Inner approximations of stochastic programs for data-driven stochastic barrier function design

Frederik Mathiesen[1*†], Licio Romao[2†], Simeon C. Calvert[3], Alessandro Abate[2], and Luca Laurenti[1]

[1]Delft Center for Systems and Control, TU Delft.
[2]Department of Computer Science, University of Oxford.
[3]Department of Transport & Planning, TU Delft.
[*]Corresponding author. Email: frederik@baymler.com.
[†]These authors contributed equally to this work.

***Abstract*— This paper studies finite-horizon safety guarantees for discrete-time piece-wise affine systems with stochastic noise of unknown distributions. Our approach is based on a novel approach to synthesise a stochastic barrier function from noise data. In particular, we first build a chance-constraint tightening to obtain an inner approximation of a stochastic program. Then, we apply this methodology for stochastic barrier function design, yielding a robust linear program to which the scenario approach theory applies. In contrast to existing approaches, our method is data efficient as it only requires the number of data to be proportional to the logarithm in the negative inverse of the confidence level and is computationally efficient due to its reduction to linear programming. Furthermore, while state-of-the-art methods assume known statistics on the noise distribution, our approach does not require any information about it. We empirically evaluate the efficacy of our method on various verification benchmarks. Experiments show a significant improvement with respect to state-of-the-art, obtaining tighter certificates with a confidence that is several orders of magnitude higher.**

I. Introduction

Modern autonomous systems are often uncertain, due to e.g., sensor noise or unknown dynamics, and are commonly employed in safety-critical applications, such as automated driving [1] or robotics [2]. These applications require formal guarantees of safety in order for the system to be deployed in real-life. Consequently, computing such guarantees for stochastic systems represents an important, but non-trivial, area of research [3]. Existing approaches to address this problem either rely on abstractions, where the original system is *abstracted* into a transition system [4], or leverage the concept of Stochastic Barrier Functions (SBFs) [5]. SBFs are Lyapunov-like functions that can be employed to bound the probability that a dynamical system will remain safe for a given time horizon, without the need to explicitly evolve the system over time. A common assumption for the vast majority of the existing approaches is that the distribution of the system is known, and often either Gaussian or of bounded support [5, 6]. Unfortunately, in practice, the noise characteristics of the system are generally not known [7, 8]. This leads to the main question of this paper: *how can we compute formal certificates of safety for stochastic systems with unknown noise distribution?*

In this paper, we present a data-driven framework for the design of SBFs for piece-wise affine (PWA) stochastic systems with unknown noise distribution. Because of their modelling flexibility and of the technical advantages coming from their local linear behaviour, PWA systems are a class of non-linear systems widely employed to model dynamical systems [9]. By relying on tools from probability theory and convex optimization, we show that the problem of synthesizing a SBF for this class of systems can be reformulated as a chance-constrained optimisation problem [10]. This reformulation allows us to employ the scenario approach theory to devise a data-driven framework to synthesize SBFs with high confidence. We show that the resulting approach is data-efficient, as it only requires the amount of data to be logarithmic in the negative inverse of the confidence, and is scalable, as it reduces to the solution of a Linear Programming (LP) problem. We experimentally evaluate the performance of our method on various systems including a model of a vehicle in windy conditions. Our analysis illustrates how our approach substantially outperforms state-of-the-art comparable methods both in terms of tightness of bounds and amount of data required.

To summarize, the main contributions of this paper are:

- A data-driven method based on the scenario approach to design piece-wise affine stochastic barrier functions.
- A novel inner chance-constrained approximation to stochastic programming.
- Empirical studies that illustrates the performance of the proposed method compared to state-of-the-art.

The structure of the paper is as follows: Section II reviews convex and scenario optimisation, which are used extensively throughout the paper. Section III describes the safety certification problem and Section IV how SBFs formally can guarantee safety. In Section V are the main results of this paper; namely the inner approximation to stochastic programming and data-driven SBF design. Empirical studies are reported in Section VI.

A. Related works

Stochastic barrier functions (SBFs) were first studied in [11] to bound the probability that a stochastic system exits

Manuscript 1545 submitted to 2023 62nd IEEE Conference on Decision and Control (CDC) . Received March 31, 2023.

a given closed set in a given time horizon using super-martingale theory. Since then, various works have employed SBFs to study non-linear stochastic systems with approaches including sum-of-squares (SoS) optimization [5, 6, 12–14] and relaxations to convex programming [15, 16]. However, all these methods assume that the model of the system is fully known. A recent set of works have started to study data-driven approaches to design SBFs for stochastic systems with partially unknown dynamics, which can be employed to obtain guarantees of safety with a confidence [13, 17]. These approaches replace the stochastic program for synthesising SBFs with a Sample Average Approximation (SAA)-based program, meaning that the expectation is replaced by the sample average with a probabilistic guarantee of satisfaction of the original expectation constraint through concentration inequalities. However, these methods require an amount of data that is proportional to the negative inverse of the confidence and assume known statistics on the noise distribution. In contrast, our approach requires a number of data that is logarithmic in the negative inverse of the confidence and does not require any knowledge on the noise distribution.

Data-driven verification of stochastic systems is a relatively new area to address the problem of verifying (partially) unknown systems [13, 17–21]. To compute formal guarantees for non-linear systems, apart from the SAA approach described in the previous paragraph, existing literature focuses either on the scenario approach [19–21] or on Gaussian processes [4, 22] or on distributional-robust approaches [7]. In particular, in [19–21] the authors rely on the data-efficiency of the scenario approach theory to build abstractions of the original system with high confidence of correctness, while in [4, 22] error bounds on performing GP regression are employed to again build abstractions that are employed to perform probabilistic model checking of the unknown system. However, all these methods are abstraction-based. Consequently, they suffer from the scalability issues inherent with abstraction-based frameworks. In this paper, our approach will combine the data-efficiency of the scenario approach with the flexibility of SBFs.

B. Notation

The set of real, non-negative real, and natural numbers are denoted with $\mathbb{R}$, $\mathbb{R}_{\geq 0}$, and $\mathbb{N}$ respectively. Vectors in the Euclidean space will be denoted by the letter $x \in \mathbb{R}^n$ and random variables in $\mathbb{R}^n$ will be denoted with bold font $\mathbf{x}$. Subscripts will be used to denote a collection of elements, i.e., $x_1, \ldots, x_m$ denote different vectors in the same space. A subset X of $\mathbb{R}^n$ is convex if $\lambda x_1 + (1-\lambda)x_2 \in X$, for all $x_1, x_2 \in X$ and $\lambda \in [0,1]$. A polyhedron $P \subseteq \mathbb{R}^n$ is a convex set defined as $P = \{x \in \mathbb{R}^n : Hx \leq h\}$, where the matrix $H \in \mathbb{R}^{m \times n}$ and the vector $h \in \mathbb{R}^m$ are given, and the inequality is interpreted element-wise. This form is called a half-space representation. A function $f : \mathbb{R}^n \mapsto \mathbb{R}$ is convex if and only if its epigraph $\mathrm{epi}(f)$, defined as $\mathrm{epi}(f) = \{(x,t) \in \mathbb{R}^{n+1} : f(x) \leq t\}$, is a convex set of $\mathbb{R}^{n+1}$. Optimisation variables will be denoted by the letter z to distinguish it from the state-space variable x.

II. Preliminaries

In this section, we review some concepts used extensively throughout the paper.

a) Robust linear programming: Robust linear programming (LP) [23] forms a backbone in this paper, hence we will reiterate its definition and crucial results. Consider the following robust LP problem for polyhedron P

$$\begin{aligned} \min_{z} \quad & c^\top z \\ \text{s.t.} \quad & z^\top x \leq b, \quad \text{for all } x \in P. \end{aligned} \tag{1}$$

The following result relates robust LP to regular LP through strong duality, allowing one to recast Problem (1) as a LP problem.

Proposition 1 (Strong duality of robust LP [23]): Consider the robust LP problem in Problem (1) and the following optimisation problem

$$\begin{aligned} \min_{z,\lambda} \quad & c^\top z \\ \text{s.t.} \quad & h^\top \lambda \leq b \\ & H^\top \lambda = z, \quad \lambda \geq 0. \end{aligned} \tag{2}$$

Let sets

$$\begin{aligned} \mathcal{Z} &= \{z \in \mathbb{R}^d : \sup_{x \in P} z^\top x \leq b\}, \\ \mathcal{Z}' &= \{z \in \mathbb{R}^d : \exists \lambda \in \mathbb{R}^m_{\geq 0},\ h^\top \lambda \leq b,\ H^\top \lambda = z\}, \end{aligned}$$

be the feasible set of Problem (1) and the feasible set of Problem (2) projected onto its first d coordinates, respectively. Then we have that $\mathcal{Z} = \mathcal{Z}'$.

Proposition 1 allows us to solve a robust LP problem by means of regular LP in a lifted space, provided we have a half-space representation of P available.

b) Scenario optimization: The scenario approach theory establishes sample complexity guarantees for the probability of constraint violation of an uncertain optimisation problem [24]. In other words, the theory quantifies the number of samples that is necessary to generate, with a given confidence level, a feasible solution for a chance-constrained optimisation problem. A chance-constrained optimisation problem is defined as follows: let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space, where Ω is the sample space, $\mathcal{F}$ is a σ-algebra over Ω, and $\mathbb{P}$ is a probability measure over $\mathcal{F}$. Assume $S = \{\omega_1, \ldots, \omega_N\}$ is a set of independent samples from the probability measure $\mathbb{P}$. The set S belongs to the space $(\Omega^N, \otimes_N \mathcal{F}, \mathbb{P}^N)$, where Ω^N is the N-fold cartesian product of Ω, and $\otimes_N \mathcal{F}$ is the product σ-algebra generated by the σ-algebra $\mathcal{F}$ and, due to independence, $\mathbb{P}^N$ represents the induced measure on Ω^N [24]. A chance-constrained program is defined as

$$\begin{aligned} \min_{z} \quad & c^\top z \\ \text{s.t.} \quad & \mathbb{P}\{\omega \in \Omega : g(z,\omega) \leq 0\} \geq 1 - \epsilon, \end{aligned} \tag{3}$$

where $z \in \mathbb{R}^d$ is the optimisation variable, $c \in \mathbb{R}^d$ is the objective cost, $g : \mathbb{R}^d \times \Omega \to \mathbb{R}$ is a function that is convex in z for each value of ω and measurable in ω for each value of z, and $\epsilon \in (0,1)$ is a given bound on constraint violation.

Manuscript 1545 submitted to 2023 62nd IEEE Conference on Decision and Control (CDC) . Received March 31, 2023.

At the core of the scenario approach is the construction of the scenario program

$$\begin{aligned} \min_{z} \quad & c^\top z \\ \text{s.t.} \quad & g(z,\omega) \leq 0, \quad \text{for all } \omega \in S. \end{aligned} \tag{4}$$

and studying the probability of constraint violation associated with the optimal solution of Problem (4). To this end, we need some standard assumption [24].

Assumption 1: Consider the scenario program in Problem (4). We assume that:

- $\mathbb{P}^N$-almost surely, the feasible set given by $\mathcal{Z} = \{z \in \mathbb{R}^d : g(z,\omega) \leq 0, \text{ for all } \omega \in S\}$, has non-empty interior.
- $\mathbb{P}^N$-almost surely, the optimal solution exists and is unique.

Denote by $z^\star(S)$ the unique, optimal solution of Problem (4). Notice that $z^\star(S)$ is a random variable from Ω^N to $\mathbb{R}^d$. The probability of constraint violation associated with $z^\star(S)$ is given by $V(z) = \mathbb{P}\{\omega \in \Omega : g(z,\omega) > 0\}$.

Proposition 2 ([24]): Let $N \in \mathbb{N}$ represent the number of available samples and $\epsilon \in (0,1)$ be given. Consider Problem (4) and suppose that Assumption 1 holds. Then we have that

$$\mathbb{P}^N\{S \in \Omega^N : V(z^\star(S)) > \epsilon\} \leq \sum_{i=0}^{d-1} \binom{N}{i} \epsilon^i (1-\epsilon)^{N-i}.$$

Proposition 2 will be key in establishing safety guarantees for the class of stochastic models considered in this paper.

III. Problem statement

In this section, we formally define the class of systems we consider and probabilistic safety, the specification considered in this paper.

A. Piece-wise affine stochastic dynamics

Let $\mathcal{P} = \{P_1, \dots, P_\ell\}$ be a polyhedral partition of the state space $X \subseteq \mathbb{R}^n$, where each P_i, $i = 1, \dots, \ell$ is given by its half-space representation. Consider the following discrete-time stochastic piece-wise affine (PWA) system:

$$\mathbf{x}(k+1) = f(\mathbf{x}(k)) + \eta(k), \quad \mathbf{x}(0) \in X_0, \tag{5}$$

where $k \in \mathbb{N}$ denotes the (discrete) time index, $X_0 \subset \mathcal{S}$ is a set of initial states, and $f : X \mapsto \mathbb{R}^n$ is a PWA vector field given by

$$f(x) = f_i(x) = A_i x + b_i, \quad x \in P_i \subseteq \mathbb{R}^n,$$

for some matrix $A_i \in \mathbb{R}^{n \times n}$ and vector $b_i \in \mathbb{R}^n$. The additive term $(\eta(k))_{k\in\mathbb{N}}$ is a stochastic process defined in the filtered probability space $(\Omega, \mathcal{F}, (\mathcal{F}_k)_{k\in\mathbb{N}}, \mathbb{P})$, where $\mathcal{F}_k$ is the natural filtration of the process[1] $\eta(k)$, i.e., it is the σ-algebra generated by the random variables $\eta(k')$, $k' \leq k$. Notice that $(\mathbf{x}(k))_{k\in\mathbb{N}}$ is also a stochastic process in the space $(\Omega, \mathcal{F}, \mathbb{P})$ that is, it is $\mathcal{F}_{k-1}$-measurable [25]. In simpler words, $\mathbf{x}(k)$ depends on the realisation of noise $\eta(k')$ for all $k' \leq k-1$.

Assumption 2: We assume that $\eta(k)$ is independent and identically distributed (iid.) for all $k \in \mathbb{N}$.

Formally, η is a measurable function $\mathbb{N} \times \Omega \to \mathbb{R}^n$, but by the iid. assumption, $(\eta(k))_{k\in\mathbb{N}}$ can be interpreted as a sequence of identically distributed random variables. As such, we may omit the dependence on k when referring to the time-invariant random variable and write $\eta(\omega)$.

B. Time-bounded probabilistic safety

Our goal is to study probabilistic safety for System (5).

Definition 1 (Probabilistic safety [5]): Let $T \in \mathbb{N}$ be a time horizon and $\mathcal{S}$ be a measurable subset of X[2]. We define probability safety for System (5) as

$$\zeta(\mathcal{S}, T) = \mathbb{P}\{\omega \in \Omega : \mathbf{x}(k) \in \mathcal{S} \text{ for all } k \in \{0, \dots, T\}\}. \tag{6}$$

We assume that, while f is known, η is unknown and we can only generate iid. samples from it. Under these assumptions, our goal in this paper is to compute a (non-trivial) lower bound on $\zeta(\mathcal{S}, T)$ for System (5).

Our approach is based on using the sampled data to synthesize a piece-wise affine (PWA) Stochastic Barrier Function (SBF) for System (5) with high confidence. In order to do that, in Section V-A we develop a novel and powerful inner approximation for the feasible set of stochastic programs in terms of chance-constrained optimisation. This result is employed in Section V-B to use the scenario approach to synthesize SBF for System (5) with high confidence and by requiring a number of data logarithmic in the negative inverse of the confidence. In Section V-C, we show that in the setting considered in this paper the resulting optimization problem reduces to LP, thus enabling efficient and scalable synthesis. Before, in the next section, we review SBFs and how they can be employed to guarantee a lower bound on $\zeta(\mathcal{S}, T)$.

IV. Stochastic barrier function (SBF)

SBFs are Lyapunov-like conditions commonly employed to compute the safety probability of stochastic systems [5].

Definition 2 (Stochastic Barrier Function): Let $\mathcal{U} = X \setminus \mathcal{S}$ be the unsafe set and X_0 the set of initial states, with $X_0 \subseteq \mathcal{S}$, then a non-negative function $B : X \mapsto \mathbb{R}_{\geq 0}$ is called a Stochastic Barrier Function if there exist non-negative constants γ, c such that

$$B(x) \leq \gamma, \quad \text{for all } x \in X_0, \tag{7}$$

$$B(x) \geq 1, \quad \text{for all } x \in \mathcal{U}, \tag{8}$$

$$\mathbb{E}\left[B(f(x) + \eta(\omega))\right] \leq B(x) + c, \quad \text{for all } x \in \mathcal{S}. \tag{9}$$

The conditions of Definition 2 lead to a lower bound on $\zeta(\mathcal{S}, T)$, as described in the next proposition.

[1]Notice that the stochastic process affecting the dynamics is a measurable function from $\mathbb{N} \times \Omega$ to the Euclidean space $\mathbb{R}^n$, as such, both processes η and $\mathbf{x}$ would have to be written as $\eta(k,\omega)$ and $\mathbf{x}(k,\omega)$. For brevity, however, we omit the dependence on ω throughout the paper. When computing probabilities associated with the process $\mathbf{x}(k,\omega)$, we use the notation $\mathbb{P}\{\omega \in \Omega : \mathbf{x}(k) \in A, \text{ for all } k \in \{1, \dots, T\}\}$, where the reader should have in mind that the process $\mathbf{x}$ is defined in the samples space Ω. Please refer to [25] for more details.

[2]If $X \neq \mathbb{R}^n$ then it may be necessary to replace $\mathbf{x}(k)$ with an equivalent stopped process $\tilde{\mathbf{x}}(k)$ [6].

Manuscript 1545 submitted to 2023 62nd IEEE Conference on Decision and Control (CDC) . Received March 31, 2023.

Proposition 3 ([11, Chapter 3, Theorem 3]): Let B be a SBF satisfying the conditions in Definition 2 for System (5), time horizon T, and safe set $\mathcal{S}$. Then, it holds that $\zeta(\mathcal{S}, T) \geq 1 - (\gamma + cT)$.

Thanks to Proposition 3, a sufficient condition to establish a lower bound on the safety probability is to design a SBF that satisfies Equations (7)-(9). This can be obtained by solving the following stochastic program

$$\min_{\gamma \geq 0,\, c \geq 0,\, \theta} \quad \gamma + cT, \tag{BP}$$

subject to the conditions in Definition 2. In other words, synthesis of a SBF can be framed as a minimisation over $\gamma + cT$. In this optimisation problem, the expectation condition (Equation (9)) can generally be computed analytically only under some strong assumptions on the noise distribution [6, 26]. Our approach proposes a new, inner chance-constrained approximation of Problem (BP), which allows us to rely on tools from scenario optimisation to synthesize a barrier [24]. The resulting approach is a distribution-free, data-driven method to obtain a SBF as a safety certificate with a high confidence of validity. Note that to guarantee the convexity of Problem (BP), B is generally restricted to be either a SoS polynomial or an exponential function [6]. In this paper, also motivated by the structure of System (5), we will consider piece-wise affine B, which have the flexibility to be able to model arbitrarily well any continuous function assuming the number of pieces of B is large enough.

V. Data-driven stochastic barrier function design

In this section, we present the main results of this paper. Namely, an inner approximation of the feasible set of Problem (BP) in terms of a chance-constrained problem (Section V-A), how the chance-constrained approximation enables use the scenario approach for data-driven synthesis (Section V-B), and a LP formulation of the scenario program for efficient and scalable certification (Section V-C).

A. A novel inner chance-constrained approximation of stochastic programs

Consider the following stochastic program, which generalizes Problem (BP),

$$\begin{aligned} \min_{z} \quad & c^\top z \\ \text{s.t.} \quad & \mathbb{E}\left\{g(x, z, \eta(\omega))\right\} \leq h(x, z), \qquad \text{for all } x \in \mathcal{S}, \end{aligned} \tag{SP}$$

where $z \in \mathbb{R}^d$ is the decision variable, $\eta : \Omega \to \mathbb{R}^m$ is a random variable on $(\Omega, \mathcal{F}, \mathbb{P})$, and $g : \mathbb{R}^n \times \mathbb{R}^d \times \mathbb{R}^m \mapsto \mathbb{R}$ is a measurable and integrable function for each pair $(x, z) \in \mathbb{R}^n \times \mathbb{R}^d$, $h : \mathbb{R}^n \times \mathbb{R}^d \mapsto \mathbb{R}$ is a convex function, and $\mathcal{S}$ is a measureable set on $\mathbb{R}^n$. The feasible set of Problem (SP) is given by

$$\mathcal{Z} = \{z \in \mathbb{R}^d : \mathbb{E}\{g(x, z, \eta(\omega))\} \leq h(x, z) \text{ for all } x \in \mathcal{S}\}.$$

Solving this class of problems is extremely challenging because analytic expressions of the expectation constraint are rarely available, even if the distribution $\mathbb{P}$ is known (which is not the case in this paper). To solve this problem, in Theorem 1, we derive a chance-constrained problem whose feasible set is a subset of $\mathcal{Z}$. Thus, its optimal solution is an upper bound to that of Problem (SP). Critically, such a relaxation allows us to rely on the scenario approach (see Section II) to derive tight confidence bounds on the resulting solution.

Theorem 1 (Inner chance-constrained approximation): Let $\epsilon \in (0, 1)$ be a given threshold and assume a uniform upper bound $M = \sup_{x,z,\omega} g(x, z, \eta(\omega))$ on g. Choose $\nu \geq \max\left(\frac{\epsilon(M - h(x,z))}{1-\epsilon}, h(x, z) - M\right)$ for all $(x, z) \in \mathbb{R}^n \times \mathbb{R}^d$. Define the set

$$E(x, z) = \{\omega \in \Omega : g(x, z, \eta(\omega)) + \nu \leq h(x, z)\},$$

and consider the chance-constrained problem

$$\begin{aligned} \min_{z} \quad & c^\top z \\ \text{s.t.} \quad & \mathbb{P}\left\{E(x, z)\right\} \geq 1 - \epsilon, \text{ for all } x \in \mathcal{S}, \end{aligned} \tag{CCP}$$

whose feasible set is given by

$$\mathcal{Z}' = \left\{z \in \mathbb{R}^d : \mathbb{P}\left\{E(x, z)\right\} \geq 1 - \epsilon, \text{ for all } x \in \mathcal{S}\right\}.$$

Then we have that $\mathcal{Z}' \subseteq \mathcal{Z}$.

Proof: Pick any $\bar{z} \in \mathcal{Z}'$. Our goal is to show that $\bar{z} \in \mathcal{Z}$. To this end, pick any $x \in \mathcal{S}$ and notice that

$$\begin{aligned} \mathbb{E}\left[g(x, \bar{z}, \eta(\omega))\right] = & \int_{E(x,\bar{z})} g(x, \bar{z}, \eta(\omega))\, d\mathbb{P}(\omega) + \\ & \int_{E(x,\bar{z})^c} g(x, \bar{z}, \eta(\omega))\, d\mathbb{P}(\omega). \end{aligned}$$

Hence, we can derive the following

$$\begin{aligned} & \mathbb{E}\left\{g(x, \bar{z}, \eta(\omega))\right\} \\ & \quad \leq (h(x, \bar{z}) - \nu)\mathbb{P}\{E(x, \bar{z})\} + M\mathbb{P}\{E(x, \bar{z})^c\} \\ & \quad = h(x, \bar{z}) - \nu + \mathbb{P}\{E(x, \bar{z})^c\}(M - h(x, \bar{z}) + \nu) \end{aligned} \tag{10}$$

where the first inequality follows from the fact that $g(x, \bar{z}, \omega)$ is less than or equal to $h(x, \bar{z}) - \nu$ on the set $E(x, \bar{z})$ and that g is uniformly upper bounded by M on the whole space Ω. The equality is obtained by substituting $\mathbb{P}\{E(x, \bar{z})\} = 1 - \mathbb{P}\{E(x, \bar{z})^c\}$. Since $\nu \geq h(x, \bar{z}) - M$ for all $(x, \bar{z}) \in \mathbb{R}^n \times \mathbb{R}^d$, then we may use the fact that $\mathbb{P}\{E(x, \bar{z})^c\} \leq \epsilon$ (due to feasibility of $\bar{z}$) to obtain an upper-bound to (10) as

$$\begin{aligned} & h(x, z) - \nu + \mathbb{P}\{E(x, z)^c\}\,(M - h(x, z) + \nu) \\ & \qquad \leq h(x, z) - \nu + \epsilon(M - h(x, z) + \nu) \\ & \qquad = h(x, z) + \epsilon(M - h(x, z)) - (1 - \epsilon)\nu \\ & \qquad \leq h(x, z), \end{aligned}$$

where the last inequality follows from the fact that $\nu \geq \frac{\epsilon(M - h(x,z))}{1-\epsilon}$ for all $(x, z) \in \mathbb{R}^n \times \mathbb{R}^d$. Hence, we observe that $\bar{z} \in \mathcal{Z}$, thus concluding the proof of the theorem. ■

Note that while the requirement that the constraints are uniformly upper bounded may seem limiting, this is trivially satisfied for SBF design where a barrier $B(x)$ is guaranteed to be bounded and non-negative.

Manuscript 1545 submitted to 2023 62nd IEEE Conference on Decision and Control (CDC) . Received March 31, 2023.

B. Data-driven stochastic barrier design

To apply Theorem 1 to synthesise SBFs, we state the following trivial, yet important, corollary of Theorem 1.

Corollary 1: Consider System (5), and the barrier function $B(x,\theta)$ as in Definition 2, where B is convex in θ. Assume a given $\epsilon \in (0,1)$ and $M \geq 1$, and define decision variables $z = (c, \gamma, \theta)$ and functions $g(x, z, \eta(\omega)) = B(f(x) + \eta(\omega), \theta)$ and $h(x,z) = B(x,\theta) + c$. Choose $\nu \geq \max\left(\frac{\epsilon(M-h(x,z))}{1-\epsilon}, h(x,z) - M\right)$ for all $(x,z) \in \mathbb{R}^n \times \mathbb{R}^d$. Then, the feasible set of

$$\begin{aligned} \min_{\gamma\geq 0,\, c\geq 0,\, \theta} \quad & \gamma + cT \\ & B(x,\theta) \in [0, M], \quad \text{for all } x \in \mathbb{R}^n, \\ & B(x,\theta) \leq \gamma, \quad \text{for all } x \in X_0, \\ \text{s.t.} \quad & B(x,\theta) \geq 1, \quad \text{for all } x \in \mathcal{U}, \\ & \mathbb{P}\left\{E(x,z)\right\} \geq 1-\epsilon, \ \text{for all } x \in \mathcal{S}, \end{aligned} \tag{CCBP}$$

is contained in the feasible set of Problem (BP).

Corollary 1 opens new ways for data-driven design of stochastic barrier functions. Rather than relying on standard concentration inequalities to approximate the expectation in Equation (9) as in [17], we can perform chance-constraint tightening with the parameter ν to guarantee the feasible set of (SBP) is an inner approximation of (CCBP). Building on this result, in Lemma 1 we use the scenario approach to design SBFs from data with high confidence.

Lemma 1: Assume that $S = \{\omega_1, \ldots, \omega_N\}$ is a collection of N independent samples from the distribution $\mathbb{P}$. Fix $\epsilon \in (0,1)$, $M \geq 1$, and $\nu \geq \max\left(\frac{\epsilon(M-h(x,z))}{1-\epsilon}, h(x,z) - M\right)$ for all $(x,z) \in \mathbb{R}^n \times \mathbb{R}^d$, and let $\beta = \sum_{i=0}^{d-1} \binom{N}{i} \epsilon^i (1-\epsilon)^{N-i}$, where $d = \ell(n+1) + 2$. Let $(c^\star, \gamma^\star, \theta^\star)$ be the optimal solution to the scenario program

$$\begin{aligned} \min_{\gamma\geq 0,\, c\geq 0,\, \theta} \quad & \gamma + cT \\ \text{s.t.} \quad & B(x,\theta) \in [0, M], && \text{for all } x \in \mathbb{R}^n, \\ & B(x,\theta) \leq \gamma, && \text{for all } x \in X_0, \\ & B(x,\theta) \geq 1, && \text{for all } x \in \mathcal{U}, \\ & g(x,z,\eta(\omega)) + \nu \leq h(x,z), \\ & \quad \text{for all } \omega \in S, && \text{for all } x \in \mathcal{S}, \end{aligned} \tag{SBP}$$

where g and h are defined as in Corollary 1. Then, with confidence $1-\beta$, $(c^\star, \gamma^\star, \theta^\star)$ defines a lower bound on the safety probability, i.e.,

$$\zeta(\mathcal{S}, T) \geq 1 - (\gamma^\star + c^\star T).$$

Remark 1: Observe that the amount of data N required to achieve a desired confidence $1-\beta$ with existing approaches based on concentration inequalities to approximate Equation (9) is proportional to $1/\beta$ [17] whereas for our approach, the amount required is proportional to $\ln(1/\beta)$ [27]. To put this into perspective, consider $\beta = 10^{-9}$, which is the gold standard in both aviation and autonomous vehicle design [1], then $1/\beta = 10^9$ while $\ln(1/\beta) \approx 20.7$.

C. Linear programming reformulation of stochastic barrier function design

Lemma 1 defines an optimization problem (Problem (SBP)) for the data-driven design of SBFs. The resulting problem can for instance be solved under the assumption that B is a SoS function using semi-definite programming [5, 6]. However, while viable, this approach can often be conservative and lack of scalability [16]. Motivated by the PWA structure of System (5), we propose instead to use a PWA function to parameterize a SBF. Then, by applying tools from robust LP (i.e., Proposition 1), we show that Problem (SBP) can be transformed into a linear program with a finite number of constraints. To this end, let $\bar{\mathcal{P}} = \{\bar{P}_1, \ldots, \bar{P}_{\bar{\ell}}\}$ be a polyhedral partition of the state space X with $\bar{\ell} \geq \ell$. Assume for simplicity that each region $\bar{P}_i$ is a subset of exactly one region $P_{r(i)}$ from the partition $\mathcal{P}$, with a surjective function $r : \{1, \ldots, \bar{\ell}\} \to \{1, \ldots, \ell\}$ mapping between indices. In other words, the partition for the PWA barrier candidate $\bar{\mathcal{P}}$ is aligned with the partition of the dynamics $\mathcal{P}$, although potentially more fine-grained. We consider a PWA SBF B defined as follows

$$B(x,\theta) = \max(B_1(x,\theta), \ldots, B_{\bar{\ell}}(x,\theta)), \tag{11}$$

where

$$B_i(x,\theta) = \begin{cases} u_i^\top x + v_i, & \text{for } x \in \bar{P}_i, \\ 0, & \text{otherwise}, \end{cases}$$

and $\theta \in \mathbb{R}^{\bar{\ell}(n+1)}$ is the set of parameters $(u_i, v_i) \in \mathbb{R}^{n+1}$, $i = 1, \ldots, \bar{\ell}$, used to define the SBF.

For convenience, we also define collections of indices from $I = \{1, \ldots, \bar{\ell}\}$ that correspond to elements of the partition $\bar{\mathcal{P}}$ that have non-empty intersection with the set of safe, unsafe, and initial states, respectively:

$$\begin{aligned} I_{\mathcal{S}} &= \{i \in I : \bar{P}_i \cap \mathcal{S} \neq \emptyset\}, \\ I_{\mathcal{U}} &= \{i \in I : \bar{P}_i \cap \mathcal{U} \neq \emptyset\}, \\ I_{X_0} &= \{i \in I : \bar{P}_i \cap X_0 \neq \emptyset\}. \end{aligned} \tag{12}$$

With the family of barrier functions defined, we turn our attention to the reduction of Problem (SBP) into a linear problem. In order to do that we need to reduce each of the constraints in Problem (SBP) into linear constraints. The reduction for the non-negativity, upper bound, initial, and unsafe set constraints follow a similar structure. Hence, for brevity, we only describe the process for the non-negativity constraint. To this end, we first make an assumption regarding the boundaries between regions, which we assume to have measure zero.

Assumption 3: We assume for any two regions i, j where $i \neq j$ that

$$\mathbb{P}\{\omega \in \Omega : \mathbf{x}(k) \in \bar{P}_i \cap \bar{P}_j \text{ for all } k = 0, \ldots, T\} = 0.$$

This assumption, generally satisfied in practice, is necessary to guarantee that the intersection between two adjacent regions has no volume. Due to Assumption 3, we can impose $B_i(x,\theta) \geq 0$ for all $x \in \bar{P}_i$ independently for each region.

Manuscript 1545 submitted to 2023 62nd IEEE Conference on Decision and Control (CDC) . Received March 31, 2023.

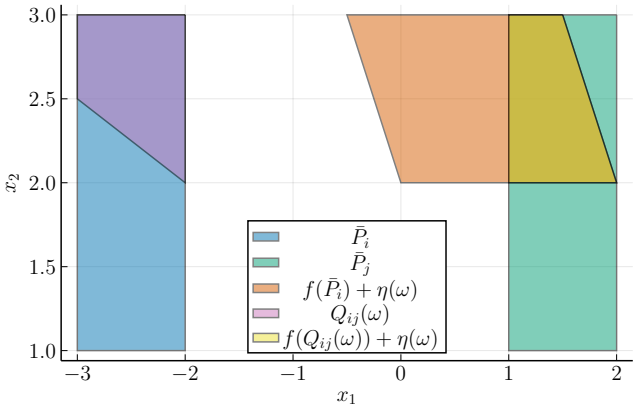

Fig. 1: Given two regions $\bar{P}_i, \bar{P}_j$ and a realisation of the noise ω, the set $Q_{ij}(\omega)$ represents the subset of $x \in \bar{P}_i$ such tat $f(x)+\eta(\omega) \in \bar{P}_j$. In other words, $Q_{ij}(\omega)$ is the subset of $\bar{P}_i$ that can reach $\bar{P}_j$ given the realisation of the noise ω.

Note that for each region i the barrier $B_i(x,\theta)$ is an affine function in x over the polyhedron $\bar{P}_i$. Hence, the resulting constraint is a robust LP constraint (See Section II). Thus, we can rely on Proposition 1 to transform the problem to a lifted space representable by a regular LP constraint. More concretely, consider the constraint $B_i(x,\theta) = u_i^\top x + v_i \geq 0$ for all $x \in \bar{P}_i$ where $\bar{P}_i$ is defined by its half-space representation $(H_i, h_i) \in \mathbb{R}^{m\times n} \times \mathbb{R}^m$. Then with dual variable $\lambda_i \in \mathbb{R}^m_{\geq 0}$, this can be replaced with the following two equivalent constraints using Proposition 1: $h_i^\top \lambda_i \leq v_i$ and $H_i^\top \lambda_i = -u_i$.

Now, consider the last constraint of Problem (SBP), namely $g(x,z,\eta(\omega)) + \nu \leq h(x,z)$ for all $\omega \in S$, for all $x \in \mathcal{S}$. For this constraint Proposition 1 is not immediately applicable, as we must consider the value of the barrier before and after a transition. Instead, we construct a robust LP constraint for each pair of regions $(i,j) \in I_{\mathcal{S}} \times I$:

$$\begin{aligned} B_j(f_{r(i)}(x)+\eta(\omega)) + \nu \leq B_i(x) + c, \\ \text{for all } \omega \in S, \text{ for all } x \in Q_{ij}(\omega). \end{aligned} \tag{13}$$

The random subset $Q_{ij}(\omega)$ of X is defined as

$$Q_{ij}(\omega) = \{x \in \bar{P}_i : f_{r(i)}(x) + \eta(\omega) \in \bar{P}_j\}, \tag{14}$$

representing the set of elements in the region $\bar{P}_i$ that are mapped to $\bar{P}_j$ under a given realisation of the noise. A pictorial example of $Q_{ij}(\omega)$ can be found in Figure 1. Since both $\bar{P}_i$ and $\bar{P}_j$ are polyhedra and $f_{r(i)}$ is an affine function, $Q_{ij}(\omega)$ is a polyhedron [23]. Thus, we can again use Proposition 1 to transform Equation (13) to linear constraints. Specifically, for a pair of regions $(i,j) \in I_{\mathcal{S}} \times I$ and a realisation of the noise $\omega \in S$, with half-space representation $(H_{ij}, h_{ij}) \in \mathbb{R}^{m\times n} \times \mathbb{R}^m$ of region $Q_{ij}(\omega)$ and dual variable $\lambda_{ij} \in \mathbb{R}^m_{\geq 0}$, the original semi-infinite constraint is transformed into the following two constraints

$$\begin{aligned} h_{ij}^\top \lambda_{ij} &\leq v_i - v_j - u_j^\top (b_{r(i)} + \eta(\omega)) + c - \nu, \\ H_{ij}^\top \lambda_{ij} &= A_{r(i)}^\top u_j - u_i. \end{aligned}$$

Collecting together all finite sets of constraints, the LP equivalent representation of Program (SBP) is as follows.

$$\begin{aligned} \min_{\gamma\geq 0,\, c\geq 0,\, \theta} \quad & \gamma + cT \\ & h_i^\top \lambda_i \leq v_i,\ H_i^\top \lambda_i = -u_i, \\ & h_i^\top \lambda_{iM} \leq M - v_i,\ H_i^\top \lambda_{iM} = u_i, \text{ for all } i \in I, \\ & h_{i0}^\top \lambda_{i0} \leq \gamma - v_i,\ H_{i0}^\top \lambda_{i0} = u_{i0}, \text{ for all } i \in I_{X_0}, \\ \text{s.t.} \quad & h_i^\top \lambda_{i\mathcal{U}} \leq v_i - 1,\ H_i^\top \lambda_{i\mathcal{U}} = -u_i, \text{ for all } i \in I_{\mathcal{U}}, \\ & h_{ij}^\top \lambda_{ij} \leq v_i - v_j - u_j^\top (b_{r(i)} + \eta(\omega)) + c - \nu, \\ & H_{ij}^\top \lambda_{ij} = A_{r(i)}^\top u_j - u_i, \text{ for all } \omega \in S, \\ & \quad \text{for all } (i,j) \in I_{\mathcal{S}} \times I, \end{aligned} \tag{FSBP}$$

where $\lambda_i, \lambda_{iM}, \lambda_{i0}, \lambda_{i\mathcal{U}}, \lambda_{ij}$ are non-negative dual variables. (H_{i0}, h_{i0}) denotes the half-space representation of $\bar{P}_i \cap X_0$.

Theorem 2: Let B be a piecewise affine (PWA) stochastic barrier function as defined in Equation (11). Then, an optimal solution $z^\star(S)$ to Problem (FSBP) is an optimal solution to Problem (SBP).

By Lemma 1 and Theorem 2, Problem (FSBP) is an equivalent LP representation of Problem (BP) that can be employed to synthesize a SBF. The number of decision variables and constraints of the resulting LP depends on the number of half-spaces necessary to represent each polyhedron. In particular, assume for simplicity that each polyhedral region is represented by m half-spaces. Then, the number of decision variables in Problem (FSBP) is

$$\underbrace{2}_{\gamma,c} + \underbrace{(n+1)\cdot\bar{\ell}}_{\theta} + \underbrace{m\cdot(2\bar{\ell} + |I_{X_0}| + |I_{\mathcal{U}}| + N|I_{\mathcal{S}}|\bar{\ell})}_{\text{dual variables}},$$

while the number of constraints is:

$$2 + m\cdot(6\bar{\ell} + 3|I_{X_0}| + 3|I_{\mathcal{U}}| + 3N|I_{\mathcal{S}}|\bar{\ell}).$$

Note that both the number of constraints and number of variables depend on term $mN|I_{\mathcal{S}}|\bar{\ell}$, where we remark that $|I_{\mathcal{S}}|$ and $\bar{\ell}$ are respectively number of pieces in the SBF that intersect with $\mathcal{S}$ and total number of pieces of the SBF. This illustrates how the dimension of the resulting LP problem grows linearly in the number of samples N and quadratically in the complexity (i.e., number of pieces) of the barrier B.

VI. Experiments

To show the efficacy of the proposed method, we evaluate it on three different benchmarks. Namely:

- a 1D linear system governed by the following dynamics $\mathbf{x}(k+1) = \mathbf{x}(k) + \eta(k)$, which is a martingale,
- a 2D linear model of longitudinal dynamics for a drone from [20],
- a 2D PWA model of a vehicle driving with constant velocity subject to a wind disturbance along its path.

For the martingale system, the goal is to quantify the probability that from any state within a radius of 0.5 around the origin the system will stay within a set of radius of 2.5 around the origin for a time horizon $T = 10$. For the drone,

Manuscript 1545 submitted to 2023 62nd IEEE Conference on Decision and Control (CDC) . Received March 31, 2023.

the goal is to certify that the speed of the drone always stays lower than 10 units, again for a time horizon $T = 10$. Please note that in [20], they consider an uncertain mass of the drone, which is not compatible with Problem (FSBP). To make the benchmark compatible, we let the mass be equal to the center of the uncertainty interval, namely $m = 1$. Finally, the last model represents a vehicle driving with constant velocity. The goal is to stay on the road within $T = 10$, despite a varying disturbance from wind along the route. Mathematically, we can describe the dynamics as follows:

$$\mathbf{x}(k+1) = \begin{bmatrix} 1 & 0 \\ 0 & 0.95\tau \end{bmatrix} \mathbf{x}(k) + \begin{bmatrix} v\tau \\ 0.5d\tau^2 \end{bmatrix} + \eta(k)$$

where we choose a velocity $v = 13.89$, a time resolution $\tau = 1$, and a disturbance $d = 0.0626$ for regions where the longitudinal position x_1 satisfies $80 \leq x_1 \leq 120$ and $d = 0$ otherwise. $\eta(k)$ Gaussian noise with diagonal covariance, which of course is assumed unknown and only iid. samples can be generated from it.

We compare our method against SAA [17], arguably the state-of-the-art for data-driven synthesis of SBFs, on the three benchmarks. For SAA, we employ a 4th degree polynomial barrier and SoS optimisation. For our method we consider a PWA barrier function with $\bar{\ell}$ pieces, where $\bar{\ell}$ equals 7 and 33 for respectively the Martingale and Drone example, while for the Vehicle example we consider different values of $\bar{\ell}$ to study its impact. The benchmarks and methods have been implemented[3] in Julia (1.8.3) with JuMP.jl (1.6.0) as the modelling framework and Mosek (9.3.11) as the LP solver. The experiments are conducted on a computer running Linux Manjaro (5.10.157) with an Intel Core i7-10610U CPU and 16GB RAM.

Table I shows the results across all three systems. The results are reported as the average over 100 trials to ensure that certification is not due to a lucky sampling of the noise. Comparing the two methods in Table I, we see that the proposed method outperforms SAA across all measures on both the Martingale and Drone system, while the vehicle is intractable for SAA. This is because the Vehicle example is a PWA system, which is not compatible with the SoS optimisation employed for SAA. Note that for any system considered in this paper, SAA can only certify with a confidence 99%. On the other hand, our method, thanks to the bounds we compute in Lemma 1, achieves a confidence of $1-10^{-9}$ (see Remark 1). In addition, our method achieves a higher certified probability of safety and is orders of magnitude faster. The latter is due the reduction to LP and to the use of the scenario approach to derive confidence bounds. To further highlight the data-efficiency, we present in Figure 2 the number of samples required to achieve a desired confidence for both methods. The figure clearly shows that our method requires orders of magnitude less samples to achieve the same confidence.

Next, we analyze the impact of increasing the number of pieces in the SBF ($\bar{l}$), towards a more expressive SBF. Table I reveals that increasing the number of partitions for the barrier (see Equation 11) yields tighter guarantees. This is expected. In fact, a PWA function with arbitrarily many pieces can approximate arbitrarily well any continuous function, thus increasing the flexibility of the framework. However, this comes at the cost of increased computation time. Note however, that computation times are always faster than SAA even for relatively large $\bar{\ell}$. We also observe that despite using fewer regions for the Drone system, it is slower to compute than for the Vehicle system with both 42 and 46 regions. To understand why note that the constraint in Equation (13) is trivially satisfied if $Q_{ij}(\omega)$ is empty, or in other words, it is impossible to reach region j from region i under the realisation of the noise ω. The Drone system has more non-empty $Q_{ij}(\omega)$ over the Vehicle system and thus is slower.

[3]Code is available at `https://github.com/DAI-Lab-HERALD/scenario-barrier` under a GNU GPLv3 license.

TABLE I: Certified safety and computation time using the method explained in Section V. Results are reported as the average over 100 trials. n is the dimensionality of the system and $\bar{\ell}$ is the number of pieces of the PWA SBF B. $1-\beta$ is the confidence in the certificate and $\zeta(\mathcal{S}, T)$ is the certified level of safety. Bold font denotes best method for each measure and system.

System	n	Method	$\bar{\ell}$	β	$\zeta(\mathcal{S},T)$	Comp. time (s)
Martingale	1	Our	7	$\mathbf{10^{-9}}$	**0.995**	**0.190**
		SAA	-	10^{-2}	0.848	89.49
Drone	2	Our	33	$\mathbf{10^{-9}}$	**0.995**	**60.3**
		SAA	-	10^{-2}	0.850	2090
Vehicle	2	Our	18	$\mathbf{10^{-9}}$	0.606	**12.4**
		Our	42	$\mathbf{10^{-9}}$	0.708	55.6
		Our	46	$\mathbf{10^{-9}}$	0.839	57.8
		Our	126	$\mathbf{10^{-9}}$	**0.995**	172
		SAA	-	N/A	N/A	N/A

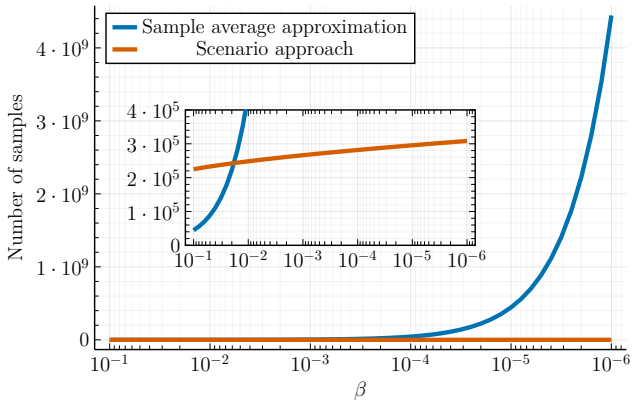

Fig. 2: A plot for the number of samples required to achieve a given confidence $1-\beta$ for SAA and the proposed method using the scenario approach. The number of samples reported in this plot is specifically for the vehicle system with 126 regions, as reported in Table I.

VII. Conclusions

We studied the problem of certifying probabilistic safety for partially known stochastic systems. The problem is important for the adoption of autonomous safety-critical systems. This safety verification problem was addressed by synthesising Stochastic Barrier Function (SBF) with a data-driven approach leveraging the scenario optimization theory. To apply the data-driven scenario approach to SBF synthesis, a novel inner chance-constrained approximation to stochastic programming was presented. The chance-constrained approximation was applied to SBFs in Corollary 1: an important consequence of it is that it can be easily extended to other classes of systems, e.g. polynomial or more general non-linear systems. Experimental studies showed that our method can certify systems with a confidence that is orders of magnitude greater than the state-of-the-art methods, while also producing tighter bounds and being faster.

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] S. C. Livingston, R. M. Murray, and J. W. Burdick, "Backtracking temporal logic synthesis for uncertain environments," in *ICRA*, 2012.

[3] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, "Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems," *Automatica*, 2008.

[4] J. Jackson, L. Laurenti, E. Frew, and M. Lahijanian, "Strategy synthesis for partially-known switched stochastic systems," *arXiv preprint arXiv:2104.02172*, 2021.

[5] S. Prajna, A. Jadbabaie, and G. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Transactions on Automatic Control*, 2007.

[6] C. Santoyo, M. Dutreix, and S. Coogan, "A barrier function approach to finite-time stochastic system verification and control," *Automatica*, 2021.

[7] I. Gracia, D. Boskos, L. Laurenti, and M. Mazo, "Distributionally robust strategy synthesis for switched stochastic systems," *arXiv preprint arXiv:2212.14260*, 2022.

[8] H. Rahimian and S. Mehrotra, "Distributionally robust optimization: A review," *arXiv preprint arXiv:1908.05659*, 2019.

[9] E. D. Sontag, "Interconnected automata and linear systems: A theoretical framework in discrete-time," in *Hybrid Systems III: Verification and Control*, Springer, 2005, pp. 436–448.

[10] A. Shapiro, D. Dentcheva, and A. Ruszczski, *Lectures on stochastic programming*. Society for Industrial & Applied Mathematics, 2021.

[11] H. J. Kushner, "Stochastic stability and control," Brown Univ Providence RI, Tech. Rep., 1967.

[12] P. Jagtap, S. Soudjani, and M. Zamani, "Temporal logic verification of stochastic systems using barrier certificates," in *ATVA*, 2018.

[13] A. Salamati and M. Zamani, "Safety verification of stochastic systems: A repetitive scenario approach," *IEEE Control Systems Letters*, 2023.

[14] A. Abate, A. Edwards, M. Giacobbe, H. Punchihewa, and D. Roy, "Quantitative verification with neural networks for probabilistic programs and stochastic systems," *arXiv preprint arXiv:2301.06136*, 2023.

[15] R. Mazouz, K. Muvvala, A. R. Babu, L. Laurenti, and M. Lahijanian, "Safety guarantees for neural network dynamic systems via stochastic barrier functions," in *Advances in Neural Information Processing Systems*, 2022.

[16] F. B. Mathiesen, S. C. Calvert, and L. Laurenti, "Safety certification for stochastic systems via neural barrier functions," *IEEE Control Systems Letters*, 2023.

[17] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates," *IFAC-PapersOnLine*, 2021.

[18] A. Abate and M. Prandini, "Approximate abstractions of stochastic systems: A randomized method," in *IEE CDC*, 2011.

[19] T. S. Badings, A. Abate, N. Jansen, D. Parker, H. A. Poonawala, and M. Stoelinga, "Sampling-based robust control of autonomous systems with non-gaussian noise," *Proceedings of the AAAI Conference on Artificial Intelligence*, 2022.

[20] T. Badings, L. Romao, A. Abate, and N. Jansen, "Probabilities are not enough: Formal controller synthesis for stochastic dynamical models with epistemic uncertainty," *arXiv preprint arXiv:2210.05989*, 2022.

[21] A. Lavaei, S. Soudjani, E. Frazzoli, and M. Zamani, "Constructing MDP abstractions using data with formal guarantees," *IEEE Control Systems Letters*, 2023.

[22] K. Hashimoto, A. Saoud, M. Kishida, T. Ushio, and D. V. Dimarogonas, "Learning-based symbolic abstractions for nonlinear control systems," *Automatica*, 2022.

[23] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambride University Press, 2004.

[24] M. Campi and S. Garatti, "The exact feasibility of randomized solutions of uncertain convex programs," *SIAM Journal on Optimization*, 2008.

[25] D. P. Bertsekas and S. E. Shreve, *Stochastic optimal control: the discrete-time case*. Athena Scientific, 2004.

[26] P. Jagtap, S. Soudjani, and M. Zamani, "Formal Synthesis of Stochastic Systems via Control Barrier Certificates," *IEEE Transactions on Automatic Control*, 2020.

[27] M. C. Campi, S. Garatti, and M. Prandini, "The scenario approach for systems and control design," *Annual Reviews in Control*, 2009.