Exponential-Condition-Based Barrier Certificate Generation for Safety Verification of Hybrid Systems*

Hui Kong[1,2,5,6], Fei He[2,5,6], Xiaoyu Song[3], William N.N. Hung[4], and Ming Gu[2,5,6]

[1] Dept. of Computer Science&Technology, Tsinghua University, Beijing, China
[2] School of Software, Tsinghua University, Beijing, China
[3] Dept. of ECE, Portland State University, Oregon, USA
[4] Synopsys Inc, Mountain View, California, USA
[5] Tsinghua National Laboratory for Information Science and Technology
[6] Key Laboratory for Information System Security, MOE, China

Abstract. A barrier certificate is an inductive invariant function which can be used for the safety verification of a hybrid system. Safety verification based on barrier certificate has the benefit of avoiding explicit computation of the exact reachable set which is usually intractable for nonlinear hybrid systems. In this paper, we propose a new barrier certificate condition, called *Exponential Condition*, for the safety verification of semi-algebraic hybrid systems. The most important benefit of *Exponential Condition* is that it has a lower conservativeness than the existing convex conditions and meanwhile it possesses the convexity. On the one hand, a less conservative barrier certificate forms a tighter over-approximation for the reachable set and hence is able to verify critical safety properties. On the other hand, the convexity guarantees its solvability by semidefinite programming method. Some examples are presented to illustrate the effectiveness and practicality of our method.

Keywords: inductive invariant, barrier certificate, safety verification, hybrid system, nonlinear system, sum of squares.

1 Introduction

Hybrid systems [1], [2] are models for those systems with interacting discrete and continuous dynamics. Embedded systems are often modeled as hybrid systems due to their involvement of both digital control software and analog plants. In recent years, as embedded systems are becoming ubiquitous, more and more researchers are devoted to the theory of hybrid systems. Reachability problems or

* This work was supported by the Chinese National 973 Plan under grant No. 2010CB328003, the NSF of China under grants No. 61272001, 60903030, 91218302, the Chinese National Key Technology R&D Program under grant No. SQ2012BAJY4052, and the Tsinghua University Initiative Scientific Research Program.

N. Sharygina and H. Veith (Eds.): CAV 2013, LNCS 8044, pp. 242–257, 2013.

safety verification problems are among the most challenging problems in verifying hybrid systems. The aim of safety verification is to decide that starting from an initial set, whether a continuous system or hybrid system can reach an unsafe set. For this purpose, many methods have been proposed for various hybrid systems with different features.

Deductive methods based on inductive invariant play an important role in the verification of hybrid systems. An inductive invariant of a hybrid system is an invariant φ that holds at the initial states of the system, and is preserved by all discrete and continuous transitions. A safety property is an invariant ψ (usually not inductive) that holds in all 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 avoid the reachability computation of the hybrid system. The key points in generating inductive invariant for hybrid systems is how to define an inductive condition that is the least conservative and how to efficiently compute the inductive invariant that satisfies the inductive condition. Usually, these two aspects contradict with each other, that is, an inductive condition with sufficiently low conservativeness often encounters the computability or complexity problem. For different class of hybrid systems, various inductive invariants and computational methods have been proposed.

Some methods were primarily proposed for constructing inductive invariant for linear hybrid systems [3], [4]. In recent years, however, researchers concentrate more and more on nonlinear hybrid systems, especially on algebraic or semi-algebraic hybrid systems (i.e. those systems whose vector fields are polynomials and whose set descriptions are polynomial equalities or inequalities), as they have a higher universality. In [5], [6], Sankaranarayanan et al. presented a computational method based on the theory of ideal over polynomial ring and quantifier elimination for automatically generating algebraic invariants for algebraic hybrid systems. Similarly, Tiwari et al. proposed in [7] a technique based on the theory of ideal over polynomial ring to generate the inductive invariant for nonlinear polynomial systems. In [8], [9], S. 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 sum-of-squares decomposition of semidefinite polynomials. In [10], C. Sloth et al. proposed a new *Barrier Certificate* for a special class of hybrid systems which can be modeled as an interconnection of subsystems. In [11], A. Platzer et al. proposed the concept of *Differential Invariant* which is a boolean combination of multiple polynomial inequalities for verifying semialgebraic hybrid systems. In [12], S. Gulwani et al. proposed an inductive invariant similar to *Differential Invariant* except that they defined a different inductive condition and they used SMT solver to solve the inductive invariant. In [13], A. Taly et al. discussed the soundness and completeness of several existing invariant condition and presented several simpler and practical invariant condition that are sound and relatively complete for different classes of inductive invariants. In [14], A. Taly et al.

proposed to use inductive controlled invariant to synthesize multi-modal continuous dynamical systems satisfying a specified safety property.

In this paper, we propose a new barrier certificate (called *Exponential Condition*) for the safety verification of semialgebraic hybrid systems. A barrier certificate is a special class of inductive invariant for the safety verification of hybrid systems: a function $\varphi(x)$ which maps all the states in the reachable set to non-positive reals and all the states in the unsafe set to positive reals. Given a dynamical system S with dynamics $\dot{x} = f(x)$ with initial set $Init$, to prove a safety property P (we use X_u to denote the unsafe set) is satisfied by S, the basic idea of *Exponential Condition* is to identify a function $\varphi(x)$ such that 1) $\varphi(x) \leq 0$ for any point $x \in Init$, 2) $\varphi(x) > 0$ for any point $x \in X_u$, and 3) $\mathcal{L}_f\varphi(x) \leq \lambda\varphi(x)$, where $\mathcal{L}_f\varphi(x) = \frac{\partial\varphi}{\partial x}f(x) = \sum_{i=1}^{n}\frac{\partial\varphi}{\partial x_i}f_i(x)$ is the Lie derivative of φ with respect to the vector field f and λ is any negative constant real value. The first condition and the third condition together guarantee that $\varphi(x) \leq 0$ for any point x in the reachable set R, which implies that $R \cap X_u = \emptyset$. Therefore, we can assert that the safety property P is satisfied by the system M as long as we can find a function $\varphi(x)$ satisfying the above condition. The above condition can be extended to semialgebraic hybrid systems naturally. The idea is to identify a set of functions $\{\varphi_i(x)\}$, one for each mode of the hybrid system, which not only satisfy the above condition but also satisfy an additional sign-preserving constraint for each discrete transition.

The most important benefit of *Exponential Condition* is that it is less conservative than *Convex Condition* [8] and *Differential Invariant* [11], where the Lie derivative of $\varphi(x)$ is required to satisfy that $\mathcal{L}_f\varphi(x) \leq 0$ (a stronger condition than $\mathcal{L}_f\varphi(x) \leq \lambda\varphi(x)$), and meanwhile, it possesses the property of convexity as well. On the one hand, a less conservative inductive invariant forms a tighter over-approximation for the reachable set and hence is able to verify critical safety properties (i.e., the unsafe region is very close to reachable region). On the other hand, a convex inductive invariant condition can be solved efficiently by semidefinite programming method, which is widely used for computing Lyapunov functions in the stability analysis of nonlinear systems. In fact, there exist some other less conservative inductive invariants than *Exponential Condition*, such as [8], [12], [13], however, these inductive conditions are not convex and thus cannot be solved by semidefinite programming method. Instead, they are usually solved by quantifier elimination and SMT solver, which usually has a much higher computational complexity than semidefinite programming method.

Given a semialgebraic hybrid system, we choose a set of polynomials of bounded degree with unknown coefficients as the candidate inductive invariant, and then we obtain a set of positive semidefinite polynomials (i.e. $P(x) \geq 0$) according to *Exponential Condition*. Therefore, the generation of barrier certificate based on *Exponential Condition* can be transformed to the problem of sum-of-squares programming of positive semidefinite polynomials [15]. Based on our theory, we develop an algorithm for generating the inductive invariant satisfying *Exponential Condition*. Experiments on both nonlinear systems and hybrid systems show the effectiveness and practicality of our method.

The remainder of this paper is organized as follows. Section 2 introduces the preliminaries of our method. Section 3 presents the barrier certificate conditions for continuous systems and hybrid systems. Section 4 introduces the computational method we use to construct barrier certificates according to the barrier certificate conditions. Section 5 gives some examples to demonstrate the application of our method to the safety verification of continuous and hybrid systems. Finally, we conclude our work in Section 6.

2 Preliminaries

In this paper, we adopt the model proposed in [16] as our modeling framework. Many other models for hybrid system can be found in [17], [2].

A continuous system is specified by a differential equation

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

where $x \in \mathbb{R}^n$ and f is a Lipschitz continuous vector function from $\mathbb{R}^n$ to $\mathbb{R}^n$. Note that the Lipschitz continuity guarantees the existence and uniqueness of the solution $x(t)$ to the system (1). A hybrid system can then be defined as:

Definition 1. ***(Hybrid System)*** *A hybrid system is a tuple* $\mathcal{H} = \langle L, X, E, R, G, I, F \rangle$*, where*

- L *is a finite set of locations (or modes);*
- $X \subseteq \mathbb{R}^n$ *is the continuous state space. The hybrid state space of the system is denoted by* $\mathcal{X} = L \times X$ *and a state is denoted by* $(l, x) \in \mathcal{X}$*;*
- $E \subseteq L \times L$ *is a set of discrete transitions;*
- $G : E \mapsto 2^X$ *is a guard mapping over discrete transitions;*
- $R : E \times X \mapsto 2^X$ *is a reset mapping over discrete transitions;*
- $I : L \mapsto 2^X$ *is an invariant mapping;*
- $F : L \mapsto (X \mapsto X)$ *is a vector field mapping which assigns to each location* l *a vector field* f_l*.*

The transition and dynamic structure of the hybrid system defines a set of trajectories. A trajectory is a sequence starting from a state $(l_0, x_0) \in \mathcal{X}_0$, where $\mathcal{X}_0 \subseteq \mathcal{X}$ is an initial set, and consisting of a series of interleaved continuous flows and discrete transitions. During the continuous flows, the system evolves following the vector field $F(l)$ at some location $l \in L$ until the invariant condition $I(l)$ is violated. At some state (l, x), if there is a discrete transition $(l, l') \in E$ such that $(l, x) \in G(l, l')$ (we write $G(l, l')$ for $G((l, l')))$, then the discrete transition can be taken and the system state can be reset to $R(l, l', x)$. The problem of safety verification of a hybrid system is to prove that the hybrid system cannot reach an unsafe set $\mathcal{X}_u$ from an initial set $\mathcal{X}_0$.

Some notations that are used in this paper are presented here. $\mathbb{R}$ denotes the real number field. $\mathcal{C}^1(\mathbb{R}^n)$ denotes the space of 1-time continuously differentiable functions mapping $X \subseteq \mathbb{R}^n$ to $\mathbb{R}$. $\mathbb{R}[x]$ denotes the polynomial ring in x over the real number field and $\mathbb{R}[x]^m$ denotes the m-dimensional polynomial vector space over $\mathbb{R}[x]$. M^T denotes the transpose of the matrix M.

3 Conditions for Constructing Barrier Certificates

3.1 Barrier Certificate Condition for Continuous Systems

Given a continuous system S, an initial set X_0 and an unsafe set X_u, a barrier certificate is a real-valued function $\varphi(x)$ of states satisfying that $\varphi(x) \leq 0$ for any point x in the reachable set R and $\varphi(x) > 0$ for any point x in the unsafe set X_u (called *General Constraint* hereafter). Therefore, if there exists such a function $\varphi(x)$, we can assert that $R \cap X_u = \emptyset$, that is, the system can not reach a state in the unsafe set from the initial set. However, the exact reachable set R is not computable for most hybrid systems, we cannot decide directly whether $\varphi(x) \leq 0$ holds for all the points in R. Therefore, various alternative inductive conditions that are equivalent to or sufficient for *General Constraint* were proposed. In what follows, we present a new barrier certificate which is a sufficient condition for *General Constraint*.

Consider a continuous system $\mathbb{C}$ specified by the differential equation (1), we assume that $X_0 (\subseteq X)$, X_u are the initial set and the unsafe set respectively. Then, we have the following theorem as a barrier certificate condition.

Theorem 1 (Exponential Condition). *Given the continuous system* (1) *and the corresponding sets X, X_0 and X_u, for any given $\lambda \in \mathbb{R}$, if there exists a barrier certificate, i.e, a real-valued function $\varphi(x) \in \mathcal{C}^1(\mathbb{R}^n)$ satisfying the following formulae:*

$$\forall x \in X_0 : \varphi(x) \leq 0 \tag{2}$$

$$\forall x \in X : \mathcal{L}_f\varphi(x) - \lambda\varphi(x) \leq 0 \tag{3}$$

$$\forall x \in X_u : \varphi(x) > 0 \tag{4}$$

then the safety property is satisfied by the system (1).

Proof. Suppose $x_0 \in X_0$ and $x(t)$ be the corresponding particular solution of the system (1). We aim to prove that for any function $\varphi(x(t))$ satisfying the formulae (2)- (4), the following formula holds:

$$\forall \zeta \geq 0 : \varphi(x(\zeta)) \leq 0. \tag{5}$$

Let $g(x) = \mathcal{L}_f\varphi(x) - \lambda\varphi(x)$, then by (3)

$$\forall x \in X : g(x) \leq 0 \tag{6}$$

Since $\frac{d\varphi(x(t))}{dt} = \frac{\partial\varphi}{\partial x}\frac{dx}{dt} = \frac{\partial\varphi}{\partial x}f(x) = \mathcal{L}_f\varphi(x)$, we have the differential equation about $\varphi(x(t))$

$$\begin{cases} \frac{d\varphi(x(t))}{dt} - \lambda\varphi(x(t)) - g(x(t)) = 0 \\ \varphi(x(0)) = \varphi(x_0) \end{cases} \tag{7}$$

By solving the differential equation (7), we have the following solution:

$$\varphi(x(t)) = (\int_0^t (g(x(\tau))e^{-\lambda\tau}d\tau + \varphi(x_0))e^{\lambda t}. \tag{8}$$

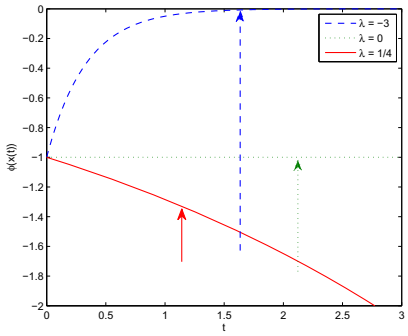


Fig. 1. Dependency of Barrier Certificate Condition on λ. As the value of λ decreases (e.g. from 1/4 to -3), the upper-bound of the value of $\varphi(x(t))$ approaches to zero infinitely, which means the barrier certificate condition becomes less conservative.

By (6), we have

$$\int_0^t (g(x(\tau))e^{-\lambda\tau}d\tau \leq 0. \tag{9}$$

then by (9) and $\varphi(x_0) \leq 0$, we finally have

$$\varphi(x(t)) \leq \varphi(x_0)e^{\lambda t} \leq 0. \tag{10}$$

Hence, for any $\zeta \geq 0$, $\varphi(x(\zeta)) \leq 0$ holds. □

Remark 1. The formulae (2) and (4) ensure that the barrier separates the initial set X_0 from the unsafe set X_u, and the formula (3) ensures that system trajectories cannot escape from inside of the barrier. These formulae together imply that $\varphi(x) \leq 0$ is an inductive invariant of the system (1).

From another point of view, the semi-algebraic set $\{x \in \mathbb{R}^n | \varphi(x) \leq 0\}$ forms an over-approximation for the reachable set of the system (1), and the zero level set of the function $\varphi(x)$ (i.e., $\{x \in \mathbb{R}^n | \varphi(x) = 0\}$) forms the boundary of the over-approximation. In order to be less conservative, we hope the boundary of the over-approximation encloses the reachable set $\{x(t) | x(0) \in X_0, \dot{x} = f(x), t \in \mathbb{R}_+\}$ as tightly as possible, in other words, to make the upper-bound of $\varphi(x(t))$ approach zero as closely as possible. According to the above proof (i.e., (10)), the scope over which the function $\varphi(x(t))$ can range depends closely on the value of the parameter λ: the less value the λ is, the closer the upper-bound of the scope that $\varphi(x(t))$ can reach is to zero (see Fig. 1). Roughly speaking, the values of λ are divided into three classes according to the conservativeness of the barrier certificate condition:

- $\lambda = 0$. In this case, the formula (3) is degenerated to $\frac{\partial \varphi}{\partial x} f(x) \leq 0$, which is the case of *Convex Condition*. This condition implies that the value of $\varphi(x(t))$ will never get close to zero over time t. Thus, the condition is very conservative. Similarly, *Differential Invariant* is a generalization of *Convex Condition* and accordingly it completely inherits the conservativeness of *Convex Condition* (Refer to [18] for a detailed explanation on this point).
- $\lambda < 0$. In this case, we know that 1) $\varphi(x(t)) \leq \varphi(x_0)e^{\lambda t} \leq 0$, and 2) $\frac{\partial \varphi}{\partial x} f(x) \leq \lambda \varphi(x) \geq 0$. These two inequalities together imply that the value of $\varphi(x(t))$ can increase over the time t but never get across the upper bound 0, provided that $\varphi(x(0)) \leq 0$ at the beginning.
- $\lambda > 0$. In this case, $\frac{\partial \varphi}{\partial x} f(x) \leq \lambda \varphi(x) \leq 0$, which means that the value of $\varphi(x(t))$ get far away from 0. Apparently, the condition is much more conservative than the first case.

Therefore, as long as we let $\lambda < 0$, we can get less conservative barrier certificate conditions than *Convex Condition* and *Differential Invariant*. Note that *Exponential Condition* is convex as well and its convexity can be easily proved by verifying that for any two functions $\varphi_1(x)$ and $\varphi_2(x)$ satisfying the formulae (2)–(4) and any θ with $0 \leq \theta \leq 1$, $\varphi(x) = \theta\varphi_1(x) + (1-\theta)\varphi_2(x)$ satisfies the formulae (2)–(4) as well. Based on this fact, we can convert the problem of constructing barrier certificate into the problem of convex optimization which we will discuss in Section 4.

In the following subsection, we extend the barrier certificate condition for continuous systems to hybrid systems.

3.2 Barrier Certificate Condition for Hybrid Systems

Different from the barrier certificate for a continuous system, the barrier certificate for a hybrid system consists of a set of functions $\{\varphi_l(x) | l \in L\}$, each of which corresponds to a discrete location of the system and forms a barrier between the reachable set and the unsafe set at that individual location. For each function $\varphi_l(x)$ at location l, in addition to defining constraints for the continuous flows, the barrier certificate conditions have to take into account all the discrete transitions starting from location l to make the overall barrier certificate an inductive invariant. Formally, we define the barrier certificate condition for hybrid systems as the following theorem.

Theorem 2 (Hybrid-Exp Condition). *Given the hybrid system* $\mathcal{H} = \langle L, X, E, R, G, I, F \rangle$, *the initial set* $\mathcal{X}_0$ *and the unsafe set* $\mathcal{X}_u$ *of* $\mathcal{H}$, *then, for any given set of constant real numbers* $S_\lambda = \{\lambda_l \in \mathbb{R} | l \in L\}$ *and any given set of constant non-negative real numbers* $S_\gamma = \{\gamma_{ll'} \in \mathbb{R}_+ | (l, l') \in E\}$, *if there exists a set of functions* $\{\varphi_l(x) | \varphi_l(x) \in \mathcal{C}^1(\mathbb{R}^n), l \in L\}$ *such that, for all* $l \in L$ *and* $(l, l') \in E$, *the following formulae hold:*

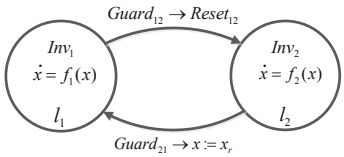


Fig. 2. A hybrid system without barrier certificate satisfying *Convex Condition*

$$\forall x \in \mathrm{Init}(l) : \varphi_l(x) \leq 0 \tag{11}$$
$$\forall x \in I(l) : \mathcal{L}_{f_l}\varphi_l(x) - \lambda_l\varphi_l(x) \leq 0 \tag{12}$$
$$\forall x \in G(l,l'), \forall x' \in R((l,l'),x) : \gamma_{ll'}\varphi_l(x) - \varphi_{l'}(x') \geq 0 \tag{13}$$
$$\forall x \in \mathrm{Unsafe}(l) : \varphi_l(x) > 0 \tag{14}$$

where $\mathrm{Init}(l)$ *and* $\mathrm{Unsafe}(l)$ *denote respectively the initial set and the unsafe set at location* l*, then the safety property is satisfied by* $\mathcal{H}$*.*

The proof of Theorem 2 can be found in [18]. Informally, the formulae (11), (12) and (14) together ensure that at each location $l \in L$, the system never evolves into an unsafe state continuously. The formula (13) ensures that the system never jumps from a safe state to an unsafe state discretely. By induction, the formulae (11)–(14) together guarantee the safety of the system.

Remark 2. The selection of the parameter set S_λ is essential to the conservativeness of the barrier certificate conditions. As discussed in Subsection 3.1, by setting all the elements of S_λ to 0, we can derive *Convex Condition* for hybrid systems. However, *Convex Condition* is too restrictive to be useful for hybrid systems. For example, see the hybrid system in Fig. 2, there is a reset operation $x = x_r$ (which is often the case) at the transition (l_2, l_1). Assume there exists a barrier certificate $\{\varphi_{l_1}(x), \varphi_{l_2}(x)\}$ if we set all the elements of S_λ to 0 and (without loss of generality) set all the elements of S_γ to 1, then for any trajectory containing at least two times of the transition (l_2, l_1), one at time instant t_1 and another at t_2, $t_1 < t_2$, respectively, we can assert that $\varphi_{l_1}(x_{l_1t_1}) > \varphi_{l_1}(x_{l_1t_2})$ according to Theorem 2, this contradicts with $x_{l_1t_1} = x_{l_1t_2} = x_r$, that is, the barrier certificate satisfying *Convex Condition* does not exist no matter what the unsafe set is. Therefore, in order to make the barrier certificate condition less conservative, we try to choose negative values for $\lambda_l \in S_\lambda$ and theoretically: the less, the better. However, in practice, the optimal domain for λ may depend on the specific computational method. For example, the interval $[-1, 0)$ appears to be optimal and not too sensitive in-between for the semidefinite programming method used in this paper.

The selection of S_γ is relatively simple. We usually set all of its elements to 1 except for the discrete jumps with a reset operation that is independent of the pre-state of the jump, for which we usually set $\gamma_{ll'}$ to 0.

4 Construction Method for Barrier Certificate

Constructing inductive invariants for general hybrid systems is very hard. Fortunately, for some existing inductive conditions, several computational methods are available for semialgebraic hybrid systems. The most representative methods include the fixed-point method based on saturation [11], the constraint-solving methods based on semidefinite programming [9] and quantifier elimination [12] and the Gröbner bases method [7], [6]. Similar to *Convex Condition*, *Exponential Condition* defines a convex set of barrier certificate functions as well and hence can be solved by semidefinite programming method supposing the hybrid system is semialgebraic and the barrier certificate function $\varphi(x)$ is a polynomial.

In our computational method, a barrier certificate is assumed to be a set $\Phi = \{\varphi_l(x)|l \in L\}$ of multivariate polynomials of fixed degrees with a set of unknown real coefficients. According to the constraint inequalities in Theorem 1 or Theorem 2, we can obtain a set of positive semidefinite (*PSD*) polynomials $Q = \{Q_i|Q_i(x) \geq 0, deg(Q_i) = 2n, x \in \mathbb{R}^n, n \in \mathbb{N}\}$, where $deg(\cdot)$ returns the degree of a polynomial. Note that a polynomial $Q(x)$ of degree $2k$ is said to be *PSD if and only if* $Q(x) \geq 0$ for all $x \in \mathbb{R}^n$. Thus, our objective is to find a set of real-valued coefficients for $\varphi_l \in \Phi$ to make all the $Q_i \in Q$ be *PSD*.

A famous sufficient condition for a polynomial $P(x)$ of degree $2k$ to be *PSD* is that it is a sum-of-squares (*SOS*) $P(x) = \sum q_i(x)^2$ for some polynomials $q_i(x)$ of degree k or less [19]. Furthermore, it is equivalent to that $P(x)$ has a positive semidefinite quadratic form, i.e., $P(x) = v(x)Mv(x)^T$, where $v(x)$ is a vector of monomials with respect to x of degree k or less and M is a real symmetric *PSD* matrix with the coefficients of $P(x)$ as its entries. Therefore, the problem of finding a *PSD* polynomial $P(x)$ can be converted to the problem of solving a linear matrix inequality (*LMI*) $M \succeq 0$ [20], which can be solved by semidefinite programming [21].

In our work, we extend SOSTOOLS based on the theory in this paper to implement an algorithm for discovering barrier certificate automatically.

4.1 Sum-of-Squares Transformation for Continuous System

In order to be solvable for the barrier certificate condition by *SOS* programming, we need to restate it with multivariate polynomials. In this context, we assume that all the state sets involved in the condition are semialgebraic, that is, they can be written as $\{x \in \mathbb{R}^n|P_1(x) \geq 0, ..., P_m(x) \geq 0, P_i(x) \in \mathbb{R}[x], 1 \leq i \leq m\}$). For convenience, we write it compactly as $\{x \in \mathbb{R}^n|\mathcal{P}(x) \geq 0, \mathcal{P}(x) \in \mathbb{R}[x]^m\}$, where $\mathcal{P}(x) = (P_1(x), P_2(x), ..., P_m(x))$. In addition, each dimension of the vector field $f(x)$ and the barrier certificate function $\varphi(x)$ are all polynomials in $\mathbb{R}[x]$. Based on the previous assumption, we present the sum-of-squares transformation of *Exponential Condition* for continuous systems as the following corollary.

Corollary 1. *Given the continuous polynomial system* (1) *and the initial set* $X_0 = \{x \in \mathbb{R}^n|I_0(x) \geq 0, I_0(x) \in \mathbb{R}[x]^r\}$ *and the unsafe set* $X_u = \{x \in \mathbb{R}^n|U(x) \geq 0, U(x) \in \mathbb{R}[x]^s\}$, *where* r *and* s *are the dimensions of the polynomial vector spaces, for any given* $\lambda \in \mathbb{R}$ *and any given real number* $\epsilon > 0$,

if there exists a polynomial function $\varphi(x) \in \mathbb{R}[x]$ *and two* SOS *polynomial vectors (i.e., every element of the vector is a* SOS *polynomial)* $\mu(x) \in \mathbb{R}[x]^r$ *and* $\eta(x) \in \mathbb{R}[x]^s$ *satisfying that the following polynomials*

$$-\varphi(x) - \mu(x)I_0(x) \tag{15}$$

$$-\mathcal{L}_f\varphi(x) + \lambda\varphi(x) \tag{16}$$

$$\varphi(x) - \eta(x)U(x) - \epsilon \tag{17}$$

are all SOS*s, then the safety property is satisfied by the system* (1).

Proof. It is sufficient to prove that any $\varphi(x)$ satisfying (15)–(17) also satisfies (2)–(4). By (15), we have $-\varphi(x) - \mu(x)I_0(x) \geq 0$, that is, $\varphi(x) \leq -\mu(x)I_0(x)$. Because for any $x \in X_0$, $-\mu(x)I_0(x) \leq 0$, this means $\varphi(x) \leq 0$. Similarly, we can derive (3) from (16). By (17), it's easy to prove that $\varphi(x) - \epsilon \geq 0$ holds for any $x \in X_u$. Since ϵ is greater than 0, then the formula (4) holds. Therefore, the system (1) is safe. □

Remark 3. Since the polynomials (15)–(17) are required to be *SOS*s, each of them can be transformed to a positive semidefinite quadratic form $v(x)M_iv(x)^T$, where M_i is a real symmetric *PSD* matrix with the coefficients of $\varphi(x)$, $\mu(x)$ and $\eta(x)$ as its variables. As a result, we obtain a set of *LMI*s $\{M_i \succeq 0\}$ which can be solved by semidefinite programming.

We use *Algorithm* 1 to compute the desired barrier certificate. In the algorithm, we first choose a small set of negative values Λ as a candidate set for λ and an integer interval $[dMin, dMax]$ as a candidate set for degree d of $\varphi(x)$. Then, we attempt to find a barrier certificate satisfying the formulae (15)–(17) for a fixed pair of λ and d until such one is found. Theoretically, according to the analysis about the dependence of conservativeness of barrier certificate on the value of λ, we should set λ to as small negative value as possible. However, experiments show that too small negative numbers for λ often lead the semidefinite programming function to numerical problems. In practice, the negative values in the interval $[-1, 0)$ are good enough for λ to verify very critical safety properties. Note that the principle for step 3 in *Algorithm 1* is that if $\varphi(x)$ has a dominating degree in both polynomials, there couldn't exist a solution that make both polynomials be *SOS*s because $-\varphi(x)$ and $\varphi(x)$ occur in (15) and (17) simultaneously. The motive for eliminating the monomials with small coefficients in step 7 is from the observation that those monomials are usually the cause of the failed *SOS* decomposition for the polynomials when the semidefinite programming function gives a seemingly feasible solution.

The idea for constructing barrier certificates for continuous systems can be easily extended to hybrid systems. We describe it in the following subsection.

4.2 Sum-of-Squares Transformation for Hybrid System

Similar to continuous system, in order to be solvable by semidefinite programming, we need to limit the hybrid system model in Section 2 to semialgebraic hybrid system.

Algorithm 1. Computing Barrier Certificate for Continuous System

Input: f: array of polynomial vector field; I_0: array of polynomials defining X_0; U: array of polynomials defining X_u
Output: φ: barrier certificate polynomial
Variables : λ: a real negative value; d: degree of φ
Constants: Λ: array of candidate values for λ; ϵ: a positive value; $dMin$, $dMax$: the minimal degree and maximal degree of φ to be found

1 Initialize. Set Λ to a set of negative values between -1 and 0; Set ϵ to a small positive value; Set $dMin$ and $dMax$ to positive integer respectively;
2 Pick λ and d. For each $\lambda \in \Lambda$ and for each d from $dMin$ to $dMax$, perform step 3–7 until a barrier certificate is found;
3 Decide the degree of $\mu(x)$ and $\eta(x)$ according to d. To be SOSs for both (15) and (17), at least one of the degrees of $\mu(x)I_0(x)$ and $\eta(x)U(x)$ is greater than or equal to the degree of $\varphi(x)$;
4 Generate complete polynomials $\varphi(x)$, $\mu(x)$ and $\eta(x)$ of specified degree with unknown coefficient variables;
5 Eliminate the monomials of odd top degrees in (15)–(17), $\mu(x)$ and $\eta(x)$, respectively. To be a SOS, a polynomial has to be of even degree. Concretely, let the coefficients of the monomials to be eliminated be zero to get equations about coefficient variables and then reduce the number of coefficient variables by solving the equations and substituting free variables for non-free variables in all the related polynomials;
6 Perform the SOS programming on the positive semidefinite constraints (15)–(17) and $\mu(x)$, $\eta(x)$;
7 Check if a feasible solution is found, if not found, continue with a new loop; else, check if the solution can indeed enable the corresponding polynomials to be SOSs, if so, return $\varphi(x)$; else, for all the polynomials in the programming, eliminate all the monomials whose coefficients have too small absolute values(usually less than 10^{-5}) by using the same method as step 5, then go to step 6 unless an empty polynomial is produced;

Consider the hybrid system $\mathbb{H} = \langle L, X, E, R, G, I, F\rangle$, where the mappings F, R, G, I of $\mathbb{H}$ are defined with respect to polynomial inequalities as follows:

- $F : l \mapsto\ f_l(x)$
- $G : (l, l') \mapsto \{x \in \mathbb{R}^n | G_{ll'}(x) \geq\ 0, G_{ll'}(x) \in \mathbb{R}[x]^{p_{ll'}}\}$
- $R : (l, l', x) \mapsto\ \{x' \in \mathbb{R}^n | R_{ll'x}(x') \geq\ 0, R_{ll'x}(x') \in \mathbb{R}[x]^{q_{ll'}}\}$
- $I : l \mapsto \{x \in \mathbb{R}^n | I_l(x) \geq\ 0, I_l(x) \in \mathbb{R}[x]^{r_l}\}$

and the mappings of the initial set and the unsafe set are defined as follows:

- $\text{Init} : l \mapsto \{x \in \mathbb{R}^n | \text{Init}_l(x) \geq 0, \text{Init}_l(x) \in \mathbb{R}[x]^{s_l}\}$
- $\text{Unsafe} : l \mapsto \{x \in \mathbb{R}^n | \text{Unsafe}_l(x) \geq 0, \text{Unsafe}_l(x) \in \mathbb{R}[x]^{t_l}\}$

where $p_{ll'}$, $q_{ll'}$, r_l, s_l and t_l are the dimensions of polynomial vector spaces. Then we have the following corollary for constructing barrier certificate for the semialgebraic hybrid system $\mathbb{H}$.

Corollary 2. *Let the hybrid system* $\mathbb{H}$ *and the initial state set mapping* Init *and the unsafe state set mapping* Unsafe *be defined as the above. Then, for any given set of constant real numbers* $S_\lambda = \{\lambda_l \in \mathbb{R} | l \in L\}$ *and any given set of constant non-negative real numbers* $S_\gamma = \{\gamma_{ll'} \in \mathbb{R}_+ | (l,l') \in E\}$ *,and any given small real number* $\epsilon > 0$*, if there exists a set of polynomial functions* $\{\varphi_l(x) \in \mathbb{R}[x] | l \in L\}$ *and five sets of* SOS *polynomial vectors* $\{\mu_l(x) \in \mathbb{R}[x]^{s_l} | l \in L\}$, $\{\theta_l(x) \in \mathbb{R}[x]^{r_l} | l \in L\}$, $\{\kappa_{ll'}(x) \in \mathbb{R}[x]^{p_{ll'}} | (l,l') \in E\}$, $\{\sigma_{ll'}(x) \in \mathbb{R}[x]^{q_{ll'}} | (l,l') \in E\}$ *and* $\{\eta_l(x) \in \mathbb{R}[x]^{t_l} | l \in L\}$*, such that the polynomials*

$$\varphi_l(x) - \mu_l(x)\,\mathrm{Init}_l(x) \tag{18}$$

$$\lambda_l \varphi_l(x) - \mathcal{L}_{f_l}\varphi_l(x) - \theta_l(x) I_l(x) \tag{19}$$

$$\gamma_{ll'}\varphi_l(x) - \varphi_{l'}(x') - \kappa_{ll'}(x) G_{ll'}(x) - \sigma_{ll'}(x') R_{ll'x}(x') \tag{20}$$

$$\varphi_l(x) - \epsilon - \eta_l(x)\,\mathrm{Unsafe}_l(x) \tag{21}$$

are SOS*s for all* $l \in L$ *and* $(l,l') \in E$*, then the safety property is satisfied by the system* $\mathbb{H}$*.*

Proof. Similar to Corollary 1, it's easy to prove that any set of polynomials $\{\varphi_l(x)\}$ satisfying (18)–(21) also satisfies (11)–(14), hence the hybrid system $\mathbb{H}$ is safe. □

The algorithm for computing the barrier certificates for hybrid systems is similar to the algorithm for continuous systems except that it needs to take into account the constraint (20) for the discrete transitions. We do not elaborate on it here any more. Note that the strategy for the selection of λ's for continuous system applies here as well and we only need to set all the elements of S_γ to 1 except for the discrete transition whose post-state is independent of the pre-state, where we set $\gamma_{ll'}$ to 0 to reduce the computational complexity.

5 Examples

5.1 Example 1

Consider the two-dimensional system (from [22] page 315)

$$\begin{bmatrix} \dot{x_1} \\ \dot{x_2} \end{bmatrix} = \begin{bmatrix} x_2 \\ -x_1 + \frac{1}{3}x_1^3 - x_2 \end{bmatrix}$$

with $\mathcal{X} = \mathbb{R}^2$, we want to verify that starting from the initial set $X_0 = \{x \in \mathbb{R}^2 | (x_1 - 1.5)^2 + x_2^2 \leq 0.25\}$, the system will never evolve into the unsafe set $X_u = \{x \in \mathbb{R}^2 | (x_1+1)^2 + (x_2+1)^2 \leq 0.16\}$. We attempted to use both the *Convex-Condition*-based method proposed in [8] and the *Exponential-Condition*-based method in this paper to find the barrier certificates with a degree ranging from 2 to 10. (Note that in [12], [13], the inductive invariants are not sufficient in general according to [14] and hence cannot be applied to our examples. The work of [19] applies only to a very special class of hybrid systems which is not applicable

to our examples either.) During this process, all the programming polynomials are complete polynomials automatically generated (instead of the non-complete polynomials consisting of painstakingly chosen terms) and all the computations are performed in the same environment. The result of the experiment is listed in Table 5.1. The first column is the degree of the barrier certificate to be found, the second column is the runtime spent by the *Convex-Condition*-based method, and the rest columns are the runtime spent by the *Exponential-Condition*-based method for different value of λ. Note that the symbol $\times$ in the table indicates that the method failed to find a barrier certificate with the corresponding degree either because the semidefinite programming function found no feasible solution or because it ran into a numerical problem.

Table 1. Computing results for *Convex Condition* and *Exponential Condition*

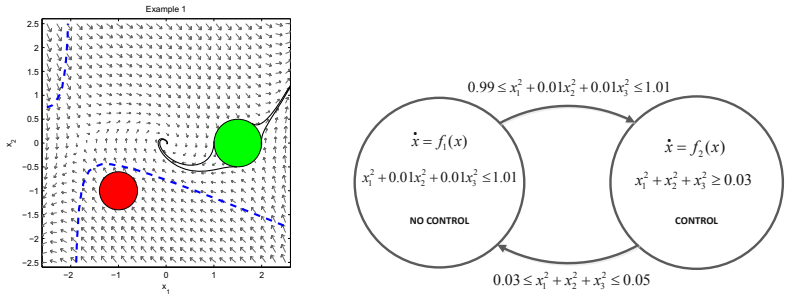
Degree of $\varphi(x)$	Convex Condition	Exponential Condition		
	$Time$(sec)	$Time$(sec)		
		$\lambda = \frac{-1}{8}$	$\lambda = \frac{-1}{4}$	$\lambda = -1$
2	$\times$	0.4867	0.4836	0.2496
3	$\times$	0.5444	0.6224	0.4976
4	0.4368	0.4103	0.4072	0.3853
5	$\times$	0.4321	0.4103	0.3947
6	$\times$	0.3214	0.3011	0.2714
7	$\times$	0.9563	0.9532	0.9453
8	$\times$	0.9188	0.8970	0.7893
9	$\times$	1.4944	1.4149	1.5132
10	$\times$	1.4336	1.3931	1.3650

As shown in Table 5.1, the *Convex-Condition*-based method succeeded only in one case ($Degree = 4$) due to the conservativeness of *Convex Condition*. Comparably, our method found all the barrier certificates of the specified degrees ranging from 2 to 10. Especially, the lowest degree of barrier certificate we found is quadratic: $\varphi(x) = -.86153 - .87278x_1 - 1.1358x_2 - .23944x_1^2 - .5866x_1x_2$ with $\mu(x) = 0.75965$ and $\eta(x) = 0.73845$ when λ is set to -1. The phase portrait of the system and the zero level set of $\varphi(x)$ are shown in Fig. 3(a). Note that being able to find a lower degree of barrier certificates is essential in reducing the computational complexity.

In addition, we can see from Table 5.1 that the runtime of *Exponential-Condition*-based method decreases with the value of λ for each fixed degree except for $Degree = 3, 9$, this observation can greatly evidence our theoretical result about λ selection: the less, the better.

5.2 Example 2

In this example, we consider a hybrid system with two discrete locations (from [9]). The discrete transition diagram of the system is shown in Fig. 3(b) and the vector fields describing the continuous behaviors are as follows:



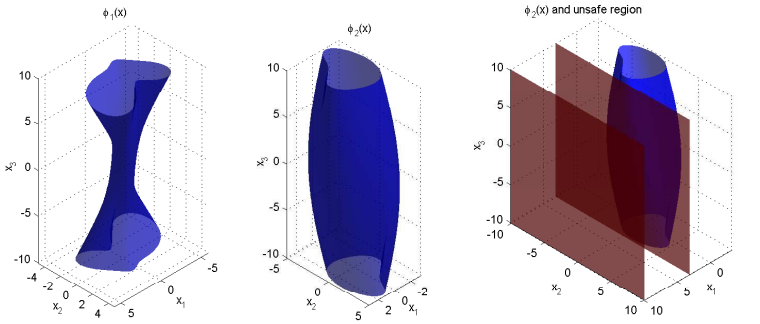
(a) Subsection 5.1 (b) Subsection 5.2

Fig. 3. (a) Phase portrait of the system in Subsection 5.1. The solid patches from right to left are X_0 and X_u, respectively, the solid lines depict the boundary of the reachable region of the system from X_0, and the dashed lines are the zero level set of a quadratic barrier certificate $\varphi(x)$ which separates the unsafe region X_u from the reachable region. (b) Discrete transition diagram of the hybrid system in Subsection 5.2.

$$f_1(x) = \begin{bmatrix} x_2 \\ -x_1 + x_3 \\ x_1 + (2x_2 + 3x_3)(1 + x_3^2) \end{bmatrix}, f_2(x) = \begin{bmatrix} x_2 \\ -x_1 + x_3 \\ -x_1 - 2x_2 - 3x_3 \end{bmatrix}$$

At the beginning, the system is initialized at some point in $X_0 = \{x \in \mathbb{R}^3 | x_1^2 + x_2^2 + x_3^2 \le 0.01\}$ and then it starts to evolve following the vector fields $f_1(x)$ at location 1(NO CONTROL mode). When the system reaches some point in the guard set $G(1,2) = \{x \in \mathbb{R}^3 | 0.99 \le x_1^2 + 0.01x_2^2 + 0.01x_3^3 \le 1.01\}$, it can jump to location 2 (CONTROL mode) nondeterministically without performing any reset operation (i.e., $R(1,2,x) = G(1,2)$). At location 2, the system will operate following the vector field $f_2(x)$, which means that a controller will take over to prevent x_1 from getting too big. As the system enters the guard set $G(2,1) = \{x \in \mathbb{R}^3 | 0.03 \le x_1^2 + x_2^2 + x_3^2 \le 0.05\}$, it will jump back to location 1 nondeterministically again without reset operation (i.e., $R(2,1,x) = G(2,1)$). Different from the experiment in [9], where the objective is to verify that $|x_1| < 5.0$ in CONTROL mode, our objective is to verify that x_1 will stay in a much more restrictive domain in CONTROL mode: $|x_1| < 3.2$.

We define the unsafe set as Unsafe(1) $= \emptyset$ and Unsafe(2) $= \{x \in \mathbb{R}^3 | 3.2 \le x_1 \le 10\} \cup \{x \in \mathbb{R}^3 | -10 \le x_1 \le -3.2\}$, which is sufficient to prove $|x_1| \le 3.2$ in CONTROL mode. Similarly, we tried to use both the method in this paper and the method in [8] to compute the barrier certificate. By setting $\lambda_1 = \lambda_2 = -\frac{1}{5}$ and $\gamma_{12} = \gamma_{21} = 1$, our method found a pair of quartic barrier certificate functions: $\phi_1(x)$ and $\phi_2(x)$, whose zero level set is shown in Fig. 4(a) and Fig. 4(b) respectively. As you can see, at each location $l = 1, 2$, the zero level set of $\phi_l(x)$ forms the boundary of the over-approximation $\phi_l(x) \le 0$ (denoting the points within the pipe) for the reachable set at location l. On the one hand, the hybrid system starts from and evolves within the corresponding over-approximation and jumps back and forth between the two over-approximations. On the other hand,



(a) $\phi_1(x) = 0$ (b) $\phi_2(x) = 0$ (c) $3.2 \leq x_1 \leq 10$, $\phi_2(x) = 0$

Fig. 4. Barrier certificates $\phi_1(x)$ and $\phi_2(x)$ for the hybrid system in Subsection 5.2. $\phi_l(x) = 0$ $(l = 1, 2)$ forms the boundary of the over-approximation $\phi_l(x) \leq 0$ and separates the inside reachable set from the outside unsafe set (e.g. $3.2 \leq x_1 \leq 10$).

the unsafe set does not intersect the over-approximation formed by $\phi_2(x) \leq 0$ (see Fig. 4(c)). Therefore, the safety of the system is guaranteed. However, using the method in [8], we cannot compute the barrier certificate, which means it cannot verify the system.

6 Conclusion

In this paper, we propose a new barrier certificate condition (called *Exponential Condition*) for the safety verification of hybrid systems. Our barrier certificate condition is parameterized by a real number λ and the conservativeness of the barrier certificate condition depends closely on the value of λ: the less value the λ is, the less conservative the barrier certificate condition is. The most important benefit of *Exponential Condition* is that it possesses a relatively low conservativeness as well as the convexity and hence can be solved efficiently by semidefinite programming method.

Based on our method, we are able to construct polynomial barrier certificate to verify very critical safety property for semialgebraic continuous systems and hybrid systems. The experiments on a continuous system and a hybrid system show the effectiveness and practicality of our method.

References

1. Henzinger, T.: The theory of hybrid automata. In: Proc. IEEE Symp. Logic in Computer Science (LICS), pp. 278–292 (1996)
2. Alur, R., Courcoubetis, C., Halbwachs, N., Henzinger, T., Ho, P., Nicollin, X., Olivero, A., Sifakis, J., Yovine, S.: The algorithmic analysis of hybrid systems. Theoretical Computer Science 138(1), 3–34 (1995)
3. Jirstrand, M.: Invariant sets for a class of hybrid systems. In: Proc. IEEE Conference on Decision and Control, vol. 4, pp. 3699–3704 (1998)

4. Rodríguez-Carbonell, E., Tiwari, A.: Generating polynomial invariants for hybrid systems. In: Morari, M., Thiele, L. (eds.) HSCC 2005. LNCS, vol. 3414, pp. 590–605. Springer, Heidelberg (2005)
5. Sankaranarayanan, S., Sipma, H.B., Manna, Z.: Constructing invariants for hybrid systems. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 539–554. Springer, Heidelberg (2004)
6. Sankaranarayanan, S.: Automatic invariant generation for hybrid systems using ideal fixed points. In: Proc. ACM International Conference on Hybrid Systems: Computation and Control, pp. 221–230 (2010)
7. Tiwari, A., Khanna, G.: Nonlinear systems: Approximating reach sets. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 600–614. Springer, Heidelberg (2004)
8. Prajna, S., Jadbabaie, A., Pappas, G.: A framework for worst-case and stochastic safety verification using barrier certificates. IEEE Transactions on Automatic Control 52(8), 1415–1428 (2007)
9. Prajna, S., Jadbabaie, A.: Safety verification of hybrid systems using barrier certificates. In: Alur, R., Pappas, G.J. (eds.) HSCC 2004. LNCS, vol. 2993, pp. 477–492. Springer, Heidelberg (2004)
10. Sloth, C., Pappas, G., Wisniewski, R.: Compositional safety analysis using barrier certificates. In: Proc. ACM International Conference on Hybrid Systems: Computation and Control, pp. 15–24 (2012)
11. Platzer, A., Clarke, E.M.: Computing differential invariants of hybrid systems as fixedpoints. In: Gupta, A., Malik, S. (eds.) CAV 2008. LNCS, vol. 5123, pp. 176–189. Springer, Heidelberg (2008)
12. Gulwani, S., Tiwari, A.: Constraint-based approach for analysis of hybrid systems. In: Gupta, A., Malik, S. (eds.) CAV 2008. LNCS, vol. 5123, pp. 190–203. Springer, Heidelberg (2008)
13. Taly, A., Tiwari, A.: Deductive verification of continuous dynamical systems. In: FSTTCS, vol. 4, pp. 383–394 (2009)
14. Taly, A., Gulwani, S., Tiwari, A.: Synthesizing switching logic using constraint solving. Intl. J. Software Tools for Technology Transfer 13(6), 519–535 (2011)
15. Prajna, S., Papachristodoulou, A., Seiler, P., Parrilo, P.: SOSTOOLS and its control applications. Positive Polynomials in Control, pp. 580–580 (2005)
16. Carloni, L., Passerone, R., Pinto, A.: Languages and tools for hybrid systems design. Foundations and Trends® in Electronic Design Automation 1(1-2) (2006)
17. Maler, O., Manna, Z., Pnueli, A.: Prom timed to hybrid systems. In: Huizing, C., de Bakker, J.W., Rozenberg, G., de Roever, W.-P. (eds.) REX 1991. LNCS, vol. 600, pp. 447–484. Springer, Heidelberg (1992)
18. Kong, H., He, F., Song, X., Hung, W.N.N., Gu, M.: Exponential-Condition-Based Barrier Certificate Generation for Safety Verification of Hybrid Systems (March 2013), ArXiv e-prints: `http://arxiv.org/abs/1303.6885`
19. Lasserre, J.: Sufficient conditions for a real polynomial to be a sum of squares. Archiv der Mathematik 89(5), 390–398 (2007)
20. Boyd, S., El Ghaoui, L., Feron, E., Balakrishnan, V.: Linear matrix inequalities in system and control theory. Society for Industrial Mathematics, vol. 15 (1994)
21. Parrilo, P.: Semidefinite programming relaxations for semialgebraic problems. Mathematical Programming 96(2), 293–320 (2003)
22. Khalil, H.K.: Nonlinear Systems, 3rd edn. Prentice Hall (2001)