m}\right).
\end{aligned}$$

Let $\phi \overset{\triangle}{=} \mathbf{V}(\pi'[\mathbb{R}^n])$ be the variety defined by the result template π'. The invariant ideal J returned by the algorithm represents the weakest algebraic precondition $\chi \overset{\triangle}{=} \mathbf{V}(J)$ such that $\chi \longrightarrow [F_2]\phi$: in other words, the largest algebraic precondition for which all instances of π' are polynomial invariants (Theorem 2(b)). Moreover, χ is also the weakest algebraic invariant included in ϕ (Theorem 2(a)). A Gröbner basis of J consists of 15 polynomials. These findings generalize those in [15,17]. In particular, one obtains the polynomial invariants of [15,17] by letting $x_0 = z_0 = q_0 = 0$. By comparison, [15] reports that their method spent 1 hour to find a subset of all instances of π'. The method in [17] reportedly takes < 1 s on this system, but again only finds a subset[11] of instances of π'. Moreover, it cannot infer the largest algebraic invariant implying the discovered laws, as we do.

Kepler laws We want to show how the $\textsc{post}$ algorithm automatically discovers the three Kepler's laws of planetary motion from Newton's law of gravitation. A nice and self-contained explanation of these laws can be found in [30]. Newton's laws are expressed below in a system of polar coordinates (r, θ) with the Sun at the origin. The meaning of the variables is as follows: r is the planet's distance from the origin; θ the angle from the positive horizontal semiaxis to the radius vector, measured counterclockwise; v_r and ω the planet's radial and angular velocity, respectively; $u = 1/r$ the distance reciprocal; for the purpose of expressing the invariants of interest, the system also includes equations for $\cos\theta$ and $\sin\theta$; moreover, we have constants (0 derivative variables) GM, a, e representing the product of the gravitational constant G and the Sun's

[10] We could dispense with these auxiliary variables by considering a complete template of degree 3.

[11] For instance, one should compare the polynomial $\psi_3 = q^2 - 2\frac{M\theta}{I_{yy}}$, which is part of the invariant cluster in [17], with the polynomial $p_2 = -\frac{1}{2}q^2 + \theta\frac{M}{I_{yy}} + \frac{1}{2}q_0^2$ in the second summand of π' above, which explicitly depends on the initial condition q_0.

mass M, the orbit's major semiaxis and its eccentricity, respectively (see below). A few more dummy constants are used to encode positivity conditions. Overall, the system's vector field F_3 consists of 15 polynomials over as many variables.

$$\begin{array}{lllll} \dot{r} = v_r & \dot{\theta} = \omega & \dot{v}_r = -GMu^2 + r\omega^2 & \dot{\omega} = -2v_r\omega u & \dot{u} = -u^2 v_r \\ & & \dot{\cos}\theta = -\omega\sin\theta & \dot{\sin}\theta = \omega\cos\theta\,. & \end{array} \tag{16}$$

Because Kepler's laws concern closed orbits,[12] we first seek for a precondition ψ such that the planet's motion is an ellipse of major semiaxis a and eccentricity e. The equation of such an ellipse in polar coordinates, with one of the foci coinciding with the origin (Sun) and the horizontal axis passing through the ellipse's center, is $p_{\text{ell}} = 0$, where

$$p_{\text{ell}} \stackrel{\triangle}{=} r(1 + e\cos\theta) - a(1 - e^2)\,. \tag{17}$$

We consider a suitable ψ_0 that implies a unitary circular orbit, which is an instance of p_{ell}, and apply Theorem 2(b): running $\text{POST}(\psi_0, \pi_1)$ for a $\pi_1 = a_1 \cdot p_{\text{ell}}$, we discover, in about 43 s, the largest (physically meaningful) precondition ψ implying $p_{\text{ell}} = 0$. In particular, for $\omega_{\text{in}} \stackrel{\triangle}{=} r^2\omega^2 - GM \cdot u \cdot (e+1)$, we have $\psi = \mathbf{V}(P)$ where

$$P = \{r - a(1-e), \theta, v_r, \omega_{\text{in}}, u \cdot r - 1, \cos\theta - 1, \sin\theta\} \cup P_+\,. \tag{18}$$

Here the set P_+ encodes positivity conditions on constants ($GM > 0, a > 0, 0 \le e < 1$) and is omitted for conciseness (further details on the computation of ψ and ψ_0 are given in Remark 3 below).

We next consider the complete polynomial template π_2 built out of monomials of degree ≤ 4 on the variables GM, a, e, r, u, dA, where $dA \stackrel{\triangle}{=} \frac{1}{2}r^2\omega$ is an auxiliary variable, representing the areal velocity – that is, the first derivative of the area swept by the radius vector. We next run $\text{POST}(\psi, \pi_2)$, which returns, after $m = 4$ iterations and about 58 s, a pair (V', J'). The vector space V' corresponds to a result template $\pi_2' = a_1 \cdot (ur - 1) + a_2 \cdot (dA^2 - a \cdot GM(1-e^2)/4) + R$, where $R = \sum_{\ell=2}^{29} a_\ell \alpha_\ell$. The term $ur - 1$, that is $u = 1/r$, obtained by setting $a_1 = 1$ and the remaining template parameters to 0, is another way of expressing Kepler's second law: indeed, it implies that $\mathcal{L}(dA) = -\omega r^2 u v_r + \omega r v_r = 0$, that is, that the areal velocity is constant. From Geometry, we know that the ellipse's area is $A = \text{Pi}\ a^2\sqrt{1-e^2}$, where $\text{Pi} = 3.1415\ldots$ denotes the transcendental mathematical constant. Since dA is a constant, the orbital period, expressed as a multiple of Pi, is $T \stackrel{\triangle}{=} a^2\sqrt{1-e^2}/dA$. Therefore, the second term in π_2', obtained by setting $a_2 = 1$ and the remaining template parameters to 0, can be read as saying that the square of the period, $T^2 = a^4(1-e^2)/dA^2$, is proportional to a^3, the cube of the semimajor axis: this is Kepler's third law. Any other summand of π_2' is either a multiple of $ur - 1$ or equivalent to the second term, hence it gives no further information.

Let $\phi' = \mathbf{V}(\pi_2[\lambda'])$. The invariant ideal J' returned by the algorithm represents the weakest algebraic precondition $\chi' \stackrel{\triangle}{=} \mathbf{V}(J')$ such that $\chi' \longrightarrow [F_3]\phi'$: in other words, the largest algebraic precondition implying both the second and the third Kepler law (Theorem 2(b)). A Gröbner basis of the invariant ideal J' is $\{ur - 1, dA^2 - a \cdot GM(1-e^2)/4\}$, hence giving precisely the same information as π_2'.

Rather than "discovering" the laws, it is also possible to verify them directly using POST, that is to check $\psi \longrightarrow [F_3]\phi_i$, with: $\phi_1 = \mathbf{V}(\{p_{\text{ell}}\})$, $\phi_2 = \mathbf{V}(\{\mathcal{L}(dA)\})$ and $\phi_3 = \mathbf{V}(\{T^2GM - 4a^3\})$. The running time for these checks is of about 45, 0.28 and 3 s, respectively.

Remark 3 *(on the computation of ψ_0 and ψ).* Concerning the precondition ψ_0, we consider a simple unitary circular orbit, that is $p_{\text{ell}} = 0$ with $GM = a = 1$ and $e = 0$. More precisely, considering as $t = 0$ to be a time when the planet is on the positive semiaxis, we let $\psi_0 = \mathbf{V}(P_0)$ with $P_0 = \{e,\ a - 1,\ GM - 1,\ r - 1,\ \theta,\ v_r,\ \omega - 1,\ u - 1\}$ and use the template $\pi_1 = a_1 \cdot p_{\text{ell}}$. We then run $\text{POST}(\psi_0, \pi_1)$, which returns a pair (V, J), in $m = 8$ iterations and about 43 s. By Theorem 2(b), $\chi \stackrel{\triangle}{=} \mathbf{V}(J)$ is the largest algebraic precondition implying $p_{\text{ell}} = 0$. A set of generators for the invariant ideal J consists of 9 polynomials (the Gröbner basis is much larger, though). However, we want to restrict ourselves to physically meaningful initial conditions at time $t = 0$, and to closed orbits. Let J_0 denote the ideal generated by the polynomial encoding of the following conditions: $v_r = \theta = \sin\theta = 0$, $u \cdot r = \cos\theta = 1$, $r = a(1-e)$ (from $p_{\text{ell}} = 0$), $dA = -r^2\omega/2$, $GM > 0$, $a > 0$ and on $0 \le e < 1$ (closed orbits). We then define $\psi \stackrel{\triangle}{=} \mathbf{V}(J + J_0) = \chi \cap \mathbf{V}(J_0)$. A small set of polynomials representing ψ is obtained by computing a Gröbner basis G of $\sqrt{J + J_0}$, the complex radical of $J + J_0$. From G, via some simple manipulations, we compute the equivalent set P in (18); that is, we have $\psi = \mathbf{V}(P)$.

7. Application to continuous semialgebraic systems

We illustrate an application of the POST algorithm to the safety verification of a class of continuous systems, where both the initial set of states and the set of unsafe ('bad') states are *semialgebraic* regions of $\mathbb{R}^N$. The family of semialgebraic sets, formally defined below, is larger than the family of algebraic sets and quite rich: for instance, in $\mathbb{R}^3$ a half-space, a disk, and

[12] Note that non closed, hyperbolic or parabolic, trajectories are also possible.

a ball are semialgebraic, but not algebraic sets. See [25] for an introduction to semialgebraic sets and related techniques. For the purpose of safety verification, the basic idea is that, once we have obtained via POST an algebraic invariant for the system at hand, we can check if this invariant, as a region of $\mathbb{R}^N$, intersects the specified unsafe region: if not, the system is safe. In pursuing this idea, we will systematically exploit the idea of auxiliary variables: we will have the obtained invariant be explicitly dependent on a set of parameters $\mathbf{x}_0$, representing a generic initial condition for the given system. Proposition 1 will guarantee that a real radical for the initial set will be easy to compute.

A set $S \subseteq \mathbb{R}^N$ is *(closed) basic semialgebraic* if there are polynomials $g_1, \ldots, g_m \in \mathbb{R}[\mathbf{x}]$ such that $S = \{v \in \mathbb{R}^N : g_1(v) \geq 0, \ldots, g_m(v) \geq 0\}$, written $S = \mathbf{S}(\{g_1 \geq 0, \ldots, g_m \geq 0\})$.[13] A (closed) semialgebraic set is a finite union of basic semialgebraic sets. In what follows, for the sake of simplicity we shall focus on basic semialgebraic sets. It is very simple to extend the approach to general semialgebraic sets: this is outlined at the end of the section. A *continuous (basic) semialgebraic system* is a triple $SA = (F, X_0, X_U)$, composed by a polynomial vector field F, an *initial region* $X_0 \subseteq \mathbb{R}^N$ and an *unsafe region* $X_U \subseteq \mathbb{R}^N$, both of which are basic semialgebraic. The system SA is *safe* if for each $v_0 \in X_0$ there is no $t \in D_{v_0}$ such that $\mathbf{x}(t; v_0) \in X_U$.

Let us now introduce some additional notation concerning auxiliary variables. Let $F = (f_1, \ldots, f_N)$ be a polynomial vector field, with $f_i \in \mathbb{R}[\mathbf{x}]$. Let $\mathbf{x}_0 = (x_{01}, \ldots, x_{0N})$ be a vector of N distinct variables, disjoint from $\mathbf{x}$: we define the *extended* vector variables and vector field as $\hat{\mathbf{x}} = (x_{01}, \ldots, x_{0N}, x_1, \ldots, x_N)$ and $\hat{F} = (0, \ldots, 0, f_1, \ldots, f_N)$, respectively. Note that $\hat{F}$ is a vector field $\mathbb{R}^{2N} \to \mathbb{R}^{2N}$, where the variables in $\mathbf{x}_0$ represent generic constants. For $v, w \in \mathbb{R}^N$, we will denote by (v, w) the element of $\mathbb{R}^{2N}$ obtained by concatenating v and w. Finally, we will denote by $g[\mathbf{x}_0/\mathbf{x}]$ the polynomial obtained from g by replacing each variable x_i with x_{i0}, for $i = 1, \ldots, N$.

The following result gives a sufficient algebraic condition for safety of a continuous basic semialgebraic system. Its intuitive interpretation is as follows. In $\mathbb{R}^{2N}$, let ψ be a precondition encoding that $\mathbf{x}_0$ is the initial condition for $\mathbf{x}$, and let J be an invariant ideal representing a corresponding postcondition, explicitly depending on $\mathbf{x}_0$. Hence, for any concrete instance of the initial conditions $\mathbf{x}_0$, we obtain from J a corresponding concrete postcondition. If there is no solution of the set of (in)equations representing the intersection of the initial region, of the postconditions and of the unsafe region, then the system is safe.

Theorem 3 *(safety of semialgebraic systems). Let $SA = (F, X_0, X_U)$ be a basic semialgebraic system, where $X_0 = \mathbf{S}(\{g_1 \geq 0, \ldots, g_m \geq 0\})$ and $X_U = \mathbf{S}(\{h_1 \geq 0, \ldots, h_n \geq 0\})$ ($g_i, h_j \in \mathbb{R}[\mathbf{x}]$). Let $\psi = \mathbf{V}(\{x_i - x_{i0} : i = 1, \ldots, N\}) \subseteq \mathbb{R}^{2N}$ and let $J = \langle \{q_1, \ldots, q_k\} \rangle \subseteq \mathbb{R}[\hat{\mathbf{x}}]$ be an invariant ideal for $\hat{F}$ such that $\mathbf{V}(J) \supseteq \psi$. Assume the following polynomial system in the variables $\hat{\mathbf{x}}$*

$$g_1[\mathbf{x}_0/\mathbf{x}] \geq 0, \ldots, g_m[\mathbf{x}_0/\mathbf{x}] \geq 0,\ h_1 \geq 0, \ldots., h_n \geq 0,\ q_1 = 0, \ldots., q_k = 0 \tag{19}$$

has no solution in $\mathbb{R}^{2N}$. Then SA is safe.

Proof. By contradiction, assume there are $w_0 \in X_0$ and $w_1 = \mathbf{x}(t_1; w_0) \in X_U$, for some $t_1 \in D_{w_0}$. We will show that $(w_0, w_1) \in \mathbb{R}^{2N}$ is a solution of (19), thus arriving at a contradiction. Indeed, by definition $g_i[\mathbf{x}_0/\mathbf{x}](w_0, w_1) = g_i(w_0) \geq 0$ and $h_j(w_0, w_1) = h_j(w_1) \geq 0$ for each $i = 1, \ldots, m$ and $j = 1, \ldots., n$. Consider now the trajectory of $\hat{F}$ originating from (w_0, w_0), that is $\hat{\mathbf{x}}(t; (w_0, w_0))$: note that, by definition of $\hat{F}$, $\hat{\mathbf{x}}(t; (w_0, w_0)) = (w_0\,, \mathbf{x}(t; w_0))$ for each $t \in D_{w_0}$. Now, since $\mathbf{V}(J) \supseteq \psi$, we have $(w_0, w_0) \in \mathbf{V}(J)$, hence, by $\hat{F}$-invariance of J, $\hat{\mathbf{x}}(t; (w_0, w_0)) \in \mathbf{V}(J)$ for each $t \in D_{(w_0, w_0)}$ (Lemma 5). In particular, considering $t = t_1$, we have $\hat{\mathbf{x}}(t_1; (w_0, w_0)) = (w_0\,, \mathbf{x}(t_1; w_0)) = (w_0, w_1) \in \mathbf{V}(J)$. But this means $q_i(w_0, w_1) = 0$ for $i = 1, \ldots, k$. In conclusion, (w_0, w_1) is a solution of (19). □

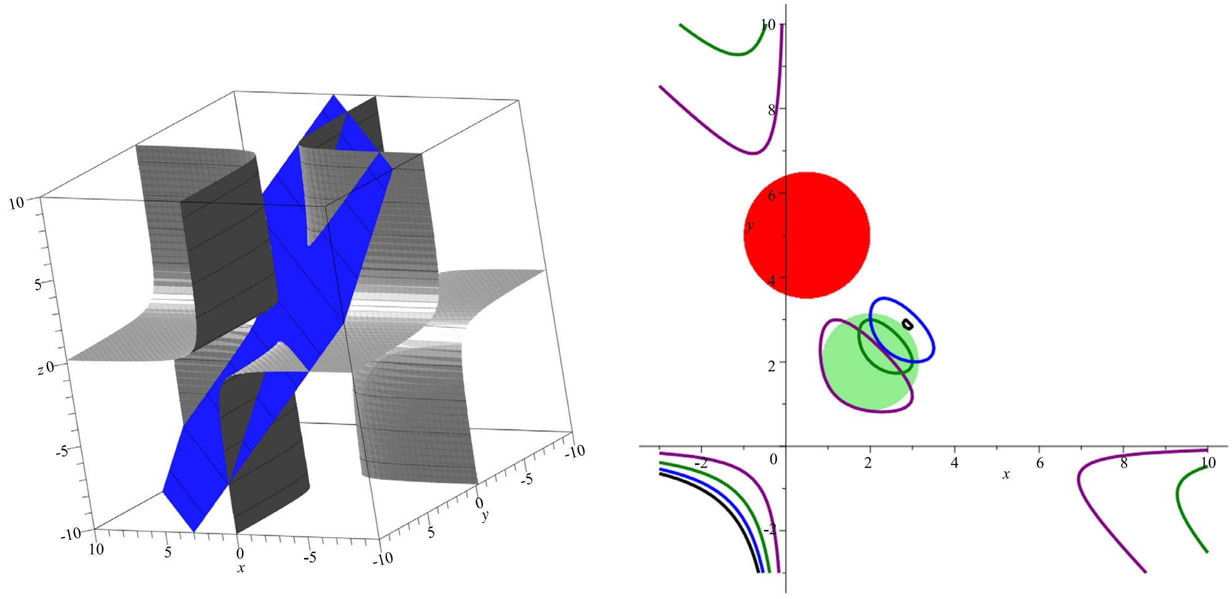
There are two aspects of the previous result that are worthwhile commenting on. First, checking that an algebraic system of (in)equalities like (19) is solvable is decidable, although NP-hard. One well-known and effective technique to establish insolvability is to rely on Positivstellensatz [38] and Sum-of-Squares programming: this also provides easy to verify *certificates* of insolvability. For the sake of completeness, we outline this technique in Appendix D.

Second, the procedure resulting from the theorem is of course incomplete, and its precision depends on how rich the ideal J is. An invariant ideal J satisfying the hypotheses of the theorem can be obtained by running $\text{POST}_{\hat{F}}(\psi, \pi)$ with ψ as specified in the statement of the theorem, and any template $\pi \in \mathbb{L}(\mathbf{a})[\hat{\mathbf{x}}]$. Indeed, if $(V, J) = \text{POST}_{\hat{F}}(\psi, \pi)$ (for some V), by Theorem 1(b) J is a $\hat{F}$-invariant ideal such that $\mathbf{V}(J) \supseteq \psi$. The last point follows because $J \subseteq I_\psi$ implies that $q(w, w) = 0$ for each $q \in J$ and $(w, w) \in \psi$. Note that this is a case where a basis for the real radical $\mathbf{I}(\psi)$ is trivial (Proposition 1), hence relative completeness holds. Therefore, by tuning the template π, one can in principle hope to obtain a J which is as precise as possible. The following example[14] illustrates this theorem.

Example 6 *(3D Lotka-Volterra).* Consider the 3D Lotka-Volterra system defined by $\mathbf{x} = (x, y, z)$ and the vector field $F = (xy - xz, yz - yx, zx - zy)$; see e.g. [34,17]. Consider the basic semialgebraic system $SA = (F, X_0, X_U)$, where $X_0 = \mathbf{S}(\{z = 3, (x -$

[13] Note that an equality $g_i = 0$ can be coded up as a pair of inequalities $g_i \geq 0$ and $-g_i \geq 0$. Similarly, a strict inequality $g_i > 0$ can be coded up using an auxiliary slack variable z as $g_i \cdot z^2 - 1 \geq 0$.

[14] SageMath/Python scripts for the examples in this section available at https://github.com/micheleatunifi/postconditions/blob/master/Post.py.



(a)

(b)

Fig. 1. With reference to the 3D Lotka-Volterra system in Example 6: (a) surfaces in $\mathbb{R}^3$ induced by the polynomials q_1 (grey) and q_2 (blue) in J, when instantiating (x_0, y_0, z_0) to $(1, 1, 1)$; the corresponding algebraic invariant coincides with the intersection of the two surfaces; (b) projection onto the (x, y)-plane of X_0 (green), of X_U (red) and of the four algebraic invariants obtained from J by instantiating (x_0, y_0, z_0) to four points in X_0: $(2 - c, 2 - c, 3)$, $(2, 2, 3)$, $(2, 3.15, 3)$ and $(2 + c, 2 + c, 3)$, where $c = 1.15/\sqrt{2}$. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

$2)^2 + (y - 2)^2 \leq 1.15^2\})$ (a disk) and $X_U = \mathbf{S}(\{(x - 1/2)^2 + (y - 5)^2 \leq 1.5^2\})$ (an infinite cylinder). We wish to prove that SA is safe.

Consider the extension of F, $\hat{F}$, over the variables $\hat{\mathbf{x}} = (x_0, y_0, z_0, x, y, z)$; let $\pi \in \mathbb{L}(\mathbf{a})[\hat{\mathbf{x}}]$ be a complete template of degree 3. Running $\text{POST}_{\hat{F}}(\psi, \pi)$ with $\psi = \mathbf{V}(\{x - x_0, y - y_0, z - z_0\})$, we get as a result (after about 40 s) a pair (V, J) where $J = \langle\, \{q_1, q_2\} \,\rangle$ and

$$
\begin{aligned}
q_1 &= xzy - xz_0y_0 - zz_0y_0 - yz_0y_0 + z_0^2y_0 + z_0y_0^2 \\
q_2 &= x_0 + y_0 + z_0 - x - y - z\,.
\end{aligned}
$$

By the above discussion, J is a $\hat{F}$-invariant ideal and $\mathbf{V}(J) \supseteq \psi$. For any instantiation of x_0, y_0, z_0 with real values, J represents a 1-dimensional variety in $\mathbb{R}^3$, that is a curve, obtained as the intersection of two surfaces. See Fig. 1(a). Any trajectory starting in such a variety will remain in it.

Fig. 1(b) shows the projection onto the (x, y)-plane of X_0, of X_U and of four curves induced by J, when instantiating (x_0, y_0, z_0) with four distinct points in X_0. None of those curves intersects the unsafe region, suggesting that the system might be safe. This can in fact be proven algebraically relying on (19), which for the present case is equivalent to the following (we have eliminated the variable z_0 exploiting the equation $z_0 = 3$ for X_0):

$$
\begin{aligned}
-(x_0 - 2)^2 - (y_0 - 2)^2 + 1.15^2 &\geq 0 \\
-(x - 1/2)^2 - (y - 5)^2 + 1.5^2 &\geq 0 \\
xzy - 3xy_0 - 3zy_0 - 3yy_0 + 9y_0 + 3y_0^2 &= 0 \\
x_0 + y_0 + 3 - x - y - z &= 0\,.
\end{aligned}
$$

This algebraic system is proven to have no solutions: we give the details, including a certificate of insolvability, in Appendix D. Therefore, by virtue of Theorem 3, SA is safe.

Theorem 3 admits the following slight generalization, that allows for a more flexible use of auxiliary variables. Condition (a) requires that ψ captures all points (v_0, v_0) for v_0 in the initial set. We report a proof in Appendix D.

Theorem 4. *Let $SA = (F, X_0, X_U)$ be a basic semialgebraic system, and $\hat{\mathbf{x}}$ and $\hat{F}$ be the extended variable vector and vector field, like in Theorem 3. For $r_1, \ldots, r_N \in \mathbb{R}[\mathbf{x}_0]$, let $\psi = \mathbf{V}(\{x_i - r_i : i = 1, \ldots, N\})$. Finally let $J = \langle\, \{q_1, \ldots, q_k\} \,\rangle \subseteq \mathbb{R}[\hat{\mathbf{x}}]$ be an invariant ideal for $\hat{F}$ such that $\mathbf{V}(J) \supseteq \psi$. Assume the following conditions hold true:*

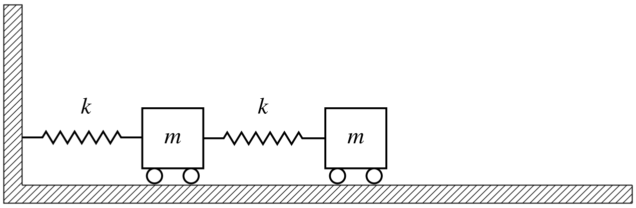


Fig. 2. A spring-mass system.

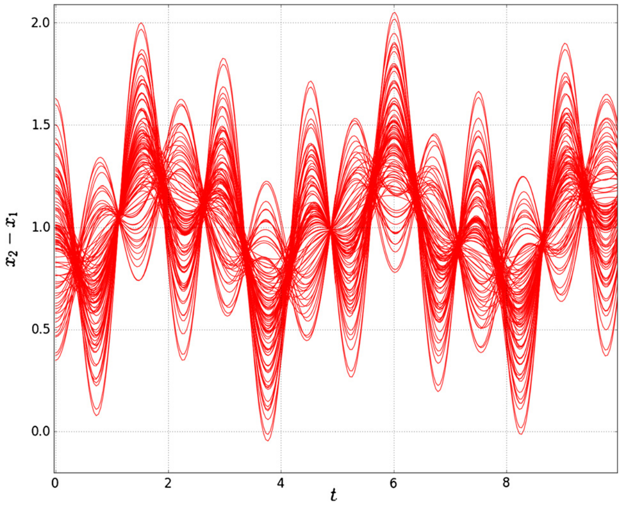


Fig. 3. With reference to the coupled spring-mass system in Example 7, plots of 100 trajectories $x_2(t) - x_1(t)$ starting from random points in X_0.

(a) $(X_0 \times X_0) \cap Id \subseteq \psi$ *($Id =$ identity relation over* $\mathbb{R}^{2N}$*);*
(b) *The polynomial system in the variables* $\hat{\mathbf{x}}$ *in* (19) *has no solution in* $\mathbb{R}^{2N}$.

Then SA *is safe.*

The slightly enhanced flexibility of Theorem 4 consists essentially in the fact that we can have a subset of the initial values fixed to constants. This is illustrated in the following example.

Example 7 *(coupled spring-mass system).* A system consists of two identical springs of elastic constant k and length L and two identical bodies of mass m, connected in cascade: wall, spring 1, mass 1, spring 2, mass 2. See Fig. 2. This system is governed by the following equations, where x_1, x_2 and v_1, v_2 denote, respectively, the bodies' positions and velocities on the horizontal axis with the origin fixed at the wall:

$$\begin{aligned}
\dot{x}_1 &= v_1 \\
\dot{v}_1 &= (k/m)(x_2 - 2x_1) \\
\dot{x}_2 &= v_2 \\
\dot{v}_2 &= -(k/m)(x_2 - x_1 - L)\,.
\end{aligned}$$

Considering k/m and L as 0-derivative variables, that is constants, we let $\mathbf{x} = (k/m, L, x_1, v_2, x_2, v_2)$ and $F = (0, 0, v_1, k/m(x_2 - 2x_1), v_2, -k/m(x_2 - x_1 - L))$. Consider the system $SA = (F, X_0, X_U)$ with initial set $X_0 = \mathbf{S}(\{k/m = 1, L = 1, (x_1 - 1/2)^2 + (x_2 - 3/2)^2 \le 1/4, v_1 = 0, v_2 = 0\})$ and unsafe set $X_U = \mathbf{S}(\{x_2 - x_1 \ge 2.17\})$. That is, we fix the value of both constants to 1 and the initial velocities to 0, and let the initial positions (x_1, x_2) of the two masses vary in a disk of radius 1/2 centered at $(1/2, 3/2)$. We then ask if the distance of the first mass from the second ever reaches or exceeds the value 2.17. Fig. 3(a), displaying the plots of $x_2(t; v_0) - x_1(t; v_0)$ for 100 random initial conditions $v_0 \in X_0$, suggests that the system might indeed be safe. We now prove this fact. Note that, despite the linearity of the system, nonlinear invariants will be essential to prove safety.

As dictated by Theorem 4, we consider an extended vector field $\hat{F}$ over the variables[15] $\hat{\mathbf{x}}$, then take a complete template π of total degree 3 over $\hat{\mathbf{x}}$ and $\psi = \mathbf{V}(\{x_1 - x_{10}, x_2 - x_{20}, v_1, v_2\})$. We obtain $(V, J) = \textsc{post}_{\hat{F}}(\psi, \pi)$, which takes about 60 s, for some V and $J = \langle \{q_1, q_2\} \rangle$, where

$$\begin{aligned} q_1 = {} & 2/3(k/m)Lx_{10} + (k/m)x_{10}^2 - 4/3(k/m)x_{10}x_{20} + 1/3(k/m)x_{20}^2 - 2/3(k/m)Lx_1 - (k/m)x_1^2 + 4/3(k/m)x_1x_2 - \\ & 1/3(k/m)x_2^2 - 1/3v_1^2 + 2/3v_1v_2 \\ q_2 = {} & 2/3(k/m)Lx_{10} + (k/m)Lx_{20} - 1/3(k/m)x_{10}x_{20} - 1/6(k/m)x_{20}^2 - 2/3(k/m)Lx_1 - (k/m)Lx_2 + 1/3(k/m)x_1x_2 \\ & +1/6(k/m)x_2^2 + 1/6v_1^2 + 2/3v_1v_2 + 1/2v_2^2 . \end{aligned}$$

(A Gröbner basis of J consists of 4 polynomials whose lengthy description is omitted here.) One can check that, once fixed $k/m = L = 1$, for any instantiation of the variables x_{10} and x_{20} in J, the dimension of the resulting variety is ≤ 2, implying it represents a good over-approximation the resulting system trajectory. Once k/m and L have been eliminated, the system (19) becomes

$$\begin{aligned} -(x_{10} - 1/2)^2 - (x_{20} - 3/2)^2 + 1/4 \geq 0 \\ x_2 - x_1 - 2.17 \geq 0 \\ x_{10}^2 - 4/3x_{10}x_{20} + 1/3x_{20}^2 - x_1^2 + 4/3x_1x_2 - 1/3x_2^2 - 1/3v_1^2 + 2/3v_1v_2 + 2/3x_{10} - 2/3x_1 = 0 \\ -1/3x_{10}x_{20} - 1/6x_{20}^2 + 1/3x_1x_2 + 1/6x_2^2 + 1/6v_1^2 + 2/3v_1v_2 + 1/2v_2^2 + 2/3x_{10} + x_{20} - 2/3x_1 - x_2 = 0 . \end{aligned}$$

This algebraic system is proven to have no solutions: we give some details in Appendix D. Therefore, by virtue of Theorem 4, SA is safe.

We end the section by remarking that the verification method discussed so far easily extends to general semialgebraic sets. Indeed, let a continuous system $SA = (F, X_0, X_U)$ have $X_0 = \bigcup_i A_i$ and $X_U = \bigcup_j B_j$ as initial and unsafe set, respectively, where A_i, B_j are basic semialgebraic sets. Then safety of SA is equivalent to safety of each one of the basic systems $SA_{ij} = (F, A_i, B_j)$.

8. Discussion

We round off the technical development so far with a discussion on what novelties and benefits our approach actually delivers, also in relation to existing work. We shall focus on three aspects: extended systems, preconditions and polynomial invariants.

Extended systems and relational abstractions Our use of auxiliary variables and of extended systems $\hat{F}$ to handle semialgebraic safety problems in Section 7 appears to be strongly connected to *relational abstractions of* ODEs, introduced by Sankaranarayanan and Tiwari, see [35, Def. 5]. Expressed in our notation, a (timeless) relational abstraction for a system of ODEs $\dot{\mathbf{x}} = F$ (with $F \in \mathbb{R}[\mathbf{x}]^N$) is a relation $R \subseteq \mathbb{R}^N \times \mathbb{R}^N$ such that whenever $(v_0, v_1) \in R$ then, for some time $t_1 \in \mathbb{R}$, we have $v_1 = \mathbf{x}(t_1; v_0)$; recall that $\mathbf{x}(t; v_0)$ denotes the unique solution of the system from v_0. In other words, a relational abstraction over-approximates the set of possible transitions between states, abstracting away from time. Seeing that relational abstractions are infinite-state transition systems, one can apply to them known verification techniques for such systems, such as k-induction: this is elaborated in [35]. Now, consider the statement of our Theorem 3, and specifically the invariant ideal J mentioned there: the condition $\mathbf{V}(J) \supseteq \psi$ precisely says that $\mathbf{V}(J)$ is a relational abstraction – the argument showing this fact is in the proof of the theorem itself. As discussed in Section 7, J can be obtained by running the POST algorithm. Therefore POST can also be seen as a relatively complete method for computing algebraic relational abstractions.

Direct and generic approaches to preconditions Throughout the preceding sections, we have been emphasizing the important role played in our approach by preconditions ψ. Summing up, there are two distinct sensible ways one can make use of this information in conjunction with the POST algorithm.

1. *Direct approach*: use ψ directly as an argument of POST, and obtain an algebraic invariant $\mathbf{V}(J)$ containing the precondition from $(V, J) = \textsc{post}_F(\psi, \pi)$.
2. *Generic approach*: introduce new variables $x_0, y_0, \ldots$ and $\psi_0 = \mathbf{V}(\{x - x_0, y - y_0, \ldots\})$ to represent arbitrary initial conditions and compute a set of parametrized invariant ideals J by running $\textsc{post}_F(\psi_0, \pi)$. Then syntactically replace $x, y, \ldots$ by $x_0, y_0 \ldots$ in the description of the precondition ψ and add the resulting system of equations, representing the constraints on the initial conditions, to J.

[15] In practice, it is superfluous to introduce auxiliary copies of the constants $k/m, L$. The same is true for v_1, v_2: as their initial values is fixed by ψ, their auxiliary copies would be anyway eliminated from the final system (19).

Table 1
Classification of polynomials in invariant ideals.

Example	# 1st integrals	# 2nd integrals	# higher order integrals
Collision Avoidance	6	0	6
Airplane Vertical Motion	3	0	12
Kepler 1st Law	0	0	9
Kepler 2nd & 3rd Laws	0	1	1
3D Lotka-Volterra	2	0	0
Spring-mass System	2	0	2

The generic approach is basically how we have handled semialgebraic problems in Section 7. It is instructive to compare the two approaches on one and the same example. Let us reconsider the 3D Lotka-Volterra system of Example 6, where we have already applied the generic approach. Let us now apply the direct approach to this system. Introducing an extra slack variable e, and extending F with $\dot{e} = 0$, we can define the set of initial conditions as the algebraic variety $\psi \stackrel{\triangle}{=} \mathbf{V}(\{z-3, (x-2)^2+(y-2)^2+e^2-1.15^2\})$. Running POST with ψ and a complete template π of degree 3, after $m=3$ iterations and < 1 s we obtain $(V, J) = \text{POST}_F(\psi, \pi)$. The invariant ideal J is generated by the polynomial

$$q = xyz - (3/2)(e^2+x^2+y^2+z^2) - 3(xy+xz+yz) + 15(x+y+z) - 33213/800$$

As $J \subseteq I_\psi$ (Theorem 1(b)), we have $\psi \longrightarrow [F]\,\mathbf{V}(J)$, that is, the system's trajectories starting from ψ never leave $\mathbf{V}(J)$. To prove safety, it is then enough to check that $\mathbf{V}(J) \cap X_U = \emptyset$. Ultimately, this reduces to proving that the algebraic system $S = \{q = 0, (x-1/2)^2 + (y-5)^2 \leq 1.5^2\}$ has no real solutions, which can be readily checked to be the case via the same SOS programming technique[16] illustrated in Section 7. In this case, the direct approach leads to a gain in terms of execution time. This gain is mainly imputable to the smaller number of variables. Moreover, in this and other examples, starting from a specific precondition apparently leads to a faster convergence of POST. However, the direct approach often fails, as the smallest algebraic invariant including ψ is simply not precise enough (too large) to establish safety. This is the case with the spring-mass system of Example 7, as there is no nontrivial algebraic invariant including the given initial set.

The generic approach appears to be more effective at chasing invariants: informally, not just one, but a whole family of polynomial invariants can be captured at once, provided the family can be described parametrically with respect to a generic point $\mathbf{x}_0$. Note however that when the dependence from $\mathbf{x}_0$ is not parametric, and invariance only holds for certain values $\mathbf{x}_0$ may take on, the generic approach fails. For instance, the system $\{\dot{x} = 2x^2y - x, \dot{y} = 2xy^2 + y\}$ has both x and y as polynomial invariants for $(0,0)$: indeed e.g. $\dot{x} = (2xy-1)x$. However, neither is found using the generic approach. Vice-versa, both invariants are found using the direct approach, with the precondition $\psi = \{(0,0)\}$, the single point where the lines $x=0$ and $y=0$ intersect.

First-, second- and higher order integrals Consider an invariant ideal J, possibly found using POST, and any $q \in J$. If $\mathcal{L}(q) \in \left\langle \{q\} \right\rangle$, q is called a *Darboux* polynomial. An important special case of Darboux polynomials is when $\mathcal{L}(q) = 0$, which, in the language of mathematical physics, makes q a so-called *first integral* of the system. In our terminology, up the to an additive constant, first integrals coincide with polynomials that are invariants *for each* $v_0 \in \mathbb{R}^N$ in the sense of Definition 1. A Darboux polynomial which is not a first integral is also known as a *second integral* in mathematical physics. Polynomials of an invariant ideal other than Darboux are collectively designated as higher order integrals; see [16, Ch. 2]. Integrals of any order are important in applications, as the knowledge of any one of them decreases the number of *degrees of freedom* of the system — in our terminology, the dimension of the smallest algebraic variety including the system's trajectories. Finding all polynomial *first* integrals, up to a given degree, can be done quite easily using just templates and linear algebra: indeed, the constraints for the derivative of the parametric template to be the zero polynomial are always linear. Things get harder when one needs to compute second integrals and beyond. POST seamlessly computes polynomial integrals of any order up to a given degree. It is interesting to inspect the invariant ideals of the examples seen so far, and check how many polynomials, in the corresponding sets of generators, are computationally interesting, i.e. *not* first integrals. Table 1 displays how many integrals of each type have been found for each example by POST. In all considered cases, but Kepler's First Law, the set of generators is also a Gröbner basis. Appendix C presents the details of a higher order integral from the Collision Avoidance example.

9. Conclusion, further and related work

We have provided complete algorithms to compute relativized strongest postconditions for systems of polynomial ODEs. These algorithms can be used to check safety assertions, to discover complete sets of polynomial invariants that fit a given template, and to compute largest algebraic varieties of initial conditions making given polynomial invariants true (weakest preconditions). Effectiveness of the algorithms has been demonstrated on nontrivial systems, including semialgebraic ones.

[16] Or, in this simple case, by just feeding S to a computer algebra system.

Our previous work [6] deals with simple initial values problems, where the precondition ψ always consists of a singleton. This restriction prevents one from dealing with the most interesting continuous systems, such as semialgebraic systems. In particular, the concepts of weakest precondition is absent in [6]. The present paper lifts the algorithm of [6] to general (semi)algebraic systems. This requires considering a general algebraic precondition, described by a Gröbner basis G, rather than a singleton. Among the new technical ingredients necessary to make this extension work the following two are crucial: (a) the property that, under suitable conditions, reduction modulo G and substitution commute with each other (Lemma 3); (b) the use of auxiliary variables and generic initial conditions to circumvent the real radical problem (see e.g. Proposition 1 and Theorem 3). The method introduced in [6] has its roots in a line of research concerning weighted automata, bisimulation and Markov chains [4,3,5]. Also related to the present paper is [8], where we apply the notion of invariant ideal to the construction of linear abstractions of continuous systems.

The study of the safety of hybrid systems can be shown to reduce constructively to the problem of generating invariants for their differential equations [27]. Many authors have therefore focused on the effective generation of invariants of a special type. For example, Tiwari and Khanna consider invariant generation based on *syzygies* and Gröbner basis [39]. Sankaranarayanan [34] characterizes greatest invariants in terms of descending chains of ideals. This iteration does not always converge, thus a relaxation in terms of bounded-degree *pseudoideals* is considered: the resulting algorithm always converges, because pseudoideals form basically a descending chain of finite-dimensional vector spaces, and returns an invariant ideal, although with no guarantee of maximality [34, Th.4.1]. By contrast, the convergence of our algorithm Post is essentially based on the stabilization of ascending chains of ideals, with completeness guarantees. Matringe et al. encode invariants constraints using symbolic matrices [31].

Our work is closely related to Ghorbal and Platzer's [15], which gives a complete characterization of what it means for an algebraic set to be invariant for a polynomial ode. It is interesting to contrast the completeness statements in [15] and of that in the present paper with one another. [15] presents a method that, given a polynomial template and an integer $N \geq 1$, determines the largest subspace of template instantiations under which a length M chain of Lie derivatives forms an invariant. Any invariant can be reduced to this form, for suitably large M. In contrast, our Theorem 1, given a template *and* an algebraic variety ψ, determines the largest subspace of the template instantiations that are polynomial invariants for trajectories starting from ψ; moreover, it determines, via J, the largest invariant variety that includes ψ. Neither of these two statements is stronger or more general than the other. From our point of view, taking the initial set explicitly into account, as we do, has some advantages. First, invariants J returned by our method can be made explicitly dependent on initial conditions, via auxiliary variables, such as x_0, z_0, w_0, u_0, q_0 in the longitudinal airplane motion. As such, these invariants can be used *directly* within semialgebraic verification methods based on Positivstellensatz: as seen in Section 7, this amounts to proving the unsatisfiability of a set of polynomial (in)equations, also involving the auxiliary variables, corresponding to the initial set, to the polynomial invariants, and to the unsafe set. Second, knowing the precondition ψ, we are in effect confining ourselves to a subset of the algebraic invariants, those that involve points in ψ: this might explain the observed gain in efficiency — practically speaking, as the worst-case complexity is left unchanged. This gain is reflected in the execution times of [15] and of our algorithm, for the examples reported in Section 6. As a more general remark, we note that the computational ingredients of [15], such as minimization of the rank of a symbolic matrix (also employed in [31]), are quite different from ours. In the future, we would like to experimentally compare these two approaches on a more systematic basis than what we have done in the present paper.

The recent work of Kong et al. [17] considers generation of invariant clusters, again based on templates. Nonlinear constraints on template parameters are resolved via symbolic computation; safety for semialgebraic systems is reduced, via Positivstellensatz, to Sum-of-Squares (SOS) programming. In terms of effectiveness, this method appears to considerably improve previous techniques. Kong et al.'s approach has strong similarities with our method for semialgebraic systems. Rather than relying on clusters, we generate families of invariants via the introduction of auxiliary variables $\mathbf{x}_0$, denoting arbitrary points in the corresponding varieties. Differently from our approach, though, [17] does not offer completeness guarantees in our sense. In particular, the method of [17] only sometimes works with chains of ideals that stabilize after one step, that is Darboux polynomials. On the other hand, compared to theirs, our approach appears to be slower. It would be interesting to investigate if the more general invariants J returned by our algorithm could be fruitfully employed in the approach of [17].

Ideas from Algebraic Geometry have been fruitfully applied also in Program Analysis. Relevant to our work is Müller-Olm and Seidl's [22], where an algorithm to compute all polynomial invariants up to a given degree of an imperative program is provided. Similarly to what we do, they reduce the core problem to a linear algebraic one. However, since the setting in [22] is discrete rather than continuous, the techniques employed there are otherwise quite different, mainly because: (a) the construction of the ideal chain is driven by the program's operational semantics, rather than by Lie derivatives; (b) only the polynomial invariants satisfied by *all* initial program states are considered, which in a continuous setting would mostly lead to the trivial strongest postcondition. A perhaps more crucial difference is that, when computing invariants, [22] regards templates essentially as polynomials in $\mathbb{R}[\mathbf{x}, \mathbf{a}]$, rather than explicitly factoring out the template parameters $\mathbf{a}$. This can make the involved computations less efficient, as known algorithms for computing Gröbner bases have a complexity which is exponential in the number of variables.

Most of the material in this paper has been extended and revised from the conference paper [7]. With respect to [7], here we include the following additional material: proofs, the discussion on the expressive power of auxiliary variables in Section 4, the algorithmic presentation and the discussion on radical ideals in Section 5, the examples about collision avoidance and Kepler laws in Section 6, the extension to semialgebraic continuous systems in Section 7, and an extended and revised discussion of related works in Section 8 and in the present section.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

The author has benefited from stimulating discussions with Khalil Ghorbal.

Appendix A. A simple algorithm for weakest preconditions

Fix a vector field F. Let $\phi = \mathbf{V}(P)$ be a user specified postcondition, with $P \subseteq \mathbb{R}[\mathbf{x}]$ a finite set of polynomials. We define inductively the sets P_j, $j \geq 0$, as follows: $P_0 \stackrel{\triangle}{=} P$ and $P_{j+1} = \mathcal{L}(P_j)$. For $j \geq 0$, we let

$$I_j \stackrel{\triangle}{=} \left\langle\ \cup_{i=0}^{j} P_i\ \right\rangle. \tag{A.1}$$

Let m be the least integer such that $I_m = I_{m+1}$, which must exist as $I_0 \subseteq I_1 \subseteq \cdots$ forms an infinite ascending chains of ideals that must eventually stabilize. We let $\text{PRE}(\phi) \stackrel{\triangle}{=} I_m$. Note that the termination condition reduces to checking equality between two ideals, which can be effectively done (Section 2).

Theorem A.1 *(correctness and completeness of* PRE*). Let ϕ be an algebraic variety and $I = \text{PRE}(\phi)$. Then $\mathbf{V}(I) = \psi_\phi$.*

Proof. Let $\chi \stackrel{\triangle}{=} \mathbf{V}(I)$. It is easy to check that $I = \big\langle \{p^{(j)} : j \geq 0 \text{ and } p \in P\} \big\rangle$ and that I is an invariant ideal. By Lemma 5 then χ is an algebraic invariant of F, that is $\chi \longrightarrow [F]\,\chi$. Moreover, as $P \subseteq I$, $\phi \supseteq \chi$, hence $\chi \longrightarrow [F]\,\phi$. This shows that χ is a valid precondition of ϕ. We now show that it is actually the largest. Consider any ψ such that $\psi \longrightarrow [F]\,\phi$ and any $v_0 \in \psi$. This means that, for each $p \in I$, p is a polynomial invariant for v_0. That is (Lemma 2), for each $p \in I$ and $j \geq 0$, $p^{(j)}(v_0) = 0$. Therefore, $v_0 \in \mathbf{V}\big(\{p^{(j)} : j \geq 0 \text{ and } p \in P\}\big) = \mathbf{V}(I) = \chi$. □

Appendix B. Proofs of Section 4

Proof of Lemma 1. The function $p(t; v_0) = p(\mathbf{x}(t; v_0)$ of the real variable t is analytic in a neighborhood of 0. Hence it is identically 0 if and only if all of its derivatives, $\frac{d^j}{dt^j} p(t; v_0)$ for $j \geq 0$, vanish at $t = 0$. Then (5) and (4) establish the result. □

In the proof of the next lemma, we shall rely on the notion of monomial ordering [10, Ch.2,§2], which we introduce below.

Definition B.1 *(monomial ordering).* Let $k \geq 1$. A *monomial ordering* $>$ on $\mathbb{N}^k$ is a relation $>$ on $\mathbb{N}^k$ such that: (i) $>$ is a total order on $\mathbb{N}^k$; (ii) whenever $\boldsymbol{\alpha} > \boldsymbol{\beta}$ and $\boldsymbol{\gamma} \in \mathbb{N}^k$ then $\boldsymbol{\alpha} + \boldsymbol{\gamma} > \boldsymbol{\beta} + \boldsymbol{\gamma}$; (iii) $>$ is a well-ordering on $\mathbb{N}^k$: every nonempty subset of $\mathbb{N}^k$ has a smallest element under $>$.

Let $\mathbf{z} = (z_1, \ldots, z_k)$ be k distinct indeterminates. For $\boldsymbol{\alpha} \in \mathbb{N}^k$, let $\mathbf{z}^{\boldsymbol{\alpha}}$ denote the monomial $z_1^{\alpha_1} \cdots z_k^{\alpha_k}$. The monomial order $>$ is lifted to the set of monomials over $\mathbf{z}$ by letting $\mathbf{z}^{\boldsymbol{\alpha}} > \mathbf{z}^{\boldsymbol{\beta}}$ iff $\boldsymbol{\alpha} > \boldsymbol{\beta}$. In $\tau = \mathbf{z}^{\boldsymbol{\alpha}}$, $\boldsymbol{\alpha}$ is the *multidegree* of τ, denoted multideg(τ). The *leading term* of a polynomial $p \in \mathbb{R}[\mathbf{z}]$ is the monomial τ appearing in p of highest multidegree; then multideg$(p) =$ multideg(τ).

An example of monomial ordering is the *lexicographic order*: at the level of multidegrees, for $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_k)$ one lets $\boldsymbol{\alpha} >_{\text{lex}} \boldsymbol{\beta}$ if the leftmost nonzero entry of the vector difference $(\boldsymbol{\alpha} - \boldsymbol{\beta}) \in \mathbb{Z}^k$ is positive. One lets $\mathbf{z}^{\alpha} >_{\text{lex}} \mathbf{z}^{\beta}$ iff $\boldsymbol{\alpha} >_{\text{lex}} \boldsymbol{\beta}$. For instance, for $\mathbf{z} = (a_1, a_2, x, y)$, one has $a_1 x y >_{\text{lex}} x^3 y^2$.

Proof of Lemma 3. Consider the template π as an element of $\mathbb{R}[\mathbf{z}]$, for $\mathbf{z} \stackrel{\triangle}{=} \mathbf{a}, \mathbf{x} = (a_1, \ldots, a_n, x_1, \ldots, x_N)$. Note that, by our choice of a lexicographic order where $a_i > x_j$ for any i, j, we have for example, multideg$(a_i^2 x_j) >$ multideg$(a_i x_j^k)$, whatever $k \geq 0$.

Now let $r = \pi \bmod G$, where again $r \in \mathbb{R}[\mathbf{a}, \mathbf{x}]$. We first prove that r is a template as well, that is, the template parameters a_i can occur only linearly in r. By the properties of multivariate division [10, Ch.2,§3,Th.3], there is a $q = \sum_\ell h_\ell g_\ell$, with $h_\ell \in \mathbb{R}[\mathbf{a}, \mathbf{x}]$ and $g_\ell \in G$, such that

$$\pi = q + r\,. \tag{B.1}$$

Moreover, again by the same result: (a) $\mathrm{multideg}(\pi) \geq \mathrm{multideg}(q)$; (b) r is a linear combination of monomials, none of which is divisible by the leading term of any polynomial in G. Assume by contradiction there is in r a summand $\mu\tau$ ($0 \neq \mu \in \mathbb{R}$), where a template parameter a_i occurs in the monomial τ with a degree > 1. By the linearity of π in the template parameters in $\mathbf{a}$ and by (B.1), we deduce that $-\mu\tau$ must be a summand of q (seen as a linear combination of monomials), so that the two terms can cancel each other. We deduce that $\mathrm{multideg}(q) \geq \mathrm{multideg}(\tau)$. Hence, by (a) above and transitivity, $\mathrm{multideg}(\pi) \geq \mathrm{multideg}(\tau)$. But this is impossible: indeed, by the chosen lexicographic order, we must have $\mathrm{multideg}(\pi) < \mathrm{multideg}(\tau)$, because π is linear in all the template parameters in $\mathbf{a}$, whereas in τ the degree of a_i is ≥ 2.

Now, consider any $\lambda \in \mathbb{R}^n$. By (B.1) we have $\pi[\lambda] = q[\lambda] + r[\lambda]$. Clearly $q[\lambda] \in \langle G \rangle$, where $\langle G \rangle$ is here the ideal in $\mathbb{R}[\mathbf{x}]$ generated by G. Moreover, (b) above implies that none of the monomials in $r[\lambda]$ is divisible by the leading term of any polynomial in G. Since G is a Gröbner basis in $\mathbb{R}[\mathbf{x}]$, these two properties say that $r[\lambda]$ is the (unique) remainder of the division of $\pi[\lambda]$ by G: see e.g. [10, Ch.2,§6,Prop.1]. In other words, $\pi[\lambda] \bmod G = r[\lambda]$. □

Proof of Lemma 4. We proceed by induction on j. The base case $j = 1$ follows from the definition of m. Assuming by induction hypothesis that $V_m = \cdots = V_{m+j}$ and that $J_m = \cdots = J_{m+j}$, we prove now that $V_m = V_{m+j+1}$ and that $J_m = J_{m+j+1}$. The key to the proof is the following fact

$$\pi^{(m+j+1)}[\lambda] \in J_m \quad \text{for each } \lambda \in V_m \, . \tag{B.2}$$

From this fact the thesis will follow, indeed:

1. $V_m = V_{m+j+1}$. To see this, observe that for each $\lambda \in V_{m+j} = V_m$ (the equality here follows from the induction hypothesis), it follows from (B.2) that $\pi^{(m+j+1)}[\lambda]$ can be written as a finite sum of the form $\sum_l h_l \cdot \pi^{(j_l)}[u_l]$, with $0 \leq j_l \leq m$ and $u_l \in V_m$. For each $0 \leq j_l \leq m$, $\pi^{(j_l)}[u_l] \bmod G = 0$ by assumption, from which it easily follows that also $\pi^{(m+j+1)}[\lambda] \bmod G = \left(\sum_l h_l \cdot \pi^{(j_l)}[u_l]\right) \bmod G = 0$. This shows that $\lambda \in V_{m+j+1}$ and proves that $V_{m+j+1} \supseteq V_{m+j} = V_m$. The reverse inclusion is obvious;
2. $J_m = J_{m+j+1}$. As a consequence of $V_{m+j+1} = V_{m+j} (= V_m)$ (the previous point), we can write
$$\begin{aligned} J_{m+j+1} &= \left\langle \, \cup_{i=1}^{m+j} \pi^{(i)}[V_{m+j}] \cup \pi^{(m+j+1)}[V_{m+j}] \, \right\rangle \\ &= \left\langle \, J_{m+j} \cup \pi^{(m+j+1)}[V_{m+j}] \, \right\rangle \\ &= \left\langle \, J_m \cup \pi^{(m+j+1)}[V_m] \, \right\rangle \end{aligned}$$
where the last step follows by induction hypothesis. From (B.2), we have that $\pi^{(m+j+1)}[V_m] \subseteq J_m$, which implies the thesis for this case, as $\langle \, J_m \, \rangle = J_m$.

We prove now (B.2). Fix any $\lambda \in V_m$. First, note that $\pi^{(m+j+1)}[\lambda] = \mathcal{L}(\pi^{(m+j)}[\lambda])$ (here we are using (9)). As by induction hypothesis $\pi^{(m+j)}[V_m] = \pi^{(m+j)}[V_{m+j}] \subseteq J_{m+j} = J_m$, we have that $\pi^{(m+j)}[\lambda]$ can be written as a finite sum $\sum_l h_l \cdot \pi^{(j_l)}[u_l]$, with $0 \leq j_l \leq m$ and $u_l \in V_m$. Applying the rules of Lie derivatives (2), (3), we find that $\pi^{(m+j+1)}[\lambda] = \mathcal{L}(\pi^{(m+j)}[\lambda])$ equals

$$\sum_l \left(h_l \cdot \pi^{(j_l+1)}[u_l] + \mathcal{L}(h_l) \cdot \pi^{(j_l)}[u_l] \right) .$$

Now, for each u_l, $u_l \in V_m = V_{m+1}$, each term $\pi^{(j_l+1)}[u_l]$, with $0 \leq j_l + 1 \leq m+1$, is by definition in $J_{m+1} = J_m$. This proves that $\pi^{(m+j+1)}[V] \in J_m$, as required. □

Proof of Lemma 5. First assume that χ is an algebraic invariant. Take $J = \mathbf{I}(\chi)$. This is by definition an ideal. We show that J is invariant. Indeed, take any $v_0 \in \chi$ and $p \in J$: by hypothesis, $\mathbf{x}(t; v_0) \in \chi$, hence $p(t; v_0) = 0$, for each $t \in D_{v_0}$, that is p is a polynomial invariant for v_0. But, by Lemma 2, this is equivalent to $p^{(j)}(v_0) = 0$ for each $j \geq 0$, in particular, $p^{(1)}(v_0) = 0$. Since $v_0 \in \chi$ is arbitrary, $p^{(1)} \in J$. Since $p \in J$ is arbitrary, we have that J is an invariant ideal.

Conversely, assume that $\chi = \mathbf{V}(J)$ for J an invariant ideal. Of course χ is algebraic. We show that χ is invariant, that is that $\chi \longrightarrow [F]\, \chi$. Indeed, take any $v_0 \in \chi$ and $p \in J$: by hypothesis, $p^{(j)} \in J$ for each $j \geq 0$, hence $p^{(j)}(v_0) = 0$ for each j. Again by Lemma 2, this means that $p(t; v_0)$ is identically 0. Since $p \in J$ is arbitrary, this means that $\mathbf{x}(t; v_0) \in \chi$ for each $t \in D_{v_0}$. Since $v_0 \in \chi$ is arbitrary, we have that χ is an invariant. □

Proof of Theorem 2. Part (a) follows directly from Theorem 1(b) and Lemma 5.

Concerning part (b), let $\chi = \psi_\phi$, the weakest precondition (algebraic variety) for $\phi = \mathbf{V}(\pi[V])$. Let $(V', J') = \textsc{post}(\chi, \pi)$. We first prove that $\pi[V] = \pi[V']$. Indeed, one hand, by definition of I_χ we have that $\pi[V] \subseteq I_\chi$ and therefore: $\pi[V'] = \pi[\mathbb{R}^n] \cap I_\chi \supseteq \pi[V] \cap I_\chi = \pi[V]$, where the first equality comes from Theorem 1(a). On the other hand, $\psi \subseteq \chi$ by definition of χ, which implies $I_\chi \subseteq I_\psi$, therefore we have: $\pi[V] = \pi[\mathbb{R}^n] \cap I_\psi \supseteq \pi[\mathbb{R}^n] \cap I_\chi = \pi[V']$, where the first equality comes again from Theorem 1(a). Thus we have proved $\pi[V] = \pi[V']$. Now by Theorem 1(b) and $\pi[V] = \pi[V']$, we deduce that $J = J'$.

Now we prove that $\chi = \mathbf{V}(J)$. Since, by definition of I_χ, $\chi \longrightarrow [F]\mathbf{V}(I_\chi)$, we must have $\chi \subseteq \mathbf{V}(I_\chi)$; but $J = J' \subseteq I_\chi$ (again Theorem 1(b)), hence we have $\mathbf{V}(J) = \mathbf{V}(J') \supseteq \mathbf{V}(I_\chi) \supseteq \chi$, that is $\mathbf{V}(J) \supseteq \chi$. On the other hand, by part (a), $\mathbf{V}(J)$ is an algebraic invariant, that is $\mathbf{V}(J) \longrightarrow [F]\mathbf{V}(J)$; hence, since $\pi[V] \subseteq J$ and $\mathbf{V}(\pi[V]) \supseteq \mathbf{V}(J)$, we get $\mathbf{V}(J) \longrightarrow [F]\mathbf{V}(\pi[V]) = \phi$; the latter implies $\mathbf{V}(J) \subseteq \chi$, by definition of χ. In conclusion, $\chi = \mathbf{V}(J)$. □

Appendix C. Details for the collision avoidance example of Section 6

The following is a Gröbner basis of the invariant ideal J w.r.t. the lexicographic order induced by the following ordering of variables: $\omega_1 > \omega_2 > x_{10} > x_{20} > y_{10} > y_{20} > d_{10} > d_{20} > e_{10} > e_{20} > x_1 > x_2 > y_1 > y_2 > d_1 > d_2 > e_1 > e_2$.

$$\begin{aligned} G = \Big\{ & (x_{10})^2 d_{20} + (x_{20})^2 d_{20} - 2x_{10}d_{20}x_1 + d_{20}x_1^2 - 2x_{20}d_{20}x_2 + d_{20}x_2^2 - 2x_{10}x_{20}d_1 + 2x_{20}x_1d_1 + 2x_{10}x_2d_1 - \\ & \quad 2x_1x_2d_1 + (x_{10})^2 d_2 - (x_{20})^2 d_2 - 2x_{10}x_1d_2 + x_1^2 d_2 + 2x_{20}x_2d_2 - x_2^2 d_2, \\ & (y_{10})^2 e_{20} + (y_{20})^2 e_{20} - 2y_{10}e_{20}y_1 + e_{20}y_1^2 - 2y_{20}e_{20}y_2 + e_{20}y_2^2 - 2y_{10}y_{20}e_1 + 2y_{20}y_1e_1 + 2y_{10}y_2e_1 - \\ & \quad 2y_1y_2e_1 + (y_{10})^2 e_2 - (y_{20})^2 e_2 - 2y_{10}y_1e_2 + y_1^2 e_2 + 2y_{20}y_2e_2 - y_2^2 e_2, \\ & \omega_1 x_{10} - \omega_1 x_1 - d_{20} + d_2, \\ & \omega_1 x_{20} - \omega_1 x_2 + d_{10} - d_1, \\ & \omega_2 y_{10} - \omega_2 y_1 - e_{20} + e_2, \\ & \omega_2 y_{20} - \omega_2 y_2 + e_{10} - e_1, \\ & x_{10}d_{10} + x_{20}d_{20} - d_{10}x_1 - d_{20}x_2 - x_{10}d_1 + x_1d_1 - x_{20}d_2 + x_2d_2, \\ & x_{20}d_{10} - x_{10}d_{20} + d_{20}x_1 - d_{10}x_2 + x_{20}d_1 - x_2d_1 - x_{10}d_2 + x_1d_2, \\ & (d_{10})^2 + (d_{20})^2 - d_1^2 - d_2^2, \\ & y_{10}e_{10} + y_{20}e_{20} - e_{10}y_1 - e_{20}y_2 - y_{10}e_1 + y_1e_1 - y_{20}e_2 + y_2e_2, \\ & y_{20}e_{10} - y_{10}e_{20} + e_{20}y_1 - e_{10}y_2 + y_{20}e_1 - y_2e_1 - y_{10}e_2 + y_1e_2, \\ & (e_{10})^2 + (e_{20})^2 - e_1^2 - e_2^2 \ \Big\} \end{aligned}$$

Let p be the first polynomial listed in G above. Let us check that p is not a first integral. In fact, p is not even a Darboux polynomial. To see this, let us compute explicitly the Lie derivative of p

$$\begin{aligned} \mathcal{L}(p) = {} & \omega_1 x_{10}^2 d_1 - \omega_1 x_{20}^2 d_1 - 2\omega_1 x_{10}x_1d_1 + \omega_1 x_1^2 d_1 + 2\omega_1 x_{20}x_2d_1 - \omega_1 x_2^2 d_1 + 2\omega_1 x_{10}x_{20}d_2 - 2\omega_1 x_{20}x_1d_2 - \\ & 2\omega_1 x_{10}x_2d_2 + 2\omega_1 x_1x_2d_2 - 2x_{10}d_{20}d_1 + 2d_{20}x_1d_1 + 2x_{20}d_1^2 - 2x_2d_1^2 - 2x_{20}d_{20}d_2 + 2d_{20}x_2d_2 + 2x_{20}d_2^2 - \\ & 2x_2d_2^2. \end{aligned}$$

It is immediate to check that $\mathcal{L}(p) \notin \langle \{p\} \rangle$ with the help of a computer algebra system. This can also be checked manually, noting that $\{p\}$ is trivially a Gröbner basis of $\langle \{p\} \rangle$ w.r.t. the lexicographic order, and that $\mathcal{L}(p) \bmod \{p\} = \mathcal{L}(p)$. Indeed, the leading monomial of $\mathcal{L}(p)$, that is $\omega_1 x_{10}^2 d_1$, is not divisible by the leading monomial of p, that is $x_{10}^2 d_{20}$. The least m such that $p^{(m+1)} \in \langle \{p, p^{(1)}, \ldots, p^{(m)}\} \rangle$ is $m = 2$.

Appendix D. Proof of Theorem 4, Positivstellensatz and SOS programming in Section 7

Proof of Theorem 4. By contradiction, assume there are $w_0 \in X_0$ and $w_1 = \mathbf{x}(t_1; w_0) \in X_U$, for some $t_1 \in D_{w_0}$. We will show that $(w_0, w_1) \in \mathbb{R}^{2N}$ is a solution of (19), thus arriving at a contradiction. Indeed, by definition $g_i[\mathbf{x}_0/\mathbf{x}](w_0, w_1) = g_i(w_0) \geq 0$ and $h_j(w_0, w_1) = h_j(w_1) \geq 0$, for each $i = 1, \ldots, m$ and $j = 1, \ldots., n$. Consider now the trajectory of $\hat{F}$ originating from (w_0, w_0), that is $\hat{\mathbf{x}}(t; (w_0, w_0))$: note that, by definition of $\hat{F}$, $\hat{\mathbf{x}}(t; (w_0, w_0)) = (w_0, \mathbf{x}(t; w_0))$ for each $t \in D_{w_0}$. Now, since $\mathbf{V}(J) \supseteq \psi \supseteq (X_0 \times X_0) \cap Id$, we have $(w_0, w_0) \in \mathbf{V}(J)$, hence, by $\hat{F}$-invariance of J, $\hat{\mathbf{x}}(t; (w_0, w_0)) \in \mathbf{V}(J)$ for each $t \in D_{(w_0, w_0)}$ (Lemma 5). In particular, considering $t = t_1$, we have $\hat{\mathbf{x}}(t_1; (w_0, w_0)) = (w_0, \mathbf{x}(t_1; w_0)) = (w_0, w_1) \in \mathbf{V}(J)$. But this means $q_i(w_0, w_1) = 0$ for $i = 1, \ldots, k$. In conclusion, (w_0, w_1) is a solution of (19). □

When working in algebraically closed fields, like $\mathbb{C}$, Hilbert's Nullstellensatz [10] implies that a system of polynomial equations P has no solution if and only if $1 \in \sqrt{\langle P \rangle}$. This gives a simple criterion to check if P is solvable. The following result, often considered as the real algebraic counterpart of Hilbert's Nullstellensatz, is due to Stengle [38]. Let us introduce the necessary terminology. In what follows, all polynomials are in $\mathbb{R}[\mathbf{x}]$ for some fixed $\mathbf{x} = (x_1, \ldots, x_N)$. A polynomial s is a *Sum of Squares (SOS)* if $s = \sum_j h_j^2$, for some polynomials h_j. Given a finite set of polynomials $A = \{f_1, \dots, f_n\}$, the *cone* generated by A is $C(A) \overset{\triangle}{=} \{\sum_{\sigma \subseteq \{1,\dots,n\}} s_\sigma \Pi_{j \in \sigma} f_j \,:\, s_\sigma \text{ are SOS}\}$.

Theorem D.1 *(Positivstellensatz). Let $A = \{f_1, \dots, f_n\}$ and $B = \{g_1, \dots, g_m\}$ be two sets of polynomials. The system of (in)equations $\{f_1 \geq 0, \dots, f_n \geq 0,\ g_1 = 0, \dots, g_m = 0\}$ has no solution in $\mathbb{R}^N$ if and only if there are $f \in C(A)$ and $g \in \langle\, B \,\rangle$ such that $f + g + 1 = 0$.*

If one writes $f \in C(A)$ as $f = s_\emptyset + \sum_{\emptyset \neq \sigma \subseteq \{1,\dots,n\}} s_\sigma \Pi_{j \in \sigma} f_j$ and $g \in \langle\, B \,\rangle$ as $g = \sum_{i=1}^m h_i g_i$, then finding $f \in C(A)$ and $g \in \langle\, B \,\rangle$ such that $f + g + 1 = 0$ can be formulated as follows:

$$\text{Find polynomials } h_i\text{'s and SOS } s_\sigma\text{'s such that } -\left(\sum_{\emptyset \neq \sigma \subseteq \{1,\dots,n\}} s_\sigma \Pi_{j \in \sigma} f_j + \sum_{i=1}^m h_i g_i + 1 \right) \text{ is SOS.} \tag{D.1}$$

Now a polynomial s is SOS if and only if there is a vector of monomials $Z = (\alpha_1, \dots, \alpha_K)$ and a real symmetric positive semidefinite $K \times K$ matrix M such that $s = ZMZ^T$. Once bases of monomials have been fixed for each of the (unknown) polynomials s_σ and h_i, one can consider a relaxation of problem (D.1), whereby one searches for polynomials built from those bases satisfying (D.1) (empty bases are allowed). Problem (D.1) becomes in this way a *semidefinite programming problem* [25], with one variable for each (unknown) polynomial coefficient, and constraints given by the various positive semidefinite conditions and by the equation (D.1). In fact, there are tools, like SOSTOOLS [29], to efficiently convert relaxations of problem (D.1) into a semidefinite programming problem and then try to solve it via numerical techniques. If successful, the obtained SOS polynomial is a certificate of insolvability of the original system. Although the number of terms in (D.1) is potentially exponential in n, experience has shown that, in practice, this technique tends to yield short (low degree) certificates, if the original system is actually not solvable.

For the continuous semialgebraic systems in Examples 6 and 7, denoting by p_0, p_U the polynomials defining X_0 and X_U in each case, problem (D.1) takes the following concrete form

$$\text{Find } h_1, h_2 \text{ and SOS } s_1, s_2, s_3 \text{ such that } -(s_1 p_0 + s_2 p_U + s_3 p_0 p_U + h_1 q_1 + h_2 q_2 + 1) \text{ is SOS.} \tag{D.2}$$

For Example 6, fixing a maximum degree of 1 for the h_i's and of 2 for the s_σ's and running SOSTOOLS under Matlab[17] we solve (D.2), finding the following polynomials, which yield a low-degree certificate:

$$\begin{aligned}
s_1 &= 2.8733x^2 - 0.15408xx_0 - 0.6222xy - 0.11367xy_0 - 0.81927xz + 4.2254x_0^2 - 1.4885x_0y - 2.4633x_0y_0 - \\
&\quad 0.61469x_0z + 1.5901y^2 - 1.3772yy_0 - 1.4399yz + 4.071y_0^2 - 0.58541y_0z + 3.1195z^2 \\
s_2 &= 1.7131x^2 + 0.063147xx_0 - 0.33468xy + 0.074991xy0 + 0.17391xz + 1.2985x_0^2 - 0.51261x_0y + \\
&\quad 0.19351x_0y_0 + 0.15971x_0z + 0.5814y^2 - 0.53211yy_0 - 0.48663yz + 1.3512y_0^2 + 0.17931y_0z + 1.9153z^2 \\
s_3 &= 0 \\
h_1 &= 0.49855x + 0.21264x_0 - 0.29621y + 0.18602y_0 + 0.35564z + 14.8214 \\
h_2 &= 13.096x + 9.6921x_0 + 0.013631y - 36.2677y_0 + 22.7601z - 16.3507\,.
\end{aligned}$$

This takes about 0.4 s on a Core i5 machine under Windows 10. A certificate for Example 7 is found in a similar way; we omit here the lengthy description of the corresponding polynomials.

Remark D.1 *(dealing with roundoff errors).* It is important to ensure that the SOS decomposition found numerically actually corresponds to a true solution, and it is not the result of roundoff errors that may arise when working in floating point arithmetic. There are several ways of doing this: for instance, by computing exact rational solutions, that can be fully verified symbolically, or by tweaking the numerical coefficients of a candidate solution; see for instance [26,36]. In particular, the SOSTOOLS `findSOS` procedure incorporates an experimental `'rational'` option, that will try to produce an exact rational SOS representation of the input polynomial. Using this option, we have checked that the solution found for the Lotka-Volterra example is indeed SOS. On the other hand, the `'rational'` option fails to find a rational representation in the spring-mass example.

References

[1] V.I. Arnold, Ordinary Differential Equations, The MIT Press, ISBN 0-262-51018-9, 1978.

[17] Matlab scripts for both examples are available at https://github.com/micheleatunifi/postconditions/blob/master/SOSSafety.m.

[2] M.L. Blinov, J.R. Faeder, B. Goldstein, W.S. Hlavacek, BioNet-Gen: software for rule-based modeling of signal transduction based on the interactions of molecular domains, Bioinformatics 20 (17) (2004) 3289–3291.

[3] F. Bonchi, M.M. Bonsangue, M. Boreale, J.J.M.M. Rutten, A. Silva, A coalgebraic perspective on linear weighted automata, Inf. Comput. 211 (2012) 77–105.

[4] M. Boreale, Weighted bisimulation in linear algebraic form, in: CONCUR 2009, in: LNCS, vol. 5710, Springer, 2009, pp. 163–177.

[5] M. Boreale, Analysis of probabilistic systems via generating functions and Padé approximation, in: ICALP 2015 (2) 2015: 82–94, in: LNCS, vol. 9135, Springer, 2015, Extended version available as DiSIA working paper 2016/10, http://local.disia.unifi.it/wp_disia/2016/wp_disia_2016_10.pdf.

[6] M. Boreale, Algebra, coalgebra, and minimization in polynomial differential equations, in: Proc. of FoSSACS 2017, in: LNCS, vol. 10203, Springer, 2017, pp. 71–87, Full version in Log. Methods Comput. Sci. 15 (1) (2019).

[7] M. Boreale, Complete algorithms for algebraic strongest postconditions and weakest preconditions in polynomial ODEs, in: SOFSEM 2018: Theory and Practice of Computer Science - 44th International Conference on Current Trends in Theory and Practice of Computer Science, in: LNCS, vol. 10706, Springer, 2018, pp. 442–455.

[8] M. Boreale, Algorithms for exact and approximate linear abstractions of polynomial continuous systems, in: HSCC 2018, ACM, 2018, pp. 207–216.

[9] B. Buchberger, Theoretical basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bull. 10 (3) (1976) 19–29, https://doi.org/10.1145/1088216.1088219, ACM.

[10] D. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms an Introduction to Computational Algebraic Geometry and Commutative Algebra, Undergraduate Texts in Mathematics, Springer, 2007.

[11] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann, Singular 4-1-2 — a computer algebra system for polynomial computations, http://www.singular.uni-kl.de, 2019.

[12] M.S. El Din, Zhi-H. Yang, L. Zhi, On the complexity of computing real radicals of polynomial systems, in: ISSAC 2018, ACM, 2018, pp. 351–358.

[13] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases, J. Pure Appl. Algebra (ISSN 0022-4049) 139 (1) (1999) 61–88, https://doi.org/10.1016/S0022-4049(99)00005-5.

[14] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero, in: Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation (ISSAC), ACM, ISBN 978-1-58113-484-1, 2002, pp. 75–83.

[15] K. Ghorbal, A. Platzer, Characterizing algebraic invariants by differential radical invariants, in: TACAS 2014, in: LNCS, vol. 8413, 2014, pp. 279–294, Extended version available from http://reports-archive.adm.cs.cmu.edu/anon/2013/CMU-CS-13-129.pdf.

[16] A. Goriely, Integrability and Nonintegrability of Dynamical Systems, Advanced Series in Nonlinear Dynamics, vol. 19, World Scientific, 2001.

[17] H. Kong, S. Bogomolov, Ch. Schilling, Yu Jiang, Th.A. Henzinger, Safety verification of nonlinear hybrid systems based on invariant clusters, in: HSCC 2017, ACM, 2017, pp. 163–172.

[18] T. Krick, A. Logar, An algorithm for the computation of the radical of an ideal in the ring of polynomials, in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC 1991, in: LNCS, vol. 539, Springer, 1991, pp. 195–205.

[19] A.S. Laplagne, An algorithm for the computation of the radical of an ideal, in: Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computation, ISSAC 2006, ACM, 2006, pp. 191–195.

[20] J-B. Lasserre, M. Laurent, B. Mourrain, P. Rostalski, Ph. Trébuchet, Moment matrices, border bases and real radical computation, J. Symb. Comput. 51 (2013) 63–85.

[21] J. Liu, N. Zhan, H. Zhao, Computing semi-algebraic invariants for polynomial dynamical systems, in: EMSOFT, ACM, 2011, pp. 97–106.

[22] M. Müller-Olm, H. Seidl, Computing polynomial program invariants, Inf. Process. Lett. 91 (5) (2004) 233–244.

[23] R. Neuhaus, Computation of real radicals of polynomial ideals - II, J. Pure Appl. Algebra 124 (1–3) (1998) 261–280.

[24] D. Novikov, S. Yakovenko, Trajectories of polynomial vector fields and ascending chains of polynomial ideals, Ann. Inst. Fourier 49 (2) (1999) 563–609.

[25] P. Parrilo, Semidefinite programming relaxations for semialgebraic problems, Math. Program. 96 (2) (2003) 293–320.

[26] H. Peyrl, P.A. Parrilo, Computing sum of squares decompositions with rational coefficients, in: Theoretical Computer Science, vol. 409, Elsevier, 2008, pp. 269–281.

[27] A. Platzer, Logics of dynamical systems, in: LICS 2012, IEEE, 2012, pp. 13–24.

[28] A. Platzer, The structure of differential invariants and differential cut elimination, Log. Methods Comput. Sci. 8 (4) (2012) 1–38.

[29] S. Prajna, A. Papachristodoulou, P. Seiler, P. Parrilo, SOSTOOLS and its control applications, in: Positive Polynomials in Control, 2005, p. 580.

[30] G.R. Putland, A self-contained derivation of Kepler's laws from Newton's laws, https://www.grputland.com/2013/12/self-contained-derivation-of-keplers-laws-from-newtons-laws.html, 2013.

[31] R. Rebiha, A.V. Moura, N. Matringe, Generating invariants for non-linear hybrid systems, Theor. Comput. Sci. 594 (2015) 180–200.

[32] SageMath, free open-source mathematics software, http://www.sagemath.org/.

[33] S. Sankaranarayanan, H. Sipma, Z. Manna, Non-linear loop invariant generation using Gröbner bases, in: POPL 2004, ACM, 2004, pp. 318–329.

[34] S. Sankaranarayanan, Automatic invariant generation for hybrid systems using ideal fixed points, in: HSCC 2010, ACM, 2010, pp. 221–230.

[35] S. Sankaranarayanan, A. Tiwari, Relational abstractions for continuous and hybrid systems, in: CAV 2011, Springer, 2011, pp. 686–702.

[36] Z. She, D. Song, M. Li, Safety verification of hybrid systems using certified multiple Lyapunov-like functions, in: Computer Algebra in Scientific Computing - 17th International Workshop, CASC 2015, in: LNCS, vol. 9301, Springer, 2015, pp. 440–456.

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

[38] G. Stengle, A Nullstellensatz and a Positivstellensatz in Semialgebraic Geometry, Math. Ann. 207 (2) (1974) 87–97.

[39] A. Tiwari, G. Khanna, Nonlinear systems: approximating reach sets, in: HSCC 2004, ACM, 2004, pp. 600–614.

[40] M. Tribastone, S. Gilmore, J. Hillston, Scalable differential analysis of process algebra models, IEEE Trans. Software Eng. 38 (1) (2012) 205–219.