Generating Semi-algebraic Invariants for Non-autonomous Polynomial Hybrid Systems

Qiuye Wang

August 8, 2016

Abstract

1 Introduction

Hybrid systems are systems including both discrete and continuous dynamics. This feature enables them to be used in many real-world engineering problems. A typical one is MDD, which stands for Model-Driven Development[5].

A core problem of verifying hybrid systems is so-called safety verification problem. It asks whether a hybrid system will reach some unsafe states from given initial states. Obviously, if we can compute the reachable set of given system, which includes all states reachable from initial states, then we can solve safety verification problem by simply examines whether any unsafe state is in reachable set or not [2].

But for common differential equations, the reachable set is usually intractable, especially when time is unbounded. So the intuitive methods of directly computing reachable set can only be used for very special systems. To avoid the computing of reachable sets, methods based on invariants are brought up[9, 8].

Invariants can be seen as a special kind of over-approximation of reachable set. Informally, invariants(or inductive invariants, if called precisely) are sets satisfying that current state included in invariants implies that states evolved from current state are all included in invariants. A virtue of invariants is that they can be computed without solving differential equations.

Non-autonomous hybrid systems, i.e. systems that evolution function $\boldsymbol{f}$ changes with time, are an important class of hybrid systems. Most previous works in that field focus on autonomous case, i.e. systems that evolution function $\boldsymbol{f}$ doesn't change with time [7]. In this article we will focus on non-autonomous case, We propose a sound and complete algorithm for verifying semi-algebraic invariants for non-autonomous polynomial hybrid system. From it, we obtain a sound and relatively complete algorithm for generating these invariants.

The basic idea is to transform the definition of continuous invariant of non-autonomous polynomial hybrid system into a first order formula of finite length,

then use quantifier elimination algorithm to obtain a equivalent quantifier-free formula. When verifying, the original formula contains only bounded variables, so the corresponding quantifier-free formula will be either *TRUE* or *FALSE*, which represents whether the verified semi-algebraic set is an invariant of our system or not. When generating, some free variables representing the coefficients of possible invariants are introduced. The resulting quantifier-free formula can be seen as a constraint on those coefficients. Any solution to the constraint yields a valid invariant, and a *no solution* result denotes no invariant satisfies given template.

The main contribution of this article include:

1. we present a whole set of definitions for continuous invariants in non-autonomous case;
2. we give a sound and complete algorithm for verifying semi-algebraic invariants for polynomial hybrid systems.
3. we give a sound and relatively complete algorithm for generating semi-algebraic invariants for polynomial hybrid systems.

The article is organized as follows: Section 2 includes definitions and some background knowledge; Section 3 illuminates our method using a simplified problem when initial sets, domain and invariants are all defined by a single polynomial; Section 4 gives detailed version of our algorithms which can be used in general semi-algebraic sets; we conclude the article with Section 5.

2 Preliminaries

2.1 Definitions

The main difficulty in handling hybrid system is to deal with continuous dynamics. If we know how to verify or generate invariant for a certain mode of hybrid system, similar methods can be easily extended to the whole system, see [8, 6]. So for simplicity, we only consider single-mode hybrid systems:

Definition 1 (Hybrid System) A hybrid system is a tuple $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, where:

1. $\boldsymbol{H} \subseteq \mathbb{R}^n$ is the domain of system state.
2. $\boldsymbol{I} \subseteq \boldsymbol{H}$ is the set of initial states, which will be called the initial set.
3. $\boldsymbol{f} \in \boldsymbol{H} \times [0, +\infty) \to \mathbb{R}^n$ is the evolution function of system. The evolution of system subjects to: $\dot{\boldsymbol{x}}(t) = \boldsymbol{f}(\boldsymbol{x}(t), t)$. □

Definition 2 (Trajectory) For a hybrid system M, the trajectory originating from state $\boldsymbol{x}_0$ and time t_0 in time T is a differentiable function $\boldsymbol{x} \in [t_0, t_0+T) \to \mathbb{R}^n$ satisfies:

1. For $t \in [t_0, t_0 + T)$, $\dot{\boldsymbol{x}}(t) = \boldsymbol{f}(\boldsymbol{x}(t), t)$; and

2. $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$.

When it's obvious from context, we will omit the phrase "from $\boldsymbol{x}_0$", "from time t_0". □

Definition 3 (Safety) Given an unsafe set $X_U \subseteq \mathbb{R}^n$, we say a hybrid system is safe, if no trajectories satisfy:

1. $\boldsymbol{x}(0) \in \boldsymbol{I}$; and
2. $\exists \tau \geq 0 : \boldsymbol{x}(\tau) \in X_U$ □

Definition 4 (Continuous Invariant) The continuous invariant of a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ is a set $\boldsymbol{A} \subseteq \mathbb{R}^n$ satisfies:

1. $\boldsymbol{I} \subseteq \boldsymbol{A}$, and
2. For any $t_0 \geq 0$, $\boldsymbol{x}_0 \in \boldsymbol{A}$ and $T > 0$, any trajectories $\boldsymbol{x}$ satisfying $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$ also satisfy: $(\forall t \in [t_0, t_0 + T], \boldsymbol{x}(t) \in \boldsymbol{H}) \Rightarrow (\forall t \in [t_0, t_0 + T], \boldsymbol{x}(t) \in \boldsymbol{A})$ □

In this article, the word *invariant* always means continuous invariant defined here, if not state explicitly otherwise.

The main subject of our study is polynomial hybrid system:

Definition 5 (Polynomial Hybrid System) We say a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ is polynomial, if:

1. Domain $\boldsymbol{H}$ is a semi-algebraic set;
2. Initial set $\boldsymbol{I}$ is a semi-algebraic set;
3. Evolution funtion $\boldsymbol{f}$ is a polynomial vector function for t and $\boldsymbol{x}$. That is to say: every $f_i(\boldsymbol{x}, t)$ in $\boldsymbol{f}(\boldsymbol{x}, t) = (f_1(\boldsymbol{x}, t), f_2(\boldsymbol{x}, t), \ldots, f_n(\boldsymbol{x}, t))$ satisfies: $f_i(\boldsymbol{x}, t) \in \mathbb{R}[\boldsymbol{x}, t]$, where $\mathbb{R}[\boldsymbol{x}, t]$ is a short version of $\mathbb{R}[x_1, x_2, \ldots, x_n, t]$. □

In this article, we always assume a hybrid system is polynomial, if not state explicitly otherwise.

It's easy to verify that polynomial functions satisfy Lipschitz condition. By the famous Picard-Lindelöf theorem, there exists a unique solution to the initial value problem locally.

2.2 Background: Semi-algebraic Set

Definition 6 (Semi-algebraic Set) A semi-algebraic set is a subset of $\mathbb{R}^n$ defined by a finite sequence of polynomial equations and inequalities , or any finite union of such sets.

Formally, a set $S \subseteq \mathbb{R}^n$ is a semi-algebraic set if and only if there exists formula ψ such that $S = \{\boldsymbol{x} \in \mathbb{R}^n \mid \psi(x) \text{ satisfies}\}$, where ψ defined by:

$$\psi \doteq \bigvee_{k=1}^{K} \bigwedge_{j=1}^{J_k} p_{kj} \rhd 0$$

where $p_{kj} \in \mathbb{R}[\boldsymbol{x}]$ and $\rhd \in \{\geq, >\}$. □

It's easy to prove that operations on semi-algebraic set is equivalent to corresponding operations on the formula defining it. More specifically, if we use $S(\psi)$ to represent semi-algebraic set defined by ψ, we have the following properties:

- $S(\psi_1) \cap S(\psi_2) = S(\psi_1 \wedge \psi_2)$
- $S(\psi_1) \cup S(\psi_2) = S(\psi_1 \vee \psi_2)$
- $S(\psi)^c = S(\neg\psi)$
- $S(\psi_1) \backslash S(\psi_2) = S(\psi_1) \cap S(\psi_2)^c = S(\psi_1 \wedge \neg\psi_2)$

2.3 Background: Lie Derivatives

Lie derivatives describe the change of a tensor field along the flow of another vector field.

Definition 7 (Lie Derivatives) For a given function ϕ, a given vector function $\boldsymbol{f}(t, \boldsymbol{x})$, we define Lie derivatives $\mathcal{L}_{t,f}$ inductively as:

$$\begin{aligned}
&\mathcal{L}^0_{t,f}\phi(\boldsymbol{x}) = \phi(\boldsymbol{x}) \\
&\mathcal{L}^k_{t,f}\phi(\boldsymbol{x}) = \langle \frac{\partial}{\partial \boldsymbol{x}} \mathcal{L}^{k-1}_{t,f}\phi(\boldsymbol{x}) \cdot \boldsymbol{f}(\boldsymbol{x}, t) \rangle, \qquad k > 0
\end{aligned}$$

where $\langle * \cdot * \rangle$ is dot product. □

Example 1 Assume $\boldsymbol{f}(x, y, t) = (-x + t, y - t)$ and $\phi(x, y) = x + y^2$, then:

$$\begin{aligned}
&\mathcal{L}^0_{t,f}\phi(x, y) = x + y^2 \\
&\mathcal{L}^1_{t,f}\phi(x, y) = 2y^2 - 2ty - x + t \\
&\mathcal{L}^2_{t,f}\phi(x, y) = 4y^2 - 6ty - x + t \\
&\qquad\qquad \cdots\cdots
\end{aligned}$$

□

Definition 8 (Pointwise Rank) For a given state $\boldsymbol{x}$ and time t, we define pointwise rank of Lie derivatives as:

$$\gamma_{f,\phi}(\boldsymbol{x}, t) = \min\{k \in \mathbb{N} \mid \mathcal{L}^k_{t,f}\phi(\boldsymbol{x}) \neq 0\}$$

□

In this article we will just call *pointwise rank* as *rank*.

Note that Lie derivatives and their rank both contains variable t.

2.4 Background: Polynomial Ideals Theory

Polynomial ideal is a powerful tool when we deal with polynomial related problems. Here we recall some basic contents about it, from [3].

For a given field $\mathbb{K}$ and variables $x_1, x_2, \ldots, x_n$, we can define polynomial ring over $\mathbb{K}$ as $\mathbb{K}[x_1, x_2, \ldots, x_n]$. We write $\mathbb{K}[\boldsymbol{x}]$ to represent $\mathbb{K}[x_1, x_2, \ldots, x_n]$ and always assume $\mathbb{K} = \mathbb{R}$, i.e. coefficients are real numbers.

Definition 9 (Polynomial Ideals) Given a polynomial ring $\mathbb{K}[\boldsymbol{x}]$, a subset $\boldsymbol{I} \subseteq \mathbb{K}[\boldsymbol{x}]$ is called ideal if:

1. $0 \in \boldsymbol{I}$;
2. For any $p(x), q(x) \in \boldsymbol{I}$, we have: $p(x) + q(x) \in \boldsymbol{I}$;
3. For any $p(x) \in \boldsymbol{I}$ and $h(x) \in \mathbb{K}[\boldsymbol{x}]$, we have: $p(x)h(x) = h(x)p(x) \in \boldsymbol{I}$. □

Definition 10 (Generated Ideals) we call

$$\boldsymbol{I} \doteq \bigcap_{p_1, p_2, \ldots, p_k \in \boldsymbol{I}', \boldsymbol{I}' \text{is a ideal}} \boldsymbol{I}'$$

ideal generated by basis $p_1, p_2, \ldots, p_k$, denoted by $\langle p_1, p_2, \ldots, p_k \rangle$.

It's easy to prove that:

$$\langle p_1, p_2, \ldots, p_k \rangle = \{\sum_{i=1}^{k} p_i h_i \mid \forall i : h_i \in \mathbb{K}[\boldsymbol{x}]\}$$

□

A well-known result is every polynomial ideal in real field can be generated by finite basis:

Theorem 1 (Hibert's Basis Theorem) *Any polynomial ideal $\boldsymbol{I} \in \mathbb{R}[\boldsymbol{x}]$ can be generated by a finite class of basis. i.e. for any ideal $\boldsymbol{I} \in \mathbb{R}[\boldsymbol{x}]$, there exists $p_1, p_2, \ldots, p_k \in \mathbb{R}[\boldsymbol{x}]$ such that $\boldsymbol{I} = \langle p_1, p_2, \ldots, p_k \rangle$.* □

The above theorem can take a different form:

Theorem 2 (Ascending Chain Theorem) *For any infinite ascending chain of ideals in $\mathbb{K}[\boldsymbol{x}]$:*

$$\boldsymbol{I}_1 \subseteq \boldsymbol{I}_2 \subseteq \ldots \boldsymbol{I}_k \subseteq \ldots$$

There exists N such that for any $l \geq N$, $\boldsymbol{I}_l = \boldsymbol{I}_N$. □

3 Simple Case

In this section, we focus on a simplified version of our original problem. More specifically, we only consider invariants that can be defined by a single polynomial inequality $\phi(\boldsymbol{x}) \geq 0$, we use Φ to denote the invariant. Also we assume that the domain $\boldsymbol{H}$ and initial set $\boldsymbol{I}$ can be defined by a single polynomial inequality. We will use $\boldsymbol{H}(\boldsymbol{x}) \geq 0$ and $\boldsymbol{I}(\boldsymbol{x}) \geq 0$ to denote them separately. In this section, if not explicitly state otherwise, we always suppose our hybrid system takes that form.

3.1 Intuitive Idea and Lie Deriavarives

Intuitively, an invariant is a set that if any time system state falls in it, it will never come out of it. Suppose we follow the trajectory of our system: when system state is inside Φ, by the continuity of system trajectories, obviously it must reach the boundary of Φ before it comes out of Φ. So the real danger of coming out of Φ occurs when system state is in the boundary of Φ. In this simple case, that is to say: for every states $\boldsymbol{x}_0$ satisfying $\phi(\boldsymbol{x}_0) = 0$ and any time $t_0 \geq 0$, there exists some positive time ϵ such that the trajectory originating from state $\boldsymbol{x}_0$ and time t_0 in time ϵ doesn't decrease the value ϕ.

To turn this intuitive idea into practical algorithm, the first step is to find a tool to describe the change of ϕ as system evolves. Lie derivatives are suitable for this.

Theorem 3 *Given polynomial ϕ and hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, $\gamma_{f,\phi}(\boldsymbol{x}_0, t) \neq 0$ if and only if $\boldsymbol{x}_0 \in S(\phi(\boldsymbol{x}) = 0)$, and if we take $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$, then it follows that:*

1. *if $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ and $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0) > 0$, then:*
$$\exists \epsilon > 0, \forall t \in (t_0, t_0 + \epsilon), \phi(\boldsymbol{x}(t)) > 0$$
2. *if $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ and $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0) < 0$, then:*
$$\exists \epsilon > 0, \forall t \in (t_0, t_0 + \epsilon), \phi(\boldsymbol{x}(t)) < 0$$
3. *if $\gamma_{f,\phi}(\boldsymbol{x}, t_0) = \infty$, then:*
$$\exists \epsilon > 0, \forall t \in (t_0, t_0 + \epsilon), \phi(\boldsymbol{x}(t)) = 0$$ □

PROOF First, recall Definition 8, $\gamma_{f,\phi}(\boldsymbol{x}_0, t) \neq 0$ if and only if $\mathcal{L}_{t,f}^0\phi(\boldsymbol{x}) = 0$, which, by Definition 7, is equivalent to $\phi(\boldsymbol{x}_0) = 0$.

Next, assume now $\gamma_{f,\phi}(\boldsymbol{x}_0, t) \neq 0$. Since $\boldsymbol{f}$ is a polynomial vector function, we know $\boldsymbol{f}$ is analytic. So the initial value problem for differential equation $\dot{\boldsymbol{x}}(t) = \boldsymbol{f}(\boldsymbol{x}(t), t)$ and $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$ exists a unique solution near t_0[11]. Since ϕ is also a polynomial function, we can conclude that $\phi(\boldsymbol{x}(t))$ is analytic near t_0. So we have:

$$\begin{aligned}\phi(\boldsymbol{x}(t)) &= \phi(\boldsymbol{x}(t_0)) + \frac{\mathrm{d}\phi}{\mathrm{d}t}(t_0) * (t - t_0) + \frac{\mathrm{d}^2\phi}{\mathrm{d}t^2} * \frac{(t - t_0)^2}{2!} + \dots \\ &= \mathcal{L}_{t_0,f}^0\phi(\boldsymbol{x}_0) + \mathcal{L}_{t_0,f}^1\phi(\boldsymbol{x}_0) * (t - t_0) + \mathcal{L}_{t_0,f}^2\phi(\boldsymbol{x}_0) * \frac{(t - t_0)^2}{2!} + \dots\end{aligned}$$

satisfies near t_0.

For the first two situations, we see that the first $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0)$ terms of the right side equation is equal to 0, and the coefficient of the dominant term has the same sign as $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0)$, so we can immediately get the corresponding conclusions.

As to the last situation, $\gamma_{f,\phi}(\boldsymbol{x}, t_0) = \infty$ implies that every term of the right side expansion is equal to 0, which means $\phi(\boldsymbol{x}(t)) = 0$ satisfies in the interval where unique solution exists and ϕ is analytic. ■

Note the three situations in theorem 3 include all possible value of $\mathcal{L}^k_{t_0,f}$, so an inverse version of this theorem is possible, we state it as a corollary:

Corollary 1 *For a sequence* $\{t_i\}$ *satisfying* $t_i > t_0$ *and* $\lim_{i\to\infty} t_i = t_0$*, we have:*

1. *if for all* i*,* $\phi(\boldsymbol{x}(t_i)) > 0$*, then* $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ *and* $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x}_0,t_0)}\phi(\boldsymbol{x}_0) > 0$*;*
2. *if for all* i*,* $\phi(\boldsymbol{x}(t_i)) < 0$*, then* $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ *and* $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x}_0,t_0)}\phi(\boldsymbol{x}_0) < 0$*;*
3. *if for all* i*,* $\phi(\boldsymbol{x}(t_i)) = 0$*, then* $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) = \infty$*;* □

3.2 Transverse Set and Invariant

We use Lie derivatives to define *transverse set* :

Definition 11 (Transverse Set) Given a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, we define transverse set of region $S(p(\boldsymbol{x}) \geq 0)$ as:

$$Trans^{(t)}_{f\uparrow p} \doteq \{\boldsymbol{x} \in \mathbb{R}^n | \gamma_{f,p}(\boldsymbol{x}, t) < \infty \wedge \mathcal{L}_{t,f}^{\gamma_{f,p}(\boldsymbol{x},t)} p(\boldsymbol{x}) < 0\}$$ □

Intuitively, transverse set of region $S(p(\boldsymbol{x}) \geq 0)$ contains elements that are either not in the region or will leave the region(as system evolves from time t) immediately.

Using transverse set, we can give the necessary and sufficient condition of continuous invariants:

Theorem 4 *Given a hybrid system* $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$*,* $S(\phi(\boldsymbol{x}) \geq 0)$ *is an invariant of the system if and only if:*

1. *It contains the initial set* $\boldsymbol{I}$*. Which is:*

$$(\boldsymbol{I}(\boldsymbol{x}) \geq 0) \Rightarrow (\phi(x) \geq 0)$$

2. *Any time, as long as system evolves within its domain, any state in the boundary* $S(\phi(\boldsymbol{x}) = 0)$ *will not come out of the region* $S(\phi(\boldsymbol{x}) \geq 0)$*. Which is:*

$$(\phi(\boldsymbol{x}) = 0) \Rightarrow (\forall t > 0 : \boldsymbol{x} \in (Trans^{(t)}_{f\uparrow\phi})^c \cup Trans^{(t)}_{f\uparrow H})$$ □

Proof First we consider the necessary part. If the first condition is not satisfied, which means $(\boldsymbol{I}(\boldsymbol{x}) \geq 0) \not\Rightarrow (\phi(x) \geq 0)$, that is to say $\boldsymbol{I} \not\subseteq S(\phi(\boldsymbol{x}) \geq 0)$, which contradicts the first condition of Definition 4.

Now if the second condition is not satisfied, which means: there exists $\boldsymbol{x}_0$ and $t_0 > 0$ such that $\phi(\boldsymbol{x_0}) = 0$ and $\boldsymbol{x}_0 \in Trans^{(t_0)}_{f\uparrow\phi} \cap (Trans^{(t_0)}_{f\uparrow H})^c$. Then by Definition 11 and Theorem 3 we know:

$$\exists \epsilon > 0, \forall t \in (t_0, t_0 + \epsilon), (\boldsymbol{H}(\boldsymbol{x}(t)) \geq 0) \cap (\phi(\boldsymbol{x}(t) < 0))$$

which contradicts the second condition of Definition 4. That concludes the proof for the necessary part.

Next, let's consider the sufficient part. It's easy to see that the first condition of this theorem is essentially the same as the first condition of Definition 4. So we only need to prove $S(\phi(\boldsymbol{x}) \geq 0)$ also satisfies the second condition of Definition 4. Suppose the second condition doesn't satisfy, which means there exists $t_0 \geq 0$, $\boldsymbol{x}_0 \in S(\phi(\boldsymbol{x}) \geq 0)$ and $T_0 > 0$ such that for a certain trajectory $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$, the following satisfies:

$$(\forall t \in [t_0, t_0 + T_0], \boldsymbol{x}(t) \in \boldsymbol{H}) \nRightarrow (\forall t \in [t_0, t_0 + T_0], \boldsymbol{x}(t) \in S(\phi(\boldsymbol{x}) \geq 0))$$

which is equivalent to:

$$(\forall t \in [t_0, t_0 + T_0], \boldsymbol{H}(\boldsymbol{x}(t)) \geq 0) \wedge (\exists t \in [t_0, t_0 + T_0], \phi(\boldsymbol{x}(t)) < 0)$$

Now consider $\phi(\boldsymbol{x}(t))$ as a function. We know that $\phi(\boldsymbol{x}(t_0)) = \phi(\boldsymbol{x}_0) \geq 0$ and for some $t_c \in [t_0, t_0 + T_0]$, $\phi(\boldsymbol{x}(t_c)) < 0$. By the continuity of $\boldsymbol{x}$, there exists $t_z \in [t_0, t_c)$ such that $\phi(\boldsymbol{x}(t_z) = 0)$, which means the set $\{t \in [t_0, t_c) \mid \phi(\boldsymbol{x}(t)) = 0\}$ is not empty.

Take $t_m \doteq \sup\{t \in [t_0, t_c] \mid \phi(\boldsymbol{x}(t)) = 0\}$, By the definition of supremum and continuity of $\phi(\boldsymbol{x}(t))$, $\phi(\boldsymbol{x}(t_m)) = 0$. Denote $\boldsymbol{x}(t_m)$ by $\boldsymbol{x}_m$. As t_m is the rightmost zero point of $\phi(\boldsymbol{x}(t))$, $\phi(\boldsymbol{x}(t_c)) < 0$, we know: $\forall t \in (t_m, t_c), \phi(\boldsymbol{x}(t)) < 0$. Use Corollary 1, we get: $\gamma_{f,\phi}(\boldsymbol{x}_m, t_m) < \infty$ and $\mathcal{L}_{t_m,f}^{\gamma_{f,\phi}(\boldsymbol{x}_m,t_m)}\phi(\boldsymbol{x}(t_m)) < 0$. Recall Definition 11, that is exactly $\boldsymbol{x}_m \in Trans_{f\uparrow\phi}^{(t_m)}$.

Since $\forall t \in [t_0, t_0+T_0], \boldsymbol{H}(\boldsymbol{x}(t)) \geq 0$, certainly there is: $\forall t \in (t_m, t_c), \boldsymbol{H}(\boldsymbol{x}(t)) \geq 0$. Combine the first and third situation of Corollary 1, we get:

1. $\gamma_{f,\phi}(\boldsymbol{x}_m, t_m) < \infty$ and $\mathcal{L}_{t_m,f}^{\gamma_{f,\phi}(\boldsymbol{x}_m,t_m)}\phi(\boldsymbol{x}(t_m)) > 0$, or:
2. $\gamma_{f,\phi}(\boldsymbol{x}_m, t_m) = \infty$;

Either way, we have: $\boldsymbol{x}_m \notin Trans_{f\uparrow H}^{(t_m)}$.

But $\phi(\boldsymbol{x}_m) = 0$, that contradicts the second condition of this theorem. That concludes the proof for the sufficient part. ∎

3.3 Ideals Generated by Lie Derivatives

The problem of Definition 11 is that it involves infinity. This subsection aims to prove that either the rank of Lie derivative is infinity, or it's less than a computable upper-bound N. The main tool used will be ideals generated by Lie derivatives:

Definition 12 (Ideal Generated by Lie Derivatives) Given polynomial hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ and polynomial $\phi(\boldsymbol{x})$,in $\mathbb{R}[\boldsymbol{x}]$ we call:

$$\boldsymbol{I}_k^{(t)} \doteq \langle \mathcal{L}_{t,f}^0\phi(\boldsymbol{x}), \mathcal{L}_{t,f}^1\phi(\boldsymbol{x}), \ldots, \mathcal{L}_{t,f}^k\phi(\boldsymbol{x})\rangle$$

as the k-th ideal generated by Lie derivatives. Also call:

$$\boldsymbol{I}^{(t)} \doteq \bigcup_k \boldsymbol{I}_k^{(t)}$$

as the ideal generated by Lie derivatives. where $t \in \mathbb{R}$ is a parameter. □

We should note here t is considered to be a parameter in $\mathbb{R}$.

We want to prove that the ideal generated by Lie derivatives can be computed by finite steps of operations, to prove the above theorem, we will need an extra definition:

Definition 13 (Total Ideal Generated by Lie Derivatives) Consider $\mathcal{L}_{t,f}^k \phi(\boldsymbol{x})$ to be a element of $\mathbb{R}[t, \boldsymbol{x}]$, we call:

$$\boldsymbol{I}_k \doteq \langle \mathcal{L}_{t,f}^0 \phi(\boldsymbol{x}), \mathcal{L}_{t,f}^1 \phi(\boldsymbol{x}), \ldots, \mathcal{L}_{t,f}^k \phi(\boldsymbol{x}) \rangle$$

as the k-th total ideal generated by Lie derivatives. Also call:

$$\boldsymbol{I} \doteq \bigcup_k \boldsymbol{I}_k$$

as the ideal generated by Lie derivatives. □

We see that total ideal is just to consider t as a variable rather than parameter.

Now we are ready to prove the main theorem of this subsection:

Theorem 5 *There exists $N \in \mathbb{N}$ such that for every $t \in \mathbb{R}$, $\boldsymbol{I}^{(t)} = \boldsymbol{I}_N^{(t)}$.* □

Proof Total ideals generated by Lie derivatives form an ascending ideal chain:

$$\boldsymbol{I}_0 \subseteq \boldsymbol{I}_1 \subseteq \cdots \subseteq \boldsymbol{I}_k \subseteq \ldots$$

By Theorem 2, we know that there exists N such that for any $l \geq N$, $\boldsymbol{I}_l = \boldsymbol{I}_N$, which means $\boldsymbol{I}_N = \boldsymbol{I}$.

Now for arbitrary $t \in \mathbb{R}$, we assert that $\boldsymbol{I}_N^{(t)} = \boldsymbol{I}^{(t)}$. To see this, let's first explore the total ideal chain. To say $\boldsymbol{I}_N = \boldsymbol{I}$ is to say for any $l \geq N$, $\mathcal{L}_{t,f}^l \phi \in \langle \mathcal{L}_{t,f}^0 \phi, \mathcal{L}_{t,f}^1 \phi, \ldots, \mathcal{L}_{t,f}^N \phi \rangle$, which means there exists $\{g_j\} \in \mathbb{R}[t, \boldsymbol{x}]$ such that:

$$\mathcal{L}_{t,f}^l \phi = \sum_{0 \leq j \leq N} g_j \mathcal{L}_{t,f}^j \phi$$

Substitute the value of t into it, we get:

$$\mathcal{L}_{t,f}^l \phi = \sum_{0 \leq j \leq N} g_j' \mathcal{L}_{t,f}^j \phi$$

where $\{g_j'\} \in \mathbb{R}[\boldsymbol{x}]$, this equation holds in $\mathbb{R}[\boldsymbol{x}]$.

So we have: for any $t \in \mathbb{R}$, any $l \geq N$, $\mathcal{L}_{t,f}^l \phi \in \boldsymbol{I}_N^{(t)}$ holds. That leads to our final conclusion. ■

Corollary 2 *There exists $N \in \mathbb{N}$ which is independent to $\boldsymbol{x}$ and t such that $\gamma_{f,\phi}(\boldsymbol{x},t) < \infty$ if and only if $\gamma_{f,\phi}(\boldsymbol{x},t) \leq N$.* □

PROOF The sufficient part is obvious. We only need to consider the necessary part.

Take the N in Theorem 5, suppose $\gamma_{f,\phi}(\boldsymbol{x},t) > N$, since $\boldsymbol{I}_N = \boldsymbol{I}$, we have: $\mathcal{L}_{t,f}^{\gamma_{f,p}(\boldsymbol{x},t)} p(\boldsymbol{x}) \in \boldsymbol{I}_N$. So:

$$\mathcal{L}_{t,f}^{\gamma_{f,p}(\boldsymbol{x},t)} p(\boldsymbol{x}) = \sum_{0 \leq j \leq N} g_j \mathcal{L}_{t,f}^j p(\boldsymbol{x})$$

But with $\gamma_{f,\phi}(\boldsymbol{x},t) > N$, for $0 \leq j \leq N$ we have: $\mathcal{L}_{t,f}^j p(\boldsymbol{x}) = 0$. Substitute it into last equation we get: $\mathcal{L}_{t,f}^{\gamma_{f,p}(\boldsymbol{x},t)} = 0$, which contradicts Definition 8. ■

Next we will present an algorithm to find such a $N \in \mathbb{N}$. First we give a lemma:

Lemma 1 (Fixed Point Theorem) *If for some i we have:*

$$\mathcal{L}_{t,f}^{i+1} \phi \in \boldsymbol{I}_i^{(t)}$$

then for any $m > i$:

$$\mathcal{L}_{t,f}^{m} \phi \in \boldsymbol{I}_i^{(t)}$$

□

PROOF To prove this lemma, we use induction. The situation $m = i + 1$ is exactly what we already have. Suppose we have proved for some $k > i$, the lemma holds. Now we consider the situation $m = k + 1$. From induction hypothesis, we know:

$$\mathcal{L}_{t,f}^{k} \phi \in \langle \mathcal{L}_{t,f}^0 \phi, \mathcal{L}_{t,f}^1 \phi, \ldots, \mathcal{L}_{t,f}^i \phi \rangle$$

that is, for $0 \leq j \leq i$, there exists $\{g_j\} \in \mathbb{R}[\boldsymbol{x}]$ such that:

$$\mathcal{L}_{t,f}^{k} \phi = \sum_{0 \leq j \leq i} g_j \mathcal{L}_{t,f}^j \phi$$

Now for $\mathcal{L}_{t,f}^{k+1} \phi$, By Definition 7:

$$\begin{aligned}
\mathcal{L}_{t,f}^{k+1} \phi &= \langle \frac{\partial}{\partial \boldsymbol{x}} \mathcal{L}_{t,f}^k \phi(\boldsymbol{x}) \cdot \boldsymbol{f} \rangle \\
&= \langle \frac{\partial}{\partial \boldsymbol{x}} \sum_{0 \leq j \leq i} g_j \mathcal{L}_{t,f}^j \phi \cdot \boldsymbol{f} \rangle \\
&= \sum_{0 \leq j \leq i} \langle \mathcal{L}_{t,f}^j \phi \frac{\partial}{\partial \boldsymbol{x}} g_j \cdot \boldsymbol{f} \rangle + \sum_{0 \leq j \leq i} \langle g_j \frac{\partial}{\partial \boldsymbol{x}} \mathcal{L}_{t,f}^j \phi \cdot \boldsymbol{f} \rangle \\
&= \sum_{0 \leq j \leq i} \langle \frac{\partial}{\partial \boldsymbol{x}} g_j \cdot \boldsymbol{f} \rangle \mathcal{L}_{t,f}^j \phi + \sum_{0 \leq j \leq i} g_j \mathcal{L}_{t,f}^{j+1} \phi \\
&= \sum_{0 \leq j \leq i} \langle \frac{\partial}{\partial \boldsymbol{x}} g_j \cdot \boldsymbol{f} \rangle \mathcal{L}_{t,f}^j \phi + \sum_{0 \leq j < i} g_j \mathcal{L}_{t,f}^{j+1} \phi + g_i \mathcal{L}_{t,f}^{i+1} \phi
\end{aligned}$$

Recall the condition of this lemma, there is: $\mathcal{L}_{t,f}^{i+1}\phi \in \langle \mathcal{L}_{t,f}^{0}\phi, \mathcal{L}_{t,f}^{1}\phi, \ldots, \mathcal{L}_{t,f}^{i}\phi \rangle$. So in summary:

$$\mathcal{L}_{t,f}^{k+1} \in \langle \mathcal{L}_{t,f}^{0}\phi, \mathcal{L}_{t,f}^{1}\phi, \ldots, \mathcal{L}_{t,f}^{i}\phi \rangle = \boldsymbol{I}_i^{(t)}$$

That concludes our proof for this lemma. ■

The basic frame of our algorithm is:

COMPUTING UPPER BOUND N: ORIGINAL

```
1  i = 0, B = {L^0_{t,f}}
2  while TRUE
3      Compute L^{i+1}_{t,f} from L^i_{t,f}
4      Generate ideal I from basis B
           Ask whether L^{i+1}_{t,f} ∈ I using Gröbner basis
5          if L^{i+1}_{t,f} ∉ I
6              B = B ∪ {L^{i+1}_{t,f}}
7              i = i + 1
8          else
9              break
10     N = i
```

This is just a naive implement of Lemma 1. Next subsection we will give an alternative algorithm to compute the upper bound N.

3.4 Alternative Algorithm to Compute N

The algorithm we present in last subsection computes N using Gröbner basis, which is a rather "expensive" operation. Here we present an algorithm that avoids Gröbner basis, but may give a larger N comparing to the original algorithm. To achieve that goal, let's first consider monomial ideals:

Definition 14 A monomial ideal of $\mathbb{R}[\boldsymbol{x}]$ is an ideal that can be generated by a finite set of monomials. More specifically, $\boldsymbol{I}$ is a monomial ideal of $\mathbb{R}[\boldsymbol{x}]$ if and only if:

$$\boldsymbol{I} = \langle m_1, m_2, \ldots, m_k \rangle$$

where m_i is a monomial in $\mathbb{R}[\boldsymbol{x}]$. □

We use $m(p)$ to represent the leading term of polynomial p i.e. term that has the largest order. For an ideal $\boldsymbol{I} = \langle p_0, p_1, \ldots, p_k \rangle$, we define $m(\boldsymbol{I}) \doteq \langle m(p_0), m(p_1), \ldots, m(p_k) \rangle$. When order monomials, we use the *degree-lexicographic order*, which is a total ordering compatible with the natural graduation by total degree.

We start with a lemma:

Lemma 2 *Given polynomials $p_0, p_1, \ldots, p_n$. Let $\boldsymbol{I}_i = \langle p_0, \ldots, p_i \rangle$. if:*

$$\boldsymbol{I}_0 \subsetneq \boldsymbol{I}_1 \subsetneq \cdots \subsetneq \boldsymbol{I}_n$$

then:

$$m(\boldsymbol{I}_0) \subsetneq m(\boldsymbol{I}_1) \subsetneq \cdots \subsetneq m(\boldsymbol{I}_n)$$ □

PROOF We prove this lemma step by step. For $\boldsymbol{I}_i$, since $\boldsymbol{I}_i \subsetneq \boldsymbol{I}_{i+1}$, we know that $p_{i+1} \notin \boldsymbol{I}_i$. If $m(\boldsymbol{p}_{i+1}) \notin m(\boldsymbol{I}_i)$, then $m(\boldsymbol{I}_i) \subsetneq m(\boldsymbol{I}_{i+1})$. Otherwise there is some $j \leq i$ such that $m(p_j)$ divides $m(p_{i+1})$. In that case, substitute p_{i+1} with non-zero rest p'_{i+1} of ordered division of p_{i+1} by p_j, note $\boldsymbol{I}_k$ and $m(\boldsymbol{I}_k)$ stay unchanged. As the order of p'_{i+1} drops, the process will end in finite steps, so we also have $m(\boldsymbol{I}_i) \subsetneq m(\boldsymbol{I}_{i+1})$.

Take i from 0 to $n-1$, we get the conclusion of this lemma. ■

Now we can give the alternative algorithm to compute N:

COMPUTING UPPER BOUND N: ALTERNATIVE

```
1  i = 0, p_0 = L^0_{t,f}, B = {m(p_0)}
2  while TRUE
3      Compute L^{i+1}_{t,f} from L^i_{t,f}, p_{i+1} = L^{i+1}_{t,f}
4      while p_{i+1} ≠ 0 and there exists m(p_j) ∈ B divides m(p_{i+1})
5          p_{i+1} = rest of ordered division of p_{i+1} by p_j
6      if p_{i+1} equals to 0
7          break
8      B = B ∪ {m(p_{i+1})}
9      i = i + 1
10 N = i
```

Every time the inside while loop executed, the degree of p_{i+1} strictly drops. So the inside while loop can only be executed finite times. As for the outer loop, it's easy to prove $\boldsymbol{B}$ of each loop execution generates a strictly ascending ideal chain, so by Theorem 2 it also ends after finite times of execution.

When the program terminates, when have $m(\boldsymbol{I}_{i+1}) = m(\boldsymbol{I}_i)$. By Lemma 2, i satisfies the condition $\boldsymbol{I}_{i+1} = \boldsymbol{I}_i$, so it is a valid upper bound N.

3.5 Verify Invariants of Hybrid System: Simple Case

Now, with previous discussions, we are ready to give the algorithm to verify invariant of hybrid system. To do this, first we translate the conditions of Theorem 4 into first order logic formula of finite length, then use quantifier elimination to get the equivalent quantifier-free formula. Since all variables are bounded, the resulting quantifier-free formula will be either *TRUE* or *FALSE*. *TRUE* means the possible invariant is indeed an invariant of our hybrid system, while *FALSE* means it is not an invariant of out hybrid system. First let's see how to do the translate:

Theorem 6 *Given a hybrid system* $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ *and a polynomial* $\phi(\boldsymbol{x})$*. We can construct a finite length formula* $\theta(\phi, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t)$ *such that* $\phi(\boldsymbol{x}) \geq 0$ *is an invariant if and only if formula* $(\boldsymbol{I}(\boldsymbol{x}) \geq 0) \rightarrow (\phi(\boldsymbol{x}) \geq 0)$ *and formula* $\theta(\phi, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t)$ *all satisfy.* □

PROOF Recall Theorem 4. Obviously, $\boldsymbol{I} \subseteq S(\phi(\boldsymbol{x}) \geq 0)$ if and only if formula

$$(\boldsymbol{I}(\boldsymbol{x}) \geq 0) \rightarrow (\phi(\boldsymbol{x}) \geq 0)$$

satisfies.

Now by Definition 11, $\forall t \geq 0, \boldsymbol{x} \in (Trans^{(t)}_{f\uparrow\phi})^c \cup Trans^{(t)}_{f\uparrow H}$ if and only if:

$$\forall t \geq 0, \neg(\gamma_{f,\phi}(\boldsymbol{x}, t) < \infty \wedge \mathcal{L}_{t,f}^{\gamma_{f,\phi}(\boldsymbol{x},t)} < 0) \vee (\gamma_{f,\boldsymbol{H}}(\boldsymbol{x}, t) < \infty \wedge \mathcal{L}_{t,f}^{\gamma_{f,H}(\boldsymbol{x},t)} < 0)$$

Use Corollary 2, it's equivalent to:

$$\forall t \geq 0, \neg(\gamma_{f,\phi}(\boldsymbol{x}, t) \leq N \wedge \mathcal{L}_{t,f}^{\gamma_{f,\phi}(\boldsymbol{x},t)} < 0) \vee (\gamma_{f,\boldsymbol{H}}(\boldsymbol{x}, t) \leq N \wedge \mathcal{L}_{t,f}^{\gamma_{f,H}(\boldsymbol{x},t)} < 0)$$

for a computable natural number N.

If we take:

$$\pi^{(0)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \phi(\boldsymbol{x}) < 0$$
$$\pi^{(i)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq (\bigwedge_{0 \leq j < i} \mathcal{L}^j_{t,f}\phi(\boldsymbol{x}) = 0) \wedge \mathcal{L}^i_{t,f}\phi(\boldsymbol{x}) < 0 \qquad i > 0$$

and let:

$$\pi(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \bigvee_{0 \leq i \leq N} \pi^{(i)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$$

then $\forall t \geq 0, \boldsymbol{x} \in (Trans^{(t)}_{f\uparrow\phi})^c \cup Trans^{(t)}_{f\uparrow H}$ if and only if formula

$$\forall t((t \geq 0) \rightarrow (\neg\pi(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \vee \pi(\boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t)))$$

which is equivalent to formula:

$$\forall t((t < 0) \vee (\pi(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \wedge \neg\pi(\boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t)))$$

satisfies.

Now the second condition of Theorem 4 can be translated into:

$$\theta(\phi, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t) \doteq (\phi(\boldsymbol{x}) = 0) \rightarrow (\forall t((t < 0) \vee (\pi(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \wedge \neg\pi(\boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t))))$$ ■

The basic structure of our verifying algorithm is as follows:

1. Use the original or alternative algorithm to compute the upper bound N for ϕ and $\boldsymbol{f}$.
2. Construct $\theta(\phi, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t)$ as in the proof of Theorem 6.
3. Apply quantifier elimination algorithms on formula $\forall \boldsymbol{x}(\theta(\phi, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{x}, t) \wedge ((\boldsymbol{I}(\boldsymbol{x}) \geq 0) \rightarrow (\phi(\boldsymbol{x}) \geq 0)))$.
4. If the result is *TRUE*, then $\phi(\boldsymbol{x}) \geq 0$ is an invariant; if the result is *FALSE*, then $\phi(\boldsymbol{x}) \geq 0$ is not an invariant.

3.6 Generate Invariants of Hybrid System: Simple Case

Using the notion of *template*, we can derive an algorithm to generate invariants of hybrid system from the algorithm we presented in last subsection. A template is a parametrized polynomial $p(\boldsymbol{u}, \boldsymbol{x}) \in \mathbb{R}[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$ where $u_1, u_2, \ldots, u_m$ are parameters. Our target is to find an invariant $\phi(\boldsymbol{x})$ such that for some $\boldsymbol{u}_0$, $p(\boldsymbol{u}_0, \boldsymbol{x}) = \phi(\boldsymbol{x})$, or report error if no such invariant exists.

First we notice that Theorem 5 and related corollaries can be extended to situation when the number of parameters is more than one:

Lemma 3 *There exists $N \in \mathbb{N}$ which is independent to $\boldsymbol{x}$ and t and $\boldsymbol{u}$ such that $\gamma_{f,\phi}(\boldsymbol{x}, t) < \infty$ if and only if $\gamma_{f,\phi}(\boldsymbol{x}, t) \leq N$.* □

Also, the original and alternative algorithm both work for multiple parameters. Now we give the structure of our generating algorithm:

1. Set a template $p(\boldsymbol{u}, \boldsymbol{x}) \in \mathbb{R}[\boldsymbol{u}, \boldsymbol{x}]$.
2. Use the original or alternative algorithm to compute the upper bound N for p and $\boldsymbol{f}$.
3. Construct $\theta(p, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{u}, \boldsymbol{x}, t)$ as in the proof of Theorem 6.
4. Apply quantifier elimination algorithms on formula $\forall \boldsymbol{x}(\theta(p, \boldsymbol{H}, \boldsymbol{f}, \boldsymbol{u}, \boldsymbol{x}, t) \wedge ((\boldsymbol{I}(\boldsymbol{x}) \geq 0) \rightarrow (p(\boldsymbol{u}, \boldsymbol{x}) \geq 0)))$.
5. Consider the obtained quantifier-free formula $\Xi(\boldsymbol{u})$ as a constrain on $\boldsymbol{u}$. If $\Xi(\boldsymbol{u}) = \mathit{FALSE}$ then report error. Otherwise use a constrain solver, such as DISCOVERER[12], to find a solution $\boldsymbol{u}_0$.
6. Let $\phi(\boldsymbol{x}) = p(\boldsymbol{u}_0, \boldsymbol{x})$, then $\phi(\boldsymbol{x}) \geq 0$ is an invariant.

4 General Case

We consider invariant verification and generation for general polynomial hybrid system in this section. The domain and initial set will be:

$$\boldsymbol{H} = S(\bigvee_{i=1}^{I} \bigwedge_{j=1}^{J_i} p_{ij}(\boldsymbol{x}) \rhd 0)$$

$$\boldsymbol{I} = S(\bigvee_{i=1}^{N} \bigwedge_{j=1}^{M_i} q_{ij}(\boldsymbol{x}) \rhd 0)$$

and the possible invariant takes form:

$$\phi = \bigvee_{k=1}^{K} \bigwedge_{j=1}^{L_k} (p_{kl}(\boldsymbol{x}) \rhd 0)$$

where $\rhd \in \{>, \geq\}$.

The basic idea is almost the same as that of last section. However, the complex boundaries of invariants, domain and initial set require some extra discussion. Strict proofs are often omitted as they are often repeat of what we did in last section.

4.1 Inward Set and Inverse Inward Set: Definitions and Properties

We define inward set as:

Definition 15 (Inward Set) Given a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, the inward set of a set A is defined as:

$$\mathrm{In}_f^{(t_0)}(A) \doteq \{\boldsymbol{x}_0 \in \mathbb{R}^n \mid \forall \boldsymbol{x} : \boldsymbol{x}(t_0) = \boldsymbol{x}_0 \wedge \exists \epsilon > 0 \forall t \in (t_0, t_0 + \epsilon), \boldsymbol{x}(t) \in A\}$$

where $\boldsymbol{x}$ is a trajectory of the hybrid system. □

Similarly, define inverse inward set as:

Definition 16 (Inverse Inward Set) Given a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, the inverse inward set of a set A is defined as:

$$\mathrm{IvIn}_f^{(t_0)}(A) \doteq \{\boldsymbol{x}_0 \in \mathbb{R}^n \mid \exists \boldsymbol{x} : \boldsymbol{x}(t_0) = \boldsymbol{x}_0 \wedge \exists \epsilon > 0 \forall t \in (t_0 - \epsilon, t_0), \boldsymbol{x}(t) \in A\}$$

where $\boldsymbol{x}$ is a trajectory of the hybrid system. □

Intuitively, $\boldsymbol{x}_0 \in \mathrm{In}_f^{(t_0)}(A)$ means any trajectories that pass $\boldsymbol{x}_0$ at t_0 must stay in A for a positive time. While $\boldsymbol{x}_0 \in \mathrm{IvIn}_f^{(t_0)}(A)$ means any trajectories that pass $\boldsymbol{x}_0$ at t_0 must come from A.

The inward set and inverse inward set are useful when describing general continuous invariants:

Theorem 7 *Given a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, a set Ψ is an invariant if and only if:*

1. $\boldsymbol{I} \subseteq \Psi$;
2. $\forall t \geq 0, \forall \boldsymbol{x}(\boldsymbol{x} \in \Psi \cap \boldsymbol{H} \cap \mathrm{In}_f^{(t)}(\boldsymbol{H}) \Rightarrow \boldsymbol{x} \in \mathrm{In}_f^{(t)}(\Psi))$;
3. $\forall t \geq 0, \forall \boldsymbol{x}(\boldsymbol{x} \in \Psi^c \cap \boldsymbol{H} \cap \mathrm{IvIn}_f^{(t)}(\boldsymbol{H}) \Rightarrow \boldsymbol{x} \in (\mathrm{IvIn}_f^{(t)}(\Psi))^c)$. □

Proof The first condition of Definitiondef:invariant and the first condition of this theorem coincides, so we only need to consider the rest.

First let's consider the sufficient part. Recall Definitiondef:invariant, if Ψ is not an invariant, then we have: there exists $t_0 \geq 0$, $\boldsymbol{x}_0 \in \Psi$ and $T_0 \geq 0$ such that:

$$(\forall t \in [t_0, t_0 + T_0], \boldsymbol{x}(t) \in \boldsymbol{H}) \nRightarrow (\forall t \in [t_0, t_0 + T_0], \boldsymbol{x}(t) \in \Psi)$$

which is equivalent to:

$$(\forall t \in [t_0, t_0 + T_0], \boldsymbol{x}(t) \in \boldsymbol{H}) \wedge (\exists t \in [t_0, t_0 + T_0], \boldsymbol{x}(t) \notin \Psi))$$

Take $t_z \in [t_0, t_0 + T_0]$ such that $\boldsymbol{x}(t_z) \notin \Psi$, and let

$$t_m = \inf\{t \in [t_0, t_c] \mid \boldsymbol{x}(t) \notin \Psi\}$$

By the definition of t_m, $\boldsymbol{x}([t_0, t_m)) \subseteq \Psi$. Now consider $\boldsymbol{x}_m \doteq \boldsymbol{x}(t_m)$.

If $\boldsymbol{x}_m \notin \Psi$, then $\boldsymbol{x}_m$ satisfies:

$$\boldsymbol{x_m} \in \Psi^c \cap \boldsymbol{H} \cap \mathrm{IvIn}_f^{(t)}(\boldsymbol{H}) \cap \mathrm{IvIn}_f^{(t)}(\Psi)$$

Which contradicts the third condition.

If $\boldsymbol{x}_m \in \Psi$, then $t_m < t_0 + T_0$, $\boldsymbol{x}_m$ satisfies:

$$\boldsymbol{x} \in \Psi \cap \boldsymbol{H} \cap \mathrm{In}_f^{(t)}(\boldsymbol{H}) \cap (\mathrm{In}_f^{(t)}(\Psi)))^c$$

Which contradicts the second condition.

Next we consider the necessary part. If the second condition doesn't hold, which is:

$$\exists t_0 \geq 0, \exists \boldsymbol{x}_0 \in \Psi \cap \boldsymbol{H} \cap \mathrm{In}_f^{(t_0)}(\boldsymbol{H}) \cap (\mathrm{In}_f^{(t_0)}(\Psi))^c$$

Recall Definition 15, that is to say: there exists a trajectory $\boldsymbol{x}$ satisfying $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$ such that: $\forall \epsilon > 0 \exists t_\epsilon \in (t_0, t_0 + \epsilon) : \boldsymbol{x}(t) \notin \Psi$, which contradicts the second condition of Definition 4.

If the third condition doesn't hold, which is:

$$\exists t_0 \geq 0, \exists \boldsymbol{x}_0 \in \Psi^c \cap \boldsymbol{H} \cap \mathrm{IvIn}_f^{(t_0)}(\boldsymbol{H}) \cap \mathrm{IvIn}_f^{(t_0)}(\Psi)$$

Recall Definition 16, that is to say: there exists a trajectory $\boldsymbol{x}$ satisfying $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$, $\exists \epsilon > 0 \forall t \in (t_0 - \epsilon, t_0) : \boldsymbol{x}(t) \in \Psi$, which also contradicts the second condition of Definition 4. ■

Inward set and inverse inward set have the following properties:

Theorem 8 *For any $A, B \subseteq \mathbb{R}^n$,*

1. *If A is a open set, then: $A \subseteq \mathrm{In}_f^{(t)}(A) A \subseteq \mathrm{IvIn}_f^{(t)}(A)$ for any $t \in \mathbb{R}$.*
2. *If $A \cap B = \emptyset$, then: $\mathrm{In}_f^{(t)}(A) \cap \mathrm{In}_f^{(t)}(B) = \emptyset$ and $\mathrm{IvIn}_f^{(t)}(A) \cap \mathrm{IvIn}_f^{(t)}(B) = \emptyset$ for any $t \in \mathbb{R}$.* □

Proof Proof can be obtained by checking definitions. Detailed proof is omitted here. ■

4.2 Inward Set and Inverse Inward Set: Lie Derivatives

We want to use Lie derivatives to describe inward set and inverse inward set. To do this, Theorem 3 should be extended to include the inverse part of trajectories:

Theorem 9 *Given polynomial ϕ and hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$, $\gamma_{f,\phi}(\boldsymbol{x}_0, t) \neq 0$ if and only if $\boldsymbol{x}_0 \in S(\phi(\boldsymbol{x}) = 0)$, and if we take $\boldsymbol{x}(t_0) = \boldsymbol{x}_0$, then it follows that:*

1. *if $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ and $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0) > 0$, then:*

$$\exists \epsilon > 0, \forall t \in (t_0, t_0 + \epsilon), \phi(\boldsymbol{x}(t)) > 0$$

2. *if $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ and $\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0) < 0$, then:*

$$\exists \epsilon > 0, \forall t \in (t_0, t_0 + \epsilon), \phi(\boldsymbol{x}(t)) < 0$$

3. *If $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ and $(-1)^{\gamma_{f,\phi}(\boldsymbol{x}_0,t_0)}\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0) > 0$, then:*

$$\exists \epsilon > 0, \forall t \in (t_0 - \epsilon, t_0), \phi(\boldsymbol{x}(t)) > 0$$

4. *If $\gamma_{f,\phi}(\boldsymbol{x}_0, t_0) < \infty$ and $(-1)^{\gamma_{f,\phi}(\boldsymbol{x}_0,t_0)}\mathcal{L}_{t_0,f}^{\gamma_{f,\phi}(\boldsymbol{x},t_0)}\phi(\boldsymbol{x}_0) < 0$, then:*

$$\exists \epsilon > 0, \forall t \in (t_0 - \epsilon, t_0), \phi(\boldsymbol{x}(t)) < 0$$

5. *if $\gamma_{f,\phi}(\boldsymbol{x}, t_0) = \infty$, then:*

$$\exists \epsilon > 0, \forall t \in (t_0 - \epsilon, t_0 + \epsilon), \phi(\boldsymbol{x}(t)) = 0$$ □

Proof The proof is almost the same of Theorem 3. ■

Then, let's consider inward set and inverse inward set of sets defined by a single polynomial. For convenience, we write $\mathrm{In}_f^{(t)}(\phi \rhd 0)$, $\mathrm{IvIn}_f^{(t)}(\phi \rhd 0)$ to denote $\mathrm{In}_f^{(t)}(S(\phi \rhd 0))$ and $\mathrm{In}_f^{(t)}(S(\phi \rhd 0))$. We have:

Theorem 10 *Given a hybrid system $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ and polynomial ϕ, we have:*

- $\mathrm{In}_f^{(t)}(\phi > 0) = \Theta_+^{(t)}(\phi, \boldsymbol{f})$
- $\mathrm{In}_f^{(t)}(\phi \geq 0) = \Theta_+^{(t)}(\phi, \boldsymbol{f}) \cup \Theta_0^{(t)}(\phi, \boldsymbol{f})$
- $\mathrm{IvIn}_f^{(t)}(\phi > 0) = \Theta_-^{(t)}(\phi, \boldsymbol{f})$
- $\mathrm{IvIn}_f^{(t)}(\phi \geq 0) = \Theta_-^{(t)}(\phi, \boldsymbol{f}) \cup \Theta_0^{(t)}(\phi, \boldsymbol{f})$

for any $t \in \mathbb{R}$.
where:

- $\Theta_+^{(t)}(\phi, \boldsymbol{f}) \doteq \{\boldsymbol{x} \in \mathbb{R}^n \mid \gamma_{\phi,f}(\boldsymbol{x},t) < \infty \wedge \mathcal{L}_{t,f}^{\gamma_{\phi,f}(\boldsymbol{x},t)}\phi(\boldsymbol{x}) > 0\}$
- $\Theta_0^{(t)}(\phi, \boldsymbol{f}) \doteq \{\boldsymbol{x} \in \mathbb{R}^n \mid \gamma_{\phi,f}(\boldsymbol{x},t) = \infty\}$
- $\Theta_-^{(t)}(\phi, \boldsymbol{f}) \doteq \{\boldsymbol{x} \in \mathbb{R}^n \mid \gamma_{\phi,f}(\boldsymbol{x},t) < \infty \wedge (-1)^{\gamma_{\phi,f}(\boldsymbol{x},t)}\mathcal{L}_{t,f}^{\gamma_{\phi,f}(\boldsymbol{x},t)}\phi(\boldsymbol{x}) > 0\}$ □

PROOF Combine Theorem 9 and Definition **??**, and apply the same method as used in the proof of Theorem 4. ■

For general semi-algebraic set

$$A \doteq \bigvee_{k=1}^{K} \bigwedge_{j=1}^{J_k} (p_{kj} \rhd 0)$$

we have:

Theorem 11

$$\mathrm{In}_f^{(t)}(A) = \bigvee_{k=1}^{K} \bigwedge_{j=1}^{J_k} \mathrm{In}_f^{(t)}(p_{kj} \rhd 0)$$

$$\mathrm{IvIn}_f^{(t)}(A) = \bigvee_{k=1}^{K} \bigwedge_{j=1}^{J_k} \mathrm{IvIn}_f^{(t)}(p_{kj} \rhd 0)$$

for any $t \in \mathbb{R}$. □

PROOF Use Theorem 8. ■

Now we are ready to give the Lie derivative description of inward set and inverse inward set:

Theorem 12 *Given a hybrid system* $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ *and semi-algebraic set A:*

$$A = \bigvee_{k=1}^{K} (\bigwedge_{j=1}^{j_k} (p_{kj} \geq 0) \wedge \bigwedge_{j=j_k+1}^{J_k} (p_{kj} > 0))$$

we have:

$$\mathrm{In}_f^{(t)}(A) = \bigvee_{k=1}^{K} (\bigwedge_{j=1}^{j_k} (\Theta_+^{(t)}(p_{kj}, \boldsymbol{f}) \cup \Theta_0^{(t)}(\phi, \boldsymbol{f})) \wedge \bigwedge_{j=j_k+1}^{J_k} \Theta_+^{(t)}(\phi, \boldsymbol{f}))$$

and:

$$\mathrm{IvIn}_f^{(t)}(A) = \bigvee_{k=1}^{K} (\bigwedge_{j=1}^{j_k} (\Theta_-^{(t)}(p_{kj}, \boldsymbol{f}) \cup \Theta_0^{(t)}(\phi, \boldsymbol{f})) \wedge \bigwedge_{j=j_k+1}^{J_k} \Theta_-^{(t)}(\phi, \boldsymbol{f}))$$

for any $t \in \mathbb{R}$.

The definition of Θ_+, Θ_- *and* Θ_0 *can be found in Theorem 10.* □

PROOF Combine Theorem 10 and Theorem 11. ■

4.3 Verify Invariants of Polynomial Hybrid System: General Case

In this subsection, we extend our verifying algorithm presented in last section to general semi-algebraic case. First we consider when the possible invariant is a polynomial, note that we can still use algorithms of 3.3 and 3.4 to compute the upper bound N despite the complexity of boundaries. We have the following theorem:

Theorem 13 *Take:*

$$\pi_+^{(0)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \phi(\boldsymbol{x}) > 0$$
$$\pi_+^{(i)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq (\bigwedge_{0 \le j < i} \mathcal{L}_{t,f}^j \phi(\boldsymbol{x}) = 0) \wedge \mathcal{L}_{t,f}^i \phi(\boldsymbol{x}) > 0 \qquad i > 0$$
$$\pi_+(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \bigvee_{0 \le i \le N} \pi_+(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$$
$$\pi_0(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \bigvee_{0 \le i \le N} \mathcal{L}_{t,f}^i \phi(\boldsymbol{x}) = 0$$
$$\pi_-^{(0)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \phi(\boldsymbol{x}) < 0$$
$$\pi_-^{(i)}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq (\bigwedge_{0 \le j < i} \mathcal{L}_{t,f}^j \phi(\boldsymbol{x}) = 0) \wedge \mathcal{L}_{t,f}^i \phi(\boldsymbol{x}) < 0 \qquad i > 0$$
$$\pi_-(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \bigvee_{0 \le i \le N} \pi_-(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$$

Then:

- $\boldsymbol{x} \in \mathrm{In}_f^{(t)}(\phi > 0)$ *if and only if formula* $\pi_+(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$ *satisfies.*
- $\boldsymbol{x} \in \mathrm{In}_f^{(t)}(\phi \ge 0)$ *if and only if formula* $\pi_{+,0}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \pi_+(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \vee \pi_0(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$ *satisfies.*
- $\boldsymbol{x} \in \mathrm{IvIn}_f^{(t)}(\phi > 0)$ *if and only if formula* $\pi_-(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$ *satisfies.*
- $\boldsymbol{x} \in \mathrm{IvIn}_f(t)(\phi \ge 0)$ *if and only if formula* $\pi_{-,0}(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \doteq \pi_-(\phi, \boldsymbol{f}, \boldsymbol{x}, t) \vee \pi_0(\phi, \boldsymbol{f}, \boldsymbol{x}, t)$*satisfies.* □

Proof Use the same technique as Theorem 6 to translate the conclusion of Theorem 10 into finite length formula. ■

Now for general semi-algebraic invariants:

Theorem 14 *Given a hybrid system* $(\boldsymbol{H}, \boldsymbol{I}, \boldsymbol{f})$ *and semi-algebraic set* Ψ *where:*

$$\boldsymbol{H} = \bigvee_{k=1}^{K} (\bigwedge_{j=1}^{j_k} (p_{kj} \ge 0) \wedge \bigwedge_{j=j_k+1}^{J_k} (p_{kj} > 0))$$
$$\Psi = \bigvee_{m=1}^{M} (\bigwedge_{l=1}^{l_m} (p_{ml} \ge 0) \wedge \bigwedge_{l=l_m+1}^{L_m} (p_{ml} > 0))$$

and let $\mathcal{I}$, $\mathcal{H}$, Ψ denote the formula that defines set $\boldsymbol{I}$, $\boldsymbol{H}$, Ψ respectively. By our assumption, $\boldsymbol{I}$, $\boldsymbol{H}$, Ψ are semi-algebraic sets, so $\mathcal{I}$, $\mathcal{H}$, Ψ are boolean combinations of polynomial formulas.

We have: Ψ is an invariant of the hybrid system if and only if formula:

$$\begin{aligned}
&\forall \boldsymbol{x} : \mathcal{I} \to \Psi \\
&\forall t : (t < 0) \vee (\forall \boldsymbol{x} : \Psi \wedge \mathcal{H} \wedge \xi_{+,H} \to \xi_{+,\Psi}) \\
&\forall t : (t < 0) \vee (\forall \boldsymbol{x} : \neg\Psi \wedge \mathcal{H} \wedge \xi_{-,H} \to \neg\xi_{-,\Psi})
\end{aligned}$$

all satify.

Where:

$$\begin{aligned}
\xi_{+,H} &\doteq \bigvee_{k=1}^{K} (\bigwedge_{j=1}^{j_k} \pi_{+,0}(p_{kj}, \boldsymbol{f}, \boldsymbol{x}, t) \wedge \bigwedge_{j=j_k+1}^{J_k} \pi_{+}(p_{kj}, \boldsymbol{f}, \boldsymbol{x}, t)) \\
\xi_{+,\Psi} &\doteq \bigvee_{m=1}^{M} (\bigwedge_{l=1}^{l_k} \pi_{+,0}(p_{ml}, \boldsymbol{f}, \boldsymbol{x}, t) \wedge \bigwedge_{l=l_k+1}^{\mathcal{L}_k} \pi_{+}(p_{ml}, \boldsymbol{f}, \boldsymbol{x}, t)) \\
\xi_{-,H} &\doteq \bigvee_{k=1}^{K} (\bigwedge_{j=1}^{j_k} \pi_{-,0}(p_{kj}, \boldsymbol{f}, \boldsymbol{x}, t) \wedge \bigwedge_{j=j_k+1}^{J_k} \pi_{-}(p_{kj}, \boldsymbol{f}, \boldsymbol{x}, t)) \\
\xi_{-,\Psi} &\doteq \bigvee_{m=1}^{M} (\bigwedge_{l=1}^{l_k} \pi_{-,0}(p_{ml}, \boldsymbol{f}, \boldsymbol{x}, t) \wedge \bigwedge_{l=l_k+1}^{\mathcal{L}_k} \pi_{-}(p_{ml}, \boldsymbol{f}, \boldsymbol{x}, t))
\end{aligned}$$

□

PROOF Use the conclusion of Theorem 14 and Theorem 11 to translate the conclusion of Theorem 7. ■

Now we give the basic structure of the verifying algorithm:

1. Use the original or alternative algorithm to compute the upper bound N for every p_{ml} and p_{kj}.
2. Construct the formula in Theorem 14.
3. Apply quantifier elimination algorithms on that formula.
4. If the result is *TRUE*, then Ψ is an invariant; if the result is *FALSE*, then Ψ is not an invariant.

4.4 Generate Invariants of Hybrid System: General Case

We also give the generating algorithm for general case:

1. Set semi-algebraic invariant template:

$$\Psi(\boldsymbol{u}, \boldsymbol{x}) = \bigvee_{m=1}^{M} (\bigwedge_{l=1}^{l_m} (p_{ml}(\boldsymbol{u}, \boldsymbol{x}) \geq 0) \wedge \bigwedge_{l=l_m+1}^{L_m} (p_{ml}(\boldsymbol{u}, \boldsymbol{x}) > 0))$$

   for some $p_{ml} \in \mathbb{R}[\boldsymbol{u}, \boldsymbol{x}]$.

2. Use the original or alternative algorithm to compute the upper bound N for every p_{ml} and p_{kj}.

3. Construct the formula in Theorem 14.

4. Apply quantifier elimination algorithms on that formula.

5. Consider the obtained quantifier-free formula $\Xi(\boldsymbol{u})$ as a constrain on $\boldsymbol{u}$. If $\Xi(\boldsymbol{u}) = \mathit{FALSE}$ then report error. Otherwise use a constrain solver, such as DISCOVERER[12], to find a solution $\boldsymbol{u}_0$.

6. Let $\Psi_0(\boldsymbol{x}) = \Psi(\boldsymbol{u}_0, \boldsymbol{x})$, then $\Psi_0(\boldsymbol{x})$ is an invariant.

5 Conclusion

In this article we propose a sound and complete algorithm to verify invariants of polynomial non-autonomous hybrid systems. From it we derive a sound and relatively complete algorithm to automatically generate invariants for such systems. "Relatively" means invariant generation needs a pre-defined template.

Quantifier elimination in real closed field play a critical role in our approach. Since the problem has a double exponential time nature[1], time consumption of our algorithm grows very quickly as the number of variables grows. Still, besides its theoretical meanings, our approach has proved to be a possible choice for automatic invariant generation for small systems.

The chain of ideals generated by Lie derivatives has finite length. A primitive recursive upper bound of that length can be found[10, 4]. This upper-bound is useful in constructive proof and time complexity analysis, but it's often too large to be practical comparing to the upper bound computed by the original and alternative algorithm presented in 3.3 and 3.4. Thus it's not included in previous sections.

Further problems: how to use heuristic strategy in choosing template and verifying invariants; find sub-problems where our approach can be more competitive.

References

[1] Christopher W Brown and James H Davenport. The complexity of quantifier elimination and cylindrical algebraic decomposition. In *Proceedings of the 2007 international symposium on Symbolic and algebraic computation*, pages 54–60. ACM, 2007.

[2] Edmund Clarke, Ansgar Fehnker, Zhi Han, Bruce Krogh, Joël Ouaknine, Olaf Stursberg, and Michael Theobald. Abstraction and counterexample-guided refinement in model checking of hybrid systems. *International Journal of Foundations of Computer Science*, 14(04):583–604, 2003.

[3] David Cox, John Little, and Donal O'shea. *Ideals, varieties, and algorithms*, volume 3. Springer, 1992.

[4] Diego Figueira, Santiago Figueira, Sylvain Schmitz, and Philippe Schnoebelen. Ackermannian and primitive-recursive bounds with dickson's lemma. In *Logic in Computer Science (LICS), 2011 26th Annual IEEE Symposium on*, pages 269–278. IEEE, 2011.

[5] Holger Giese and Stefan Henkler. A survey of approaches for the visual model-driven development of next generation software-intensive systems. *Journal of Visual Languages & Computing*, 17(6):528–550, 2006.

[6] Hui Kong, Sergiy Bogomolov, Christian Schilling, Yu Jiang, and Thomas A Henzinger. Invariant clusters for hybrid systems. *arXiv preprint arXiv:1605.01450*, 2016.

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

[8] Stephen Prajna and Ali Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems: Computation and Control*, pages 477–492. Springer, 2004.

[9] Sriram Sankaranarayanan, Henny B Sipma, and Zohar Manna. Constructing invariants for hybrid systems. In *Hybrid Systems: Computation and Control*, pages 539–554. Springer, 2004.

[10] Guillermo Moreno Socias. Length of polynomial ascending chains and primitive recursiveness. *Mathematica Scandinavica*, 71:181–205, 1992.

[11] Morris Tenenbaum and Harry Pollard. *Ordinary differential equations: An elementary textbook for students of mathematics, engineering, and the sciences*, chapter 9, pages 562–563. Courier Corporation, 1963.

[12] Bican Xia. Discoverer: a tool for solving semi-algebraic systems. *ACM Communications in Computer Algebra*, 41(3):102–103, 2007.