2021 60th IEEE Conference on Decision and Control (CDC)
December 13-15, 2021. Austin, Texas

Safety-Critical Control of Stochastic Systems using Stochastic Control Barrier Functions

Chuanzheng Wang[†], Yiming Meng[†], Stephen L. Smith, Jun Liu

2021 60th IEEE Conference on Decision and Control (CDC) | 978-1-6654-3659-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CDC45484.2021.9683349

Abstract— **Control barrier functions have been widely used for synthesizing safety-critical controls, often via solving quadratic programs. However, the existence of Gaussian-type noise may lead to unsafe actions and result in severe consequences. In this paper, we study systems modeled by stochastic differential equations (SDEs) driven by Brownian motions. We propose a notion of stochastic control barrier functions (SCBFs) and show that SCBFs can significantly reduce the control efforts, especially in the presence of noise, compared to stochastic reciprocal control barrier functions (SRCBFs), and offer a less conservative estimation of safety probability, compared to stochastic zeroing control barrier functions (SZCBFs). Based on this less conservative probabilistic estimation for the proposed notion of SCBFs, we further extend the results to handle high relative degree safety constraints using high-order SCBFs. We demonstrate that the proposed SCBFs achieve good trade-offs of performance and control efforts, both through theoretical analysis and numerical simulations.**

I. INTRODUCTION

For some real-world control problems, safety-critical control must be used in order to prevent severe consequences. It requires not only achieving control objectives, but also providing control actions with guaranteed safety [8]. Hence incorporating safety criteria is of great importance in practice when designing controllers. These requirements need to be satisfied in practice both with or without noise and disturbance. In [12], the notion of safety control was first proposed in the form of correctness. It was then formalized in [1], where the authors stated that a safety property stipulates that some “bad thing” does not happen during execution. There has been extensive research in safety verification problems using , e.g. discrete approximations [16] and computation of reachable sets [9].

One recent framework is to use control barrier functions (CBFs) to deal with safety criteria [2]. CBFs are combined with control Lyapunov functions (CLFs) as constraints of quadratic programming (QP) problems in [3]. The authors show that safety criteria can be transformed into linear constraints of the QP problems for control inputs. By solving the QP problems, we will find out a sequence of actions that generate safe trajectories during execution. It is shown in [17] that finding safe control inputs by solving QP problems can be extended to an arbitrary number of constraints and any nominal control law. As a result, CBFs are widely used recently in a variety of applications such as lane keeping [4] and obstacle avoidance [5]. Since solving QP problems using CBFs requires that the derivative of CBFs is dependent of the control input, which is not always the case for real time application of robotics [10], CBFs are extended to handle high order relative degree as in [14] and [22]. The authors of [14] propose a way of designing exponential control barrier functions (ECBFs) using input-output linearization and in [22] the authors propose a more general form of high-order control barrier functions (HOCBFs).

In practice, models used to design controllers are imperfect and this imperfection may lead to unsafe or even dangerous behavior. As a result, synthesizing a controller considering uncertainty is of great importance. Bounded disturbance is used to model such uncertainty as in [20] and [21], in which the time derivative of barrier functions are separated into the time derivative of the nominal barrier function and a remainder that can be approximated using neural networks. For systems driven by Gaussian-type noise, stochastic differential equations against Brownian motions are usually used to characterize the effect of randomness. Previous studies on stochastic stability, given diffusion-type SDEs, have a wide variety of applications in verifying probabilistic quantification of safe set invariance [11]. Investigations are focused on the worst-case safety verification utilizing SZCBFs regardless of the intensity of noise. The authors in [18] proposed a method for synthesizing polynomial state feedback controllers that achieve a specified probability of safety based on the existing verification results. In connection to stochastic hybrid systems with more complex specifications, [15] proposed a compositional framework for the construction of control barrier functions for networks of continuous-time stochastic hybrid systems enforcing complex logic specifications expressed by finite-state automata. However, the conservative quantification fails to be applied to high-order control systems due to the low-quality estimation. The authors in [19] applied the strong set-invariance certificate (generated by SRCBFs) from [6] to high-order stochastic control systems. The conditions are rather strong and able to effectively cancel the effects of diffusion to force a probability-one path safety. However, the above results admit unbounded control inputs; the hard constraints may cause failures of satisfying safety specifications.

A. Contributions

Motivated by the need to reduce potentially severe control constraints generated by SRCBF certificates [6] in the neighborhood of the safety boundary (see Section III-B for

[†]Equal contribution

Chuanzheng Wang, Yiming Meng and Jun Liu are with the Department of Applied Mathematics, University of Waterloo, Waterloo, Ontario, Canada, {cz.wang, yiming.meng, j.liu}@uwaterloo.ca

Stephen L. Smith is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada, stephen.smith@uwaterloo.ca

an illustrative example and Section IV-A for numerical comparisons), and improving the worst-case safety probability provided by SZCBF certificates, we propose SCBFs as a middle ground to characterize safety properties for systems driven by Brownian motions in this paper. We show that SCBFs generate milder conditions compared to SRCBFs at the cost of sacrificing the almost-sure safety. The verification results, which provide a non-vanishing lower bound of safety probability for any finite time period, are still less conservative than widely used SZCBFs.

Unlike control systems with relative degree one, where optimal control schemes can be applied to synthesize finite-time almost-surely reachability/safety controller [11, Chapter 5] or even to characterize the probabilistic winning set of finite-time reachability/safety with a priori probability requirement [7], off-the-shelf optimal control schemes and numerical tools cannot be straightforwardly applied for stochastic control systems with high relative degree. Nonetheless, we make a first attempt to discover high-order SCBFs properties.

The main contributions are summarized as follows.

- We propose a notion of stochastic control barrier functions (SCBFs) for safety-critical control. We show both theoretically and empirically that the proposed SCBFs achieve good trade-offs between mitigating the severe control constraints (potentially unbounded control inputs) and quantifying the worse-case safety probability.
- Based on the less conservative worse-case safety probability, we extend our result to high-order SCBFs in handling high relative degree safety constraints and formally prove the worst-case safety probability.
- We validate our work in simulation and show that the proposed SCBFs with high relative degree have less control effort compared with SRCBFs and better safe probability compared with SZCBFs.

Notation

We denote the Euclidean space by $\mathbb{R}^n$ for $n > 1$. Let $(\Omega, \mathscr{F}, \{\mathscr{F}_t\}_{t\geq 0}, \mathbb{P})$ be a filtered probability space. For any continuous-time stochastic processes $\{X_t\}_{t\geq 0}$ we use the shorthand notation $X := \{X_t\}_{t\geq 0}$ instead, and denote $\langle X \rangle_t$ by the quadratic variation. We denote $\mathbf{u}$ by a set of constrained control signals. In addition, let $\mathbb{P}_x$ be the probability measure of a stochastic process X with the initial condition $X_0 = x$ $\mathbb{P}$-a.s.; correspondingly, we denote $\mathbb{E}^x$ by the expectation w.r.t. the probability measure $\mathbb{P}_x$ (i.e. $\mathbb{E}^x[f(X_t)] := \mathbb{E}[f(X_t)|X_0 = x]$).

We say a function $\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ belongs to class $\mathcal{K}$ if it is continuous, zero at zero, and strictly increasing. It is said to belong to $\mathcal{K}_\infty$ if it belongs to class $\mathcal{K}$ and is unbounded. For a given set $\mathcal{C}$, we refer $\mathcal{C}^\circ$ as the interior.

II. Preliminary and Problem Definition

A. System Description

Given a filtered probability space $(\Omega, \mathscr{F}, \{\mathscr{F}_t\}, \mathbb{P})$ with a natrual filtration, a state space $\mathcal{X} \subseteq \mathbb{R}^n$, a (compact) set of control values $\mathcal{U} \subset \mathbb{R}^p$, consider a continuous-time stochastic process $X : [0, \infty) \times \Omega \to \mathcal{X}$ that solves the SDE

$$dX_t = (f(X_t) + g(X_t)u(t))dt + \sigma(X_t)dW_t, \qquad (1)$$

where $u : \mathbb{R}_{\geq 0} \to \mathcal{U}$ is a bounded measurable control signal; W is a d-dimensional standard $\{\mathscr{F}\}_t$-Brownian motion; $f : \mathcal{X} \to \mathbb{R}^n$ is a nonlinear vector field; $g : \mathcal{X} \to \mathbb{R}^{n\times p}$ and $\sigma : \mathcal{X} \to \mathbb{R}^{n\times d}$ are smooth mappings.

Assumption II.1. *We make the following assumptions on system* (1) *for the rest of this paper:*

(i) *There is a $\xi \in \mathcal{X}$ such that $\mathbb{P}[X_0 = \xi] = 1$;*
(ii) *The mappings f, g, σ satisfy local Lipschitz continuity and a linear growth condition.*

Definition II.2 (Strong solutions)**.** *A stochastic process X is said to be a strong solution to* (1) *if it satisfies the following integral equation*

$$X_t = \xi + \int_0^t (f(X_s) + g(X_s)u(s))ds + \int_0^t \sigma(X_s)dW_s, \quad (2)$$

where the stochastic integral is constructed based on the given Brownian motion W.

Remark II.3. (i) *Under Assumption II.1, the SDE* (1) *admits a unique strong solution.*
(ii) *Weak solutions are in the sense that Brownian motions are constructed posteriori for the stochastic integrals.*

We exclude the consideration of weak solutions in this paper to guarantee that Lyapunov-type analysis on sample paths behaviors is based on the same Brownian motion.

Definition II.4 (Infinitesimal generator of X_t)**.** *Let X be the strong solution to* (1)*, the infinitesimal generator $\mathcal{A}$ of X_t is defined by*

$$\mathcal{A}h(x) = \lim_{t\downarrow 0} \frac{\mathbb{E}^x[h(X_t)] - h(x)}{t}; \;\; x \in \mathbb{R}^n, \qquad (3)$$

where $h : \mathbb{R}^n \to \mathbb{R}$ is in a set $\mathcal{D}(\mathcal{A})$ (called the domain of the operator $\mathcal{A}$) of functions such that the limit exists at x.

Proposition II.5 (Dynkin)**.** *Let X solve* (1)*. If $h \in C_0^2(\mathbb{R}^n)$ then $h \in \mathcal{D}(\mathcal{A})$ and*

$$\mathcal{A}h(x) = \frac{\partial h}{\partial x}(f(x)+g(x)u(t)) + \frac{1}{2}\sum_{i,j}\left(\sigma\sigma^T\right)_{i,j}(x)\frac{\partial^2 h}{\partial x_i \partial x_j}. \qquad (4)$$

Remark II.6. *The solution X to* (1) *is right continuous and satisfies strong Markov properties, and for any finite stopping time τ and $h \in C_0^2(\mathbb{R}^n)$, we have the following Dynkin's formula*

$$\mathbb{E}^\xi[h(X_\tau)] = h(\xi) + \mathbb{E}^\xi\left[\int_0^\tau \mathcal{A}h(X_s)ds\right],$$

and therefore

$$h(X_\tau) = h(\xi) + \int_0^t \mathcal{A}h(X_s)ds + \int_0^\tau \nabla_x h(X_s)dW_s.$$

The above is an analogue of the evolution of h along trajectories

$$h(x(t)) = h(\xi) + \int_0^t [L_f h(x(s)) + L_g h(x(s))u(s)]ds$$

driven by deterministic dynamics $\dot{x} = f(x) + g(x)u$, where $L_f h = \nabla_x h(x) \cdot f(x)$ and $L_g h = \nabla_x h(x) \cdot g(x)$.

B. Set Invariance and Control

In deterministic settings, a set $\mathcal{C} \subseteq \mathcal{X}$ is said to be invariant for a dynamical system $\dot{x} = f(x)$ if, for all $x(0) \in \mathcal{C}$, the solution $x(t)$ is well defined and $x(t) \in \mathcal{C}$ for all $t \geq 0$. As for stochastic analogies, we have the following probabilistic characterization of set invariance.

Definition II.7 (Probabilistic set invariance)**.** *Let X be a stochastic process. A set $\mathcal{C} \subset \mathcal{X}$ is said to be invariant w.r.t. a tuple (x, T, p) for X, where $x \in \mathcal{C}$, $T \geq 0$, and $p \in [0, 1]$, if $X_0 = x$ a.s. implies*

$$\mathbb{P}_x[X_t \in \mathcal{C},\ 0 \leq t \leq T] \geq p. \tag{5}$$

Moreover, if $\mathcal{C} \subset \mathcal{X}$ is invariant w.r.t. $(x, T, 1)$ for all $x \in \mathcal{C}$ and $T \geq 0$, then $\mathcal{C}$ is strongly invariant for X.

For stochastic dynamical systems with controls such as system (1), we would like to define similar probabilistic set invariance property for the controlled processes. Before that, we first define the following concepts.

Definition II.8 (Control strategy)**.** *A control strategy is a set-valued function*

$$\kappa : \mathcal{X} \to 2^{\mathcal{U}}. \tag{6}$$

We use a boldface $\mathbf{u}$ to indicate a set of constrained control signals. A special set of such signals is given by a control strategy as defined below.

Definition II.9 (State-dependent control)**.** *We say that a control signal u conforms to a control strategy κ for (1), and writes $u \in \mathbf{u}_\kappa$, if*

$$u(t) \in \kappa(X_t), \quad \forall t \geq 0, \tag{7}$$

where X satisfies (1) with u as input. The set of all control signals that confirm to κ is denoted by $\mathbf{u}_\kappa$.

Definition II.10 (Controlled probabilistic invariance)**.** *Given system* (1) *and a set of control signals* $\mathbf{u}$*, a set $\mathcal{C} \subset \mathcal{X}$ is said to be controlled invariant under* $\mathbf{u}$ *w.r.t. a tuple (x, T, p) for system* (1)*, if for all $u \in \mathbf{u}$, $\mathcal{C}$ is invariant w.r.t. (x, T, p) for X, where X is the solution to* (1) *with u as input.*

Similarly, $\mathcal{C} \subset \mathcal{X}$ is strongly controlled invariant under $\mathbf{u}$ *if $\mathcal{C} \subset \mathcal{X}$ is controlled invariant under* $\mathbf{u}$ *w.r.t. $(x, T, 1)$ for all $x \in \mathcal{C}$ and $T \geq 0$.*

C. Problem Definition

For the rest of this paper, we consider a safe set of the form

$$\mathcal{C} := \{x \in \mathcal{X} : h(x) \geq 0\}, \tag{8}$$

where $h : \mathcal{X} \to \mathbb{R}$ is a high-order continuously differentiable function. We also define the boundary and interior of $\mathcal{C}$ explicitly as below

$$\partial\mathcal{C} := \{x \in \mathcal{X} : h(x) = 0\}, \tag{9}$$

$$\mathcal{C}^\circ := \{x \in \mathcal{X} : h(x) > 0\}. \tag{10}$$

Problem II.11 (Probabilistic set invariance control)**.** *Given a compact set $\mathcal{C} \subset \mathcal{X}$ defined in* (8)*, a point $\xi \in \mathcal{C}^\circ$, and a tuple (ξ, T, p), design a control strategy κ such that under $\mathbf{u}_\kappa$, the interior $\mathcal{C}^\circ$ is controlled invariant w.r.t. (ξ, T, p) for the resulting strong solutions to* (1).

III. Safe-critical Control Design via Barrier Functions

In this section, we propose stochastic barrier certificates that can be used to design a control strategy κ for Problem II.11. Before proceeding, it is necessary to review (stochastic) control barrier functions to interpret (probabilistic) set invariance. Note that we consider the safe set as constructed in (8), where the function h is given a priori.

A. Stochastic Reciprocal and Zeroing Barrier Functions

Similar to the terminology for deterministic cases [4], we introduce the construction of stochastic control barrier functions as follows.

Definition III.1 (SRCBF)**.** *A function $B : \mathcal{C}^\circ \to \mathbb{R}$ is called a stochastic reciprocal control barrier function (SRCBF) for system* (1) *if $B \in \mathcal{D}(\mathcal{A})$ and satisfies the following properties:*

(i) *there exist class-$\mathcal{K}$ functions α_1, α_2 such that for all $x \in \mathcal{X}$ we have*

$$\frac{1}{\alpha_1(h(x))} \leq B(x) \leq \frac{1}{\alpha_2(h(x))}; \tag{11}$$

(ii) *there exists a class-$\mathcal{K}$ function α_3 such that*

$$\inf_{u \in \mathcal{U}} [\mathcal{A}B(x) - \alpha_3(h(x))] \leq 0. \tag{12}$$

We refer to the control strategy generated by (12) *as*

$$\varrho(x) := \{u \in \mathcal{U} : \mathcal{A}B(x) - \alpha_3(h(x)) \leq 0\} \tag{13}$$

and the corresponding control constraint as $\mathbf{u}_\varrho$ (see in Definition II.9).

Proposition III.2 ([6])**.** *Suppose that there exists an SRCBF for system* (1)*. If $u(t) \in \mathbf{u}_\upsilon$, then for all $t \geq 0$ and $X_0 = \xi \in \mathcal{C}^\circ$, we have $\mathbb{P}_\xi[X_t \in \mathcal{C}^\circ] = 1$ for all $t \geq 0$.*

Remark III.3. *The result admits a $\mathbb{P}$-a.s. controlled invariant set for the marginals of X, and is easily extended to a pathwise $\mathbb{P}$-a.s. controlled set invariance. Note that the strong solution is right continuous. Let $\{t_n,\ n = 1, 2, ...\}$ be the set of all rational numbers in $[0, \infty)$, and put*

$$\Omega^* := \bigcap_{1 \leq n < \infty} \{\omega : X_{t_n} \in \mathcal{C}^\circ\},$$

then $\Omega^* \in \mathscr{F}$ *(a* σ*-algebra is closed w.r.t. countable intersections). Since* $\mathbb{Q}$ *is dense in* $\mathbb{R}$*,* X *is right continuous, and* h *is continuous, we have*

$$\Omega^* := \{\omega : X_t \in \mathcal{C}^\circ,\ \forall t \in [0, \infty)\}.$$

Note that $\mathbb{P}_\xi[\Omega^*] \equiv 1$ *from the marginal result.*

Definition III.4 (SZCBF)**.** *A function* $B : \mathcal{C} \to \mathbb{R}$ *is called a stochastic zeroing control barrier function (SZCBF) for system* (1) *if* $B \in \mathcal{D}(\mathcal{A})$ *and*

(i) $B(x) \geq 0$ *for all* $x \in \mathcal{C}$*;*
(ii) $B(x) < 0$ *for all* $x \notin \mathcal{C}$*;*
(iii) *there exists an extended* $\mathcal{K}_\infty$ *function* α *such that*

$$\sup_{u \in \mathcal{U}} [\mathcal{A}B(x) + \alpha(B(x))] \geq 0. \tag{14}$$

We refer the control strategy generated by (14) *as*

$$\varkappa(x) := \{u \in \mathcal{U} : \mathcal{A}B(x) + \alpha(B(x)) \geq 0\} \tag{15}$$

and the corresponding set of constrained control signals as $\mathbf{u}_\varkappa$*.*

Proposition III.5 (Worst-case probabilistic quantification)**.** *Suppose the mapping* h *is an SZCBF with linear function* kx *as the class-*$\mathcal{K}$ *function (where* $k > 0$*), and the control strategy as* $\varkappa(x) = \{u \in \mathcal{U} : \mathcal{A}h(x) + kh(x) \geq 0\}$*. Let* $c = \sup_{x \in \mathcal{C}} h(x)$ *and* $X_0 = \xi \in \mathcal{C}^\circ$*, then under any* $u \in \mathbf{u}_\varkappa$ *we have the following worst-case probability estimation:*

$$\mathbb{P}_\xi [X_t \in \mathcal{C}^\circ,\ 0 \leq t \leq T] \geq \left(\frac{h(\xi)}{c}\right) e^{-cT}. \tag{16}$$

Proof. Let $s = c - h(\xi)$ and $V(x) = c - h(x)$, then $V(x) \in [0, c]$ for all $x \in \mathcal{C}$. It is clear that $\mathcal{A}V(x) = -\mathcal{A}h(x)$. For $u(t) \in \mathbf{u}_\varkappa$ for all $t \in [0, T]$, we have

$$\mathcal{A}V(x) \leq -kV(x) + kc.$$

By [11, Theorem 3.1],

$$\mathbb{P}_\xi \left[\sup_{t \in [0,T]} V(X_t) \geq c\right] \leq 1 - \left(1 - \frac{s}{c}\right) e^{-cT}. \tag{17}$$

The result follows directly after this. □

In proposing stochastic control barrier functions for high-order control systems, the above SRCBF and SZCBF are building blocks. The authors in [19] constructed high-order SRCBF and have found the sufficient conditions to guarantee pathwise set invariance with probability 1. While the results seem strong, they come with significant costs. At the safety boundary, the control inputs need to be unbounded (as shown in the motivating example below and in the numerical experiments in Section IV). On the other hand, the synthesis of controller for a high-order system via SZCBF is with mild constraints. The trade-off is that the probability estimation of set invariance is of low quality (note that the worst-case probability estimation using first-order barrier function is already lower bounded by a small value over a relatively long time period). We propose high-order stochastic control barrier functions in subsection C in order to reduce the high control efforts and improve the worst-case quantification. Before proceeding, we illustrate the above motivation through examples.

B. A Motivating Example

In this section, we will discuss how reciprocal control barrier functions (RCBFs) and SRCBFs perform differently around the boundary of the safe set. We show that for deterministic systems, RCBFs can guarantee safety with bounded control while for stochastic systems, SRCBFs require unbounded control in order to keep systems safe. We use the following two simple one-dimensional systems:

$$\dot{x} = x + u,$$

and

$$dx = (x + u)dt + \sigma dW,$$

for the comparison. Suppose that our safe set is $\{x \in \mathbb{R} \big| x < 1\}$ so that we can use $h(x) = 1 - x$. Accordingly, a RCBF for the deterministic system is $B = \frac{1}{h}$. We choose $\gamma = 1$ as in [4] and [6] and, as a result, the condition using the RCBF is

$$L_f B(x) + L_g B(x) u = \frac{1}{h^2}(x + u) \leq h,$$
$$u \leq (1 - x)^3 - x.$$

It means that we can control the system safely using a control bounded by $(1 - x)^3 - x$ when $x \to 1$. However, for the stochastic system, we have $\frac{\partial^2 B}{\partial x^2} = \frac{2}{h^3}$. Then the SRCBF condition is

$$\mathcal{A}B = \frac{1}{h^2}(x + u) + \frac{\sigma^2}{h^3} \leq h,$$
$$u \leq h^3 - x - \frac{\sigma^2}{h}.$$

As x approaches 1, the control approaches $-\infty$. This implies that in order to guarantee safety, we requires an unbounded control around the boundary of the safe set for stochastic systems, which can be difficult to satisfy for some practical applications, as shown in Section IV-A.

C. High-order Stochastic Control Barrier Functions

To obtain non-vanishing worst-case probability estimation (compared to SZCBF), we propose a safety certificate via a stochastic Lyapunov-like control barrier function [11].

Definition III.6 (Stochastic control barrier functions)**.** *A continuously differentiable function* $B : \mathbb{R}^n \to \mathbb{R}$ *is said to be a stochastic control barrier function (SCBF) if* $B \in \mathcal{D}(\mathcal{A})$ *and the following conditions are satisfied:*

(i) $B(x) \geq 0$ *for all* $x \in \mathcal{C}$*;*
(ii) $B(x) < 0$ *for all* $x \notin \mathcal{C}$*;*
(iii) $\sup_{u \in \mathcal{U}} \mathcal{A}B(x) \geq 0$.

We refer the control strategy generated by (iii) as

$$\upsilon(x) := \{u \in \mathcal{U} : \mathcal{A}B(x) \geq 0\} \tag{18}$$

and the corresponding set of constrained control signals as $\mathbf{u}_\upsilon$.

Remark III.7. *Condition (iii) of the above definition is an analogue of* $\sup_{u\in\mathcal{U}}[L_fB(x)+L_gB(x)u] \geq 0$ *for the deterministic settings. The consequence is such that* $\mathbb{E}^\xi[B(x)] \geq B(x)$ *for all* $x \in \mathcal{C}$*. A relaxation of condition (iii) is given in the deterministic case such that the set invariance can still be guaranteed [21],*

$$\sup_{u\in\mathcal{U}}[L_fB(x)+L_gB(x)u] \geq -\alpha(B(x)),$$

where α *is a class-*$\mathcal{K}$ *function. If* $\alpha(x) = kx$ *where* $k > 0$*, under the stochastic settings, the condition formulates an SZCBF and provides a much weaker quantitative estimation of the lower bound of satisfaction probability. In comparison with SZCBF, we provide the worst-case quantification in the following proposition.*

Proposition III.8. *Suppose the mapping* h *is an SCBF with the corresponding control strategy* $\upsilon(x)$*. Let* $c = \sup_{x\in\mathcal{C}} h(x)$ *and* $X_0 = \xi \in \mathcal{C}^\circ$*, then under the set of constrained control signals* $\mathbf{u}_\upsilon$*, we have the following worst-case probability estimation:*

$$\mathbb{P}_\xi\left[X_t \in \mathcal{C}^\circ,\ 0 \leq t < \infty\right] \geq \frac{h(\xi)}{c}.$$

Proof. Let $V = c - h(x)$, then $V(x) \geq 0$ for all $x \in \mathcal{X}$ and $\mathcal{A}V \leq 0$. Let $s = c - h(\xi)$ then $s \leq c$ by definition. The result for every finite time interval $t \in [0, T]$ is followed by [11, Lemma 2.1],

$$\mathbb{P}_\xi\left[X_t \in \mathcal{C}^\circ,\ 0 \leq t < T\right] \geq 1 - \frac{s}{c}.$$

The result follows by letting $T \to \infty$. □

Definition III.9. *A function* $B : \mathcal{X} \to \mathbb{R}$ *is called a stochastic control barrier function with relative degree* r *for system* (1) *if* $B \in \mathcal{D}(\mathcal{A}^r)$*, and* $\mathcal{A}\circ\mathcal{A}^{r-1}h(x) \neq 0$ *as well as* $\mathcal{A}\circ\mathcal{A}^{j-1}h(x) = 0$ *for* $j = 1, 2, \ldots, r-1$ *and* $x \in \mathcal{C}$*.*

If the system (1) is an r^{th}-order stochastic control system, to steer the process X to satisfy probabilistic set invariance w.r.t. $\mathcal{C}$, we recast the mapping h as an SCBF with relative degree r. For $h \in \mathcal{D}(\mathcal{A}^r)$, we define a series of functions $b_0, b_j : \mathcal{X} \to \mathbb{R}$ such that for each $j = 1, 2, \ldots, r$ $b_0, b_j \in \mathcal{D}(\mathcal{A})$ and

$$\begin{aligned} &b_0(x) = h(x),\\ &b_j(x) = \mathcal{A}\circ\mathcal{A}^{j-1}b_0(x). \end{aligned} \tag{19}$$

We further define the corresponding superlevel sets $\mathcal{C}_j$ for $j = 1, 2, \ldots, r$ as

$$\mathcal{C}_j = \{x \in \mathbb{R}^n : b_j(x) \geq 0\}. \tag{20}$$

Theorem III.10. *If the mapping* h *is an SCBF with relative degree* r*, the corresponding control strategy is given as* $\upsilon(x) = \{u \in \mathcal{U} : \mathcal{A}^r h(x) \geq 0\}$*. Let* $c_j =: \sup_{x\in\mathcal{C}_j} b_j(x)$ *for each* $j = 0, 1, ..., r$ *and* $X_0 = \xi \in \bigcap_{j=0}^r \mathcal{C}_j^\circ$*. Then under the set of constrained control signals* $\mathbf{u}_\upsilon$*, we have the following worst-case probability estimation:*

$$\mathbb{P}_\xi[X_t \in \mathcal{C}^\circ,\ 0 \leq t < \infty] \geq \prod_{j=0}^{r-1}\frac{b_j(\xi)}{c_j}.$$

Proof. We introduce the notations $p_j := \mathbb{P}_\xi[X_t \in \mathcal{C}_j^\circ,\ 0 \leq t < \infty]$, $\hat{p}_j := \mathbb{P}_\xi[X_t \in \mathcal{C}_j^\circ,\ 0 \leq t < \infty \mid \mathcal{A}b_j \geq 0]$.

The control signal $u(t) \in \{u \in \mathcal{U} : \mathcal{A}^r b(x) \geq 0\}$ for all $t \geq 0$ provides $\mathcal{A}b_{r-1} \geq 0$. By Proposition III.8,

$$\begin{aligned} p_{r-1} &= \mathbb{P}_\xi[X_t \in \mathcal{C}_{r-1}^\circ,\ 0 \leq t < \infty]\\ &= \mathbb{P}_\xi[X_t \in \mathcal{C}_{r-1}^\circ,\ 0 \leq t < \infty \mid \mathcal{A}b_{r-1} \geq 0]\\ &= \hat{p}_{r-1}. \end{aligned} \tag{21}$$

For $j = 0, 1, ..., r-2$, and $0 \leq t < \infty$, we have the following recursion:

$$\begin{aligned} p_j &= \mathbb{P}_\xi[X_t \in \mathcal{C}_j^\circ]\\ &= \mathbb{E}^\xi[\mathbb{1}_{\{X_t\in C_j^\circ\}}\mathbb{1}_{\{X_t\in C_{j+1}^\circ\}}] + \mathbb{E}^\xi[\mathbb{1}_{\{X_t\in C_j^\circ\}}\mathbb{1}_{\{X_t\notin C_{j+1}^\circ\}}]\\ &= \mathbb{P}_\xi[X_t \in C_j^\circ\ |\mathbb{1}_{\{X_t\in C_{j+1}^\circ\}}]\cdot\mathbb{P}_\xi[X_t \in C_{j+1}^\circ]\\ &+ \mathbb{P}_\xi[X_t \in C_j^\circ\ |\mathbb{1}_{\{X_t\notin C_{j+1}^\circ\}}]\cdot\mathbb{P}_\xi[X_t \notin C_{j+1}^\circ], \end{aligned} \tag{22}$$

where we have used shorthand notations $\{X_t \in \mathcal{C}_j\} := \{X_t \in \mathcal{C}_j,\ 0 \leq t < \infty\}$ and $\{X_t \notin C_{j+1}\} := \{X_t \notin C_{j+1}$ for some $0 \leq t < \infty\}$. Indeed, we have

$$X_t = X_t\mathbb{1}_{\{X_t\in C_{j+1}^\circ\}} + X_t\mathbb{1}_{\{X_t\notin C_{j+1}^\circ\}},$$

then

$$\mathbb{E}[X_t] = \mathbb{E}[X_t\mathbb{1}_{\{X_t\in C_{j+1}^\circ\}}] + \mathbb{E}[X_t\mathbb{1}_{\{X_t\notin C_{j+1}^\circ\}}],$$

and (22) follows. Note that

$$\begin{aligned} &\mathbb{P}_\xi[X_t \in C_j^\circ\ |\mathbb{1}_{\{X_t\in C_{j+1}^\circ\}}]\\ &\geq \mathbb{P}_\xi[X_t \in C_j^\circ\ |\mathcal{A}b_j \geq 0] = \hat{p}_j, \end{aligned} \tag{23}$$

and therefore

$$\mathbb{P}_\xi[X_t \in C_j^\circ\ |\mathbb{1}_{\{X_t\in C_{j+1}^\circ\}}]\cdot\mathbb{P}_\xi[X_t \in C_{j+1}^\circ] \geq \hat{p}_j p_{j+1}.$$

Now define stopping times $\tau_j = \inf\{t : b_j(X_t) \leq 0\}$ for $j = 0, 1, ..., r-2$, then $b_j(X_{t\wedge\tau_j}) \geq 0$ a.s.. In addition,

$$X_{t\wedge\tau_j} = \mathbb{1}_{\{\tau_j\leq\tau_{j+1}\}}X_{t\wedge\tau_j} + \mathbb{1}_{\{\tau_j>\tau_{j+1}\}}X_{t\wedge\tau_j}$$

Assume the worst scenario, which is for all $t \geq \tau_{j+1}$, we have $\mathcal{A}b_j \leq 0$. On $\{\mathcal{A}b_j < 0\} \cap \{\tau_j > \tau_{j+1}\}$, we have $b_j(X_{\tau_{j+1}}) > 0$ and $\mathbb{E}^\xi[b_j(X_{t\wedge\tau_j})] \leq b_j(X_{\tau_{j+1}}) - \int_{\tau_{j+1}}^t \varepsilon(s)ds$ for some $\varepsilon : \mathbb{R}_{\geq 0} \to \mathbb{R}_{>0}$ and $t \geq \tau_{j+1}$. Therefore, the process $b_j(X_{t\wedge\tau_j})$ is a nonnegative supermartingale and $\mathbb{P}_\xi[\sup_{T\leq t<\infty} b_j(X_{t\wedge\tau_j}) \geq \lambda] \leq \frac{b_j(X_{\tau_{j+1}})-\int_{\tau_{j+1}}^T \varepsilon(s)ds}{\lambda}$ by Doob's supermartingale inequality. For any $\lambda > 0$, we can find a finite $T \geq \tau_{j+1}$ such that $\mathbb{P}_\xi[\sup_{T\leq t<\infty} b_j(X_{t\wedge\tau_j}) \geq \lambda] = 0$. Since λ is arbitrarily selected, we must have $\mathbb{P}_\xi[\sup_{T\leq t<\infty} b_j(X_{t\wedge\tau_j}) > 0] = 0$, which means τ_j is triggered within finite time. On the other hand, on $\{\mathcal{A}b_j < 0\} \cap \{\tau_j \leq \tau_{j+1}\}$, τ_j has been already triggered. Therefore,

$\{X_t \notin \mathcal{C}_j^\circ$ for some $0 \leq t < \infty\}$ a.s. given $\{\mathcal{A}b_j < 0\}$. Hence,

$$\begin{aligned} &\mathbb{P}_\xi[X_t \in C_j^\circ \,|\mathbb{1}_{\{X_t \notin C_{j+1}^\circ\}}] \\ &\geq \mathbb{P}_\xi[X_t \in C_j^\circ \,|\mathbb{1}_{\{X_t \notin C_{j+1}^\circ,\, \forall t \geq \tau_{j+1}\}}] \\ &\geq \mathbb{P}_\xi[X_t \in C_j^\circ \,|\mathbb{1}_{\{\mathcal{A}b_j < 0,\, \forall t \geq \tau_{j+1}\}}] = 0 \end{aligned} \tag{24}$$

Combining the above, for $j = 0, 1, ..., r-2$, we have

$$p_j \geq \hat{p}_j p_{j+1},$$

and ultimately $p_0 \geq \prod_{j=0}^{r-1} \hat{p}_j$. □

Remark III.11. *The above result estimates the lower bound of the safety probability given the constrained control signals $\mathbf{u}_\upsilon$. Based on recursion (22), we can easily obtain the same result by dropping the last term. However, we argued that under some extreme conditions the worst case may happen. Indeed, we have assumed that $t \geq \tau_{j+1} \implies \mathcal{A}b_j \leq 0$. This conservative assumption is made such that within finite time X will cross the boundary of each $\mathcal{C}_j$.*

Another implicit condition may cause the worst-case lower bound as well, that is when $\bigcup_{j=0}^{r-1}\{\mathcal{A}b_j = 0,\ 0 \leq t < \infty\}$ is a $\mathbb{P}_\xi$-null set. This, however, is practically possible since the controller indirectly influences the value of $\mathcal{A}b_j$ for all $j < r$, the strong invariance of the level set $\{\mathcal{A}b_j = 0\}$ is not guaranteed using QP scheme.

Remark III.12. *A nice selection of controller is to implicitly reduce the total time a sample path spends in $\{\mathcal{A}b_j \leq 0\}$ for each j. However, this is a challenging task by only steering the bottom-level flow, which in turn gives us a future research direction.*

IV. Simulation Results

In this section, we use two examples to validate our result. We show that the proposed SCBFs have smaller control effort compared to SRCBFs and higher safe probability compared to SZCBFs.

A. Example 1

In the first example, we use an automatic cruise control example as in [6] and [4]. The model is given by the following three-dimensional system:

$$d\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -F_r(x)/M \\ 0 \\ x_2 - x_1 \end{bmatrix} dt + \begin{bmatrix} 1/M \\ 0 \\ 0 \end{bmatrix} u dt + \Sigma dW,$$

where x_1 and x_2 denote the velocity of the following vehicle and leading vehicle, respectively, and x_3 is the distance between two vehicles and

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \sigma_2 \end{bmatrix}.$$

The aerodynamic drag is $F_r(x) = f_0 + f_1 x_1 + f_2 x_1^2$ with $f_0 = 0.1,\ f_1 = 5,\ f_2 = 0.25$ and the mass of the vehicle is $M = 1650$. The initial state is chosen as $[x_1, x_2, x_3] = [18, 10, 150]^T$ and W is a three-dimensional Brownian motion representing uncertainty in the velocity of following vehicle and the distance of two vehicles. The goal of the following vehicle is to achieve a desired velocity $x_d = 22$ while keeping the collision constraint $h(x) = x_3 - \tau x_1 > 0$. We use a Lyapunov function $V(x) = (x_1 - x_d)^2$ to control the velocity of the following vehicle. We use $B(x) = \frac{1}{h(x)}$ as the SRCBF and $h(x)$ as the SCBF. We solve QP problems using SRCBF as

$$\begin{aligned} &[u^*, \delta^*] = \underset{u,\delta}{\arg\min} \frac{1}{2}(u^2 + \delta^2) \quad \text{s.t.} \\ &\frac{\partial V(x)}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\operatorname{tr}\left(\Sigma^T \Sigma \frac{\partial^2 V(x)}{\partial x^2}\right) \leq \delta, \\ &\frac{\partial B(x)}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\operatorname{tr}\left(\Sigma^T \Sigma \frac{\partial^2 B(x)}{\partial x^2}\right) \leq \frac{\gamma}{B(x)}, \end{aligned}$$

and SCBF as

$$\begin{aligned} &[u^*, \delta^*] = \underset{u,\delta}{\arg\min} \frac{1}{2}(u^2 + \delta^2) \quad \text{s.t.} \\ &\frac{\partial V(x)}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\operatorname{tr}\left(\Sigma^T \Sigma \frac{\partial^2 V(x)}{\partial x^2}\right) \leq \delta, \\ &\frac{\partial h(x)}{\partial x}(f(x) + g(x)u) + \frac{1}{2}\operatorname{tr}\left(\Sigma^T \Sigma \frac{\partial^2 h(x)}{\partial x^2}\right) \geq 0. \end{aligned}$$

We present the simulation results by showing the scaled control value $u/(Mg)$ and control effort $J = u^2$ for SCBF and SRCBF as in Figure 1 and Figure 2. For simplicity, we choose noise level to be $\sigma_1 = \sigma_2 = 1$. In both figures, the red curves are for the SRCBF and the blue curves are for the SCBF. From the figures, we can find out that SRCBF requires an impulse control signal to make the system safe when approaching the boundary. The peak value of J using SRCBF is almost $1.75e^9$ while it is less than $0.1e^9$ for that of using SCBFs. In practice, this implies that we need a very large acceleration in order to keep the system staying within the safe set. As a result, we bound the scaled control to be $u/(Mg) > -0.5$ and show the safe probability as in Table I. The table shows that for unbounded control, the safe probability using SRCBF is 90% compared to 70% by using SCBF. However, the safe probability drops to only 25% when we use SRCBF while the safe probability is 65% for SCBF under bounded control input. As a result, we can see that the safety probability obtained by SCBF is more robust to saturation of control inputs.

B. Example 2

In the second example, we test our SCBF using a differential drive model as in [13]:

$$ds = d\begin{bmatrix} x \\ y \\ \vartheta \end{bmatrix} = \begin{bmatrix} \cos\vartheta & 0 \\ \sin\vartheta & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} v \\ w \end{bmatrix} dt + \begin{bmatrix} \sigma_1 & 0 & 0 \\ 0 & \sigma_2 & 0 \\ 0 & 0 & 0 \end{bmatrix} dW,$$

where x and y are the planar positions of the center of the vehicle, ϑ is its orientation, $v = 2$ is its forward velocity, the angular velocity w is the control of the system and W is a

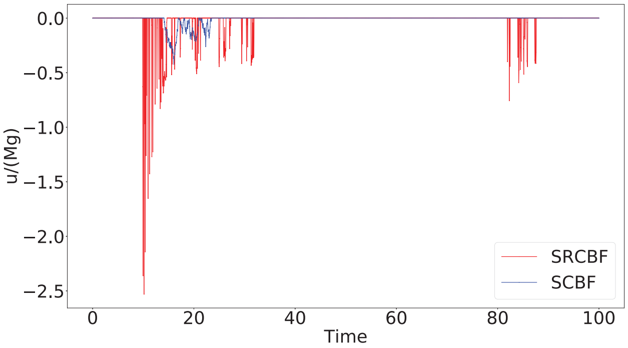

Fig. 1. Plot of scaled control $u/(Mg)$ for Example 1.

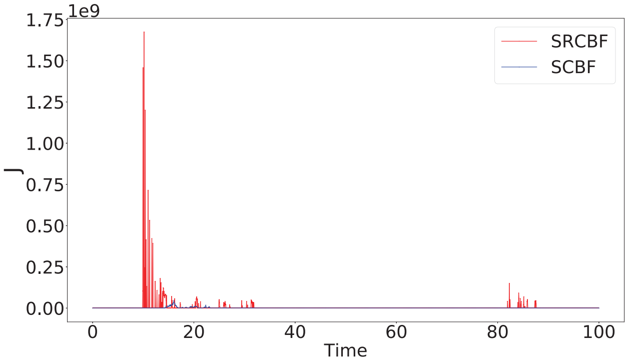

Fig. 2. Plot of control effort $J = u^2$ for Example 1.

standard Brownian motion representing uncertainty in x and y. The working space of the vehicle is a circle centered at $(0, 0)$ with a radius of $r = 3$. Our objective is to control the vehicle within the working space and as a result, the safety requirement can be encoded using $h(s) = r^2 - x^2 - y^2$. We solve QP problems using constraints that are obtained from Theorem III.10 as

$$\mathcal{A} \circ \mathcal{A}(9 - x^2 - y^2) \geq 0 \tag{25}$$

We first test safe probability for different initial positions. We use our SCBF to test this probability under different noise levels within $[0, 0.3]$. For simplicity, we set $\sigma_1 = \sigma_2 = \sigma$. For each value of σ, we sample 1000 trajectories and calculate the safe probability. We also compare the result between SCBF and a high-order SZCBF, which is an extension of the work [18] as

$$h_1(s) = \mathcal{A}h(s) + \alpha_1 h(s),$$
$$h_2(s) = \mathcal{A}h_1(s) + \alpha_2 h(s).$$

The constraints from SZCBF that $h_2(s) \geq 0$ are used to solve QP problems. We first compare the safe probability between SCBF and SZCBF for different noise level within $[0, 0.2]$. For each value of σ, we randomly sample 1000 initial points and generate 1000 trajectories accordingly. We calculate safe probability over this 1000 trajectories and plot the result as in Figure 3. We can find out that SCBF has a better safe probability over SZCBF. In another experiment, we randomly sample 10 initial points. Then we generate 500 trajectories using SCBF and SZCBF for each initial point. We fix the noise to be $\sigma = 0.2$. The result is shown as in Figure 4. From the figure, we can find out that SCBF has a overall better performance than SZCBF under randomly sampled initial points.

	SRCBF	SCBF
Unbounded control	90%	70%
Bounded control	25%	65%

TABLE I: Safe probability of Example 1 between SRCBF and SCBF under bounded (saturated) and unbounded control inputs. We sample 20 trajectories for each case and calculate the safe probability. The simulation step time is chosen to be $t = 0.0005s$. We can see from this table that the proposed SCBF is more robust to control input saturation than SRCBF, which tend to require unbounded control inputs at the boundary of the safe set. See also Section III-B for a simple illustrative example. Note that the 90% safety is due to the numerical error.

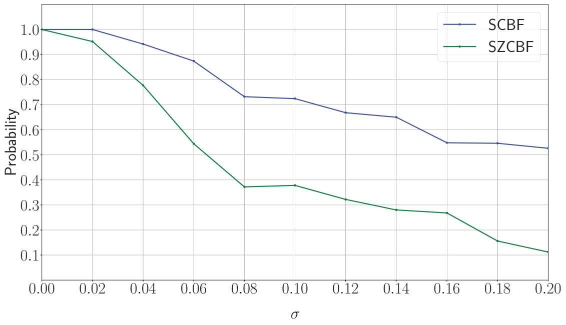

Fig. 3. Safe probability between SCBF and SZCBF. We compare noise level within [0,0.2]. For each value of σ, we sample 1000 initial points to calculate safe probability.

V. Conclusion

In this work, considering the pros and cons of the existing formulations for stochastic barrier functions (such as frequently used SRCBFs and SZCBFs), we propose stochastic control barrier functions (SCBFs) for safety-critical control of stochastic systems and extend the worst-case safety probability estimation to high-order SCBFs. We show that the proposed SCBFs provide good trade-offs between the imposed control constraints and the conservatism in the estimation of safety probability, which are demonstrated both theoretically and empirically. In particular, the proposed scheme is utilized to control an automatic cruise control model and a differential drive mobile robot model.

While the estimate of the safety probability in the high relative degree case appears to be conservative, as partly discussed in Remark III.11 and III.12, worst-case scenarios do exist when the control scheme generated by SCBFs loses

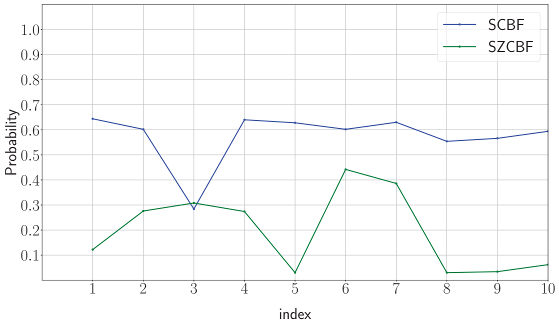

Fig. 4. Safe probability of 10 randomly sample initial points. For each initial point, we sample 500 trajectories using SCBF and SZCBF respectively. The horizontal axis represents the index of the initial points.

dominance on the intermediate supper-level sets. To accurately obtain the probabilistic winning sets, it is necessary to capture how the probability measure is distorted by the input processes. However, this may be computationally challenging for stochastic control systems with high relative degree.

For future work, it is intriguing to connect Lyapunov-type characterizations with exit-time problems, such that despite of a direct bottom-level control, the probability of satisfaction for the controlled paths (dependent on time and initial positions) on each intermediate super level set can be provided with more accuracy. To embed the Lyapunov scenario into the existing HJB solver, topological analysis is needed to reduce the effect of discontinuity [7]. In addition, since the existing exit-time provides an off-line synthesis of controller, a direct combination of Lyapunov-type controller synthesis via quadratic programming and off-line exit-time probability solution may not be desirable. It would be applicable to consider learning algorithm to maintain the ignorable error whilst alleviate computational complexity. At last, more complex stochastic specification and control synthesis via Lyapunov could be investigated as in the deterministic cases.

References

[1] Bowen Alpern and Fred B Schneider. Defining liveness. *Information Processing Letters*, 21(4):181–185, 1985.

[2] Aaron D Ames, Samuel Coogan, Magnus Egerstedt, Gennaro Notomista, Koushil Sreenath, and Paulo Tabuada. Control barrier functions: Theory and applications. In *Proc. of ECC*, pages 3420–3431. IEEE, 2019.

[3] Aaron D Ames, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In *Proc. of CDC*, pages 6271–6278. IEEE, 2014.

[4] Aaron D Ames, Xiangru Xu, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 62(8):3861–3876, 2016.

[5] Yuxiao Chen, Huei Peng, and Jessy Grizzle. Obstacle avoidance for low-speed autonomous vehicles with barrier function. *IEEE Transactions on Control Systems Technology*, 26(1):194–206, 2017.

[6] Andrew Clark. Control barrier functions for complete and incomplete information stochastic systems. In *Proc. of ACC*, pages 2928–2935. IEEE, 2019.

[7] Peyman Mohajerin Esfahani, Debasish Chatterjee, and John Lygeros. The stochastic reach-avoid problem and set characterization for diffusions. *Automatica*, 70:43–56, 2016.

[8] Javier Garcıa and Fernando Fernández. A comprehensive survey on safe reinforcement learning. *Journal of Machine Learning Research*, 16(1):1437–1480, 2015.

[9] Antoine Girard, Colas Le Guernic, and Oded Maler. Efficient computation of reachable sets of linear time-invariant systems with inputs. In *Proc. of HSCC*, pages 257–271. Springer, 2006.

[10] Shao-Chen Hsu, Xiangru Xu, and Aaron D Ames. Control barrier function based quadratic programs with application to bipedal robotic walking. In *Proc. of ACC*, pages 4542–4548. IEEE, 2015.

[11] Harold J Kushner. *Stochastic Stability and Control*. Academic Press, 1967.

[12] Leslie Lamport. Proving the correctness of multiprocess programs. *IEEE Transactions on Software Engineering*, (2):125–143, 1977.

[13] Steven M LaValle. *Planning Algorithms*. Cambridge University Press, 2006.

[14] Quan Nguyen and Koushil Sreenath. Exponential control barrier functions for enforcing high relative-degree safety-critical constraints. In *Proc. of ACC*, pages 322–328. IEEE, 2016.

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

[16] Stefan Ratschan and Zhikun She. Safety verification of hybrid systems by constraint propagation-based abstraction refinement. *ACM Transactions on Embedded Computing Systems (TECS)*, 6(1):8–es, 2007.

[17] Manuel Rauscher, Melanie Kimmel, and Sandra Hirche. Constrained robot control using control barrier functions. In *Proc. of IROS*, pages 279–285. IEEE, 2016.

[18] Cesar Santoyo, Maxence Dutreix, and Samuel Coogan. A barrier function approach to finite-time stochastic system verification and control. *Automatica*, 125:109439, 2021.

[19] Meenakshi Sarkar, Debasish Ghose, and Evangelos A Theodorou. High-relative degree stochastic control Lyapunov and barrier functions. *arXiv preprint arXiv:2004.03856*, 2020.

[20] Andrew Taylor, Andrew Singletary, Yisong Yue, and Aaron Ames. Learning for safety-critical control with control barrier functions. In *Proc. of L4DC*, pages 708–717. PMLR, 2020.

[21] Chuanzheng Wang, Yinan Li, Yiming Meng, Stephen L Smith, and Jun Liu. Learning control barrier functions with high relative degree for safety-critical control. In *Proc. of ECC, to appear*, 2021.

[22] Wei Xiao and Calin Belta. Control barrier functions for systems with high relative degree. In *Proc. of CDC*, pages 474–479. IEEE, 2019.