2025 IEEE 64th Conference on Decision and Control (CDC)
December 10-12, 2025. Rio de Janeiro, Brazil

Piecewise Control Barrier Functions for Stochastic Systems

Rayan Mazouz[1], Luca Laurenti[2], Morteza Lahijanian[1]

2025 IEEE 64th Conference on Decision and Control (CDC) | 979-8-3315-2627-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/CDC57313.2025.11312583

Abstract— **This paper presents a method for the simultaneous synthesis of a barrier certificate and a safe controller for discrete-time nonlinear stochastic systems. Our approach, based on *piecewise stochastic control barrier functions*, reduces the synthesis problem to a minimax optimization, which we solve exactly using a dual linear program with zero gap. This enables the joint optimization of the barrier certificate and safe controller within a single formulation. The method accommodates stochastic dynamics with additive noise and a bounded continuous control set. The synthesized controllers and barrier certificates provide a formally guaranteed lower bound on probabilistic safety. Case studies on linear and nonlinear stochastic systems validate the effectiveness of our approach.**

I. Introduction

Real-world controlled systems often exhibit intricate dynamics and inherent uncertainty, making safety assurance a critical challenge in *safety-critical* applications, such as autonomous vehicles [1], robotic systems [2], and aerospace applications [3], [4]. Traditional control design methods for such systems are often time-consuming and error-prone, with safety analysis relying heavily on extensive testing [5], [6]. In contrast, formal approaches such as *Control Barrier Functions (CBFs)* [7], [8] provide a principled framework for synthesizing *safe-by-design* controllers [9], [10]. However, extending CBF synthesis to nonlinear systems with stochastic disturbances remains a significant challenge. In this work, we address this gap by introducing a method for synthesizing stochastic CBFs for general discrete-time nonlinear stochastic systems.

A CBF is a Lyapunov-like function used to enforce safety constraints by ensuring the *forward invariance* of a defined safe set. When the CBF conditions are satisfied, a control law can be synthesized (extracted) to keep the system within a safe region. CBFs have been extensively studied for deterministic systems [7], [8]. For stochastic systems, *Stochastic Barrier Functions (SBFs)* provide a formal framework for probabilistic safety verification under a given control policy [11]. The synthesis of CBFs using SBF certificates is an emerging research area [12]–[14]. In [12], a safe feedback law is obtained through an iterative synthesis of an SBF; however, this approach is limited to polynomial systems and lacks guarantees on termination. In [13], an Sum-of-Squares (SOS) approach is employed to identify a safe control policy for generalized polynomial dynamics under uncertainty. In [14], the SOS-convex property of the synthesized certificate is leveraged to derive a safe controller for general nonlinear systems. However, ensuring the SOS-convex property, even with Semi-Definite Programming (SDP) solvers, is not always guaranteed [15].

In this work, we propose a stochastic CBF (s-CBF) synthesis method for discrete-time nonlinear stochastic systems with continuous control sets to ensure safety over finite or infinite time horizons. Unlike traditional CBF and SBF methods [12]–[14], which typically assume that either the barrier function or the controller is predefined, our approach jointly synthesizes both. However, this introduces a key challenge: the functional optimization problem requires simultaneously searching for both the barrier function (SBF) and a safe controller (CBF), which generally leads to a nonconvex bilevel optimization problem. To address this complexity, we leverage *piecewise* SBFs [11], constraining the functional optimization to a structured class of piecewise functions. In particular, we show that by focusing on piecewise constant (PWC) functions, the synthesis of s-CBFs can be formulated as a minimax optimization problem. Notably, we demonstrate that this minimax problem can be efficiently solved via linear programming (LP), enabling the use of a wide variety of LP solvers and enhancing scalability. Our evaluations on both linear and nonlinear stochastic systems with varying dimensionalities validate the theoretical guarantees and illustrate the method's effectiveness for complex systems.

In short, this work makes the following contributions: (i) a derivation of PWC s-CBFs, formulated as a minimax optimization problem, (ii) an exact (and iteration-free) approach to solving the PWC s-CBF synthesis (minimax optimization) problem, using a linear program, and (iii) validation of the theory and illustrating the performance of the proposed method through a series of benchmark problems on linear and nonlinear stochastic systems.

Related Work Probabilistic safe control design is a rich field that has been extensively researched from various lenses. In [16], the problem of safe control synthesis using CBFs is extended to stochastic systems and formulated as a quadratic program. In that work, the CBFs are designed manually, making the solution optimal for a given barrier. The same holds for the method presented in [17], which takes a belief-space approach to synthesize safe controllers for continuous-time affine-in-control SDEs under a predefined level set. Predefining the barrier or policy a priori is a suboptimal approach. In this work, we simultaneously synthesize a safe controller and a barrier certificate for systems with general discrete-time nonlinear dynamics and unbounded-support additive noise.

This work was supported by the Air Force Research Laboratory/RVSW under Contract No. FA945324CX026.

[1]Authors are with the University of Colorado Boulder, USA {firstname.lastname}@colorado.edu
[2]Authors are with Delft University of Technology, Netherlands {l.laurenti}tudelft.nl

In [18], a method for safe control synthesis is proposed using Interval Markov Decision Processes under finite actions via dynamic programming. That work is extended to continuous action spaces in [19] under certain convexity conditions on the control space. Other methods include data-driven and learning based approaches that identify regions of the control space that ensure safe behavior, referred to as permissible strategies [20] and shields [21]. These approaches do not directly synthesize a safe controller that maximizes the probability of safety. In [22], a distributionally robust control synthesis method is proposed for switched stochastic systems with uncertain distributions. Learning-based approaches have also been introduced for safe reach-avoid specifications [23], safe reinforcement learning, and learning safe controllers using Gaussian Processes [24]. None of these works simultaneously synthesize a barrier certificate and a safe controller as a single LP optimization.

II. Problem Formulation

We consider a controlled discrete-time stochastic system described by the following stochastic difference equation

$$\mathbf{x}_{k+1} = f(\mathbf{x}_k, \mathbf{u}_k) + \mathbf{w}_k, \tag{1}$$

where $\mathbf{x}_k \in \mathbb{R}^n$ and $\mathbf{u}_k \in U \subset \mathbb{R}^m$ are respectively the state and control input at time $k \in \mathbb{N}$, and $f : \mathbb{R}^n \times U \to \mathbb{R}^n$ is a possibly nonlinear function that is assumed to be continuous. Term $\mathbf{w}_k$ is random variable that is independent and identically distributed at every time-step with values in $\mathbb{R}^w$, which we assume to be Gaussian with zero-mean and covariance matrix Σ, i.e., $\mathbf{w}_k \sim p_{\mathbf{w}} = \mathcal{N}(0, \Sigma)$. Control $\mathbf{u}_k$ at state x is determined by a stationary feedback controller $\pi : \mathbb{R}^n \to U$, i.e., $\mathbf{u}_k = \pi(x)$. Intuitively, System (1) represents a nonlinear dynamical model with additive noise, whose one-step dynamics are represented by vector field f.

For a given state $x \in \mathbb{R}^n$, action $u \in U$ and (Borel measurable) set $X \subseteq \mathbb{R}^n$, we define the transition kernel $T(X \mid x, u)$ for System (1) as

$$T(X \mid x, u) := \int_{\mathbb{R}^w} \mathbf{1}_X(f(x, u) + w) p_{\mathbf{w}}(w) dw, \tag{2}$$

where $\mathbf{1}_X$ is the indicator function for X such that $\mathbf{1}_X(x) = 1$ if $x \in X$ and $\mathbf{1}_X(x) = 0$ if $x \notin X$. For a given a controller π, the kernel induces a unique probability measure Pr for System (1) [25] such that for any $N \in \mathbb{N}_{\geq 0}$, initial condition $x_0 \in \mathbb{R}^n$ and measurable sets $X_0, X_k \subseteq X$,

$$\begin{aligned} &\Pr[\mathbf{x}_0 \in X_0] = \mathbf{1}_{X_0}(x_0), \\ &\Pr[\mathbf{x}_k \in X_k \mid \mathbf{x}_{k-1} = x, \pi] = T(X_k \mid x, \pi(x)). \end{aligned} \tag{3}$$

We now define Probabilistic Safety, which is the main objective we want to optimize in this paper, through the synthesis of the controller π.

Definition 1 (Probabilistic Safety)**.** *Given a bounded safe set $X_{\mathrm{s}} \subset \mathbb{R}^n$ and initial set $X_0 \subseteq X_{\mathrm{s}}$,* probabilistic safety *of System* (1) *under controller π for N steps is defined as*

$$P_{\mathrm{s}}(X_{\mathrm{s}}, X_0, N, \pi) = \inf_{x_0 \in X_0} \Pr[\mathbf{x}_k \in X_{\mathrm{s}} \; \forall k \leq N \mid \mathbf{x}_0 = x_0, \pi].$$

We now state our goal in this paper: synthesizing a controller that maximizes probabilistic safety for System (1).

Problem 1 (Safe Control Synthesis)**.** *Consider stochastic System* (1)*, compact safe set $X_{\mathrm{s}} \subset \mathbb{R}^n$, and initial set $X_0 \subseteq X_{\mathrm{s}}$. Given a time horizon $N \in \mathbb{N}_0 \cup \{\infty\}$, synthesize a controller π^* such that $\pi^* \in \arg\max_\pi P_{\mathrm{s}}(X_{\mathrm{s}}, X_0, N, \pi^*)$.*

Problem 1 seeks an optimal feedback controller that maximizes Probabilistic Safety for System (1). Because of the nonlinearity of f, despite the additivity of the noise, this problem presents several challenges that need to be addressed. First of all, P_{s} cannot be computed in closed form. Furthermore, we seek an optimal feedback controller with U possibly containing uncountable many controls. Consequently, existing approaches that generally consider a finite number of actions in U cannot be applied in this setting [18].

Remark 1. *The Gaussian assumption on $\mathbf{w}_k$ is not strictly required by our framework and is made solely for clarity of presentation. In fact, the only requirement on $\mathbf{w}_k$ is that the resulting transition kernel satisfies $T(X \mid x, u)$ being computable (or analytically over-approximable).*

III. Stochastic Control Barrier Functions

In this section, we provide an overview of piecewise constant (PWC) stochastic CBFs (s-CBFs), and their relation to safe control synthesis. Consider System (1) with safe set $X_{\mathrm{s}} \subset \mathbb{R}^n$, initial set $X_0 \subseteq X_{\mathrm{s}}$, and unsafe set $X_{\mathrm{u}} = \mathbb{R}^n \setminus X_{\mathrm{s}}$.

Finding an s-CBF requires solving a functional optimization problem [12], [14]. This problem is particularly challenging due to the simultaneous search for both a function B and a controller π that maximizes safety. Unlike standard verification and control synthesis problems, where either B or π are fixed, respectively, here both must be optimized.

A. Piecewise Constant s-CBFs

PWC functions provide an expressive class of functions for barrier synthesis while addressing some of the challenges in the functional optimization problem [11]. Consider a partition $\{X_1, \ldots, X_K\}$ of set X_{s} in $K \in \mathbb{N}$ compact sets,

$$\cup_{i=1}^K X_i = X_{\mathrm{s}} \quad \text{and} \quad X_i \cap X_j = \emptyset \quad \forall i \neq j \in \mathbb{N}_{\leq K}, \tag{4}$$

such that vector field f is continuous in each region X_i. Note that the boundary of each set has measure zero w.r.t. $T(\cdot \mid x, \pi)$ for any $x \in X_{\mathrm{s}}$. Further, let B be a PWC function such that, for all $i \in \mathbb{N}_{\leq K}$, $b_i \in \mathbb{R}_{\geq 0}$ and

$$B(x) = \begin{cases} b_i & \text{if } x \in X_i \\ 1 & \text{otherwise.} \end{cases} \tag{5}$$

Then, the following corollary characterizes the PWC s-CBF.

Corollary 1 (PWC s-CBF)**.** *The PWC function in* (5) *is an s-CBF for System* (1) *if, for every $i \in \mathbb{N}_{\leq K}$, there exist control $u_i \in U$ and scalars $\eta, \beta_i \in [0, 1]$ such that*

$$b_i \geq 0, \qquad \forall x \in X_i, \tag{6a}$$

$$b_i \leq \eta, \qquad \forall x \in X_i \cap X_0, \tag{6b}$$

$$\sum_{j=1}^K b_j T(X_j \mid x, u_i) + T(X_{\mathrm{u}} \mid x, u_i) \leq b_i + \beta_i \quad \forall x \in X_i, \tag{6c}$$

where T is the transition kernel in (2)*. Then, for a controller π that assigns $\pi(x) = u_i$ for all $x \in X_i$ and for all $i \in \mathbb{N}_{\leq K}$,*

$$P_{\mathrm{s}}(X_{\mathrm{s}}, X_0, N, \pi) \geq 1 - (\eta + N \cdot \max_{i \in \mathbb{N}_{\leq K}} \beta_i). \tag{7}$$

The proof follows directly from [11, Theorem 2]. Following this corollary, the synthesis of PWC s-CBF can be formulated as an optimization problem, where the size of the partition is a design parameter.

B. Piecewise Constant s-CBFs

The challenge however lies in the characterization of transition kernel T, which is parameterized with u_i.

IV. PWC s-CBF Synthesis

In this section, we formally set up the general optimization problem for synthesis of PWC s-CBF. For covariance Σ of noise $\mathbf{w}_k$, let $\mathcal{T}$ denote the Mahalanobis (linear) transformation. Denote by $\mathcal{T}(X_s)$, the transformation of X_s by $\mathcal{T}$. Then, we consider the partition in (4) to be an axis-aligned grid in $\mathcal{T}(X_s)$, i.e., for every $i \in \mathbb{N}_{\leq K}$, $\mathcal{T}(X_i)$ is a hyper-rectangle. Using this partition, we derive an exact expression for the transition kernel.

Proposition 1 ([18, Proposition 1])**.** *Let $X_j \subset \mathbb{R}^n$ be a region such that $\mathcal{T}(X_j) = [\underline{v}^{(1)}, \bar{v}^{(1)}] \times \ldots \times [\underline{v}^{(n)}, \bar{v}^{(n)}]$ is a hyper-rectangle, where $\underline{v}^{(i)}, \bar{v}^{(i)} \in \mathbb{R}$ denote the lower and upper bounds of the i-th dimension of the hyper-rectangle. Then, for a given point $x \in \mathbb{R}^n$ and control $u \in U$,*

$$T(X_j|x,u) = \frac{1}{2^n} \prod_{i=1}^{n} \left(erf(\frac{y^{(i)} - \underline{v}^{(i)}}{\sqrt{2}}) - erf(\frac{y^{(i)} - \bar{v}^{(i)}}{\sqrt{2}}) \right), \tag{8}$$

where $erf(\cdot)$ is the error function, $y = \mathcal{T} f(x,u)$, and $y^{(i)}$ is the i-th component of y.

Proposition 1 provides an analytical expression for T given x and u, facilitating the formulation of the s-CBF constraint in (6c). Nevertheless, note that the constraint in (6c) must hold for all $x \in X_i$. To simplify its formulation, we aim to derive affine lower and upper bounds on (8) for all $x \in X_i$. The following lemma allows us to obtain these bounds using Interval Bound Propagation (IBP) techniques [26]–[28].

Lemma 1 (Affine Transition Kernel Bounds)**.** *Consider partition regions X_i, X_j and the transition kernel in* (8) *for $x \in X_i$ and $u \in U$. Then, using IBP, affine functions*

$$\underline{T}_{ij} = A_{ij}^{\perp}[x, u_i]^T + c_{ij}^{\perp}, \qquad \overline{T}_{ij} = A_{ij}^{\top}[x, u_i]^T + c_{ij}^{\top},$$

where $A_{ij}^{\top}, A_{ij}^{\perp} \in \mathbb{R}^{1 \times (n+m)}$ are vectors and $c_{ij}^{\top}, c_{ij}^{\perp} \in \mathbb{R}$ are scalars, can be computed such that $\forall x \in X_i$ and $\forall u \in U$,

$$\underline{T}_{ij}(x,u) \leq T(X_j \mid x, u) \leq \overline{T}_{ij}(x,u). \tag{10}$$

Proof. Using backward mode linear relaxation perturbation analysis (LiRPA), the lower and upper bounds are sound. The proof follows directly from [28, Theorem 1]. □

Remark 2. *Lemma 1 can be extended to transition kernels beyond* (8)*. In fact, it can be generalized for any continuous and differentiable kernel. This implies that our approach is not limited to Gaussian noise $\mathbf{w}_k$, as stated in Remark 1.*

The benefit of Lemma 1 is that it allows us to represent the bounds of T using parameterizations in x and u. However, these parameters are different in nature when it comes to PWC s-CBF synthesis. That is, x is a free parameter, i.e., s-CBF properties have to hold for all $x \in X_i$, whereas $u \in U$ is a decision variable, i.e., we seek to find the optimal u. With this view and using the bounds in (10), we can define the feasible set of the transition kernels for a given $u \in U$ as

$$\begin{aligned}\mathcal{P}_i(u) = \Big\{ &T_i = (T_{i1}, \ldots, T_{iK}, T_{i\mathrm{u}}) \in [0,1]^{K+1} \quad s.t. \\ &\underline{T}_{ij}(x,u) \leq T_{ij} \leq \overline{T}_{ij}(x,u) \quad \forall j \in \mathbb{N}_{\leq K} \cup \{\mathrm{u}\}, \forall x \in X_i \\ &\sum_{j=1}^{K} T_{ij} + T_{i\mathrm{u}} = 1, \Big\}.\end{aligned} \tag{11}$$

This feasible transition kernel $\mathcal{P}_i(u)$ set forms a simplex. This implies that we can rewrite the constraint in (6c) as a set of linear constraints. Based on this, the following theorem defines the general PWC s-CBF optimization problem.

Theorem 1 (PWC s-CBF Synthesis)**.** *Given a K-partition of X_{s}, let $\mathcal{B}_K$ be the set of PWC functions of the form in* (5)*. Further, let vector $\vec{u} = (u_1, \ldots, u_K) \in U^K$ and $\mathcal{P}(\vec{u}) = \mathcal{P}_1(u_1) \times \ldots \times \mathcal{P}_K(u_K)$, where each $\mathcal{P}_i(u)$ is the set of feasible transition kernels in* (11)*. Finally, let B^* and $\vec{u}^*$ be the solutions to the following optimization problem*

$$(B^*, \vec{u}^*) = \arg \min_{B \in \mathcal{B}_K, \vec{u} \in U^K} \max_{(T_i)_{i=1}^K \in \mathcal{P}(\vec{u})} \eta + N\beta \tag{12}$$

subject to

$$b_i \geq 0, \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{13a}$$

$$b_i \leq \eta, \qquad \forall i : X_i \cap X_0 \neq \emptyset, \tag{13b}$$

$$\sum_{j=1}^{K} b_j \cdot T_{ij} + T_{i\mathrm{u}} \leq b_i + \beta_i \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{13c}$$

$$T_{ij} \in [\underline{T}_{ij}(x,u_i), \overline{T}_{ij}(x,u_i)] \quad \forall x \in X_i, \forall i \in \mathbb{N}_{\leq K}, \tag{13d}$$

$$0 \leq \beta_i \leq \beta \qquad \forall i \in \mathbb{N}_{\leq K}. \tag{13e}$$

Then, B^* is a PWC s-CBF along with $\vec{u}^*$ that maximize safety probability, i.e., the RHS of (7)*.*

The proof can be found in the extended version [29].

Remark 3. *By setting $\beta_i = 0$ for all $i \in \mathbb{N}_{\leq K}$, the theorem can be extended to infinite-horizon problems.*

By solving the optimization problem in Theorem 1, we obtain a PWC controller as defined in Corollary 1, i.e., $\pi(x) = u_i^*$ for all $x \in X_i$. This controller is optimal within the class of PWC controllers for the given K-partition. In fact, this controller approximates the true optimal stationary controller π^* as $K \to \infty$. Specifically, per [11, Proposition 1], as the partition size increases, the PWC SBF converges to a safety probability that is at most the optimal safety probability achievable with continuous SBFs. Consequently, if an optimal continuous s-CBF exists that maximizes P_{s}, the same P_{s} can be attained with a sufficiently large K.

In the next section, we present an exact method for solving the problem in Theorem 1 using dual programming.

V. DUAL LINEAR PROGRAM

The optimization problem in Theorem 1 is a minimax problem, with the following decision variables:

$$b = (b_1, \dots, b_K) \in \mathbb{R}^K_{\geq 0}, \tag{14a}$$
$$\vec{u} = (u_1, \dots, u_K) \in U^K, \tag{14b}$$
$$T_i = (T_{i1}, \dots, T_{iK}, T_{iu}) \in \mathcal{P}_i(u_i) \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{14c}$$
$$\beta_i \in \mathbb{R}_{\geq 0} \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{14d}$$
$$\eta, \beta \in \mathbb{R}_{\geq 0}. \tag{14e}$$

The difficulty in the computability of this optimization problem is twofold. First, the product of decision variables b_j and T_{ij} makes the optimization problem bilinear. Second, the transition kernels T_i are dependent on the control u_i, which makes this an embedded optimization problem. Generally, this class of optimization problems is non-convex, thus convex solvers which provide efficiency and convergence guarantees cannot be utilized. In this section, we propose a lossless convexification of the problem based on dual linear programming, such that the optimal solution to the problem can be efficiently computed.

We start by observing that x is an independent variable, and u_i a decision variable. Since $x \in X_i$ is free, for every $i \in \mathbb{N}_{\leq K}$, we can set $x = x'_i - x''_i$, where decision variables $x'_i, x''_i \geq 0$. We conveniently define the vector $\tilde{z}_i = [x'_i - x''_i, u_i]^T \in \mathbb{R}^{(n+m)\times 1}$. Then, the feasible transition kernel set $\mathcal{P}_i(u_i)$, which is a simplex, can be represented as

$$\mathcal{P}_i(u_i) = \{T_i : H_i \begin{bmatrix} T_i \\ \tilde{z}_i \end{bmatrix} \leq h_i\},$$
$$:= \underbrace{\begin{bmatrix} -I_{K+1} & A_i^{\perp} \\ -\vec{1} & \vec{0} \\ \vec{0}_{n+m} & -\vec{1}_{n+m} \\ \hline I_{K+1} & -A_i^{\top} \\ \vec{1} & \vec{0} \\ \vec{0}_{n+m} & \vec{1}_{n+m} \end{bmatrix}}_{H_i} \begin{bmatrix} T_i \\ \tilde{z}_i \end{bmatrix} \leq \underbrace{\begin{bmatrix} -c_i^{\perp} \\ -1 \\ -\tilde{z}_i^{\perp} \\ \hline c_i^{\top} \\ 1 \\ \tilde{z}_i^{\top} \end{bmatrix}}_{h_i}, \tag{15}$$

where matrix $H_i \in \mathbb{R}^{2(K+n+m+2)\times(K+n+m+1)}$, vector $h_i \in \mathbb{R}^{2(K+n+m+1)\times 1}$, I_{K+1} is the identity matrix of size $(K+1)\times(K+1)$, and $\vec{0}$ and $\vec{1}$ are vectors of zeros and ones of appropriate dimensions, respectively. The inequality in (15) is applied element-wise to vectors. The bounds on $\tilde{z}_i$ are denoted by $\tilde{z}_i^{\perp}$ and $\tilde{z}_i^{\top} \in \mathbb{R}^{n+m}$, respectively. Further,

$$A_i^{\perp} = [A_{i1}^{\perp}, \dots A_{iK}^{\perp}, \quad A_{iu}^{\perp}]^T \qquad \in \mathbb{R}^{(K+1)\times(n+m)},$$
$$A_i^{\top} = [A_{i1}^{\top}, \dots A_{iK}^{\top}, \quad A_{iu}^{\top}]^T \qquad \in \mathbb{R}^{(K+1)\times(n+m)},$$
$$c_i^{\perp} = [c_{i1}^{\perp}, \dots c_{iK}^{\perp}, \quad c_{iu}^{\perp}]^T \qquad \in \mathbb{R}^{(K+1)\times 1},$$
$$c_i^{\top} = [c_{i1}^{\top}, \dots c_{iK}^{\top}, \quad c_{iu}^{\top}]^T \qquad \in \mathbb{R}^{(K+1)\times 1}.$$

To constrain the sum of T_{ij} to 1 per (11), two inequality constraints are added. For convenience, the rows of the matrix H_i and vector h_i can be rearranged

$$\tilde{H}_i = \begin{bmatrix} -I_{K+1} & A_i^{\perp} \\ I_{K+1} & -A_i^{\top} \\ -\vec{1} & \vec{0} \\ \vec{1} & \vec{0} \\ \hline \vec{0}_{n+m} & -\vec{1}_{n+m} \\ \vec{0}_{n+m} & \vec{1}_{n+m} \end{bmatrix} = \begin{bmatrix} \tilde{H}_i^p \\ \hline \tilde{H}_i^z \end{bmatrix}, \; \tilde{h}_i = \begin{bmatrix} -c_i^{\perp} \\ c_i^{\top} \\ -1 \\ 1 \\ \hline -\tilde{z}_i^{\perp} \\ \tilde{z}_i^{\top} \end{bmatrix} = \begin{bmatrix} \tilde{h}_i^p \\ \hline \tilde{h}_i^z \end{bmatrix}.$$

Using $\tilde{H}_i$ and $\tilde{h}_i$, the inequality can be decomposed into two separate inequalities. It is noted that inequality $\tilde{H}_i^z \tilde{z}_i \leq \tilde{h}_i^z$ simply denotes the bounds on decision variables $\tilde{z}_i$. The second inequality establishes the bounds on the transition kernels T_i, parameterized by $\tilde{z}_i$, and can be written as

$$\underbrace{\begin{bmatrix} \tilde{H}_i^{p1} & \tilde{H}_i^{p2} \end{bmatrix}}_{\tilde{H}_i^p} \begin{bmatrix} T_i \\ \tilde{z}_i \end{bmatrix} \leq \underbrace{\begin{bmatrix} -c_i^{\perp} \\ c_i^{\top} \end{bmatrix}}_{\tilde{h}_i^p}, \text{ where} \tag{16}$$
$$\tilde{H}_i^{p1} = [-I_{K+1}, \; I_{K+1}; \; -\vec{1}; \; \vec{1}]^T \qquad \in \mathbb{R}^{2(K+2)\times(K+1)}$$
$$\tilde{H}_i^{p2} = [A_i^{\perp}, \; -A_i^{\top}; \; \vec{0}; \; \vec{0}]^T \qquad \in \mathbb{R}^{2(K+2)\times(n+m)}$$

Next, define vector $\bar{b} = (b, 1)$, where b is as defined in (14a), and dual variable $\lambda_i \in \mathbb{R}^{2(K+2)}_{\geq 0}$. Using duality, the problem in Theorem 1 can be formalized as an LP.

Theorem 2 (PWC s-CBF Dual LP)**.** *The optimal solution $(b^*, u^*, \beta^*, \eta^*)$ to the LP formulated below is equivalent (i.e., zero duality gap) to the optimal solution of the optimization problem in Theorem 1.*

$$\min_{b, t_i, \lambda_i} \eta + \beta N$$

subject to

$$0 \leq b_i \leq 1 \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17a}$$
$$b_i \leq \eta \qquad \forall i : X_i \cap X_0 \neq \emptyset, \tag{17b}$$
$$(\tilde{h}_i^p)^T \lambda_i \leq t_i \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17c}$$
$$(\tilde{H}_i^{p1})^T \lambda_i = \bar{b} \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17d}$$
$$(\tilde{H}_i^{p2})^T \lambda_i = 0 \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17e}$$
$$\tilde{z}_i^{\perp} \leq \tilde{z}_i \leq \tilde{z}_i^{\top} \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17f}$$
$$\lambda_i \geq 0 \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17g}$$
$$t_i \geq 0 \qquad \forall i \in \mathbb{N}_{\leq K}, \tag{17h}$$
$$0 \leq \beta_i \leq \beta \qquad \forall i \in \mathbb{N}_{\leq K}. \tag{17i}$$

For the proof and an analysis of the computational complexity, we refer the reader to the extended version [29].

VI. EXPERIMENTS

We demonstrate the efficacy of our approach on various benchmarks. We consider a 2D linear system with a convex and nonconvex safe set, a 3D polynomial room temperature model [30]), and a 4D nonlinear unicycle model [31]. More detailed results can be found in [29]

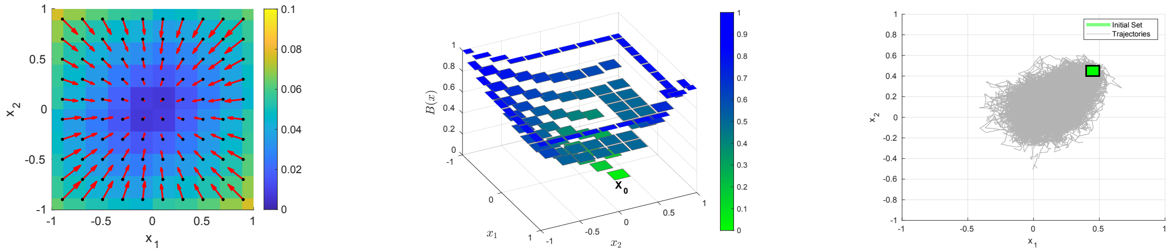
Our IBP code that computes affine transition kernel bounds is in Python, and the PWC s-CBF tool is in Julia. All computations were performed on a Linux machine with 3.9 GHz 8-core CPU and 128 GB memory. In each experiment, we set a threshold of $\delta_s = 0.95$ for $N = 50$ time-steps. Results for the various benchmarks considered are reported in Table I. As can be observed, with sufficient partitions for each case study, our method is able to synthesize controllers and a barrier certificate that yield $P_s \geq \delta_s = 0.95$.

A. Linear System

We consider the following unstable linear system

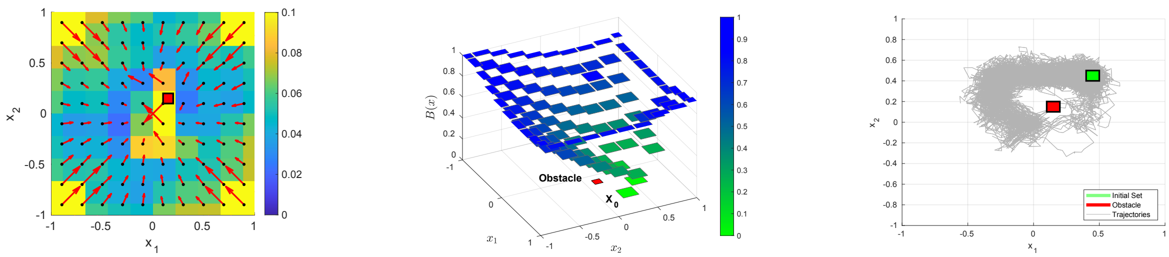
$$x_{k+1} = 1.05\, x_k + 0.1\, u_k + \mathbf{w}$$

where $\mathbf{w} \sim \mathcal{N}(0, 10^{-2} I)$. We study two cases with operating domain $X \in [-1, 1]^2$ and initial set $X_0 \in [0.4, 0.5]^2$



(a) Closed-loop vector field. (b) PWC s-CBF. (c) Monte-Carlo Simulations.

Fig. 1: Convex safe set case study on a linear system. (a) Visualization of the closed-loop vector field, where the background color represents the control magnitude. (b) Representation of the Piecewise Stochastic Control Barrier Function. (c) Results from Monte Carlo simulations, showing 500 trajectories over $N = 50$ steps.



(a) Closed-loop vector field. (b) PWC s-CBF. (c) Monte Carlo simulations.

Fig. 2: Non-convex safe set case study on a linear system. (a) Visualization of the closed-loop vector field, where the background color represents the control magnitude. (b) Representation of the Piecewise Stochastic Control Barrier Function. (c) Results from Monte Carlo simulations, showing 500 trajectories over $N = 50$ steps.

1) Convex safe set: $X_s = X$ (see Fig. 1c), and
2) Non-convex safe set $X_s = X \setminus \mathcal{O}_1(c_1, \epsilon_1)$, where for obstacle $\mathcal{O}_1$: $c_1 = (0.15, 0.15)$ and $\epsilon_1 = (0.05, 0.05)$.

For the convex case, the synthesized control law and barrier are shown in Figs. 1a and 1b, respectively. The probability of safety for the $N = 50$ time-steps is $P_s = 0.98$. In Fig. 1c, a Monte Carlo simulation plot is provided under the synthesized controller for 500 trajectories over a duration of 50 time-steps. In each case, the randomly sampled trajectories resulted in zero violations, i.e., the system is 100% safe. This is in line with the lower bound on P_s that we obtain. To get to $P_s = 0.98$, the barrier and control synthesis computation takes $\approx 2.42s$ (for $K = 100$ partitions).

TABLE I: Benchmark results. In the table, K denotes the size of the partition of X_s, and t_{synth} is the optimization (PWC s-CBF synthesis) time. All experiments use $N = 50$.

System	K	η	β	P_s	t_{synth} (s)
2D Linear Convex	81	0.090	0.00420	0.70	0.91
	100	0.002	0.00036	0.98	2.42
	400	0.002	0.00034	0.98	19.85
2D Linear Non-Convex	81	0.11	0.00610	0.59	1.47
	100	0.03	0.00022	0.96	3.19
	400	0.03	0.00019	0.96	27.89
3D Temp. Model	500	0.0475	0.00025	0.94	301.47
	900	0.0429	0.00023	0.95	497.03
4D Unicycle	1800	0.07	0.0220	0.82	2789.67
	2400	0.02	0.0006	0.95	3945.77

For the non-convex case, the obtained probability of safety for $N = 50$ equals $P_s = 0.96$. The synthesized control law and barrier are shown in Figs. 2a and 2b, respectively. Observe in Fig. 2b that, different from the convex case, the barrier value equals to one at the obstacle region. Further, notice in Fig. 2a that the controller near the obstacle properly pushes the vector field in a direction away from unsafety.

The Monte Carlo simulations are depicted in Fig. 2c. A total of 6 out of 500 trajectories violated the safety boundaries, entering the unsafe set (obstacle region). This indicates a frequentist probability of safety of 99%, slightly higher than the bound we obtain. For this experiment, computation takes about $3.19s$ for the $K = 100$ partitions, to get to $P_s \geq \delta_s$.

B. Temperature Regulation

The following room temperature regulation model has deterministic dynamics

$$\begin{aligned}\mathrm{T}^i_{k+1} =& \mathrm{T}^i_k + \alpha_1(\mathrm{T}^{i+1}_k + \mathrm{T}^{i-1}_k - 2\mathrm{T}^i_k) + \alpha_2(\mathrm{T}_e - \mathrm{T}^i_k) \\ &+ \alpha_3(\mathrm{T}_h - \mathrm{T}^i_k)u_i + \mathbf{w},\end{aligned}$$

to which noise $\mathbf{w} \sim \mathcal{N}(0, 10^{-2}I)$ is added. A total of $n = 3$ rooms are considered, where $\mathrm{T}^{i+1}_k, \mathrm{T}^{i-1}_k$ denote the neighboring rooms. The ambient and heater temperature are $\mathrm{T}_e = -1^\circ$ and $\mathrm{T}_h = 50^\circ$, respectively. The conduction factors are $\alpha_1 = 0.45$, $\alpha_2 = 0.045$ and $\alpha_3 = 0.09$. The controller $u_i \in [0, 0.5]$, while the regions of interest are $X_s = [17, 21]^3$ and $X_0 = [18.5, 19.5] \times [18.5, 19.0]^2$.

For $N = 50$ time-steps, the lower bound on the probabilistic safety for the system is $P_s = 0.95$. Total CBF and SBF synthesis time is $497.03s$ for $K = 900$ partitions. Verifying the system, without the controller, yields $P_s = 0$.

C. Nonlinear Unicycle

Finally, we consider the dynamics of a unicycle

$$\dot{x} = v\cos\theta, \quad \dot{y} = v\sin\theta, \quad \dot{\theta} = \omega, \quad \dot{v} = a.$$

The Cartesian position is defined by $x \in [-1.0, 0.5]$ and $y \in [-1.0, 1.0]$. Further, $\theta \in [-1.75, 0.5]$ represents the orientation relative to the x-axis, and $v \in [-0.5, 1.0]$ denotes the speed. The initial set is chosen to be $X_0 \in \mathcal{B}_{\mathbb{R}^4}((-0.4, -0.4, 0, 0), 0.1)$. The inputs are defined by the steering rate ω and a as the acceleration. For the discrete-time model, $\Delta t = 0.01$ is used alongside the Euler method. Noise is added to this system, where $\mathbf{w} \sim \mathcal{N}(0, 10^{-4}I)$, capturing the discretization error inherent to the Euler method.

For $N = 50$ time-steps, the probability of safety is 95%. The optimization time ($K = 2400$ partitions) is $3945.77s$.

VII. Conclusion

This paper presents a method for jointly synthesizing a barrier certificate and a safe controller for discrete-time nonlinear stochastic systems. Using piecewise stochastic CBFs, we frame the problem as a minimax optimization, efficiently solved via linear programming. Our approach handles non-additive dynamics with unbounded-support noise. Case studies on linear and nonlinear systems validate its effectiveness in achieving the desired safety probability.

Future work includes improving scalability through faster dual LP solvers, extending to higher-dimensional systems, and incorporating adaptive partitioning for efficiency. This also includes a more rigorous analysis to guide the selection of the partition size. Additionally, we aim to minimize control effort in synthesis and integrate reach-avoid objectives for broader applicability in safety-critical settings.

References

[1] S. Shalev-Shwartz, S. Shammah, and A. Shashua, "On a Formal Model of Safe and Scalable Self-driving Cars," *arXiv preprint arXiv:1708.06374*, 2017.

[2] J. Guiochet, M. Machin, and H. Waeselynck, "Safety-Critical Advanced Robots: A Survey," *Robotics and Autonomous Systems*, vol. 94, pp. 43–52, 2017.

[3] R. Mazouz, M. Quadrelli, and R. Beauchamp, "Dynamics and optimal control for free-flight and tethered arrays in low earth orbit," in *2021 IEEE aerospace conference (50100)*. IEEE, 2021, pp. 1–20.

[4] R. Reed, H. Schaub, and M. Lahijanian, "Shielded Deep Reinforcement Learning for Complex Spacecraft Tasking," *arXiv preprint arXiv:2403.05693*, 2024.

[5] H. Kress-Gazit, M. Lahijanian, and V. Raman, "Synthesis for robots: Guarantees and feedback for robot behavior," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, no. 1, pp. 211–236, 2018.

[6] K. Elimelech, M. Lahijanian, L. E. Kavraki, and M. Y. Vardi, "Falsification of Autonomous Systems in Rich Environments," *arXiv preprint arXiv:2412.17992*, 2024.

[7] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control Barrier Functions: Theory and Applications," in *2019 18th European control conference (ECC)*. Ieee, 2019, pp. 3420–3431.

[8] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control Barrier Function based Quadratic Programs for Safety Critical Systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2016.

[9] P. Tabuada, *Verification and Control of Hybrid Systems: a Symbolic Approach*. Springer Science & Business Media, 2009.

[10] M. Lahijanian, S. B. Andersson, and C. Belta, "Formal Verification and Synthesis for Discrete-time Stochastic Systems," *IEEE Transactions on Automatic Control*, vol. 60, no. 8, pp. 2031–2045, 2015.

[11] R. Mazouz, F. Baymler Mathiesen, L. Laurenti, and M. Lahijanian, "Piecewise Stochastic Barrier Functions," *arXiv preprint arXiv:2404.16986*, 2024.

[12] C. Santoyo, M. Dutreix, and S. Coogan, "A Barrier Function Approach to Finite-time Stochastic System Verification and Control," *Automatica*, vol. 125, p. 109439, 2021.

[13] P. Jagtap, S. Soudjani, and M. Zamani, "Formal Synthesis of Stochastic Systems via Control Barrier Certificates," *IEEE Transactions on Automatic Control*, vol. 66, no. 7, pp. 3097–3110, 2020.

[14] R. Mazouz, K. Muvvala, A. Ratheesh, L. Laurenti, and M. Lahijanian, "Safety Guarantees for Neural Network Dynamic Systems via Stochastic Barrier Functions," *Advances in Neural Information Processing Systems*, 2022.

[15] A. A. Ahmadi and P. A. Parrilo, "Sum of Squares and Polynomial Convexity," in *Proc. IEEE Conf. Decision Control*, 2009.

[16] R. K. Cosner, P. Culbertson, A. J. Taylor, and A. D. Ames, "Robust Safety under Stochastic Uncertainty with Discrete-time Control Barrier Functions," *arXiv preprint arXiv:2302.07469*, 2023.

[17] M. Vahs and J. Tumova, "Non-smooth Control Barrier Functions for Stochastic Dynamical Systems," in *2024 European Control Conference (ECC)*. IEEE, 2024, pp. 2200–2205.

[18] N. Cauchi, L. Laurenti, M. Lahijanian, A. Abate, M. Kwiatkowska, and L. Cardelli, "Efficiency through Uncertainty: Scalable Formal Synthesis for Stochastic Hybrid Systems," in *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, 2019, pp. 240–251.

[19] G. Delimpaltadakis, M. Lahijanian, M. Mazo Jr, and L. Laurenti, "Interval Markov Decision Processes with Continuous Action-spaces," in *Proceedings of the 26th ACM International Conference on Hybrid Systems: Computation and Control*, 2023, pp. 1–10.

[20] R. Mazouz, J. Skovbekk, F. B. Mathiesen, E. Frew, L. Laurenti, and M. Lahijanian, "Data-Driven Permissible Safe Control with Barrier Certificates," *arXiv preprint arXiv:2405.00136*, 2024.

[21] R. Reed and M. Lahijanian, "Learning-Based Shielding for Safe Autonomy under Unknown Dynamics," *arXiv preprint arXiv:2410.07359*, 2024.

[22] I. Gracia, L. Laurenti, M. Mazo Jr, A. Abate, and M. Lahijanian, "Temporal Logic Control for Nonlinear Stochastic Systems Under Unknown Disturbances," *arXiv preprint arXiv:2412.11343*, 2024.

[23] Đ. Žikelić, M. Lechner, T. A. Henzinger, and K. Chatterjee, "Learning Control Policies for Stochastic Systems with Reach-avoid Guarantees," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 37, no. 10, 2023, pp. 11 926–11 935.

[24] F. Berkenkamp, A. P. Schoellig, and A. Krause, "Safe controller optimization for quadrotors with Gaussian processes," in *2016 IEEE international conference on robotics and automation (ICRA)*. IEEE, 2016, pp. 491–496.

[25] D. P. Bertsekas and S. Shreve, *Stochastic Optimal Control: the Discrete-time Case*. Athena Scientific, 2004.

[26] H. Zhang, T.-W. Weng, P.-Y. Chen, C.-J. Hsieh, and L. Daniel, "Efficient Neural Network Robustness Certification with General Activation Functions," *Advances in neural information processing systems*, vol. 31, 2018.

[27] F. B. Mathiesen, "Bound propagation," https://github.com/Zinoex/bound_propagation, 2022.

[28] K. Xu, Z. Shi, H. Zhang, Y. Wang, K.-W. Chang, M. Huang, B. Kailkhura, X. Lin, and C.-J. Hsieh, "Automatic Perturbation Analysis for Scalable Certified Robustness and Beyond," *Advances in Neural Information Processing Systems*, vol. 33, pp. 1129–1141, 2020.

[29] R. Mazouz, L. Laurenti, and M. Lahijanian, "Piecewise control barrier functions for stochastic systems," *arXiv preprint arXiv:2507.17703*, 2025.

[30] A. Girard, G. Gössler, and S. Mouelhi, "Safety Controller Synthesis for Incrementally Stable Switched Systems using Multiscale Symbolic Models," *IEEE Transactions on Automatic Control*, vol. 61, no. 6, pp. 1537–1549, 2015.

[31] A. De Luca, G. Oriolo, and M. Vendittelli, "Stabilization of the Unicycle via Dynamic Feedback Linearization," *IFAC Proceedings Volumes*, vol. 33, no. 27, pp. 687–692, 2000.