Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 4149059, 10 pages
http://dx.doi.org/10.1155/2016/4149059

Research Article

Safety Verification of Interconnected Hybrid Systems Using Barrier Certificates

Guobin Wang,[1,2] Jifeng He,[1,2] Jing Liu,[1,2] Haiying Sun,[1,2] Zuohua Ding,[3] and Miaomiao Zhang[4]

[1] *Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai 200062, China*
[2] *National Trustworthy Embedded Software Engineering Technology Research Center, East China Normal University, Shanghai 200062, China*
[3] *School of Informatics and Electronics, Zhejiang Sci-Tech University, Hangzhou 310018, China*
[4] *School of Software Engineering, Tongji University, Shanghai 201804, China*

Correspondence should be addressed to Jing Liu; jliu@sei.ecnu.edu.cn

Received 23 October 2015; Accepted 26 January 2016

Academic Editor: Bogdan Dumitrescu

Safety verification determines whether any trajectory starting from admissible initial states would intersect with a set of unsafe states. In this paper, we propose a numerical method for verifying safety of a network of interconnected hybrid dynamical systems with a state constraint based on bilinear sum-of-squares programming. The safety verification is conducted by the construction of a function of states called barrier certificate. We consider a finite number of interconnected hybrid systems satisfying the input-to-state property and the networked interconnections satisfying a dissipativity property. Through constructing a barrier certificate for each subsystem and imposing dissipation-inequality-like constraints on the interconnections, safety verification is formulated as a bilinear sum-of-squares feasibility problem. As a result, safety of the interconnected hybrid systems could be determined by solving an optimization problem, rather than solving differential equations. The proposed method makes it possible to verify the safety of interconnected hybrid systems, which is demonstrated by a numerical example.

1. Introduction

The problem of safety verification of hybrid dynamical systems has always been a fundamental issue within the systems, control, and computer communities. In principle, safety verification of hybrid dynamical systems aims to determine that any trajectory starting at admissible initial states cannot evolve to unsafe region in the state space [1]. Numerous methods have been developed for the past two decades [2] and a variety of dynamical characteristics have been researched. Particularly, we concentrate on safety verification of a special kind of nonlinear hybrid dynamical system called polynomial hybrid system. Polynomial hybrid systems are hybrid systems where both the dynamical behavior description and the states constraints are given in terms of polynomial nonlinearities. A wide range of applications could be modeled as, transformed into, or approximated by polynomial hybrid systems, for example, in power systems [3] and process control [4]. In [5–7], computational verification methods based on symbolic computation have been proposed; those methods are mainly based on the theory of ideal over polynomial ring together with techniques such as abstract interpretation. On the other hand, computational verification methods based on numerical computation which originated from [8] have also been well developed. One of the typical methods called barrier certificate generalizes these numerical verification methods and imposes its theoretical foundation on linear matrix inequalities (LMI), semidefinite programming (SDP), sum-of-squares (SOS) programming, and bilinear SOS programming.

Generally speaking, barrier certificate is a function of states whose zero level set separates an unsafe region from all system trajectories starting from an admissible set of initial states. The existence of a barrier certificate is sufficient for safety of dynamical systems, which is analogous to the sufficiency of the existence of a Lyapunov function for asymptotic stability of dynamical systems. As an important numerical method of safety verification of dynamical systems, barrier certificates have been well developed under the frameworks of general nonlinear systems [9], time-delayed systems [10, 11], stochastic systems [12], interconnected continuous systems [13, 14], and hybrid systems [1, 15]. Besides, converse theorem of barrier certificates was discussed recently in [16].

Hybrid systems are dynamical systems exhibiting both continuous and discrete dynamic behaviors, and interconnected hybrid systems are an interconnection of several hybrid systems consisting of assignments relating the inputs and outputs of the individual hybrid systems. Therefore, safety of interconnected hybrid systems relies on both safety of the individual subsystems and their interconnections. In this paper, we propose compositional barrier certificates for safety verification of interconnected hybrid systems. As we know, many networked embedded systems, particularly recently proposed Internet-of-Things and Cyber-Physical Systems [17], are characterized by interconnected hybrid systems; however, safety verification for interconnected hybrid systems has not been well developed. Thus, there is a need to study safety verification method for interconnected hybrid systems. Motivated by the above-mentioned reasons and the practical background, we consider the issue of developing compositional barrier certificates of interconnected hybrid systems for their safety verification. To the best of our knowledge, safety verification has been discussed only for interconnected continuous systems [13, 18–20], but not for interconnected hybrid systems yet, which also motivated our research.

Due to the new features deriving from interconnected hybrid systems, finding a compositional barrier certificate for safety verification presents more technical challenges. Considering that the existences of barrier certificates of each interconnected hybrid system are not sufficient for safety of interconnected hybrid systems, additional dissipation-inequality-like constraints are required to be imposed on interconnections. Compositional barrier certificates in our paper impose additional dissipation-inequality-like coupling constraints on a set of individual barrier certificates for each subsystem. Furthermore, constructing compositional barrier certificates satisfying dissipation-inequality-like constraints is intractable in general; however, through applying SOS relaxation and generalized S-procedure, some conservative compositional barrier certificates could be derived through numerical computation. Once these compositional barrier certificates composed of individual barrier certificates and coupling constraints are feasible, bilinear SOS programming could be applied to construct such compositional barrier certificates through purely numerical computation. Numerical SOS programming solvers such as SOSTOOLS [21] and SOSOPT [22] are developed for such computations. With this methodology, we are able to verify safety of interconnected hybrid systems without resorting exhaustive simulations.

The paper is organized as follows. Section 2 introduces the notations as well as some preliminary definitions. Section 3 adopts the compositional hybrid I/O automata framework to describe interconnected hybrid systems and presents the formal definition of safety. Section 4 explains how to formulate the verification problem by incorporating interconnections satisfying diagonal stability property with individual barrier certificates. Section 5 shows how to construct the compositional barrier certificates through solving a feasibility problem of bilinear SOS programming. Section 6 presents a numerical example to show the validity of the proposed method and Section 7 comprises conclusions.

2. Mathematical Preliminaries

Notations. Let $\mathscr{R}$ denote the field of real numbers, and $\mathscr{R}^n$ stand for the n-dimensional real vector space. $\mathscr{R}_{>0}, \mathscr{N}_{>0}$ refer to the sets of positive real numbers and positive natural numbers, respectively. Lower case alphabets such as i, j, k, l, m, n represent variables, while symbols such as $\vec{x}, \vec{u}, \vec{y}$ are vectorial variables. $\|\cdot\|$ refers to the Euclidean vector norm. For matrices or vectors, the superscript "T" denotes matrix transposition. $I^{m\times m}$ is the identity matrix, $\vec{0}$ denotes zero vector, 0 is scalar, and $0^{m\times n}$ is an $m \times n$ zero matrix. The notation diag$\{\cdot\}$ indicates a square diagonal matrix with the arguments along the diagonal. A^{-1} is the inverse of matrix A.

Definition 1 (positive-definite polynomial and its Lie-derivative). Let $\vec{x}$ denote the n-tuple $(x_1, \dots, x_n)$, $\mathscr{P}_n^m$ will be taken as the polynomial field over variables in $\vec{x}$ with the highest degree of m, and a polynomial function $p(\vec{x}) \in \mathscr{P}_n^m$ is said to be positive definite iff

$$p(\vec{x}) > 0 \tag{1}$$

for all $\vec{x} \in \mathscr{R}^n \setminus \{\vec{0}\}$ with $p(\vec{0}) = 0$. The first-order Lie-derivative of $p(\vec{x})$ along a continuous flow $f(\vec{x}) = (f_1(\vec{x}), \dots, f_n(\vec{x}))$ is as follows:

$$\mathfrak{L}_{f(\vec{x})} p(\vec{x}) = \sum_{i}^{n} \frac{\partial p(\vec{x})}{\partial x_i} f_i(\vec{x}). \tag{2}$$

Definition 2 (SOS polynomial). A multivariate polynomial $p(\vec{x})$ is an SOS polynomial if there exist finite polynomials $p_1(\vec{x}), \dots, p_k(\vec{x})$ such that

$$p(\vec{x}) = \sum_{i=1}^{k} p_i^2(\vec{x}). \tag{3}$$

Let Σ_n^{2m} (Σ_n for short) denote the set of all SOS polynomials in $\vec{x}$ under the degree of $2m$.

Definition 3 (semialgebraic set). A set $\{\vec{x} \in \mathscr{R}^n : p_1(\vec{x}) \geq 0, \dots, p_s(\vec{x}) \geq 0\}$ is called a semialgebraic set iff $p_1(\vec{x}), \dots, p_s(\vec{x}) \in \mathscr{P}_n^m$ and $s \in \mathscr{N}_{>0}$ is finite.

Definition 4 ($\mathscr{K}$ polynomial function). A polynomial function $\alpha(\|\vec{x}\|) : \mathscr{R}_{\geq 0} \to \mathscr{R}_{\geq 0}$ is of class $\mathscr{K}$; equivalently $\alpha(\|\vec{x}\|) \in \mathscr{P}_n^m \cap \mathscr{K}$, if it is strictly increasing and $\alpha(\vec{0}) = 0$.

Definition 5 (Kronecker product). Let $A = [a_{i,j}] \in \mathscr{R}^{m\times n}$, $B \in \mathscr{R}^{p\times q}$ denote two matrices, and then the Kronecker product of A and B is defined as the matrix:

$$A \otimes B = \begin{pmatrix} a_{1,1}B & \cdots & a_{1,n}B \\ \vdots & \ddots & \vdots \\ a_{m,1}B & \cdots & a_{m,n}B \end{pmatrix}. \tag{4}$$

Definition 6 (≤ for matrices). For two matrices $A = [a_{i,j}] \in \mathscr{R}^{m\times n}$, $B = [b_{i,j}] \in \mathscr{R}^{m\times n}$, $A \leq B$ if and only if

$$a_{i,j} \leq b_{i,j} \quad \forall 1 \leq i \leq m,\ 1 \leq j \leq n. \tag{5}$$

The bilinear SOS program is a subclass of nonlinear program which takes the following form.

Definition 7 (bilinear SOS program, see [22]). Standard bilinear SOS program form is

$$\begin{aligned} \text{Min} \quad & \text{scalar variable } t \\ \text{s.t.} \quad & t b_k\left(\vec{x},\vec{d}\right) - a_k\left(\vec{x},\vec{d}\right) \in \Sigma_n, \quad k = 1,\ldots,N_g \\ & b_k\left(\vec{x},\vec{d}\right) \in \Sigma_n, \quad k = 1,\ldots,N_g \\ & c_j\left(\vec{x},\vec{d}\right) = 0, \quad k = 1,\ldots,N_e, \end{aligned} \tag{6}$$

where $t \in \mathscr{R}$, $\vec{x} \in \mathscr{R}^n$, and $\vec{d} \in \mathscr{R}^r$ are decision variables. $\{a_k(\vec{x},\vec{d})\}$, $\{b_k(\vec{x},\vec{d})\}$, $\{c_j(\vec{x},\vec{d})\}$ are polynomials with given data and affine in $\vec{d}$.

3. Formal Models of Interconnected Systems

Throughout this paper, we adopt the compositional hybrid I/O automata framework discussed in [23] for describing interconnected hybrid systems. Interactions of individual hybrid dynamics occur at both the continuous and discrete levels. In this section, we would like to present the formal model of compositional hybrid I/O automata $\mathbb{H}$ which is a composition of finite hybrid I/O automaton $\mathbb{H}_{i\in\mathbb{I}}$ indexed by the finite set $\mathbb{I}$. To provide the formal definition of compositional hybrid I/O automata, we initially consider the individual hybrid I/O automata.

Definition 8 (individual hybrid I/O automaton). An individual hybrid I/O automaton $\mathbb{H}_i$ of $\mathbb{H}$ is a tuple $\mathbb{H}_i = \{\mathbb{X}_i, \mathbb{U}_i, \mathbb{Y}_i, \mathbb{S}_i, \mathbb{Q}_i, \mathbb{G}_i, \mathbb{F}_i, \mathbb{T}_i, \mathbb{X}_i^0, \mathbb{X}_i^u\}$ with the following components:

(i) $\mathbb{X}_i \subseteq \mathscr{R}^{n_i}$ is a set of real-valued system internal variables $\vec{x}_i \in \mathbb{X}_i$. The number n_i is called the dimension of $\mathbb{H}_i$.

(ii) $\mathbb{U}_i \subseteq \mathscr{R}^r$ is a set of real-valued system external inputs $\vec{u}_i^c, \vec{u}_i^d \in \mathbb{U}_i$, where $\vec{u}_i^c$ denotes the continuous input while $\vec{u}_i^d$ denotes the discrete input. $\mathbb{U}_i$ is disjoint from $\mathbb{X}_i$.

(iii) $\mathbb{Y}_i \subseteq \mathscr{R}^r$ is a set of real-valued system external outputs $\vec{y}_i^c, \vec{y}_i^d \in \mathbb{Y}_i$, where $\vec{y}_i^c$ denotes the continuous output while $\vec{y}_i^d$ denotes the discrete output. $\mathbb{Y}_i$ is disjoint from $\mathbb{X}_i \cup \mathbb{U}_i$.

(iv) $\mathbb{S}_i$ is a finite set of indexes of switching signals. The index function $\sigma(t) : [0,T] \rightarrow \mathbb{S}_i = \{1_i,\ldots,j_i, l_i,\ldots,s_i\}$ denotes the sequence of activated switching signals $\mathbb{S}_i$ over the continuous-time interval $[0,T]$.

(v) $\mathbb{Q}_i$ is a finite set of modes. The overall state space of individual hybrid systems $\mathbb{H}_i$ is $\mathbb{Q}_i \times \mathbb{X}_i$, and a state is denoted by $(q_i, \vec{x}_i) \in \mathbb{Q}_i \times \mathbb{X}_i$. $q_i^j, q_i^k \in \mathbb{Q}_i$ denote different modes of $\mathbb{H}_i$ when $j \neq k$.

(vi) $\mathbb{G}_i \subseteq \mathbb{X}_i$ is the set of guard conditions for $\mathbb{H}_i$. A switching is enabled at $t_i^\star$ once $\vec{x}_i(t_i^\star) \in \mathbb{G}_i$ holds, namely, a state-dependent switching. Throughout this paper, all switchings of $\mathbb{H}_i$ are assumed to be state-dependent. Furthermore, $\mathbb{C}_i$ is taken as the complement of $\mathbb{G}_i$ ($\mathbb{C}_i = \mathbb{X}_i - \mathbb{G}_i$).

(vii) $\mathbb{F}_i : \mathbb{C}_i \rightarrow 2^{\mathbb{X}_i}$ is a set of continuous vector fields. For each state $(q_i, \vec{x}_i) \in \mathbb{Q}_i \times \mathbb{X}_i$, $\mathbb{F}_i$ incorporates a differential constraint on the continuous evolution according to the differential equation:

$$\dot{\vec{x}}_i = f_i^{\sigma_i(t_i)}\left(t_i, \vec{x}_i\left(t_i\right), \vec{u}_i^c\right), \tag{7}$$

where $\vec{x} \in \mathbb{C}_i$, $t_i \in (t_i^{k-1}, t_i^k]$, $k \in \mathscr{N}_{>0}$, and $\sigma_i(t_i) \in \mathbb{S}_i$.

(viii) $\mathbb{T}_i : \mathbb{Q}_i \times \mathbb{G}_i \times \mathbb{S} \rightarrow \mathbb{Q}_i$ is a relation capturing discrete switchings between two modes. Here a switching $(q_i^j, \vec{x}_i(t_i^\star), \sigma_i(t_i^\star)) \xrightarrow{\vec{x}_i(t_i^\star)\in\mathbb{G}_i} q_i^k$ indicates that from mode q_i^j, $\mathbb{H}_i$ can undergo a switching to the mode q_i^k at the instant $t_i^\star$. Only finite switchings are allowed over finite-time intervals.

(ix) $\mathbb{X}_i^0 \subseteq \mathbb{X}$ is the set of admissible initial states of $\mathbb{H}_i$.

(x) $\mathbb{X}_i^u \subseteq \mathbb{X}$ is the set of unsafe states of $\mathbb{H}_i$.

Trajectories of $\mathbb{H}_i$ start from the admissible initial states $\vec{x}_i^0$ and are concatenations of a sequence of continuous evolutions in $\vec{x}_i$ and discrete switchings among different modes $q_i^j, q_i^k \in Q_i$ satisfying the following.

Initiation. $\vec{x}_i^0 \in \mathbb{X}_i^0$ is an admissible initial state of $\mathbb{H}_i$.

Discrete Consecution. At the instant $t_i^\star : \vec{x}_i(t_i^\star) \in \mathbb{G}_i$, the switching signal $\sigma_i(t_i^\star) \in \mathbb{S}_i$

$$\begin{gathered} \left(q_i^j, \vec{x}_i\left(t_i^\star\right), \sigma_i\left(t_i^\star\right)\right) \xrightarrow{\vec{x}_i(t_i^\star)\in\mathbb{G}_i} q_i^k \Longrightarrow \\ \lim_{t_i\rightarrow t_i^{\star-}} q_i^{\sigma_i(t_i)} = q_i^j \wedge \lim_{t_i\rightarrow t_i^{\star+}} q_i^{\sigma_i(t_i)} = q_i^k \end{gathered} \tag{8}$$

activates and produces a discrete output according to

$$\vec{y}_i^d\left(t_i^\star\right) = h_i^d\left(t_i^\star, \vec{x}_i\left(t_i^\star\right)\right) \tag{9}$$

simultaneously.

Continuous Consecution. For an activating mode $q_i^j \in \mathbb{Q}_i$ over the $[t_i^k, t_i^{k+1})$

$$\vec{x}_i(t_i) \in \mathbb{C}_i \wedge \dot{\vec{x}}_i = f_i^{q_i^j}(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \quad \forall t_i \in [t_i^k, t_i^{k+1}) \tag{10}$$

holds and produces continuous outputs according to

$$\vec{y}_i^c(t_i) = h_i^c(t_i, \vec{x}_i(t_i)) \quad \forall t_i \in [t_i^k, t_i^{k+1}) \tag{11}$$

over the continuous interval.

Here, $t_i^{\star -}$ denotes the left limit of $t_i^\star$ and $t_i^{\star +}$ denotes its right limit. Additionally, $f_i(t_i, \vec{x}_i, \vec{u}_i^c)$s, $h^c(t_i, \vec{x}_i(t_i))$s, and $h^d(t_i, \vec{x}_i(t_i))$s are all restricted to polynomials throughout this paper.

Compositional hybrid I/O automaton $\mathbb{H}$ is given as an interconnection of finite individual hybrid I/O automaton consisting of assignments relating the inputs and outputs of interconnected $\mathbb{H}_i$.

Definition 9 (compositional hybrid I/O automaton). A compositional hybrid I/O automaton $\mathbb{H}$ is a finite set of interconnected hybrid I/O automata $\mathbb{H}_i$ indexed by $i \in \mathbb{I}$. Formally, $\mathbb{H}$ is a tuple $\mathbb{H} = \{\mathbb{I}, \bigcup_{i\in\mathbb{I}}\{\mathbb{H}_i\}, \mathbb{N}^c, \mathbb{N}^d, \mathbb{K}\}$ with the following components:

(i) $\mathbb{I}$ is a finite set of indexes of interconnected hybrid automaton $\{\mathbb{H}_i\}$. Without loss of generality, we assume $\mathbb{I}$ has $M \in \mathcal{N}_{>0}$ elements.

(ii) $\bigcup_{i\in\mathbb{I}}\{\mathbb{H}_i\}$ is a finite set of interconnected hybrid I/O automata. $\mathbb{X}, \mathbb{U}, \mathbb{Y}, \mathbb{S}, \mathbb{Q}, \mathbb{F}, \mathbb{T}, \mathbb{X}^0, \mathbb{X}^u$ of $\mathbb{H}$ are the Cartesian products of each corresponding item of all individual $\mathbb{H}_i$s, respectively. Particularly, $\mathbb{G} = \{\langle \vec{x}_1, \ldots, \vec{x}_i, \ldots, \vec{x}_M \rangle \in \mathbb{X} : \exists i \in \mathbb{I},\ \vec{x}_i \in \mathbb{G}_i\}$, which means $\vec{x} \in \mathbb{G}$ if there exists an $\vec{x}_i$ of $\mathbb{H}_i$ which intersects corresponding guard $\mathbb{G}_i$. Dually, $\mathbb{C} \subseteq \mathbb{X}$ is defined as $\{\langle \vec{x}_1, \ldots, \vec{x}_i, \ldots, \vec{x}_M \rangle \in \mathbb{X} : \forall i \in \mathbb{I},\ \vec{x}_i \in \mathbb{C}_i\}$. Besides, only finite switchings are allowed over any finite-time intervals.

(iii) $\mathbb{K}$ represents the static topology of the interconnection, which is in the form of an $M \times M$ matrix $K = [a_{j,k}]_{M\times M}$, $a_{j,k} \in \{0, 1\}$, $1 \leq j, k \leq M$.

(iv) $\mathbb{N}^c$ is a finite set of interconnections following continuous assignments

$$\vec{u}_i^c = g_i^c(a_{i,1} \cdot \vec{y}_1^c, \ldots, 0 \cdot \vec{y}_i^c, \ldots, a_{i,M} \cdot \vec{y}_M^c) \tag{12}$$

over continuous-time intervals, where $\vec{u}_i^c$ is the interconnection over a continuous-time interval. $[a_{i,1}, \ldots, a_{i,M}]$ is the ith row of $\mathbb{K}$. $g_i^c(\vec{y}_1^c, \ldots, \widehat{\vec{y}_i}^c, \ldots, \vec{y}_M^c)$s are assumed to be polynomial functions.

(v) $\mathbb{N}^d$ is a finite set of interconnections following discrete assignments

$$\vec{u}_i^d = g_i^d(a_{i,1} \cdot \vec{y}_1^d, \ldots, 0 \cdot \vec{y}_i^d, \ldots, a_{i,M} \cdot \vec{y}_M^d) \tag{13}$$

at discrete instants, where $\vec{u}_i^d$ is the interconnection at switching instant, and $[a_{i,1}, \ldots, a_{i,M}]$ is the ith row of $\mathbb{K}$. $g_i^d(\vec{y}_1^d, \ldots, \widehat{\vec{d}_i}^c, \ldots, \vec{d}_M^c)$s are assumed to be polynomial functions.

Intuitively, trajectory of $\mathbb{H}$ is the composition of trajectories of $\mathbb{H}_i$s under restrictions of the interconnections. We take $\phi_i(t_i, \vec{x}_i^0, \vec{x}_i, \vec{u}_i^c, \vec{u}_i^d, \vec{y}_i^c, \vec{y}_i^d)$ to represent the trajectory of $\mathbb{H}_i$; thus, the trajectory $\phi(t, \vec{x}^0, \vec{x}, \vec{u}^c, \vec{u}^d, \vec{y}^c, \vec{y}^d)$ of $\mathbb{H}$ is a Cartesian product satisfying the following.

Initiation. $\vec{x}^0 = \langle \vec{x}_1^0, \ldots, \vec{x}_M^0 \rangle \in \mathbb{X}^0$ for all $\vec{x}_i^0 \in \mathbb{X}_i^0$.

Discrete Consecution. For $\vec{x} \in \mathbb{G}$, at least one $\phi_i(t_i, \vec{x}_i^0, \vec{x}_i, \vec{u}_i^c, \vec{u}_i^d, \vec{y}_i^c, \vec{y}_i^d)$ would undergo a switching. Switchings of interconnected trajectories are not required to occur simultaneously under our framework. At each instant of discrete consecution, an impulsive interconnection occurs according to the following algebraic equations:

$$\begin{gathered}
\vec{u}_1^d = g_i^d(0 \cdot \vec{y}_1^d, \ldots, a_{1,i} \cdot \vec{y}_i^d, \ldots, a_{1,M} \cdot \vec{y}_M^d), \\
a_{1,1}, \ldots, a_{1,M} \in \{0, 1\} \\
\vdots \\
\vec{u}_M^d = g_i^d(a_{M,1} \cdot \vec{y}_1^d, \ldots, a_{M,i} \cdot \vec{y}_i^d, \ldots, 0 \cdot \vec{y}_M^d), \\
a_{M,1}, \ldots, a_{M,M} \in \{0, 1\}.
\end{gathered} \tag{14}$$

Continuous Consecution. For $\vec{x} \in \mathbb{C}$, states of all trajectories of $\mathbb{H}_i$ evolve continuously under the continuous interconnections according to the following differential equations:

$$\begin{gathered}
\vec{u}_1^c = g_i^c(0 \cdot \vec{y}_1^c, \ldots, a_{1,i} \cdot \vec{y}_i^c, \ldots, a_{1,M} \cdot \vec{y}_M^c), \\
a_{1,1}, \ldots, a_{1,M} \in \{0, 1\} \\
\vdots \\
\vec{u}_M^c = g_i^c(a_{M,1} \cdot \vec{y}_1^c, \ldots, a_{M,i} \cdot \vec{y}_i^c, \ldots, 0 \cdot \vec{y}_M^c), \\
a_{M,1}, \ldots, a_{M,M} \in \{0, 1\}.
\end{gathered} \tag{15}$$

For compositional hybrid I/O automata $\mathbb{H}$, $\vec{x} \in \mathbb{X}$ evolves continuously when all trajectories of $\mathbb{H}_i$s evolve continuously, while switchings occur once there exists a discrete consecution among $\mathbb{H}_i$s.

Based on the concept of trajectories of $\mathbb{H}$, safety of $\mathbb{H}$ could be formalized as follows.

Definition 10 (safety of $\mathbb{H}$). Let an interconnected hybrid I/O automaton $\mathbb{H} = \{\mathbb{I}, \bigcup_{i\in\mathbb{I}}\{\mathbb{H}_i\}, \mathbb{N}^c, \mathbb{N}^d, \mathbb{K}\}$ be given. Take $\phi(t, \vec{x}^0, \vec{x}, \vec{u}^c, \vec{u}^d, \vec{y}^c, \vec{y}^d)$ as the trajectory of $\mathbb{H}$; then $\mathbb{H}$ is unsafe if there exists an instant $t_i^\star \in [0, T]$ such that $\forall t \in [0, T]$: $\phi(t, \vec{x}^0, \vec{x}, \vec{u}^c, \vec{u}^d, \vec{y}^c, \vec{y}^d) \in \mathbb{X}$

$$\begin{gathered}
\exists \vec{u}^c : \phi(t^\star, \vec{x}^0, \vec{x}(t_i^\star), \vec{u}^c(t^\star)) \\
\in \mathbb{X}^u \cup \exists \vec{u}^d : \phi_i(t^\star, \vec{x}^0, \vec{x}(t_i^\star), \vec{u}^d(t^\star)) \in \mathbb{X}^u
\end{gathered} \tag{16}$$

holds. Furthermore, $\mathbb{H}$ is safe when none of the trajectories of $\mathbb{H}$ starting from admissible initial states would intersect unsafe states $\mathbb{X}^u$ of $\mathbb{H}$.

4. Compositional Barrier Certificates

In this section, we present a brief introduction to the barrier certificate method and propose the compositional barrier certificate for safety verification of compositional hybrid I/O automaton.

4.1. Intuitive Interpretation of Barrier Certificates. To address the safety verification, we need to determine whether a trajectory starting from admissible initial states would reach the set of unsafe states. Barrier certificate methodology could certify safety of a dynamical system through constructing a function called barrier certificate. Generally speaking, barrier certificate $B : \vec{X} \rightarrow \mathscr{R}$ ($\vec{X}$ denotes the state space) is a function of states satisfying a set of constraints on both the function itself and states evolution along the trajectories, and states $\vec{x} \in \vec{X}$ satisfying $B(\vec{x}) = 0$ form a barrier separating all unsafe states from possible system trajectories. $B(\vec{x})$ takes different values on different regions: for example, for each $\vec{x} \in X^u$ (X^u denotes unsafe states region), it satisfies $B(\vec{x} > 0)$, while for each $\vec{x} \in X^s$ (X^s denotes reachable states region of trajectories) $B(\vec{x} \leq 0)$ holds. Thus, system safety could be certified by the existence of a barrier certificate. An intuitive illustration of a barrier certificate is presented in Figure 1. As shown in the figure, unsafe states region is separated from states of trajectories by the barrier certificate.

4.2. Compositional Barrier Certificates. In the following, we present two lemmas to show sufficiency of the existence of barrier certificates for safety of individual hybrid I/O automaton and discuss how to impose inequality constraints on interconnections to construct compositional barrier certificates.

Lemma 11 (conservative barrier certificates for $\mathbb{H}_i$). *Let an interconnected individual hybrid I/O automaton $\mathbb{H}_i = \{\mathbb{X}_i, \mathbb{U}_i, \mathbb{Y}_i, \mathbb{S}_i, \mathbb{Q}_i, \mathbb{G}_i, \mathbb{F}_i, \mathbb{T}_i, \mathbb{X}_i^0, \mathbb{X}_i^u\}$ be given. For each $\vec{u}_i^c, \vec{u}_i^d \in \mathbb{U}_i$, suppose there exists a function $B_i(\vec{x}_i)$ for all m_i modes of $\mathbb{H}_i$. $B_i(\vec{x}_i)$ is piecewise differentiable with respect to its state variable and satisfies*

$$B_i(\vec{x}_i) > 0, \quad \forall \vec{x}_i \in \mathbb{X}_i^u, \tag{17}$$

$$B_i(\vec{x}_i) \leq 0, \quad \forall \vec{x}_i \in \mathbb{X}_i^0, \tag{18}$$

$$\begin{gathered} \frac{\partial B_i(\vec{x}_i)}{\partial \vec{x}_i} f_i^j(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \leq 0, \\ \forall \vec{x}_i \in \mathbb{X}_i \wedge B_i(\vec{x}_i) = 0, \end{gathered} \tag{19}$$

$$\begin{gathered} B_i(q_i^k) \leq B_i(q_i^j), \\ \forall \vec{x}_i \in \mathbb{G}_i, \ q_i^k \neq q_i^j, \ q_i^j, q_i^k \in \mathbb{Q}_i, \end{gathered} \tag{20}$$

where, for the case in (20), $\mathbb{H}_i$ undergoes a switching from mode q_i^j to mode q_i^k. If such $B_i(\vec{x}_i)$ exists, then the safety of $\mathbb{H}_i$ is guaranteed.

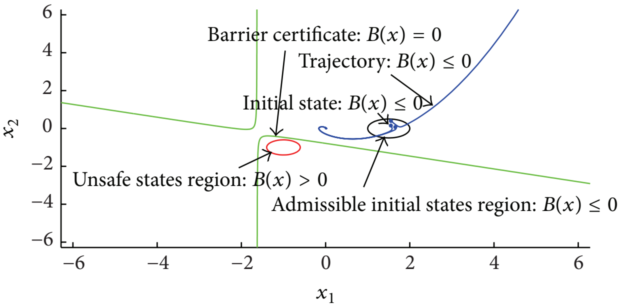


FIGURE 1: Intuitive interpretation of barrier certificates.

Proof (by contradiction). For each $\vec{u}_i^c$, assume that barrier certificates $B_i^j(\vec{x}_i)$ satisfying (17)–(20) can be found and suppose there exists an instant $t_i^\star \in [0, T]$ when $\vec{x}_i(t_i^\star) \in \mathbb{X}_i^u$. Suppose there exist two sequences of instants $0 = t_i^0 < t_i^1 < \cdots < t_i^{p_i} = t_i^\star$ and $0 = t^0 < t^1 < \cdots < t^p = t_i^\star$. $p_i, p \in \mathscr{N}_{>0}$ are either finite or infinite. At each $t_i^{p_i}$, mode $q_i^{p_i} \in \mathbb{Q}_i$ is activated, while, at each t^p, an impulsive interconnection rather than the continuous-time interconnection is activated. From (17), we derive $B_i^{q_i^{p_i}}(\vec{x}_i(t^\star)) > 0$. The impulsive interconnection $\vec{u}_i^d$ could be omitted considering

$$\sum_{l=1}^{p} \int_{t^l}^{t^l} \frac{\partial B_i(\vec{x}_i)}{\partial \vec{x}_i} f_i^j\left(t_i, \vec{x}_i(t_i), \vec{u}_i^d\right) = 0 \tag{21}$$

for any finite p. And from (20), it concludes that $B_i(\vec{x}_i)$ decreases at each switching. Over the continuous-time interval $[0, t_i^\star]$, we have

$$\begin{aligned} B_i(\vec{x}_i(t_i^\star)) &= B_i\left(\vec{x}_i\left(t_i^0\right)\right) \\ &\quad + \sum_{l=1}^{p_i} \int_{t_i^l}^{t_i^{l+1}} \frac{\partial B_i^j(\vec{x}_i)}{\partial \vec{x}_i} f_i^j(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \\ &\quad + \sum_{l=1}^{p} \left(\vec{u}_i^d\right)^T f_i^j(t_i, \vec{x}_i(t_i)) \\ &\quad + \sum_{l=1}^{p} \left(B_i(\vec{x}_i) - B_i^l(\vec{x}_i)\right) \\ &\leq B_i\left(\vec{x}_i\left(t_i^0\right)\right) \\ &\quad + \sum_{l=1}^{p_i} \int_{t_i^l}^{t_i^{l+1}} \frac{\partial B_i(\vec{x}_i)}{\partial \vec{x}_i} f_i^j(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \\ &\leq B_i\left(\vec{x}_i\left(t_i^0\right)\right) + \sum_{l=1}^{p_i} \ln B_i\left(\vec{x}_i\left(t_i^{l+1}\right)\right) \\ &\quad - \ln B_i\left(\vec{x}_i\left(t_i^l\right)\right) \leq B_i\left(\vec{x}_i\left(t_i^0\right)\right) \leq 0. \end{aligned} \tag{22}$$

Therefore, the derived $B_i(\vec{x}_i(t_i^\star)) \leq 0$ contradicts the assumption $B_i(\vec{x}_i(t_i^\star)) > 0$. Thus, we conclude that any trajectory starting from admissible initial states would not intersect unsafe states. In conclusion, the existence of barrier certificates $B_i(\vec{x}_i)$ is sufficient for safety of $\mathbb{H}_i$. □

Remark 12. Intuitively, the value of $B_i(\vec{x}_i)$ decreases along both continuous flows as well as switchings, since $B_i(\vec{x}_i^0) < 0$, all states of trajectories of $\mathbb{H}_i$ are negative, and reachable states would not intersect with the unsafe states region. It should be admitted that $B_i(\vec{x}_i)$ derived in Lemma 11 is conservative; however, for the safety of interconnected hybrid systems $\mathbb{H}$, this conservatism is justified.

For the convenience of expression, output as well as feedback $h_i^c(\vec{x}_i)$, $g_i^c(\vec{y}_1^c, \ldots, \vec{y}_M^c)$ is rewritten as

$$\begin{array}{c|c} h_i^c\left(\vec{x}_i\right) & g_i^c\left(\vec{y}_1^c, \ldots, \vec{y}_M^c\right) \\ \hline H_i = \begin{pmatrix} h_{1,1} & \cdots & h_{1,M_i} \\ \vdots & \ddots & \vdots \\ h_{M_i,1} & \cdots & h_{M_i,M} \end{pmatrix} \begin{pmatrix} x_{1,1_i} \\ \vdots \\ x_{M_i,1_i} \end{pmatrix} & G_i = \begin{pmatrix} g_{1,1} & \cdots & g_{1,M} \\ \vdots & \ddots & \vdots \\ g_{M,1} & \cdots & g_{M,M} \end{pmatrix} \begin{pmatrix} \vec{y}_1^c \\ \vdots \\ \vec{y}_M^c \end{pmatrix} \end{array}, \tag{23}$$

where $\vec{x}_i = [x_{1,1_i}, \ldots, x_{M_i,1_i}]^T$ ($x_{1,1_i}$ denotes the 1st-row, 1st-column element of vector $\vec{x}_i$) and $[\vec{y}_1^c, \ldots, \vec{y}_M^c]^T$ is a concatenation of vectors $\vec{y}_1^c, \ldots, \vec{y}_M^c$. Additionally, H_i, G_i are polynomial matrices; please distinguish them from the symbols $\mathbb{H}_i, \mathbb{G}_i$.

Lemma 13 (coupling constraints on interconnections). *Let an interconnected I/O automaton $\mathbb{H}$ be given. For each interconnected individual hybrid system $\mathbb{H}_i$, define $H = [H_1{}^T, \ldots, H_M{}^T]$ and $G = [G_1{}^T, \ldots, G_M{}^T]$, if there exists $\Gamma = \operatorname{diag}\{\gamma_1, \ldots, \gamma_M\} > 0^{M\times M}$ such that*

$$G \otimes I^{r\times r} \leq \Gamma H^T K^T K H \otimes I^{r\times r} \tag{24}$$

holds, where $\gamma_1, \ldots, \gamma_M \in \mathscr{R}_{>0}$. Then there exits $\vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c \leq 0$, $\forall i = 1, 2, \ldots, M$, satisfying

$$\frac{\partial B_i\left(\vec{x}_i\right)}{\partial \vec{x}_i} f_i^j\left(t_i, \vec{x}_i\left(t_i\right), \vec{u}_i^c\right) \leq \vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c, \qquad \forall \vec{x}_i \in \mathbb{X}_i \wedge B_i\left(\vec{x}_i\right) = 0 \tag{25}$$

for all $i \in \mathbb{I}$.

Proof. Since there exists $\Gamma = \operatorname{diag}\{\gamma_1, \ldots, \gamma_M\} > 0^{M\times M}$ with $\gamma_1, \ldots, \gamma_M \in \mathscr{R}_{>0}$ such that $G \otimes I^{r\times r} \leq \Gamma H^T K^T K H \otimes I^{r\times r}$, it could be verified that each column of $G \otimes I^{r\times r} \leq \Gamma H^T K^T K H \otimes I^{r\times r} = \vec{u}^{cT} \vec{y}^c - \Gamma \vec{y}^{cT} \vec{y}^c \leq 0$ through matrix computation; therefore, $\forall i \in \mathbb{I} : \vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c$ stands. Under constraint (19), the rest is proved by contradiction. Assume that, $\forall \gamma_i \in \mathscr{R}_{>0}$ satisfying (24), $(\partial B_i(\vec{x}_i)/\partial \vec{x}_i) f_i^j(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \geq \vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c$ holds; then take $\Gamma = (\vec{y}^c)^{-1} \vec{u}^{cT}$, and derive $(\partial B_i(\vec{x}_i)/\partial \vec{x}_i) f_i^j(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \geq 0$, which is contradiction to constraint (19). Therefore, Γ satisfying (24) is sufficient for $(\partial B_i(\vec{x}_i)/\partial \vec{x}_i) f_i^j(t_i, \vec{x}_i(t_i), \vec{u}_i^c) \leq \vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c, \forall \vec{x}_i \in \mathbb{X}_i \wedge B_i(\vec{x}_i) = 0$. □

Remark 14. Note that if inequality constraint (24) is satisfied, then Lie-derivative of $B_i(\vec{x}_i)$ is negative definite under the constraint of $\vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c$. Those constraints imposed on interconnections are enlightened by the dissipation inequalities, which guarantees the structural stability of interconnected hybrid systems. It should be noticed that such dissipation-inequality-like constraints are imposed on nondefinite barrier functions, while dissipation inequalities impose constraints on positive-definite energy functions.

Theorem 15 (compositional barrier certificate for $\mathbb{H}$). *Let an interconnected hybrid I/O automaton $\mathbb{H}$ be given. For each interconnected individual hybrid system $\mathbb{H}_i$, suppose that both $B_i(\vec{x}_i)$ satisfying constraints (17)–(20) in Lemma 11 and a vector $\Gamma = \operatorname{diag}\{\gamma_1, \ldots, \gamma_M\}$ satisfying (24) in Lemma 13 have been found, if there exists a diagonal matrix $D = \operatorname{diag}\{d_1, \ldots, d_M\} > 0^{M\times M}$ such that*

$$D\left(GK - \Gamma\right) + \left(KG - \Gamma\right)^T D \leq 0, \tag{26}$$

where $d_1, \ldots, d_M \in \mathscr{R}_{>0}$; then $\mathbb{H}$ is safe.

Proof. Since $B_i(\vec{x}_i)$s satisfying (17)–(20) and $\Gamma = \operatorname{diag}\{\gamma_1, \ldots, \gamma_M\}$ satisfying (24) exist, and there is a diagonal matrix $D = \operatorname{diag}\{d_1, \ldots, d_M\} > 0^{M\times M}$ satisfying (26), a compositional function $B(\vec{x})$ is built as

$$B\left(\vec{x}\right) = \sum_{i\in\mathbb{I}} \gamma_i B_i\left(\vec{x}_i\right). \tag{27}$$

Since we have $B_i(\vec{x}_i^0) < 0$, for $\vec{x} = \{\vec{x}_i^0\} \in \mathbb{X}^0$, it yields $B(\vec{x}) = \gamma_1 B_1(\vec{x}_1^0) + \cdots + \gamma_M B_M(\vec{x}_M^0) < 0$. Similarly, $\forall \vec{x} = \{\vec{x}_i^u\} \in \mathbb{X}^u : B(\vec{x}) \geq 0$ is derived. Through introducing (24) and (26), for all $\vec{x} \in \mathbb{X} - \mathbb{X}^u$, we derive

$$\begin{aligned} \frac{\partial B\left(\vec{x}\right)}{\partial \vec{x}} \vec{f}\left(t, \vec{x}\left(t\right), \vec{u}^c\right) &= \sum_{i\in\mathbb{I}} \frac{\partial B_i\left(\vec{x}_i\right)}{\partial \vec{x}_i} f_i\left(t_i, \vec{x}_i\left(t_i\right), \vec{u}_i^c\right) \\ &\leq \sum_{i\in\mathbb{I}} d_i \vec{u}_i^{cT} \vec{y}_i^c - \gamma_i \vec{y}_i^{cT} \vec{y}_i^c \\ &= \vec{y}_i^{cT} \left(D \otimes I^{M\times M}\right) \vec{u}_i^c - \vec{y}_i^{cT} \left(\left(D\Gamma\right) \otimes I^{M\times M}\right) \vec{y}_i^c \\ &= \vec{y}_i^{cT} \left(D \otimes I^{M\times M}\right) \left(KG \otimes I^{M\times M}\right) \vec{y}_i^c \\ &\quad - \vec{y}_i^{cT} \left(\left(D\Gamma\right) \otimes I^{M\times M}\right) \vec{y}_i^c \end{aligned}$$

$$\begin{aligned}&= \vec{y}_i^{cT} \left(D\left(GK-\Gamma\right) + \left(KG-\Gamma\right)^T D\right) \otimes I^{M\times M} \vec{y}_i^{c} \\ &\leq 0.\end{aligned} \tag{28}$$

Considering $\forall i \in \mathbb{I}\ \forall \vec{x}_l \in \mathbb{G}_i : B_i(q_i^k) \leq B_i(q_i^j)$, where $q_i^k \neq q_i^j$, $q_i^j, q_i^k \in \mathbb{Q}_i$, we derive $\sum_{l\in\mathbb{I}, l\neq i} \gamma_l B_l(\vec{x}_l) + B_i(q_i^k) \leq \sum_{l\in\mathbb{I}, l\neq i} \gamma_l B_l(\vec{x}_l) + B_i(q_i^j)$; equivalently, $B(\vec{x})$ is nonincreasing at mode switchings. Therefore, $B(\vec{x})$ is the barrier certificate for $\mathbb{H}$; furthermore, safety of $\mathbb{H}$ is guaranteed. □

Remark 16. On the assumption of existences of barrier certificates for each $\mathbb{H}_i$ and appropriate $D = \operatorname{diag}\{d_1, \ldots, d_M\} > 0^{M\times M}$, Lie-derivatives of each $B_i(\vec{x}_i)$ would be negative definite consistently. Then, $B(\vec{x})$ is negative definite along their trajectories of states under the restrictions of interconnections. Naturally, safety of $\mathbb{H}$ is guaranteed.

5. Computation of Barrier Certificates

In this section, we discuss how to construct compositional barrier certificates from the conditions set up in Section 4. Bilinear SOS programming is applied to support the computation of barrier certificates for $\mathbb{H}$. $\mathbb{H}$ is defined on semialgebraic sets with all vector fields that are restricted to be polynomial equality as well as inequality. Here, we parameterize the barrier certificates $B_i(\vec{x}_i)$s as polynomials and require the state space and initial, unsafe, and guard sets to be given by polynomial equality or inequality constraints. Through applying generalized S-procedure, constraints in the forms of semialgebraic sets could be incorporated into constraints (17)–(20); then Lemma 11 is formulated as a bilinear SOS program (feasibility problem). With the help of numerical solvers such as SOSTOOLS [21] and SOSOPT [22], those barrier certificates could be computed automatically.

5.1. Computation of Individual Barrier Certificates for $\mathbb{H}_i$s.

To compute individual barrier certificates, all the sets of states in (17)–(20) should be transformed into semialgebraic sets. Let $\mathbb{X}_i = \{\vec{x}_i : p_{\mathbb{X}_i}(\vec{x}_i) \geq 0\}$, $\mathbb{X}_i^0 = \{\vec{x}_i : p_{\mathbb{X}_i^0}(\vec{x}_i) \geq 0\}$, $\mathbb{X}_i^u = \{\vec{x}_i : p_{\mathbb{X}_i^u}(\vec{x}_i) \geq 0\}$, and $\mathbb{G}_i = \{\vec{x}_i : p_{\mathbb{G}_i}(\vec{x}_i) \geq 0\}$ be given as vectors of polynomials $p_{\mathbb{X}_i}(\vec{x}_i), p_{\mathbb{X}_i^0}(\vec{x}_i), p_{\mathbb{X}_i^u}(\vec{x}_i), p_{\mathbb{G}_i}(\vec{x}_i) \in \mathscr{P}_{n_i}$ in $\vec{x}_i$, where those inequalities are satisfied entry-wise. For example, when $\mathbb{X}$ is defined as $\{\vec{x}_i : \vec{x}_{\min} \leq \vec{x}_i \leq \vec{x}_{\max}\}$, it is equivalent to the semialgebraic set $\mathbb{X} = \{\vec{x}_i : p_{\mathbb{X}_i}(\vec{x}_i) = (\vec{x}_{\max} - \vec{x}_i)(\vec{x}_i - \vec{x}_{\min}) \geq 0\}$.

Generalized S-procedure is then introduced to corporate those semialgebraic sets constraints with (17)–(20) and Lemma 11 is formulated as a bilinear SOS program.

Lemma 17 (generalized S-procedure, see [24]). *Given functions $p_0(\vec{x}), p_1(\vec{x}), \ldots, p_m(\vec{x}) \in \mathscr{P}_n$, if there exist $s_1(\vec{x})$, $s_2(\vec{x}), \ldots, s_m(\vec{x}) \in \Sigma_n$ such that $p_0(\vec{x}) - \sum_{i=1}^m s_i(\vec{x}) p_i(\vec{x}) \in \Sigma_n$, then it holds that*

$$\begin{aligned}&\left\{\vec{x} \in \mathscr{R}^n : p_1(\vec{x}), \ldots, p_m(\vec{x}) \geq 0\right\} \\ &\quad \subseteq \left\{\vec{x} \in \mathscr{R}^n : p_0(\vec{x}) \geq 0\right\}.\end{aligned} \tag{29}$$

For more details on generalized S-procedure, please refer to [24].

Theorem 18 (barrier certificates as bilinear SOS program). *Let an interconnected hybrid I/O automaton $\mathbb{H}_i = \{\mathbb{X}_i, \mathbb{U}_i, \mathbb{Y}_i, \mathbb{S}_i, \mathbb{Q}_i, \mathbb{G}_i, \mathbb{F}_i, \mathbb{T}_i, \mathbb{X}_i^0, \mathbb{X}_i^u\}$ be given, and $\mathbb{X}_i, \mathbb{X}_i^0, \mathbb{X}_i^u, \mathbb{G}_i$ have been transformed into semialgebraic sets. The polynomial barrier certificate $B_i(\vec{x}_i)$ could be computed through solving the following bilinear SOS program:*

$$B_i(\vec{x}_i) - \epsilon_i - s_1(\vec{x}_i)(\vec{x})\, p_{\mathbb{X}_i^u}(\vec{x}_i) \in \Sigma_n, \tag{30}$$

$$-B_i(\vec{x}_i) - s_2(\vec{x}_i)(\vec{x}_i)\, p_{\mathbb{X}_i^0}(\vec{x}_i) \in \Sigma_n, \tag{31}$$

$$\begin{aligned}&-\frac{\partial B_i(\vec{x}_i)}{\partial \vec{x}_i} f_i^{q_i}\left(t_i, \vec{x}_i(t_i), \vec{u}_i^c\right) + s_3(\vec{x}_i)\, p_{\mathbb{G}_i}(\vec{x}_i) \\ &\quad + \lambda_i(\vec{x}_i) B_i(\vec{x}_i) \in \Sigma_n, \quad \forall q_i \in \mathbb{Q}_i,\end{aligned} \tag{32}$$

$$-\nu_i - s_4(\vec{x}_i)\, p_{\mathbb{G}_i}(\vec{x}_i) \in \Sigma_n, \tag{33}$$

where $\lambda_i(\vec{x}_i) \in \mathscr{P}_n$ is a polynomial decision variable, $\epsilon_i, \nu_i \in \mathscr{R}_{>0}$ are scalar decision variables, and $s_1(\vec{x}_i), s_2(\vec{x}_i), s_3(\vec{x}_i)$, $s_4(\vec{x}_i)$ are all SOS polynomial decision variables.

Proof. Notice that there exists a coupling between the polynomial decision variables $\lambda_i(\vec{x}_i)$ and $B_i(\vec{x}_i)$, and this programming problem is bilinear. Here is the sketch of a proof. Since $\mathbb{X}_i^u = \{\vec{x}_i : p_{\mathbb{X}_i^u}(\vec{x}_i) \geq 0\}$, and $\forall \vec{x}_i \in \mathbb{X}_i^u : B_i(\vec{x}_i) \geq 0$, the positive definiteness could be guaranteed by $B_i(\vec{x}_i) - \epsilon_i - s_1(\vec{x}_i)(\vec{x}) p_{\mathbb{X}_i^u}(\vec{x}_i) \in \Sigma_n$ by applying generalized S-procedure. Similarly, (31)–(33) could be derived. Scalar ν_i decision variable introduced in (33) is for the switching. Therefore, $B_i(\vec{x}_i)$ derived by solving the bilinear SOS program satisfying (30)–(33) is a barrier certificate for $\mathbb{H}_i$. □

Remark 19. Loosely speaking, generalized S-procedure is for determining satisfaction of an inequality constraint $p_0(\vec{x}) \geq 0$ when other inequality constraints $p_1(\vec{x}) \geq 0, \ldots, p_m(\vec{x}) \geq 0$ are fulfilled. Through applying generalized S-procedure, the above theorem formulates inequalities (30)–(33) together as a bilinear SOS program computationally tractable for the feasibility of barrier certificates constrained by (17)–(20).

5.2. Computation of Compositional Barrier Certificate for $\mathbb{H}$.

In order to derive the compositional barrier certificate for $\mathbb{H}$, Γ should be estimated first by solving the following optimization problem:

$$\begin{aligned}\text{Min}\quad & \Gamma = \operatorname{diag}\left\{\gamma_1, \ldots, \gamma_M\right\} \\ \text{s.t.}\quad & G \otimes I^{r\times r} \leq \Gamma H^T K^T K H \otimes I^{r\times r} \\ & \Gamma > 0^{M\times M}.\end{aligned} \tag{34}$$

The above optimization is a linear program problem which could be solved with the help of linear programming solvers. With derived Γ, compositional barrier certificates for $\mathbb{H}$ could be computed directly by solving a bilinear SOS program.

Theorem 20 (compositional barrier certificate for $\mathbb{H}$ as bilinear SOS program). *Let an interconnected hybrid I/O automaton $\mathbb{H}$ be given. For each interconnected $\mathbb{H}_i$, there exists an individual barrier certificate $B_i(\vec{x}_i)$; then, the compositional barrier certificate $B(\vec{x})$ could be computed through solving the following bilinear SOS program:*

$$\begin{aligned}
\text{Min}\quad & D = \operatorname{diag}\{d_1, \ldots, d_m\} && (35)\\
\text{s.t.}\quad & -DB(\vec{x}) - s_1(\vec{x})\left(p_{\mathbb{X}^s}(\vec{x})\right) \in \Sigma_{n\times m_i} && (36)\\
& D - \epsilon - s_2(\vec{x})\left(p_{\mathbb{X}^u}(\vec{x})\right) \in \Sigma_{n\times m_i} && (37)\\
& -H^T\left(\left(D\otimes I^{r\times r}\right)\left(KG\otimes I^{r\times r}\right) + \left(KG\otimes I^{r\times r}\right)^T\left(D\otimes I^{r\times r}\right)\right)H - 1_m^T D\left(-\Gamma H^2\right) + p(\vec{x})\,DB(\vec{x}) \in \Sigma_{n\times m_i} && (38)\\
& D > 0^{m\times m}, && (39)
\end{aligned}$$

where $B(\vec{x}) = [B_1(\vec{x}_1), \ldots, B_m(\vec{x}_m)]^T$, $p_{\mathbb{X}^s}(\vec{x}) = [p_{\mathbb{X}_1^s}(\vec{x}_1), \ldots, p_{\mathbb{X}_m^s}(\vec{x}_m)]^T$, $p_{\mathbb{X}^u}(\vec{x}) = [p_{\mathbb{X}_1^u}(\vec{x}_1), \ldots, p_{\mathbb{X}_m^u}(\vec{x}_m)]^T$ ($\forall i \in \mathbb{I}$: $p_{\mathbb{X}_i^s}(\vec{x}_i) = p_{\mathbb{X}_i}(\vec{x}_i) - p_{\mathbb{X}_i^u}(\vec{x}_i)$). D is a scalar matrix decision variable, $\epsilon = [\epsilon_1, \ldots, \epsilon_m]$ is a scalar vectorial decision variable, $s_1(\vec{x}), s_2(\vec{x})$ are SOS polynomials decision variables, and $p(\vec{x})$ is a polynomial decision variable.

Proof. Here is the sketch of a proof. As indicated in the above theorem, $B_1(\vec{x}_1), \ldots, B_m(\vec{x}_m)$ are barrier certificates for $\mathbb{H}_i$s. Constraints (36) and (37) imply that $B(\vec{x})$ is nonpositive on $\mathbb{X}^u$ and positive on $\mathbb{X}^s = \mathbb{X} - \mathbb{X}^u$. Constraints (38) and (39) imply that

$$\begin{aligned}
& -H^T\left(\left(D\otimes I^{r\times r}\right)\left(KG\otimes I^{r\times r}\right)\right.\\
&\quad \left.+ \left(KG\otimes I^{r\times r}\right)^T\left(D\otimes I^{r\times r}\right)\right)H + 1_m^T D\left(H^T\Gamma H\right)\\
&\quad \geq 0 \Longrightarrow\\
& H^T\left(GKD + (DKG)^T\right)H - 1_m^T D\left(H^T\Gamma H\right) \leq 0 \Longrightarrow\\
& H^T\left(GKD + (DKG)^T\right)H - H^T D^T \Gamma D H \leq 0 \Longrightarrow\\
& D(GK - \Gamma) + (KG - \Gamma)^T D \leq 0.
\end{aligned} \tag{40}$$

In conclusion, the derived $B(\vec{x})$ satisfies Theorem 15, and $B(\vec{x})$ is the compositional barrier certificate for $\mathbb{H}$; thus, $\mathbb{H}$ is safe. □

Remark 21. Since $p(\vec{x})$ is coupled with D, the above programming problem satisfying (36)–(39) is a bilinear SOS program. Theorem 20 then formulates the construction of a compositional barrier certificate as a feasibility problem in bilinear SOS problem. It should be noted that compositional barrier certificates derived by Theorem 20 are more conservative than that by Theorem 15; however, Theorem 20 provides a theoretically tractable method to construct compositional barrier certificates. Numerical solvers such as SOSTOOLS or SOSOPT for MATLAB could be used for solving bilinear SOS program automatically. More details on the issues of numerical computation are omitted; we strongly suggest that readers refer to [21] or [22].

6. Example

In this example, we consider the following interconnected hybrid systems $\mathbb{H}$ consisting of two coupled hybrid systems $\mathbb{H}_1, \mathbb{H}_2$:

$$\begin{aligned}
& \mathbb{H}_1\colon \dot{\vec{x}}_1 = A\vec{x}_1 + \vec{k}_1\vec{x}_2, \quad \vec{x}_1 = \left[x_{11}, x_{12}\right]^T\\
& \vec{x}_1^0 = \left\{\vec{x}_1 : \left(4 - x_{11}\right)\left(x_{11} + 4\right) \geq 0, \left(4 - x_{12}\right)\left(x_{12} + 4\right)\right.\\
&\quad \left.\geq 0\right\},\\
& \vec{x}_1^u = \left\{\vec{x}_1 : \left(10 - x_{11}\right)\left(x_{11} + 10\right)\right.\\
&\quad \left.\geq 0, \left(10 - x_{12}\right)\left(x_{12} + 10\right) \geq 0\right\},\\
& x_{11}x_{12} < 0 : A_1 = \begin{pmatrix} 0.1 & -1 \\ 2 & 0.1 \end{pmatrix},\\
& x_{11}x_{12} \geq 0 : A_2 = \begin{pmatrix} 0.1 & -2 \\ 1 & 0.1 \end{pmatrix}\\
& \vec{k}_1 = \begin{pmatrix} -2 & 0 \\ -3 & -4 \end{pmatrix}\\
& \mathbb{H}_2\colon \dot{\vec{x}}_2 = B\vec{x}_2 + \vec{k}_2\vec{x}_1, \quad \vec{x}_2 = \left[x_{21}, x_{22}\right]^T\\
& \vec{x}_2^0 = \left\{\vec{x}_2 : \left(4 - x_{21}\right)\left(x_{21} + 4\right) \geq 0, \left(4 - x_{22}\right)\left(x_{22} + 4\right)\right.\\
&\quad \left.\geq 0\right\},\\
& \vec{x}_2^u = \left\{\vec{x}_2 : \left(10 - x_{21}\right)\left(x_{21} + 10\right)\right.\\
&\quad \left.\geq 0, \left(10 - x_{22}\right)\left(x_{22} + 10\right) \geq 0\right\},\\
& x_{21}x_{22} < 0 : B_1 = \begin{pmatrix} -5 & -4 \\ -1 & -2 \end{pmatrix},\\
& x_{21}x_{22} \geq 0 : B_2 = \begin{pmatrix} -2 & -4 \\ 20 & -2 \end{pmatrix}\\
& \vec{k}_2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},
\end{aligned} \tag{41}$$

where $\vec{x}_1^0, \vec{x}_2^0$ are admissible initial states, $\vec{x}_1^u, \vec{x}_2^u$ are unsafe states, and inequalities $x_{11}x_{12} < 0$, $x_{11}x_{12} \geq 0$, $x_{21}x_{22} < 0$, and $x_{21}x_{22} \geq 0$ are switching conditions. A_1, A_2 and B_1, B_2 are modes of $\mathbb{H}_1$ and $\mathbb{H}_2$, respectively. $\vec{k}_1, \vec{k}_2$ are interconnection matrices. The derived barrier certificate is $-0.01x_{11}^3 - 1.88x_{11}^2x_{12} - 0.3x_{11}^2x_{21} - 476.42x_{11}^2 + 5.77x_{11}x_{12}^2 - 0.03x_{11}x_{12}x_{21} - 0.03x_{11}x_{12}x_{22} + 77.25x_{11}x_{12} - 16.43x_{11}x_{21}^2 + 0.03x_{11}x_{21}x_{22} + 475.47x_{11}x_{21} - 0.03x_{11}x_{22}^2 + 0.5x_{11}x_{22} - 0.51x_{11} - 0.01x_{12}^3 + 0.02x_{12}^2x_{21} - 0.42x_{12}^2x_{22} - 154.77x_{12}^2 + 11.13x_{12}x_{21}^2 + 0.01x_{12}x_{21}x_{22} + 254.32x_{12}x_{21} - 2.1x_{12}x_{22}^2 + 102x_{12}x_{22} + 1.12x_{12} + 1.85x_{21}^2x_{22} + 191.09x_{21}^2 + 1.95x_{21}x_{22}^2 - 27.16x_{21}x_{22} + 1.21x_{21} - 0.01x_{22}^3 - 65.95x_{22}^2 + 1.48x_{22} - 1847.27$. The software environment to test our method consists of SOSTOOLS and SeDuMi on MATLAB (R2013b) and monomials whose coefficients less than 0.01 are omitted. Since the barrier certificate exists, safety of $\mathbb{H}$ is verified.

7. Conclusion

In this paper, we have considered a network of interconnected hybrid systems with a safety constraint. We proposed a numerical method for verifying safety by constructing a compositional barrier certificate comprised of individual barrier certificates for each subsystem. The constructed compositional barrier function certifies global safety using individual barrier certificates and diagonal stability property of the network interconnection. Such a compositional barrier certificate is then formulated into a bilinear SOS program that is computationally tractable. With the help of numerical solvers such as SOSTOOLS and SOSOPT, safety verification of interconnected hybrid systems could be automatically accomplished. In the end, a numerical example is presented to show the validity of the proposed method.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The work is partially supported by the projects funded by the NSFC Key Project 61332008, NSFC Creative Team 61321064, NSFC 61572195. The Shanghai Trustworthy Computing Key Lab is supported by Shanghai Knowledge Service Platform ZF 1213. Jing Liu would like to acknowledge the support of NSFC 91418203 and Shanghai Project (14511100400), NSFC Trustworthy Software Track 91318301. Miaomiao Zhang would like to acknowledge the support of NSFC 61472279.

References

[1] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems: Computation and Control: 7th International Workshop, HSCC 2004, Philadelphia, PA, USA, March 25–27, 2004. Proceedings*, vol. 2993 of *Lecture Notes in Computer Science*, pp. 477–492, Springer, Berlin, Germany, 2004.

[2] H. Guéguen, M.-A. Lefebvre, J. Zaytoon, and O. Nasri, "Safety verification and reachability analysis for hybrid systems," *Annual Reviews in Control*, vol. 33, no. 1, pp. 25–36, 2009.

[3] M. Anghel, F. Milano, and A. Papachristodoulou, "Algorithmic construction of Lyapunov functions for power system stability analysis," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 60, no. 9, pp. 2533–2546, 2013.

[4] A. Y. Sendjaja and V. Kariwala, "Achievable PID performance using sums of squares programming," *Journal of Process Control*, vol. 19, no. 6, pp. 1061–1065, 2009.

[5] S. Sankaranarayanan, H. B. Sipma, and Z. Manna, "Constructing invariants for hybrid systems," *Formal Methods in System Design*, vol. 32, no. 1, pp. 25–55, 2008.

[6] 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 (HSCC '10)*, pp. 221–230, Stockholm, Sweden, April 2010.

[7] E. Rodríguez-Carbonell and A. Tiwari, "Generating polynomial invariants for hybrid systems," in *Hybrid Systems: Computation and Control: 8th International Workshop, HSCC 2005, Zurich, Switzerland, March 9–11, 2005. Proceedings*, vol. 3414 of *Lecture Notes in Computer Science*, pp. 590–605, Springer, Berlin, Germany, 2005.

[8] P. A. Parrilo, *Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization [Ph.D. thesis]*, California Institute of Technology, 2000.

[9] S. Prajna and A. Papachristodoulou, "Analysis of switched and hybrid systems-beyond piecewise quadratic methods," in *Proceedings of the American Control Conference (ACC '03)*, vol. 4, pp. 2779–2784, IEEE, Denver, Colo, USA, June 2003.

[10] A. Papachristodoulou, "Analysis of nonlinear time-delay systems using the sum of squares decomposition," in *Proceedings of the American Control Conference (ACC '04)*, vol. 5, pp. 4153–4158, IEEE, Boston, Mass, USA, July 2004.

[11] A. Papachristodoulou, M. M. Peet, and S. Lall, "Analysis of polynomial systems with time delays via the sum of squares decomposition," *IEEE Transactions on Automatic Control*, vol. 54, no. 5, pp. 1058–1064, 2009.

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

[13] C. Sloth, G. J. Pappas, and R. Wisniewski, "Compositional safety analysis using barrier certificates," in *Proceedings of the 15th ACM international conference on Hybrid Systems: Computation and Control (HSCC '12)*, pp. 15–24, Beijing, China, April 2012.

[14] C. Sloth, R. Wisniewski, and G. J. Pappas, "On the existence of compositional barrier certificates," in *Proceedings of the 51st IEEE Conference on Decision and Control (CDC '12)*, pp. 4580–4585, Maui, Hawaii, USA, December 2012.

[15] H. Kong, X. Song, D. Han, M. Gu, and J. Sun, "A new barrier certificate for safety verification of hybrid systems," *The Computer Journal*, vol. 57, no. 7, pp. 1033–1045, 2014.

[16] R. Wisniewski and C. Sloth, "Converse barrier certificate theorem," in *Proceedings of the IEEE 52nd Annual Conference on Decision and Control (CDC '13)*, pp. 4713–4718, IEEE, Firenze, Italy, December 2013.

[17] R. Alur, "Formal verification of hybrid systems," in *Proceedings of the International Conference on Embedded Software (EMSOFT '11)*, pp. 273–278, IEEE, 2011.

[18] S. Coogan and M. Arcak, “Verifying safety of interconnected passive systems using SOS programming,” in *Proceedings of the 52nd IEEE Conference on Decision and Control (CDC ’13)*, pp. 5951–5956, Firenze, Italy, December 2013.

[19] S. Coogan and M. Arcak, “A dissipativity approach to safety verification for interconnected systems,” *Institute of Electrical and Electronics Engineers. Transactions on Automatic Control*, vol. 60, no. 6, pp. 1722–1727, 2015.

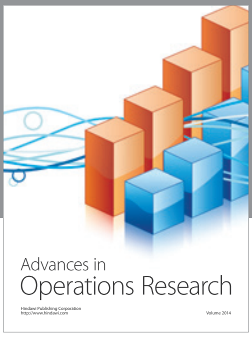
[20] G. H. Hines, M. Arcak, and A. K. Packard, “Equilibrium-independent passivity: a new definition and numerical certification,” *Automatica*, vol. 47, no. 9, pp. 1949–1956, 2011.

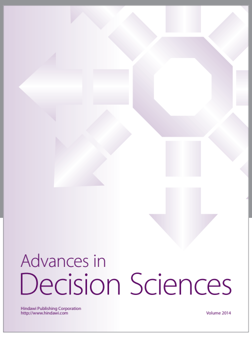
[21] A. Papachristodoulou, J. Anderson, G. Valmorbida, S. Prajna, P. Seiler, and P. Parrilo, “SOSTOOLS version 3.00 sum of squares optimization toolbox for MATLAB,” http://arxiv.org/abs/1310.4716.

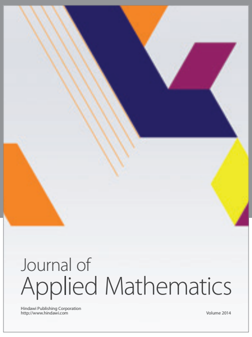
[22] P. Seiler, “Sosopt: a toolbox for polynomial optimization,” http://arxiv.org/abs/1308.1889.

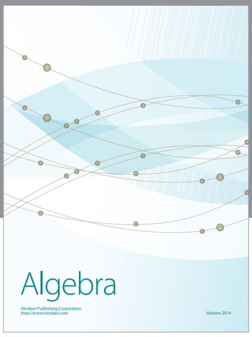
[23] N. Lynch, R. Segala, and F. Vaandrager, “Hybrid I/O automata,” *Information and Computation*, vol. 185, no. 1, pp. 105–157, 2003.

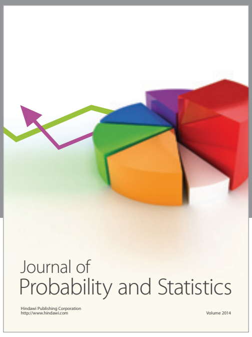
[24] Z. Jarvis-Wloszek, R. Feeley, W. Tan, K. Sun, and A. Packard, “Control applications of sum of squares programming,” in *Positive Polynomials in Control*, vol. 312, pp. 3–22, Springer, Berlin, Germany, 2005.


Advances in
Operations Research

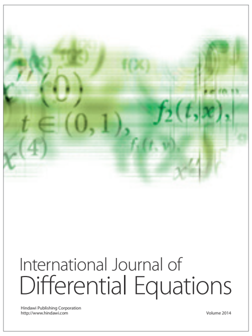

Advances in
Decision Sciences


Journal of
Applied Mathematics

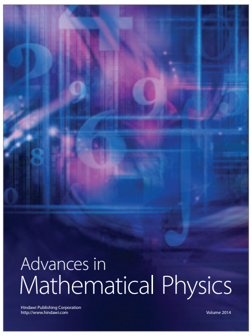

Algebra

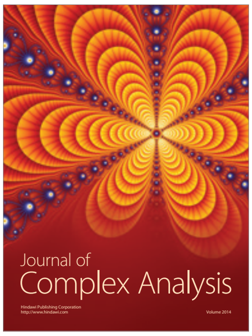

Journal of
Probability and Statistics

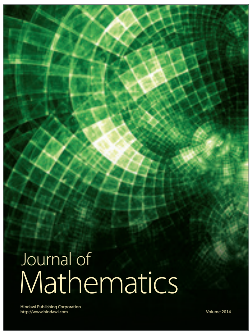
The Scientific
World Journal

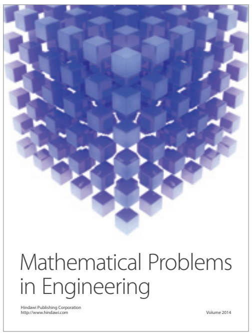

International Journal of
Differential Equations

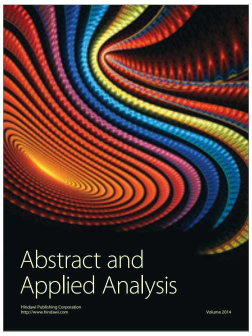
International Journal of
Combinatorics

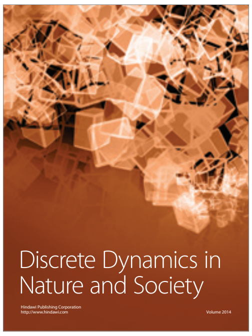

Advances in
Mathematical Physics

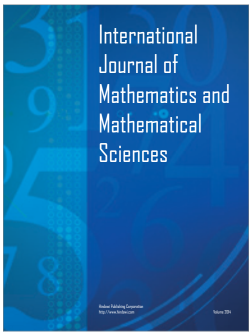

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

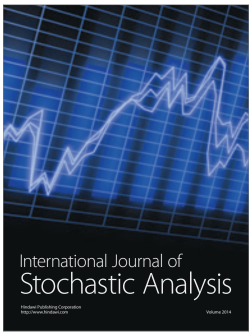

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization