A Framework for Worst-Case and Stochastic Safety Verification Using Barrier Certificates

Stephen Prajna, Ali Jadbabaie, and George J. Pappas

***Abstract*— This paper presents a methodology for safety verification of continuous and hybrid systems in the worst-case and stochastic settings. In the worst-case setting, a function of state termed barrier certificate is used to certify that all trajectories of the system starting from a given initial set do not enter an unsafe region. No explicit computation of reachable sets is required in the construction of barrier certificates, which makes it possible to handle nonlinearity, uncertainty, and constraints directly within this framework. In the stochastic setting, our method computes an upper bound on the probability that a trajectory of the system reaches the unsafe set, a bound whose validity is proven by the existence of a barrier certificate. For polynomial systems, barrier certificates can be constructed using convex optimization, and hence the method is computationally tractable. Some examples are provided to illustrate the use of the method.**

***Index Terms*— safety verification, nonlinear systems, hybrid systems, stochastic systems, barrier certificates, sum of squares optimization.**

I. Introduction

COMPLEX behaviors that can be exhibited by modern engineering systems, many of which have hybrid (i.e., a mixture of continuous and discrete) dynamics, make the safety verification of such systems both crucial and challenging. The importance of safety verification increases tremendously for systems whose functions are safety critical, such as air traffic control [20], [47], life support devices [17], etc. In principle, safety verification aims to show that starting at some initial conditions, a system cannot evolve to some unsafe region in the state space. The verification can be cast either in *the worst-case setting* or *the stochastic setting*. A problem instance in the former setting may consist of a system with an uncertain disturbance input, where a hard bound on the input magnitude is known, and we are asked to show that for all possible disturbance input the system cannot evolve to the unsafe region. On the other hand, in the latter setting no hard bound is given, but instead a stochastic characterization of the disturbance is available and we are asked to show that the probability of the system evolving to the unsafe region is sufficiently small.

For safety verification of continuous and hybrid systems in the worst-case setting, various methods have been proposed. Explicit computation of either exact or approximate reachable sets corresponding to the continuous dynamics is crucial for most of these methods. For linear continuous systems with certain eigenvalue structures and semialgebraic initial sets, *exact* reachable set calculation using quantifier elimination has been proposed in [4], [27]. Unfortunately, their approach requires knowing the exact solution of the differential equations, and hence does not seem extendable to the nonlinear case. In another vein, several techniques have also been developed for *approximate* reachable set calculation. For linear systems, there are results based on quantifier elimination [44], ellipsoidal calculus [10], [25], polygonal approximation [6], [8], geometric programming [50], and real algebraic geometry [51]. Other techniques have been proposed for nonlinear systems, for example, based on the Hamilton Jacobi equations [47], polygonal approximations [13], and approximating the system as a piecewise linear system [5]. In the case of hybrid systems, most of the techniques are based on constructing abstractions (i.e., discrete quotients) of the systems, and then performing model checking on the resulting discrete systems. See for instance [3], [6], [13], [45].

In this paper, we will present a method for safety verification that is different from the above approaches as it does not require computation of reachable sets, but instead relies on a deductive inference using what we term barrier certificates, which have been previously used in the context of nonlinear model validation [34]. For a continuous system, a barrier certificate is a function of state satisfying a set of inequalities on both the function itself and its Lie derivative along the flow of the system. In the state space, the zero level set of a barrier certificate separates an unsafe region from all system trajectories starting from a set of possible initial states. Therefore, the existence of such a function provides an exact certificate/proof of system safety.

Similar to the Lyapunov approach for proving stability [24], the main idea here is to study properties of the system without the need to compute the flow explicitly. Although an over-approximation of the reachable set may also be used as a proof for safety, a barrier certificate can be much easier to compute when the system is nonlinear and uncertain. Moreover, barrier certificate can be easily used to verify safety in infinite time horizon. Note also that there are some connections between our method and viability theory [7], invariant set theory [7], [9], and also the verification approaches in [21], [42], [46]. We will discuss these connections later as we progress.

Our method can be easily extended to handle hybrid systems. In the hybrid case, a barrier certificate is constructed from a set of functions of continuous state indexed by the

Submitted to IEEE Transactions on Automatic Control. Preliminary versions of this paper appeared at the Hybrid Systems: Computation and Control 2004 and the IEEE Conference on Decision and Control 2004.

S. Prajna is with the Control and Dynamical Systems option, California Institute of Technology, Pasadena, CA 91125, USA. Email: prajna@cds.caltech.edu

A. Jadbabaie and G. J. Pappas are with the Department of Electrical and Systems Engineering, University of Pennsylvania, Philadelphia, PA 19104, USA. Emails: {jadbabai,pappasg}@seas.upenn.edu

system location[1]. Instead of satisfying the aforementioned inequalities in the whole continuous state space, each function needs to satisfy the inequalities only within the invariant of the location. Functions corresponding to different locations are linked via appropriate conditions that must be satisfied during discrete transitions between the locations. The idea is analogous to using multiple Lyapunov-like functions [22] for stability analysis of hybrid systems.

With this methodology, it is possible to treat a large class of hybrid systems, including those with nonlinear continuous dynamics, uncertainty, and constraints. 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 called sum of squares optimization [31], [32], [38], [39] can be utilized for constructing a polynomial barrier certificate, e.g., using the software SOSTOOLS [38], [39]. While the computational cost of this construction depends on the degrees of the vector fields and the barrier certificate in addition to the number of discrete locations and the continuous state dimension, for fixed polynomial degrees the complexity grows polynomially with respect to the other quantities. Hence we expect our method to be more scalable than many other existing methods. Successful application of our method to a NASA life support system, which is a nonlinear hybrid systems with 6 discrete modes and 10 continuous states, has been reported in [17].

In addition to the worst-case setting outlined above, we will also consider safety verification of continuous and hybrid systems in the stochastic setting. The stochasticity of a continuous system may originate from random inputs to the dynamics, which can be taken into account by considering stochastic differential equations. In the case of stochastic hybrid systems, stochasticity may also be induced by randomness in the discrete transitions. Study of systems modelled by stochastic differential equations has a long history and readers can find relevant references in [30]. On the other hand, only quite recently have people started to consider stochastic hybrid systems. See [14], [16], [18], [19], and [33] for an overview.

When the system is stochastic, answering the safety verification question in a worst-case non-stochastic manner will usually lead to a very conservative and restrictive answer, since there is no hard bound on the value of stochastic input. Indeed it is more natural to formulate and consider a safety verification problem that has a probabilistic interpretation. For example, it may be of interest to prove that the *probability* that a system trajectory reaches the unsafe region is *lower* than a certain safety margin. For some references on safety verification of stochastic continuous and hybrid systems, readers are referred to [11], [12], [20], [49].

The approach that we take to solve the stochastic safety verification problem still relies on barrier certificates. However, instead of using a barrier certificate whose zero level set separates the unsafe region from all possible system trajectories, we will use a barrier certificate that yields a *supermartingale* (loosely speaking, its expected value along time is non-increasing) under the given system dynamics. In addition, we ask that the value of the barrier certificate at the initial state be lower than its value at the unsafe region. The probability of reaching the unsafe region can then be bounded from above using a Chebyshev-like inequality for supermartingales. We derive conditions that must be satisfied by barrier certificates for stochastic continuous systems and a class of stochastic hybrid systems called switching diffusion processes. Similar to their non-stochastic counterpart, polynomial barrier certificates can be computed using sum of squares optimization when the description of the system is polynomial and the sets are semialgebraic.

For the above classes of systems, our method can be used to efficiently compute an *exactly guaranteed* upper bound on the probability that a system trajectory reaches the unsafe set. The references [11], [12], for example, suggest (theoretical) ways to calculate such a probability, yet they have not provided a computational technique for that. The reference [20] does provide a computational method to approximate the reach probability for stochastic differential equations, but since their method is based on discretizing the state space, there are still some unresolved issues with guaranteeing the accuracy of the computed probability and the scalability of the method. Finally, the work in [49] approximates the reach probability for stochastic discrete time systems using randomized simulations, and currently there is no accuracy guarantee either.

The outline of the paper is as follows. In Section II, we consider safety verification in the worst case setting. Safety verification in the stochastic setting is addressed in Section III. Computation of barrier certificates using sum of squares optimization is discussed in Section IV. Some examples will be given in Section V, and finally the paper will be ended by conclusions in Section VI.

1) Notations: Most of the notations are standard. We denote the set of real numbers by $\mathbb{R}$ and the Euclidean n-space by $\mathbb{R}^n$. The trace of an $n \times n$ matrix M, i.e., the sum of its diagonal elements, is denoted by $\mathrm{Tr}(M)$. By $f : X \to Y$ we mean a function f mapping $X \subseteq \mathbb{R}^n$ to $Y \subseteq \mathbb{R}^m$. We denote the spaces of k-times continuously differentiable functions mapping $X \subseteq \mathbb{R}^n$ to $\mathbb{R}^m$ by $C^k(X, \mathbb{R}^m)$, and when $m = 1$ we will write $C^k(X)$. Correspondingly, the spaces of continuous functions on X are denoted by $C(X, \mathbb{R}^m)$ and $C(X)$. For a differentiable function $F : \mathbb{R}^n \to \mathbb{R}$, we use $\frac{\partial F}{\partial x}(x)$ to denote the row vector of partial derivatives of F with respect to $x_1, \dots x_n$. The Hessian of a twice differentiable function $F : \mathbb{R}^n \to \mathbb{R}$ is denoted by $\frac{\partial^2 F}{\partial x^2}(x)$. Finally, $P\{ \cdot \}$ and $P\{ \cdot \mid \cdot \}$ denote the total and conditional probability, respectively, whereas $E[\cdot]$ and $E[\cdot \mid \cdot]$ denote the total and conditional expectation.

II. Safety Verification in the Worst-Case Setting

A. Continuous Systems

1) Convex Conditions: Consider a continuous system described by a set of ordinary differential equations:

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

[1]The term "location" here means discrete state; cf. Section II-B.1.

with the state $x(t)$ taking its value in $\mathbb{R}^n$ and the disturbance input $d(t)$ taking its value in $\mathcal{D} \subseteq \mathbb{R}^m$. Here $d(t)$ is assumed to be piecewise continuous and bounded on any finite time interval. Some smoothness conditions will be imposed on the vector field $f(x, d)$. At the least it will be continuous, which makes $x(t)$ piecewise continuously differentiable.

In safety verification, only parts of trajectories that are contained in a given set $\mathcal{X} \subseteq \mathbb{R}^n$ and that start from a given set of possible initial states $\mathcal{X}_0 \subseteq \mathcal{X}$ are considered. We denote the unsafe region of the system by $\mathcal{X}_u$, with $\mathcal{X}_u \subseteq \mathcal{X}$. With these notations, the safety property in the worst-case setting can be defined as follows. The definition can be directly extended for other classes of systems as needed.

Definition 1 (Safety): Given the system (1), the state set $\mathcal{X} \subseteq \mathbb{R}^n$, the initial set $\mathcal{X}_0 \subseteq \mathcal{X}$, the unsafe set $\mathcal{X}_u \subseteq \mathcal{X}$, and the disturbance set $\mathcal{D} \subseteq \mathbb{R}^m$, we say that the *safety* property holds if there exist no time instant $T \geq 0$ and a piecewise continuous and bounded disturbance $d : [0, T] \to \mathcal{D}$ that gives rise to an unsafe system trajectory, i.e., a trajectory $x : [0, T] \to \mathbb{R}^n$ satisfying $x(0) \in \mathcal{X}_0$, $x(T) \in \mathcal{X}_u$, and $x(t) \in \mathcal{X}\ \forall t \in [0, T]$.

Our method for verifying safety relies on the existence of what we will call barrier certificate. For continuous systems, the following proposition states the conditions that are satisfied by a barrier certificate.

Proposition 2: Let the system $\dot{x} = f(x, d)$ and the sets $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{X}_0 \subseteq \mathcal{X}$, $\mathcal{X}_u \subseteq \mathcal{X}$, $\mathcal{D} \subseteq \mathbb{R}^m$ be given, with $f \in C(\mathbb{R}^{n+m}, \mathbb{R}^n)$. Suppose there exists a differentiable function $B : \mathbb{R}^n \to \mathbb{R}$ such that

$$B(x) \leq 0 \qquad \forall x \in \mathcal{X}_0, \tag{2}$$

$$B(x) > 0 \qquad \forall x \in \mathcal{X}_u, \tag{3}$$

$$\frac{\partial B}{\partial x}(x) f(x, d) \leq 0 \qquad \forall (x, d) \in \mathcal{X} \times \mathcal{D}, \tag{4}$$

then the safety of the system in the sense of Definition 1 is guaranteed.

Proof: Our proof is by contradiction. Assume that there exists a barrier certificate $B(x)$ satisfying conditions (2)–(4), while at the same time the system is not safe, i.e., there exist a time instance $T \geq 0$, a disturbance signal $d : [0, T] \to \mathcal{D}$, and an initial condition $x_0 \in \mathcal{X}_0$ such that a trajectory $x(t)$ of the system starting at $x(0) = x_0$ satisfies $x(t) \in \mathcal{X}$ for all $t \in [0, T]$ and $x(T) \in \mathcal{X}_u$. Condition (4) implies that the derivative of $B(x(t))$ with respect to time is non-positive on the time interval $[0, T]$. A direct consequence of this (which for example can be shown using the mean value theorem) is that $B(x(T))$ must be less than or equal to $B(x(0))$, which is contradictory to (2)–(3). Thus the initial hypothesis is not correct: the system must be safe. ■

A function $B(x)$ satisfying the conditions in Proposition 2 is termed a barrier certificate. The zero level set of $B(x)$ provides a "barrier" between possible system trajectories and the given unsafe region, in the sense that no trajectory of the system starting from the initial set can cross this level set to reach the unsafe region. In proving that the system is safe, no explicit computation of system trajectories nor reachable sets is required.

In the above proposition we have assumed that the disturbance input can vary arbitrarily fast. If the variation of the disturbance is bounded, 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 (4) we need to take into account the extra derivative term $\frac{\partial B}{\partial d}(x, d)\dot{d}$, with the disturbance variation $\dot{d}$ taking its value in some bounded set.

Note that the set of barrier certificates satisfying the conditions in Proposition 2 is convex. This can be established by taking arbitrary $B_1(x)$ and $B_2(x)$ satisfying the above conditions and showing that for all $\alpha \in [0, 1]$, $B(x) = \alpha B_1(x) + (1 - \alpha) B_2(x)$ satisfies the conditions as well. The convexity property is very beneficial for the computation of $B(x)$. As we will see later in Section IV-A, a barrier certificate $B(x)$ in this convex set can be searched directly using convex optimization.

Since the set $\{x \in \mathcal{X} : B(x) \leq 0\}$ is actually an invariant set within $\mathcal{X}$, the method presented above is closely related to the smallest invariant set approach for safety verification (see, e.g., [21]). The latter approach differs from ours in that it tries to compute the smallest invariant set that contains $\mathcal{X}_0$, and then show that this set does not intersect $\mathcal{X}_u$. However, among invariant sets whose descriptions have *bounded complexity* (e.g., sets described using finite degree polynomials), the smallest set may not be one that does not intersect $\mathcal{X}_u$. Not only that, such smallest invariant set may be very difficult to find and may not be unique. Our approach, on the other hand, uses an arbitrary invariant set containing $\mathcal{X}_0$ that does not intersect $\mathcal{X}_u$. As such, our method is computationally much easier than the smallest invariant set approach.

We would like to remark that other approaches similar to ours are also presented in [42], [46]. These papers address the verification problem from a computer science point of view, and propose methods for constructing *invariants* of the system. An invariant here is a property that holds for every reachable state of the system. Thus, in the barrier certificate framework, for example, $B(x) \leq 0$ is an invariant of the system. The difference is that their conditions for the invariants are more restrictive than ours, and the invariants are not computed using convex optimization, but instead using Gröbner basis method followed by solving a system of linear equations.

2) Non-Convex Conditions: Although the conditions in Proposition 2 are good for computation since they define a convex set of barrier certificates, the conditions seem rather conservative (i.e., within a class of barrier certificates with bounded complexity) as the derivative inequality (4) needs to be satisfied on the whole state set $\mathcal{X}$. It is natural to expect that the conditions can be relaxed by requiring a similar derivative inequality to hold only on and near the set of $x \in \mathcal{X}$ for which $B(x) = 0$. This kind of condition is used in Proposition 3 below. Unfortunately, the set of barrier certificates will no longer be convex, hence a direct computation of a barrier certificate using convex optimization is not possible, although we can still try to search for a barrier certificate in the non-convex set using an iterative method, as we will see in Section IV-B.

Proposition 3: Let the system $\dot{x} = f(x,d)$ and the sets $\mathcal{X} \subseteq \mathbb{R}^n$, $\mathcal{X}_0 \subseteq \mathcal{X}$, $\mathcal{X}_u \subseteq \mathcal{X}$, $\mathcal{D} \subseteq \mathbb{R}^m$ be given, with $f \in C(\mathbb{R}^{n+m}, \mathbb{R}^n)$. If there exists a function $B \in C^1(\mathbb{R}^n)$ that satisfies the following conditions:

$$B(x) \leq 0 \quad \forall x \in \mathcal{X}_0, \tag{5}$$

$$B(x) > 0 \quad \forall x \in \mathcal{X}_u, \tag{6}$$

$$\frac{\partial B}{\partial x}(x) f(x,d) < 0 \quad \forall (x,d) \in \mathcal{X} \times \mathcal{D} \text{ s.t. } B(x) = 0, \tag{7}$$

then the safety of the system in the sense of Definition 1 is guaranteed.

Proof: Suppose that a disturbance signal $d : [0,T] \to \mathcal{D}$ and a corresponding unsafe trajectory $x : [0,T] \to \mathcal{X}$ exist. Let t_1 and t_2 be two time instants such that $0 \leq t_1 < t_2 \leq T$, $B(x(t_1)) \leq 0$, $B(x(t_2)) \geq 0$, and

$$\frac{\partial B}{\partial x}(x(t)) f(x(t), d(t)) < 0 \quad \forall t \in [t_1, t_2].$$

Now integrate $\frac{\partial B}{\partial x}(x(t)) f(x(t), d(t))$ over the time interval $[t_1, t_2]$ to obtain a contradiction, thus proving that the system is safe. ∎

The above proposition is sufficient for our purposes and also the proof is straightforward. However, it is interesting to note that other (non-convex) conditions can be derived using viability theory [7]. Interested readers are referred to [35].

B. Hybrid Systems

1) Modelling Framework: Throughout this subsection, 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 $H = (\mathcal{X}, L, X_0, I, F, \mathcal{T})$ 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 a 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 $\dot{x}(t) \in F(l(t), x(t))$.
- $\mathcal{T} \subseteq X \times X$ is a relation capturing discrete transitions between two locations. Here a transition $((l,x),(l',x')) \in \mathcal{T}$ indicates that from the state (l,x) the system can undergo a discrete jump to the state (l',x').

Valid trajectories of the hybrid system H start at 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 $\dot{x}(t) \in F(l(t), x(t))$, with $x(t)$ remains inside the invariant set $I(l(t))$. For our purpose, we will model the uncertainty in the continuous flow is by some disturbance inputs in the following manner:

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

where $f_l(x,d)$ is a vector field that governs the flow of the system at location l, and $d(t)$ is a vector of disturbance inputs that takes value in the set $\mathcal{D}(l(t)) \subseteq \mathbb{R}^m$. We assume that $d(t)$ is piecewise continuous and bounded on any finite time interval, and that $f_l \in C(\mathbb{R}^{n+m}, \mathbb{R}^n)$ for all $l \in L$. Finally, at a state (l_1, x_1), a discrete transition to (l_2, x_2) can occur if $((l_1,x_1),(l_2,x_2)) \in \mathcal{T}$. We assume non-determinism in the discrete transition, i.e., the transition may or may not occur, but no stochastic characterization is used or given.

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 valid trajectories of the hybrid system H cannot enter the unsafe region X_u. More specifically, the safety property is defined as follows.

Definition 4 (Safety – Hybrid Systems): Given a hybrid system H and an unsafe set $X_u \subseteq X$, the safety property holds if there exist no time instant $T \geq 0$, a piecewise continuous and bounded disturbance input $d : [0,T] \to \mathbb{R}^m$, and a finite sequence of transition times $0 \leq t_1 \leq t_2 \leq \ldots \leq t_N \leq T$ that give rise to an unsafe system trajectory, i.e., a trajectory $(l,x) : [0,T] \to X$ satisfying $(l(0), x(0)) \in X_0$, $x(t) \in I(l(t))$ for $t \in [0,T]$, and $(l(T), x(T)) \in X_u$. (Note that the disturbance input here must also satisfy $d(t) \in \mathcal{D}(l(t))$ for all $t \in [0,T]$.)

In our analysis conditions, we will also need the following definitions. For each location $l \in L$, the sets of initial and unsafe continuous states are defined as $\text{Init}(l) = \{x \in \mathcal{X} : (l,x) \in X_0\}$ and $\text{Unsafe}(l) = \{x \in \mathcal{X} : (l,x) \in X_u\}$, both of which can be empty. To each tuple $(l,l') \in L^2$ with $l \neq l'$, we associate a guard set $\text{Guard}(l,l') = \{x \in \mathcal{X} : ((l,x),(l',x')) \in \mathcal{T} \text{ for some } x' \in \mathcal{X}\}$, which is the set of continuous states from which the system can undergo a transition from location l to location l', and a (possibly set valued) reset map $\text{Reset}(l,l') : x \mapsto \{x' \in \mathcal{X} : ((l,x),(l',x')) \in \mathcal{T}\}$, whose domain is $\text{Guard}(l,l')$. Obviously, if no discrete transition from location l to location l' is possible, then $\text{Guard}(l,l')$ will be regarded as empty, and the associated reset map needs not be defined.

2) Conditions for Safety: Verification of hybrid systems should use 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) or (5)–(7) in the invariant associated to its location. Functions corresponding to different locations are linked via appropriate conditions that take care of possible discrete transitions between the locations. Analogous idea was used in stability analysis of affine hybrid systems using piecewise quadratic Lyapunov functions [22].

We state the conditions that must be satisfied by the barrier

certificate in the following theorem. The notations and assumptions imposed on the system are as described in Section II-B.1.

Theorem 5: Let the hybrid system H and the unsafe set $X_u \subseteq X$ be given. Suppose there exists a collection $\{B_l(x) : l \in L\}$ of functions $B_l \in C^1(\mathbb{R}^n)$ which, for all $l \in L$ and $(l, l') \in L^2$, $l \neq l'$, satisfy

$$B_l(x) \leq 0 \quad \forall x \in \text{Init}(l), \tag{8}$$

$$B_l(x) > 0 \quad \forall x \in \text{Unsafe}(l), \tag{9}$$

$$\frac{\partial B_l}{\partial x}(x) f_l(x, d) < 0 \quad \forall (x, d) \in I(l) \times \mathcal{D}(l) \text{ such that } B_l(x) = 0, \tag{10}$$

$$B_{l'}(x') \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x), \text{ for all } x \in \text{Guard}(l, l') \text{ s.t. } B_l(x) \leq 0. \tag{11}$$

Then the safety of the system in the sense of Definition 4 is guaranteed.

Proof: Assume that a barrier certificate $\{B_l(x) : l \in L\}$ 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. Condition (8) asserts that $B_{l_0}(x_0) \leq 0$. Next, (10) implies that during a segment of continuous flow $B_{l(t)}(x(t))$ cannot become positive, which can be shown using Proposition 3. On the other hand, (11) 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 (8). We conclude that the safety of the system is guaranteed. ∎

Similar to what we encounter in the continuous case, conditions (10)–(11) 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 theorem.

Theorem 6: Let the hybrid system H, the unsafe set $X_u \subseteq X$, and a collection of nonnegative constants $\{\lambda_{l,l'} \in \mathbb{R} : (l, l') \in L^2,\ l \neq l'\}$ be given. Suppose there exists a collection $\{B_l(x) : l \in L\}$ of differentiable functions $B_l : \mathbb{R}^n \to \mathbb{R}$ which, for all $l \in L$ and $(l, l') \in L^2$, $l \neq l'$, satisfy

$$B_l(x) \leq 0 \quad \forall x \in \text{Init}(l), \tag{12}$$

$$B_l(x) > 0 \quad \forall x \in \text{Unsafe}(l), \tag{13}$$

$$\frac{\partial B_l}{\partial x}(x) f_l(x, d) \leq 0 \quad \forall (x, d) \in I(l) \times \mathcal{D}(l), \tag{14}$$

$$B_{l'}(x') - \lambda_{l,l'} B_l(x) \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x), \text{ for all } x \in \text{Guard}(l, l'). \tag{15}$$

Then the safety of the system in the sense of Definition 4 is guaranteed.

Proof: Analogous to the proof of Theorem 5, but with Proposition 2 now being used to show that during a segment of continuous flow $B_{l(t)}(x(t))$ cannot become positive. ∎

Remark 7: The convexity of the set of barrier certificates in Theorem 6 can be established by taking two arbitrary collections $\left\{B_l^1(x) : l \in L\right\}$ and $\left\{B_l^2(x) : l \in L\right\}$ satisfying the conditions in the theorem and showing that for all $\alpha \in [0, 1]$ the collection $\left\{\alpha B_l^1(x) + (1 - \alpha) B_l^2(x) : l \in L\right\}$ satisfies the conditions as well. Note that for this convexity it is crucial that the multipliers $\lambda_{l,l'}$ are fixed in advance.

Remark 8: Two possible choices for $\lambda_{l,l'}$ are 0 and 1. The choice $\lambda_{l,l'} = 0$ corresponds to modifying (11) to $B_{l'}(x') \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x)$, for some $l \in L$ 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 $\lambda_{l,l'} = 1$ is useful for handling integral constraints, as we will shortly see.

3) Hybrid Systems with Constraints: In the remainder of this subsection we will briefly discuss how constraints can be incorporated in verification of hybrid systems. There are three kinds of constraints that can be handled: algebraic equality, algebraic inequality, and integral constraints. Here we will focus on integral constraints, as verification by explicit calculation of reachable sets is the most difficult when such constraints exist. To the best of our knowledge, the only existing literature addressing this problem is [23], in which a method for bounding an image of the flow map between two affine switching surfaces for affine hybrid systems with integral quadratic constraints is presented.

Instead of assuming that the disturbance $d(t)$ is contained in $\mathcal{D}(l(t))$, suppose now that $d(t)$ and the continuous state $x(t)$ is constrained via a "hard" integral constraint[2]

$$\int_0^t \sigma(x(\tau), d(\tau)) d\tau \geq 0 \quad \forall t \geq 0, \tag{16}$$

where $d(t)$ is again assumed to be piecewise continuous and bounded on any finite time interval. Constraints like this usually arise in systems analysis in the form of integral quadratic constraints [28] and are useful, e.g., for describing a set of norm-bounded operators (cf. the example in Section V-B), which may represent unmodelled continuous dynamics. Apart from this change, valid trajectories of the system are generated in the same manner as in Section II-B.1. Conditions guaranteeing safety when an integral constraint is present are given in the following theorem.

Theorem 9: Let the hybrid system H, the unsafe set $X_u \subseteq X$, and the constraint (16) be given, with $\sigma \in C(\mathbb{R}^{n+m}, \mathbb{R}^r)$. Suppose there exist a collection $\{B_l(x) : l \in L\}$ of functions $B_l \in C^1(\mathbb{R}^n)$ and constant multipliers $\lambda \in \mathbb{R}^r$ that satisfy

$$B_l(x) \leq 0 \quad \forall x \in \text{Init}(l), \tag{17}$$

$$B_l(x) > 0 \quad \forall x \in \text{Unsafe}(l), \tag{18}$$

$$\frac{\partial B_l}{\partial x}(x) f_l(x, d) + \lambda^T \sigma(x, d) \leq 0 \quad \forall (x, d) \in I(l) \times \mathbb{R}^m, \tag{19}$$

$$B_{l'}(x') - B_l(x) \leq 0 \quad \forall x' \in \text{Reset}(l, l')(x), \text{ for all } x \in \text{Guard}(l, l'), \tag{20}$$

$$\lambda \geq 0, \tag{21}$$

for all $l \in L$ and $(l, l') \in L^2$, $l' \neq l$. Then the safety of the system is guaranteed in the sense of Definition 4 (except that $d(t)$ is not contained in $\mathcal{D}(l(t))$, but instead must satisfy (16)).

[2]The notion "hard" here means that the constraint must be satisfied for all $t \geq 0$; a "soft" integral constraint has the form $\int_0^\infty \sigma(x(\tau), d(\tau)) d\tau \geq 0$. Some important integral constraints for robustness analysis of uncertain systems [28] are soft constraints.

Proof: Assume that a barrier certificate satisfying the above conditions can be found, but at the same time there exists a $T \geq 0$ and a valid trajectory of the hybrid system on the time interval $[0, T]$ such that $(l(t), x(t)) \in X_u$. 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 (19) and (21) we obtain

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

Now, (20) 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 $B_{l_N}(x(T)) \leq B_{l_0}(x_0)$. Using (17)–(18) we obtain a contradiction, thus proving the theorem. ∎

Remark 10: The set of $\{B_l(x) : l \in L\}$ and λ satisfying the conditions in Theorem 9 is convex.

III. Safety Verification in the Stochastic Setting

A. Continuous Systems

Consider a complete probability space $(\Omega, \mathcal{F}, P)$ and a standard $\mathbb{R}^m$-valued Wiener process $w(t)$ defined on this space. In this subsection, we will be dealing with stochastic differential equations of the form

$$dx(t) = f(x(t))dt + g(x(t))dw(t), \tag{22}$$

where $x(t) \in \mathbb{R}^n$, and $f(x)$, $g(x)$ are of appropriate dimensions. We denote the state space, the initial set, and the unsafe set respectively by $\mathcal{X}$, $\mathcal{X}_0$, and $\mathcal{X}_u$, all of which are subsets of $\mathbb{R}^n$, with $\mathcal{X}$ assumed to be bounded and $\mathcal{X}_0 \subseteq \mathcal{X},\ \mathcal{X}_u \subseteq \mathcal{X}$. To guarantee the existence and uniqueness of solution, we will also assume that both $f(x)$ and $g(x)$ satisfy the local Lipschitz continuity and the linear growth condition on $\mathcal{X}$. Since $\mathcal{X}$ is bounded, the last condition can be replaced by the boundedness of $f(x)$ and $g(x)$ on $\mathcal{X}$.

It can be shown that the process $x(t)$ described above is right continuous and a strong Markov process [30]. The generator A of the process $x(t)$ is defined as follows.

Definition 11 (Generator): The (infinitesimal) generator A of the process $x(t)$ is defined by

$$AB(x_0) = \lim_{t \downarrow 0} \frac{E[B(x(t)) \mid x(0) = x_0] - B(x_0)}{t},$$

and the domain of the generator is the set of all functions $B : \mathbb{R}^n \to \mathbb{R}$ such that the above limit exists for all x_0.

The generator can be considered as the stochastic analog of the Lie derivative, and characterizes the evolution of the expectation of $B(x(t))$ via the so-called Dynkin's formula (see, e.g., [41]):

$$E[B(\tilde{x}(t_2))|\tilde{x}(t_1)] = B(\tilde{x}(t_1)) + E[\int_{t_1}^{t_2} AB(\tilde{x}(t))dt|\tilde{x}(t_1)]$$

for $t_2 \geq t_1$ and for any function $B(x)$ in the domain of the generator.

Since in general the process $x(t)$ is not guaranteed to always lie inside the set $\mathcal{X}$, we define the stopped process corresponding to $x(t)$ and $\mathcal{X}$ as follows.

Definition 12 (Stopped Process): Suppose that τ is the first time of exit of $x(t)$ from the open set $\mathrm{int}(\mathcal{X})$. The stopped process $\tilde{x}(t)$ is defined by

$$\tilde{x}(t) = \begin{cases} x(t) & \text{for } t < \tau, \\ x(\tau) & \text{for } t \geq \tau. \end{cases}$$

The stopped process $\tilde{x}(t)$ satisfies various properties. For example, it inherits the right continuity and strong Markovian property of $x(t)$. Furthermore, in most cases the generator corresponding to $\tilde{x}(t)$ is identical to the one corresponding to $x(t)$ on the set $\mathrm{int}(\mathcal{X})$, and is equal to zero outside of the set [26]. This will be implicitly assumed throughout the chapter. Having defined the system and the stopped process $\tilde{x}(t)$, we can now formulate the safety verification problem for stochastic differential equations as follows.

Problem 13: Given the system (22) and the bounded sets $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_0 \subseteq \mathcal{X},\ \mathcal{X}_u \subseteq \mathcal{X}$, compute an upper bound for the probability of the process $\tilde{x}(t)$ to reach $\mathcal{X}_u$. In other words, find $\gamma \in [0, 1]$ such that

$$P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0 \mid \tilde{x}(0) = x_0\} \leq \gamma, \tag{23}$$

for all $x_0 \in \mathcal{X}_0$, or,

$$P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0\} \leq \gamma, \tag{24}$$

if an initial probability distribution μ_0 whose support is in $\mathcal{X}_0$ is also given for $\tilde{x}(0)$.

Obviously, the ultimate objective of safety verification is to show that the above probability is small enough, for example less than some safety margin. Hence it is of interest to obtain an upper bound γ that is as tight as possible.

In this section, our approach to solve the above problem is based on finding an appropriate barrier certificate $B(x)$ from which we can deduce an upper bound γ. As in the non-stochastic case, the approach is again analogous to using Lyapunov functions for proving stability[3]. However, instead of requiring the value of $B(\tilde{x}(t))$ to decrease along the trajectory of the system, we ask that the *expected* value of $B(\tilde{x}(t))$ decreases or stays constant as time increases. A process satisfying such a property is called a *supermartingale* [41]. In our setting, a process $B(\tilde{x}(t))$ is a supermartingale with respect to the filtration $\{\mathcal{M}_t : t \geq 0\}$ generated by the process $\tilde{x}(t)$, if $B(\tilde{x}(t))$ is $\mathcal{M}_t$-measurable for all $t \geq 0$, $E[|B(\tilde{x}(t))|] < \infty$ for all $t \geq 0$, and

$$E[B(\tilde{x}(t_2))|\tilde{x}(t_1)] \leq B(\tilde{x}(t_1))$$

[3]See, e.g., [26] for some notions of stochastic stability and stochastic Lyapunov functions.

for all $t_2 \geq t_1$. Since we will use $B(x)$ that is twice continuously differentiable and $\tilde{x}(t)$ takes its value in a bounded set $\mathcal{X}$, the first and second conditions are always fulfilled. For nonnegative supermartingales, there exists the following result, which will be used several times in this chapter.

Lemma 14 ([26]; see [15] for the discrete version): Let $B(\tilde{x}(t))$ be a supermartingale with respect to the process $\tilde{x}(t)$ and $B(x)$ be nonnegative on $\mathcal{X}$. Then for a positive λ and any initial condition $x_0 \in \mathcal{X}$,

$$P\left\{ \sup_{0\leq t<\infty} B(\tilde{x}(t)) \geq \lambda \;\middle|\; \tilde{x}(0) = x_0 \right\} \leq \frac{B(x_0)}{\lambda}. \quad (25)$$

At this point, we are ready to state and prove our first main result in the stochastic setting.

Theorem 15: Let the stochastic differential equation (22) and the bounded sets $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_0 \subseteq \mathcal{X}$, $\mathcal{X}_u \subseteq \mathcal{X}$ be given, with $f(x)$, $g(x)$ being locally Lipschitz continuous and bounded on $\mathcal{X}$. Consider the stopped process $\tilde{x}(t)$. Suppose there exists a function $B \in C^2(\mathbb{R}^n)$ such that

$$B(x) \leq \gamma \quad \forall x \in \mathcal{X}_0, \quad (26)$$

$$B(x) \geq 1 \quad \forall x \in \mathcal{X}_u, \quad (27)$$

$$B(x) \geq 0 \quad \forall x \in \mathcal{X}, \quad (28)$$

$$\frac{\partial B}{\partial x}(x) f(x) + \frac{1}{2}\mathrm{Tr}\left(g^T(x) \frac{\partial^2 B}{\partial x^2}(x) g(x) \right) \leq 0 \quad \forall x \in \mathcal{X}, \quad (29)$$

then the probability bound (23) holds. If an initial probability distribution μ_0 is given, then (27)–(29) and

$$\int_{\mathcal{X}_0} B(x) d\mu_0(x) \leq \gamma \quad (30)$$

imply that the probability bound (24) holds.

Proof: For the stochastic differential equation (22), the generator of the process is given by (see, e.g., [30])

$$AB(x) = \frac{\partial B}{\partial x}(x) f(x) + \frac{1}{2}\mathrm{Tr}\left(g^T(x) \frac{\partial^2 B}{\partial x^2}(x) g(x) \right),$$

where the domain of the generator is the set of twice continuously differentiable functions with compact support. Since $\mathcal{X}$ is bounded, we can use any $B \in C^2(\mathbb{R}^n)$. Next, using Dynkin's formula, we have for $0 \leq t_1 \leq t_2 < \infty$

$$\begin{aligned} E[B(\tilde{x}(t_2))|\tilde{x}(t_1)] &= B(\tilde{x}(t_1)) + E[\int_{t_1}^{t_2} AB(\tilde{x}(t))dt|\tilde{x}(t_1)] \\ &\leq B(\tilde{x}(t_1)), \end{aligned}$$

and therefore (29) will imply that $B(\tilde{x}(t))$ is a supermartingale. By (28) and Lemma 14 we conclude that (25) holds. Now use (26) and the fact that $\mathcal{X}_u \subseteq \{x \in \mathcal{X} : B(x) \geq 1\}$, which follows from (27), to obtain the following series of inequalities:

$$\begin{aligned} &P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0 \mid \tilde{x}(0) = x_0\} \\ &\quad \leq P\left\{ \sup_{0\leq t<\infty} B(\tilde{x}(t)) \geq 1 \;\middle|\; \tilde{x}(0) = x_0 \right\} \\ &\quad \leq B(x_0) \leq \gamma \quad \forall x_0 \in \mathcal{X}_0. \end{aligned}$$

Thus the probability bound (23) is proven.

Finally, if an initial probability distribution μ_0 is given, then the above derivation can be combined with the law of total probability and (30) to obtain

$$P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0\} \leq \int_{\mathcal{X}_0} B(x) d\mu_0(x) \leq \gamma,$$

hence finishing the proof. ∎

Note that it is possible to choose γ to be at most equal to one, since when $\gamma = 1$ the function $B(x) = 1$ will satisfy (26)–(29) and (30). The intuitive idea behind the theorem is clear. The process $B(\tilde{x}(t))$ is a supermartingale, and therefore its value is likely to stay constant or decrease as time increases. When we start from a lower initial value of $B(x)$ (i.e., as γ gets smaller) it becomes less likely for the trajectory to reach the unsafe set, on which the value of $B(x)$ is greater than or equal to one. This is quantified by Lemma 14, which provides a Chebyshev-like inequality for bounding the probability of the distribution tail.

B. Hybrid Systems

In this subsection, we consider a class of stochastic hybrid systems called the switching diffusion processes [16]. Systems in this class have both continuous and discrete states, where the continuous state differential equation that depends on the discrete state, and the discrete trajectory itself is a Markov chain whose transition matrix depends on the continuous state. As implied by the name, these systems are switching systems, meaning that the value of the continuous state does not change during a discrete transition. The method proposed in Section III-A can be extended to handle switching diffusion processes. The main idea is similar to before, i.e., use the appropriate generator for the process, find a barrier certificate from the domain of the generator that yields a supermartingale, and then bound the reach probability using the barrier certificate.

Formally, a switching diffusion process is a tuple $H = (\mathcal{X}, L, \mu_0, f_l, g_l, \lambda_{ll'})$ with the following components:

- $\mathcal{X} \subseteq \mathbb{R}^n$ is the continuous state space, assumed to be bounded.
- L is a finite set of locations. The overall state space of the system is $X = L \times \mathcal{X}$, and the state is denoted by $(l, x) \in L \times \mathcal{X}$.
- μ_0 is an initial probability measure, with its support in $X_0 \subseteq X$.
- $f_l : \mathcal{X} \to \mathbb{R}^n$, $l \in L$, is a set of drift vector fields.
- $g_l : \mathcal{X} \to \mathbb{R}^{n\times m}$, $l \in L$, is a set of diffusion coefficients, where the i-th column of g_l corresponds to the i-th component of the $\mathbb{R}^m$-valued Wiener process $w(t)$.
- $\lambda_{ll'} : \mathcal{X} \to \mathbb{R}$, $(l, l') \in L^2$, is a set of x-dependent transition rates, with $\lambda_{ll'}(x) \geq 0$ for all x if $l \neq l'$, and $\sum_{l' \in L} \lambda_{ll'}(x) = 0$ for all $l \in L$.

Here we denote the unsafe set by $\mathcal{X}_u$, with $\mathcal{X}_u \subseteq \mathcal{X}$.

A trajectory of the system starts with an initial condition drawn from the initial probability measure μ_0. As mentioned above, the continuous part of the state evolves according to a stochastic differential equation, which at location l is given by

$$dx(t) = f_l(x(t))dt + g_l(x(t))dw(t).$$

On the other hand, the dynamics of the discrete state is described by the following transition probability:

$$P\{l(t+\Delta)=j \mid l(t)=i\} = \begin{cases} \lambda_{ij}(x(t))\Delta + o(\Delta), & \text{if } i \neq j, \\ 1+\lambda_{ii}(x(t))\Delta + o(\Delta), & \text{if } i=j, \end{cases}$$

with $\Delta > 0$. See [16] for more details on how the discrete transitions are generated. During a discrete transition, the value of the continuous state is held constant. It is assumed that the discrete transition is independent from the Wiener process $w(t)$. In addition, we assume that $f_l(x)$, $g_l(x)$, and $\lambda_{ll'}(x)$ are bounded and locally Lipschitz continuous. Under these assumptions, the solution to the stochastic differential equation at each location exists and is unique, and also that $(l(t), x(t))$ is a Markov process and almost every sample path of it is a right continuous function [16]. Similar to the continuous case, we stop the process when $x(t)$ goes out from int($\mathcal{X}$).

The conditions for a barrier certificate are stated in the following theorem.

Theorem 16: Let the switching diffusion process $H = (\mathcal{X}, L, \mu_0, f_l, g_l, \lambda_{ll'})$ be given, with bounded $\mathcal{X}$ and bounded, locally Lipschitz continuous $f_l(x)$'s, $g_l(x)$'s, and $\lambda_{ll'}(x)$'s. Suppose there exists a collection $\{B_l(x) : l \in L\}$ of functions $B_l \in C^2(\mathbb{R}^n)$, which satisfy

$$B_l(x) \geq 1 \quad \forall x \in \mathcal{X}_u, \tag{31}$$

$$B_l(x) \geq 0 \quad \forall x \in \mathcal{X}, \tag{32}$$

$$\frac{\partial B_l}{\partial x}(x) f_l(x) + \frac{1}{2}\mathrm{Tr}\left(g_l^T(x)\frac{\partial^2 B_l}{\partial x^2}(x) g_l(x)\right) + \sum_{l' \in L} \lambda_{ll'}(x) B_{l'}(x) \leq 0 \quad \forall x \in \mathcal{X}, \tag{33}$$

for all $l \in L$, and

$$\sum_{l \in L} \int_{\mathcal{X}} B_l(x) d\mu_0(l, x) \leq \gamma. \tag{34}$$

Then $P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0\} \leq \gamma$.

Proof: Define $B(l(t), x(t)) = B_{l(t)}(x(t))$. In this case,

$$AB(l,x) = \frac{\partial B_l}{\partial x}(x) f_l(x) + \frac{1}{2}\mathrm{Tr}\left(g_l^T(x)\frac{\partial^2 B_l}{\partial x^2}(x) g_l(x)\right) + \sum_{l' \in L} \lambda_{ll'}(x) B_{l'}(x)$$

is the generator of the process, and $B(l,x)$ is in the domain of the generator if $B_l \in C^2(\mathbb{R}^n)$ $\forall l \in L$. See [16]. Condition (33) implies that $B(l(t), x(t))$ is a supermartingale, which can be shown using Dynkin's formula. Since $B(l(t), x(t))$ is also nonnegative (as implied by (32)), Lemma 14 can be applied. The rest of the proof is similar to the proof of Theorem 15. ∎

In principle, other classes of stochastic hybrid systems such as piecewise deterministic Markov processes [14], stochastic hybrid systems of Hu et al. [19], and stochastic hybrid systems of Hespanha [18] can be handled in a similar fashion, by using the suitable generator for each class and modifying the other conditions for $B_l(x)$ appropriately.

IV. Computational Method

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 for constructing a barrier certificate exists if we also postulate the barrier certificate to be polynomial. The method uses sum of squares optimization [31], [32], [38], [39] — a convex relaxation framework based on sum of squares decompositions of multivariate polynomials [40] and semidefinite programming [48].

A sum of squares (SOS) program is a convex optimization problem of the following form:

$$\text{Minimize } \sum_{j=1}^{m} w_j c_j$$

subject to

$$a_{i,0}(x) + \sum_{j=1}^{m} a_{i,j}(x) c_j \text{ is SOS, for } i = 1, ..., p,$$

where the c_j's are scalar real decision variables, the w_j's are given real numbers, and the $a_{i,j}(x)$ are given polynomials (with fixed coefficients). See also another equivalent canonical form of SOS programs in [38]. Here we say that the polynomial $f(x) = a_{i,0}(x) + \sum_{j=1}^{m} a_{i,j}(x) c_j$ is an SOS if it can be decomposed as $f(x) = \sum_{k=1}^{\ell} f_k^2(x)$ for some polynomials $f_k(x)$, $k = 1, \ldots, \ell$. Sum of squares programs can be solved via semidefinite programming, e.g., using the software SOSTOOLS [38], [39] in conjunction with a semidefinite programming solver such as SeDuMi [43].

A. Direct Computation of Barrier Certificates

The setting of Section II-B.2 is used in this and the next subsections; other settings can be treated analogously. Consider a hybrid system H whose vector fields $f_l(x, d)$ are polynomial for all $l \in L$. Furthermore, assume that for all $l \in L$ the invariant region $I(l)$ is given by

$$I(l) = \{x \in \mathbb{R}^n : g_{I(l)}(x) \geq 0\}.$$

In these set descriptions, the $g_{I(l)}$'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 $\mathcal{D}(l)$, Init(l), Unsafe(l), and Guard(l, l') by the inequalities $g_{\mathcal{D}(l)}(d) \geq 0$, $g_{\text{Init}(l)}(x) \geq 0$, $g_{\text{Unsafe}(l)}(x) \geq 0$, and $g_{\text{Guard}(l,l')}(x) \geq 0$. Finally, assume

$$\text{Reset}(l, l')(x) = \{x' \in \mathbb{R}^n : g_{\text{Reset}(l,l')}(x, x') \geq 0\}$$

to be the value of the reset map Reset(l, l') evaluated at $x \in$ Guard(l, l').

To compute a polynomial barrier certificate for this system, real coefficients $c_{1,l}, ..., c_{m,l}$ are used to parameterize sets of

candidates for the functions $B_l(x)$, $\forall l \in L$, in the following way:

$$B_l(x) = \sum_j c_{j,l} b_{j,l}(x), \tag{35}$$

where the $b_{j,l}(x)$'s are elements of some finite polynomial basis; for example, they could be monomials of degree less than or equal to some pre-chosen bound. Then the search for a barrier certificate $\{B_l(x) : l \in L\}$, or equivalently the values of $c_{j,l}$'s, such that the convex conditions in Theorem 6 are satisfied can be directly performed by solving a SOS program, as stated in the following algorithm.

Algorithm 17 (Direct Method): Let the hybrid system H and the descriptions of $I(l)$, $\mathcal{D}(l)$, $\mathrm{Init}(l)$, $\mathrm{Unsafe}(l)$, $\mathrm{Guard}(l,l')$, and $\mathrm{Reset}(l,l')(x)$ be given, along with some nonnegative constants $\lambda_{l,l'}$, for each $l \in L$ and $(l,l') \in L^2$, $l \neq l'$.

1) **Parameterize $B_l(x)$'s:** Fix a degree bound for the barrier certificate, and parameterize $B_l(x)$ $\forall l \in L$ in terms of some unknown coefficients $c_{j,l}$'s as in (35), by having all monomials whose degrees are less than the degree bound as the $b_{j,l}(x)$'s.
2) **Parameterize the multipliers:** In a similar way, fix some degree bounds and use some other unknown coefficients to parameterize polynomial vectors $\lambda_{\mathrm{Init}(l)}(x)$, $\lambda_{\mathrm{Unsafe}(l)}(x)$, $\lambda_{I(l)}(x,d)$, $\lambda_{\mathcal{D}(l)}(x,d)$, $\lambda_{\mathrm{Guard}(l,l')}(x,x')$, $\lambda_{\mathrm{Reset}(l,l')}(x,x')$ of the same dimensions as the corresponding $g_*(\cdot)$'s.
3) **Compute the coefficients:** Choose a small positive number ϵ. Use SOS optimization to find values of the coefficients which make the expressions

$$-B_l(x) - \lambda^T_{\mathrm{Init}(l)}(x) g_{\mathrm{Init}(l)}(x), \tag{36}$$

$$+B_l(x) - \epsilon - \lambda^T_{\mathrm{Unsafe}(l)}(x) g_{\mathrm{Unsafe}(l)}(x), \tag{37}$$

$$-\frac{\partial B_l}{\partial x}(x) f_l(x,d) - \lambda^T_{I(l)}(x,d) g_{I(l)}(x) - \lambda^T_{D(l)}(x,d) g_{D(l)}(d), \tag{38}$$

$$-B_{l'}(x') + \lambda_{l,l'} B_l(x) - \lambda^T_{\mathrm{Guard}(l,l')}(x,x') g_{\mathrm{Guard}(l,l')}(x) - \lambda^T_{\mathrm{Reset}(l,l')}(x,x') g_{\mathrm{Reset}(l,l')}(x,x') \tag{39}$$

and the entries of $\lambda_{\mathrm{Init}(l)}(x)$, $\lambda_{\mathrm{Unsafe}(l)}(x)$, $\lambda_{I(l)}(x,d)$, $\lambda_{\mathcal{D}(l)}(x,d)$, $\lambda_{\mathrm{Guard}(l,l')}(x,x')$, $\lambda_{\mathrm{Reset}(l,l')}(x,x')$ sums of squares, for each $l \in L$ and $(l,l') \in L^2$, $l \neq l'$.

Proposition 18: If the sum of squares optimization problem given in Algorithm 17 is feasible, then the polynomials $\{B_l(x) : l \in L\}$ obtained by substituting the corresponding values of $c_{j,l}$'s to their polynomial parameterization satisfy the conditions of Theorem 6, and therefore $\{B_l(x) : l \in L\}$ is a barrier certificate.

Proof: We show that the entries of $\lambda_{\mathrm{Init}(l)}(x)$ and (36) being SOS implies (8) as follows. Notice that $-B_l(x) - \lambda^T_{\mathrm{Init}(l)}(x) g_{\mathrm{Init}(l)}(x)$ is globally nonnegative since it is a SOS and also that for any $x \in \mathrm{Init}(l)$ the second term is nonnegative. Thus $-B_l(x) \geq \lambda^T_{\mathrm{Init}(l)}(x) g_{\mathrm{Init}(l)}(x) \geq 0 \quad \forall x \in \mathrm{Init}(l)$, i.e., condition (8) holds. Similar arguments can be used for the other conditions. ∎

Remark 19: If the reset map $\mathrm{Reset}(l,l')$ actually maps $x \in \mathrm{Guard}(l,l')$ to a singleton, e.g., if $\mathrm{Reset}(l,l') : x \mapsto g_{\mathrm{Reset}(l,l')}(x)$ for some polynomial vector $g_{\mathrm{Reset}(l,l')}(x)$, then expression (39) can be simplified to $-B_{l'}(g_{\mathrm{Reset}(l,l')}(x)) + \lambda_{l,l'} B_l(x) - \lambda^T_{\mathrm{Guard}(l,l')}(x) g_{\mathrm{Guard}(l,l')}(x)$.

The computational cost of Algorithm 17 depends on three factors: the degrees of (36)–(39), the cardinality of L, and the dimension of (x,d). For fixed degrees, however, the required computations grow polynomially with respect to the cardinality of L and/or the dimension of (x,d). A hierarchy of computations can then be proposed, where we start with a low degree for the barrier certificate and increase it as needed. In many cases, a low degree barrier certificate can be used to verify safety if the system is "sufficiently" safe (in the sense that a small perturbation will not make the system unsafe).

B. Iterative Computation

The SOS optimization approach described in the previous subsection can be used to find a barrier certificate that lies in the *convex* set defined by the conditions in Theorem 6. The conditions in Theorem 5, however, define a *non-convex* set of barrier certificate. As a consequence, the search for a barrier certificate in this set cannot be performed through direct SOS optimization, although conditions for the barrier certificate can still be formulated as sum of squares conditions as follows.

Proposition 20: Let the hybrid system H and the descriptions of $I(l)$, $\mathcal{D}(l)$, $\mathrm{Init}(l)$, $\mathrm{Unsafe}(l)$, $\mathrm{Guard}(l,l')$, and $\mathrm{Reset}(l,l')(x)$ be given. Suppose there exist polynomials $B_l(x)$ and $\lambda_{B_l}(x,d)$; positive numbers ϵ_1 and ϵ_2; and vectors of sums of squares $\lambda_{\mathrm{Unsafe}(l)}(x)$, $\lambda_{\mathrm{Init}(l)}(x)$, $\lambda_{I(l)}(x,d)$, $\lambda_{\mathcal{D}(l)}(x,d)$, $\lambda_{\mathrm{Guard}(l,l')}(x,x')$, $\lambda_{\mathrm{Reset}(l,l')}(x,x')$, and $\lambda_{l,l'}(x,x')$; such that the following expressions:

$$-B_l(x) - \lambda^T_{\mathrm{Init}(l)}(x) g_{\mathrm{Init}(l)}(x), \tag{40}$$

$$+B_l(x) - \epsilon_1 - \lambda^T_{\mathrm{Unsafe}(l)}(x) g_{\mathrm{Unsafe}(l)}(x), \tag{41}$$

$$-\frac{\partial B_l}{\partial x}(x) f_l(x,d) - \epsilon_2 - \lambda^T_{D(l)}(x,d) g_{D(l)}(d) - \lambda^T_{I(l)}(x,d) g_{I(l)}(x) - \lambda_{B_l}(x,d) B_l(x), \tag{42}$$

$$-B_{l'}(x') + \lambda_{l,l'}(x,x') B_l(x) - \lambda^T_{\mathrm{Guard}(l,l')}(x,x') g_{\mathrm{Guard}(l,l')}(x) - \lambda^T_{\mathrm{Reset}(l,l')}(x,x') g_{\mathrm{Reset}(l,l')}(x,x') \tag{43}$$

are sums of squares for all $l \in L$ and $(l,l') \in L^2$, $l \neq l'$. Then the collection $\{B_l(x) : l \in L\}$ satisfies the conditions in Theorem 5, and therefore the safety property holds.

Proof: Analogous to the proof of Proposition 18. ∎

In this case, direct computation of $\{B_l(x) : l \in L\}$ via SOS optimization is impossible due to the multiplication of the unknown coefficients of $B_l(x)$'s with those of $\lambda_{B_l}(x,d)$'s and $\lambda_{l,l'}(x,x')$'s in (42)–(43). By fixing either of them, all the unknown coefficients will be constrained in an affine manner, which reduces the problem[4] to a SOS program. For example, fixing the multipliers will convexify the set of $\{B_l(x) : l \in$

[4]Note that the original problem is actually equivalent to a bilinear matrix inequality (BMI) problem [29].

$L\}$'s satisfying the conditions (40)–(43), resulting in a smaller convex set contained in the original non-convex set.

The motivation to search for barrier certificates in the original non-convex set is that when we put a bound on their complexity (e.g., by bounding the polynomial degrees), such barrier certificates are generally less conservative than barrier certificates in the convex set (cf. the comment at the beginning of Section II-A.2). For instance, the former may prove safety for larger disturbance sets, guard sets, unsafe sets, etc. We will now present a simple iterative method to search for a barrier certificate in the non-convex set. In the iteration we start with some sufficiently small sets, and increase their sizes as the iteration progresses.

Algorithm 21 (Iterative Method):

1) **Initialization:** Start with sufficiently small $\mathcal{D}(l)$, 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 $B_l(x)$'s and the remaining multipliers using SOS optimization as described in Algorithm 17.
2) **Fix the barrier certificate:** Fix the $B_l(x)$'s obtained from the previous step. Enlarge $\mathcal{D}(l)$, Guard(l,l'), etc. Search for $\lambda_{B_l}(x,d)$'s, $\sigma_{l,l'}(x,x')$'s, and the remaining multipliers.
3) **Fix the multipliers:** Fix the $\lambda_{B_l}(x,d)$'s and $\sigma_{l,l'}(x,x')$'s obtained from the previous step. Enlarge $\mathcal{D}(l)$, Guard(l,l'), etc. Search for $B_l(x)$'s and the remaining multipliers. Repeat to Step 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.

C. Computation of Barrier Certificates for Stochastic Systems

When the description of the stochastic differential equation in Section III-A is polynomial and the sets are semialgebraic, an upper bound γ and a polynomial barrier certificate $B(x)$ which certifies the upper bound can be computed by formulating conditions (26)–(29) or (27)–(29) and (30) as a sum of squares optimization problem, similar to what we describe in Section IV-A. Furthermore, γ can be chosen as the objective function of the SOS program, whose value is to be minimized. The minimum value of γ obtained from the optimization will be the tightest upper bound for a given polynomial and sum of squares parameterization. Obviously we may get a better bound as we expand the parameterization, for example, when we use higher degree barrier certificates. However, there is a trade-off between using a larger set of candidate barrier certificates and the computational complexity of finding a true certificate within it.

Similar to the stochastic differential equation case, a polynomial barrier certificate $\{B_l(x) : l \in L\}$ for a switching diffusion processes can be computed using sum of squares optimization, provided $f_l(x)$, $g_l(x)$, and $\lambda_{ll'}(x)$ are polynomials and the sets $\mathcal{X}$, $\mathcal{X}_u$ are semialgebraic.

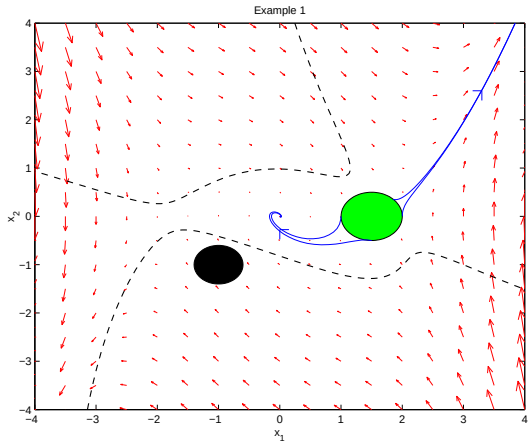

Fig. 1. Phase portrait of the system in Section V-A. Solid patches are (from left to right) $\mathcal{X}_u$ and $\mathcal{X}_0$, respectively. Dashed curves are the zero level set of $B(x)$, whereas solid curves are some trajectories of the system. The function $B(x)$ is strictly greater than zero for all $x \in \mathcal{X}_u$ and strictly less than zero for all $x \in \mathcal{X}_0$.

V. Examples

Here we will present two examples in the worst-case setting and one example in the stochastic setting. More examples can be found in [36], [37]. For an application to a NASA life support system, which is a hybrid system with 6 discrete locations and 10 continuous state variables, see [17].

A. Continuous System

Consider the two-dimensional system (taken from [24, page 180])

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} x_2 \\ -x_1 + \frac{1}{3}x_1^3 - x_2 \end{bmatrix},$$

with $\mathcal{X} = \mathbb{R}^2$. We want to verify that all trajectories of the system starting from the initial set $\mathcal{X}_0 = \{x \in \mathbb{R}^2 : (x_1 - 1.5)^2 + x_2^2 \leq 0.25\}$ will never reach the unsafe set $\mathcal{X}_u = \{x \in \mathbb{R}^2 : (x_1+1)^2 + (x_2+1)^2 \leq 0.16\}$. Note that the system has a stable focus at the origin and two saddle points at $(\pm\sqrt{3}, 0)$. Since $\mathcal{X}_0$ contains a 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.

A polynomial barrier certificate $B(x)$ that satisfies (2)–(4) is given by, e.g., $B(x) = -13 + 7x_1^2 + 16x_2^2 - 6x_1^2x_2^2 - \frac{7}{6}x_1^4 - 3x_1x_2^3 + 12x_1x_2 - \frac{12}{3}x_1^3x_2$. For example, that the Lie derivative $\frac{\partial B}{\partial x}f(x)$ is less than or equal to zero can be shown by exhibiting the quadratic form $-\frac{\partial B}{\partial x}f(x) = Z(x)^T Q Z(x)$, with

$$Q = \begin{bmatrix} 20 & 0 & 15 & 0 & -15/2 & -5 \\ 0 & 3 & 0 & 3/2 & 0 & 0 \\ 15 & 0 & 12 & 0 & -6 & -4 \\ 0 & 3/2 & 0 & 6 & 0 & 0 \\ -15/2 & 0 & -6 & 0 & 3 & 2 \\ -5 & 0 & -4 & 0 & 2 & 4/3 \end{bmatrix},$$

and $Z(x) = \mathrm{col}(x_2, x_2^2, x_1, x_1x_2, x_1^2x_2, x_1^3)$. In this case, the matrix Q is positive semidefinite, which implies the existence

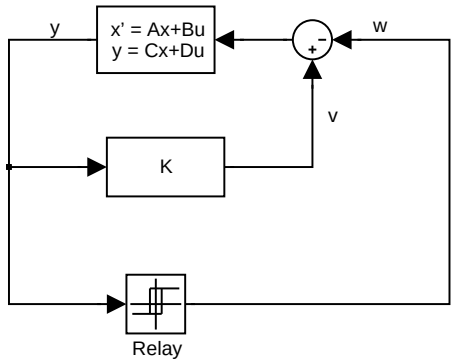

Fig. 2. Block diagram of the system in Section V-B. We ask if it is possible to design a controller K that steers the system from an initial set $\mathcal{X}_0$ to a destination set $\mathcal{X}_u$, subject to some other specifications.

of a sum of squares decomposition for $-\frac{\partial B}{\partial x} f(x)$ (and hence its nonnegativity). That (2)–(3) are satisfied can be shown by sum of squares arguments as well, and is also depicted pictorially in Figure 1. The zero level set of the barrier certificate separates $\mathcal{X}_u$ from all trajectories starting from $\mathcal{X}_0$. Hence the safety of the system is verified.

B. Hybrid System with Integral Constraint

This example illustrates a possible application of safety verification techniques to determine limit of design. More specifically, we will analyze the reachability property of a linear system in feedback interconnection with a relay. The block diagram of the system is shown in Figure 2, with the matrices A, B, C, and D given by

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

and the relay element having the following characteristic:

$$w = \begin{cases} 10, & \text{if } y \geq 0, \\ -10, & \text{if } y < 0. \end{cases}$$

For the sets

$$\mathcal{X} = \{x \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 \leq 4^2\},$$
$$\mathcal{X}_0 = \{x \in \mathbb{R}^3 : (x_1 + 2)^2 + x_2^2 + x_3^2 \leq 0.1^2\},$$
$$\mathcal{X}_u = \{x \in \mathbb{R}^3 : (x_1 - 2)^2 + x_2^2 + x_3^2 \leq 0.1^2\},$$

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 $\mathcal{X}$?

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) [28]

$$\int_0^T [y^2(t) - v^2(t)]dt \geq 0 \qquad \forall T \geq 0.$$

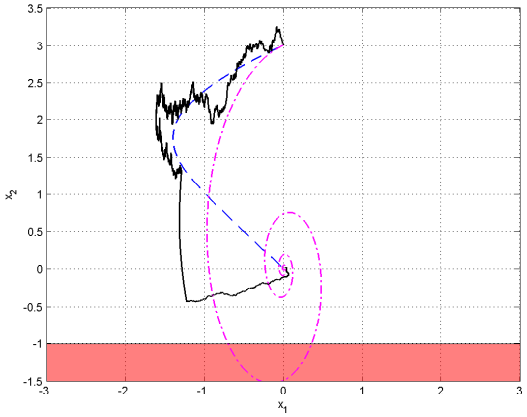

Fig. 3. Phase portrait of the system in Section V-C. Trajectories of the systems $\dot{x} = A_1 x$ and $\dot{x} = A_2 x$ starting at $x(0) = (0, 3)$ are shown by the dashed and dash-dotted curves, respectively. A realization of the switching diffusion process for $\lambda = 10$ is depicted by the solid curve. Shaded region at the bottom of the figure is the unsafe set.

This specification introduces dynamic uncertainty to the problem. 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 9). 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.

C. Switching Diffusion Process

In this example, we consider the system

$$dx(t) = A_{l(t)}x(t) + \sigma(x(t))dw(t),$$

where $l(t) \in \{1, 2\}$ and

$$A_1 = \begin{bmatrix} -5 & -4 \\ -1 & -2 \end{bmatrix}, \; A_2 = \begin{bmatrix} -2 & -4 \\ 20 & -2 \end{bmatrix}, \; \sigma(x) = \begin{bmatrix} 0 \\ 0.5x_2 \end{bmatrix}.$$

It can be shown using a common polynomial Lyapunov function of degree six that the deterministic system corresponding to $\sigma(x) = 0$ is globally asymptotically stable under arbitrary switching.

We assume that the initial condition is given by $l(0) = 1$ or 2, with equal probability for both locations, and $x(0) = (0, 3)$. For the initial continuous condition $x(0) = (0, 3)$, trajectories of the deterministic system corresponding to the first and second locations are shown in Figure 3. We choose $\mathcal{X} = \{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 \leq 4^2, -1.5 \leq x_2 \leq 4\}$ as the set of continuous states, and $\mathcal{X}_u = \{(x_1, x_2) \in \mathcal{X} : x_2 \leq -1\}$ as the unsafe set. The safety of the stochastic system with transition rates $\lambda_{11} = -0.5$, $\lambda_{12} = 0.5$, $\lambda_{21} = \lambda$, $\lambda_{22} = -\lambda$, is to be verified, where the nonnegative parameter λ will be varied. Larger λ means that from location 2 the system tends to switch to location 1 faster.

This problem can be given the following interpretation. Although in both locations the system will evolve toward the origin, location 2 is different from location 1 in the sense that it has an oscillatory response which tends to bring the system to the unsafe region whereas the trajectory corresponding to

location 1 will evolve directly to the origin without going through the unsafe region. In the verification, we will show that by using a large λ, i.e., making the system be in location 1 for most of the time, the probability of reaching the unsafe set can be kept small.

Using polynomial barrier certificates of degree 10, we can prove that the probability of reaching the unsafe region is bounded by $\gamma = 0.346$ for $\lambda = 10$, $\gamma = 0.145$ for $\lambda = 20$, and $\gamma = 0.069$ for $\lambda = 30$. As expected, the probability bound decreases when we increase λ.

VI. Conclusions

We have presented in the previous sections a framework based on deductive inference and functions of states termed barrier certificates for verifying system safety in the worst-case and stochastic settings. In the worst-case setting, such property can be verified without explicitly computing the set of reachable states. This makes the methodology directly applicable to continuous and hybrid systems with nonlinear, uncertain, and constrained dynamics. In addition, by using barrier certificates that generate nonnegative supermartingales under the given system dynamics, we are able to handle safety verification of stochastic continuous and hybrid systems by computing certified upper bounds on the probability of reaching the unsafe region.

Most of the conditions satisfied by barrier certificates form convex optimization problems. When the system is described in terms of polynomials, this provides the possibility to search for appropriate barrier certificates using a convex relaxation framework called sum of squares optimization. For non-convex conditions, an iterative method for computing barrier certificates has also been proposed. A hierarchical search based on bounding the degrees of the polynomial expressions can be performed, such that at each level the complexity grows polynomially with respect to the system size. Some examples have been presented to illustrate the use of the proposed methodology.

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, Heidelberg, 2003.

[3] R. Alur, T. Henzinger, G. Lafferriere, and G. J. Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88(2):971–984, 2000.

[4] 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, Heidelberg, 2001.

[5] E. Asarin, T. Dang, and A. Girard. Reachability analysis of nonlinear systems using conservative approximation. In *Hybrid Systems: Computation and Control, LNCS 2623*, pages 20–35. Springer-Verlag, Heidelberg, 2003.

[6] 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, Heidelber, 2002.

[7] J.-P. Aubin. *Viability Theory*. Birkhäuser, Boston, MA, 1991.

[8] 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, Heidelberg, 2000.

[9] F. Blanchini. Set invariance in control. *Automatica*, 35(11):1747–1767, 1999.

[10] 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, Heidelberg, 2000.

[11] M. L. Bujorianu. Extended stochastic hybrid systems and their reachability problem. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 234–249. Springer-Verlag, Heidelberg, 2004.

[12] M. L. Bujorianu and J. Lygeros. Reachability questions in piecewise deterministic Markov processes. In *Hybrid Systems: Computation and Control, LNCS 2623*, pages 126–140. Springer-Verlag, Heidelberg, 2003.

[13] A. Chutinan and B. H. Krogh. Computational techniques for hybrid system verification. *IEEE Transactions on Automatic Control*, 48(1):64–75, 2003.

[14] M. H. A. Davis. *Markov Processes and Optimization*. Chapman-Hall, London, 1993.

[15] G. A. Edgar and L. Sucheston. *Stopping Times and Directed Processes*. Cambridge University Press, Cambridge, 1992.

[16] M. K. Ghosh, A. Arapostathis, and S. I. Marcus. Optimal control of switching diffusions with application to flexible manufacturing systems. *SIAM Journal on Control and Optimization*, 31(5):1183–1204, 1993.

[17] S. Glavaski, A. Papachristodoulou, and K. Ariyur. Controlled hybrid system safety verification: Advanced life support system testbed. Submitted to American Control Conference, 2005.

[18] J. P. Hespanha. Stochastic hybrid systems: Application to communication networks. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 387–401. Springer-Verlag, Heidelberg, 2004.

[19] J. Hu, J. Lygeros, and S. Sastry. Towards a theory of stochastic hybrid systems. In *Hybrid Systems: Computation and Control, LNCS 1790*, pages 160–173. Springer-Verlag, Heidelberg, 2000.

[20] J. Hu, M. Prandini, and S. Sastry. Probabilistic safety analysis in three dimensional aircraft flight. In *Proceedings of the IEEE Conference on Decision and Control*, 2003.

[21] M. Jirstrand. Invariant sets for a class of hybrid systems. In *Proceedings of the IEEE Conference on Decision and Control*, 1998.

[22] M. Johansson and A. Rantzer. Computation of piecewise quadratic Lyapunov functions for hybrid systems. *IEEE Transactions on Automatic Control*, 43(4):555–559, 1998.

[23] U. T. Jönsson. On reachability analysis of uncertain hybrid systems. In *Proceedings of the IEEE Conference on Decision and Control*, 2002.

[24] H. K. Khalil. *Nonlinear Systems*. Prentice-Hall, Inc., Upper Saddle River, NJ, second edition, 1996.

[25] A. Kurzhanski and P. Varaiya. Ellipsoidal techniques for reachability analysis. In *Hybrid Systems: Computation and Control, LNCS 1790*, pages 202–214. Springer-Verlag, Heidelberg, 2000.

[26] H. J. Kushner. *Stochastic Stability and Control*. Academic Press, New York, 1967.

[27] G. Lafferriere, G. J. Pappas, and S. Yovine. Symbolic reachability computations for families of linear vector fields. *Journal of Symbolic Computation*, 32(3):231–253, 2001.

[28] A. Megretski and A. Rantzer. System analysis via integral quadratic constraints. *IEEE Transactions on Automatic Control*, 42(6):819–830, 1997.

[29] M. Mesbahi, M. G. Safonov, and G. P. Papavassilopoulos. Bilinearity and complementarity in robust control. In *Advances in Linear Matrix Inequality Methods in Control*, pages 269–292. SIAM, Philadelphia, PA, 2000.

[30] B. Øksendal. *Stochastic Differential Equations: An Introduction with Applications*. Springer-Verlag, Berlin, 2000.

[31] P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, Pasadena, CA, 2000.

[32] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming Series B*, 96(2):293–320, 2003.

[33] G. Pola, M. L. Bujorianu, J. Lygeros, and M. D. Di Benedetto. Stochastic hybrid models: An overview. In *Proceedings IFAC Conference on Analysis and Design of Hybrid Systems*, 2003.

[34] S. Prajna. Barrier certificates for nonlinear model validation. In *Proceedings of the IEEE Conference on Decision and Control*, 2003.

[35] S. Prajna. *Optimization-Based Methods for Nonlinear and Hybrid Systems Verification*. PhD thesis, California Institute of Technology, Pasadena, CA, 2005.

[36] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 477–492. Springer-Verlag, Heidelberg, 2004.

[37] S. Prajna, A. Jadbabaie, and G. J. Pappas. Stochastic safety verification using barrier certificates. In *Proceedings of the IEEE Conference on Decision and Control*, 2004.

[38] S. Prajna, A. Papachristodoulou, and P. A. Parrilo. Introducing SOSTOOLS: A general purpose sum of squares programming solver. In *Proceedings of the IEEE Conference on Decision and Control*, 2002. Software available at `http://www.cds.caltech.edu/sostools` and `http://www.mit.edu/~parrilo/sostools`.

[39] S. Prajna, A. Papachristodoulou, P. Seiler, and P. A. Parrilo. SOSTOOLS and its control applications. In *Positive Polynomials in Control*. Springer-Verlag, 2005. To appear.

[40] B. Reznick. Some concrete aspects of Hilbert's 17th Problem. In *Real Algebraic Geometry and Ordered Structures*, pages 251–272. American Mathematical Society, Providence, RI, 2000.

[41] L. C. G. Rogers and D. Williams. *Diffusions, Markov Processes and Martingales. Volume 1: Foundations*. Cambridge University Press, Cambridge, 2000.

[42] S. Sankaranarayanan, H. Sipma, and Z. Manna. Constructing invariants for hybrid systems. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 539–554. Springer-Verlag, Heidelberg, 2004.

[43] J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11–12:625–653, 1999. Software available at `http://fewcal.kub.nl/sturm/software/sedumi.html`.

[44] A. Tiwari. Approximate reachability for linear systems. In *Hybrid Systems: Computation and Control, LNCS 2623*, pages 514–525. Springer-Verlag, Heidelberg, 2003.

[45] A. Tiwari and G. Khanna. Series of abstractions for hybrid automata. In *Hybrid Systems: Computation and Control, LNCS 2289*, pages 465–478. Springer-Verlag, Heidelberg, 2002.

[46] A. Tiwari and G. Khanna. Nonlinear systems: Approximating reach sets. In *Hybrid Systems: Computation and Control, LNCS 2993*, pages 600–614. Springer-Verlag, Heidelberg, 2004.

[47] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.

[48] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[49] O. Watkins and J. Lygeros. Stochastic reachability for discrete time systems: An application to aircraft collision avoidance. In *Proceedings IEEE Conference on Decision and Control*, 2003.

[50] H. Yazarel and G. J. Pappas. Geometric programming relaxations for linear systems reachability. In *Proceedings of the American Control Conference*, 2004.

[51] H. Yazarel, S. Prajna, and G. J. Pappas. SOS for safety. In *Proceedings of the IEEE Conference on Decision and Control*, 2004.