43rd IEEE Conference on Decision and Control
December 14-17, 2004
Atlantis, Paradise Island, Bahamas

Stochastic Safety Verification Using Barrier Certificates

Stephen Prajna, Ali Jadbabaie, and George J. Pappas

Abstract— **We develop a new method for safety verification of stochastic systems based on functions of states termed barrier certificates. Given a stochastic continuous or hybrid system and sets of initial and unsafe states, 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, both the upper bound and its corresponding barrier certificate can be computed using convex optimization, and hence the method is computationally tractable.**

I. Introduction

Complex behaviors that can be exhibited by modern engineering systems, which typically have hybrid (i.e., a mixture of continuous and discrete) dynamics, 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. The importance of safety verification here is underscored by the fact that many applications which employ this kind of systems are safety critical. For example, hybrid systems appear in air traffic control, life support devices, etc.

For verifying safety, several methods have been proposed in the recent years. Explicit computation of either exact or approximate reachable sets corresponding to the continuous dynamics is crucial for virtually all of these methods (see e.g. [3], [13], [2], [1], [6], [21], [22]). In a different vein, we have recently proposed a safety verification method that differs from the above techniques in the sense that it does not require explicit computation of reachable sets, but instead relies on functions of states termed *barrier certificates* [19]. 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. The method is applicable to 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 (IQCs).

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 [16] and semidefinite programming [23] can be utilized for constructing a polynomial barrier certificate, e.g., using the software [20]. For fixed polynomial degrees, the complexity of this construction grows polynomially with respect to the state dimension. Hence we expect our method to be more scalable than many other existing methods.

In the present paper, we will consider safety verification of stochastic continuous and hybrid systems. 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 e.g. in [15], [12]. On the other hand, only quite recently have people started to consider stochastic hybrid systems. See e.g. [7], [14], [11], [17], [10]. When stochasticity is present in the system, answering the safety verification question in a worst-case non-stochastic manner (i.e., to verify whether or not a trajectory of the system can reach the unsafe set) will usually lead to a very conservative and restrictive answer, since in most cases 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* of the system trajectories reaching the unsafe region is *lower* than a certain safety margin. For some recent work on stochastic reachability analysis, readers are referred to [5], [24], [4].

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 is a *supermartingale* (i.e., its expected value is non-increasing along time) 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 is then bounded from above using a Chebyshev-like inequality for supermartingales. We derive the conditions that are satisfied by barrier certificates for stochastic continuous systems and a class of stochastic hybrid systems, namely that of switching diffusion processes, and we will briefly discuss possible extension of this method to handle other classes of hybrid systems. Similar to their non-stochastic counterpart, barrier certificates for stochastic polynomial systems can be computed using the sum of squares decomposition and

S. Prajna is with Control and Dynamical Systems, California Institute Technology, Pasadena, CA 91125, USA. E-mail: 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. E-mail: jadbabai@seas.upenn.edu, pappasg@seas.upenn.edu

0-7803-8682-5/04/$20.00 ©2004 IEEE

semidefinite programming.

For the above classes of systems, our method can be used to efficiently compute an *exactly guaranteed* upper bound on the probability that the system trajectories reach the unsafe set. The references [5], [4], for example, suggest ways to calculate such a probability, yet have not provided a computational technique for that. On the other hand, the work in [24] does provide a computational method to approximate the above probability for the class of stochastic discrete time systems, but since their method is based on randomized algorithm, there has been no guarantee on the accuracy of the computed probability.

The paper is organized as follows. In Section II we present a brief review of our previous results on non-stochastic safety verification using barrier certificates. We will consider verification of stochastic continuous systems in Section III and verification of stochastic hybrid systems in Section IV. Section V contains some examples, and finally the paper is ended by conclusions in Section VI.

II. Review of Previous Results

A. Non-stochastic Verification Using Barrier Certificates

Let us consider the continuous system

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

where $x(t) \in \mathcal{X}$ is the state of the system, and $d(t) \in D$ is a collection of uncertain disturbance inputs (usually corresponding to a bounded D). We assume that the system trajectories start at some $x(0) \in \mathcal{X}_0$. Additionally, denote the unsafe region by $\mathcal{X}_u$.

In worst-case non-stochastic safety verification, we are interested in proving that for *all* possible disturbance signals $d : [0, \infty) \to D$, the system trajectories starting at any $x(0) \in \mathcal{X}_0$ never reach the unsafe set $\mathcal{X}_u$. This safety property can be shown by the existence of a barrier certificate [18], [19]. Proposition 1 states the conditions that are satisfied by a barrier certificate $B(x)$. Such a certificate proves that the system is safe by depicting a 'barrier' which separates possible system trajectories and the unsafe region — in the formulation below, the 'barrier' is provided by the zero level set of $B(x)$.

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 continuously differentiable function $B : \mathcal{X} \to \mathbb{R}$ such that

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

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

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

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

Safety verification of hybrid systems can also be handled using this methodology. We refer the reader to [19] for details and examples.

B. Computation of Barrier Certificates

Construction of barrier certificates is generally not easy. However, for systems whose vector fields are polynomial and whose initial sets, safety sets, etc. 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 [16] and semidefinite programming [23]. Here real coefficients $c_1, ..., c_m$ are used to parameterize a set of candidate barrier certificates in an affine manner, e.g., $\mathcal{B} = \{B(x) : B(x) = \sum_{i=1}^{m} c_i b_i(x), c_i \in \mathbb{R}\}$, where the $b_i(x)$'s are some monomials in x. For example, one can 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 $B(x) \in \mathcal{B}$ (or equivalently coefficients c_i's) such that the conditions in Proposition 1 are satisfied can be formulated as the following sum of squares problem, which can then be solved by semidefinite programming, e.g. using the software SOSTOOLS [20].

Proposition 2: Let the system (1) be given, the sets $\mathcal{X}$, $\mathcal{X}_0$, $\mathcal{X}_u$, and D be described by $\mathcal{X} = \{x \in \mathbb{R}^n : g_{\mathcal{X}}(x) \geq 0\}$, $\mathcal{X}_0 = \{x \in \mathbb{R}^n : g_{\mathcal{X}_0}(x) \geq 0\}$, $\mathcal{X}_u = \{x \in \mathbb{R}^n : g_{\mathcal{X}_u}(x) \geq 0\}$, $D = \{d \in \mathbb{R}^m : g_D(d) \geq 0\}$, where the g's are polynomials, and the parameterization of candidate barrier certificates $\mathcal{B}$ be given. Suppose there exists $B(x) \in \mathcal{B}$, a positive number ϵ, and SOS polynomials $\sigma_{\mathcal{X}_u}(x)$, $\sigma_{\mathcal{X}_0}(x)$, $\sigma_{\mathcal{X}}(x, d)$, $\sigma_D(x, d)$ that satisfy the following conditions:

$$\begin{aligned}
&B(x) - \epsilon - \sigma_{\mathcal{X}_u}(x) g_{\mathcal{X}_u}(x) \text{ is SOS,} \\
&-B(x) - \sigma_{\mathcal{X}_0}(x) g_{\mathcal{X}_0}(x) \text{ is SOS,} \\
&-\frac{\partial B}{\partial x} f(x, d) - \sigma_{\mathcal{X}}(x, d) g_{\mathcal{X}}(x) - \sigma_D(x, d) g_D(d) \text{ is SOS,}
\end{aligned}$$

then the safety of the system is guaranteed.

Given the above formulation, the software SOSTOOLS can compute a $B(x) \in \mathcal{B}$ and multipliers σ's satisfying all the required conditions, or tell if there is no feasible solution in the given set of candidates — note however that the latter does not necessarily imply that the system is unsafe.

III. Safety Verification of Stochastic Continuous Systems

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

$$dx(t) = f(x(t))dt + g(x(t))dw(t), \tag{5}$$

where $x(t) \in \mathbb{R}^n$ for all $t \geq 0$. 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 $\mathbb{R}^n$ and assumed compact. To guarantee the existence and uniqueness of solution, we will also assume that both f and g satisfy the local Lipschitz condition and the linear growth condition on $\mathcal{X}$ [15]. For

bounded $\mathcal{X}$, the last condition can be replaced by the boundedness of f and g on $\mathcal{X}$.

It can be shown that the process $x(t)$ described above is a strong Markov process. We have the following definition for the infinitesimal generator A of the process $x(t)$ — see e.g. [15].

Definition 3: 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.

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 [12].

Definition 4: Suppose that τ is the first time of exit of $x(t)$ from the open set 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 infinitesimal generator corresponding to $\tilde{x}(t)$ is identical to the one corresponding to $x(t)$ on the set Int($\mathcal{X}$), and is equal to zero outside of the set [12]. This will be implicitly assumed throughout the paper. Having defined the system and the stopped process $\tilde{x}(t)$, we can now state the stochastic safety verification problem as follows.

Problem 5: Given the system (5) and the sets $\mathcal{X}$, $\mathcal{X}_0$ and $\mathcal{X}_u$, compute an upper bound for the probability of a process $\tilde{x}(t)$ starting at $\mathcal{X}_0$ to reach $\mathcal{X}_u$. In other words, find $\gamma \in [0, 1]$ such that $P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0 \mid \tilde{x}(0)\} \leq \gamma$. for all $\tilde{x}(0) \in \mathcal{X}_0$.

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 paper, 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 (see e.g. [12] for some notions of stochastic stability and stochastic Lyapunov functions). However, instead of requiring the value of $B(x)$ to decrease along the trajectory of the system, we ask that the *expected* value of $B(x)$ decreases or stays constant as time increases. A function satisfying such a property is called a supermartingale (see [15] for the technical definition). For nonnegative supermartingales, there exists the following result [12], [8], which will be used several times in this paper.

Lemma 6: Let $B(\tilde{x}(t))$ be a supermartingale of the process $\tilde{x}(t)$ and be nonnegative on $\mathcal{X}$. Then, for any initial condition $\tilde{x}(0) \in \mathcal{X}$,

$$P\left\{ \sup_{0 \leq t < \infty} B(\tilde{x}(t)) \geq \lambda \;\middle|\; \tilde{x}(0) \right\} \leq \frac{B(\tilde{x}(0))}{\lambda}. \quad (6)$$

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

Theorem 7: Let the stochastic differential equation (5) and the sets $\mathcal{X}$, $\mathcal{X}_0$, $\mathcal{X}_u$ be given, and consider the stopped process $\tilde{x}(t)$ starting at some $\tilde{x}(0) \in \mathcal{X}_0$. Suppose there exists a twice continuously differentiable function $B : \mathcal{X} \to \mathbb{R}$, such that

$$B(x) \geq 0 \quad \forall x \in \mathcal{X}, \quad (7)$$

$$B(x) \geq 1 \quad \forall x \in \mathcal{X}_u, \quad (8)$$

$$B(x) \leq \gamma \quad \forall x \in \mathcal{X}_0, \quad (9)$$

$$\frac{\partial B}{\partial x} f(x) + \frac{1}{2} \text{Trace} \left(g^T(x) \frac{\partial^2 B}{\partial x^2} g(x) \right) \leq 0 \quad \forall x \in \mathcal{X}, \quad (10)$$

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

Proof: For the stochastic differential equation (5), the infinitesimal generator of the process is given by [15]

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

where B belongs to the domain of the generator (i.e., is twice continuously differentiable). Now, using Dynkin's formula [15], we have for $0 \leq t_1 \leq t_2 < \infty$

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

and therefore (10) will imply that B is a supermartingale. By (7) and Lemma 6 we conclude that (6) holds. Finally, use (9) and the fact that $\mathcal{X}_u \subseteq \{x : B(x) \geq 1\}$, which follows from (8), to obtain the following series of inequalities:

$$P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0 \mid \tilde{x}(0)\} \leq P\left\{ \sup_{0 \leq t < \infty} B(\tilde{x}(t)) \geq 1 \;\middle|\; \tilde{x}(0) \right\} \leq B(\tilde{x}(0)) \leq \gamma,$$

and thus the probability bound is proven. ■

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 (7)–(10). The intuitive idea behind the theorem is clear. The function $B(x)$ is a supermartingale of the process, 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 6, which provides a Chebyshev-like inequality for bounding the probability of the distribution tail.

With regard to computation, an upper bound γ and a barrier certificate $B(x)$ which certifies the upper bound can be computed by formulating conditions (7)–(10) as a sum of squares optimization problem, similar to the one in

Section II-B. Furthermore, γ can be chosen as the objective function 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.

Sometimes an initial probability measure μ_0 (whose support is in $\mathcal{X}_0$) is known for $\tilde{x}(0)$, and we may want to estimate the *total* (unconditional) probability of the system trajectories reaching the unsafe set. In this case, (9) can be replaced by $\int_{\mathcal{X}_0} B(x)d\mu_0(x) \leq \gamma$ and γ is then minimized to obtain a tight bound. Computation of γ and $B(x)$ can still be performed using sum of squares decomposition and semidefinite programming, since the left hand side of the above inequality is simply an affine function of the unknown coefficients in $B(x)$. See also the next section.

IV. Safety Verification of Stochastic Hybrid Systems

The idea used in Section III can also be applied to stochastic hybrid systems. In this section, we will consider a class of stochastic hybrid systems called the switching diffusion processes [9], [14], [17]. Systems in this class have both continuous and discrete states, where the continuous state evolves according to a stochastic differential equation that depends on the discrete state, and the discrete trajectory is a Markov chain whose transition matrix depends on the continuous state. As implied by the name, they are switching systems, meaning that the value of the continuous state does not change during a discrete transition.

Formally, a switching diffusion process is a tuple $H = (\mathcal{X}, L, \mu_0, f, g, \lambda_{ij})$ with the following components [17]:

- $\mathcal{X} \subseteq \mathbb{R}^n$ 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 $(l, x) \in L \times \mathcal{X}$.
- $\mu_0 : \mathcal{B}(L \times \mathcal{X}) \rightarrow [0, 1]$ is an initial probability measure, with its support in $X_0 \subseteq X$.
- $f : X \rightarrow \mathbb{R}^n$ is the drift vector field.
- $g : X \rightarrow \mathbb{R}^{n\times m}$, where the i-th column of g corresponds to the i-th component of the $\mathbb{R}^m$-valued Wiener process w.
- $\lambda_{ij} : \mathcal{X} \rightarrow \mathbb{R}$, $i, j \in L$ are a set of x-dependent transition rates, with $\lambda_{ij}(x) \geq 0$ for all x if $i \neq j$, and $\sum_j \lambda_{ij}(x) = 0$ for all $i \in L$.

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:

$$P\{l(t+\Delta) = j \mid l(t) = i\} = \begin{cases} \lambda_{ij}(x(t))\Delta + o(\Delta), & \text{if } i \neq j, \\ 1 + \lambda_{ii}(x(t))\Delta + o(\Delta), & \text{if } i = j, \end{cases} \quad (11)$$

with $\Delta > 0$. During a discrete jump, the value of the continuous state is held constant. It is assumed that the discrete jump is independent from the Wiener process $w(t)$. In addition, we assume that f, g, and λ_{ij} are bounded and Lipschitz continuous with respect to x on $\mathcal{X}$. Under these assumptions, the solution to the stochastic differential equation at each location exists and is unique, and also that almost every sample path of $l(t)$ is a right continuous function [9], [17].

To obtain a bound like what we have in the previous section, it is crucial to know the following infinitesimal generator of the process $(l(t), x(t))$ [9]:

$$AB(l,x) = \frac{\partial B}{\partial x}(l,x)f(l,x) + \sum_{l'\in L} \lambda_{ll'}(x)B(l',x) + \frac{1}{2}\text{Trace}\left(g^T(l,x)\frac{\partial^2 B}{\partial x^2}(l,x)g(l,x)\right)$$

for $B(l, x)$ in the domain of the generator. For our purpose, it is enough to consider $B(l, x)$ that is twice continuously differentiable in the second argument for each $l \in L$. Similar to the continuous case, we stop the process when $x(t)$ goes out from Int$(\mathcal{X})$.

For this class of systems, the barrier certificate $B(l, x)$ will be constructed from several functions $B_l(x)$, where each $B_l(x)$ corresponds to a discrete location and we define $B(l, x) = B_l(x)$. The conditions that are satisfied by the barrier certificate are stated in the following theorem.

Theorem 8: Let the switching diffusion process H be given, and define $\mathcal{X}_{0,l} = \{x \in \mathcal{X} : (l, x) \in X_0\}$. Suppose there exists a collection of twice differentiable functions $B_l(x)$, which for each $l \in L$, satisfy

$$B_l(x) \geq 0 \quad \forall x \in \mathcal{X}, \quad (12)$$

$$B_l(x) \geq 1 \quad \forall x \in \mathcal{X}_u, \quad (13)$$

$$\frac{\partial B_l}{\partial x}f(l,x) + \frac{1}{2}\text{Trace}\left(g^T(l,x)\frac{\partial^2 B_l}{\partial x^2}g(l,x)\right) + \sum_{l'\in L}\lambda_{ll'}(x)B_{l'}(x) \leq 0 \quad \forall x \in \mathcal{X}, \quad (14)$$

and in addition,

$$\sum_{l\in L}\int_{\mathcal{X}_{0,l}} B_l(x)d\mu_0(l,x) \leq \gamma. \quad (15)$$

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

Proof: Define $B(l, x) = B_l(x)$. In this case, Dynkin's formula

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

and (14) again imply that $B(\tilde{l}(t), \tilde{x}(t))$ is a supermartingale. Since it is also nonnegative (as implied by (12)), Lemma 6 can be applied, and therefore we have

$$\begin{aligned} P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0 \mid (\tilde{l}(0), \tilde{x}(0))\} \\ \leq P\left\{ \sup_{0 \leq t < \infty} B(\tilde{l}(t), \tilde{x}(t)) \geq 1 \middle| (\tilde{l}(0), \tilde{x}(0)) \right\} \\ \leq B(\tilde{l}(0), \tilde{x}(0)). \end{aligned}$$

Now use the law of total probability and (15) to obtain

$$\begin{aligned} P\{\tilde{x}(t) \in \mathcal{X}_u \text{ for some } t \geq 0\} &\leq \int_{X_0} B(l,x) d\mu_0(l,x) \\ &= \sum_{l \in L} \int_{\mathcal{X}_{0,l}} B_l(x) d\mu_0(l,x) \leq \gamma, \end{aligned}$$

hence finishing the proof. ∎

In principle, other classes of stochastic hybrid systems such as the ones in [11], [17], [10] can be handled in a similar fashion, by using the suitable infinitesimal generator for each class and modifying the other conditions for $B_l(x)$ appropriately. This will be considered in the future.

V. Examples

A. Example 1: Continuous System

Consider the nonlinear stochastic differential equation

$$\begin{aligned} dx_1(t) &= x_2(t)dt, \\ dx_2(t) &= (-x_1(t) - x_2(t) - 0.5x_1^3(t))dt + \sigma dw(t), \end{aligned}$$

where the diffusion coefficient σ is assumed to be a constant. In this case, the corresponding deterministic system $\dot{x}(t) = f(x(t))$ has a globally asymptotically stable equilibrium at the origin, as can be proven by a quartic Lyapunov function. Because of the asymptotic stability of the deterministic system, we expect that for small enough noise the trajectories of the stochastic system will also evolve to a region around the origin.

We use $\mathcal{X}_0 = \{(x_1, x_2) : (x_1 + 2)^2 + x_2^2 \leq 0.1^2\}$ as the initial set, and $\mathcal{X} = \{(x_1, x_2) : -3 \leq x_1 \leq 3, -3 \leq x_2 \leq 3, x_1^2 + x_2^2 \geq 0.5^2\}$ as the state space. Since the stochastic input $dw(t)$ drives the system persistently, we stop the process when (x_1, x_2) gets near to the origin. Finally, the set $\mathcal{X}_u = \{(x_1, x_2) \in \mathcal{X} : x_2 \geq 2.25\}$ will be regarded as the unsafe set. Some realizations of the process $\tilde{x}(t)$ are shown in Figure 1.

We will compute an upper bound γ on the probability that a stopped process starting from $\mathcal{X}_0$ intersects $\mathcal{X}_u$, as the state evolves toward the origin. For example, this may correspond to the control objective of keeping the value of x_2 lower than the given threshold. Using the theory and the computational method described in Sections III and II-B, we are able to compute upper bounds as well as polynomial barrier certificates that prove these upper bounds. The verification results for various degrees of barrier certificates and various values of σ are given in Table I. As we include more candidates in the set of candidate barrier certificates to be searched (i.e., as we increase the degree of the barrier certificate), we are able to obtain a better upper bound. However, the computational complexity of solving the sum of squares problem also increases. When we decrease σ, the probability of reaching the unsafe set decreases as well — this agrees with our intuition, as the system is safe when there is no stochastic input.

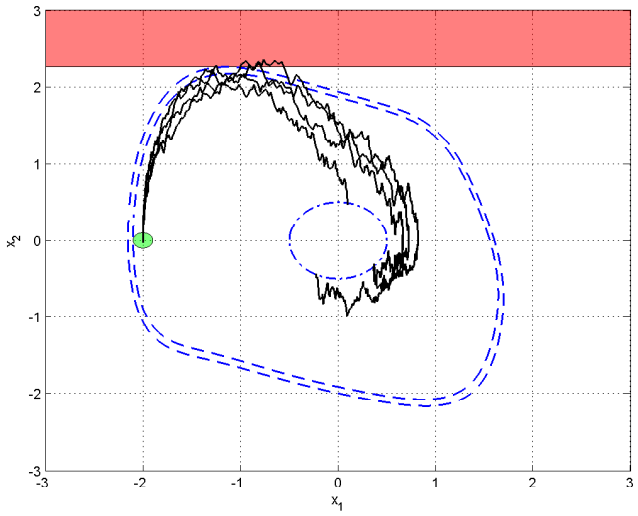

Fig. 1. Black curves are some realizations of the stopped process $\tilde{x}(t)$ in Section V-A for $\sigma = 0.5$, all starting at $\tilde{x}(0) = (-2, 0)$; we stop the process $x(t)$ when it enters $\{x : x_1^2(t) + x_2^2(t) \leq 0.5^2\}$, the region whose boundary is depicted by the dash-dotted curve. The shaded region at the top is the unsafe set. Shown as dashed curves are the level sets $B(x) = 1$ (outer) and $B(x) = 0.792$ (inner) of the degree eight barrier certificate that proves the upper bound $\gamma = 0.792$ (cf. Table I).

	Degree= 4	Degree= 6	Degree= 8	Degree= 10
$\sigma = 0.5$	$\gamma = 1$	$\gamma = 0.847$	$\gamma = 0.792$	$\gamma = 0.771$
$\sigma = 0.25$	$\gamma = 0.848$	$\gamma = 0.616$	$\gamma = 0.472$	$\gamma = 0.412$
$\sigma = 0.1$	$\gamma = 0.824$	$\gamma = 0.450$	$\gamma = 0.257$	$\gamma = 0.157$

TABLE I

Stochastic safety verification results in Section V-A.

B. Example 2: Switching Diffusion Process

In this example we use the system $dx(t) = A_{l(t)}x(t) + \sigma(x(t))dw(t)$, where $l(t) \in \{1, 2\}$ for each t and

$$A_1 = \begin{bmatrix} -5 & -4 \\ -1 & -2 \end{bmatrix}; \quad A_2 = \begin{bmatrix} -2 & -4 \\ 20 & -2 \end{bmatrix}.$$

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 2. The set $\{(x_1, x_2) \in \mathbb{R}^2 : x_1^2 \leq 4^2, -1.5 \leq x_2 \leq 4\}$ is chosen as the continuous state space $\mathcal{X}$, and the unsafe set is given by $\mathcal{X}_u = \{(x_1, x_2) \in \mathcal{X} : x_2 \leq -1\}$. We are interested in

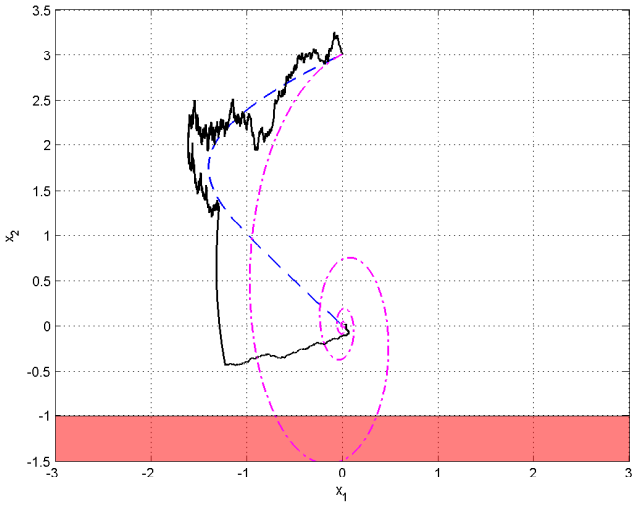

Fig. 2. Trajectories of the systems $\dot{x} = A_1 x$ (dashed curve) and $\dot{x} = A_2 x$ (dash-dotted curve) in Section V-B starting at $x(0) = (0, 3)$ are shown. A realization $\tilde{x}(t)$ of the switching diffusion process for $\lambda = 10$ is depicted by the solid curve. Shaded region at the bottom of the figure is the unsafe set. Larger λ makes it less likely for the trajectory to reach the unsafe set.

verifying the safety of the stochastic system with $\sigma(x) = \begin{bmatrix} 0 & 0.5x_2 \end{bmatrix}^T$ and transition rates $\lambda_{11} = -0.5$, $\lambda_{12} = 0.5$, $\lambda_{21} = \lambda$, $\lambda_{22} = -\lambda$, 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 proposed a new approach to safety verification of stochastic continuous and hybrid systems. Based on suitable barrier certificates, our method provides an upper bound on the probability that a system trajectory reaches the unsafe region. For polynomial systems, computation of barrier certificates can be performed in a tractable fashion by convex optimization, utilizing the sum of squares decomposition of multivariate polynomials and semidefinite programming.

In this paper, we considered continuous stochastic systems and switching diffusion processes, and presented some examples to illustrate the use of our method. Other classes of stochastic hybrid systems can also be handled by using the appropriate infinitesimal generator for each class, which we hope to address in the future.

References

[1] R. Alur, T. Dang, and F. Ivancic, "Progress on reachability analysis of hybrid systems using predicate abstraction," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2003.

[2] E. Asarin, T. Dang, and O. Maler, "The d/dt tool for verification of hybrid systems," in *Computer Aided Verification, LNCS 2404*. Springer-Verlag, 2002, pp. 365–370.

[3] 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*. Heidelberg: Springer-Verlag, 2000.

[4] M. L. Bujorianu, "Extended stochastic hybrid systems and their reachability problem," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2004.

[5] M. L. Bujorianu and J. Lygeros, "Reachability questions in piecewise deterministic Markov processes," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2003.

[6] A. Chutinan and B. H. Krogh, "Computational techniques for hybrid system verification," *IEEE Trans. Automatic Control*, vol. 48, no. 1, pp. 64–75, 2003.

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

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

[9] M. K. Ghosh, A. Arapostathis, and S. I. Marcus, "Ergodic control of switching diffusions," *SIAM Journal on Control and Optimization*, vol. 35, no. 6, pp. 1952–1988, 1997.

[10] J. P. Hespanha, "Stochastic hybrid systems: Application to communication networks," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2004.

[11] J. Hu, J. Lygeros, and S. Sastry, "Towards a theory of stochastic hybrid systems," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2000.

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

[13] G. Lafferriere, G. J. Pappas, and S. Yovine, "Symbolic reachability computations for families of linear vector fields," *J. Symbolic Computation*, vol. 32, no. 3, pp. 231–253, 2001.

[14] X. Mao, "Stability of stochastic differential equations with Markovian switching," *Stochastic Processes and Their Applications*, vol. 79, no. 1, pp. 45–67, 1999.

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

[16] P. A. Parrilo, "Structured semidefinite programs and semialgebraic geometry methods in robustness and optimization," Ph.D. dissertation, Caltech, Pasadena, CA, 2000.

[17] 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.

[18] S. Prajna, "Barrier certificates for nonlinear model validation," in *Proceedings IEEE Conference on Decision and Control*, 2003.

[19] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2004.

[20] S. Prajna, A. Papachristodoulou, and P. A. Parrilo, "Introducing SOSTOOLS: A general purpose sum of squares programming solver," in *Proceedings IEEE Conference on Decision and Control*, 2002, available at http://www.cds.caltech.edu/sostools and http://www.aut.ee.ethz.ch/~parrilo/sostools.

[21] A. Tiwari, "Approximate reachability for linear systems," in *Hybrid Systems: Computation and Control*. Heidelberg: Springer-Verlag, 2003.

[22] C. J. Tomlin, I. Mitchell, A. M. Bayen, and M. Oishi, "Computational techniques for the verification of hybrid systems," *Proc. of the IEEE*, vol. 91, no. 7, pp. 986–1001, 2003.

[23] L. Vandenberghe and S. Boyd, "Semidefinite programming," *SIAM Review*, vol. 38, no. 1, pp. 49–95, 1996.

[24] 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.