TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 12/12 pp211-222
Volume 19, Number 2, April 2014

Safety Verification of Semi-Algebraic Dynamical Systems via Inductive Invariant

Hui Kong*, Fei He, Xiaoyu Song, Ming Gu, Hongyan Tan, and Jiaguang Sun

Abstract: To verify the safety of nonlinear dynamical systems based on inductive invariants, key issues include defining the most complete inductive condition and discovering an inductive invariant that satisfies the specified inductive condition. In this paper, to lay a solid foundation for future research into the safety verification of semi-algebraic dynamical systems, we first establish a formal framework for evaluating the quality of continuous inductive conditions. In addition, we propose a new complete and computable inductive condition for verifying the safety of semi-algebraic dynamical systems. Compared with the existing complete and computable inductive condition, this new inductive condition can be easily adapted to achieve a set of sufficient inductive conditions with different level of conservativeness and computational complexity, which provides us with a means to trade off between the verification power and complexity. These inductive conditions can be solved by quantifier elimination and SMT solvers.

Key words: inductive invariant; semi-algebraic dynamical system; safety verification; hybrid system; nonlinear system

1 Introduction

Hybrid systems[1,2] are models for systems with interacting discrete and continuous dynamics. Embedded systems are often modeled as hybrid systems because they involve both digital control software and analog plants. In recent years, as embedded systems have become more ubiquitous, an increasing number of persons have begun to research hybrid system theory. Reachability problems or safety verification problems are among the most challenging problems in verifying hybrid systems. The biggest obstacle to hybrid system safety verification results mainly from the continuous dynamics. Therefore, addressing the problem of safety verification of continuous dynamical systems is essential to the safety verification of hybrid systems.

Inductive invariant based methods play an important role in the verification of continuous dynamical systems. An inductive invariant of a continuous dynamical system is an invariant φ that holds at the initial states of the system, and is preserved by the continuous transitions. A safety property is an invariant ψ (usually not inductive) that holds at all the reachable states of the system. The standard technique for proving a given property ψ is to generate an inductive invariant φ that implies ψ. Therefore, the problem of safety verification is converted to the problem of inductive invariant generation and hence avoiding the explicit computation of the reachable set of the system.

The key issues in generating inductive invariant for continuous dynamical system are how to define an

• Hui Kong, Fei He, Ming Gu, and Jiaguang Sun are with the School of Software, Tsinghua University, Beijing 100084, China. E-mail: kong-h08@mails.tsinghua.edu.cn.

• Xiaoyu Song is with the Department of ECE, Portland State University, OR 97207, USA.

• Hongyan Tan is with the Institute of Acoustics, Chinese Academy of Sciences, Beijing 100190, China.

∗ To whom correspondence should be addressed.

Manuscript received: 2013-09-18; revised: 2013-12-16; accepted: 2013-12-30

inductive condition that is as complete as possible and how to efficiently discover the inductive invariant that satisfies the inductive condition. However, these two aspects usually contradict each other. On the one hand, a complete inductive condition defines a largest set of inductive invariants and hence owns the strongest verification power. In other words, the completeness of an inductive condition guarantees the existence of an inductive invariant as long as the system is indeed safe. On the other hand, a complete inductive condition usually has the problem of computability or complexity, which means that we may not be able to find the invariant even if it does exist. Currently, the only complete and computable continuous inductive condition was proposed by Liu et al.[3] However, this complete condition has very limited applicability due to its high computational complexity, although it is computable in theory.

In this paper, we propose a new complete and computable continuous inductive condition. Our interest lies in a special class of dynamical systems which are specified in polynomials and polynomial inequalities, called semi-algebraic dynamical systems. The basic idea of our complete inductive condition is as follows. We assume that the inductive invariant is in the form of the polynomial inequality $\varphi(x) \leqslant 0$. From the geometric point of view, the point set $\{x \in \mathbb{R}^n \mid \varphi(x) \leqslant 0\}$ forms an over approximation for the reachable set of the system and the point set $\{x \in \mathbb{R}^n \mid \varphi(x) = 0\}$ forms the boundary of the over-approximation. In order for the trajectories of the system not to get across the boundary from the region of $\varphi(x) \leqslant 0$, we require that the trajectories that reach the boundary should: (1) either continue to move following the boundary, (2) or move inwards the region of $\varphi(x) \leqslant 0$. These two requirements can be specified in the higher-order Lie derivatives of $\varphi(x)$ with respect to the vector field f respectively as: (1) $\bigwedge_{i=1}^{\infty} \mathcal{L}_f^i \varphi = 0$, (2) $\bigvee_{j=1}^{\infty}(\bigwedge_{i=1}^{j-1} \mathcal{L}_f^i \varphi = 0 \wedge \mathcal{L}_f^j \varphi < 0)$. Furthermore, based on a theoretical result in Ref. [3], the above formulae consisting of an infinite number of sub-formulae can be reduced to finite-form formulae: (1) $\bigwedge_{i=1}^{N_{f,\varphi}} \mathcal{L}_f^i \varphi = 0$, (2) $\bigvee_{j=1}^{N_{f,\varphi}}(\bigwedge_{i=1}^{j-1} \mathcal{L}_f^i \varphi = 0 \wedge \mathcal{L}_f^j \varphi < 0)$, where $N_{f,\varphi}$ is constant depending on f and φ. Finally, by choosing a polynomial $\varphi(c, x)$ of fixed degree as the template for the inductive invariant, where c is the unknown coefficients to be decided, we can obtain a set of $\exists\forall$ formulae, which can be solved by using quantifier elimination and SMT solver.

The main contributions of this paper are as follows. First, we establish a formal framework for the properties of continuous inductive conditions, which helps formalize the discussion of the quality of a continuous inductive condition. Second, we propose a new complete and computable continuous inductive condition. Compared with the existing complete and computable continuous inductive condition, our condition can be easily adapted to achieve a set of sufficient inductive conditions with different levels of conservativeness and computational complexity, which provides us with a means to trade off between the verification power and the complexity.

2 Preliminaries

2.1 Continuous dynamical systems

Definition 1 (Continuous dynamical system) A continuous dynamical system is a 3-tuple $\langle X, f, \mathrm{Init}\rangle$, where

- X is a set of real-valued variables and $\mathcal{X} = \mathbb{R}^{|X|}$ is the set of all valuations of the variables X;
- $f\colon \mathcal{X} \mapsto \mathcal{X}$ is a vector field which specifies the continuous dynamics of the system. Note that f is assumed to be local Lipschitz continuous;
- Init$\subseteq \mathcal{X}$ is the initial set.

A continuous dynamical system defines a set of trajectories following which the system continuously evolves. The formal definition of a *trajectory* is as follows.

Definition 2 (Trajectory) Given a continuous dynamical system $\mathcal{S} = \langle X, f, \mathrm{Init}\rangle$, a trajectory starting from a state $x_0 \in \mathrm{Init}$ is a set of states $\mathrm{Tr}(f, x_0)$: $\mathrm{Tr}(f, x_0) \triangleq \{x : [0, +\infty) \mapsto \mathbb{R}^{|x|} \mid \dot{x} = f, x(0) = x_0\}$. For simplicity, we write it as $x(x_0, t)$.

Based on this definition, we can formally present the definition of the reachable set of a continuous dynamical system.

Definition 3 (Reachable set) Given a continuous dynamical system $\mathcal{S}$, the reachable set, which is denoted by Reach($\mathcal{S}$), is the set of all the trajectories starting from the initial set Init:

$$\mathrm{Reach}(\mathcal{S}) = \bigcup_{x_0 \in \mathrm{Init}} \mathrm{Tr}(f, x_0).$$

2.2 Semi-algebraic dynamical systems

A *polynomial formula* is a Boolean combination of multiple polynomial inequalities $q_{ij} \rhd 0$ joined by the connectives $\{\vee, \wedge, \neg, \Longrightarrow\}$, where $\rhd \in \{\geqslant, >, =, <, \leqslant, \neq\}$. Each polynomial formula, say $\Phi(x)$, can be converted into a normal form:

$$\Phi(x) = \bigvee_{i \in I} \bigwedge_{j \in J_i} q_{ij}(x) \rhd 0,$$

where $q_{ij}(x) \in \mathbb{R}[x]$ and $\rhd \in \{>, =\}$.

Definition 4 (Semi-algebraic set) A set $S \subseteq \mathbb{R}^{|x|}$ is a semi-algebraic set if it can be expressed in the following form:

$$S = \{x \in \mathbb{R}^{|x|} \mid \Phi(x)\} \tag{1}$$

where $\Phi(x)$ is a polynomial formula.

Note that in this paper, we usually use the polynomial formula $\Phi(x)$ to represent the semi-algebraic set S.

Definition 5 (Semi-algebraic dynamical system) A continuous dynamical system $\mathcal{S} = \langle X, f, \text{Init}\rangle$ is called a semi-algebraic dynamical system if the vector field f is a polynomial vector in $\mathbb{R}[x]^n$ and the initial set Init is a semi-algebraic set.

2.3 Lie derivative

An important concept that is frequently used in defining continuous inductive conditions is the Lie derivative. Given a scalar function $\varphi(x)$ and a continuous dynamical system $\mathcal{C} = \langle X, f, \text{Init}\rangle$, the Lie derivative $\mathcal{L}_f\varphi$ of φ with respect to the vector field f is essentially the first derivative of φ with respect to time t, $\dfrac{\mathrm{d}\varphi}{\mathrm{d}t}$, which reflects the change rate of $\varphi(x)$ over time t following the trajectories of the system $\mathcal{S}$. Similarly, the higher-order derivatives $\dfrac{\mathrm{d}^n\varphi}{\mathrm{d}t^n}$ can be represented by the higher-order Lie derivatives $\mathcal{L}_f^n\varphi(x)$. Let $\varphi(x)$ be a polynomial over the ring $\mathbb{R}[x]$, then the gradient of φ is an n-dimension polynomial vector over $\mathbb{R}[x]^n$, which is defined as follows:

$$\nabla\varphi \triangleq \left(\frac{\partial}{\partial x_1}\varphi, \frac{\partial}{\partial x_2}\varphi, \cdots, \frac{\partial}{\partial x_n}\varphi\right).$$

Therefore, the higher-order Lie derivatives can be defined inductively as follows:

$$\mathcal{L}_f^n\varphi \triangleq \begin{cases} \varphi(x), & n = 0; \\ \nabla(\mathcal{L}_f^{n-1}\varphi) \cdot f, & n \geqslant 1 \end{cases} \tag{2}$$

where $\boldsymbol{a} \cdot \boldsymbol{b} \triangleq \sum_{i=1}^n a_i b_i$ is the inner product of the vector $\boldsymbol{a} = (a_1, a_2, \cdots, a_n)$ and $\boldsymbol{b} = (b_1, b_2, \cdots, b_n)$.

2.4 Polynomial ideal theory

Let $\mathbb{K}$ be a real closed field and $\mathbb{K}[x]$ denote the polynomial ring with coefficients in $\mathbb{K}$, where $x = (x_1, \cdots, x_n)$ and $n = |x|$, then an ideal is a subset of $\mathbb{K}[x]$ with the following properties.

Definition 6 (Ideal) A subset I of $\mathbb{K}[x]$ is called an ideal if

(1) $0 \in I$;

(2) if $p(x), q(x) \in I$, then $p(x) + q(x) \in I$;

(3) if $p(x) \in I, q(x) \in \mathbb{K}[x]$, then $p(x)q(x) \in I$.

The ideal generated by a set $P = \{p_1(x), \cdots, p_m(x)\}$ is expressed as

$$\langle p_1(x), \cdots, p_m(x)\rangle = \{\sum_{i=1}^m p_i(x)q_i(x) | q_i(x) \in \mathbb{K}[x]\}.$$

A typical problem in polynomial ideal theory is the decision of ideal membership, that is, for a given polynomial $p(x) \in \mathbb{K}[x]$, we need to decide whether $p(x) \in I$. Gröbner Basis theory provides us with a general method to solve the membership problem[4]. Specifically, a polynomial $p(x) \in \mathbb{K}[x]$ belongs to I if the normal form of $p(x)$ with respect to the Gröbner Basis of I is 0.

3 Formal Evaluation Framework for Continuous Inductive Conditions

In recent years, various inductive conditions have been proposed for the safety verification of hybrid systems. The soundness and completeness of the inductive conditions are the main concerns of researchers. First, soundness is essential to an inductive condition in that it guarantees that the inductive invariant satisfying the inductive condition is indeed able to prove the safety property. However, some of the existing inductive conditions turn out to be unsound due to the neglects in some extreme cases. In addition, completeness means that the inductive condition defines an invariant set which is large enough to include all the inductive invariants that are able to prove the safety property. Because a complete and (efficiently) computable inductive condition is very hard to find, it is possible to find as complete inductive conditions as possible under the premise of computability. However, for any two given inductive conditions, there is currently no available method to decide which one is "closer" to being complete. In this section, we aim to establish a formal evaluation framework to assess the soundness of an inductive invariant condition and the relative conservativeness of two given inductive conditions.

We first present the formal definition of the safety verification problem of continuous systems.

Definition 7 (Safety Verification Problem (SVP)) Given a continuous dynamical system $\mathcal{S}$ and a safety property, denoted by a set of states Safety $\subseteq \mathbb{R}^{|x|}$, the *safety verification problem* is to decide that whether $\text{Reach}(\mathcal{S}) \subseteq$ Safety.

Definition 8 (Continuous inductive invariant) Given a continuous dynamic system $\mathcal{S} = \langle X, f, \text{Init}\rangle$, a set $\text{Inv} \subseteq \mathbb{R}^{|x|}$ is said to be a continuous inductive invariant of $\mathcal{S}$ iff

A_1 : (Initialization) $\text{Init} \subseteq \text{Inv}$;

A_2 : (Induction) $\bigcup_{x_0 \in \text{Inv}} \text{Tr}(f, x_0) \subseteq \text{Inv}$.

In the above definition, the condition A_1 means that the initial set Init is a subset of the set Inv and the condition A_2 means that no trajectory starting from Inv will escape from Inv. Therefore, a combination of the conditions A_1 and A_2 implies that no trajectory starting from Init will escape from Inv, i.e., $\text{Reach}(\mathcal{S}) \subseteq \text{Inv}$.

This is a general definition of continuous inductive invariant. In this paper, we focus on the inductive invariant for safety verification and we therefore need to take into account the safety property. We will discuss this in the following section. In addition, an inductive invariant is called a *semi-algebraic inductive invariant* if it can be expressed as a semi-algebraic set.

Definition 9 (Continuous inductive condition) For any given continuous dynamical system $\mathcal{S}$, a continuous inductive condition is a Boolean combination of multiple constraints which defines a set of continuous inductive invariants on $\mathcal{S}$.

In this paper, we write $\text{Inv} \models \rho$ if an inductive invariant Inv satisfies the inductive condition ρ. Correspondingly, the invariant set corresponding to ρ, denoted by $\mathcal{V}(\rho)$, is the following set:

$$\mathcal{V}(\rho) \triangleq \{\text{Inv} \mid \text{Inv} \models \rho\}.$$

Proposition 1 (Deduction rule of safety verification) For a given continuous dynamical system $\mathcal{S}$, a safety property Safe can be verified by an inductive invariant Inv according to the following inference rule:

$$\frac{\begin{array}{lll} A_1: & \text{(Initialization)} & \text{Init} \subseteq \text{Inv}; \\ A_2: & \text{(Induction)} & \bigcup_{x_0 \in \text{Inv}} \text{Tr}(f, x_0) \subseteq \text{Inv}; \\ A_3: & \text{(Property)} & \text{Inv} \subseteq \text{Safety} \end{array}}{\text{Reach}(\mathcal{S}) \subseteq \text{Safety}}$$

Proof The proof of the above deduction rule is trivial. Because A_1 and A_2 together imply that $\text{Reach}(S) \subseteq \text{Inv}$, then according to A_3, we can conclude that $\text{Reach}(\mathcal{S}) \subseteq$ Safety. ■

Remark 1 In the deduction rule, we take into account the safety property (i.e., A_3) for the purpose of safety verification. Therefore, **we hereafter refer to a constraint satisfying the conjunction of A_1–A_3 as the *continuous inductive condition for SVP*, or *continuous inductive condition*.**

Definition 10 (Soundness) For any given continuous dynamical system $\mathcal{S}$ and safety property Safe, a continuous inductive condition for SVP ρ is said to be sound iff:

$$\forall \text{Inv} : \text{Inv} \models \rho \implies \text{Inv} \models A_1 \wedge A_2 \wedge A_3.$$

The definition of soundness tells us that any inductive invariant that satisfies the inductive condition must satisfy A_1–A_3 and hence proves the safety of the system. However, soundness is not a trivial property for inductive conditions, there exists some widely used inductive conditions which have been proved to be unsafe[5,6]. Therefore, an inductive condition has to undergo a strict proof to guarantee its soundness.

Definition 11 (Completeness) For any given continuous dynamical system $\mathcal{S}$ and safety property Safe, a continuous inductive condition ρ is said to be complete with respect to $\mathcal{S}$ and Safe iff:

$$\forall \text{Inv}: \text{Inv} \models A_1 \wedge A_2 \wedge A_3 \implies \text{Inv} \models \rho.$$

The definition of *completeness* states that any inductive invariant that satisfies A_1–A_3 must satisfies ρ. A complete inductive condition defines a largest set of inductive invariants which can consist of a variety of functions such as logarithmic functions, exponential functions, trigonometric functions, and polynomial functions. Because the algebraic computation on transcendental functions is complicated, it is very difficult to define a complete inductive condition based on transcendental functions. Therefore, we prefer to achieve a "relaxed completeness" by confining the inductive invariant to a specific form, e.g., a polynomial formula.

Definition 12 (Weak completeness) For any given continuous dynamical system $\mathcal{S}$ and safety property Safe, a continuous inductive condition ρ is said to be weakly complete with respect to $\mathcal{S}$ and Safe iff there exists a set of inductive invariant ϕ such that

$$\forall \text{Inv}: \text{Inv} \in \phi \wedge \text{Inv} \models A_1 \wedge A_2 \wedge A_3 \implies \text{Inv} \models \rho.$$

Generally, we choose to construct semi-algebraic inductive invariants for semi-algebraic dynamical systems and the inductive invariant set ϕ is adopted as $\mathbb{R}[x]$ or $\mathbb{Q}[x]$.

Oftentimes, we need to decide which one of a pair of inductive conditions is more powerful in verifying safety properties of continuous dynamical systems. Therefore, we propose the concept of *relative* *conservativeness*.

Definition 13 (Relative conservativeness) Given two different continuous inductive conditions ρ_1 and ρ_2 for a continuous dynamical system, we say that ρ_1 is less conservative than ρ_2 if $\mathcal{V}(\rho_2) \subseteq \mathcal{V}(\rho_1)$.

According to the definition of *relative conservativeness*, a less conservative inductive condition defines a larger set of inductive invariants, which means that it may have more potential to have a member which is able to verify the safety property. From another point of view, relative conservativeness reflects the extent to which an inductive condition is relatively prone to be complete. Therefore, defining an inductive condition with lower relative conservativeness is challenging.

4 A Complete Inductive Condition for Continuous Dynamical Systems

4.1 Basic form of semi-algebraic continuous inductive condition

In recent years, various methods based on continuous inductive invariants have been proposed for safety verification of continuous dynamical systems. The key problem in discovering continuous inductive invariants is defining a sound and complete continuous inductive condition and how to efficiently computing a continuous inductive invariant that satisfies the continuous inductive condition. Unfortunately, it is hard to achieve these objectives simultaneously, because the interest of completeness often contradicts the requirement for computability, that is, a continuous inductive invariant with a sufficiently low conservativeness often encounters either computability problem or complexity problem. Therefore, the most common strategy is to achieve computability by sacrificing completeness.

Currently, the only sound and weakly complete as well as computable inductive condition was proposed by Liu et al.[3] In this inductive condition, there is an important constant $N_{f,\varphi}$ which depends closely on the vector field f and the template of inductive invariant $\varphi(x)$. Usually, $N_{f,\varphi}$ is a large number, which often causes the condition to be unsolvable because of its high computational complexity. In the following subsection, inspired by the work of Liu et al.[3], we present a new sound and weakly complete as well as computable continuous inductive condition. Compared with the condition in Ref. [3], our continuous inductive condition is much more flexible in that it can be easily adapted to achieve a set of sound and computable continuous inductive conditions with different levels of conservativeness.

It is difficult to compute a continuous inductive invariant for a general continuous dynamical system is very hard. However, for a given semi-algebraic dynamical system, some inductive continuous conditions and the corresponding computational methods are proposed. Given a semi-algebraic dynamical system $\mathcal{S} = \langle X, f, I(x)\rangle$ and a safety property $\mathrm{Safe}(x)$, where $I(x)$ and $\mathrm{Safe}(x)$ are polynomial formulae, the most common approach is to find a semi-algebraic inductive invariant $\varphi(x) \leqslant 0$ (or $\varphi(x) \geqslant 0$) that satisfies the constraints A_1–A_3 in Proposition 1. In general, the inductive condition on the polynomial $\varphi(x)$ has the following form:

$$\begin{array}{lll} B_1: & \text{(Initialization)} & I(x) \implies \varphi(x) \leqslant 0;\\ B_{f,\varphi}: & \text{(Induction)} & \mathrm{InductOn}(\varphi(x));\\ B_3: & \text{(Property)} & \varphi(x) \leqslant 0 \implies \mathrm{Safe}(x). \end{array}$$

Obviously, the formulae B_1 and B_3 are equivalent to A_1 and A_3 respectively. Therefore, the key problem lies in defining a formula B_2 that is at least sufficient for, if not equivalent to, the formula A_2. According to the formula A_2, let $\mathrm{Inv} \triangleq \varphi(x) \leqslant 0$, then the formula $\bigcup_{x_0\in\mathrm{Inv}} \mathrm{Tr}(f, x_0) \subseteq \mathrm{Inv}$ means that when starting from any point x_0 in the region of $\varphi(x) \leqslant 0$, the system will never evolve into the region $\varphi(x) > 0$ following the vector field f, as shown in Fig. 1. Therefore, our objective is to define a formula $\mathrm{InductOn}(\varphi(x))$ that satisfies that for any trajectory $x(x_0, t)$ of $\mathcal{S}$, the following formula holds:

$$\forall x_0 \in \mathbb{R}^{|x|}: \forall t \in [0,\infty): \varphi(x_0) \leqslant 0 \wedge \mathrm{InductOn}(\varphi(x)) \implies \varphi(x(x_0,t)) \leqslant 0 \tag{3}$$

4.2 A sound and weakly complete inductive invariant condition

A semi-algebraic inductive invariant $\mathrm{Inv} \triangleq \varphi(x) \leqslant 0$ represents a closed field, and the boundary of this

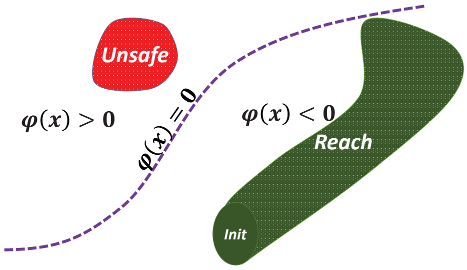


Fig. 1 Semi-algebraic inductive invariant $\varphi(x) \leqslant 0$. No trajectory can get across the boundary $\varphi(x)$=0.

field is the set of points satisfying $\varphi(x) = 0$, written as ∂Inv. Given a semi-algebraic dynamical system $\mathcal{S} = \langle X, f, I(x)\rangle$ and a trajectory $\pi \triangleq x(x_0, t)$ starting within the closed field Inv, a general idea for preventing π from escaping from the closed field Inv is that π stops immediately moving outwards once it reaches a point $x_\tau = x(x_0, \tau)$ at the boundary ∂Inv, which means that when $\varphi(x_\tau) = 0$, π has only two options to continue:

O_1: moving forward following the tangent line to the boundary at the point x_τ, or

O_2: moving inwards at the point x_τ.

These above two options can be specified formally with respect to the higher-order Lie derivatives (2).

Let

$$\Phi^{(k)}_{f,\varphi} \triangleq \bigwedge_{i=1}^{k} \mathcal{L}^i_f \varphi = 0 \tag{4}$$

$$\Psi^{(k)}_{f,\varphi} \triangleq \Phi^{(k-1)}_{f,\varphi} \wedge \mathcal{L}^k_f \varphi < 0 \tag{5}$$

then the move options O_1 and O_2 for π can be formalized as $\mathcal{F}_{f,\varphi}$ and $\mathcal{G}_{f,\varphi}$, respectively:

$$\mathcal{F}_{f,\varphi} \triangleq \Phi^{(\infty)}_{f,\varphi} \tag{6}$$

$$\mathcal{G}_{f,\varphi} \triangleq \bigvee_{k=1}^{\infty} \Psi^{(k)}_{f,\varphi} \tag{7}$$

Based on the previous formal definition on the possible moving direction of π, we have the following sound and complete inductive condition:

$$B_{f,\varphi} \triangleq \forall x : \varphi(x) = 0 \implies \mathcal{F}_{f,\varphi} \vee \mathcal{G}_{f,\varphi}.$$

To be readily understandable, we present the above sound and complete inductive condition as the following theorem and prove the soundness and completeness respectively.

Theorem 1 Given a semi-algebraic dynamical system SDS $= \langle X, f, I(x)\rangle$ and a safety property Safe(x) (where $I(x)$ and Safe(x) are polynomial formulae denoting semi-algebraic set), a polynomial inequality $\varphi(x) \leqslant 0$ (where $\varphi(x) \in \mathbb{R}[x]$) satisfies the condition $A_1 \wedge A_2 \wedge A_3$ if and only if $\varphi(x)$ satisfies the inductive condition $B_1 \wedge B_{f,\varphi} \wedge B_3$.

Proof (Soundness) By contradiction. Assume that $\varphi(x)$ is a polynomial function satisfying $B_1 \wedge B_{f,\varphi} \wedge B_3$; meanwhile, there exists a trajectory $\pi = x(x_0, t)$ (hereafter written as $x(t)$ for short hereafter) that can reach a point $x(\xi)$ such that $\varphi(x(\xi)) > 0$, where $x_0 = x(0) \in I(x)$ (i.e., $\neg(A_1 \wedge A_2 \wedge A_3)$). Since $\varphi(x_0) \leqslant 0$ and $\varphi(x(\xi)) > 0$, according to the continuity of $\varphi(x(t))$, there exists at least one time instant $\tau \in [0, \xi)$, and a real value $\delta > 0$ such that

$\mathcal{C}_1$: $\varphi(x_\tau) = 0$, where $x_\tau = x(\tau)$,

$\mathcal{C}_2$: $\forall t \in (\tau, \tau + \delta) : \varphi(x(t)) > 0$.

However, this contradicts the formula $B_{f,\varphi}$. According to $B_{f,\varphi}$, $\varphi(x_\tau) = 0$ implies that either $\mathcal{F}_{f,\varphi}$ or $\mathcal{G}_{f,\varphi}$ holds, which is equivalent to stating that one of the following two formulae holds:

$\mathcal{D}_1$: $\forall n \in [1, \infty) : \dfrac{\mathrm{d}^n \varphi(x_\tau)}{\mathrm{d}t^n} = 0$;

$\mathcal{D}_2$: $\exists n \in [1, \infty) : \bigwedge_{i=1}^{n-1} \dfrac{\mathrm{d}^i \varphi(x_\tau)}{\mathrm{d}t^i} = 0 \wedge \dfrac{\mathrm{d}^n \varphi(x_\tau)}{\mathrm{d}t^n} < 0$.

To capture the local profile of $\varphi(x(t))$, we present *Taylor Expansion* of $\varphi(x(t))$ at the point x_τ,

$$\varphi(x(t)) = \varphi(x_\tau) + \sum_{n=1}^{\infty} \frac{1}{n!} \frac{\mathrm{d}^n \varphi(x_\tau)}{\mathrm{d}t^n} (t - \tau)^n \tag{8}$$

According to Formula (8), there exists an infinitesimal $\epsilon > 0$ such that for all $t \in (\tau, \tau + \epsilon)$,

$\mathcal{E}_1$: $\varphi(x(t)) = \varphi(x_\tau) = 0$, if $\mathcal{D}_1$ holds;

$\mathcal{E}_2$: $\varphi(x(t)) = \varphi(x_\tau) + \frac{1}{n!} \dfrac{\mathrm{d}^n \varphi(x_\tau)}{\mathrm{d}t^n} (t - \tau)^n + O((t - \tau)^n) < 0$, if $\mathcal{D}_2$ holds.

This means that $\varphi(x(t)) \leqslant 0$ holds for all $t \in (\tau, \tau + \epsilon)$, which contradicts the formula $\mathcal{C}_2$. Therefore, the soundness of the inductive condition is proved.

(Weak Completeness) By contradiction. Assume that there exists a semi-algebraic inductive invariant Inv $\triangleq \varphi(x) \leqslant 0$ that satisfies the safety property Safe(x) but not the inductive condition $B_1 \wedge B_{f,\varphi} \wedge B_3$. According to our assumption and Definition 8, the formula $A_2 \wedge \neg B_{f,\varphi}$ must hold. To derive a contradiction, we will prove that $A_2 \wedge \neg B_{f,\varphi}$ is unsatisfiable.

The following equivalence relation is easily proved.

$$\neg B_{f,\varphi} \Leftrightarrow \exists x_\tau \in \mathbb{R}^{|x|} : \exists k \in \mathbb{Z}_+ : \varphi(x_\tau) = 0 \wedge \bigwedge_{i=1}^{k-1} \mathcal{L}^i_f \varphi = 0 \wedge \mathcal{L}^k_f \varphi > 0 \tag{9}$$

Let $x(x_\tau, t)$ be a trajectory satisfying $A_2 \wedge \neg B_{f,\varphi}$. Since $\neg B_{f,\varphi}$ holds, according to Formulae (8) and (9), there exists an infinitesimal $\epsilon > 0$ such that

$$\forall t \in (0, \epsilon) : \varphi(x(x_\tau, t)) > 0 \tag{10}$$

However, since $\varphi(x_\tau) = 0$, then $x_\tau \in$ Inv. According to the formula A_2, we know that Tr$(f, x_\tau) \subseteq$ Inv, that is,

$$\forall t \in (0, \infty) : \varphi(x(x_\tau, t)) \leqslant 0 \tag{11}$$

Therefore, Formulae (10) and (11) contradict each other, which means that $A_2 \wedge \neg B_{f,\varphi}$ is unsatisfiable. Hence, we can conclude that the completeness holds. ■

In Theorem 1, we present a sound and complete inductive condition which essentially defines a set $\mathcal{S}$

of inductive invariants for a specific semi-algebraic dynamical system. On the one hand, for being sound, it guarantees that any inductive invariant in $\mathcal{S}$ can assure the safety property of the system. On the other hand, for being complete, it guarantees that any semi-algebraic inductive invariant of the form $\varphi(x) \leqslant 0$ verifying the safety property is contained in $\mathcal{S}$.

However, the inductive condition in Theorem 1 is incomputable because its definition consists of an infinite number of sub-formulas. To make it computable, we need to achieve its finite form. As mentioned in Section 4.1, the continuous inductive condition proposed by Liu et al. involves an important constant $N_{f,\varphi}$, which results from the fact that there exists a computable upper bound $N_{f,\varphi}$ for a specific pair of (f, φ) such that (see Ref. [3])

$$\forall i \in \mathbb{N} : \varphi(x) = 0 \wedge \mathcal{L}_f^i \varphi \neq 0 \implies i \leqslant N_{f,\varphi} \quad (12)$$

In fact, the upper bound $N_{f,\varphi}$ applies here as well. According to the above definition of $N_{f,\varphi}$, we can easily derive an equivalent form of $\mathcal{F}_{f,\varphi}$ and $\mathcal{G}_{f,\varphi}$,

$$\widetilde{\mathcal{F}}_{f,\varphi} \triangleq \Phi_{f,\varphi}^{(N_{f,\varphi})},$$

$$\widetilde{\mathcal{G}}_{f,\varphi} \triangleq \bigvee_{k=1}^{N_{f,\varphi}} \Psi_{f,\varphi}^{(k)}.$$

Correspondingly, an equivalent form of $B_{f,\varphi}$:

$$\widetilde{B}_{f,\varphi} \triangleq \varphi(x) = 0 \implies \widetilde{\mathcal{F}}_{f,\varphi} \vee \widetilde{\mathcal{G}}_{f,\varphi}.$$

Based on the above definition, we obtain a finite form of the sound and complete inductive condition $B_1 \wedge \widetilde{B}_{f,\varphi} \wedge B_3$. A benefit of a complete inductive condition is that it provides us with a largest set of inductive invariants and hence possesses the strongest power to verify the safety property. However, in most cases, it may not be feasible to make use of the strongest power of a complete inductive condition because of its high computational complexity, or sometimes it may not be necessary to waste the strongest power on a non-critical safety property (i.e., the unsafe region is far away from the reachable set). Therefore, the ability to dynamically adjust the verification power of an inductive condition without loss of soundness is very appealing. However, this is not possible for the inductive condition in Ref. [3] because its soundness is based on the combination of $N_{f,\varphi}$ sub-formulae as a whole and eliminating any one of the sub-formulae may result in an unsound inductive condition. By comparison, our inductive condition is adaptable and is introduced in the following subsection.

4.3 The sufficient conditions

In fact, keeping any (non-zero) number of the disjuncts in $\widetilde{\mathcal{F}}_{f,\varphi} \vee \widetilde{\mathcal{G}}_{f,\varphi}$ will produce a sound but not necessarily complete inductive condition. In other words, $\widetilde{B}_{f,\varphi}$ can be easily customized to achieve a set of sound inductive conditions by compromising completeness. For example, if we keep only the disjunct $\widetilde{\mathcal{F}}_{f,\varphi}$, we can obtain the sound inductive condition $\varphi(x) = 0 \implies \widetilde{\mathcal{F}}_{f,\varphi}(x)$, which means that once a trajectory reaches the boundary of $\varphi(x) \leqslant 0$, it will continue to follow the boundary permanently. In practice, this assumption is so perfect that there rarely exists an inductive invariant that satisfies this requirement. However, by adding to $\widetilde{\mathcal{F}}_{f,\varphi}$ a disjunct of $\widetilde{\mathcal{G}}_{f,\varphi}$, we can easily achieve a relaxed inductive condition that allows a trajectory to return from the boundary of $\varphi(x) \leqslant 0$ to its interior. From this example, we can see the flexibility of the condition $\widetilde{B}_{f,\varphi}$ in the inductive invariant discovery.

As mentioned in Section 4.2, although completeness is essential in verifying some critical safety properties, the sufficient condition is more practical in many cases for the sake of efficiency. We now present the general form of the sufficient condition derived from $\widetilde{B}_{f,\varphi}$.

Let

$$\begin{aligned} \widetilde{\mathcal{G}}_{f,\varphi}^U &\triangleq \bigvee^{k \in U} \Psi_{f,\varphi}^{(k)}, \\ S &\triangleq [1, N_{f,\varphi}], \\ \Xi &\triangleq \{\mathrm{T}, \mathrm{F}\}, \\ \Gamma &\triangleq 2^S \times \Xi \setminus (\emptyset, \mathrm{F}) \end{aligned} \quad (13)$$

where T = TRUE, F = FALSE. Then, the general form of a sufficient inductive condition can be written as

$$\widehat{B}_{f,\varphi}^{(U,\theta)} \triangleq \forall x : \varphi(x) = 0 \implies (\theta \implies \widetilde{\mathcal{F}}_{f,\varphi}) \vee \widetilde{\mathcal{G}}_{f,\varphi}^U \quad (14)$$

where $(U, \theta) \in \Gamma$.

By setting the pair of (U, θ) to different values, we can derive from $\widehat{B}_{f,\varphi}^{(U,\theta)}$ a set of different inductive conditions. Moreover, the conservativeness of the resulting inductive condition depends closely on the pair of (U, θ). For convenience of presentation, we define a binary relation over Γ:

$$(U_1, \theta_1) \preceq (U_2, \theta_2) \iff U_1 \subseteq U_2 \wedge (\theta_1 \implies \theta_2).$$

It is easy to prove that the binary relation is a *partial order* relation. Based on this *partial order* relation, we have the following proposition.

Proposition 2 Given any two pairs of γ_1 and γ_2, where $\gamma_i = (U_i, \theta_i) \in \Gamma$, $i = 1, 2$, if $\gamma_1 \preceq \gamma_2$ holds, then the inductive condition $B_1 \wedge \widehat{B}^{\gamma_2}_{f,\varphi} \wedge B_3$ is less conservative than $B_1 \wedge \widehat{B}^{\gamma_1}_{f,\varphi} \wedge B_3$.

Proof According to Definition 13, it suffices to prove that any function $\varphi(x)$ satisfying $\widehat{B}^{\gamma_1}_{f,\varphi}$ also satisfies $\widehat{B}^{\gamma_2}_{f,\varphi}$. Since $\gamma_1 \preceq \gamma_2$ holds, it is easy to prove that $\widetilde{\mathcal{G}}^{U_1}_{f,\varphi} \implies \widetilde{\mathcal{G}}^{U_2}_{f,\varphi}$ hold. Hence, $\widehat{B}^{\gamma_1}_{f,\varphi} \implies \widehat{B}^{\gamma_2}_{f,\varphi}$ holds. ■

As mentioned earlier, a less conservative inductive condition defines a larger set of inductive invariants and hence is more prone to include an element capable of verifying the safety property. According to Proposition 2, to minimize the conservativeness of an inductive condition, we only need to make the tuple (U, θ) as large as possible, i.e., make the right-hand side of the formula $\widehat{B}^{(U,\theta)}_{f,\varphi}$ include as many disjuncts as possible. However, an increase of the tuple (U, θ) leads to an increase of the computational complexity. In particular, the resulting inductive condition could be intractable when the constant $N_{f,\varphi}$ is too big. Therefore, we have to make a trade-off between the conservativeness and computational complexity. Our strategy for solving this problem is to choose an increasing sequence $\gamma_1 \preceq \cdots \preceq \gamma_m$ as candidates for (U, θ), where $\gamma_i \in \Gamma$, $1 \leqslant i \leqslant m$. Starting from the smallest element in the sequence, we gradually reduce the conservativeness of the inductive condition $B_1 \wedge \widehat{B}^{\gamma_i}_{f,\varphi} \wedge B_3$ until an inductive invariant is found, or the largest element $(\mathcal{S}, T)$ has been attempted.

In the following section, we introduce a method to compute an inductive invariant based on our inductive condition.

5 Computational Method for Constructing Inductive Invariant

It is very difficult to construct inductive invariants for general dynamical systems. Fortunately, for some existing inductive conditions, several computational methods are available for semialgebraic dynamical systems. The most representative methods include the fixed-point method based on saturation[7], the constraint-solving methods based on semidefinite programming[5] and Quantifier Elimination (QE)[6] as well as the Gröbner Basis method[8,9]. Considering the feature of our inductive condition, we choose the QE-based constraint-solving method as our computational method to discover inductive invariants for semi-algebraic dynamical systems.

For a given semi-algebraic dynamical system $\mathcal{S} = \langle X, f, I(x) \rangle$, the basic idea of the QE-based constraint-solving method is as follows:

(1) Choosing a parametric polynomial inequality $\varphi(c, x) \leqslant 0$ of fixed degree k as the template for the inductive invariant function, where x is a vector of variables and c is a vector of the unknown real coefficients of monomials. Usually, the parametric polynomial is chosen as a complete polynomial, i.e., a polynomial consisting of all the monomials of degree k or less:

$$\varphi(c, x) = \sum_{i_1 + \cdots + i_n \leqslant k} c_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \tag{15}$$

(2) Computing the constant $N_{f,\varphi}$ based on the template $\varphi(c, x)$ and choosing an increasing sequence $\gamma_1 \preceq \cdots \preceq \gamma_m$ from Γ as the candidates for (U, θ). In the below, we will introduce how to compute $N_{f,\varphi}$ using Gröbner Basis;

(3) Picking in turn each element γ_i of the above candidate sequence from the least one to the greatest one to perform the following steps until an inductive invariant is found or until the greatest element has been attempted;

(4) Performing the QE over the constraint $\alpha \triangleq \exists c : \forall x : (B_1 \wedge \widehat{B}^{\gamma_i}_{f,\varphi} \wedge B_3)_{\varphi(x) \mapsto \varphi(c,x)}$, where $\varphi(x) \mapsto \varphi(c, x)$ means the substitution of $\varphi(c, x)$ for the occurrences of $\varphi(x)$. Note that we only eliminate the universal quantifier in this step and the output of QE over α is an equivalent existentially quantified formula $\beta(c)$;

(5) Attempting to discover an inductive invariant by solving the formula $\beta(c)$ using an SMT solver. Note that $\beta(c)$ defines a set of inductive invariants and our objective is to choose one element from the invariant set with the aid of an SMT solver.

In the above computing method, one important thing to note is the computation of the constant $N_{f,\varphi}$ in Step 2. In Ref. [3], Liu et al. presented a computational method based on the following definition:

$$N_{f,\varphi} \triangleq \min\{i \mid \mathcal{L}_f^{i+1}\varphi \in \langle \mathcal{L}_f^0\varphi, \cdots, \mathcal{L}_f^i\varphi \rangle\} \tag{16}$$

The key problem in computing $N_{f,\varphi}$ is the determination of ideal membership. The Gröbner Basis theory provides us with a method to determine whether a constant-coefficient polynomial belongs to an ideal generated by a group of constant-coefficient polynomials. However, the problem here is that

$\mathcal{L}_f^k\varphi(c,x)$ is a parametric polynomial (with c as its coefficients) for all $k \in \mathbb{Z}_+$ and the ideal is generated by a group of parametric polynomials $\{\mathcal{L}_f^k\varphi|k = 0\cdots i\}$ as well, hence, the value of $N_{f,\varphi}$ is a variable depending on the specific assignment of c. Nevertheless, there exists an upper bound N_c for the values of $N_{f,\varphi}$ over all possible assignments of c (see Ref. [3]). In other words, the existence of the upper bound N_c results from the fact that the parametric polynomials $\{\mathcal{L}_f^k\varphi|k \in \mathbb{Z}_+\}$ over $\mathbb{R}[x]$ are actually constant-coefficient polynomials over $\mathbb{R}[c,x]$, which implies the existence of a constant N_c satisfying Formula (12). To obtain the value of N_c, we only need to check the ideal membership over $\mathbb{R}[c,x]$ instead of over $\mathbb{R}[x]$. Currently, many tools have the support packages for checking the ideal membership based on the Gröbner Basis, such as the mathematic software tools *Maple* and *Mathematic*.

Another two important computations are QE in Step 4 and solving the existentially quantified formula in Step 5. Currently, a number of well-known tools are available for these purposes, such as QEPCAD, Redlog for QE, and Z3, Yices, and OpenSMT for solving quantifier-free formulae. In our case study, we use QEPCAD and Z3 as computing tools. In the following section, we use an example to demonstrate the application of our method to the safety verification of c of a semi-algebraic dynamical system.

6 Case Study

Consider the two-dimensional system $\mathcal{S}$,

$$\begin{bmatrix}\dot{x}\\ \dot{y}\end{bmatrix} = \begin{bmatrix}x+y\\ x-y\end{bmatrix} \tag{17}$$

we want to verify that starting from the initial set $X_0 = \left\{(x,y)\in\mathbb{R}^2|(x-3)^2 + \left(y+\frac{3}{2}\right)^2 \leqslant \frac{1}{4}\right\}$, the system will never evolve into the unsafe set $X_u = \left\{(x,y)\in\mathbb{R}^2|(x-6)^2 + \left(y+\frac{5}{4}\right)^2 \leqslant \frac{4}{5}\right\}$.

In order to verify the above safety property, we first choose $\varphi(x,y) = a + bx + cy \leqslant 0$ as the template for the inductive invariant, where a, b, and c are the real-valued coefficients to be decided. Based on the given template, we can easily compute the constant $N_{f,\varphi} = 2$ by Formula (16). Then, we can construct the set Γ by Formula (13), from which an increasing candidate sequence for γ_i can be selected. In our case study, the selected candidate sequence γ_i $(i = 1,2,3)$ is as follows:

$$(\{1\},F) \preceq (\{1,2\},F) \preceq (\{1,2\},T).$$

Note that $\gamma_3 = (\{1,2\},T)$ is the largest parameter which results in a complete inductive condition.

According to the definition of the inductive condition $B_1 \wedge \widehat{B}_{f,\varphi}^{\gamma_i} \wedge B_3$, we can obtain the following first order logical formulae:

- B_1. $\exists a,b,c : \forall x,y : (x-3)^2 + \left(y+\frac{3}{2}\right)^2 \leqslant \frac{1}{4} \Longrightarrow a + bx + cy \leqslant 0.$
- B_3. $\exists a,b,c : \forall x,y : (x-6)^2 + \left(y+\frac{5}{4}\right)^2 \leqslant \frac{4}{5} \Longrightarrow a + bx + cy > 0.$
- $\widehat{B}_{f,\varphi}^{\gamma_i} : i = 1,2,3.$
  (1) γ_1. $\exists a,b,c : \forall x,y : a + bx + cy = 0 \Longrightarrow (b+c)x + (b-c)y < 0.$
  (2) γ_2. $\exists a,b,c : \forall x,y : a + bx + cy = 0 \Longrightarrow ((b+c)x+(b-c)y < 0 \vee ((b+c)x+(b-c)y = 0 \wedge bx + cy < 0)).$
  (3) γ_3. $\exists a,b,c : \forall x,y : a + bx + cy = 0 \Longrightarrow ((b+c)x+(b-c)y < 0 \vee ((b+c)x+(b-c)y = 0 \wedge bx + cy < 0) \vee ((b+c)x + (b-c)y = 0 \wedge bx + cy = 0)).$

In the next step, we perform the QE over the above first order logical formulae and we obtain the following existentially quantified formulae:

- B_1. $\exists a,b,c : 8c^2 - 36bc - 12ac + 35b^2 + 24ab + 4a^2 \geqslant 0 \wedge 3c - 5b - 2a \geqslant 0 \wedge (a \geqslant 0 \vee 3c - 5b - 2a > 0).$
- B_3. $\exists a,b,c : 561c^2 - 6000bc - 1000ac + 14\,336b^2 + 4800ab + 400a^2 > 0 \wedge 25c - 112b - 20a < 0.$
- $\widehat{B}_{f,\varphi}^{\gamma_i} : i = 1,2,3.$
  (1) γ_1. $\exists a,b,c : c^2 + 2bc - b^2 = 0 \wedge ((a > 0 \wedge b \geqslant 0 \wedge c > 0) \vee (a > 0 \wedge b \leqslant 0 \wedge c \leqslant 0) \vee (a < 0 \wedge b \geqslant 0 \wedge c \leqslant 0) \vee (a < 0 \wedge b \leqslant 0 \wedge c > 0)).$
  (2) γ_2. $\exists a,b,c : c^2 + 2bc - b^2 = 0 \wedge ((a > 0 \wedge b \geqslant 0 \wedge c > 0) \vee (a > 0 \wedge b \leqslant 0 \wedge c \leqslant 0) \vee (a < 0 \wedge b \geqslant 0 \wedge c \leqslant 0) \vee (a < 0 \wedge b \leqslant 0 \wedge c > 0)).$
  (3) γ_3. $\exists a,b,c : c^2 + 2bc - b^2 = 0 \wedge ((a \geqslant 0 \wedge b \geqslant 0 \wedge c > 0) \vee (a \geqslant 0 \wedge b \leqslant 0 \wedge c \leqslant 0) \vee (a \leqslant 0 \wedge b \geqslant 0 \wedge c \leqslant 0) \vee (a \leqslant 0 \wedge b \leqslant 0 \wedge c > 0)).$

Notice that the above existentially quantified formulae show that the conditions $\widehat{B}_{f,\varphi}^{\gamma_1}$ and $\widehat{B}_{f,\varphi}^{\gamma_2}$ are equivalent, which means that $\widehat{B}_{f,\varphi}^{\gamma_2}$ has the same verification power as $\widehat{B}_{f,\varphi}^{\gamma_1}$. Hence, we can reduce the candidate sequence of inductive conditions to

$B_1 \wedge \widehat{B}^{\gamma_1}_{f,\varphi} \wedge B_3$, and $B_1 \wedge \widehat{B}^{\gamma_3}_{f,\varphi} \wedge B_3$.

Next, we need to solve these two inductive conditions with Z3 in turn. In fact, it finally turned out that the condition $B_1 \wedge \widehat{B}^{\gamma_1}_{f,\varphi} \wedge B_3$ is sufficient to verify the safety property and hence the strongest verification possessed by the complete inductive condition $B_1 \wedge \widehat{B}^{\gamma_3}_{f,\varphi} \wedge B_3$ can be saved here. Comparably, the inductive condition in Ref. [3] cannot be used this way, it has to be used in the most complex form for the safety verification each time, which usually is not cost-effective for complex systems.

In order to get a deep insight into the difference between the two candidate inductive conditions, we tried to solve the condition $B_1 \wedge \widehat{B}^{\gamma_3}_{f,\varphi} \wedge B_3$ similarly. The result is that we obtained an identical solution for these two conditions:

$$\begin{aligned} a &= -\frac{127}{16}, \\ b &= 1, \\ c &= -\sqrt{2} - 1. \end{aligned}$$

Then, the expression of φ is $\varphi(x, y) = -\frac{127}{16} + x - (\sqrt{2}+1)y$. The phase portrait of the system (17) and the zero level set of $\varphi(x, y)$ (i.e., $\{(x, y) \in \mathbb{R}^2 | \varphi(x, y) = 0\}$) are shown in Fig. 2.

In Fig. 2, we can see that the reachable set Reach completely lies above the line of $\varphi(x, y) = 0$, which means that $\varphi(x, y) \leqslant 0$ for any $(x, y) \in$ Reach. On the other hand, the unsafe set X_{u} lies under the line of $\varphi(x, y) = 0$ and hence guarantees that $\varphi(x, y) > 0$ for any $(x, y) \in X_{\mathrm{u}}$. Therefore, the system is verified to be safe due to the existence of an inductive invariant $\varphi(x, y) \leqslant 0$.

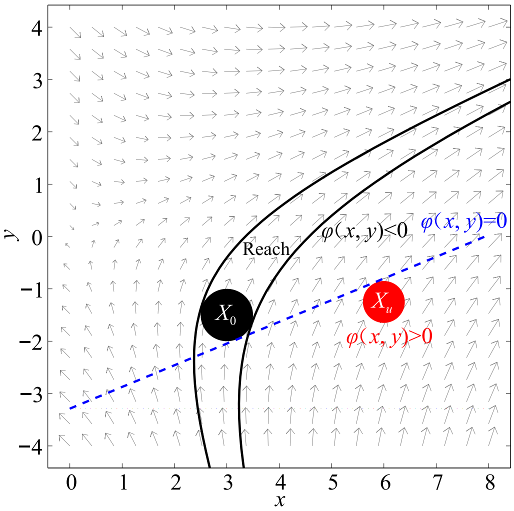


Fig. 2 Phase portrait of the system (17) and the inductive invariant $\varphi(x,y) \leqslant 0$. The solid patches from left to right are the initial set X_0 and the unsafe set X_{u}, respectively. The enclosed area Reach, which starts from X_0, is the reachable set of the system and the area above the line of $\varphi(x, y) = 0$ is the set of points satisfying the inductive invariant $\varphi(x,y)<0$.

7 Related Work

Some methods have been proposed for the construction of inductive invariants for linear hybrid systems. Jirstrand[10] presented a method based on convex optimization and linear matrix inequalities for constructing ellipsoidal invariants and quadratic cone invariants for piecewise linear systems. Different from the optimization method, Rodríguez-Carbonell and Tiwari[11] proposed to generate algebraic invariant (i.e., $P(x) = 0$) for linear hybrid systems based on Gröbner Basis and abstract interpretation.

In recent years, researchers have focused more on nonlinear hybrid systems, especially on algebraic or semi-algebraic hybrid systems, as they have a higher universality. In Refs. [9, 12], Sankaranarayanan et al. presented a computational method based on the theory of ideal over polynomial ring and QE for automatically generating algebraic invariants for algebraic hybrid systems. Similarly, Tiwari and Khanna[8] proposed a technique that is based on the theory of ideal over polynomial ring to generate the inductive invariant for nonlinear polynomial systems. In Refs. [5, 13], Prajna et al. proposed a new inductive invariant called *Barrier Certificate* for verifying the safety of semialgebraic hybrid systems and the computational method they applied is the technique of the sum-of-squares decomposition of semidefinite polynomials. Platzer and Clarke[7] proposed a generalized concept called differential invariant which is a Boolean combination of multiple polynomial inequalities and they introduced a fixedpoint algorithm to compute the differential invariant for semi-algebraic hybrid systems. Gulwani and Tiwari[6] proposed an inductive invariant that is similar to the differential invariant except that they defined a different inductive condition and they used an SMT solver to solve the constraint derived from the inductive condition. Taly and Tiwari[14] presented several simple but incomplete inductive conditions for different classes of inductive invariants. Sloth et al.[15] proposed a new *Barrier*

Certificate for a special class of hybrid systems which can be modeled as an interconnection of subsystems. Liu et al.[3] proposed a new sound and relatively complete invariant condition for verifying hybrid systems and the generation of the invariant is based on the method of QE. In Ref. [16], we proposed a new inductive condition, called *Exponential Condition*, for the safety verification of hybrid systems and we use the semi-definite programming method to discover the inductive invariant.

8 Conclusions and Future Work

Addressing the safety verification problem of continuous dynamical systems is essential to advance the development of the theory of hybrid system safety verification. In this paper, we first established a formal framework for the properties of continuous inductive conditions, which helps to formalize the discussion of the quality of continuous inductive conditions. In addition, we proposed a new complete continuous inductive condition. Compared with the existing complete and computable continuous inductive condition, our condition can be easily adapted to achieve a set of sufficient inductive conditions with different levels of conservativeness and computational complexity, which provides us with a means to trade off between the verification power and the complexity. Using a case study, we showed the applicability of our method.

Currently, the method is limited to linear semi-algebraic inductive invariant because of the high computation complexity in quantifier elimination. In the future, we aim to identify more efficient computational method. Moreover, we will extend our method to the safety verification to hybrid systems.

Acknowledgements

This work was supported by the National Key Basic Research and Development (973) Program of China (No. 2010CB328003), the National Natural Science Foundation of China (Nos. 61272001, 60903030, and 91218302), the National Key Technology Research and Development Program (No. SQ2012BAJY4052), and the Tsinghua University Initiative Scientific Research Program.

References

[1] T. Henzinger, The theory of hybrid automata, in *Logic in Computer Science, 1996. LICS'96. Proceeding., Eleventh Annual IEEE Symposium on*, IEEE, 1996, pp. 278-292.

[2] R. Alur, C. Courcoubetis, N. Halbwachs, T. Henzinger, P. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine, The algorithmic analysis of hybrid systems, *Theoretical Computer Science,* vol. 138, no. 1, pp. 3-34, 1995.

[3] J. Liu, N. Zhan, and H. Zhao, Computing semialgebraic invariants for polynomial dynamical systems, in *Proceedings of the Ninth ACM International Conference on Embedded Software*, ACM, 2011, pp. 97-106

[4] B. Mishra and C. Yap, Notes on Gröbner bases, *Information Sciences*, vol. 48, no. 3, pp. 219-252, 1989.

[5] S. Prajna and A. Jadbabaie, Safety verification of hybrid systems using barrier certificates, *Hybrid Systems: Computation and Control*, pp. 271-274, 2004.

[6] S. Gulwani and A. Tiwari, Constraint-based approach for analysis of hybrid systems, in *Computer Aided Verification*, Springer, 2008, pp. 190-203.

[7] A. Platzer and E. Clarke, Computing differential invariants of hybrid systems as fixedpoints, in *Computer Aided Verification*, Springer, 2008, pp. 176-189.

[8] A. Tiwari and G. Khanna, Nonlinear systems: Approximating reach sets, *Hybrid Systems: Computation and Control*, pp. 171-174, 2004.

[9] S. Sankaranarayanan, Automatic invariant generation for hybrid systems using ideal fixed points, in *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control*, ACM, 2010, pp. 221-230.

[10] M. Jirstrand, Invariant sets for a class of hybrid systems, in *Decision and Control, in Proceedings of the 37th IEEE Conference on*, IEEE, 1998, pp. 3699-3704.

[11] E. Rodríguez-Carbonell and A. Tiwari, Generating polynomial invariants for hybrid systems, *Hybrid Systems: Computation and Control*, pp. 590-605, 2005.

[12] S. Sankaranarayanan, H. Sipma, and Z. Manna, Constructing invariants for hybrid systems, *Hybrid Systems: Computation and Control*, pp. 69-77, 2004.

[13] S. Prajna, A. Jadbabaie, and G. Pappas, A framework for worst-case and stochastic safety verification using barrier certificates, *Automatic Control, IEEE Transactions on*, vol. 52, no. 8, pp. 1415-1428, 2007.

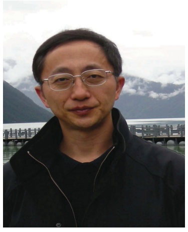
[14] A. Taly and A. Tiwari, Deductive verification of continuous dynamical systems, in *FSTTCS*, 2009, pp. 383-394.

[15] C. Sloth, G. Pappas, and R. Wisniewski, Compositional safety analysis using barrier certificates, in *Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control*, ACM, 2012, pp. 15-24.

[16] H. Kong, F. He, X. Song, W. Hung, and M. Gu, Exponential-condition-based barrier certificate generation for safety verification of hybrid systems, *Lecture Notes in Computer Science*, vol. 8044, pp. 242-257, 2013.

Hui Kong received the BS degree in mathematics from Wuhan University, China, in 2001 and the MS degree in mathematics from National University of Defence Technology, China, in 2003. He is currently a PhD candidate in computer science at Tsinghua University. His research interests include hybrid system safety verification, model checking, and theorem proving.

Fei He is an associate professor in the School of Software at Tsinghua University, Beijing, China. He received the BS degree from National University of Defense Technology in 2002, and the PhD degree from Tsinghua University in 2008. His research interests include satisfiability, model checking, compositional reasoning, and their applications in embedded systems.



Xiaoyu Song received the PhD degree from the University of Pisa, Italy, in 1991. His current research interests include formal methods, design automation, embedded system design, and emerging technologies.

Ming Gu received the BS degree in computer science from the National University of Defence Technology, China, in 1984, and the MS degree in computer science from the Chinese Academy of Science in 1986. Since 1993, she has been working as a lecturer/associate professor/researcher at Tsinghua University. She is also serving as the vice dean of the School of Software at Tsinghua University. Her research interests include formal methods, middleware technology, and distributed applications.

Hongyan Tan is an associate professor of High Performance Network Lab, Institute of Acoustics, China Academy of Sciences, the supervisor of master candidate. She received the BS degree from Lanzhou University in 1984, and the MS degree from Lanzhou University in 1988. Her major research interests include broadband wireless multimedia communication technology, internet of things, mobile internet, and cloud computing.

Jiaguang Sun received the BS degree in automation science from Tsinghua University in 1970. He is currently a professor in Tsinghua University. He is dedicated in teaching and R&D activities in computer graphics, computer-aided design, formal verification of software, and system architecture. He is currently the director of the School of Information Science & Technology and the School of Software in Tsinghua University. He is also the director of the National Laboratory for Information Science & Technology. He has been a member of the Chinese Academy of Engineering since 1999.