[13] Gillespie, D.T., "Exact Stochastic Simulation of Coupled Chemical Reactions", Journal of Physical Chemistry, 81:2340-2361, 1977.
[14] Kurtz, G.T., "Approximation of Discontinuous Processes by Continuous Processes", in L. Arnold and R. Lefever, eds., Stochastic Nonlinear Systems in Physics, Chemistry and Biology, Springer-Verlag, Berlin, 1981
[15] He, J., Zhang, H., Chen, J., and Y. Yang, Macromolecules **30**, 8010, 1997.
[16] Rao, C., and A. Arkin, Journal Chem. Phys. *submitted*.
[17] Janssen, J.A.M., Journal of Statistical Physics, **57**, 171, 1989.
[18] Vlad, M.O., and A. Pop, Physica A **155**, 276, 1989.
[19] Gillespie, D.T., Physica A **188**, 404, 1992.
[20] Resat, H, H.S. Wiley, and D.A. Dixon, Journal of Physical Chemistry B **105**, 11026, 2001.
[21] Idaker, T., Science, 2001.
[22] Ostergaard, S., National Biotechnical Journal, 2000.
[23] Gardner, T.J., Cantor, C.R, Collins, J.J., Construction of a Genetic Toggle Switch in Escherichia Coli, Nature, 2000.403.339-342.
[24] Goss & Peccoud, Proc. Nat. Acad. Sci., 1998.

Safety Verification of Hybrid Systems Using Barrier Certificates

Stephen Prajna[1⋆] and Ali Jadbabaie[2]

[1] Control and Dynamical Systems, California Institute of Technology, Pasadena, CA 91125 - USA,
prajna@cds.caltech.edu
[2] Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104 - USA,
jadbabai@seas.upenn.edu

Abstract. This paper presents a novel methodology for safety verification of hybrid systems. For proving that all trajectories of a hybrid system do not enter an unsafe region, the proposed method uses a function of state termed a barrier certificate. The zero level set of a barrier certificate separates the unsafe region from all possible trajectories starting from a given set of initial conditions, hence providing an exact proof of system safety. No explicit computation of reachable sets is required in the construction of barrier certificates, which makes nonlinearity, uncertainty, and constraints can be handled directly within this framework. The method is also computationally tractable, since barrier certificates can be constructed using the sum of squares decomposition and semidefinite programming. Some examples are provided to illustrate the use of the method.

1 Introduction

Much research effort has been devoted to the development of hybrid systems theory in the recent years. This is partly due to the ubiquity of engineering and physical systems that are best modelled as hybrid systems. One important example is the class of embedded systems [16], whose dynamics involve interaction between digital control software and analog plants via sensors and actuators.

Complex behaviors that can be exhibited by hybrid systems make the safety verification of such systems both critical and challenging. In principle, safety verification or reachability analysis aims to show that starting at some initial conditions, a system cannot evolve to some unsafe region in the state space. Verification of purely discrete systems using temporal logic [10] as well as verification of continuous systems within the framework of robust control theory [26] are mature areas with many success stories. Unfortunately, neither of them is adequate for handling hybrid systems.

⋆ The work of the first author was supported by funding from AFOSR.

R. Alur and G.J. Pappas (Eds.): HSCC 2004, LNCS 2993, pp. 477–492, 2004.

For verification of hybrid systems, several methods have since been proposed. Explicit computation of either exact or approximate reachable sets corresponding to the continuous dynamics is crucial for virtually all of these methods. For linear systems with certain eigenstructures and semialgebraic initial sets, exact reachability set calculation using quantifier elimination has been addressed in [14,3]. It has been extended to approximate analysis of linear systems with almost arbitrary eigenstructures in [22]. Recently, a scalable method based on geometric programming relaxations has been proposed by [25] for linear systems with polytopic sets. In another vein, several other techniques have also been developed for approximate reachability analysis. Such techniques rely on numerical methods for solving the Hamilton Jacobi equations [23], ellipsoidal calculus [13, 6], flow-pipe approximations [9], and polygonal approximations [5,4,2].

In this paper, we present a new method for safety verification that is different from the above approaches as it does not require computation of reachable sets, but instead relies on what we term barrier certificates, which were previously used in the context of nonlinear model validation [19]. For a continuous system, a barrier certificate is a function of state satisfying a set of inequalities on both the function itself and its time derivative along the flow of the system (cf. Theorem 1). In the state space, the zero level set of a barrier certificate separates an unsafe region from all system trajectories starting from a given set of initial conditions, and therefore the existence of such a function provides an exact certificate/proof of system safety. Similar to the Lyapunov stability results, the main idea is to study properties of the system (reachability in this case) without the need to compute the flow explicitly. Although an over-approximation of the reachable set may also be a witness for safety, a barrier certificate can be much easier to compute when the system is nonlinear and uncertain, and the latter is notably more exact when the safety is to be verified for infinite time horizon.

The method described in the previous paragraph can be easily extended to handle hybrid systems. In this case, a barrier certificate is constructed from a set of functions of continuous state indexed by the system location. Instead of satisfying the aforementioned inequalities in the whole continuous state space, each function needs to satisfy the inequalities only within the invariant set of its location. Functions corresponding to different locations are linked via appropriate conditions that must be satisfied during discrete transitions between the locations. The idea here is again analogous to using multiple Lyapunov-like functions [8,11] for stability analysis of hybrid systems.

With this methodology, we are able to treat a large class of hybrid systems, including those with nonlinear continuous dynamics, uncertain inputs, uncertain parameters, and constraints (even dynamic constraints such as integral quadratic constraints [15], a tool of robust control which can be used to represent e.g. unmodelled system dynamics). When the vector fields of the system are polynomials and the sets in the system description are semialgebraic (i.e., described by polynomial equalities and inequalities), a tractable computational method using the sum of squares decomposition [18] and semidefinite programming [24] can be utilized for constructing a polynomial barrier certificate, e.g., using the software [20]. While the computational cost of this construction depends on the

degrees of the vector fields and the barrier certificate in addition to the dimension of the continuous state, for fixed degrees the complexity grows polynomially with respect to the state dimension. Hence we expect our method to be more scalable than many other existing methods.

This paper is organized as follows. Section 2 describes the hybrid modelling framework that we use in this paper. In Section 3, safety verification of continuous and hybrid systems using barrier certificates is addressed. We present two sets of convex and non-convex conditions for barrier certificates, either of which guarantees the safety of the system. Later in the same section we incorporate constraints, in particular integral constraints, into the framework. In Section 4, we first show how a barrier certificate satisfying the convex conditions can be computed by convex optimization, and then we present an iterative scheme for handling the non-convex conditions, which potentially yield a less conservative barrier certificate. Section 5 contains detailed examples illustrating the use of the methodology. Finally, we end the paper by conclusions in Section 6.

2 Preliminaries

Throughout the paper, we adopt the hybrid modelling framework that was first proposed in [1]; see also [2] for a more detailed explanation and example. A hybrid system is a tuple $H = (\mathcal{X}, L, X_0, I, F, T)$ with the following components:

- $\mathcal{X} \subseteq \mathbb{R}^n$ is the continuous state space.
- L is a finite set of locations. The overall state space of the system is $X = L \times \mathcal{X}$, and a state of the system is denoted by $(l, x) \in L \times \mathcal{X}$.
- $X_0 \subseteq X$ is the set of initial states.
- $I : L \to 2^{\mathcal{X}}$ is the invariant, which assigns to each location l an invariant set $I(l) \subseteq \mathcal{X}$ that contains all possible continuous states while at location l.
- $F : X \to 2^{\mathbb{R}^n}$ is a set of vector fields. F assigns to each $(l, x) \in X$ a set $F(l, x) \subseteq \mathbb{R}^n$ which constrains the evolution of the continuous state according to the differential inclusion $\dot{x} \in F(l, x)$.
- $T \subseteq X \times X$ is a relation capturing discrete transitions between two locations. Here a transition $((l, x), (l', x')) \in T$ indicates that from the state (l, x) the system can undergo a discrete jump to the state (l', x').

Trajectories of the hybrid system H start from some initial state $(l_0, x_0) \in X_0$ and are concatenations of a sequence of continuous flows and discrete transitions. During a continuous flow, the discrete location l is maintained and the continuous state evolves according to the differential inclusion $\dot{x} \in F(l, x)$, as long as x remains inside the invariant set $I(l)$. At a state (l_1, x_1), a discrete transition to (l_2, x_2) can occur if $((l_1, x_1), (l_2, x_2)) \in T$. Given a hybrid system H and a set of unsafe states $X_u \subseteq X$, the safety verification problem is concerned with proving that all trajectories of the hybrid system H cannot enter the unsafe region X_u.

For computational purposes, we will assume that the uncertainty in the continuous flow is caused by some disturbance inputs in the following manner:

$$F(l, x) = \{\dot{x} \in \mathbb{R}^n : \dot{x} = f_l(x, d), \text{ for some } d \in D(l)\},$$

where $f_l(x,d)$ is a vector field that governs the flow of the system at location l, and d is a vector of disturbance inputs that takes value in the set $D(l) \subset \mathbb{R}^m$. In addition, for each location $l \in L$, we define the set of initial and unsafe continuous states as $\text{Init}(l) = \{x \in \mathcal{X} : (l,x) \in X_0\}$ and $\text{Unsafe}(l) = \{x \in \mathcal{X} : (l,x) \in X_u\}$. To each tuple $(l,l') \in L \times L$ with $l \neq l'$, we associate a guard set $\text{Guard}(l,l') = \{x \in \mathcal{X} : ((l,x),(l',x')) \in T \text{ for some } x' \in \mathcal{X}\}$, and a (possibly set valued) reset map $\text{Reset}(l,l') : x \mapsto \{x' \in \mathcal{X} : ((l,x),(l',x')) \in T\}$, whose domain is $\text{Guard}(l,l')$. Obviously, if no discrete transition from location l to location l' is possible, then the set $\text{Guard}(l,l')$ will be regarded as empty, and the associated reset map needs not be defined.

Although not explicitly stated, it is assumed that the description of the hybrid system given above is well-posed. For example, $(l,x) \in X_0$ automatically implies that $x \in I(l)$, and $((l,x),(l',x')) \in T$ implies that $x \in I(l)$ and $x' \in I(l')$.

3 Safety Verification Using Barrier Certificates

3.1 Continuous Systems

In this subsection we address the safety verification of continuous systems, to establish a foundation for the subsequent results. Consider a continuous system

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

where $x \in \mathcal{X}$ is the state of the system, and $d \in D$ is a collection of uncertain disturbance inputs. We assume that the system trajectories start at $x(0) \in \mathcal{X}_0$. Analogous to the notation described in Section 2, the unsafe region here is denoted by $\mathcal{X}_u$.

Our method for verifying safety relies on the existence of barrier certificates [19]. As mentioned in the introduction, a barrier certificate is a function of state satisfying some conditions on both the function itself and its time derivative along the flow of the system. It proves that a given system is safe by depicting a 'barrier' between possible system trajectories and the given unsafe region (cf. Section 5.1 for a visual illustration). In achieving this, no explicit computation of system flows nor reachable sets is required. The following theorem states the conditions that must be satisfied by a barrier certificate.

Theorem 1. *Let the system (1) and the sets $\mathcal{X}$, D, $\mathcal{X}_0$ and $\mathcal{X}_u$ be given. Suppose there exists a barrier certificate, namely a function $B : \mathcal{X} \to \mathbb{R}$ that is differentiable with respect to its argument and satisfies the following conditions:*

$$B(x) > 0 \quad \forall (x) \in \mathcal{X}_u, \tag{2}$$

$$B(x) \leq 0 \quad \forall (x) \in \mathcal{X}_0, \tag{3}$$

$$\frac{\partial B}{\partial x}(x) f(x,d) \leq 0 \quad \forall (x,d) \in \mathcal{X} \times D \text{ such that } B(x) = 0, \tag{4}$$

then the safety of the system (1) is guaranteed. That is, there exists no trajectory of the system (1) contained in $\mathcal{X}$ that starts from an initial state in $\mathcal{X}_0$ and reaches another state in $\mathcal{X}_u$.

Proof. Assume that a barrier certificate satisfying the above conditions can be found. Take any trajectory $x(t)$ in $\mathcal{X}$ that starts at some $x_0 \in \mathcal{X}_0$ and consider the evolution of $B(x(t))$ along this trajectory. Condition (3) asserts that $B(x_0) \leq 0$. Together with (4) this implies that along the flow of the system $B(x(t))$ cannot become positive. Consequently, any such trajectory can never reach an unsafe state $x_u \in \mathcal{X}_u$, whose $B(x_u)$ is positive according to (2). We conclude that the safety of the system is guaranteed.

In the above theorem we have assumed that the unknown disturbance input can vary arbitrarily fast. If it is known that the variation of the disturbance input is bounded (e.g. when there are uncertain parameters, which can be regarded as time-invariant disturbance), then a less conservative verification can be performed by considering a barrier certificate $B(x, d)$ that also depends on the instantaneous value of the disturbance and modifying (2)–(4) accordingly. For example, in condition (4) we need to take into account the extra derivative term $\frac{\partial B}{\partial d}(x, d)\dot{d}$, with $\dot{d}$ taking its value in some bounded set.

At this point, we would like to note that the set of barrier certificates satisfying (2)–(4) is unfortunately non-convex, due to the restriction $B(x) = 0$ in (4). As a consequence, the construction of such barrier certificates cannot be performed using convex optimization, even though in Section 4 we will present an iterative method that can be used to search for a barrier certificate in this set. Nevertheless, it is useful to know that alternative conditions defining a convex set of barrier certificates can be derived. They are given in Proposition 1 below.

Proposition 1. *Let the system (1) and the sets $\mathcal{X}$, D, $\mathcal{X}_0$ and $\mathcal{X}_u$ be given. Suppose there exists a barrier certificate $B : \mathcal{X} \to \mathbb{R}$ that is differentiable with respect to the first argument and satisfies the conditions (2)–(3) and*

$$\frac{\partial B}{\partial x}(x) f(x, d) \leq 0 \quad \forall (x, d) \in \mathcal{X} \times D.$$

Then the safety of the system (1) is guaranteed. Moreover, the set of barrier certificates that satisfy the above conditions is a convex set.

Proof. It can be directly seen that a barrier certificate satisfying the above conditions also satisfies (2)–(4) because of the set inclusion $\{x \in \mathcal{X} : B(x) = 0\} \subset \mathcal{X}$, and thus the system safety is guaranteed. The fact that the set of barrier certificates is convex can be established by taking arbitrary $B_1(x)$ and $B_2(x)$ satisfying the above conditions and showing that for $\alpha \in [0, 1]$, $B(x) = \alpha B_1(x) + (1 - \alpha) B_2(x)$ satisfies the conditions as well.

The conditions in the above proposition are obviously more restrictive than those in Theorem 1 and therefore the conclusion that we can draw is generally also more conservative. However, a barrier certificate satisfying the convex conditions can be sought directly using convex optimization. As we will see later, this will be useful for initializing the iterative search for a better barrier certificate in the non-convex set.

3.2 Hybrid Systems

Verification of hybrid systems requires the use of a barrier certificate that not only is a function of the continuous state, but also depends on the discrete location. For this purpose, we construct a barrier certificate from a set of functions of continuous state, where each function corresponds to a discrete location of the system. Since in each location the continuous state can only take value within the invariant of the location, each function only needs to satisfy inequalities similar to (2)–(4) in the invariant set associated to it. Functions corresponding to different locations are linked via appropriate conditions that take care of possible discrete transitions between the locations. We state the conditions that must be satisfied by the barrier certificate in the following theorem.

Theorem 2. *Let the hybrid system $H = (\mathcal{X}, L, X_0, I, F, T)$ and the unsafe set X_u be given. Suppose there exists a barrier certificate, i.e., a collection of differentiable functions $B_l(x)$ which, for each $l \in L$ and $(l, l') \in L^2$, $l' \neq l$, satisfy*

$$B_l(x) > 0 \quad \forall x \in \text{Unsafe}(l), \tag{5}$$

$$B_l(x) \leq 0 \quad \forall x \in \text{Init}(l), \tag{6}$$

$$\frac{\partial B_l}{\partial x}(x) f_l(x, d) \leq 0 \quad \forall (x, d) \in I(l) \times D(l) \text{ such that } B_l(x) = 0, \tag{7}$$

$$B_{l'}(x') \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x), \text{ for all } x \in \text{Guard}(l, l') \text{ s.t. } B_l(x) \leq 0. \tag{8}$$

Then the safety of the hybrid system H is guaranteed.

Proof. Assume that a barrier certificate $\{B_l(x)\}$ satisfying the above conditions can be found. Take any trajectory of the hybrid system that starts at arbitrary $(l_0, x_0) \in X_0$, and consider the evolution of $B_{l(t)}(x(t))$ along this trajectory. The condition (6) asserts that $B_{l_0}(x_0) \leq 0$. Next, (7) implies that during a segment of continuous flow $B_{l(t)}(x(t))$ cannot become positive, while (8) guarantees that during a discrete transition $B_{l(t)}(x(t))$ cannot jump to a positive value. Consequently, any such trajectory can never reach an unsafe state $(l_u, x_u) \in X_u$, whose $B_{l_u}(x_u)$ is positive according to (5). We conclude that the safety of the system is guaranteed.

Similar to what we encounter in the continuous case, the conditions (7)–(8) in the above theorem define a non-convex set of barrier certificates. Conditions defining a convex set of barrier certificates are given in the following proposition.

Proposition 2. *Let the hybrid system $H = (\mathcal{X}, L, X_0, I, F, T)$, the unsafe set X_u, and some* fixed *nonnegative constants $\sigma_{l,l'}$ be given. Suppose there exists a barrier certificate, i.e., a collection $\{B_l(x)\}$ of differentiable functions $B_l(x)$ which, for each $l \in L$ and $(l, l') \in L^2$, $l' \neq l$, satisfy (5)–(6) and*

$$\frac{\partial B_l}{\partial x}(x) f_l(x, d) \leq 0 \quad \forall (x, d) \in I(l) \times D(l),$$

$$B_{l'}(x') - \sigma_{l,l'} B_l(x) \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x), \; x \in \text{Guard}(l, l').$$

Then the safety of the hybrid system H is guaranteed. Moreover, all barrier certificates that satisfy the above conditions form a convex set.

Proof. Analogous to the proof of Proposition 1.

Remark 1. Two possible choices for $\sigma_{l,l'}$ are 0 and 1. The choice $\sigma_{l,l'} = 0$ corresponds to modifying (8) to

$$B_{l'}(x') \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x), \text{ for some } l \in L \text{ and } x \in \text{Guard}(l, l'),$$

and in this case a successful verification will actually prove that the system is safe even if during a transition from location l to l' the continuous state is allowed to jump to any continuous state x' in the image of the reset map. On the other hand, choosing $\sigma_{l,l'} = 1$ is useful for handling integral constraints, as we will shortly see.

3.3 Incorporating Constraints

In the remainder of this section we will briefly discuss how constraints can be handled within this framework. There are three kinds of constraints that can be incorporated: algebraic equality, algebraic inequality, and integral constraints; see [19] for a more thorough discussion. Here we will focus on integral constraints, as no existing methods can explicitly compute reachable sets when such constraints exist. Instead of assuming that the disturbance d is confined in $D(l)$, let us now assume that d and the continuous state x is constrained via

$$\int_0^T \phi(x(t), d(t))dt \geq 0, \quad \forall T > 0. \tag{9}$$

Constraints like this usually arise in systems analysis in the form of integral quadratic constraints [15] and are useful e.g. for describing a set of norm-bounded operators (cf. the example in Section 5.3), which may represent unmodelled continuous dynamics. Conditions guaranteeing safety when an integral constraint is present are given in the following theorem.

Theorem 3. *Let the hybrid system $H = (\mathcal{X}, L, X_0, I, F, T)$, the unsafe set X_u, and the constraint (9) be given. Suppose there exist a nonnegative constant multiplier σ and a collection $\{B_l(x)\}$ of differentiable functions $B_l(x)$ that satisfy*

$$B_l(x) > 0 \quad \forall x \in \text{Unsafe}(l), \tag{10}$$

$$B_l(x) \leq 0 \quad \forall x \in \text{Init}(l), \tag{11}$$

$$\frac{\partial B_l}{\partial x}(x) f_l(x, d) + \sigma\phi(x, d) \leq 0 \quad \forall (x, d) \in I(l) \times \mathbb{R}^m, \tag{12}$$

$$B_{l'}(x') \leq B_l(x) \quad \forall x' \in \text{Reset}(l, l')(x), \ x \in \text{Guard}(l, l') \tag{13}$$

for each $l \in L$ and $(l, l') \in L^2$, $l' \neq l$. Then $\{B_l(x)\}$ is a barrier certificate proving the safety of the system.

Proof. Assume that a barrier certificate satisfying the above conditions can be found. Consider any trajectory of the hybrid system on the time interval $[0, T]$ that starts at arbitrary $(l_0, x_0) \in X_0$. Assume that discrete transitions for this trajectory occur at time t_1, t_2, ..., t_N where the system switches to location l_1,

l_2, ..., l_N. Denote the continuous states before and after the i-th transition by x_i^- and x_i^+, respectively. Then from (12) we obtain

$$\begin{aligned}
&B_{l_0}(x_1^-) - B_{l_0}(x_0) + B_{l_1}(x_2^-) - B_{l_1}(x_1^+) + ... + B_{l_N}(x(T)) - B_{l_N}(x_N^+) \\
&= \int_0^{t_1^-} \frac{\partial B_{l_0}}{\partial x}(.) f_{l_0}(.) dt + \int_{t_1^+}^{t_2^-} \frac{\partial B_{l_1}}{\partial x}(.) f_{l_1}(.) dt + ... + \int_{t_N^+}^{T} \frac{\partial B_{l_N}}{\partial x}(.) f_{l_N}(.) dt \\
&\leq -\sigma \int_0^T \phi(x, d) dt \leq 0.
\end{aligned}$$

Now, (13) guarantees that $B_{l_i}(x_i^+) - B_{l_{i-1}}(x_i^-) \leq 0$ for $i = 1, ..., N$, and hence it follows from the above inequality that $B_{l_N}(x(T)) \leq B_{l_0}(x_0)$. By (10)–(11) we conclude that $x(T)$ is outside the unsafe region. The safety of the system is thus guaranteed, since both the trajectory and the final time T are arbitrary.

4 Computational Method

Construction of barrier certificates is generally not easy, as is the case with Lyapunov function synthesis. However, for systems whose vector fields are polynomial and whose set descriptions are semialgebraic (i.e., described by polynomial equalities and inequalities), a tractable computational method exists if we also postulate the barrier certificate to be polynomial. The method uses the sum of squares decomposition of multivariate polynomials [18] and semidefinite programming [24], which we will describe now.

A multivariate polynomial $f(x)$ is a sum of squares if there exist polynomials $f_1(x), ..., f_m(x)$ such that $f(x) = \sum_{i=1}^m f_i^2(x)$. This is equivalent to the existence of a quadratic form $f(x) = Z^T(x) Q Z(x)$ for some positive semidefinite matrix Q and vector of monomials $Z(x)$. A sum of squares decomposition for $f(x)$ can be computed using semidefinite programming, since it accounts to searching for an element Q in the intersection of the cone of positive semidefinite matrices and a set defined by some affine constraints. Together they provide a polynomial-time computational relaxation for proving global nonnegativity of multivariate polynomials [21,18] (since $f(x)$ is obviously nonnegative if it can be decomposed as a sum of squares), which belongs to the class of NP-hard problems. They have also been exploited for algorithmically constructing Lyapunov functions for nonlinear systems [18,17].

The same technique can be used in the computation of barrier certificates. Real coefficients $c_1, ..., c_m$ are used to parameterize a set of candidate barrier certificates in an affine manner, e.g., $\mathcal{B}_l = \{B_l(x) : B_l(x) = b_{0,l}(x) + \sum_{i=1}^m c_{i,l} b_{i,l}(x)\}$, for each $l \in L$, where the $b_{i,l}(x)$'s are some monomials in x. For example, one could arbitrarily determine an upper bound on the degree of the barrier certificate and then include all monomials whose degrees are less than or equal to the bound. The search for a barrier certificate $\{B_l(x) \in \mathcal{B}_l\}$, or equivalently coefficients $c_{i,l}$'s, such that the conditions in Theorems 2–3 or Proposition 2 are satisfied can be formulated as a sum of squares problem. In

the case of Proposition 2 or Theorem 3, the resulting sum of squares problem can be solved directly using semidefinite programming (cf. Section 4.1), while in the other case it can be solved by an iterative method, which we will describe in Section 4.2.

Even though the computational approach discussed in this section assumes that the system is described by polynomials, non-polynomial descriptions can be handled (although possibly with some conservatism) and non-polynomial barrier certificates can be constructed by recasting of variables as proposed in [17], or by over-approximating the system by one that has polynomial vector fields and semialgebraic set descriptions.

4.1 Sum of Squares Formulation

Let us now consider a concrete example of a hybrid system $H = (\mathcal{X}, L, X_0, I, F, T)$ whose vector fields $f_l(x, d)$ are polynomial for each $l \in L$, and assume that the invariant sets $I(l)$ are described as $I(l) = \{x \in \mathbb{R}^n : g_{I(l)}(x) \geq 0\}$. In these set descriptions, the g's are vectors of polynomials, and the inequalities are satisfied entry-wise. For example, when $I(l)$ is the n-dimensional hypercube $[\underline{x_1}, \overline{x_1}] \times ... \times [\underline{x_n}, \overline{x_n}]$, we may define

$$g_{I(l)}(x) = \begin{bmatrix} (x_1 - \underline{x_1})(\overline{x_1} - x_1) \\ \vdots \\ (x_n - \underline{x_n})(\overline{x_n} - x_n) \end{bmatrix}.$$

Similarly, define the sets $D(l)$, $\mathrm{Init}(l)$, $\mathrm{Unsafe}(l)$, and $\mathrm{Guard}(l, l')$ by the inequalities $g_{D(l)}(d) \geq 0$, $g_{\mathrm{Init}(l)}(x) \geq 0$, $g_{\mathrm{Unsafe}(l)}(x) \geq 0$, and $g_{\mathrm{Guard}(l,l')}(x) \geq 0$. Finally, let the value of the reset map $\mathrm{Reset}(l, l')$ evaluated at $x \in \mathrm{Guard}(l, l')$ also be defined as $\mathrm{Reset}(l, l')(x) = \{x' \in \mathbb{R}^n : g_{\mathrm{Reset}(l,l')}(x, x') \geq 0\}$.

For this system, the search for a barrier certificate can be formulated as the sum of squares optimization problem given in the following proposition.

Proposition 3. *Let the hybrid system H and the descriptions of all the sets $I(l)$, $D(l)$, $\mathrm{Init}(l)$, $\mathrm{Unsafe}(l)$, $\mathrm{Guard}(l, l')$, and $\mathrm{Reset}(l, l')(x)$ be given. Suppose there exist polynomials $B_l(x)$ and $\lambda_{B_l}(x, d)$, a positive number ϵ, and vectors of sums of squares $\sigma_{\mathrm{Unsafe}(l)}(x)$, $\sigma_{\mathrm{Init}(l)}(x)$, $\sigma_{I(l)}(x, d)$, $\sigma_{D(l)}(x, d)$, $\sigma_{\mathrm{Guard}(l,l')}(x, x')$, $\sigma_{\mathrm{Reset}(l,l')}(x, x')$, and $\sigma_{l,l'}(x, x')$, such that the following expressions:*

$$B_l(x) - \epsilon - \sigma^T_{\mathrm{Unsafe}(l)}(x) g_{\mathrm{Unsafe}(l)}(x) \tag{14}$$

$$- B_l(x) - \sigma^T_{\mathrm{Init}(l)}(x) g_{\mathrm{Init}(l)}(x) \tag{15}$$

$$- \frac{\partial B_l}{\partial x}(x) f_l(x, d) - \sigma^T_{D(l)}(x, d) g_{D(l)}(d) - \sigma^T_{I(l)}(x, d) g_{I(l)}(x) - \lambda_{B_l}(x, d) B_l(x) \tag{16}$$

$$\begin{aligned} - B_{l'}(x') + \sigma_{l,l'}(x, x') B_l(x) - \sigma^T_{\mathrm{Guard}(l,l')}(x, x') g_{\mathrm{Guard}(l,l')}(x) ... \\ - \sigma^T_{\mathrm{Reset}(l,l')}(x, x') g_{\mathrm{Reset}(l,l')}(x, x') \end{aligned} \tag{17}$$

are sums of squares for each $l \in L$ and $(l, l') \in L^2$, $l' \neq l$. Then $\{B_l(x)\}$ satisfies the conditions in Theorem 2, and therefore the safety of the system is guaranteed.

Proof. First notice that the expressions (14)–(17) are nonnegative, since they are sums of squares. Now take any $x \in \text{Unsafe}(l)$. For any such x the last term in (14) are nonpositive, and therefore it follows that $B_l(x) - \epsilon \geq 0$. Since ϵ is positive, condition (5) is immediately satisfied. Applying the same argument to the second, third, and fourth expressions, it is straightforward to show that (6)–(8) are satisfied by $B_l(x)$ for each $l \in L$, and thus we conclude that the collection $\{B_l(x)\}$ is a barrier certificate.

Remark 2. If the reset map $\text{Reset}(l, l')$ actually maps $x \in \text{Guard}(l, l')$ to a singleton, e.g., if $\text{Reset}(l, l') : x \mapsto g_{\text{Reset}(l,l')}(x)$ for some polynomial vector $g_{\text{Reset}(l,l')}$, then (17) can be simplified to

$$- B_{l'}(g_{\text{Reset}(l,l')}(x)) + \sigma_{l,l'}(x) B_l(x) - \sigma^T_{\text{Guard}(l,l')}(x) g_{\text{Guard}(l,l')}(x),$$

where $\sigma_{l,l'}(x)$ and the entries of $\sigma^T_{\text{Guard}(l,l')}(x)$ are sums of squares.

Remark 3. The conditions (14)–(17) can be regarded as a generalization of the S-procedure [7], which verifies the nonnegativity of a quadratic form $x^T Q x$ on the set $\mathcal{Q} = \{x : x^T Q_i x \geq 0, \text{ for } i = 1, ..., n\}$ by finding nonnegative scalar multipliers σ_i, $i = 1, ..., n$ such that the matrix $Q - \sum_{i=1}^n \sigma_i Q_i$ is positive semidefinite. They are a special case of *positivstellensatz*, a central result in real algebraic geometry for proving emptiness of semialgebraic sets, which also provides a nested family of less conservative tests for nonnegativity. See [18] for details.

The sum of squares problem stated in Proposition 3 can be solved using semidefinite programming, if either the barrier certificate $\{B_l(x)\}$ or the multipliers $\lambda_{B_l}(x, d)$ and $\sigma_{l,l'}(x, x')$ are fixed in advance. By fixing either of them, we eliminate the products between unknown coefficients in the multipliers and the $B_l(x)$'s; this results in all the unknown coefficients being constrained in an affine manner, which is necessary for converting the problem to a semidefinite program. For example, the convex conditions in Proposition 2 are formulated in terms of a sum of squares problem similar to the one stated above, with the multipliers $\lambda_{B_l}(x, d)$ set equal to zero and $\sigma_{l,l'}(x, x')$ set equal to some nonnegative constants $\sigma_{l,l'}$ (cf. also Remark 1). In this case, a barrier certificate $\{B_l(x)\}$ can be searched directly using semidefinite programming, e.g. with the help of the software [20]. While the computational cost of this search depends on both the degrees of (14)–(17) and the dimension of (x, d), for fixed degrees the required computations grow polynomially with respect to the dimension of (x, d).

4.2 Iterative Approach

Fixing multipliers as explained in the previous subsection yields a barrier certificate that lies in the convex set defined by the conditions in Proposition 2. We

will now present an iterative method for searching a barrier certificate that is not necessarily in the above set, but nevertheless still lies in the non-convex set of Theorem 2.

The reason to search for a barrier certificate in the non-convex set is that such a barrier certificate is generally less conservative than a barrier certificate in the convex set. For instance, the former may prove safety for larger disturbance sets, guard sets, unsafe sets, etc. Thus in the iteration we may start with some sufficiently small sets, and increase their sizes as the iteration progresses.

Algorithm 1

1. **Initialization:** Start with sufficiently small $D(l)$, Guard(l, l') etc. Specify $\lambda_{B_l}(x, d)$ and $\sigma_{l,l'}(x, x')$ in advance, e.g., by choosing $\lambda_{B_l}(x) = 0$ and $\sigma_{l,l'}(x, x') = 0$ or 1. Search for $B_l(x)$ and the remaining multipliers.
2. **Fixing the barrier certificate:** Fix the $B_l(x)$ obtained from the previous step. Enlarge $D(l)$, Guard(l, l'), etc. Search for $\lambda_{B_l}(x, d)$, $\sigma_{l,l'}(x, x')$, and the remaining multipliers.
3. **Fixing the multipliers:** Fix the $\lambda_{B_l}(x, d)$ and $\sigma_{l,l'}(x, x')$ obtained from the previous step. Enlarge $D(l)$, Guard(l, l'), etc. Search for $B_l(x)$ and the remaining multipliers. Repeat to Step 2.

For an example illustrating the benefit of using this method, we refer the reader to Section 5.2. It should be noted, however, that solving a non-convex optimization problem by an iteration like this is not guaranteed to yield the globally optimal solution, as the iteration may actually converge to a local optimum. In our case, the barrier certificate we obtain at the end of our iteration may not be a barrier certificate that is able to prove safety for the maximum possible disturbance sets etc.

5 Examples

5.1 Example 1

Consider the two-dimensional system (taken from [12, page 180]) $\dot{x}_1 = x_2$, $\dot{x}_2 = -x_1 + \frac{p}{3}x_1^3 - x_2$, where the uncertain time-invariant parameter p lies in the interval $[0.9, 1.1]$. We want to verify that for any p in the above interval, all trajectories of the system starting at $\mathcal{X}_0 = \{x \in \mathbb{R}^2 : (x_1 - 1.5)^2 + x_2^2 \leq 0.25\}$ will never reach the unsafe set $\mathcal{X}_u = \{x \in \mathbb{R}^2 : (x_1 + 1)^2 + (x_2 + 1)^2 \leq 0.16\}$. Using the computational method described in Section 4, we are able to find a quartic barrier certificate $B(x, p)$, linearly parameterized by p, that satisfies the conditions in Proposition 1. Hence the safety of the system is verified. In fact, this barrier certificate proves that all trajectories starting from the zero sublevel set of $B(x, p)$ cannot reach any state for which $B(x, p) > 0$.

For $p = 1$, the phase portrait of the system and the zero level set of the barrier certificate are shown in Figure 1. The system has a stable focus at the origin, and two saddle points at $(\pm\sqrt{3}, 0)$. The zero level set of the barrier certificate separates $\mathcal{X}_u$ from all trajectories starting at $\mathcal{X}_0$. Note that since $\mathcal{X}_0$ contains a

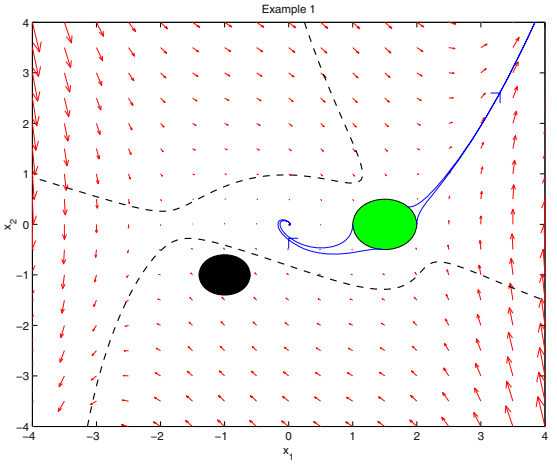

Fig. 1. Phase portrait of the system in Example 1. Solid patches are (from the left) $\mathcal{X}_u$ and $\mathcal{X}_0$, respectively. Dashed curves are the zero level set of $B(x,p)$, whereas solid curves are some trajectories of the system.

part of the unstable manifold corresponding to the equilibrium $(\sqrt{3},0)$, the safety of this system cannot be verified exactly by computation of forward reachable sets in a finite time horizon.

5.2 Example 2

Consider a hybrid system whose discrete transition diagram is depicted in Figure 2. The system starts in location 1 (NO CONTROL mode), with its continuous state initialized at $\{x \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 \leq 0.01\}$. In this location, the continuous state evolves according to $\dot{x} = f_1(x,d)$, until it reaches some point in the guard set $\text{Guard}(1,2) = \{x \in \mathbb{R}^3 : 0.99 \leq x_1^2 + 0.01x_2^2 + 0.01x_3^2 \leq 1.01\}$, at which instance a controller whose objective is to prevent $|x_1|$ from getting too big will be turned on, and the system jumps to location 2 (CONTROL mode). In location 2, the continuous dynamics is described by $\dot{x} = f_2(x,d)$. The system will remain in this location until the continuous state enters the second guard set $\text{Guard}(2,1) = \{x \in \mathbb{R}^3 : 0.03 \leq x_1^2 + x_2^2 + x_3^2 \leq 0.05\}$, where the controller will be turned off and the system jumps to location 1. We assume nondeterminism in the jump from location 1 to location 2 and vice versa. The invariant sets of both locations are shown in Figure 2, and the vector fields are given by

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

Our task in this example is to verify that $|x_1|$ never gets bigger than 5, if the instantaneous magnitude of the disturbance d is bounded by 1. We define our unsafe sets as $\text{Unsafe}(1) = \emptyset$, $\text{Unsafe}(2) = \{x \in \mathbb{R}^3 : 5 \leq x_1 \leq 5.1\} \cup \{x \in$

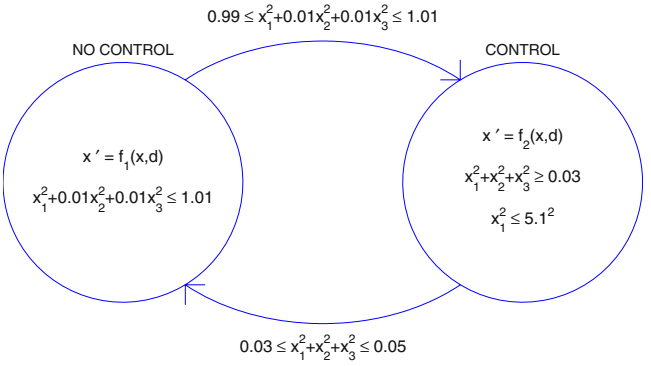

Fig. 2. Discrete transition diagram of the system in Example 2. This system has two discrete locations: NO CONTROL and CONTROL, with the vector field and the invariant of each location depicted inside the corresponding circle. The text labelling the transition between locations describes the guard set.

Table 1. Description and results of the iterative method used in Example 2. The third column indicates the disturbance range for which safety is verified.

Iteration	Description	Verified
1	Set $\lambda_{B_l}(x,d) = 0$, find $B_l(x)$.	$-0.005 \leq d \leq 0.005$
2	Fix $B_l(x)$, find $\lambda_{B_l}(x,d)$.	$-0.625 \leq d \leq 0.625$
3	Fix $\lambda_{B_l}(x,d)$, find $B_l(x)$.	$-1 \leq d \leq 1$

$\mathbb{R}^3 : -5.1 \leq x_1 \leq -5\}$, and compute a quartic barrier certificate satisfying the conditions in Theorem 2. Using the iterative method described in Section 4 to enlarge the verifiable disturbance set, we obtain the results shown in Table 1. At the third iteration, we are able to prove the safety of the system.

5.3 Example 3

In this example, we analyze the reachability of a linear system in feedback interconnection with a relay. The block diagram of the system is shown in Figure 3, with the matrices A, B, C, and D given by

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -0.2 & -0.3 & -1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ 0.1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}^T, \quad D = 0,$$

and the relay element having the following characteristic: $w = 10$ if $y \geq 0$, and $w = -10$ if $y < 0$. For the sets $\mathcal{X} = \{x \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 \leq 4^2\}$, $\mathcal{X}_0 = \{x \in \mathbb{R}^3 : (x_1+2)^2 + x_2^2 + x_3^2 \leq 0.1^2\}$, and $\mathcal{X}_u = \{x \in \mathbb{R}^3 : (x_1-2)^2 + x_2^2 + x_3^2 \leq 0.1^2\}$, we pose the following question: is it possible to design a controller K (possibly nonlinear and time-varying) with the L_2-gain no greater than one, which is connected to the system in the way shown in Figure 2, such that the system can be steered from $\mathcal{X}_0$ to $\mathcal{X}_u$ while maintaining the state in $\mathcal{X}$?

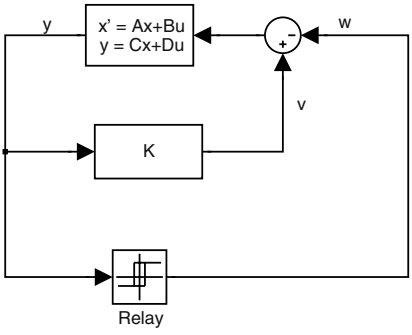

Fig. 3. Block diagram of the system in Example 3. We ask if it is possible to design a controller K that steers the system from an initial set $\mathcal{X}_0$ to a destination set $\mathcal{X}_u$, subject to some other specifications.

The requirement that the L_2-gain of the controller is no greater than one can be equivalently formulated as an integral quadratic constraint (IQC) [15] $\int_0^T [y^2(t) - v^2(t)]dt \geq 0, \forall T > 0$. This specification introduces dynamic uncertainty to the problem, and consequently the reachable sets cannot be computed explicitly with existing methods. Nevertheless, we can perform reachability analysis by adjoining the above IQC using a nonnegative constant multiplier to the conditions on the time derivative of barrier certificates (cf. Theorem 3). For this example, a quartic barrier certificate that satisfies the required conditions can be found. Hence we conclude that the given specification is impossible to meet.

6 Conclusions

In this paper, we presented a novel approach for reachability refutation of uncertain hybrid systems with nonlinear continuous dynamics. Our approach is based on the construction of a barrier certificate, whose zero level set separates all trajectories emanating from a set of initial conditions from some given unsafe set. Contrary to most existing techniques, our method does not require computing the flow of the system. Rather, we utilize a Lyapunov-like formalism to construct a safety proof.

Our approach is suitable for hybrid systems whose continuous dynamics are described by polynomial vector fields and whose invariant sets, guard sets, etc are described by polynomial equalities and inequalities. By formulating the conditions for barrier certificates as sum of squares problems and using semidefinite programming to solve them, it is possible to search for barrier certificates in a computationally tractable fashion. We demonstrated the efficacy of our approach by some examples of nonlinear and uncertain hybrid systems. Higher dimensional problems can also be handled by our method, since the computational cost of constructing barrier certificates grows polynomially with respect to the state dimension.

References

1. R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Oliviero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.
2. R. Alur, T. Dang, and F. Ivancic. Progress on reachability analysis of hybrid systems using predicate abstraction. In *Hybrid Systems: Computation and Control, LNCS 2623*, pages 4–19. Springer-Verlag, 2003.
3. H. Anai and V. Weispfenning. Reach set computations using real quantifier elimination. In *Hybrid Systems: Computation and Control, LNCS 2034*, pages 63–76. Springer-Verlag, 2001.
4. E. Asarin, T. Dang, and O. Maler. The d/dt tool for verification of hybrid systems. In *Computer Aided Verification, LNCS 2404*, pages 365–370. Springer-Verlag, 2002.
5. A. Bemporad, F. D. Torrisi, and M. Morari. Optimization-based verification and stability characterization of piecewise affine and hybrid systems. In *Hybrid Systems: Computation and Control, LNCS 1790*, pages 45–58. Springer-Verlag, 2000.
6. O. Botchkarev and S. Tripakis. Verification of hybrid systems with linear differential inclusions using ellipsoidal approximations. In *Hybrid Systems: Computation and Control, LNCS 1790*, pages 73–88. Springer-Verlag, 2000.
7. S. Boyd, L. El Ghaoui, E. Feron, and V. Balakrishnan. *Linear Matrix Inequalities in System and Control Theory*. SIAM, Philadelphia, PA, 1994.
8. M. S. Branicky. Multiple Lyapunov functions and other analysis tools for switched and hybrid systems. *IEEE Trans. Automatic Control*, 43(4):475–482, 1998.
9. A. Chutinan and B. H. Krogh. Computational techniques for hybrid system verification. *IEEE Trans. Automatic Control*, 48(1):64–75, 2003.
10. E. M. Clarke and R. P. Kurshan. Computer-aided verification. *IEEE Spectrum*, 33(6):61–67, 1996.
11. M. Johansson and A. Rantzer. Computation of piecewise quadratic Lyapunov functions for hybrid systems. *IEEE Trans. Automat. Control*, 43(4):555–559, 1998.
12. H. K. Khalil. *Nonlinear Systems*. Prentice-Hall, Inc., Upper Saddle River, NJ, second edition, 1996.
13. A. Kurzhanski and P. Varaiya. Ellipsoidal techniques for reachability analysis. In *Hybrid Systems: Computation and Control, LNCS 1790*, pages 203–213. Springer-Verlag, 2000.
14. G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computations for families of linear vector fields. *J. Symbolic Computation*, 32(3):231–253, 2001.
15. A. Megretski and A. Rantzer. System analysis via integral quadratic constraints. *IEEE Trans. Automatic Control*, 42(6):819–830, 1997.
16. R. M. Murray (Ed.). *Control in an Information Rich World: Report of the Panel on Future Directions in Control, Dynamics, and Systems*. SIAM, Philadelphia, PA, 2003. Available at http://www.cds.caltech.edu/~murray/cdspanel.
17. A. Papachristodoulou and S. Prajna. On the construction of Lyapunov functions using the sum of squares decomposition. In *Proceedings IEEE CDC*, 2002.
18. P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, Caltech, Pasadena, CA, 2000.
19. S. Prajna. Barrier certificates for nonlinear model validation. In *Proceedings IEEE Conference on Decision and Control*, 2003.
20. S. Prajna, A. Papachristodoulou, and P. A. Parrilo. Introducing SOSTOOLS: A general purpose sum of squares programming solver. In *Proceedings IEEE CDC*, 2002. Available at http://www.cds.caltech.edu/sostools and http://www.aut.ee.ethz.ch/~parrilo/sostools.