A Barrier Function Approach to Finite-Time Stochastic System Verification and Control

Cesar Santoyo, Maxence Dutreix, and Samuel Coogan

Abstract

We study the problem of synthesizing a control strategy to enforce safety of affine-in-control stochastic dynamical systems over finite time horizons. We use stochastic control barrier functions to quantify the probability that a system exits a given safe region of the state space in finite-time and consider both continuous-time and discrete-time systems. A barrier certificate condition that bounds the expected value of the barrier function over the time horizon is recast as a sum-of-squares optimization problem for efficient numerical computation. Unlike prior works, the proposed certificate condition includes a state-dependent upper bound on the evolution of the expectation, allowing for tighter probability bounds. Two examples are presented.

1 Introduction

A dynamical system is considered *safe* if its trajectories do not enter an unsafe region of the statespace. A common approach to safety verification in deterministic systems is via *barrier functions* which provide Lyapunov-like guarantees of system behavior [12]. Recent work has extended this approach to allow for control inputs, resulting in *control barrier functions* applicable to affine-in-control systems [2, 4, 21]. Control barrier functions have been demonstrated in cruise control applications [3, 4] and collision avoidance in robotic swarms [20].

In the stochastic setting, continuous-time safety verification via barrier certificates for infinite time horizons was also introduced in [12], which provides a framework for bounding the probability a system will exit a safe region based on a non-negative barrier function. The barrier function based stochastic verification framework functions without performing state abstractions like in [19] which stands in contrast to the *abstraction-based* techniques of [15].

To obtain such guarantees, the infinitesimal generator, which dictates the expected value evolution of a stochastic process, is required to be to be non-positive; i.e., the barrier function is required to be a *supermartingale*. The paper [16] relaxes the supermartingale condition to allow for finite-time safety verification and instead provides a barrier certificate which only requires the infinitesimal generator of the barrier process to be upper bounded by a constant. Such processes, called *c-martingales*, allow the expected value of the barrier function to increase over time.

The formulation of control barrier functions in discrete-time is significantly distinct from the continuous-time counterpart. Nonetheless, discrete-time control barrier functions have been used to certify safety for bi-pedal robots [1] and for temporal logic verification of discrete-time systems [6, 7].

The present note studies the problem of synthesizing controllers for stochastic systems to ensure safety on finite-time horizons for both continuous-time and discrete-time domains. We propose a barrier certificate constraint that imposes a state-dependent bound on the evolution of the stochastic system. This bound was originally proposed and studied by Kushner in [8, 9, 10] in the context of stochastic stability. The proposed barrier certificate allows the expected value of the barrier to increase and covers the c-martingale condition of [16] as a special case. However, our formulation also accounts for the system dynamics in the expectation constraint. This allows for probability bounds that are no worse than the c-martingale condition, and in many cases, provides better probability bounds. As in [12, 16], we compute barrier functions and feedback control strategies using *sum-of-squares* (SOS) optimization. Like in [12], but unlike [16], we utilize polynomial barrier functions. This provides a simpler formulation of the probability of failure on a finite time horizon when compared to the exponential barrier function approach in [16].

Our preliminary work in the conference paper [14] focuses only on continuous-time. In this note, we extend this approach to discrete-time and present a unified framework for safe control synthesis.

[1] The authors are with the School of Electrical & Computer Engineering, Georgia Institute of Technology, Atlanta, GA, 30318, USA. S. Coogan is also with the School of Civil and Environmental Engineering, Georgia Institute of Technology, Atlanta, GA, 30318, USA. {csantoyo, maxdutreix, sam.coogan}@gatech.edu. This work was partially supported by NSF under Grant #1749357. C. Santoyo was supported by the NSF Graduate Research Fellowship Program under Grant No. DGE-1650044.

2 Problem Formulation

We consider an n-dimensional stochastic process x in continuous-time or discrete-time so that x satisfies either the stochastic differential equation

$$dx(t) = (f(x(t)) + g(x(t))u(x(t)))dt + \sigma(x(t))dw \quad (1)$$

or the stochastic difference equation

$$x[k+1] = f(x[k]) + g(x[k])u(x[k]) + \sigma(x[k])\xi[k] \quad (2)$$

where $f : \mathcal{X} \to \mathbb{R}^n$, $g : \mathcal{X} \to \mathbb{R}^{n\times p}$, $\sigma : \mathcal{X} \to \mathbb{R}^{n\times m}$, w is a m-dimensional Wiener process, ξ is a stochastic process whose value is governed by some probabilistic distribution, and $u : \mathcal{X} \to \mathbb{R}^p$ is a state feedback control law. We generally use rounded brackets and the index t to denote continuous time, while square brackets and the index k denote discrete time. We make the following assumption for (1)–(2).

Assumption 1 *The functions f, g, and σ are polynomial in x.*

In this paper, we are concerned with bounding the probability that a stochastic process satisfying either (1) or (2) enters an unsafe region during a finite-time horizon, which is deemed a *failure* of the system. We will not be concerned with solutions that exit $\mathbf{int}(\mathcal{X})$, the interior of $\mathcal{X}$, and thus we always assume x is a *stopped* process that stops evolving upon exiting $\mathbf{int}(\mathcal{X})$; see, *e.g.*, [12], for a formal characterization of stopped processes.

Objective: Given the system (1) or (2), a fixed time horizon, a set of unsafe states, and a set of possible initial conditions, synthesize a feedback control law $u(x)$ to achieve a desired maximum probability of failure.

One of the main theoretical tools we employ to solve this objective is that of *barrier functions*, and we recall two fundamental results that employ barrier functions to obtain failure probability bounds for (1) and (2).

Proposition 1 *Given (1) and the sets $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_u \subseteq \mathcal{X}, \mathcal{X}_0 \subseteq \mathcal{X} \setminus \mathcal{X}_u$ with $F(x) = f(x) + g(x)u(x)$ and $\sigma(x)$ locally Lipschitz continuous, where $u(x)$ is some feedback control law. Suppose there exists a twice differentiable function B such that*

$$B(x) \le \gamma \ \forall x \in \mathcal{X}_0, \quad (3)$$
$$B(x) \ge 1 \ \forall x \in \mathcal{X}_u, \quad (4)$$
$$B(x) \ge 0 \ \forall x \in \mathcal{X}, \ \textit{and} \quad (5)$$
$$\frac{\partial B}{\partial x}F(x) + \frac{1}{2}\mathit{Trace}\left(\sigma^T(x)\frac{\partial^2 B}{\partial x^2}\sigma(x)\right) \le -\alpha B(x) + \beta \quad \forall x \in \mathcal{X} \setminus \mathcal{X}_u \quad (6)$$

for some $\alpha \ge 0$, $\beta \ge 0$ and $\gamma \in [0, 1)$. Define

$$\rho_u := P\{\tilde{x}(t) \in \mathcal{X}_u \ \textit{for some} \ 0 \le t \le T \mid \tilde{x}(0) \in \mathcal{X}_0\}, \quad (7)$$

$$\rho_B := P\left\{\sup_{0\le t\le T} B\big(\tilde{x}(t)\big) \ge 1 \mid \tilde{x}(0) \in \mathcal{X}_0\right\} \quad (8)$$

where $\tilde{x}(t)$ is a stopped solution of (1). Then

- *If $\alpha > 0$ and $\frac{\beta}{\alpha} \le 1$,*
$$\rho_u \le \rho_B \le 1 - \left(1-\gamma\right)e^{-\beta T}. \quad (9)$$
- *If $\alpha > 0$ and $\frac{\beta}{\alpha} \ge 1$,*
$$\rho_u \le \rho_B \le \frac{\gamma + (e^{\beta T} - 1)\frac{\beta}{\alpha}}{e^{\beta T}}. \quad (10)$$
- *If $\alpha = 0$,*
$$\rho_u \le \rho_B \le \gamma + \beta T. \quad (11)$$

Proposition 1 is an immediate corollary of [10, Chapter 3, Theorem 1] and recovers the supermartingale condition [12, Theorem 15] and c-martingale condition [16, Theorem 2.4] as special cases.

An analogous result holds in discrete-time as shown in the next proposition, an immediate corollary of [10, Chapter 3, Theorem 3].

Proposition 2 *Given (2) and the sets $\mathcal{X} \subset \mathbb{R}^n$, $\mathcal{X}_u \subseteq \mathcal{X}, \mathcal{X}_0 \subseteq \mathcal{X} \setminus \mathcal{X}_u$ with $F(x, \xi) = f(x) + g(x)u(x) + \sigma(x)\xi$ where $u(x)$ is some feedback control law. Suppose there exists a function B such that*

$$B(x) \le \gamma \ \forall x \in \mathcal{X}_0, \quad (12)$$
$$B(x) \ge 1 \ \forall x \in \mathcal{X}_u, \quad (13)$$
$$B(x) \ge 0 \ \forall x \in \mathcal{X}, \ \textit{and} \quad (14)$$
$$\mathbb{E}[B(F(x,\xi)) \mid x] \le \frac{B(x)}{\tilde{\alpha}} + \tilde{\beta} \quad \forall x \in \mathcal{X} \setminus \mathcal{X}_u \quad (15)$$

for some $\tilde{\alpha} \ge 1$, $0 \le \tilde{\beta} < 1$ and $\gamma \in [0, 1)$. Define

$$\rho_u := P\{\tilde{x}[k] \in \mathcal{X}_u \ \textit{for some} \ 0 \le k \le N \mid \tilde{x}[0] \in \mathcal{X}_0\} \quad (16)$$

$$\rho_B := P\left\{\sup_{0\le k\le N} B(\tilde{x}[k]) \ge 1 \mid \tilde{x}[0] \in \mathcal{X}_0\right\} \quad (17)$$

where $\tilde{x}[k]$ is a stopped solution of (2). Then

- *If $\tilde{\alpha} > 1$ and $\frac{\tilde{\beta}\tilde{\alpha}}{\tilde{\alpha}-1} \le 1$,*
$$\rho_u \le \rho_B \le 1 - \left(1-\gamma\right)\prod_{0}^{N-1}\left(1-\tilde{\beta}\right). \quad (18)$$
- *If $\tilde{\alpha} > 1$ and $\frac{\tilde{\beta}\tilde{\alpha}}{\tilde{\alpha}-1} > 1$,*
$$\rho_u \le \rho_B \le \gamma\tilde{\alpha}^{-N} + \frac{(1-\tilde{\alpha}^{-N})\tilde{\alpha}\tilde{\beta}}{(\tilde{\alpha}-1)}. \quad (19)$$
- *If $\tilde{\alpha} = 1$,*
$$\rho_u \le \rho_B \le \gamma + \tilde{\beta}N. \quad (20)$$

If $B(x)$ satisfies the conditions of Proposition 1 or Proposition 2, then we call $B(x)$ a *stochastic control barrier function* for a given control policy $u(x)$.

3 SOS Formulations & Numerical Procedures

In this section we present our main result, a numerical procedure to synthesize a feedback control strategy $u(x)$, along with a stochastic control barrier function $B(x)$, in order to obtain a controlled system that achieves a desired maximum probability of failure over a finite time horizon. The main tool is that of *sum-of-squares (SOS)* programming.

Definition 1 *Define* $\mathbb{R}[x]$ *as the set of all polynomials in* $x \in \mathbb{R}^n$. *Then*

$$\Sigma[x] \triangleq \left\{ s(x) \in \mathbb{R}[x] : s(x) = \sum_{i=1}^{m} g_i(x)^2, g_i(x) \in \mathbb{R}[x] \right\}$$

is the set of sum-of-squares polynomials.

Definition 2 *Given* $p_i(x) \in \mathbb{R}[x]$ *for* $i = 0, \ldots, m$, *the problem of finding* $q_i(x) \in \Sigma[x]$ *for* $i = 1, \ldots, \hat{m}$ *and* $q_i(x) \in \mathbb{R}[x]$ *for* $i = \hat{m}+1, \ldots, m$ *such that*

$$p_0(x) + \sum_{i=1}^{m} p_i(x) q_i(x) \in \Sigma[x]$$

is a sum-of-squares program (SOSP).

SOSPs can be efficiently converted to semidefinite programs using tools such as SOSTOOLS [11].

We restrict our search for feedback control policies to polynomial $u(x)$ and for stochastic control barrier functions to polynomial $B(x)$. First, we show how the conditions of Proposition 1 and Proposition 2 can be recast as SOS constraints.

Theorem 1 *Consider a system of the form of (1), with control polynomial* $u(x)$, *and the sets* $\mathcal{X}$, $\mathcal{X}_0$, *and* $\mathcal{X}_u$ *and assume these sets are described as* $\mathcal{X} = \{x \in \mathbb{R}^n : s_{\mathcal{X}}(x) \geq 0\}$, $\mathcal{X}_0 = \{x \in \mathbb{R}^n : s_{\mathcal{X}_o}(x) \geq 0\}$, $\mathcal{X}_u = \{x \in \mathbb{R}^n : s_{\mathcal{X}_u}(x) \geq 0\}$, *and* $\mathcal{X} \setminus \mathcal{X}_u = \{x \in \mathbb{R}^n : s_{\mathcal{X}\setminus\mathcal{X}_u}(x) \geq 0\}$ *for some polynomials* $s_{\mathcal{X}}$, $s_{\mathcal{X}_o}$, $s_{\mathcal{X}_u}$, *and* $s_{\mathcal{X}\setminus\mathcal{X}_u}(x)$. *Suppose there exists a polynomial* $B(x)$, *and SOS polynomials* $\lambda_{\mathcal{X}}(x)$, $\lambda_{\mathcal{X}_o}(x)$, $\lambda_{\mathcal{X}_u}(x)$, *and* $\lambda_{\mathcal{X}\setminus\mathcal{X}_u}(x)$ *that satisfy*

$$B(x) - \lambda_{\mathcal{X}}(x) s_{\mathcal{X}}(x) \in \Sigma[x] \tag{21}$$
$$B(x) - \lambda_{\mathcal{X}_u}(x) s_{\mathcal{X}_u}(x) - 1 \in \Sigma[x] \tag{22}$$
$$-B(x) - \lambda_{\mathcal{X}_o}(x) s_{\mathcal{X}_o}(x) + \gamma \in \Sigma[x] \tag{23}$$
$$-\frac{\partial B(x)}{\partial x} F(x) - \frac{1}{2} Trace\left(\sigma^T(x) \frac{\partial^2 B}{\partial x^2} \sigma(x) \right) - \alpha B(x) + \beta - \lambda_{\mathcal{X}\setminus\mathcal{X}_u}(x) s_{\mathcal{X}\setminus\mathcal{X}_u}(x) \in \Sigma[x] \tag{24}$$

where $F(x) = f(x) + g(x)u(x)$. *Then, the probability of failure satisfies (9), (10) or (11).*

The analogous result for discrete-time follows.

Theorem 2 *Consider a system of the form of (2), with control polynomial* $u(x)$, *and the sets* $\mathcal{X}$, $\mathcal{X}_0$, *and* $\mathcal{X}_u$ *and assume these sets can be described as* $\mathcal{X} = \{x \in \mathbb{R}^n : s_{\mathcal{X}}(x) \geq 0\}$, $\mathcal{X}_0 = \{x \in \mathbb{R}^n : s_{\mathcal{X}_o}(x) \geq 0\}$, $\mathcal{X}_u = \{x \in \mathbb{R}^n : s_{\mathcal{X}_u}(x) \geq 0\}$, *and* $\mathcal{X} \setminus \mathcal{X}_u = \{x \in \mathbb{R}^n : s_{\mathcal{X}\setminus\mathcal{X}_u}(x) \geq 0\}$ *for some polynomials* $s_{\mathcal{X}}$, $s_{\mathcal{X}_o}$, $s_{\mathcal{X}_u}$, *and* $s_{\mathcal{X}\setminus\mathcal{X}_u}(x)$. *Suppose there exists a polynomial* $B(x)$, *and SOS polynomials* $\lambda_{\mathcal{X}}(x)$, $\lambda_{\mathcal{X}_o}(x)$, $\lambda_{\mathcal{X}_u}(x)$, *and* $\lambda_{\mathcal{X}\setminus\mathcal{X}_u}(x)$ *that satisfy the following*

$$B(x) - \lambda_{\mathcal{X}}(x) s_{\mathcal{X}}(x) \in \Sigma[x] \tag{25}$$
$$B(x) - \lambda_{\mathcal{X}_u}(x) s_{\mathcal{X}_u}(x) - 1 \in \Sigma[x] \tag{26}$$
$$-B(x) - \lambda_{\mathcal{X}_o}(x) s_{\mathcal{X}_o}(x) + \gamma \in \Sigma[x] \tag{27}$$
$$-\mathbb{E}[B(F(x,\xi)) \mid x] + \frac{B(x)}{\tilde{\alpha}} + \tilde{\beta} - \lambda_{\mathcal{X}\setminus\mathcal{X}_u}(x) s_{\mathcal{X}\setminus\mathcal{X}_u}(x) \in \Sigma[x] \tag{28}$$

where $F(x,\xi) = f(x) + g(x)u(x) + \sigma(x)\xi$. *Then, the probability of failure satisfies (18), (19) or (20).*

We omit the proofs for Theorems 1 and 2, which follow the general approach for relaxing set constraints to SOS programs using the *Positivstellensatz* condition; see the documentation of [11] for details.

In order to be a valid SOSP as in Definition 2, all expressions appearing in the constraints (21)–(28) must be polynomials, and any decision polynomials or variables must enter affinely in the SOS constraints of Theorems 1 and 2. We address the second point by alternately solving for a subset of decision polynomials and variables as detailed subsequently, however, both points require two further assumptions on $\mathbb{E}[B(F(x,\xi))|x]$ appearing in (28), which need not a priori be polynomial, as detailed next.

Assumption 2 *The only possible non-polynomial expression in Theorem 2 is the term* $\mathbb{E}[B(F(x,\xi))|x]$. *Therefore, we first assume* $\mathbb{E}[B(F(x,\xi))|x]$ *is expressible as a closed-form polynomial in* x. *For example, this is the case when* ξ *is a normally distributed random variable since, in this case, the moments* $\mathbb{E}[\xi^n]$ *are available in closed form and* $B(x)$ *and* $F(x)$ *are assumed polynomial in* x *as described above. Moreover, as described below, for control synthesis, we require the coefficients of the polynomial expression* $\mathbb{E}[B(F(x,\xi))|x]$ *to be affine in the coefficients of the decision polynomial* $u(x)$. *Thus, we further assume that when* $B(x)$ *and* $F(x)$ *are assumed fixed and* $u(x)$ *assumed to be a decision polynomial of fixed degree, the coefficients of* $u(x)$ *appear affinely in the expression for* $\mathbb{E}[B(F(x,\xi))|x]$. *For example, if* $B(x)$ *is affine this assumption would hold.*

We highlight an important difference between the continuous-time and discrete-time instantiations of these algorithms. For control synthesis, in continuous-time, the condition (24) is always affine in the decision variables of the polynomial control $u(x)$, however, this is generally not true for the discrete-time counterpart in (28).

The SOS constraints in Theorem 1 and Theorem 2 are not SOSPs when all of the parameters α, β, $\tilde{\alpha}$, $\tilde{\beta}$ and polynomials $u(x)$, $B(x)$ are considered variables along with the SOS polynomials $\lambda_{\mathcal{X}}(x)$, $\lambda_{\mathcal{X}_o}(x)$, $\lambda_{\mathcal{X}_u}(x)$, and $\lambda_{\mathcal{X}\setminus\mathcal{X}_u}(x)$. Therefore, in order to leverage Theorems 1 and 2 for control synthesis, we propose several algorithms which consider a subset of the variables to be fixed, solving for the remaining variables by formulating an appropriate SOSP from the conditions of Theorems 1 and 2. By iterating among these algorithms, we obtain a computationally tractable control synthesis procedure.

First, we consider the case when $u(x)$ is a given, fixed polynomial feedback control policy. Under this condition, Algorithm 1 computes a barrier function $B(x)$ satisfying the conditions in Theorem 1 (respectively, Theorem 2). Therefore, Algorithm 1 is interpreted as solving a verification problem that computes an upper bound on

Algorithm 1 Compute $B(x)$

procedure COMPUTE-$B(l_\alpha, u_\alpha, d, \sigma, u(x), n_B)$
  l_α & u_α are lower/upper α values spaced d apart
  $u(x)$ is the control poly. and n_B is order of $B(x)$
  $A \leftarrow Range(l_\alpha, u_\alpha, d)$ ▷ Assign α values d apart
  $P^* \leftarrow 1$
  Initialize P, i.e., upper bound on probability
  for $\alpha \in A$ **do**
    $\min \gamma + \beta$
    Continuous-time:
    subject to (21)–(24)
    Compute P, using (9), (10) or (11)
    Discrete-time:
    subject to (25)–(28)
    Compute P, using (18), (19) or (20).
    if $P < P^*$ **then**
      $\alpha^* := \alpha_i$
      $\beta^* := \beta$
      $P^* := P$
    end if
  end for
  return α^*, β^*, P^*
end procedure

Algorithm 2 Initialize $u(x)$

procedure COMPUTE-$u(B(x), \alpha, \beta, n_u)$
  $u(x) = z^T Q z$ ▷ $u(x)$ is an n_u power polynomial
    ▷ $B(x)$ is fixed z is a vector of state monomials
  min c
  subject to $c\mathbb{1} - \text{vec}(Q) \geq 0$
    $\text{vec}(Q) + c\mathbb{1} \geq 0$
    Continuous-time: (24)
    Discrete-time: (28)
  return $u(x), c, Q$
end procedure

the probability of failure, along with a stochastic control barrier function $B(x)$, when the control policy $u(x)$ is fixed.

Next, we propose Algorithm 2 to solve for a feedback control policy $u(x)$ to achieve a desired probability of failure using a fixed stochastic control barrier function $B(x)$. To choose among a potentially large set of satisfying control policies, we propose a cost metric that seeks to minimize the absolute value of the coefficients of the polynomial $u(x)$, which roughly aims to reduce the magnitude of the control input, although other cost metrics are easily considered, such as a metric that gives higher penalty to higher order terms in the controller in order to reduce controller complexity. To incorporate such a cost, we observe that within solvers such as SOSTOOLS, the polynomial $u(x)$ is represented in the form $u(x) = z^T Q z$ where z is a vector of monomials in x of a specified order and Q is a coefficient matrix of appropriate dimensions. Then, the condition that the absolute value of each entry of Q is less than some constant c is written as $c\mathbb{1} - \text{vec}(Q) \geq 0$ and $\text{vec}(Q) + c\mathbb{1} \geq 0$ where $\text{vec}(Q)$ is the vector form of matrix Q and $\mathbb{1}$ is the vector of ones of appropriate dimension.

Finally, we propose solving our primary control synthesis objective using Algorithm 3 which interleaves Algorithm

Algorithm 3 Search for control polynomial $u(x)$

procedure COMPUTE-$u_{goal}(P_{goal}, \sigma, \alpha, n_B, n_u, \epsilon)$
  $i_{count} = 1$ ▷ Counting var., $\tilde{\alpha}$ & $\tilde{\beta}$ for discrete-time
  while $|P^* - P_{goal}| > \epsilon$ **do**
    if $i_{count} = 1$ **then**
      $\beta, P \leftarrow$ COMPUTE- $B(l_\alpha, u_\alpha, d, \sigma, u(x), n_B)$
      $u(x) \equiv 0$ ▷ Since α fixed, $l_\alpha = u_\alpha$
      $i_{count} := i_{count} + 1$
    else
      $u(x), c, Q \leftarrow$ COMPUTE-$u(B(x), \alpha, \beta, n_u)$
      $\beta, P \leftarrow$ COMPUTE-$B(l_\alpha, u_\alpha, d, \sigma, u(x), n_B)$
    end if
    if $P < P_{goal}$ **and** $c < c^*$ **then**
      $\beta^* := \beta$, $P^* := P$, $c^* := c$
      ▷ c^* is initialized as a large number
    end if
    if $P > P_{goal}$ **then**
      $\beta := a_{dec}\beta$ ▷ $a_{inc} > 1$ & $a_{dec} < 1$ are scalars
    else
      $\beta := a_{inc}\beta$
    end if
  end while
  return $u^*(x), c^*, Q$
end procedure

1 and Algorithm 2. First, Algorithm 3 computes a polynomial barrier $B(x)$ given a fixed nominal control policy, namely, $u(x) \equiv 0$. Then, Algorithm 3 iteratively synthesizes a feedback control law by adjusting the parameter β. While effective, Algorithm 3 is not guaranteed to find either a control polynomial or a barrier function which satisfy the SOSP constraints. As a result, during implementation a designer will have to introduce algorithm termination conditions. Algorithm 3 is not computationally intensive for well chosen step sizes of α, i.e., $0.01 \leq d \leq 1$. For discrete-time, the reciprocal of these values can be used for $\tilde{\alpha}$. Coarser spacing values can lead to trivial bounds. Notably, computational time increases significantly with the number of system states.

4 Case Studies

In this section, we utilize SOSTOOLS [11] and the semidefinite program solver SDPT3 [17, 18] to solve SOSPs for several case studies conducted on a 2.3 GHz Intel Core i5 computer with 8GB of memory. [2]

4.1 Continuous-time Control Synthesis

Consider the stochastic nonlinear dynamics

$$dx_1 = x_2 dt \tag{29}$$

$$dx_2 = \Big(-x_1 - x_2 - x_1^3 + u(x) \Big) dt + \sigma dw \tag{30}$$

with constant σ. This system is studied in [13] without the input term $u(x)$.

We define the state space as $\mathcal{X} = \{(x_1, x_2) \mid -3 \leq x_1 \leq 2, -2 \leq x_2 \leq 3\}$, $\mathcal{X}_u = \{x_2 \mid x_2 \geq 2.25\}$, and $\mathcal{X}_0 =$

[2] The MATLAB source code for the case studies is contained at `https://github.com/gtfactslab/stochasticbarrierfunctions`

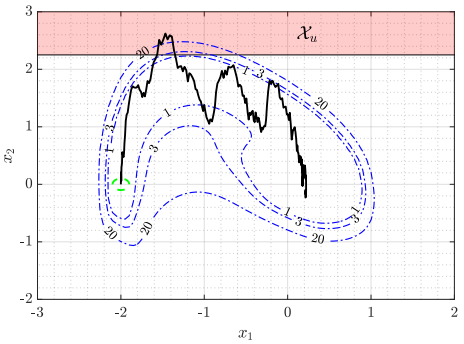

Fig. 1. Given the initial conditions $x_0 = [-2, 0]$, the single trajectory dynamics of (29)–(30) for a time horizon of $T = 2$ and a $\sigma = 1.0$ are illustrated. The unsafe region is $\mathcal{X}_u = \{x_2 \mid x_2 \geq 2.25\}$ with the level sets of $B(x)$ and their respective values given as dashed blue lines.

σ	$\mathbf{P_{u(x)\equiv 0}}$	α	$\min \mathbf{c}$
0.6	0.860	1.4	2.1821
0.9	0.919	1.3	0.5251
1.0	0.912	1.3	0.6396
1.3	0.949	1.5	1.1488

Table 1
The resulting control polynomial $u(x)$ which reduces the probability of failure to $P_{goal} = 0.10$ for (29)–(30). The upper-bound on the probability of failure without a given control input is given for comparison.

$\{(x_1, x_2) | (x_1 + 2)^2 + x_2^2 \leq 0.1^2\}$. A sample trajectory of (29)–(30) is illustrated in Fig. 1. Additionally, level sets of $B(x)$, computed from Algorithm 1 assuming $u(x) \equiv 0$, are projected onto the state space.

In this particular trajectory illustration, the evolution of system noise is enough for the system to enter the predefined unsafe set. For values of σ ranging from 0.5 to 1.5, Monte Carlo simulations indicate that the probability of failure over a finite-time horizon ranges from about 0.3 to 0.8. Our objective is to compute a feedback control law to reduce the probability of failure to $P_{goal} = 0.10$, where we consider several values for σ. We restrict the search to a second order polynomial controller $u(x)$ and tenth order $B(x)$, and the results of Algorithm 3 are highlighted in Table 1 for select values of σ and specific α values.

4.2 Discrete-Time Population Model

Consider the discrete-time population growth model adapted from [5]

$$x_1[k+1] = m_3 x_2[k] + u(x[k]) \tag{31}$$
$$x_2[k+1] = m_1 x_1[k] + m_2 x_2[k] + \sigma\xi[k] \tag{32}$$

where $m_1 = 0.5$, $m_2 = 0.95$, and $m_3 = 0.5$. Here, ξ is a stochastic disturbance with a standard normal distribution. For (31)–(32), we perform control synthesis using 1st order barrier functions as a result of the observation made in Section 3 regarding the term $\mathbb{E}[B(F(x, \xi))]$.

We define $\mathcal{X} = \{x_1, x_2 \mid 0 \leq x_1 \leq 4, 0 \leq x_2 \leq 4\}$, $\mathcal{X}_u = \{x_1 \mid 2 \leq x_1 \leq 4\}$ and $\mathcal{X}_0 = \{x_1, x_2 \mid x_1^2 + x_2^2 \leq 1.5\}$,

σ	$\mathbf{P_{u(x)\equiv 0}}$	$\tilde{\alpha}$	$\min \mathbf{c}$
1.0	0.499	2	1.44
1.5	0.512	2.05	2.074
2.0	0.523	2.10	2.488
2.5	0.544	2.20	2.986

Table 2
The c values from implementing Algorithm 3 for (31)–(32) using a 1st order barrier function for $P_{goal} = 0.10$. The last column gives the value of c which encourages a low-energy control effort for a 2nd order $u(x)$.

and we consider affine barrier functions $B(x)$. We take $N = 3$ and $P_{goal} = 0.10$. The results of control synthesis are presented in Table 2.

5 Conclusion

We consider both continuous-time and discrete-time stochastic control barrier functions whose existence provides a means of quantifying an upper bound on a system's probability of failure. Having found a barrier function for a particular system, we propose a numerical method which relies on such a barrier function to compute control polynomials that reduce the bound on a system's probability of failure. As a result, this reduces a system's probability of failure. Furthermore, we build upon techniques developed for continuous-time systems in the discrete-time domain. We present two case studies which illustrate the control synthesis techniques over a finite-time horizon.

References

[1] Agrawal, A. and Sreenath, K. (2017). Discrete control barrier functions for safety-critical control of discrete systems with application to bipedal robot navigation. In *Robotics: Science and Systems*.

[2] Ames, A. D., Coogan, S., Egerstedt, M., Notomista, G., Sreenath, K., and Tabuada, P. (2019). Control barrier functions: Theory and applications. In *2019 18th European Control Conference (ECC)*, pages 3420–3431. IEEE.

[3] Ames, A. D., Grizzle, J. W., and Tabuada, P. (2014). Control barrier function based quadratic programs with application to adaptive cruise control. In *IEEE Conference on Decision and Control (CDC)*, pages 6271–6278. IEEE.

[4] Ames, A. D., Xu, X., Grizzle, J. W., and Tabuada, P. (2017). Control barrier function based quadratic programs for safety critical systems. *Automatic Control, IEEE Transactions on*, 62(8):3861–3876.

[5] Iannelli, M. and Pugliese, A. (2015). *An Introduction to Mathematical Population Dynamics: Along the Trail of Volterra and Lotka*, volume 79. Springer.

[6] Jagtap, P., Soudjani, S., and Zamani, M. (2018). Temporal logic verification of stochastic systems using barrier certificates. In *International Symposium on Automated Technology for Verification and Analysis*, pages 177–193. Springer.

[7] Jagtap, P., Soudjani, S., and Zamani, M. (2019). Formal synthesis of stochastic systems via control barrier certificates. *arXiv preprint arXiv:1905.04585*.

[8] Kushner, H. (1966). Finite time stochastic stability and the analysis of tracking systems. *Automatic Control, IEEE Transactions on*, 11(2):219–227.

[9] Kushner, H. (1971). Introduction to stochastic control. Technical report, Brown University Providence, RI Division of Applied Mathematics.

[10] Kushner, H. J. (1967). *Stochastic stability and control*. Mathematics in science and engineering, v.33. Academic Press, New York.

[11] Papachristodoulou, A., Anderson, J., Valmorbida, G., Prajna, S., Seiler, P., and Parrilo, P. A. (2013). *SOSTOOLS: Sum of squares optimization toolbox for MATLAB*. `http://arxiv.org/abs/1310.4716`.

[12] Prajna, S., Jadbabaie, A., and Pappas, G. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *Automatic Control, IEEE Transactions on*, 52(8):1415–1428.

[13] Prajna, S., Jadbabaie, A., and Pappas, G. J. (2004). Stochastic safety verification using barrier certificates. In *IEEE Conference on Decision and Control, 2004*, pages 929–934. IEEE.

[14] Santoyo, C., Dutreix, M., and Coogan, S. (2019). Verification and control for finite-time safety of stochastic systems via barrier functions. In *2019 IEEE Conference on Control Technology and Applications (CCTA)*, pages 712–717. IEEE.

[15] Soudjani, S. E. Z., Gevaerts, C., and Abate, A. (2015). FAUST^2 : Formal abstractions of uncountable-state stochastic processes. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 272–286. Springer.

[16] Steinhardt, J. and Tedrake, R. (2012). Finite-time regional verification of stochastic non-linear systems. *The International Journal of Robotics Research*, 31(7):901–923.

[17] Toh, K., Todd, M., and Tutuncu, R. (1999). SDPT3 - a MATLAB software package for semidefinite programming, version 1.3. *Optimization Methods & Software*, 11-2(1–4):545–581.

[18] Toh, K. C., Todd, M. J., and Tutuncu, R. (2003). Solving semidefinite-quadratic-linear programs using sdpt3. *Mathematical Programming*, 95(2):189–217.

[19] Vinod, A. P., Gleason, J. D., and Oishi, M. M. (2019). SReachTools: a MATLAB stochastic reachability toolbox. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, pages 33–38. ACM.

[20] Wang, L., Ames, A. D., and Egerstedt, M. (2017). Safety barrier certificates for collisions-free multirobot systems. *Robotics, IEEE Transactions on*, 33(3):661–674.

[21] Wieland, P. and Allgöwer, F. (2007). Constructive safety using control barrier functions. *IFAC Proceedings Volumes*, 40(12):462–467.