Computing Semi-algebraic Invariants for Polynomial Dynamical Systems *

Jiang Liu
State Key Lab. of Comp. Sci.
Institute of Software
Chinese Academy of Sciences
liuj@ios.ac.cn

Naijun Zhan
State Key Lab. of Comp. Sci.
Institute of Software
Chinese Academy of Sciences
znj@ios.ac.cn

Hengjun Zhao†
State Key Lab. of Comp. Sci.
Institute of Software
Chinese Academy of Sciences
zhaohj@ios.ac.cn

ABSTRACT

In this paper, we consider an extended concept of invariant for polynomial dynamical systems (PDSs) with domain and initial condition, and establish a sound and complete criterion for checking semi-algebraic invariants (SAIs) for such PDSs. The main idea is encoding relevant dynamical properties as conditions on the high order Lie derivatives of polynomials occurring in the SAI. A direct consequence of this criterion is a relatively complete method of SAI generation based on template assumption and semi-algebraic constraint solving. Relative completeness means if there is an SAI in the form of a predefined template, then our method can indeed find one.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*Algebraic algorithms*; D.2.4 [**Software Engineering**]: Software/Program Verification—*Formal methods*

General Terms

Theory, Verification

Keywords

Invariant, Semi-algebraic set, Polynomial dynamical system

1. INTRODUCTION

Hybrid systems are those systems involving both continuous evolutions and discrete transitions. How to design correct (desired) hybrid systems is a grand challenge in computer science and control theory. From a computer scientist's point of view, the main concern about hybrid systems up to now is to verify so-called safety properties. A safety property claims that some unsafe state is never reachable from any initial state along with any trajectory of the system.

1.1 Motivation

Directly computing the reachable set is a natural way to address this issue. As we know, there are two well-developed techniques for computing reachable set so far, that is, techniques based on model-checking [5, 23] and the decision procedure of Tarski algebra [29], respectively. However, the former technique requires the decidability and therefore can only be applied to some simple hybrid systems, e.g. timed automata [2], multirate automata [1], rectangular automata [22, 11], and so on. Comparably speaking, the latter technique has a wider scope of applications. For example, in [14] how to compute reachable sets for three classes of special linear hybrid systems are investigated. However, this technique heavily depends on whether the explicit solutions of the considered differential equations are or can be reduced to polynomials. So, this approach can not be applied to general linear hybrid systems, let alone nonlinear systems.

To deal with more complicated systems, recently, a deductive method has been established and successfully applied in practice [18, 19], which can be seen as a generalization of the so-called Floyd-Hoare-Naur inductive assertion method. Inductive assertion method is thought to be the dominant method for the verification of sequential programs. To generalize the inductive method to hybrid systems, a logic similar to Hoare logic which can deal with continuous dynamics is necessary. For example, differential-algebraic dynamic logic [17] due to Platzer was invented by extending dynamic logic with continuous statements. Recently, Liu et al [15] had another effort by extending Hoare logic to hybrid systems for the same purpose.

The most challenging part of the inductive method is how to discover invariants of hybrid systems. An invariant is a property that holds at all reachable states from any initial state that satisfies this property. If we can get invariants that are strong enough to imply the safety property to be verified, then we succeed in safety verification without solving differential equations, while differential equations have to be exactly solved or approximated in the methods via directly computing reachable sets. In particular, if the term expressions of a hybrid system are or can be reduced to polynomials, the so-called *inductive invariants* [26] can be effectively generated using the constraint-based approach [9].

The key issue in generating inductive invariants of a hy-

*This work is supported in part by the projects NSFC-91018012, NSFC-60970031, NSFC-60736017.

†Corresponding author: No. 4 South Fourth Street, Zhong Guan Cun, Beijing, 100190, P.R. China, zhaohj@ios.ac.cn

EMSOFT'11, October 9–14, 2011, Taipei, Taiwan.

brid system is to deal with continuous dynamics, i.e. to generate continuous invariants of the continuous evolution at each location (mode) of the hybrid system. A location (mode) of a hybrid system is usually represented by a *continuous dynamical system with domain and initial condition* (CDSwDI for short) of the form $(H, \mathbf{f}, \Xi)$, where $\mathbf{f}$ is a vector field, H is a domain restriction of continuous evolution, and $\Xi \subseteq H$ is a set of initial states. A property φ is called a *continuous invariant* (CI for short) of $(H, \mathbf{f}, \Xi)$, if it is always satisfied along any trajectory whose starting point satisfies φ, as long as the trajectory still remains in domain H. For φ to be a CI of $(H, \mathbf{f}, \Xi)$, the more complex the forms of H, $\mathbf{f}$, Ξ and φ are, the more intricate constraints should be induced accordingly. A global (discrete) inductive invariant of a hybrid system consists of a set of CIs such that: the initial condition of the initial location (mode) entails the CI of the initial location, and if there is a discrete transition between two locations of the system, then the CI at the pre-location implies the CI at the post-location w.r.t. the discrete transition. There are many methods, e.g. [32], for certifying and generating global inductive invariants of a system by using the global inductiveness. Therefore in this paper we only focus on how to generate CI at a single location (mode), i.e. a CDSwDI.

1.2 Related Work

In the literature, lots of efforts have been made towards algebraic or semi-algebraic continuous invariants generation for polynomial dynamical systems, even though CI may have different synonyms.

The generation of algebraic invariants, i.e. sets defined by polynomial equations are usually based on the theory of ideals in polynomial ring. In [26], to handle continuous differential equations, two strong continuous consecution conditions are imposed on the predefined templates, and then the two conditions are encoded as ideal membership statements. The work in [24] showed that the set of algebraic invariants of a linear system, which forms a polynomial ideal, is computable. The above two approaches both use *Gröbner bases* computation. An efficient technique that computes algebraic invariants as the greatest fixed point of a monotone operator over *pseudo ideals* was presented in [25].

As for the polynomial inequality case, to guarantee that $p \geq 0$ is a CI of a PDS $(H, \mathbf{f}, \Xi)$, it is useful to analyze the direction of $\mathbf{f}$ with regard to the set $p \geq 0$. In [20, 21], the authors proposed the notion *barrier certificates* for safety verification of hybrid systems. A polynomial p could be a barrier certificate if the unsafe region is included in $p < 0$, and at any point in $p = 0$, $\mathbf{f}$ points (strictly) inwards the set $p \geq 0$. Such polynomial barrier certificates can be effectively computed using sum of squares decomposition and semi-definite programming. In [9] a similar idea is adopted and by reducing the conditions of CIs to semi-algebraic constraints, continuous invariants that are boolean combinations of polynomial equations and inequalities can be generated. Unfortunately, the approaches in [20, 9] were discovered in [28, 27, 17] to have certain problems with their soundness, if at the boundary of a CI, $\mathbf{f}$ is not strictly inward the invariant set. In [18] the authors proposed the notion of *differential invariant* and the principle of differential induction. Basically, $p \geq 0$ is a differential invariant of $(H, \mathbf{f}, \Xi)$ if at any point in H, the directional derivative of p in the direction of $\mathbf{f}$ is non-negative. Such requirement is strong, but provide a sound and effective way of generating complex semi-algebraic continuous invariants.

1.3 Our Contribution

The problem of checking inductiveness for continuous dynamical systems was considered in [28] and [27]. Therein various sound checking rules are presented, which are also complete for classes of continuous invariants, e.g. linear, quadratic, convex and smooth invariants. The authors even proposed a sound and relatively complete rule using higher order *Lie derivatives*, which is quite similar to ours. However, in their relatively complete rule there are infinitely many candidate tests and thus is computationally infeasible. Our work in this paper actually resolves this problem and completes the gap left open in [28, 27]

The relative completeness of our method means that for a given PDS, if there is an SAI of the predefined template, then our method can indeed discover one. Thus, there are two advantages with our approach comparing with the well-established approaches: firstly, more general SAIs can be generated; secondly, a by-product of the completeness of our approach is that whether a given semi-algebraic set is really an SAI of a given PDS is decidable. This is quite useful in the interplay of discrete invariant generation (global) and CI generation (local).

1.4 Paper Organization

The rest of this paper is organized as follows. Section 2 presents some basic notions and fundamental theories on algebraic geometry and dynamical system. Section 3 gives a formal definition of the SAI generation problem. In Section 4, we prove the fundamental results based on which our method is developed. Section 5 illustrates the basic idea of our approach in simple cases. How to apply our approach to general cases is investigated in Section 6. Two case studies are given in Section 7. Section 8 concludes this paper with a discussion of future work.

2. PRELIMINARIES

In this section, we will recall some basic notions.

2.1 Polynomial Ideal Theory

Let $\mathbb{K}$ be an algebraic field and $\mathbb{K}[x_1, \ldots, x_n]$ denote the polynomial ring with coefficients in $\mathbb{K}$. In this paper, $\mathbb{K}$ will be taken as the rational number field $\mathbb{Q}$. Customarily, let $\mathbf{x}$ denote the n-tuple $(x_1, \cdots, x_n)$ with $\dim(\mathbf{x}) = n$, and a polynomial in $\mathbb{Q}[x_1, \ldots, x_n]$ ($\mathbb{Q}[\mathbf{x}]$ for short) may be written as $p(\mathbf{x})$ or p simply. A parametric polynomial

$$p(\mathbf{u}, \mathbf{x}) \in \mathbb{Q}[u_1, u_2, \ldots, u_t, x_1, x_2, \ldots, x_n]$$

is called a *template*, where $\mathbf{x}$ are variables taking values from $\mathbb{R}^n$ and $\mathbf{u}$ are coefficient parameters taking values from $\mathbb{R}^t$. Given $\mathbf{u}_0 \in \mathbb{R}^t$, we call the polynomial $p_{\mathbf{u}_0}(\mathbf{x})$ resulted by substituting $\mathbf{u}_0$ for $\mathbf{u}$ in $p(\mathbf{u}, \mathbf{x})$ an *instantiation* of $p(\mathbf{u}, \mathbf{x})$.

In what follows, we recall the theory of polynomial ideal (refer to [6]).

DEFINITION 1. *A subset $I \subseteq \mathbb{K}[\mathbf{x}]$ is called an* ideal *if*

i) $0 \in I$.

ii) *If* $p(\mathbf{x}), g(\mathbf{x}) \in I$, *then* $p(\mathbf{x}) + g(\mathbf{x}) \in I$.

iii) *If* $p(\mathbf{x}) \in I$ *and* $h(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$, *then* $p(\mathbf{x})h(\mathbf{x}) \in I$.

It is easy to check that if $p_1, \cdots, p_k \in \mathbb{K}[\mathbf{x}]$, then

$$\langle p_1, \cdots, p_k \rangle = \{\sum_{i=1}^{k} p_i h_i \mid \forall i \in [1,k].\, h_i \in \mathbb{K}[\mathbf{x}]\}$$

is an ideal. In general, we say an ideal I is *generated* by polynomials $g_1, \ldots, g_k \in \mathbb{K}[\mathbf{x}]$ if $I = \langle g_1, \ldots, g_k \rangle$, and $\{g_1, \ldots, g_k\}$ is called a set of *generators* of I.

THEOREM 2 (HILBERT BASIS THEOREM). *Every ideal $I \subseteq \mathbb{K}[\mathbf{x}]$ has a finite generating set. That is, $I = \langle g_1, \ldots, g_k \rangle$ for some $g_1, \ldots, g_k \in \mathbb{K}[\mathbf{x}]$.*

For its proof, please refer to [6]. Based upon this result, it is easy to see that

THEOREM 3 (ASCENDING CHAIN CONDITION). *For any ascending chain*

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_\ell \subseteq \cdots$$

of ideals in polynomial ring $\mathbb{K}[\mathbf{x}]$, there must be N such that for all $\ell \geq N$, $I_\ell = I_N$.

2.2 Semi-algebraic Set

An atomic polynomial formula over variables $x_1, x_2, \ldots, x_n$ is $p \triangleright 0$, where p is a polynomial in $\mathbb{Q}[\mathbf{x}]$ and $\triangleright \in \{\geq, >, \leq, <, =, \neq\}$. A quantifier free polynomial formula is a boolean combination of atomic polynomial formulas using connectives $\vee, \wedge, \neg, \Rightarrow$, etc.

DEFINITION 4 (SEMI-ALGEBRAIC SET). *A subset S of $\mathbb{R}^n$ is called a semi-algebraic set, if there is a quantifier free polynomial formula φ s.t.*

$$S = \{\mathbf{x} \in \mathbb{R}^n \mid \varphi(\mathbf{x}) \ \textit{is true}\} \ .$$

We will use $\mathcal{S}(\varphi)$ to denote the semi-algebraic set defined by a quantifier free polynomial formula φ. It is easy to check that any semi-algebraic set can be transformed into the form

$$\mathcal{S}(\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} p_{ij} \triangleright 0), \text{ where } \triangleright \in \{\geq, >\} \ .$$

Note that semi-algebraic sets are closed under basic set operations, since

- $\mathcal{S}(\varphi_1) \cap \mathcal{S}(\varphi_2) = \mathcal{S}(\varphi_1 \wedge \varphi_2)$;
- $\mathcal{S}(\varphi_1) \cup \mathcal{S}(\varphi_2) = \mathcal{S}(\varphi_1 \vee \varphi_2)$;
- $\mathcal{S}(\varphi_1)^c = \mathcal{S}(\neg\varphi_1)$;
- $\mathcal{S}(\varphi_1) \setminus \mathcal{S}(\varphi_2) = \mathcal{S}(\varphi_1) \cap \mathcal{S}(\varphi_2)^c = \mathcal{S}(\varphi_1 \wedge \neg\varphi_2)$,

where A^c and $A \setminus B$ stand for the complement and subtraction operation of sets respectively.

2.3 Continuous Dynamical System

We recall the theory of continuous dynamical systems in the following. Please refer to [12] for details.

2.3.1 Trajectories of Continuous Dynamical System

An autonomous *continuous dynamical system* (CDS) is modeled by first-order ordinary differential equations

$$\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x}) \ , \tag{1}$$

where $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{f}$ is a vector function from $\mathbb{R}^n$ to $\mathbb{R}^n$, which is also called a *vector field* in $\mathbb{R}^n$.

If $\mathbf{f}$ satisfies the *local Lipschitz condition*, then given $\mathbf{x}_0 \in \mathbb{R}^n$, there exists a unique solution $\mathbf{x}(\mathbf{x}_0; t)$ of (1) defined on (a, b) with $a < 0 < b$ s.t.

$$\forall t \in (a,b).\, \frac{\mathrm{d}\mathbf{x}(\mathbf{x}_0, t)}{\mathrm{d}t} = \mathbf{f}(\mathbf{x}(\mathbf{x}_0; t)) \quad \text{and} \quad \mathbf{x}(\mathbf{x}_0; 0) = \mathbf{x}_0.$$

When $\mathbf{x}_0$ is clear from the context, we just write $\mathbf{x}(\mathbf{x}_0; t)$ as $\mathbf{x}(t)$. Based upon this, we shall use the following useful notions for our discussion in the sequel.

DEFINITION 5 (TRAJECTORY). *Suppose $\mathbf{x}(\mathbf{x}_0; t)$ is the solution to (1) defined on (a, b) with $a < 0 < b$, as stated above. Then*

- *$\mathbf{x}(\mathbf{x}_0; t)$ ($\mathbf{x}(t)$ for short) defined on $[0, b)$ is called the trajectory of (1) starting from $\mathbf{x}_0$;*
- *$\mathbf{x}(\mathbf{x}_0; -t)$ ($\mathbf{x}(-t)$ for short) defined on $[0, -a)$, resulted by substituting $-t$ for t in $\mathbf{x}(\mathbf{x}_0; t)$, is called the inverse trajectory of (1) starting from $\mathbf{x}_0$.*

2.3.2 Polynomial Vector Field and Lie Derivatives

In this paper, we focus on vector fields defined by polynomials.

DEFINITION 6 (POLYNOMIAL VECTOR FIELD). *Suppose $\mathbf{f} = (f_1, f_2, \cdots, f_n)$ in (1). If for all $1 \leq i \leq n$, f_i is a polynomial in $\mathbb{Q}[x_1, x_2, \ldots, x_n]$, then $\mathbf{f}$ is called a polynomial vector field, denoted by $\mathbf{f} \in \mathbb{Q}^n[\mathbf{x}]$.*

Obviously polynomial vector fields satisfy the local Lipschitz condition. Let p be a polynomial in ring $\mathbb{Q}[\mathbf{x}]$, which is a scalar function. Then the gradient of p :

$$\frac{\partial}{\partial \mathbf{x}} p \mathrel{\widehat{=}} (\frac{\partial p}{\partial x_1}, \frac{\partial p}{\partial x_2}, \cdots, \frac{\partial p}{\partial x_n})$$

is a vector of polynomials with dimension $\dim(\mathbf{x})$. Thus the inner product of a polynomial vector field $\mathbf{f}$ and the gradient of a polynomial p is still a polynomial, if $\mathbf{f} \in \mathbb{Q}^n[\mathbf{x}]$ and $\dim(\mathbf{x}) = n$ (in the rest of the paper, this will be assumed implicitly). Therefore we can inductively define the *Lie derivatives* of p along $\mathbf{f}$, $L_{\mathbf{f}}^k p : \mathbb{R}^n \to \mathbb{R}$, for $k \in \mathbb{N}$, as follows:

- $L_{\mathbf{f}}^0 p(\mathbf{x}) = p(\mathbf{x})$,
- $L_{\mathbf{f}}^k p(\mathbf{x}) = (\frac{\partial}{\partial \mathbf{x}} L_{\mathbf{f}}^{k-1} p(\mathbf{x}), \mathbf{f}(\mathbf{x}))$, for $k > 0$,

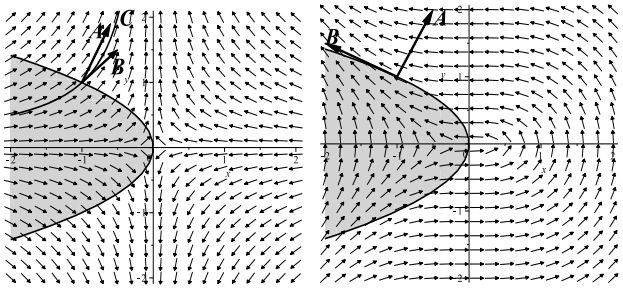
where $(\cdot, \cdot)$ is the inner product of two vectors, that is, $(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^{n} a_i b_i$ for $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$.

EXAMPLE 7. *Suppose $\mathbf{f} = (-x, y)$ and $p(x, y) = x + y^2$, then*

$$\begin{aligned} L_{\mathbf{f}}^0 p &= x + y^2 \\ L_{\mathbf{f}}^1 p &= -x + 2y^2 \\ L_{\mathbf{f}}^2 p &= x + 4y^2 \\ &\vdots \end{aligned}$$

For a parametric polynomial $p(\mathbf{u}, \mathbf{x})$, we can define the Lie derivatives of p along $\mathbf{f}$ similarly if the gradient of $p(\mathbf{u}, \mathbf{x})$ is taken as $\frac{\partial}{\partial \mathbf{x}} p(\mathbf{u}, \mathbf{x})$, and all $L_{\mathbf{f}}^i p(\mathbf{u}, \mathbf{x})$ are still parametric polynomials.

Given a polynomial vector field, we can make use of Lie derivatives to investigate the tendency of its trajectory in terms of a polynomial p (as an energy function). To capture this, look at Example 7 shown in I of Figure 1.



I: 1-order Lie Derivative and Gradient II: Demand for High Order Lie Derivative

Figure 1: Lie Derivatives

In I of Figure 1, vector B denote the corresponding evolution direction according to the vector field $\mathbf{f} = (-x, y)$, and we could imagine the points on the parabola $p(x, y) = x + y^2$ with zero energy, and the points in white area have positive energy, i.e., $p(x, y) > 0$. Vector A is the gradient $\frac{\partial}{\partial \mathbf{x}} p|_{(-1,1)}$ of $p(x, y)$, which infers that the trajectory starting at $(-1, 1)$ will enter white area immediately if the angle, between $\frac{\partial}{\partial \mathbf{x}} p|_{(-1,1)}$ and the evolution direction at $(-1, 1)$, is less than $\frac{\pi}{2}$, that is, the 1-order Lie derivative is positive. Thus the 1-order Lie derivative $L^1_{\mathbf{f}} p|_{(-1,1)} = 3$ of p along $\mathbf{f}$ (the inner product of $\frac{\partial}{\partial \mathbf{x}} p|_{(-1,1)}$ and $\mathbf{f}(x, y)|_{(-1,1)}$) predicts that there is some positive $d > 0$ such that the trajectory starting at $(-1, 1)$ (curve C) has the property $p(\mathbf{x}((-1, 1), t)) > 0$ for all $t \in (0, d)$.

However, if the angle between gradient and evolution direction is $\frac{\pi}{2}$ or the gradient is zero-vector, then 1-order Lie derivative is zero and it is impossible to predict trajectory tendency by means of 1-order Lie derivative. In this case, we resort to nonzero higher order Lie derivatives. For this purpose, we introduce the *pointwise rank* of p with respect to $\mathbf{f}$ as the function $\gamma_{p,\mathbf{f}} : \mathbb{R}^n \to \mathbb{N} \cup \{\infty\}$ defined by

$$\gamma_{p,\mathbf{f}}(\mathbf{x}) = \min\{k \in \mathbb{N} \mid L^k_{\mathbf{f}} p(\mathbf{x}) \neq 0\},$$

if such k exists, otherwise $\gamma_{p,\mathbf{f}}(\mathbf{x}) = \infty$.

EXAMPLE 8. *Let* $\mathbf{f}(x, y) = (\dot{x} = -2y, \dot{y} = x^2)$ *and* $h(x, y) = x + y^2$, *then*

$$\begin{aligned} L^0_{\mathbf{f}} h(x, y) &= x + y^2 \\ L^1_{\mathbf{f}} h(x, y) &= -2y + 2x^2 y \\ L^2_{\mathbf{f}} h(x, y) &= -8y^2 x - (2 - 2x^2)x^2 \\ &\vdots \end{aligned}$$

Here, $\gamma_{h,\mathbf{f}}(0, 0) = \infty$, $\gamma_{h,\mathbf{f}}(-4, 2) = 1$, *etc.*

Look at II of Figure 1. At point $(-1, 1)$ *on curve* $h(x, y) = 0$, *the gradient of* h *is* $(1, 2)$ *(vector A) and the evolution direction is* $(-2, 1)$ *(vector B), so their inner product is zero. Thus it is impossible to predict the tendency (in terms of curve* $h(x, y) = 0$*) of trajectory starting from* $(-1, 1)$ *via its 1-order Lie derivative. By a simple computation, its 2-order Lie derivative is* 8. *Hence* $\gamma_{h,\mathbf{f}}(-1, 1) = 2$. *In the sequel, we shall show how to use such high order Lie derivatives to analyze the trajectory tendency.*

For analyzing trajectory tendency by high order Lie derivatives, we need the following fact.

PROPOSITION 9. *Given polynomial functions* p *and* $\mathbf{f}$, *then* $\mathbf{x}_0$ *is on the boundary* $\mathcal{S}(p(\mathbf{x}) = 0)$ *if and only if* $\gamma_{p,\mathbf{f}}(\mathbf{x}_0) \neq 0$. *Suppose* $\mathbf{x}_0 = \mathbf{x}(0)$, *then it follows that*

(a) if $\gamma_{p,\mathbf{f}}(\mathbf{x}_0) < \infty$ *and* $L^{\gamma_{p,\mathbf{f}}(\mathbf{x}_0)}_{\mathbf{f}} p(\mathbf{x}_0) > 0$, *then*

$$\exists \epsilon > 0, \forall t \in (0, \epsilon). p(\mathbf{x}(t)) > 0;$$

(b) if $\gamma_{p,\mathbf{f}}(\mathbf{x}_0) < \infty$ *and* $L^{\gamma_{p,\mathbf{f}}(\mathbf{x}_0)}_{\mathbf{f}} p(\mathbf{x}_0) < 0$, *then*

$$\exists \epsilon > 0, \forall t \in (0, \epsilon). p(\mathbf{x}(t)) < 0;$$

(c) if $\gamma_{p,\mathbf{f}}(\mathbf{x}_0) = \infty$, *then*

$$\exists \epsilon > 0, \forall t \in (0, \epsilon). p(\mathbf{x}(t)) = 0.$$

PROOF. Polynomial functions are analytic, so $\mathbf{f}$ is analytic and thus $\mathbf{x}(t)$ is analytic in a small interval (a, b) containing zero [30]. Besides, p is analytic, so the Taylor expansion of $p(\mathbf{x}(t))$ at $t = 0$

$$\begin{aligned} p(\mathbf{x}(t)) &= p(\mathbf{x}_0) + \frac{\mathrm{d}p}{\mathrm{d}t} \cdot t + \frac{\mathrm{d}^2 p}{\mathrm{d}t^2} \cdot \frac{t^2}{2!} + \cdots \\ &= L^0_{\mathbf{f}} p(\mathbf{x}_0) + L^1_{\mathbf{f}} p(\mathbf{x}_0) \cdot t + L^2_{\mathbf{f}} p(\mathbf{x}_0) \cdot \frac{t^2}{2!} + \cdots \quad (2) \end{aligned}$$

converges in another small interval (a', b') containing zero [13]. Then the conclusion of Proposition 9 follows immediately from formula (2) by case analysis on the sign of $L^{\gamma_{p,\mathbf{f}}(\mathbf{x}_0)}_{\mathbf{f}} p(\mathbf{x}_0)$. □

Based on this proposition, we introduce the notion of *transverse set* to indicate the tendency of the trajectories of a considered polynomial vector field in terms of the first nonzero Lie derivative of a underlying polynomial as follows.

DEFINITION 10. *Given a polynomial* p *and a polynomial vector field* $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$, *the transverse set of* $\mathbf{f}$ *over the domain* $\mathcal{S}(p(\mathbf{x}) \geq 0)$ *is*

$$Trans_{\mathbf{f}\uparrow p} \widehat{=} \{\mathbf{x} \in \mathbb{R}^n \mid \gamma_{p,\mathbf{f}}(\mathbf{x}) < \infty \wedge L^{\gamma_{p,\mathbf{f}}(\mathbf{x})}_{\mathbf{f}} p(\mathbf{x}) < 0\}.$$

Intuitively, if $\mathbf{x} \in Trans_{\mathbf{f}\uparrow p}$, then either $\mathbf{x}$ is not in $\mathcal{S}(p(\mathbf{x}) \geq 0)$ or $\mathbf{x}$ is on the boundary of $\mathcal{S}(p(\mathbf{x}) \geq 0)$ such that the trajectory $\mathbf{x}(t)$ starting with $\mathbf{x}$ will exit $\mathcal{S}(p(\mathbf{x}) \geq 0)$ immediately.

3. SEMI-ALGEBRAIC INVARIANT

A hybrid system consists of a set of CDSs, a set of jumps between these CDSs, and a set of initial states. The CDSs in a hybrid system are a little different from the standard ones, as normally they are equipped with a domain and a set of initial states, in the form $(H, \mathbf{f}, \Xi)$, where H is used to force some jumps outgoing the mode to happen, that is, a hybrid system can stay within a mode only if the domain of the current mode holds, and Ξ is a subset of H, standing for the set of initial states. Obviously, a CDS can be seen as a special CDSwDI by letting $H = \mathbb{R}^n$. The goal of this paper is to present a relatively complete method for automatically discovering SAIs of PDSs, based on which, as we discussed in the introduction, we can finally verify polynomial hybrid systems.

3.1 Continuous Invariants of CDSwDI

The notion of *continuous invariant* of CDSwDI is quite similar to the one of positive invariant set of CDS [3]. Informally, a continuous invariant P of a CDwDI $(H, \mathbf{f}, \Xi)$ is a superset of Ξ such that all continuous evolutions starting from $P \cap H$ keep within P if they are within H. Here, we give a formal definition of CI adapted from [18] as follows:

DEFINITION 11 (CONTINUOUS INVARIANT [18]). *Given a CDSwDI $(H, \mathbf{f}, \Xi)$ with $\Xi \subseteq H \subseteq \mathbb{R}^n$ and $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$ that is locally Lipschitz continuous, a set $P \subseteq \mathbb{R}^n$ is called a* continuous invariant *of $(H, \mathbf{f}, \Xi)$, if*

1. *$\Xi \subseteq P$; and*
2. *for all $\mathbf{x}_0 \in P$, and for any $T \geq 0$,*

$$(\forall t \in [0, T].\mathbf{x}(\mathbf{x}_0; t) \in H) \Rightarrow (\forall t \in [0, T].\mathbf{x}(\mathbf{x}_0; t) \in P).$$

Regarding Definition 11, we would like to give the following remarks.

1. Continuous invariant in Definition 11 is more general than standard positive invariant set of continuous dynamical systems. However, if $H = \mathbb{R}^n$ and $\Xi = P$, then the two notions coincide.
2. One may have noticed that in Definition 11, a continuous invariant set P is not necessarily a subset of domain H. In fact, any P satisfying $H \subseteq P$ is a continuous invariant of $(H, \mathbf{f}, \Xi)$. This seems weird at first sight, because such continuous invariant sets are useless if we only concern the CDSwDI in isolation. However, it would be quite useful in the verification of a hybrid system if we assume that the continuous invariant of a mode always holds when the hybrid system does not stay within the mode.

3.2 PDS and SAI

DEFINITION 12. *A CDSwDI $(H, \mathbf{f}, \Xi)$ is called a polynomial dynamical system with semi-algebraic domain and initial condition (PDS), if H and Ξ are semi-algebraic sets and $\mathbf{f}$ is a polynomial vector field.*

A continuous invariant of a PDS is called a semi-algebraic invariant *(SAI) if it is a semi-algebraic set.*

In the subsequent sections, we will present a sound and relatively complete method to automatically discover SAIs for a PDS.

4. FUNDAMENTAL RESULTS

The set $Trans_{\mathbf{f}\uparrow p}$ in Definition 10 plays a crucial role in our theory. First of all, we have

THEOREM 13. *The set $Trans_{\mathbf{f}\uparrow p}$ is a semi-algebraic set if p is a polynomial and $\mathbf{f}$ is a polynomial vector field, and hence it is computable.*

To prove this theorem, it suffices to show $\gamma_{p,\mathbf{f}}(\mathbf{x})$ is computable for each $\mathbf{x} \in \mathbb{R}^n$. However, $\gamma_{p,\mathbf{f}}(\mathbf{x})$ may be infinite for some $\mathbf{x}$. Thus, it seems that we have to compute $L^k_{\mathbf{f}} p(\mathbf{x})$ infinite times for such $\mathbf{x}$ to determine if $\mathbf{x} \in Trans_{\mathbf{f}\uparrow p}$. Fortunately, we can find a uniform upper bound on $\gamma_{p,\mathbf{f}}(\mathbf{x})$ for all $\mathbf{x}$ with $\gamma_{p,\mathbf{f}}(\mathbf{x})$ being finite.

THEOREM 14 (RANK THEOREM). *If p and $\mathbf{f}$ are polynomial functions, then there is an integer N such that for all $\mathbf{x} \in \mathbb{R}^n$, $\gamma_{p,\mathbf{f}}(\mathbf{x}) < \infty$ implies $\gamma_{p,\mathbf{f}}(\mathbf{x}) \leq N$. Later on, such an N is called the rank of p and $\mathbf{f}$, denoted by $\gamma_{p,\mathbf{f}}$.*

PROOF. Let $D_l = \{\mathbf{x} \mid \forall m < l. L^m_{\mathbf{f}} p(\mathbf{x}) = 0\}$ for $l \geq 0$. Note that the sequence $\{D_l\}_{l \in \mathbb{N}}$ is decreasing. We will show that there is an N such that $D_l = D_N$ for all $l \geq N$.

Since p and $\mathbf{f}$ are polynomial functions, all $L^m_{\mathbf{f}} p(\mathbf{x})$ must be polynomials for any $m \in \mathbb{N}$. We consider the polynomial ideal I generated by $\{L^m_{\mathbf{f}} p(\mathbf{x}) \mid m \in \mathbb{N}\}$. Let $I_m = \langle L^0_{\mathbf{f}} p(\mathbf{x}), L^1_{\mathbf{f}} p(\mathbf{x}), \cdots, L^m_{\mathbf{f}} p(\mathbf{x})\rangle$. Then $I = \cup_m I_n$. By Theorem 3, there is k such that $I = I_k$. Thus for all $l > k$, there are $g_i \in \mathbb{R}[x_1, \cdots, x_n]$ for $i \leq k$ such that $L^l_{\mathbf{f}} p(\mathbf{x}) = \sum_{i \leq k} g_i L^i_{\mathbf{f}} p(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^n$.

Fix $l > k$. If $\mathbf{x} \in D_l$, then $L^l_{\mathbf{f}} p(\mathbf{x}) = \sum_{i \leq k} g_i L^i_{\mathbf{f}} p(\mathbf{x}) = 0$ since all $L^i_{\mathbf{f}} p(\mathbf{x}) = 0$ for $i \leq k$ as $\mathbf{x} \in D_l$. Let $N = k + 1$. Then $D_l = D_N$ for all $l \geq N$. Thus, if $\mathbf{x} \in D_N$ then $\gamma_{p,\mathbf{f}}(\mathbf{x}) = \infty$. Therefore, $\gamma_{p,\mathbf{f}}(\mathbf{x}) < \infty$ implies $\gamma_{p,\mathbf{f}}(\mathbf{x}) \leq N$. □

Now, it suffices to compute the values

$$L^0_{\mathbf{f}} p(\mathbf{x}_0), L^1_{\mathbf{f}} p(\mathbf{x}_0) \cdots, L^{\gamma_{p,\mathbf{f}}}_{\mathbf{f}} p(\mathbf{x}_0)$$

to determine whether $\gamma_{p,\mathbf{f}}(\mathbf{x}_0)$ is infinite. Therefore if $\gamma_{p,\mathbf{f}}$ is computable then $Trans_{\mathbf{f}\uparrow p}$ is computable too. It is desirable to get an expression of $\gamma_{p,\mathbf{f}}$ for given p and $\mathbf{f}$. However, we did not find it yet. Nevertheless, a computable upper bound for $\gamma_{p,\mathbf{f}}$ can indeed be found effectively according to the following theorem.

THEOREM 15 (FIXED POINT THEOREM). *If*

$$L^{i+1}_{\mathbf{f}} p \in \langle L^0_{\mathbf{f}} p, L^1_{\mathbf{f}} p, \cdots, L^i_{\mathbf{f}} p\rangle,$$

then $L^m_{\mathbf{f}} p \in \langle L^0_{\mathbf{f}} p, L^1_{\mathbf{f}} p, \cdots, L^i_{\mathbf{f}} p\rangle$, for all $m > i$.

PROOF. We prove this theorem by induction. Assume this conclusion is true for all $l \leq k$ with $k > i$. Especially, $L^k_{\mathbf{f}} p \in \langle L^0_{\mathbf{f}} p, L^1_{\mathbf{f}} p, \cdots, L^i_{\mathbf{f}} p\rangle$. Then there are $g_j \in \mathbb{R}[x_1, \cdots, x_n]$ for $j \leq i$ such that

$$L^k_{\mathbf{f}} p = \sum_{j \leq i} g_j L^j_{\mathbf{f}} p. \tag{3}$$

By the definition of Lie derivative and equation (3), it follows that

$$\begin{aligned}
&L^{k+1}_{\mathbf{f}} p \\
&= (\frac{\partial}{\partial \mathbf{x}} L^k_{\mathbf{f}} p, \mathbf{f}) \\
&= (\frac{\partial}{\partial \mathbf{x}} (\sum_{j \leq i} g_j L^j_{\mathbf{f}} p), \mathbf{f}) \\
&= \sum_{j \leq i} (L^j_{\mathbf{f}} p \frac{\partial}{\partial \mathbf{x}} g_j, \mathbf{f}) + \sum_{j \leq i} (g_j \frac{\partial}{\partial \mathbf{x}} L^j_{\mathbf{f}} p, \mathbf{f}) \\
&= \sum_{j \leq i} (\frac{\partial}{\partial \mathbf{x}} g_j, \mathbf{f}) L^j_{\mathbf{f}} p + \sum_{j \leq i} g_j L^{j+1}_{\mathbf{f}} p \\
&= \sum_{j \leq i} (\frac{\partial}{\partial \mathbf{x}} g_j, \mathbf{f}) L^j_{\mathbf{f}} p + \sum_{j < i} g_j L^{j+1}_{\mathbf{f}} p + g_i L^{i+1}_{\mathbf{f}} p.
\end{aligned}$$

By induction hypothesis, $L^{i+1}_{\mathbf{f}} p$ is in $\langle L^0_{\mathbf{f}} p, L^1_{\mathbf{f}} p, \cdots, L^i_{\mathbf{f}} p\rangle$. So

$$L^{k+1}_{\mathbf{f}} p \in \langle L^0_{\mathbf{f}} p, L^1_{\mathbf{f}} p, \cdots, L^i_{\mathbf{f}} p\rangle.$$

By induction, the theorem follows immediately. □

Let $N_{p,\mathbf{f}}$ be the minimal i satisfying the condition of Theorem 15 in the sequel. Then $\gamma_{p,\mathbf{f}} \leq N_{p,\mathbf{f}}$. We can compute $N_{p,\mathbf{f}}$ by solving the *ideal membership* problem using Gröbner bases [6]. For Example 8, we can get $N_{h,\mathbf{f}} = 2$. Now, applying above two theorems we can prove Theorem 13.

PROOF OF THEOREM 13. Since $\gamma_{p,\mathbf{f}} \leq N_{p,\mathbf{f}}$,

$$\mathbf{x} \in Trans_{\mathbf{f}\uparrow p} \text{ iff } \gamma_{p,\mathbf{f}}(\mathbf{x}) \leq N_{p,\mathbf{f}} \wedge L_{\mathbf{f}}^{\gamma_{p,\mathbf{f}}(\mathbf{x})} p(\mathbf{x}) < 0.$$

Therefore, $Trans_{\mathbf{f}\uparrow p}$ is computable as $N_{p,\mathbf{f}}$ is computable according to Theorem 15. Given p and $\mathbf{f}$, let

$$\pi^{(0)}(p,\mathbf{f},\mathbf{x}) \widehat{=}\ p(\mathbf{x}) < 0,$$

for $1 \leq i \in \mathbb{N}$,

$$\pi^{(i)}(p,\mathbf{f},\mathbf{x}) \widehat{=}\ \left(\bigwedge_{0\leq j<i} L_{\mathbf{f}}^{j} p(\mathbf{x}) = 0\right) \wedge L_{\mathbf{f}}^{i} p(\mathbf{x}) < 0,$$

and

$$\pi(p,\mathbf{f},\mathbf{x}) \quad \widehat{=} \quad \bigvee_{0\leq i\leq N_{p,\mathbf{f}}} \pi^{(i)}(p,\mathbf{f},\mathbf{x}).$$

By Theorem 14 and $\gamma_{p,\mathbf{f}} \leq N_{p,\mathbf{f}}$, we have another equivalence

$$\mathbf{x} \in Trans_{\mathbf{f}\uparrow p} \text{ iff } \pi(p,\mathbf{f},\mathbf{x}) \text{holds}. \tag{4}$$

In fact, $\pi^{(i)}(p,\mathbf{f},\mathbf{x})$ here is a particular semi-algebraic system, and so $\pi(p,\mathbf{f},\mathbf{x})$ is a union of semi-algebraic systems. Thus $Trans_{\mathbf{f}\uparrow p}$ is actually a semi-algebraic set. □

In the SAI generation, it actually makes use of parametric polynomials $p(\mathbf{u},\mathbf{x})$ with parameters $\mathbf{u} = (u_1, u_2, \ldots, u_t)$. The following theorem indicates Theorem 14 still holds after substituting $p(\mathbf{u},\mathbf{x})$ for $p(\mathbf{x})$.

THEOREM 16 (PARAMETRIC RANK THEOREM). *Given polynomial functions $p(\mathbf{u},\mathbf{x})$ and $\mathbf{f}$, there is an integer N such that $\gamma_{p_{\mathbf{u}_0},\mathbf{f}}(\mathbf{x}) < \infty$ implies $\gamma_{p_{\mathbf{u}_0},\mathbf{f}}(\mathbf{x}) \leq N$ for all $\mathbf{x} \in \mathbb{R}^n$ and all $\mathbf{u}_0 \in \mathbb{R}^t$.*

This proof is quite close to the one of Theorem 14. The difference, between the proof of this theorem and the one of Theorem 14, lies in the settings of polynomials. Here, we consider polynomials p and $\mathbf{f}$ in the polynomial ring $\mathbb{Q}[\mathbf{u},\mathbf{x}]$. Similarly, we also introduce the rank function on polynomials with parameters, still denoted by $\gamma_{p,\mathbf{f}}$. Accordingly, let $N_{p,\mathbf{f}}$ denote the upper bound computed by a similarity of Theorem 15 .

5. GENERATING SAI IN SIMPLE CASE

Given a polynomial vector field $\dot{\mathbf{x}} = \mathbf{f}(\mathbf{x})$ with a semi-algebraic domain H and initial condition Ξ, our task is to find a semi-algebraic set P such that P is an SAI of $(H,\mathbf{f},\Xi)$.

First of all, we illustrate our idea by showing how to compute an SAI of the simple form $P \widehat{=} p(\mathbf{x}) \geq 0$ for a simple domain $H \widehat{=} h(\mathbf{x}) \geq 0$. For convenience, we will simply write PDS $(h(\mathbf{x}) \geq 0, \mathbf{f}, \Xi)$ as $(h,\mathbf{f},\Xi)$. Notice that P is an SAI of $(h,\mathbf{f},\Xi)$ only if $\forall\mathbf{x}(\Xi(\mathbf{x}) \Rightarrow P(\mathbf{x}))$. It is evident that if $\mathbf{x}(0)$ is in the interior of $\mathcal{S}(p(\mathbf{x}) \geq 0) \cap \mathcal{S}(h(\mathbf{x}) \geq 0)$, then the trajectory $\mathbf{x}(t)$ starting at $\mathbf{x}(0)$ will remain in the interior within adequately small $t > 0$. Therefore, the condition of continuous invariant could be violated only at the points on the boundary $\mathcal{S}(p(\mathbf{x}) = 0)$ of $\mathcal{S}(p(\mathbf{x}) \geq 0)$. Thus by Definition 10 and Proposition 9, $p \geq 0$ is an invariant of $(h,\mathbf{f},\Xi)$ if and only if it meets $\forall\mathbf{x}(\Xi(\mathbf{x}) \Rightarrow P(\mathbf{x}))$ and

$$\mathbf{x} \in \mathcal{S}(p(\mathbf{x}) = 0) \Rightarrow \mathbf{x} \notin Trans_{\mathbf{f}\uparrow p} \setminus Trans_{\mathbf{f}\uparrow h},$$

i.e.

$$\mathbf{x} \in \mathcal{S}(p(\mathbf{x}) = 0) \Rightarrow \mathbf{x} \in (Trans_{\mathbf{f}\uparrow p})^c \cup Trans_{\mathbf{f}\uparrow h}. \tag{5}$$

By equivalences (4), the formula (5) is equivalent to

$$p(\mathbf{x}) = 0 \Rightarrow (\neg\pi(p,\mathbf{f},\mathbf{x}) \vee \pi(h,\mathbf{f},\mathbf{x})),$$

i.e.

$$\big(p(\mathbf{x}) = 0 \wedge \pi(p,\mathbf{f},\mathbf{x})\big) \Rightarrow \pi(h,\mathbf{f},\mathbf{x}). \tag{6}$$

Let $\theta(h,p,\mathbf{f},\mathbf{x})$ denote the formula (6). According to this equivalence, we obtain the sufficient and necessary condition for P being an SAI as follows.

THEOREM 17 (CRITERION THEOREM). *Given a polynomial p, $p(\mathbf{x}) \geq 0$ is an SAI of PDS $(h,\mathbf{f},\Xi)$ if and only if the formula $\theta(h,p,\mathbf{f},\mathbf{x}) \wedge (\Xi(\mathbf{x}) \Rightarrow p(\mathbf{x}) \geq 0)$ is true for all $\mathbf{x} \in \mathbb{R}^n$.*

Now, we are ready to present a constraint based method for generating polynomial continuous invariants. The basic idea is as follows:

I. First, set a parametric polynomial p of degree d as

$$p(\mathbf{u},\mathbf{x}) \widehat{=} \sum_{i_1+i_2+\cdots+i_n=k\leq d} u_{i_1 i_2\cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Such a parametric polynomial is called a *template* conventionally. There are $t = \binom{n+d}{d}$ many terms and accordingly t many parameters $u_{i_1 i_2\cdots i_n}$. For simplicity, let $\mathbf{u}$ denote such a t-tuple $\{u_{i_1 i_2\cdots i_n}\}_{i_1+i_2+\cdots+i_n=k\leq d}$.

II. Then we appy the quantifier elimination (QE[1] for short) to the formula $\forall\mathbf{x}.(\theta(h,p,\mathbf{f},\mathbf{x}) \wedge (\Xi(\mathbf{x}) \Rightarrow p(\mathbf{x}) \geq 0))$. If the output is *false*, then there is no polynomial continuous invariant of degree $\leq d$ for $(h,\mathbf{f},\Xi)$. Otherwise, it will give us a constraint on $\mathbf{u}$, denoted by $R(\mathbf{u})$. In fact, $R(\mathbf{u})$ is a union of semi-algebraic systems (refer to [29]).

III. Let S_{Inv} be the set of solutions to $R(\mathbf{u})$. Now, using a tool like DISCOVERER [31] to pick a $\mathbf{u}_0 \in S_{Inv}$ and then $p_{\mathbf{u}_0}(\mathbf{x}) \geq 0$ is a continuous invariant of $(h,\mathbf{f},\Xi)$ by Theorem 17.

Remark

1) Note that in real applications, one usually picks up the specific terms with nonzero coefficients. A simplified template could make the resulted polynomial satisfy special conditions and also reduce the complexity of the searching process.

2) In the above Step III, if the dimension of S_{Inv} equals t, then we can easily select a rational sample point $\mathbf{u}_0$ from S_{Inv} and the obtained $p_{\mathbf{u}_0}(\mathbf{x}) \geq 0$ is an SAI in $\mathbb{R}^n$; otherwise when it is difficult (or impossible) to get a rational instantiation for $\mathbf{u}$, we can always compute an algebraic sample point $\mathbf{u}_0 \in S_{Inv}$, that is, $\mathbf{u}_0$ is itself

[1]QE has been implemented in many computer algebra tools such as DISCOVERER [31], QEPCAD [4] and Redlog [8].

defined by polynomial equations. It is easy to show that in the latter case, $p_{\mathbf{u}_0}(\mathbf{x}) \geq 0$ is also an SAI in $\mathbb{R}^n$.

EXAMPLE 18. *Again, we make use of Example 8 to demonstrate above method. That is,* $\mathbf{f}(x,y)\widehat{=}(\dot{x} = -2y, \dot{y} = x^2)$. *Here, we take*

$$H\widehat{=}\{(x,y) \in \mathbb{R}^2 \mid h(x,y) = -x - y^2 \geq 0\}$$

as the domain and

$$\Xi\widehat{=}\{(-1, 0.5), (-0.5, -0.6)\}$$

as the initial states. Apply procedure (I-III), we have:

1. *Set a template* $p(\mathbf{u},\mathbf{x}) := ay(x-y) \geq 0$ *where* $\mathbf{u}\widehat{=}\langle a\rangle$. *Then we have* $\gamma_{p,\mathbf{f}} \leq N_{p,\mathbf{f}} = 2$.

2. *Compute the corresponding formula*

$$\begin{array}{rcl}\theta(h,p,\mathbf{f},\mathbf{x}) & \widehat{=} & p = 0 \wedge (\pi^{(0)}_{p,\mathbf{f},\mathbf{x}} \vee \pi^{(1)}_{p,\mathbf{f},\mathbf{x}} \vee \pi^{(2)}_{p,\mathbf{f},\mathbf{x}}) \Rightarrow \\ & & (\pi^{(0)}_{h,\mathbf{f},\mathbf{x}} \vee \pi^{(1)}_{h,\mathbf{f},\mathbf{x}} \vee \pi^{(2)}_{h,\mathbf{f},\mathbf{x}})\end{array}$$

where

$$\begin{array}{rcl}\pi^{(0)}_{h,\mathbf{f},\mathbf{x}} & \widehat{=} & -x - y^2 < 0, \\ \pi^{(1)}_{h,\mathbf{f},\mathbf{x}} & \widehat{=} & -x - y^2 = 0 \wedge 2y - 2x^2 y < 0, \\ \pi^{(2)}_{h,\mathbf{f},\mathbf{x}} & \widehat{=} & -x - y^2 = 0 \wedge 2y - 2x^2 y = 0 \wedge \\ & & 8xy^2 + 2x^2 - 2x^4 < 0, \\ \pi^{(0)}_{p,\mathbf{f},\mathbf{x}} & \widehat{=} & ay(x-y) < 0, \\ \pi^{(1)}_{p,\mathbf{f},\mathbf{x}} & \widehat{=} & ay(x-y) = 0 \wedge -2ay^2 + ax^3 - 2yax^2 < 0, \\ \pi^{(2)}_{p,\mathbf{f},\mathbf{x}} & \widehat{=} & ay(x-y) = 0 \wedge -2ay^2 + ax^3 - 2yax^2 = 0 \\ & & \wedge\, 40axy^2 - 16ay^3 + 32ax^3 y - 10ax^4 < 0.\end{array}$$

Then we apply quantifier elimination to formula

$$\forall x, y \left(\begin{array}{l} \theta(h,p,\mathbf{f},\mathbf{x}) \wedge 0.5a(-1-0.5) \geq 0 \wedge \\ -0.6a(-0.5+0.6) \geq 0 \end{array} \right) .$$

It results that the constraint on a *is* $a \leq 0$.

3. *Just pick* $a = -1$, *and then* $-xy + y^2 \geq 0$ *is a continuous invariant for* $(H,\mathbf{f},\Xi)$. *The grey part of the picture III is the intersection of this invariant and domain* H.

6. GENERAL CASE

Now, we consider how to automatically discover SAIs of a PDS in general case. Given a PDS $(H,\mathbf{f},\Xi)$ with

$$H = \mathcal{S}(\bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i} p_{ij}(\mathbf{x}) \triangleright 0),\ \Xi = \mathcal{S}(\bigvee_{i=1}^{N}\bigwedge_{j=1}^{M_i} q_{ij}(\mathbf{x}) \triangleright 0) \quad (7)$$

and $\mathbf{f} \in \mathbb{Q}^n[\mathbf{x}]$, where $\Xi \subseteq H$ and $\triangleright \in \{\geq, >\}$. The procedure of automatically generating SAIs with a general template

$$P = \mathcal{S}(\bigvee_{k=1}^{K}\bigwedge_{l=1}^{L_k} p_{kl}(\mathbf{u}_{kl},\mathbf{x}) \triangleright 0)\ ,\ \text{where} \triangleright \in \{\geq, >\}$$

for $(H,\mathbf{f},\Xi)$, is essentially the same as the steps (I-III) depicted in the previous section. However, we must sophisticatedly handle the complex combinations due to the complicated boundaries. In what follows, we shall outline our main results without giving strict proofs due to page limit. Please refer to [16] for details.

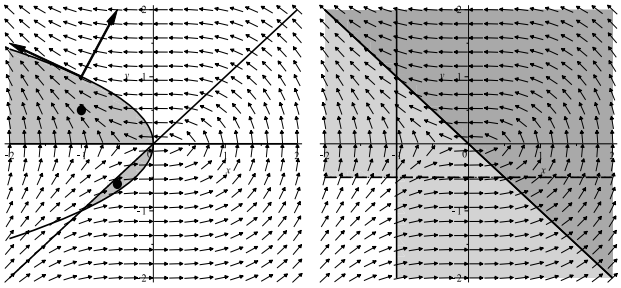


Figure 2: Semi-Algebraic Invariants

6.1 Necessary-Sufficient Condition for CI

First of all, we study a necessary and sufficient condition like formula (5) for P being a CI of $(H,\mathbf{f},\Xi)$. To analyze the evolution tendency of trajectories dominated by a locally Lipschitz continuous vector field $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$ in terms of a subset A of $\mathbb{R}^n$, we need the following notions and notations.

$$\begin{array}{c}\mathrm{In}_{\mathbf{f}}(A)\widehat{=}\{\mathbf{x}_0 \in \mathbb{R}^n \mid \exists\epsilon > 0 \forall t \in (0,\epsilon).\, \mathbf{x}(\mathbf{x}_0;t) \in A\}, \\ \mathrm{IvIn}_{\mathbf{f}}(A)\widehat{=}\{\mathbf{x}_0 \in \mathbb{R}^n \mid \exists\epsilon > 0 \forall t \in (0,\epsilon).\, \mathbf{x}(\mathbf{x}_0;-t) \in A\}.\end{array}$$

Intuitively, $\mathbf{x}_0 \in \mathrm{In}_{\mathbf{f}}(A)$ means that the trajectory starting from $\mathbf{x}_0$ enters A immediately and keeps inside A for certain positive time; $\mathbf{x}_0 \in \mathrm{IvIn}_{\mathbf{f}}(A)$ means that the trajectory through $\mathbf{x}_0$ reaches $\mathbf{x}_0$ from the interior of A. According to the notion of CI, we can prove

THEOREM 19. *Given a CDSwDI* $(H,\mathbf{f},\Xi)$ *with* $H \subseteq \mathbb{R}^n$ *and locally Lipschitz continuous* $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$, *a subset* P *of* $\mathbb{R}^n$ *is a CI of* $(H,\mathbf{f},\Xi)$ *if and only if*

1. $\Xi \subseteq P$;
2. $\forall \mathbf{x} \in P \cap H \cap \mathrm{In}_{\mathbf{f}}(H).\, \mathbf{x} \in \mathrm{In}_{\mathbf{f}}(P)$;
3. $\forall \mathbf{x} \in P^c \cap H \cap \mathrm{IvIn}_{\mathbf{f}}(H).\, \mathbf{x} \in \big(\mathrm{IvIn}_{\mathbf{f}}(P)\big)^c$.

6.2 Necessary-Sufficient Condition for SAI

Given a PDS $(H,\mathbf{f},\Xi)$ and an SAI P, to encode the conditions in Theorem 19 as polynomial formulas, it is sufficient to show that $\mathrm{In}_{\mathbf{f}}(H)$, $\mathrm{In}_{\mathbf{f}}(P)$, $\mathrm{IvIn}_{\mathbf{f}}(H)$ and $\mathrm{IvIn}_{\mathbf{f}}(P)$ are all semi-algebraic sets. By the structure of H, it is natural to consider the relation between $\mathrm{In}_{\mathbf{f}}(H)$ and $\mathrm{In}_{\mathbf{f}}\big(\mathcal{S}(p_{ij} \triangleright 0)\big)$. Through a careful analysis, we establish the following crucial equality:

LEMMA 20. *For a semi-algebraic set* H *defined by formula (7) and a polynomial vector field* $\mathbf{f}$, *we have*

$$\mathrm{In}_{\mathbf{f}}(H) = \bigcup_{i=1}^{I}\bigcap_{j=1}^{J_i} \mathrm{In}_{\mathbf{f}}\big(\mathcal{S}(p_{ij} \triangleright 0)\big).$$

That is, computing $\mathrm{In}_{\mathbf{f}}(H)$ amounts to compute $\mathrm{In}_{\mathbf{f}}\big(\mathcal{S}(p_{ij} \triangleright 0)\big)$ for each basic component $\mathcal{S}(p_{ij} \triangleright 0)$ of H. We can further show that:

LEMMA 21. *For any polynomial p and vector field $\mathbf{f}$,*

$$\mathrm{In}_{\mathbf{f}}(\mathcal{S}(p>0)) = \mathcal{S}(\psi^{+}(p,\mathbf{f},\mathbf{x})),\ \textit{and}$$
$$\mathrm{In}_{\mathbf{f}}(\mathcal{S}(p\geq 0)) = \mathcal{S}\Big(\psi^{+}(p,\mathbf{f},\mathbf{x}) \vee \big(\bigwedge_{0\leq j\leq N_{p,\mathbf{f}}} L_{\mathbf{f}}^{j}p(\mathbf{x})=0\big)\Big)$$

where

$$\psi^{+}(p,\mathbf{f},\mathbf{x}) \widehat{=} \bigvee_{0\leq i\leq N_{p,\mathbf{f}}} \psi^{(i)}(p,\mathbf{f},\mathbf{x})\ \textit{with}$$
$$\psi^{(i)}(p,\mathbf{f},\mathbf{x}) \widehat{=} \left(\bigwedge_{0\leq j<i} L_{\mathbf{f}}^{j}p(\mathbf{x})=0\right) \wedge L_{\mathbf{f}}^{i}p(\mathbf{x})>0.$$

Therefore, $\mathrm{In}_{\mathbf{f}}(H)$ can be translated into a polynomial formula. By a similar argument, we are able to prove that

LEMMA 22. *For a semi-algebraic set H defined by formula (7) and a polynomial vector field $\mathbf{f}$, we have*

$$\mathrm{IvIn}_{\mathbf{f}}(H) = \bigcup_{i=1}^{I}\bigcap_{j=1}^{J_i} \mathrm{IvIn}_{\mathbf{f}}\big(\mathcal{S}(p_{ij}\triangleright 0)\big).$$

Accordingly,

LEMMA 23. *For any polynomial p and vector field $\mathbf{f}$,*

$$\mathrm{IvIn}_{\mathbf{f}}\big(\mathcal{S}(p>0)\big) = \mathcal{S}\big(\varphi^{+}(p,\mathbf{f},\mathbf{x})\big),\ \textit{and}$$
$$\mathrm{IvIn}_{\mathbf{f}}\big(\mathcal{S}(p\geq 0)\big) = \mathcal{S}\Big(\varphi^{+}(p,\mathbf{f},\mathbf{x}) \vee \big(\bigwedge_{0\leq j\leq N_{p,\mathbf{f}}} L_{\mathbf{f}}^{j}p(\mathbf{x})=0\big)\Big)$$

where

$$\varphi^{+}(p,\mathbf{f},\mathbf{x}) \widehat{=} \bigvee_{0\leq i\leq N_{p,\mathbf{f}}} \varphi^{(i)}(p,\mathbf{f},\mathbf{x}) \qquad \textit{with}$$
$$\varphi^{(i)}(p,\mathbf{f},\mathbf{x}) \widehat{=} \Big(\bigwedge_{0\leq j<i} L_{\mathbf{f}}^{j}p(\mathbf{x})=0\Big) \wedge \Big((-1)^{i}\cdot L_{\mathbf{f}}^{i}p(\mathbf{x})>0\Big).$$

Now we are able to present our main result of automatic SAI generation for PDSs.

THEOREM 24 (MAIN RESULT). *A semi-algebraic set $\mathcal{S}(P)$ with*

$$P \widehat{=} \bigvee_{k=1}^{K}\left(\bigwedge_{j=1}^{j_k} p_{kj}(\mathbf{u}_{kj},\mathbf{x})\geq 0 \quad \wedge \bigwedge_{j=j_k+1}^{J_k} p_{kj}(\mathbf{u}_{kj},\mathbf{x})>0\right)$$

is a continuous invariant of the PDS $\big(H(\mathbf{x}),\mathbf{f},\Xi(\mathbf{x})\big)$ with

$$H \widehat{=} \bigvee_{m=1}^{M}\left(\bigwedge_{l=1}^{l_m} p_{ml}(\mathbf{x})\geq 0 \quad \wedge \bigwedge_{l=l_m+1}^{L_m} p_{ml}(\mathbf{x})>0\right),$$

if and only if $\mathbf{u}\widehat{=}\langle\mathbf{u}_{kj}\rangle$ satisfy

$$\forall\mathbf{x}.\left(\begin{array}{l}(\Xi(\mathbf{x})\Rightarrow P(\mathbf{u},\mathbf{x}))\wedge\\ \big(P\wedge H\wedge\varphi_H\Rightarrow\varphi_P\big)\wedge\big(\neg P\wedge H\wedge\varphi_H^{\mathrm{Iv}}\Rightarrow\neg\varphi_P^{\mathrm{Iv}}\big)\end{array}\right),$$

where

$$\varphi_H \widehat{=} \bigvee_{m=1}^{M}\left(\bigwedge_{l=1}^{l_m}\psi_0^{+}(p_{ml},\mathbf{f})\wedge\bigwedge_{l=l_m+1}^{L_m}\psi^{+}(p_{ml},\mathbf{f})\right),$$
$$\varphi_P \widehat{=} \bigvee_{k=1}^{K}\left(\bigwedge_{j=1}^{j_k}\psi_0^{+}(p_{kj},\mathbf{f})\wedge\bigwedge_{j=j_k+1}^{J_k}\psi^{+}(p_{kj},\mathbf{f})\right),$$
$$\varphi_H^{\mathrm{Iv}} \widehat{=} \bigvee_{m=1}^{M}\left(\bigwedge_{l=1}^{l_m}\varphi_0^{+}(p_{ml},\mathbf{f})\wedge\bigwedge_{l=l_m+1}^{L_m}\varphi^{+}(p_{ml},\mathbf{f})\right),$$
$$\varphi_P^{\mathrm{Iv}} \widehat{=} \bigvee_{k=1}^{K}\left(\bigwedge_{j=1}^{j_k}\varphi_0^{+}(p_{kj},\mathbf{f})\wedge\bigwedge_{j=j_k+1}^{J_k}\varphi^{+}(p_{kj},\mathbf{f})\right),$$

with $\psi_0^{+}(p,\mathbf{f})\widehat{=}\psi^{+}(p,\mathbf{f},\mathbf{x})\vee\phi(p,\mathbf{f})$, $\varphi_0^{+}(p,\mathbf{f})\widehat{=}\varphi^{+}(p,\mathbf{f},\mathbf{x})\vee\phi(p,\mathbf{f})$, and $\phi(p,\mathbf{f})\widehat{=}\bigwedge_{0\leq j\leq N_{p,\mathbf{f}}} L_{\mathbf{f}}^{j}p(\mathbf{x})=0$.

Note that φ_H and φ_H^{Iv} are trivially "true" when H is the whole space $\mathbb{R}^n$. Compared to related work, e.g [18, 20, 21, 28], our method for SAI generation based on Theorem 24 has the following two features:

1. Given a PDS with arbitrary semi-algebraic domain and initial condition, we consider generating arbitrary semi-algebraic sets as continuous invariants, which are of complicated forms and may be neither open nor closed.
2. Our criterion for checking semi-algebraic invariants for a PDS is sound and complete; our method for automatically generating semi-algebraic invariants is sound, and relatively complete w.r.t the predefined template.

Now we demonstrate how our approach can be used to generate a general SAI by the following example.

EXAMPLE 25. *Let $\mathbf{f}(x,y)=(\dot{x}=-2y,\dot{y}=x^2)$ with $H\widehat{=}\mathbb{R}^2$ and $\Xi\widehat{=}x+y\geq 0$. Take a template: $\tau\widehat{=}x-a\geq 0\vee y-b>0$. By Theorem 24, τ is an SAI of $(H,\mathbf{f},\Xi)$ if and only if (a,b) satisfy the following two formulas*

$$x+y\geq 0\Rightarrow(x-a\geq 0\vee y-b>0) \tag{8}$$
$$(\tau\Rightarrow\zeta)\wedge(\neg\tau\Rightarrow\neg\xi) \tag{9}$$

for all $(x,y)\in\mathbb{R}^2$, where

$$\begin{aligned}\zeta\widehat{=}&(x-a>0)\vee(x-a=0\wedge-2y>0)\\ &\vee(x-a=0\wedge-2y=0\wedge-2x^2\geq 0)\\ &\vee(y-b>0)\vee(y-b=0\wedge x^2>0)\\ &\vee(y-b=0\wedge x^2=0\wedge-4yx>0)\\ &\vee(y-b=0\wedge x^2=0\wedge-4yx=0\wedge 8y^2-4x^3>0)\\ \xi\widehat{=}&(x-a>0)\vee(x-a=0\wedge-2y<0)\\ &\vee(x-a=0\wedge-2y=0\wedge-2x^2\geq 0)\\ &\vee(y-b>0)\vee(y-b=0\wedge x^2<0)\\ &\vee(y-b=0\wedge x^2=0\wedge-4yx>0)\\ &\vee(y-b=0\wedge x^2=0\wedge-4yx=0\wedge 8y^2-4x^3<0)\end{aligned}$$

By applying quantifier elimination to this formula, we get $a+b\leq 0\wedge b\leq 0$. Let $a=-1$ and $b=-0.5$, and it results that $\{(x,y)\in\mathbb{R}^2\mid x\geq -1\vee y>-0.5\}$ is an SAI for this PDS, which is shown in IV of Figure 2.

Note that in the above example, the generated SAI is a general semi-algebraic set that is a union of two simple semi-algebraic sets, which is neither closed nor open.

7. CASE STUDIES

In this section, we show that our method presented above can be used to generate continuous invariants for some real systems.

7.1 Formal Verification of CTCS-3

In [15], the authors use *HCSP* [10, 34] to formally model the *Chinese Train Control System at Level 3 (CTCS-3)* [33]. They also propose a calculus of HCSP for the purpose of verifying safety properties of CTCS-3. For this calculus to work, effective techniques for dealing with continuous dynamics must be incorporated.

Consider the following fragment of the HCSP model of CTCS-3:

$$P_{ebi} \mathrel{\widehat{=}} \langle \dot{s} = v, \dot{v} = a \rangle \twoheadrightarrow v \geq v.Seg ; flag_{EB} := true ; P_{EB} .$$

Process P_{ebi} models the running of a train, with s, v, a representing its position, velocity and acceleration (a is a constant) respectively. Once v exceeds the speed limit $v.Seg$ of the current segment, $flag_{EB}$ for emergency brake is set to *true* and the train starts braking immediately, expressed by the subprocess P_{EB}.

The safety property needs to be verified about P_{ebi} can be stated as

$$Inv \mathrel{\widehat{=}} v \geq v.Seg \Rightarrow flag_{EB} = true ,$$

which means whenever the train's speed exceeds certain limit, it must execute the emergency brake process.

To verify this property, i.e. to check that Inv is indeed an invariant of P_{ebi}, according to the calculus in [15], it amounts to check that $v < v.Seg$ is a continuous invariant of the PDS $(H, \mathbf{f}, \Xi)$, where $H \mathrel{\widehat{=}} \mathcal{S}(v < v.Seg)$, $\mathbf{f} \mathrel{\widehat{=}} (v, a)$ and $\Xi \mathrel{\widehat{=}} \{(s_0, v_0)\}$ with $v_0 < v.Seg$. According to our method, this can be further reduced to the checking of the validity of

$$\forall v.(v = v.Seg \wedge v < v.Seg \Rightarrow a \leq 0),$$

which is obvious.

Perhaps this example seems a bit trivial, for the continuous dynamics is an affine system and the required invariant coincides with the domain. What we want to stress here is the completeness of our criterion for checking continuous invariants compared to others. For example, the principle given in [18] requires the directional derivative of an invariant in the direction of the vector field to have the same sign in the domain. As a result, it may fail to generate the above invariant $\mathcal{S}(v < v.Seg)$, because

$$\forall v.(v < v.Seg \Rightarrow \dot{v} = a < 0)$$

is *false* when $a \geq 0$.

7.2 Collision Avoidance Maneuvers

We consider the following two-aircraft flight dynamics from [19]:

$$\mathbf{f} \mathrel{\widehat{=}} \begin{bmatrix} \dot{x}_1 = d_1 & \dot{y}_1 = e_1 & \dot{d}_1 = -\omega d_2 & \dot{e}_1 = -\theta e_2 \\ \dot{x}_2 = d_2 & \dot{y}_2 = e_2 & \dot{d}_2 = \omega d_1 & \dot{e}_2 = \theta e_1 \end{bmatrix} . \quad (10)$$

System (10) has 8 variables: (x_1, x_2) and (y_1, y_2) represent the positions of aircraft 1 and 2 respectively, and (d_1, d_2) and (e_1, e_2) represent their velocities. The parameters ω and θ denote the angular speed of the two aircrafts.

We shall use our method to generate special continuous invariants of form $p = 0$ for the PDS $(H, \mathbf{f}, \Xi)$ with $H \mathrel{\widehat{=}} \mathbb{R}^8$ and $\mathbf{f}$ defined in (10). For simplicity, we take Ξ to be a singleton $\{(x_1^0, x_2^0, d_1^0, d_2^0, y_1^0, y_2^0, e_1^0, e_2^0)\}$.

In order to determine candidates for continuous invariants of $(H, \mathbf{f}, \Xi)$, we enumerate parametric polynomials $p \mathrel{\widehat{=}} p(\mathbf{u}, \mathbf{x})$ by the degree of p and the number of variables appearing in it. For example, we can choose the linear template $p(\mathbf{u}, \mathbf{x}) \mathrel{\widehat{=}} u_1 x_1 + u_2 x_2 + u_3 d_1 + u_4 d_2 + u_0$.

According to Theorem 24, it is easy to check that $p(\mathbf{u}, \mathbf{x}) = 0$ is a continuous invariant of $(H, \mathbf{f}, \Xi)$ if and only if $\mathbf{u}$ satisfy

- $\forall \mathbf{x}. (\Xi \Rightarrow p = 0)$; and
- $\forall \mathbf{x}. \left(p = 0 \Rightarrow \bigwedge_{i=1}^{N_{p,\mathbf{f}}} L_{\mathbf{f}}^i p(\mathbf{u}, \mathbf{x}) = 0\right)$.

For the template defined above, we can get $N_{p,\mathbf{f}} = 2$. By applying quantifier elimination to the corresponding constraint, we get $u_2 - u_3\omega = 0 \wedge u_1 + u_4\omega = 0 \wedge u_0 + u_1 x_1^0 + u_2 x_2^0 + u_3 d_1^0 + u_4 d_2^0 = 0$. Thus we can obtain the following continuous invariants by assigning suitable values to u_is:

- $\omega x_2 + d_1 - \omega x_2^0 - d_1^0 = 0$;
- $-\omega x_1 + d_2 + \omega x_1^0 - d_2^0 = 0$;
- $-\omega x_1 + \omega x_2 + d_1 + d_2 + \omega x_1^0 - \omega x_2^0 - d_1^0 - d_2^0 = 0$.

If we use the quadratic template $p \mathrel{\widehat{=}} u_1 d_1^2 + u_2 d_2^2 + u_0$, we can also get $N_{p,\mathbf{f}} = 2$, and the constraint for $\mathbf{u}$ is $u_1 - u_2 = 0 \wedge u_0 + u_1 (d_1^0)^2 + u_2 (d_2^0)^2 = 0$. Let $u_1 = u_2 = 1$ and we obtain a CI

$$d_1^2 + d_2^2 - (d_1^0)^2 - (d_2^0)^2 = 0 \ .$$

Using arbitrary semi-algebraic templates, we can generate continuous invariants beyond polynomial equations for $(H, \mathbf{f}, \Xi)$, at the cost of heavier computation.

8. CONCLUSIONS

In this paper, we present a sound and complete criterion for checking SAIs for PDSs, as well as a relatively complete method for automatic SAI generation using templates. Relative completeness means if there is an SAI in the form of a predefined template, then our method can indeed find one. Our approach is based on the computable algebraic-geometry theory. Our work in this paper actually completes the gap left open in [28]. Compared with the related work, more invariants can be generated through our approach. This is demonstrated by simple examples and case studies.

In the future, we will concentrate on the following problems. Firstly, we believe that our method can be applied to generate invariant sets for stability analysis, controller synthesis and so on in control theory, in particular for construction of Lyapunov functions. Secondly, we will consider how to extend the approach to more general dynamical systems whose vector fields are functions beyond polynomials. Since our approach makes use of first-order quantifier elimination which is with doubly exponential cost [7], how to improve the efficiency of our approach will be our main future work. For instance of linear templates, it is helpful to reduce the complexity via linear programming.

9. ACKNOWLEDGEMENTS

We would like to thank Prof. Zhou Chaochen, Prof. Yang Lu and Prof. Xia Bican for their insightful comments on the earlier drafts. We thank Dr. Xu Ming, Zou Liang and Quan Zhao for helpful discussions and technical support. We also want to thank the anonymous referees for their valuable suggestions on improving the previous versions.

10. REFERENCES

[1] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P. H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theor. Comput. Sci.*, 138(1):3–34, Feb. 1995.

[2] R. Alur and D. L. Dill. A theory of timed automata. *Theor. Comput. Sci.*, 126(2):183–235, Apr. 1994.

[3] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, Nov. 1999.

[4] C. W. Brown. QEPCAD B: A program for computing with semi-algebraic sets using CADs. *SIGSAM Bull.*, 37:97–108, Dec. 2003.

[5] E. M. Clarke, E. A. Emerson, and A. P. Sistla. Automatic verification of finite-state concurrent systems using temporal logic specifications. *ACM Trans. Program. Lang. Syst.*, 8:244–263, Apr. 1986.

[6] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer, second edition, 1997.

[7] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *J. Symb. Comput.*, 5(1-2):29–35, 1988.

[8] A. Dolzmann, A. Seidl, and T. Sturm. *Redlog User Manual*, Edition 3.1, for Redlog Version 3.06 (Reduce 3.8) edition, Nov. 2006. `http://redlog.dolzmann.de/downloads/`.

[9] S. Gulwani and A. Tiwari. Constraint-based approach for analysis of hybrid systems. In *CAV '08*, volume 5123 of *LNCS*, pages 190–203. Springer, 2008.

[10] J. He. From CSP to hybrid systems. In *A Classical Mind, Essays in Honour of C.A.R. Hoare*, pages 171–189. Prentice Hall International (UK) Ltd., 1994.

[11] T. A. Henzinger, P. W. Kopke, A. Puri, and P. Varaiya. What's decidable about hybrid automata? In *STOC '95*, pages 373–382. ACM, 1995.

[12] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, third edition, Dec. 2001.

[13] S. Krantz and H. Parks. *A Primer of Real Analytic Functions*. Birkhäuser Boston, second edition, June 2002.

[14] G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computation for families of linear vector fields. *J. Symb. Comput.*, 32:231–253, Sept. 2001.

[15] J. Liu, J. Lv, Z. Quan, N. Zhan, H. Zhao, C. Zhou, and L. Zou. A calculus for hybrid CSP. In *APLAS '10*, volume 6461 of *LNCS*, pages 1–15. Springer, 2010.

[16] J. Liu, N. Zhan, and H. Zhao. Computing semi-algebraic invariants for polynomial dynamical systems. *ArXiv e-prints*, Feb. 2011. `http://arxiv.org/abs/1102.0705`.

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

[18] A. Platzer and E. M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In *CAV '08*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008.

[19] A. Platzer and E. M. Clarke. Formal verification of curved flight collision avoidance maneuvers: A case study. In *FM '09*, volume 5850 of *LNCS*, pages 547–562. Springer, 2009.

[20] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *HSCC '04*, volume 2993 of *LNCS*, pages 477–492. Springer, 2004.

[21] S. Prajna, A. Jadbabaie, and G. J. Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Trans. Autom. Control*, 52(8):1415–1428, Aug. 2007.

[22] A. Puri and P. Varaiya. Decidability of hybrid systems with rectangular differential inclusions. In *CAV '94*, volume 818 of *LNCS*, pages 95–104. Springer, 1994.

[23] J.-P. Queille and J. Sifakis. Specification and verification of concurrent systems in CESAR. In *Proc. of the 5th Colloquium on International Symposium on Programming*, pages 337–351. Springer-Verlag, 1982.

[24] E. Rodríguez-Carbonell and A. Tiwari. Generating polynomial invariants for hybrid systems. In *HSCC '05*, volume 3414 of *LNCS*, pages 590–605. Springer, 2005.

[25] S. Sankaranarayanan. Automatic invariant generation for hybrid systems using ideal fixed points. In *HSCC '10*, pages 221–230. ACM, 2010.

[26] S. Sankaranarayanan, H. B. Sipma, and Z. Manna. Constructing invariants for hybrid systems. In *HSCC '04*, volume 2993 of *LNCS*, pages 539–554. Springer, 2004.

[27] A. Taly, S. Gulwani, and A. Tiwari. Synthesizing switching logic using constraint solving. In *VMCAI '09*, volume 5403 of *LNCS*, pages 305–319. Springer, 2009.

[28] A. Taly and A. Tiwari. Deductive verification of continuous dynamical systems. In *FSTTCS '09*, volume 4 of *LIPIcs*, pages 383–394, 2009.

[29] A. Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley, May 1951.

[30] M. Tenenbaum and H. Pollard. *Ordinary Differential Equations*. Dover Publications, Oct. 1985.

[31] B. Xia. DISCOVERER: a tool for solving semi-algebraic systems. *ACM Commun. Comput. Algebra*, 41:102–103, Sept. 2007.

[32] L. Yang, C. Zhou, N. Zhan, and B. Xia. Recent advances in program verification through computer algebra. *Frontiers of Computer Science in China*, 4:1–16, 2010.

[33] S. Zhang. *The General Technical Solutions to Chinese Train Control System at Level 3 (CTCS-3)*. China Railway Publishing House, 2008. in Chinese.

[34] C. Zhou, J. Wang, and A. Ravn. A formal description of hybrid systems. In *Hybrid Systems III*, volume 1066 of *LNCS*, pages 511–530. Springer, 1996.