Automatica 159 (2024) 111323

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Data-driven verification and synthesis of stochastic systems via barrier certificates ☆

Ali Salamati [a,*], Abolfazl Lavaei [b], Sadegh Soudjani [b], Majid Zamani [c,a]

[a] Department of Computer Science, Ludwig-Maximilians-Universität München, Germany
[b] School of Computing, Newcastle University, United Kingdom
[c] Department of Computer Science, University of Colorado Boulder, USA

ARTICLE INFO

Article history:
Received 5 November 2021
Received in revised form 24 July 2023
Accepted 24 August 2023
Available online 7 November 2023

Keywords:
Stochastic systems
Safety specification
Formal synthesis
Data-driven barrier certificate
Robust convex program
Scenario convex program

ABSTRACT

In this work, we study verification and synthesis problems for safety specifications over unknown discrete-time stochastic systems. When a model of the system is available, barrier certificates have been successfully applied for ensuring the satisfaction of safety specifications. In this work, we formulate the computation of barrier certificates as a robust convex program (RCP). Solving the acquired RCP is hard in general because the model of the system that appears in one of the constraints of the RCP is unknown. We propose a data-driven approach that replaces the uncountable number of constraints in the RCP with a finite number of constraints by taking finitely many random samples from the trajectories of the system. We thus replace the original RCP with a scenario convex program (SCP) and show how to relate their optimizers. We guarantee that the solution of the SCP is a solution of the RCP with a priori guaranteed confidence when the number of samples is larger than a specific value. This provides a lower bound on the safety probability of the original unknown system together with a controller in the case of synthesis. We also discuss an extension of our verification approach to a case where the associated robust program is non-convex and show how a similar methodology can be applied. Finally, the applicability of our proposed approach is illustrated through three case studies.

1. Introduction

Ensuring safety and temporal requirements on cyber–physical systems is becoming more important in many applications including self-driving cars, power grids, traffic networks, and integrated medical devices. Complex requirements for such real-life practical systems can be expressed as linear temporal logic formulae (Kesten, Pnueli, & Raviv, 1998). Model-based approaches for satisfying such requirements have been studied extensively in the literature (Baier & Katoen, 2008; Belta, Yordanov, & Gol, 2017; Girard, 2005; Tabuada, 2009). In the setting of formal approaches for stochastic systems, a number of abstraction-based methods has been developed for the verification and synthesis of dynamical systems in order to either verify the desired specifications or synthesize controllers enforcing these systems to satisfy such specifications (Lahijanian, Andersson, & Belta, 2015; Majumdar, Mallik, & Soudjani, 2020; Svoreňová et al., 2017; Zamani, Esfahani, Majumdar, Abate, & Lygeros, 2014). In order to improve scalability of abstraction-based methods, some other techniques such as sequential gridding (Soudjani & Abate, 2013; Soudjani, Gevaerts and Abate, 2015), discretization-free abstraction (Zamani, Tkachev, & Abate, 2017), and compositional abstraction-based techniques (Soudjani, Abate and Majumdar, 2015) have been introduced in the literature in order to efficiently deal with the verification and synthesis problems.

An approach for formal verification and synthesis with respect to safety specifications in dynamical systems is to use a notion of barrier certificates (Prajna & Jadbabaie, 2004). Barrier certificates have been the focus of the recent literature as an abstraction-free technique that is scalable with the dimension of the system, i.e., they do not require construction of an abstraction of the system and can provide directly the controller together with the guarantee on the satisfaction of the safety specification (Borrmann, Wang, Ames, & Egerstedt, 2015; Yang, Wu, & Lin, 2020; Zhang, She, Ratschan, Hermanns, & Hahn, 2010). A barrier-based methodology is introduced by Prajna and Jadbabaie (2004) in order to verify safety in deterministic hybrid systems. Prajna, Jadbabaie, and Pappas (2007) propose a framework for

☆ This work was supported in part by the National Science Foundation (NSF), USA, under grants CNS-2145184, CNS-1952223, and A22-0123-S003, and by the EPSRC-funded CodeCPS project (EP/V043676/1). The material in this paper was partially presented at the 7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS), July 7–9, 2021, Brussels, Belgium. This paper was recommended for publication in revised form by Associate Editor Subhrakanti Dey under the direction of Editor Ian R. Petersen.

* Corresponding author.
E-mail addresses: ali.salamati@lmu.de (A. Salamati), abolfazl.lavaei@newcastle.ac.uk (A. Lavaei), sadegh.soudjani@newcastle.ac.uk (S. Soudjani), majid.zamani@colorado.edu (M. Zamani).

https://doi.org/10.1016/j.automatica.2023.111323
0005-1098/

safety verification of stochastic systems using barrier certificates which is extended to stochastic hybrid systems. Wang, Ames, and Egerstedt (2017) present barrier certificates that ensure collision-free behaviors in multi-robot systems by minimizing the difference between the actual and the nominal controllers subject to safety constraints. Sloth, Pappas, and Wisniewski (2012) propose a compositional analysis for verifying the safety of an interconnection of subsystems using barrier certificates. Jagtap, Soudjani and Zamani (2020) use barrier certificates for the synthesis of controllers against complex requirements expressed as co-safe linear temporal logic formulas.

The common requirement of the approaches mentioned above is the fact that they need a mathematical model of the system. However, a precise model of dynamical systems is either not available in many application scenarios or too complex to be of any use. Therefore, there is a need to develop approaches which are capable of verifying or synthesizing controllers against safety specifications only based on collected data from the system.

Related Literature. Data-driven methods have gained significant attentions recently for formally verifying some desired specifications. Coulson, Lygeros, and Dörfler (2020) introduce A data-enabled predictive control that utilizes noisy data of the system and produces optimal control inputs ensuring the satisfaction of desired chance constraints with high probability. A data-driven model predictive control scheme is proposed by Berberich, Köhler, Muller, and Allgower (2020) which only requires initially measured input–output trajectories together with an upper bound on the dimension of the unknown system. Tabuada and Fraile (2020) develop a methodology in order to make a single-input single-output system stable only based on data. The stability problem of black-box linear switching systems with desired confidences is investigated by Kenanian, Balkan, Jungers, and Tabuada (2019) based on collected data. This approach is extended by Wang and Jungers (2019) by providing a methodology for computing the invariant sets of discrete-time black-box systems. A novel Bayes-adaptive planning algorithm for data-efficient verification of uncertain Markov decision processes is introduced by Wijesuriya and Abate (2019). A framework is proposed by Sadraddini and Belta (2018) to provide a formal guarantee on data-driven model identification and controller synthesis. Salamati, Soudjani, and Zamani (2020) develop a methodology for providing a probabilistic confidence over the verification of signal temporal logic properties for partially unknown stochastic systems based on collected data. Plambeck, Fey, and Schyga (2022) propose a framework to learn a decision tree as a model for a black box continuous system.

The work by Dawson, Qin, Gao, and Fan (2022) develops a method to synthesize robust feedback controllers with safety and stability guarantees. Robey, Lindemann, Tu, and Matni (2021) propose a data-driven approach in order to synthesize controllers for deterministic hybrid systems using barrier certificates while providing a correctness guarantee on the obtained barrier certificate. A data-driven, model-based approach is developed by Abate, Ahmed, Giacobbe, and Peruffo (2020) to provide stability guarantees using Satisfiability Modulo Theories (SMT). Niu, Zhang, and Clark (2021) developed a data-driven technique to synthesize controllers for unknown deterministic systems. The framework developed by Clark (2021) computes barrier certificates for complete- and incomplete-information systems affected by Gaussian process and measurement noises under unbounded inputs. Majumdar, Salamati, and Soudjani (2023) cosidered the memory blow-up problem for data-driven learned abstractions of dynamical systems and proposed a two-step memory efficient method that first trains compact neural reperesentation for the abstraction and then verifies the soundness of the trained representation.

An optimization-based approach is proposed by Robey et al. (2020) to learn a control barrier certificate through safe trajectories under suitable Lipschitz smoothness assumption on the dynamical system. A sub-linear algorithm is developed by Han, Topcu, and Pappas (2015) for the barrier-based data-driven model validation of dynamical systems which computes the barrier function using a large dataset of trajectories. Jagtap, Pappas and Zamani (2020) propose a two-step procedure to synthesize a controller for an unknown nonlinear system, where the first step is to learn a Gaussian process as a replacement of the unknown dynamics, and the second step is to construct the control barrier function for the learned dynamics.

A data-driven optimization called *scenario convex program* (SCP) is introduced by Calafiore and Campi (2006) to solve robust convex optimizations. This approach replaces the infinite number of constraints in the robust optimization with a finite number of constrained by sampling the uncertain variables from their distributions. The approach relates the feasibility of the SCP to that of the robust optimization while providing bounds on the probability of violating the constraints. Kanamori and Takeda (2012) study the same approach and relates worst-case violation of the constraints to the probability of their violation. While Calafiore and Campi (2006) and Kanamori and Takeda (2012) focus on feasibility, Esfahani, Sutter, and Lygeros (2014) establish a quantitative relation between the optimal value of the robust optimization and its associated SCP.

The results by Esfahani et al. (2014) are employed in Nejati, Lavaei, Jagtap, Soudjani, and Zamani (2021) for data-driven verification of dynamical systems using some inequalities characterizing barrier certificates. Our results presented here differ from the ones by Nejati et al. (2021) in three main directions. First, our approach is developed for stochastic dynamical systems subject to random disturbances with unknown distributions, while the other work is restricted to deterministic systems. Second, our approach also tackles controller synthesis problems, while the other work only deals with the verification ones. Last but not least, we study a class of non-convex optimization problems that makes our approach applicable to larger classes of systems, while the result in the other work is restricted to only convex problems.

Contributions. Here, we propose formal verification and synthesis procedures for unknown stochastic systems with respect to safety specifications based on collected data. We first cast a barrier-based safety problem as a robust convex program (RCP). Solving the obtained RCP is hard in general because the unknown model of the system appears in the constraints. To tackle this issue, we resort to a scenario-driven approach by collecting samples from the system. Using the results by Esfahani et al. (2014), we connect the optimal solution of the acquired scenario convex program (SCP) with that of the original RCP. We provide a lower bound on the safety probability of the unknown stochastic system using a certain number of data which is related to the desired confidence. We extend this result to provide a new confidence bound for a class of non-convex barrier-based safety problems. We conclude the paper by three case studies to illustrate the applicability of our approach.

Outline. The structure of this paper is as follows. Section 2 gives the system definition and the problem statement, and presents the safety verification of stochastic systems using barrier certificates. In Section 3, we introduce the scenario convex program for the barrier-based safety problem and we connect its optimizer to that of the original optimization. Our approach for the safety verification of the unknown stochastic system is presented in Section 4. In Section 5, we explain our data-driven synthesis approach which enforces the safety specification with a certain confidence. An extension of the verification problem for a class of non-convex safety problems is discussed in Section 6. To illustrate the effectiveness of our approach, three case studies are presented in Section 7. Finally, Section 8 concludes the paper.

2. Preliminaries and problem statement

2.1. Notations and preliminaries

The set of positive integers, non-negative integers, real numbers, non-negative real numbers, and positive real numbers are denoted by $\mathbb{N} := \{1, 2, 3, \ldots\}$, $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$, $\mathbb{R}$, $\mathbb{R}_0^+$, and $\mathbb{R}^+$, respectively. We denote the indicator function of a set $\mathscr{A} \subseteq X$ by $\mathbb{1}_{\mathscr{A}} : X \to \{0, 1\}$, where $\mathbb{1}_{\mathscr{A}}(x)$ is 1 if $x \in \mathscr{A}$, and 0 otherwise. Notation $\mathbf{1}_m$ is used to indicate a column vector of ones in $\mathbb{R}^{m\times 1}$. We denote by $\|x\|$ the Euclidean norm of any $x \in \mathbb{R}^n$. We also denote the induced norm of any matrix $A \in \mathbb{R}^{m\times n}$ by $\|A\| = \sup_{x\neq 0} \|Ax\|/\|x\|$. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}$, and $i \in \{1, \ldots, N\}$, we use $[x_1; \ldots; x_N]$ and $[x_1, \ldots, x_N]$ to denote the corresponding column and row vectors, respectively, with dimension $\sum_i n_i$. The absolute value of a real number x is denoted by $|x|$. For a function $f : X \to Y$, we denote its inverse by $f^{-1} : Y \to X$, whenever exists. A regularized incomplete beta function for parameters $(z; a, b)$ is defined as $\mathrm{I}(z; a, b) = \frac{\int_0^z u^{a-1}(1-u)^{b-1}du}{\int_0^1 u^{a-1}(1-u)^{b-1}du}$. If a system, denoted by $\mathcal{S}$, satisfies a property Ψ during a time horizon $\mathcal{H}$, it is denoted by $\mathcal{S} \models_{\mathcal{H}} \Psi$. We also use $\models$ in this paper to show the feasibility of a solution for an optimization problem.

The sample space of random variables is denoted by Ω. The Borel σ-algebras on a set X is denoted by $\mathfrak{B}(X)$. The measurable space on X is denoted by $(X, \mathfrak{B}(X))$. We have two probability spaces in this work. The first one is represented by $(X, \mathfrak{B}(X), \mathbb{P})$ which is the probability space defined over the state set X with $\mathbb{P}$ as a probability measure. The second one, $(V_w, \mathfrak{B}(V_w), \mathbb{P}_w)$, defines the probability space over V_w for the random variable w affecting the stochastic system with $\mathbb{P}_w$ as its probability measure. With a slight abuse of the notation, we use the same $\mathbb{P}$ and $\mathbb{P}_w$ when the product measures are needed in the formulations. Considering a random variable z, $\mathrm{Var}(z) := \mathbb{E}(z^2) - (\mathbb{E}(z))^2$ denotes its variance with $\mathbb{E}$ being the expectation operator.

2.2. System definition

In this work, we first deal with (potentially) unknown discrete-time continuous-space stochastic dynamical systems as formalized next.

Definition 2.1. A discrete-time stochastic system (dt-SS) is a tuple $\mathcal{S} = (X, V_w, w, f)$, where the Borel set $X \subset \mathbb{R}^n$ is the state set of the system, the Borel set V_w is the uncertainty space, $w := \{w(t) : \Omega \to V_w, t \in \mathbb{N}_0\}$ is a sequence of independent and identically distributed (i.i.d.) random variables on the Borel space V_w with some distribution $\mathbb{P}_w$, and the map $f : X \times V_w \to X$ is a measurable function that characterizes the state evolution of the system. The state trajectory of the system is constructed according to

$$\mathcal{S} : x(t+1) = f(x(t), w(t)), \quad t \in \mathbb{N}_0. \tag{2.1}$$

We denote a finite trajectory of the system by $\xi(t) := x(0)x(1)\ldots x(t)$, $t \in \mathbb{N}_0$.

In this work, we assume that the map f and the distribution of the uncertainty $\mathbb{P}_w$ are unknown. Instead, we assume we can collect N *independent* and *identically distributed* state pairs (x_i, x_i^+) by initializing the system at x_i and observing its next state as $x_i^+ = f(x_i, w_i)$ for some random sample w_i. The collected dataset is denoted by

$$\mathcal{D} := \left\{(x_i, x_i^+)\right\} \subset X^2, \quad i \in \{1, \ldots, N\}. \tag{2.2}$$

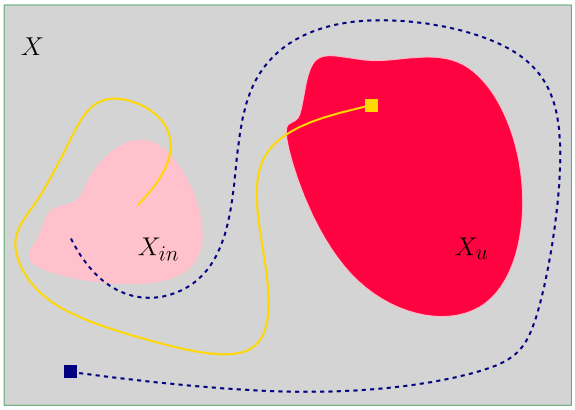

Fig. 1. A set X containing initial and unsafe sets X_{in} and X_u. The (blue) dashed line illustrates a safe trajectory of the system, whereas the yellow one demonstrates an unsafe trajectory. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

2.3. Problem statement

Definition 2.2. Given a set of initial states $X_{in} \subset X$, a set of unsafe states $X_u \subset X$, and a finite time horizon $\mathcal{H} \in \mathbb{N}_0$, the system $\mathcal{S}$ is called safe if all trajectories of $\mathcal{S}$ that start from X_{in} never reach X_u within horizon $\mathcal{H}$. We denote this safety property by Ψ and its satisfaction by $\mathcal{S}$ is written as $\mathcal{S} \models_{\mathcal{H}} \Psi$. A state set X containing the initial and unsafe sets is illustrated in Fig. 1.

Since the system is stochastic and we do not know the distribution of w and the map f, we are interested in establishing a lower bound on the probability that the safety property Ψ is satisfied by the trajectories of $\mathcal{S}$ while using only a dataset of the form (2.2). Now, we state the main problem we are interested to solve here.

Problem 2.3. Consider an unknown dt-SS $\mathcal{S}$ as in Definition 2.1. Provide a lower bound $(1-\rho) \in [0, 1]$ on the probability of satisfying Ψ, *i.e.*, $\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1-\rho$, together with a confidence $(1-\beta) \in [0, 1]$ using only a dataset $\mathcal{D}$ of the form (2.2). Moreover, establish a connection between the required size of dataset $\mathcal{D}$ and the desired confidence $1-\beta$.

Therefore, we are interested in finding a potentially tight lower bound. The confidence $1-\beta$ in the statement of the problem is with respect to the probability distribution of the dataset $\mathcal{D}$ and is seen from the frequentist interpretation of probability: any algorithm that solves this problem collects dataset $\mathcal{D}$ using a probability distribution; while running the algorithm multiple times with different datasets $\mathcal{D}$, the algorithm gives wrong results (incorrect lower bound on the safety probability) in at most β portion of the algorithm runs.

Fig. 2 shows an overview of our approach. The block on the left represents a stochastic safety problem. The RCP block reformulates the safety problem as a robust optimization problem. Blocks SCP_N and $\mathrm{SCP}_{N,\hat{N}}$ solve the optimization problem introduced by the RCP block using finite number of samples. Finally, Theorem 4.4 connects SCP's solutions to the original safety problem.

2.4. Safety verification via barrier certificates

Definition 2.4. Given a dt-SS $\mathcal{S} = (X, V_w, w, f)$, a nonnegative function $\mathrm{B} : X \to \mathbb{R}_0^+$ is called a barrier certificate (BC) for $\mathcal{S}$ if there exist constants $\lambda > 1$ and $c \in \mathbb{R}_0^+$ such that

$$\mathrm{B}(x) \leq 1, \qquad \forall x \in X_{in}, \tag{2.3}$$

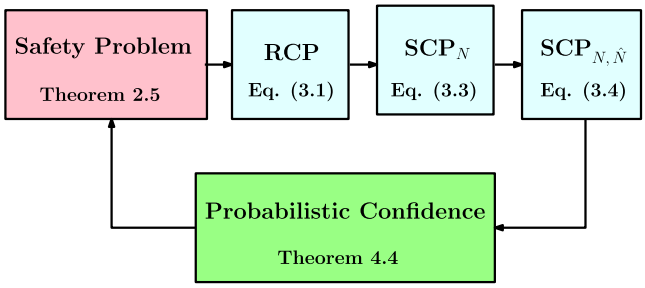

Fig. 2. This figure shows an overview of the proposed scenario approach for verification of the safety specification.

$$\mathrm{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{2.4}$$

$$\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \mathrm{B}(x) + c, \qquad \forall x \in X, \tag{2.5}$$

where $X_{in} \subset X$ and $X_u \subset X$ are initial and unsafe sets corresponding to a given safety specification Ψ, respectively.

Next theorem, borrowed from Jagtap, Soudjani et al. (2020), provides a lower bound on the probability of satisfaction of the safety specification for a dt-SS.

Theorem 2.5. *Consider a dt-SS $\mathcal{S}$ and a safety specification Ψ. Assume there exists a non-negative barrier certificate $\mathrm{B}(x)$ which satisfies conditions (2.3)–(2.5) with constants λ and c. Then*

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \frac{1 + c\ \mathcal{H}}{\lambda}, \tag{2.6}$$

with $\mathcal{H} \in \mathbb{N}_0$ being the finite time horizon associated with Ψ.

In this work, we consider polynomial-type barrier certificates denoted by $\mathrm{B}(b,x)$, where b is the vector containing the coefficients of the polynomial. Such a polynomial with degree $k \in \mathbb{N}_0$ has the form

$$\mathrm{B}(b,x) = \sum_{\iota_1=0}^{k} \dots \sum_{\iota_n=0}^{k} b_{\iota_1,\dots,\iota_n} (x_1^{\iota_1} \dots x_n^{\iota_n}), \tag{2.7}$$

with $b_{\iota_1,\dots,\iota_n} = 0$ for $\iota_1 + \dots + \iota_n > k$. Hence, finding a polynomial barrier certificate reduces to determining the coefficients of the polynomial, namely $b_{\iota_1,\dots,\iota_n}$. In the next section, we provide our data-driven approach for the construction of polynomial-type barrier certificates.

3. Data-driven safety verification

We first cast the barrier-based safety problem in Theorem 2.5 as a robust convex programming (RCP). We then provide a scenario-based approach in order to solve the obtained RCP using data collected from the system.

Satisfying the conditions of Theorem 2.5 is equivalent to having a non-positive value for the optimal solution of the following RCP (i.e., $\mathcal{K} \leq 0$):

$$\text{RCP}: \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max\limits_{z} \big(g_z(x,d)\big) \leq 0, z \in \{1,\dots,5\}, \forall x \in X, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1,\dots,\iota_n}], \\ & \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{3.1}$$

in which,

$$g_1(x,d) = -\mathrm{B}(b,x) - \mathcal{K},$$
$$g_2(x,d) = (\mathrm{B}(b,x) - 1 - \mathcal{K})\mathbb{1}_{X_{in}}(x),$$
$$g_3(x,d) = (-\mathrm{B}(b,x) + \lambda - \mathcal{K})\mathbb{1}_{X_u}(x),$$
$$g_4(x,d) = \frac{1 + c\ \mathcal{H}}{\rho} - \lambda - \mathcal{K},$$
$$g_5(x,d) = \mathbb{E}\Big[\mathrm{B}(b,f(x,w)) \mid x\Big] - \mathrm{B}(b,x) - c - \mathcal{K}, \tag{3.2}$$

where $(1-\rho)$ is a given lower bound for the safety probability.

Remark 3.1. The RCP (3.1) is in fact a robust convex optimization. It is a convex optimization since the constraints are convex with respect to decision variables in d and objective function. It is a robust optimization since the constraints have to hold for all $x \in X$.

Remark 3.2. The RCP (3.1) always has a feasible solution. For instance, by choosing coefficients of $\mathrm{B}(b,x)$ equal to zero, $\lambda = 2$, $c = 0$, and $\mathcal{K} \geq \frac{1}{\rho} - 2$, we get a feasible solution for the RCP. Moreover, the barrier certificate obtained from this RCP satisfies conditions (2.3)–(2.5) as long as $\mathcal{K} \leq 0$.

Finding an optimal solution for the RCP in (3.1) is hard in general because the map f is unknown, the probability measure $\mathbb{P}_w$ is also unknown (thus the expectation in g_5 cannot be computed analytically), and there are infinitely many constraints in the robust optimization since $x \in X$, where X is a continuous set. To tackle this, we first assign a probability distribution to the state set, take N i.i.d. samples $\{x_1, x_2, \dots, x_N\}$ from this distribution, and replace the robust quantifier $\forall x \in X$ with $\forall x_i \in X$, $i \in \{1,2,\dots,N\}$. This results in the following scenario convex program denoted by SCP$_N$:

$$\text{SCP}_N: \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max\limits_{z} g_z(x_i,d) \leq 0,\ \ \forall i \in \{1,\dots,N\}, \\ & \quad z \in \{1,\dots,5\}, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1,\dots,\iota_n}], \\ & \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0. \end{cases} \tag{3.3}$$

To tackle the issue of unknown $\mathbb{P}_w$, we replace the expectation in g_5 with its empirical approximation by sampling $\hat{N}$ i.i.d. values w_j, $j \in \{1,\dots,\hat{N}\}$, from $\mathbb{P}_w$ for each x_i, which gives the following scenario convex program denoted by SCP$_{N,\hat{N}}$:

$$\text{SCP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max\limits_{z} \bar{g}_z(x_i,d) \leq 0,\ \ \forall i \in \{1,\dots,N\}, \\ & \quad z \in \{1,\dots,5\}, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1,\dots,\iota_n}], \\ & \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0, \end{cases} \tag{3.4}$$

where $\bar{g}_z := g_z$ for all $z \in \{1,2,3,4\}$ and

$$\bar{g}_5(x_i,d) := \frac{1}{\hat{N}} \sum_{j=1}^{\hat{N}} \mathrm{B}(b,f(x_i,w_j)) - \mathrm{B}(b,x_i) - c + \delta - \mathcal{K}. \tag{3.5}$$

In SCP$_{N,\hat{N}}$, $f(x_i,w_j)$ is the next state of the system from the current state x_i with the noise realization w_j. Therefore, the solution of the SCP$_{N,\hat{N}}$ can be obtained using only the dataset $\mathcal{D}$ without the knowledge of f and $\mathbb{P}_w$. The optimal value for the objective function of SCP$_{N,\hat{N}}$ is denoted by $\mathcal{K}^*(\mathcal{D})$. We also denote by $\hat{\mathrm{B}}(b,x \mid \mathcal{D})$ the barrier function constructed based on the solution of SCP$_{N,\hat{N}}$ in (3.4).

Note that $\bar{g}_5(x_i,d)$ in (3.5) has an additional parameter $\delta > 0$ compared to g_5. This parameter is added to make the last inequality more conservative in order to capture the error coming from replacing the expectation with the empirical mean. We use Chebyshev's inequality (Hernández, 2001) to quantify such an

error with the associated confidence. Let us define the variance of the empirical approximation as

$$\sigma^2 := \mathrm{Var}\Big(\frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x, w_j))\Big), \tag{3.6}$$

where the variance is taken with respect to w_j. We assume that there is a bound $\hat{M}$ such that

$$\mathrm{Var}\big(\mathrm{B}(b, f(x, w))\big) \leq \hat{M}, \quad \forall x \in X. \tag{3.7}$$

This assumption gives us a bound for σ^2 in (3.6) as $\sigma^2 \leq \frac{\hat{M}}{\hat{N}}$ due to w_j being independent. The idea of replacing the expectation by the empirical mean in an optimization problem and relating the associated solutions based on Chebyshev's inequality is also used by Soudjani and Majumdar (2018). Next theorem shows that the barrier certificate computed using the optimal solution of the $\mathrm{SCP}_{N,\hat{N}}$ is a feasible barrier certificate for SCP_N in (3.3) with a certain confidence.

Theorem 3.3. *Let $\hat{\mathrm{B}}(b, x \mid \mathcal{D})$ be a feasible solution of the $\mathrm{SCP}_{N,\hat{N}}$ for some $\delta > 0$, and assume the inequality (3.7) holds with a given $\hat{M}$. Then for any $\beta_s \in (0, 1]$, we get*

$$\mathbb{P}_w\Big(\hat{\mathrm{B}}(b, x \mid \mathcal{D}) \models \mathrm{SCP}_N\Big) \geq 1 - \beta_s, \tag{3.8}$$

provided that the number of samples in the empirical mean satisfies $\hat{N} \geq \frac{\hat{M}}{\delta^2 \beta_s}$.

Proof. By the statement of the theorem, we have $\hat{\mathrm{B}}(b, x \mid \mathcal{D}) \models \mathrm{SCP}_{N,\hat{N}}$. The difference between the empirical mean in (3.5) and the expected value in (3.3) can be quantified by invoking the Chebyshev's inequality as:

$$\mathbb{P}_w\Big(|\mathbb{E}\big[\mathrm{B}(b, f(x, w)) \mid x\big] - \frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b, f(x, w_j))| \leq \delta\Big) \geq 1 - \frac{\sigma^2}{\delta^2}, \tag{3.9}$$

where $\delta \in \mathbb{R}^+$, and σ^2 is defined in (3.6) (Hernández, 2001). Since all the first four feasibility conditions are the same as in (3.3) and (3.4), $\hat{\mathrm{B}}(b, x \mid \mathcal{D})$ is a feasible solution for those conditions of SCP_N with probability one. The only remaining concern is the last feasibility condition. According to (3.9), one can deduce that $\hat{\mathrm{B}}(b, x \mid \mathcal{D})$ is a feasible solution for SCP_N with a confidence of at least $1 - \frac{\sigma^2}{\delta^2}$. Furthermore, we have $\sigma^2 \leq \frac{\hat{M}}{\hat{N}}$ by having $\mathrm{Var}(\mathrm{B}(b, f(x, w))) \leq \hat{M}$, and hence

$$\mathbb{P}_w\big(\hat{\mathrm{B}}(b, x \mid \mathcal{D}) \models \mathrm{SCP}_N\big) \geq 1 - \frac{\hat{M}}{\delta^2 \hat{N}}.$$

By the above inequality, we get $\beta_s \geq \frac{\hat{M}}{\delta^2 \hat{N}}$ and consequently $\hat{N} \geq \frac{\hat{M}}{\delta^2 \beta_s}$. This completes the proof. □

Remark 3.4. When the system has additive noise, *i.e.,*

$$x(t+1) = f_a(x(t)) + w(t),$$

the condition (3.7) can be established by having a bound on $f_a(\cdot)$ and bounds on moments of the noise w. For instance, in the case of one-dimensional systems (i.e., $n = 1$), we have $\mathrm{B}(b, x) = \sum_{\iota=0}^{k} b_\iota x^\iota$ and the variance of $\mathrm{B}(\cdot)$ can be expanded as follows:

$$\begin{aligned}
&Var(\mathrm{B}(b, f(x, w))) = Var\Big(\sum_{\iota=0}^{k} b_\iota f(x, w)^\iota\Big) \\
&= Var\Big(\sum_{\iota=0}^{k} b_\iota (f_a(x) + w)^\iota\Big) = Var\Big(\sum_{\iota}^{k}\sum_{j=0}^{\iota} b_\iota \binom{\iota}{j} f_a(x)^{\iota-j} w^j\Big) \\
&= Var\Big(\sum_{j=1}^{k} g_j(x) w^j\Big) \ with\ g_j(x) := \sum_{\iota=j}^{k} b_\iota \binom{\iota}{j} f_a(x)^{\iota-j} \\
&= \sum_{j=1}^{k}\sum_{z=1}^{k} g_j(x) g_z(x)(\mathbb{E}[w^{j+z}] - \mathbb{E}[w^j]\mathbb{E}[w^z]).
\end{aligned}$$

This means the variance can be bounded using upper bounds of $f_a(\cdot)$ and moments of w.

As it can be seen from Theorem 3.3, higher number of samples $\hat{N}$ is needed in order to have a smaller empirical approximation error δ, and to provide a better confidence bound. In fact, $\hat{N}$ and δ are required to solve the $\mathrm{SCP}_{N,\hat{N}}$ in (3.4). Later in the next section, we show how the value of β_s affects the total confidence concerning the safety of the stochastic system.

Remark 3.5. Note that our results presented in this paper are valid for any choice of the probability distribution $\mathbb{P}$ with its support being the state set X that satisfies a regularity assumption formulated in the next section (cf. Assumption 4.2). This assumption holds for a wide range of distributions including uniform, truncated normal, and exponential distributions. From the algorithmic perspective, this distribution affects the collected data points x_i and the optimal solution of the SCP_N. The confidence formulated in our paper is also with respect to this distribution. We choose $\mathbb{P}$ to be a uniform distribution in the case study section.

4. Safety guarantee over unknown stochastic systems

In the previous section, we established the connection between the two optimizations SCP_N and $\mathrm{SCP}_{N,\hat{N}}$, and showed that the solution of $\mathrm{SCP}_{N,\hat{N}}$ is a feasible solution for SCP_N with a certain confidence if the number of samples $\hat{N}$ is chosen appropriately (cf. Theorem 3.3). In this section, we focus on the relation between the original RCP and the SCP_N utilizing the fundamental result by Esfahani et al. (2014) and provide an end-to-end safety guarantee over the unknown stochastic system with a priori guaranteed confidence. To do so, we need to raise the following regularity assumptions on the functions and the chosen probability measure $\mathbb{P}$.

Assumption 4.1. Functions g_1, g_2, g_3, and g_5 are all Lipschitz continuous with respect to x with Lipschitz constants L_{x_1}, L_{x_2}, L_{x_3}, and L_{x_5}, respectively. Therefore, the Lipschitz constant $\mathrm{L}_x := \mathrm{L}_{x_1} + \mathrm{L}_{x_2} + \mathrm{L}_{x_3} + \mathrm{L}_{x_5}$ is a Lipschitz constant for $\max_z g_z(x, d), z \in \{1, \ldots, 5\} \setminus \{4\}$. In addition, if g_1, g_2, g_3, and g_5 are analytic over a compact domain X, the Lipschitz constant of $\max_z g_z(x, d)$ is $\mathrm{L}_x := \max\{\mathrm{L}_{x_1}, \mathrm{L}_{x_2}, \mathrm{L}_{x_3}, \mathrm{L}_{x_5}\}$.

Assumption 4.2. There is a strictly increasing function $G : \mathbb{R}_0^+ \to [0, 1]$, where $G(0) = 0$ such that

$$\mathbb{P}[\mathrm{b}(x, r)] \geq G(r) \qquad \forall x \in X, \tag{4.1}$$

where $\mathrm{b}(x, r) \subset X$ is an open ball centered at point x with radius r.

Note that any probability distribution, for which the above lower bound function $G(r)$ can be computed, can be used in our approach for sampling.

Remark 4.3. The probability distribution from which x_i is sampled must satisfy Assumption 4.2. This assumption requires having a strictly increasing function $G : \mathbb{R}_0^+ \to [0, 1]$ that satisfies

$$\mathbb{P}[\mathrm{b}(x, r)] \geq G(r), \qquad \forall x \in X.$$

Then, the probability distribution $\mathbb{P}$ should assign positive probability to any ball with positive radius. This means no ball $\mathrm{b}(x, r) \subset X$ could be excluded from sampling in the approach with some non-trivial probability.

Next, we introduce the main result which connects the safety of an unknown stochastic system directly to data collected from the system.

Theorem 4.4. *Consider an unknown dt-SS, as in (2.1), and safety specification Ψ. Let Assumptions 4.1 and 4.2 hold with Lipschitz constant L_x and function $G(r)$, respectively. Assume $\hat{N}$ is selected for the $\mathrm{SCP}_{N,\hat{N}}$ as in Theorem 3.3 in order to provide confidence $1 - \beta_s$. Denote by $\mathcal{K}^*(\mathcal{D})$ the optimal value of the optimization problem in (3.4) using N samples and parameter $\rho \in (0, 1]$. For any $\beta \in [0, 1]$, the following statement holds with a confidence of at least $(1 - 3\beta - \beta_s)$:*

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho,$$

if

$$\mathcal{K}^*(\mathcal{D}) + L_x\, G^{-1}(\epsilon) \leq 0, \tag{4.2}$$

where function G defined in (4.1), and $\epsilon = I^{-1}(1 - \beta; \mathcal{Q} + 3, N - \mathcal{Q} - 2)$.

Proof. Denote the optimal values of the RCP and the SCP_N by $\mathcal{K}^*$ and $\mathcal{K}^*_{\mathrm{m}}(\mathcal{D})$, respectively. According to Esfahani et al. (2014, Theorem 3.6), one has

$$\mathbb{P}\big(\mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) \leq \mathcal{K}^* \leq \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) + \mathrm{L}_{sp} H(\epsilon)\big) \geq 1 - \beta,$$

for a chosen ϵ and any $N \geq N(\epsilon, \beta)$ as in Esfahani et al. (2014, Theorem 2.2). Equivalently, the above inequality holds for a given N and $\epsilon \leq \mathrm{I}^{-1}(1 - \beta; \mathrm{d}, N - \mathrm{d} + 1)$. In this expression, d is the number of decision variables, and $H(\cdot)$ is a uniform level-set bound as defied in Esfahani et al. (2014, Definition 3.1). Constant L_{sp} is a Slater constant as defined in Esfahani et al. (2014, equation (5)). Since the original RCP in (3.1) is a min–max optimization problem, the constant L_{sp} can be selected as one according to Esfahani et al. (2014, Remark 3.5). By choosing $\mathrm{d} := \mathcal{Q} + 3$, one obtains the parameters of the incomplete beta function in the theorem statement. Based on Esfahani et al. (2014, Proposition 3.8), $H(\epsilon) = \mathrm{L}_x G^{-1}(\epsilon)$, where L_x is the Lipschitz constant of RCP as in Assumption 4.1, and $G(\cdot)$ as in (4.1). Now, one can readily deduce that

$$\mathbb{P}\big(\mathcal{K}^* \leq \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\big) \geq 1 - 3\beta. \tag{4.3}$$

Confidence β is multiplied by 3 since the Lipschitz continuity is needed in (3.1) in three different regions and, hence, we leverage the results by Murali, Trivedi, and Zamani (2022) to deal with this issue by multiplying β by three. On the other hand, due to the particular selection of $\hat{N}$ and β_s according to Theorem 3.3, we know that (3.8) holds. Therefore,

$$\mathbb{P}\left(\mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\right) \geq 1 - \beta_s. \tag{4.4}$$

Define the events $\mathcal{A} := \{\mathcal{D} \mid \mathcal{K}^* \leq \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\}$, $\mathcal{B} := \{\mathcal{D} \mid \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\}$, and $\mathcal{C} := \{\mathcal{D} \mid \mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq 0\}$, where $\mathbb{P}(\mathcal{A}) \geq 1 - 3\beta$ and $\mathbb{P}(\mathcal{B}) \geq 1 - \beta_s$. The inequalities in $\mathcal{A}$ and $\mathcal{B}$ satisfy

$$\mathcal{K}^* \leq \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq \mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon). \tag{4.5}$$

Note that any element $\mathcal{D}$ that belongs to $\mathcal{C}$ will make the right-hand side of (4.5) non-positive. In addition, if this element also belongs to $\mathcal{A} \cap \mathcal{B}$, the two inequalities in (4.5) will also hold, and we get $\mathcal{K}^* \leq 0$.

$$\mathbb{P}(\mathcal{K}^* \leq 0) \geq \mathbb{P}(\mathcal{A} \cap \mathcal{B}) \geq 1 - \mathbb{P}(\mathcal{A}^c) - \mathbb{P}(\mathcal{B}^c) \geq 1 - 3\beta - \beta_s.$$

This completes the proof since non-positiveness of $\mathcal{K}^*$ ensures a safety lower bound $(1 - \rho)$ with confidence of at least $1 - 3\beta - \beta_s$. □

Corollary 4.5. *If samples are collected uniformly from a hyper rectangular state set with edges of length $\eta_x(i)$ in each dimension i, then one can compute $G(\epsilon)$ as $\frac{a\epsilon^n}{\prod_{i=1}^n \eta_x(i)}$, where $a = \frac{1}{2^n} \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}$ with the Gamma function defined as $\Gamma(k) = 1 \times 2 \times 3 \ldots \times (k-1)$ and $\Gamma(k + \frac{1}{2}) = \frac{1}{2} \times \frac{3}{2} \times \cdots (k - \frac{3}{2})(k - \frac{1}{2})\pi^{\frac{1}{2}}$ for all positive integers.*

Corollary 4.6. *If the state set is an n-dimensional hypersphere with radius $\tilde{r}$ and the data is sampled uniformly, then one has*

$$G(\epsilon) = \frac{1}{2}\Big[I(1 - \frac{c_1^2}{\tilde{r}^2}; \frac{n+1}{2}, \frac{1}{2}) + \frac{\epsilon^n}{\tilde{r}^n} I(1 - \frac{c_2^2}{\epsilon^2}; \frac{n+1}{2}, \frac{1}{2})\Big],$$

where $c_1 = \frac{2\tilde{r}^2 - \epsilon^2}{2\tilde{r}}$, and $c_2 = \frac{\epsilon^2}{2\tilde{r}}$.

Remark 4.7. For uniform sampling, the function $G(r)$ is proportional to r^n. Therefore, the sample complexity of the proposed approach is in the order of $(\frac{v \mathrm{L}_x}{\epsilon})^n$, where v is the volume of state set and n is the dimension of the state set.

Remark 4.8. The barrier function constructed based on the finite number of samples according to the above theorem together with the obtained parameters c and λ satisfies the conditions (2.3)–(2.5) in Definition 2.4 with a confidence of at least $1 - 3\beta - \beta_s$.

Remark 4.9. Note that the constraint g_4 in (3.1) enforces the constraint $\mathbb{P}(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1 - \rho$ for a given ρ. When ρ is not fixed, one can eliminate this constraint from the optimization and guarantee directly the following inequality

$$\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1 - \frac{1 + c^* \mathcal{H}^*}{\lambda},$$

where c^* and λ^* are the optimal values of the $\mathrm{SCP}_{N,\hat{N}}$. This increases the likelihood of getting a feasible optimization and gives the best possible lower bound on the safety probability.

For the sake of clarity, we present the steps required for applying Theorem 4.4 in Algorithm 1.

Both Theorem 4.4 and Algorithm 1 require knowing an upper bound for Lipschitz constant L_x. The following lemma shows how to get this constant for quadratic barrier certificates and systems with additive noises. A similar reasoning can be used for other polynomial-type barrier certificates by casting them as quadratic functions of monomials.

Lemma 4.10. *Consider a nonlinear system with additive noise*

$$x(t + 1) = f_a(x(t)) + w(t), \quad t \in \mathbb{N}_0, \tag{4.6}$$

and a bounded state set X such that $\|x\| \leq \mathcal{L}$ for all $x \in X$. Without loss of generality, we assume that the mean of noise is zero. Let $\|f_a(x)\| \leq L_1\|x\| + L_2$ and $\|\boldsymbol{J}_x\| \leq \hat{L}$ for some $L_1, L_2, \hat{L} \geq 0, \forall x \in X$, where $\boldsymbol{J}_x$ is the Jacobian matrix of $f_a(x)$. Given a quadratic barrier function $x^T P x$ with a symmetric positive definite matrix P, the Lipschitz constant L_x can be upper-bounded by

$$2\|P\|(L_1 \mathcal{L} \hat{L} + L_2 \hat{L} + \mathcal{L}).$$

Algorithm 1: Safety verification of an unknown dt-SS $\mathcal{S} = (X, V_w, w, f)$ using collected data.

Input: Confidence parameters $\beta \in [0, 1]$ and $\beta_s \in [0, 1)$, parameters $\rho \in (0, 1]$, $\delta \in \mathbb{R}^+$, $\hat{M} \in \mathbb{R}^+$, $L_x \in \mathbb{R}^+$, and the degree of barrier certificate $\mathcal{Q}$

1: Compute the number of samples $\hat{N} \geq \hat{M}/(\delta^2\beta_s)$ to be used for the empirical average (Theorem 3.3)

2: Choose the number of samples N

3: Compute $\epsilon = I^{-1}(1-\beta; \mathcal{Q}+3, N-\mathcal{Q}-2)$

4: Select a probability measure $\mathbb{P}$ for the state set X

5: Collect $N\hat{N}$ state pairs from the system

$$\mathcal{D} = \{(x_i, x_{ij}^+) \in X^2,\ x_{ij}^+ = f(x_i, w_{ij})\}_{i,j}$$

6: Solve $SCP_{N,\hat{N}}$ in (3.4) with $\mathcal{D}$ and obtain the optimal solution $\mathcal{K}^*(\mathcal{D})$

Output: If $\mathcal{K}^*(\mathcal{D}) + L_x G^{-1}(\epsilon) \leq 0$, then $\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1 - \rho$ with a confidence of at least $1 - 3\beta - \beta_s$.

Proof. We first compute the Lipschitz constant of g_5 in (2.5) as

$$L_{x_5} = \max\left\{\left\|\frac{\partial g_5(x)}{\partial x}\right\|,\ x \in X,\ \|x\| \leq \mathcal{L}\right\},$$

where

$$\begin{aligned} g_5(x) =& \mathbb{E}\big[(f^T(x(t)) + w^T(t))P(f(x(t)) + w(t))\big] \\ & - x^T(t)Px(t) - c \\ =& f^T(x(t))Pf(x(t)) - x^T(t)Px(t) + \mathbb{E}\big[w^T(t)Pw(t)\big] - c. \end{aligned}$$

By considering $\mathbf{J}_x = [\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}]$, one has

$$\begin{aligned} L_{x_5} &= \max_x \|2(f(x(t))^T P\, \mathbf{J}_x - x^T(t)P)\| \\ &\leq \max_x\ 2\|f(x(t))^T\|\|P\|\|\mathbf{J}_x\| + 2\|x^T(t)\|\|P\| \\ &\leq 2(L_1\mathcal{L} + L_2)\|P\|\hat{L} + 2\mathcal{L}\|P\| \\ &= 2\|P\|(L_1\mathcal{L}\hat{L} + L_2\hat{L} + \mathcal{L}). \end{aligned}$$

Similarly, one can readily deduce that $L_{x_1} = L_{x_2} = L_{x_3} = 2\mathcal{L}\|P\|$, and $L_{x_4} = 0$. Then $L_x = \max(L_{x_1}, L_{x_2}, L_{x_3}, L_{x_4}, L_{x_5}) = 2\|P\|(L_1\mathcal{L}\hat{L} + L_2\hat{L} + \mathcal{L})$, which completes the proof. □

Remark 4.11. Note that according to the above lemma, computing the upper bound for Lipschitz constant L_x depends on $\|P\|$. On the other hand, computing the entries of P depends on Lipschitz constant L_x. In order to tackle this circulatory issue, we consider an upper bound for $\|P\|$ and enforce it as an additional constraint while solving the SCP in (3.4). If there is no solution with the selected upper bound, we iteratively increase the upper bound until we find a solution or a predefined maximum number of iterations is reached.

Remark 4.12. If the underlying dynamics is affine in the form of $x(t+1) = Ax(t) + B + w(t)$ with $A \in \mathbb{R}^{n\times n}$ and $B \in \mathbb{R}^{n\times 1}$, we can set $L_1 = \hat{L}$ as an upper bound on $\|A\|$ and L_2 as an upper bound on $\|B\|$.

Remark 4.13. The Lipschitz constant in Assumption 4.1 can also be estimated directly from the data using Extreme Value Theory with the estimation approach described in the work by Wood and Zhang (1996). For instance, to estimate the Lipschitz constant of g_5 in (3.2), we gather data $\left\{(x_{i1}, x_{i2}) \mid i_1, i_2 = 1, \ldots, \tilde{N}\right\}$ and compute

$$\hat{L} = \max \frac{\|g_5(x_{i_1}) - g_5(x_{i_2})\|}{\|x_{i_1} - x_{i_2}\|}, \qquad i_1, i_2 \in \{1, \ldots, \tilde{N}\}. \tag{4.7}$$

The Lipschitz constant of g_5 is computed by fitting a Reverse Weibull distribution to the samples of the random variable $\hat{L}$, and then computing the location parameter of that distribution.

5. Data-driven controller synthesis

In this section, we study the problem of synthesizing a controller for an unknown stochastic control system using data to satisfy safety specifications. Our approach is to use *control barrier certificates*, fix a parameterized set of controllers, and design the parameters using an SCP. The stochastic control system is defined next.

Definition 5.1. A discrete-time stochastic control system (dt-SCS) is a tuple $\mathcal{S} = (X, U, V_w, w, f)$, where X, V_w, w are as in Definition 2.1, $U \subset \mathbb{R}^m$ is the input set, and $f : X \times U \times V_w \to X$ is the state transition map. The evolution of the state is according to equation

$$\mathcal{S} : x(t+1) = f(x(t), u(t), w(t)),\ t \in \mathbb{N}_0. \tag{5.1}$$

We assume that the map f and distribution of w is unknown but we can gather data (x_i, u_i, x_i^+) by initializing the system at x_i, applying the input u_i, and observing the next state of the system $x_i^+ = x_i(t+1)$. The collected dataset is

$$\mathcal{D} := \left\{(x_i, u_i, f(x_i, u_i, w_j))\right\}_{i,j} \subset X \times U \times X. \tag{5.2}$$

Now, we state the main problem we are interested to solve here.

Problem 5.2. Consider an unknown dt-SCS $\mathcal{S}$ as in Definition 5.1, with a safety specification Ψ specified by the initial set X_{in}, unsafe set X_u, and time horizon $\mathcal{H}$. Using a dataset $\mathcal{D}$ of the form (5.2), find a controller $k : X \to U$ together with a constant $\rho \in [0, 1)$ and confidence $(1-\beta) \in [0, 1]$ such that $\mathcal{S}$ under this controller satisfies Ψ with a probability of at least $(1-\rho)$, *i.e.*, $\mathbb{P}_w^k\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho,\quad \forall x(0) \in X_{in}$, with a confidence $1-\beta$. Moreover, establish a connection between the required size of $\mathcal{D}$ and the confidence $1-\beta$.

Similar to the verification problem discussed in the previous sections, we use the notion of control barrier certificates with a parameterized set of controllers introduced by Jagtap, Soudjani et al. (2020) to get a characterization of the controller together with the lower bound on the safety probability.

Definition 5.3. Given a dt-SCS $\mathcal{S} = (X, U, V_w, w, f)$ with $U \subset \mathbb{R}^m$, initial set $X_{in} \subset X$, and unsafe set $X_u \subset X$, a function $B : X \to \mathbb{R}_0^+$ is called a control barrier certificate (CBC) for $\mathcal{S}$ if there exist constants $\lambda > 1$, $c \geq 0$, and functions $\mathscr{P}_\ell(x) : X \to \mathbb{R}_0^+$, $\ell \in \{1, 2, \ldots, m\}$, such that constraints in (2.3) and (2.4) hold, and

$$\begin{aligned} &\mathbb{E}\Big[B(f(x, u, w)) \mid x, u\Big] + \sum_{\ell=1}^{m}(u_\ell - \mathscr{P}_\ell(x)) \leq B(x) + c \\ &\qquad \forall x \in X,\ \forall u = [u_1; \ldots; u_m] \in U. \end{aligned} \tag{5.3}$$

Theorem 5.4. *A CBC $B(x)$ as in Definition 5.3 guarantees that $\mathbb{P}_w^k\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho,\quad \forall x(0) \in X_{in}$, under the controller $k(x) = [\mathscr{P}_1(x); \mathscr{P}_2(x); \ldots; \mathscr{P}_m(x)]$, where $\rho = (1 + c\mathcal{H})/\lambda$ with $\mathcal{H}$ being the time horizon of the safety specification.*

Let us consider polynomial-type CBC and controllers. The number of CBC coefficients is denoted by $\mathcal{Q}$. Polynomial $\mathscr{P}_\ell$ has the following form for some $k' \in \mathbb{N}_0$:

$$\mathscr{P}_\ell(p^\ell, x) = \sum_{\iota_1=0}^{k'} \dots \sum_{\iota_n=0}^{k'} p^\ell_{\iota_1,\dots,\iota_n}(x_1^{\iota_1} \dots x_n^{\iota_n}), \tag{5.4}$$

with $p^\ell_{\iota_1,\dots,\iota_n} = 0$ for $\iota_1 + \dots + \iota_n > k'$.

The overall number of all coefficients of m polynomials $\mathscr{P}_\ell(p^\ell, x)$ is denoted by $\mathcal{P}$. We also assume that the input set U is a polytope of the form

$$U = \left\{u \in \mathbb{R}^m \mid \mathcal{A}u \leq \mathfrak{b}\right\}, \tag{5.5}$$

for some $\mathcal{A} \in \mathbb{R}^{q\times m}$ and $\mathfrak{b} \in \mathbb{R}^{q\times 1}$.

Under these assumptions, the inequalities in Definition 5.3 and Theorem 5.4 can be written as an RCP:

$$\text{RCP}: \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max\limits_{z} \ \ g_z(x,u,d) \leq 0, \\ & z \in \{1,2,\dots,5+q\}, \forall x \in X, \forall u \in U, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1,\dots,\iota_n}; p^\ell_{\iota_1,\dots,\iota_n}], \\ & \mathcal{K} \in \mathbb{R}, \ \lambda > 1, \ c \geq 0, \end{cases} \tag{5.6}$$

where $g_z(x,d), z \in \{1,\dots,4\}$, are the same as (3.2), and

$$\begin{aligned} g_5(x,u,d) &= \mathbb{E}\Big[\mathrm{B}(b,f(x,u,w)) \mid x,u\Big] + \sum_{\ell=1}^{m}(u_\ell - \mathscr{P}_\ell(p^\ell,x)) \\ &- \mathrm{B}(b,x) - c - \mathcal{K}, \\ [g_6(x,d);\dots;g_{5+q}(x,d)] &= \ \mathcal{A}\,[\mathscr{P}_1(p^1,x);\dots;\mathscr{P}_m(p^m,x)] - \\ \mathfrak{b} &- \ \mathcal{K}\mathbf{1}_{q\times 1}. \end{aligned} \tag{5.7}$$

Note that the last inequality in (5.7) encodes the fact that the control input should be inside the set U specified by the polytope (5.5).

The constraints in the RCP is always feasible. A solution can be constructed as follows. Set the coefficients of $\mathrm{B}(b,x)$ and $\mathscr{P}_\ell(p^\ell,x)$ equal to zero, $c = 0$, $\lambda = 2$, and $u_\ell = \mathscr{P}_\ell(p^\ell,x)\ \forall \ell \in \{1,\dots,m\}$. Also select $\mathcal{K}$ large enough such that $\mathcal{K} \geq \frac{1}{\rho} - 2$ together with $\mathcal{K}\ \mathbf{1}_{m\times 1} \geq -\mathfrak{b}$.

The RCP in (5.6) is in general hard to solve since the map f and the probability measure $\mathbb{P}_w$ are unknown. Hence, similar to the verification approach discussed in Section 3, we assign a probability distribution to both state and input sets, and collect N i.i.d. pairs (x_i,u_i) from this assigned distribution, and replace the robust quantifiers $\forall x \in X$ and $\forall u \in U$ with $\forall x_i \in X$ and $\forall u_i \in U, i \in \{1,\dots,N\}$, respectively. This results in a scenario convex program called SCP_N, which is not presented here for the sake of brevity.

To address the issue of unknown f and $\mathbb{P}_w$, the expectation in g_5 is replaced with its empirical approximation by sampling $\hat{N}$ i.i.d. values $w_j,\ j \in \{1,\dots,\hat{N}\}$, from $\mathbb{P}_w$ for each pair of (x_i,u_i), which results in the following scenario convex program denoted by $\text{SCP}_{N,\hat{N}}$:

$$\text{SCP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} & \mathcal{K} \\ \text{s.t.} & \max\limits_{z} \ \bar{g}_z(x_i,u_i,d) \leq 0, \\ & z \in \{1,2,\dots,5+q\}, \\ & \forall x_i \in X, \ \forall u_i \in U, \forall i \in \{1,\dots,N\}, \\ & d = [\mathcal{K}; \lambda; c; b_{\iota_1,\dots,\iota_n}; p^\ell_{\iota_1,\dots,\iota_n}], \\ & \mathcal{K} \in \mathbb{R}, \ \lambda > 1, \ c \geq 0, \end{cases} \tag{5.8}$$

where $\bar{g}_z := g_z$ for all $z \in \{1,2,\dots,5+q\} \setminus \{5\}$, and

$$\begin{aligned} \bar{g}_5(x_i,u_i,d) &= \frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b,f(x_i,u_i,w_j)) + \\ &\sum_{\ell=1}^{m}(u_{i_\ell} - \mathscr{P}_\ell(p^\ell,x_i)) - \ \mathrm{B}(b,x_i) - c + \delta - \mathcal{K}. \end{aligned} \tag{5.9}$$

Using empirical approximation introduces an error which is demonstrated by δ in the above optimization problem. We denote by $\hat{\mathrm{B}}_u(b,x \mid \mathcal{D})$ the constructed control barrier certificate with coefficients computed by solving the $\text{SCP}_{N,\hat{N}}$.

Remark 5.5. Similar to Theorem 3.3, under the assumption

$$Var\big(\mathrm{B}(b,f(x,u,w))\big) \leq \hat{M},$$

for some $\hat{M} > 0$, a desired confidence $\beta_s \in (0,1]$, and an error δ, one has

$$\mathbb{P}^{\mathrm{k}}_w\Big(\hat{\mathrm{B}}_u(b,x \mid \mathcal{D}) \models \text{SCP}_N\Big) \geq 1 - \beta_s, \tag{5.10}$$

provided that $\hat{N} \geq \frac{\hat{M}}{\delta^2\beta_s}$.

To provide the main results here, we need the following assumptions.

Assumption 5.6. Function g_5 is Lipschitz continuous with respect to (x,u) with Lipschitz constant L_5. Functions $g_1, g_2, g_3, g_6, \dots, g_{5+q}$ are also Lipschitz continuous with respect to x with Lipschitz constants $\mathrm{L}_1, \mathrm{L}_2, \mathrm{L}_3, \mathrm{L}_6, \dots, \mathrm{L}_{5+q}$, respectively. Then, the Lipshitz constat of maximum of these function is $\mathrm{L}_1+\mathrm{L}_2+\mathrm{L}_3+\mathrm{L}_5+\mathrm{L}_6+\dots+\mathrm{L}_{5+q}$. Furthermore, if all functions g are analytic over a compact domain $X \times U$, the Lipschitz constant of their maximum is $\max(\mathrm{L}_1,\mathrm{L}_2,\mathrm{L}_3,\mathrm{L}_5,\mathrm{L}_6,\dots,\mathrm{L}_{5+q})$, which we denote it by $\mathrm{L}_{x,u}$.

Assumption 5.7. There is a strictly increasing function $G(r) : \mathbb{R}^+ \to [0,1]$ such that

$$\mathbb{P}[\mathfrak{b}(x,u,r)] \geq G(r) \qquad \forall (x,u) \in X \times U, \tag{5.11}$$

where $\mathfrak{b}(x,u,r)$ is an open ball in the product space $X \times U$ centered at the point (x,u) with radius r.

Now, we have all the ingredients to propose the main results here.

Theorem 5.8. *Consider an unknown dt-SCS as in Definition 5.1 and a safety specification Ψ. Let Assumptions 5.6–5.7 hold with constant $\mathrm{L}_{x,u}$ and function $G(r)$. Suppose that $\mathcal{K}^*(\mathcal{D})$ is the optimal value of $\text{SCP}_{N,\hat{N}}$ in (5.8) with number of samples N, a given $\rho \in (0,1]$, and for $\hat{N}$ selected based on Remark 5.5 with confidence of $1-\beta_s$. Suppose*

$$\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_{x,u}G^{-1}(\epsilon) \leq 0, \tag{5.12}$$

where function G is defined in (5.11) and $\epsilon = I^{-1}(1-\beta; \mathcal{Q}+\mathcal{P}+3, N-\mathcal{Q}-\mathcal{P}-2)$ with confidence parameter $\beta \in [0,1]$, and $\mathcal{Q}$ and $\mathcal{P}$ being respectively the number of coefficients of the polynomial control barrier certificate and the overall number of coefficients of polynomials $\mathscr{P}_\ell(p^\ell,x)$ for m inputs. Then, the following statement is valid with a confidence of at least $1-3\beta-\beta_s$: the system $\mathcal{S}$ together with the constructed control input

$$k(x) := [\mathscr{P}_1(p^1,x);\dots;\mathscr{P}_m(p^m,x)],$$

for which coefficients $p^\ell, \ell \in \{1,\dots,m\}$, are obtained from the solution of $\text{SCP}_{N,\hat{N}}$, is safe within the time horizon $\mathcal{H}$ with a probability of at least $1-\rho$, i.e.,

$$\mathbb{P}^k_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1 - \rho. \tag{5.13}$$

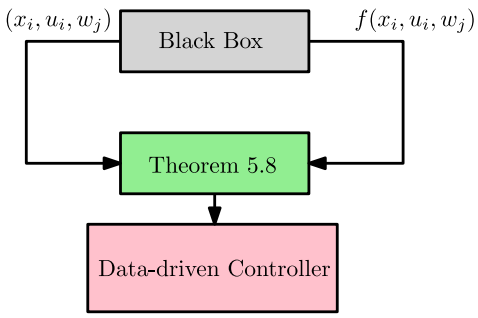

Fig. 3. A schematic overview of the data-driven synthesis presented in Section 5.

Proof. The proof is similar to the proof of Theorem 4.4 by replacing $\mathbb{P}_w$ with $\mathbb{P}^{\mathrm{k}}_w$ for the RCP (5.6) and its associated SCPs. The function $G(\epsilon)$ is defined as in (5.11). The number of coefficients is $\mathcal{Q}+\mathcal{P}+3$ where $\mathcal{P}$ is the overall number of coefficients of m polynomials defining the controller, which results in the new arguments of the regularized incomplete beta function I in the theorem statement. □

Corollary 5.9. *If samples are collected uniformly from a hyper rectangular sets X and U, respectively, with edges of length $\eta_x(i)$ and $\eta_u(j)$ in each dimension i and j, then one can compute $G(\epsilon)$ as $\frac{a\epsilon^{n+m}}{\prod_{i=1}^{n}\eta_x(i)\prod_{j=1}^{m}\eta_u(j)}$, where $a=\frac{1}{2^{n+m}}\frac{\pi^{\frac{n+m}{2}}}{\Gamma(\frac{n+m}{2}+1)}$ with Gamma function defined in Corollary 4.5.*

Proof. The proof is similar to the proof of Corollary 4.5 in Appendix B based on the new definition of $G(r)$ in Assumption 5.7.

Remark 5.10. When ρ is not fixed, one can eliminate constraint g_4 from (5.6) and directly provide the following inequality

$$\mathbb{P}^{\mathrm{k}}_w(\mathcal{S}\models_{\mathcal{H}}\Psi)\geq 1-\frac{1+c^*\mathcal{H}^*}{\lambda},$$

in which c^* and λ^* are the optimal solutions of $\mathrm{SCP}_{N,\hat{N}}$ in (5.8). This increases the likelihood of getting a feasible solution and gives the best possible lower bound on the safety probability for $\mathcal{S}$. A schematic overview of our synthesis approach is presented in Fig. 3.

Algorithm 2: Data-driven synthesis for safety specification on an unknown dt-SCS $\mathcal{S}=(X,U,V_w,w,f)$.

Input: Confidence parameters $\beta\in[0,1]$, $\beta_s\in(0,1]$, parameters $\rho\in(0,1]$, $\delta\in\mathbb{R}^+$, $\hat{M}\in\mathbb{R}^+$, $\mathrm{L}_{x,u}\in\mathbb{R}^+$, degree of the barrier certificate $\mathcal{Q}$, and degree of the polynomial functions for the controller $\mathcal{P}$
1: Compute the number of samples $\hat{N}\geq\hat{M}/(\delta^2\beta_s)$ for the empirical average (Remark 5.5)
2: Choose the number of samples N
3: Compute $\epsilon=\mathrm{I}^{-1}(1-\beta;\mathcal{Q}+\mathcal{P}+3,N-\mathcal{Q}-\mathcal{P}-2)$
4: Select a probability measure $\mathbb{P}$ for the state-input set (X,U)
5: Collect $N\hat{N}$ tuples from the system $\mathcal{D}:=\{(x_i,u_i,x'_{ij})\in X\times U\times X,\ x'_{ij}=f(x_i,u_i,w_{ij})\}_{i,j}$
6: Solve $\mathrm{SCP}_{N,\hat{N}}$ in (5.8) with $\mathcal{D}$ and obtain the optimal solution $\mathcal{K}^*(\mathcal{D})$
Output: If $\mathcal{K}^*(\mathcal{D})+\mathrm{L}_{x,u}G^{-1}(\epsilon)\leq 0$, then $\mathbb{P}^{\mathrm{k}}_w(\mathcal{S}\models_{\mathcal{H}}\Psi)\geq 1-\rho$ with a confidence of at least $1-3\beta-\beta_s$ and with the controller $\mathrm{k}(x):=[\mathscr{P}_1(p^1,x);\ldots;\mathscr{P}_m(p^m,x)]$.

Next lemma provides an upper bound for Lipschitz constant $\mathrm{L}_{x,u}$, which is required in Theorem 5.8, in the case that the system is affected by an additive noise.

Lemma 5.11. *Consider a nonlinear dt-SCS as in Definition 5.1 which is affected by an additive noise as the following:*

$$x(t+1)=f_a(x(t),u(t))+w(t), \tag{5.14}$$

and a bounded state set X and input set U such that $\|x\|\leq\mathcal{L}_x$ for all $x\in X$, and $\|u\|\leq\mathcal{L}_u$ for all $u\in U$. Without loss of generality, we assume that the mean of the noise is zero. Let $\|f_a(x,u)\|\leq L_1\|x\|+L_2\|u\|+L_3$, $\|\mathbf{J}_x\|\leq\hat{L}_x$, and $\|\mathbf{J}_u\|\leq\hat{L}_u$, for some $\mathcal{L}_x,\mathcal{L}_u,L_1,L_2,L_3,\hat{L}_x,\hat{L}_u\geq 0$, where $\mathbf{J}_x$ and $\mathbf{J}_u$ are Jacobian matrices of $f_a(x,u)$ with respect to x and u, respectively. Given a quadratic barrier function x^TPx, and a set of quadratic functions $x^TP_\ell x$, $\ell\in\{1,\ldots,m\}$, representing each of $\mathscr{P}_\ell(p^\ell,x)$ with symmetric matrices P and P_ℓ, the Lipschitz constant $\mathrm{L}_{x,u}$ can be upper-bounded by $\sqrt{\mathscr{L}_x^2+\mathscr{L}_u^2}$, where

$$\begin{aligned}\mathscr{L}_x=&\,2\mathcal{L}_xL_1\hat{L}_x\|P\|+2\mathcal{L}_uL_2\hat{L}_x\|P\|+2L_3\hat{L}_x\|P\|\\&+\mathcal{L}_x\|P\|+\mathcal{L}_x\sum_{\ell=1}^{m}\|P_\ell\|,\end{aligned}\tag{5.15}$$

$$\mathscr{L}_u=2\mathcal{L}_xL_1\hat{L}_u\|P\|+2\mathcal{L}_uL_2\hat{L}_u\|P\|+2L_3\hat{L}_u\|P\|+\sqrt{m}.$$

Proof. We first compute the Lipschitz constant regarding $g_5(x,u,d)$ in (5.7), where

$$\begin{aligned}g_5(x,u,d)=&\,\mathbb{E}\big[(f^T(x(t),u(t))+w^T(t))\mathrm{P}(f(x(t),u(t))+\\&w(t))\big]+\sum_{\ell=1}^{m}(u_\ell-\mathscr{P}_\ell(p^\ell,x))-x^T(t)\mathrm{P}x(t)-c.\end{aligned}$$

Considering $\mathbb{E}[w(t)]=0$, we compute the upper bounds for Lipschitz constant with respect to x and u separately denoted by L_{5_x} and L_{5_u}, respectively. We define $\mathbf{J}_x=[\frac{\partial f}{\partial x_1},\ldots,\frac{\partial f}{\partial x_n}]$ and $\mathbf{J}_u=[\frac{\partial f}{\partial u_1},\ldots,\frac{\partial f}{\partial u_m}]$ as Jacobian matrices with respect to x and u, respectively.

$$\begin{aligned}\mathrm{L}_{5_x}=&\max_{x,u}\|\frac{\partial g_5(x,u,d)}{\partial x}\|=\max_{x,u}\|2f(x(t),u(t))^T\mathrm{P}\,\mathbf{J}_x\\&-x^T(t)\mathrm{P}-x^T(t)\sum_{\ell=1}^{m}\mathrm{P}_\ell\|\\\leq&\,2\mathcal{L}_xL_1\hat{L}_x\|\mathrm{P}\|+2\mathcal{L}_uL_2\hat{L}_x\|\mathrm{P}\|+2L_3\hat{L}_x\|\mathrm{P}\|+\\&\mathcal{L}_x\|\mathrm{P}\|+\mathcal{L}_x\sum_{\ell=1}^{m}\|\mathrm{P}_\ell\|,\end{aligned}$$

and accordingly,

$$\begin{aligned}\mathrm{L}_{5_u}=&\max_{x,u}\|\frac{\partial g_5(x,u,d)}{\partial u}\|\\=&\,\|2f(x(t),u(t))^T\mathrm{P}\mathbf{J}_u+\mathbf{1}_m\|\\\leq&\,2\mathcal{L}_xL_1\hat{L}_u\|\mathrm{P}\|+2\mathcal{L}_uL_2\hat{L}_u\|\mathrm{P}\|+2L_3\hat{L}_u\|\mathrm{P}\|+\sqrt{m}.\end{aligned}$$

Now it can be deduced that $\mathrm{L}_5\leq\sqrt{\mathrm{L}_{5_x}^2+\mathrm{L}_{5_u}^2}$. Similar to the proof of Lemma 4.10, it is straightforward to compute the upper bounds of Lipschitz constants for other constraints in (5.7) and show that the computed upper bound is greater than all of them. We ignore this part for the sake of brevity. Then, $\mathrm{L}_{x,u}\leq\max\big(\mathrm{L}_i,i\in\{1,2,\ldots,5+q\}\setminus\{4\}\big)=\sqrt{\mathrm{L}_{5_x}^2+\mathrm{L}_{5_u}^2}$ which is equivalent to $\sqrt{\mathscr{L}_x^2+\mathscr{L}_u^2}$ with $\mathscr{L}_x$ and $\mathscr{L}_u$ as in (5.15). □

Note that one can use similar results as in Remark 4.13 to estimate the Lipschitz constant via data.

6. Data-driven barrier certificates for non-convex setting

In this section, we extend the proposed result in Section 4 to a case of having non-convex constraints. We modify the constraint (2.5) in Definition 2.4 as follows:

$$\mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \kappa\ \mathrm{B}(x) + c, \quad \forall x \in X, \tag{6.1}$$

where $\kappa \in (0,1)$.

According to the fundamental results by Kushner (1967), choosing κ in the interval $(0,1)$ provides a better lower bound for the probability of safety satisfaction in (2.6), namely:

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1-\rho,$$

with

$$\rho = \begin{cases} 1-(1-\frac{1}{\lambda})(1-\frac{c}{\lambda}) & \text{if } \lambda \geq \frac{c}{\kappa} \\ \frac{1}{\lambda}(1-\kappa)^{\mathcal{H}} + \frac{c}{\kappa\lambda}\big(1-(1-\kappa)^{\mathcal{H}}\big) & \text{if } \lambda < \frac{c}{\kappa}, \end{cases} \tag{6.2}$$

where parameters c, λ, and $\mathcal{H}$ are the same as in Definition 2.4. Another advantage of choosing κ in the interval $(0,1)$ is that this new formulation can be utilized in the context of compositionality and interconnected systems (Swikir & Zamani, 2019; Zamani & Arcak, 2018).

Replacing the last condition of RCP in (3.2) with the modified constraint in (6.1) leads to the following optimization problem which is not convex anymore:

$$\mathrm{RP}: \begin{cases} \min\limits_{d} \quad \mathcal{K} \\ \text{s.t.} \quad \max\limits_{z}\big(g_z(x,d)\big) \leq 0, z \in \{1,\dots,4\}, \forall x \in X, \\ \qquad d = [\mathcal{K};\lambda;c;b_{\iota_1,\dots,\iota_n};\kappa], \\ \qquad \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0,\ \kappa \in (0,1), \end{cases} \tag{6.3}$$

in which $g_z(x,d), z \in \{1,2,3\}$, are the same as in (3.2), and

$$g_4(x,d) = \mathbb{E}\Big[\mathrm{B}(f(x,w)) \mid x\Big] \leq \kappa\ \mathrm{B}(x) + c, \quad \forall x \in X. \tag{6.4}$$

The non-convexity comes from the multiplication of κ and coefficients of barrier function $\mathrm{B}(b,x_i)$ in (6.1). With the same reasoning in Section 3, solving the above RP is not straightforward generally. Therefore, we construct an SP by taking samples and then connect the solution of the obtained scenario programming to the safety of the stochastic system in (2.1). By collecting i.i.d. samples $x_i,\ i \in \{1,\dots,N\}$, from an assigned probability distribution over the state set, and approximating the expectation term in (6.1) results in a non-convex programming as the following:

$$\mathrm{SP}_{N,\hat{N}}: \begin{cases} \min\limits_{d} \quad \mathcal{K} \\ \text{s.t.} \quad \max\limits_{z}\ \bar{g}_z(x_i,d) \leq 0,\ \ \forall i \in \{1,\dots,N\}, \\ \qquad\qquad z \in \{1,\dots,4\}, \\ \qquad d = [\mathcal{K};\lambda;c;b_{\iota_1,\dots,\iota_n};\kappa], \\ \qquad \mathcal{K} \in \mathbb{R},\ \lambda > 1,\ c \geq 0,\ \kappa \in (0,1), \end{cases} \tag{6.5}$$

where $\bar{g}_z := g_z$ for all $z \in \{1,2,3\}$ and

$$\bar{g}_4(x_i,d) = \frac{1}{\hat{N}}\sum_{j=1}^{\hat{N}} \mathrm{B}(b,f(x_i,w_j)) - \kappa\ \mathrm{B}(b,x_i) - c + \delta - \mathcal{K}. \tag{6.6}$$

Note that in this new scenario programming, we eliminated the constraint that forces a fixed probability lower bound $1-\rho$ on the safety of the stochastic system, namely, g_4 in (3.2). Instead, we are interested in providing the tightest possible lower bound of the safety probability according to Remark 4.9. The main issue underlying here is that by considering $\kappa \in (0,1)$, the obtained scenario program is not convex anymore, and accordingly, one cannot naively utilize the results proposed in Theorems 4.4. Hence, one cannot solve the SP in (6.5) by simply applying bisection over κ, while still utilizing the proposed results in the previous sections.

Now we state the main problem we aim to address in this section.

Problem 6.1. Consider an unknown dt-SS $\mathcal{S}$ as in Definition 2.1. Compute the largest lower bound $(1-\rho) \in [0,1]$ on the probability of satisfying Ψ, *i.e.,*

$$\mathbb{P}_w\big(\mathcal{S} \models_{\mathcal{H}} \Psi\big) \geq 1-\rho,$$

according to (6.2) together with a confidence $(1-\beta) \in [0,1]$ using a dataset $\mathcal{D}$ of the form (2.2). Moreover, establish a connection between the required size of dataset $\mathcal{D}$, the cardinality of the set from which the parameter κ is selected, and the desired confidence $1-\beta$.

In the next theorem, we present our solution to Problem 6.1 by proposing a new confidence bound which is always valid even for the non-convex scenario program in (6.5).

Theorem 6.2. *Consider an unknown dt-SS as in (2.1) together with the safety specification Ψ. Let M be the cardinality of a finite set from which κ takes value in (0,1). Suppose that Assumptions 4.1–4.2 hold for the RP in (6.3) with function $G(\cdot)$ and $L_x := \max\big(L_{x_1}, L_{x_2}, L_{x_3}, L_{x_4}\big)$, where $L_{x_i}, i \in \{1,\dots,4\}$, is an upper bound on the Lipschitz constant of the ith constraint in (6.3). Assume $\hat{N}$ is selected for the $\mathrm{SP}_{N,\hat{N}}$ similar to Theorem 3.3 in order to provide confidence $1-\beta_s$. Suppose $\mathcal{K}^*(\mathcal{D})$ is the optimal value of the optimization problem in (6.5) using $\hat{N}$ and N. Furthermore, $\epsilon = I^{-1}(1-M\beta;\mathcal{Q}+3, N-\mathcal{Q}-2)$ for $\beta \in [0,1]$, where $\mathcal{Q}$ is the number of coefficients of the barrier certificate. Then the following statement holds with a confidence of at least $1-3\beta-\beta_s$: if $\mathcal{K}^*(\mathcal{D}) + L_x G^{-1}(\epsilon) \leq 0$, then*

$$\mathbb{P}_w(\mathcal{S} \models_{\mathcal{H}} \Psi) \geq 1-\rho^*, \tag{6.7}$$

where ρ^* is computed as in (6.2) using optimal solutions of $\mathrm{SP}_{N,\hat{N}}$, namely, c^*, λ^*, and κ^*. More importantly, with a confidence of at least $1-3\beta-\beta_s$, $\mathrm{B}(b^*,x)$ is a barrier certificate for S, satisfying (2.3), (2.4), and (6.1), where b^* is the optimal solution of $\mathrm{SP}_{N,\hat{N}}$.

Proof. Denote the optimal values of the RP and its equivalent scenario programming before the empirical approximation of the expectation term in g_4, namely, SP_N, by $\mathcal{K}^*$ and $\mathcal{K}^*_{\mathrm{m}}(\mathcal{D})$, respectively. Similar to (4.3), one has

$$\mathbb{P}\big(\mathcal{K}^* \leq \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\big) \geq 1-3\beta,$$

for any $N \geq \tilde{N}(\epsilon_1,\dots,\epsilon_{\mathrm{M}},\beta)$, where

$$\tilde{N}(\epsilon_1,\dots,\epsilon_{\mathrm{M}},\beta) := \min\Big\{N \in \mathbb{N} \mid \sum_{z=1}^{\mathrm{M}}\sum_{i=0}^{\mathrm{d}-1}\binom{N}{i}\epsilon_z^{\,i}(1-\epsilon_z)^{N-i} \leq \beta\Big\}.$$

Alternatively, one can set $\epsilon := \epsilon_1 = \epsilon_2 = \cdots = \epsilon_{\mathrm{M}}$ in the above expression to get the inequality $\epsilon \leq \mathrm{I}^{-1}(1-\mathrm{M}\beta;\mathrm{d},N-\mathrm{d}+1)$, where M is the cardinality of the set from which κ is selected, and d is the number of decision variables. By choosing $\mathrm{d} := \mathcal{Q}+3$, one gets the parameters of the incomplete beta function in the theorem statement. On the other hand, due to the particular selection of $\hat{N}$ and β_s similar to Theorem 3.3, it can be deduced that

$$\mathbb{P}_w\Big(\hat{\mathrm{B}}(b,x \mid \mathcal{D}) \models \mathrm{SP}_N\Big) \geq 1-\beta_s,$$

where $\hat{\mathrm{B}}(b,x \mid \mathcal{D})$ is the barrier function whose coefficients are the optimal solution of SP_N. Therefore, we have

$$\mathbb{P}\left(\mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\right) \geq 1-\beta_s. \tag{6.8}$$

By defining events $\mathcal{A} := \{\mathcal{D} \mid \mathcal{K}^* \leq \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon)\}$, $\mathcal{B} := \{\mathcal{D} \mid \mathcal{K}^*_{\mathrm{m}}(\mathcal{D}) \leq \mathcal{K}^*(\mathcal{D})\}$, and $\mathcal{C} := \{\mathcal{D} \mid \mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) \leq 0\}$, where $\mathbb{P}(\mathcal{A}) \geq 1 - 3\beta$ and $\mathbb{P}(\mathcal{B}) \geq 1 - \beta_s$, it is easy to conclude using the same reasoning as in the second part of proof of Theorem 4.4 that

$$\mathbb{P}(\mathcal{K} \leq 0) \geq 1 - 3\beta - \beta_s,$$

which ensures safety of the stochastic system with a lower bound $1 - \rho$ and a confidence of at least $1 - 3\beta - \beta_s$. □

7. Numerical examples

The simulations of this section are performed on an iMac 3.5 GHz Quad-Core Intel Core i7. The optimizations are solved by CVX Toolbox (Grant & Boyd, 2014) with Mosek (Andersen & Andersen, 2000) as the solver.

7.1. Temperature verification for three rooms

Consider a temperature regulation problem for three rooms characterized by the following discrete-time stochastic system:

$$\begin{aligned}
\mathrm{T}_1(t+1) =& \big(1 - \tau_s(\alpha + \alpha_e)\big)\mathrm{T}_1(t) + \tau_s\alpha \mathrm{T}_2(t) + \\
& \tau_s\alpha_e T_e + w_1(t) \\
\mathrm{T}_2(t+1) =& \big(1 - \tau_s(2\alpha + \alpha_e)\big)\mathrm{T}_2(t) + \tau_s\alpha(\mathrm{T}_1(t) + \mathrm{T}_3(t)) + \\
& \tau_s\alpha_e T_e + w_2(t) \\
\mathrm{T}_3(t+1) =& \big(1 - \tau_s(\alpha + \alpha_e)\big)\mathrm{T}_3(t) + \tau_s\alpha \mathrm{T}_2(t) + \\
& \tau_s\alpha_e T_e + w_3(t),
\end{aligned} \tag{7.1}$$

where $\mathrm{T}_1(t)$, $\mathrm{T}_2(t)$, and $\mathrm{T}_3(t)$ are temperatures of three rooms, respectively. Terms $w_1(t)$, $w_2(t)$, and $w_3(t)$ are additive zero-mean Gaussian noises with standard deviations of 0.01, which model the environmental uncertainties. Parameter $T_e = 10$ °C is the ambient temperature. Constants $\alpha_e = 8 \times 10^{-3}$ and $\alpha = 6.2 \times 10^{-3}$ are heat exchange coefficients between rooms and the ambient, and individual rooms, respectively. The model for each room is adapted from Girard, Gössler, and Mouelhi (2016) discretized by $\tau_s = 5$ min. Let us consider the regions of interest for each room as $X_{in} = [17\ °\mathrm{C}, 18\ °\mathrm{C}]$, $X_u = [29\ °\mathrm{C}, 30\ °\mathrm{C}]$, and $X = [17\ °\mathrm{C}, 30\ °\mathrm{C}]$. We assume the model of the system and the distribution of the noise are unknown. The main goal is to verify whether the temperature of each room remains in the comfort zone $[17, 29]$ for the time horizon $\mathcal{H} = 3$ which is equivalent to 15 min, with a priori confidence of 99%.

Let us consider a barrier certificate with degree $k = 2$ in the polynomial form as $[T1; T2; T3]^T \mathrm{P}[T1; T2; T3] = b_0 T_1^2 + b_1 T_2^2 + b_2 T_3^2 + b_3 T_1 T_2 + b_4 T_1 T_3 + b_5 T_2 T_3 + b_6 T_1 + b_7 T_2 + b_8 T_3 + b_9$, where

$$\mathrm{P} = \begin{bmatrix} b_0 & \frac{b_3}{2} & \frac{b_4}{2} & \frac{b_6}{2} \\ \frac{b_3}{2} & b_1 & \frac{b_5}{2} & \frac{b_7}{2} \\ \frac{b_4}{2} & \frac{b_5}{2} & b_2 & \frac{b_8}{2} \\ \frac{b_6}{2} & \frac{b_7}{2} & \frac{b_8}{2} & b_9 \end{bmatrix}. \tag{7.2}$$

According to Algorithm 1, we first choose the desired confidence parameters β and β_s as $\frac{0.005}{3}$ and 0.005, respectively. The value of empirical approximation error is selected as $\delta = 0.05$. We choose $\rho = 0.2$. The Lipschitz constant is computed as 1.5 according to Remark 4.13. By enforcing $\hat{M} = 0.005$, the required number of samples for the approximation of the expected value in (3.4) is $\hat{N} = 400$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with the number of samples $N = 6 \times 10^6$ and the computed $\hat{N} = 400$, which gives us the optimal objective value $\mathcal{K}^*(\mathcal{D}) = -0.46$. The computation time is about 5 min. For $N = 6 \times 10^6$ and $\beta = \frac{0.005}{3}$, ϵ is computed as 4.36×10^{-6}. Function $G^{-1}(\epsilon)$ is also computed as $16.09\epsilon^{\frac{1}{3}}$ according to Corollary 4.5.

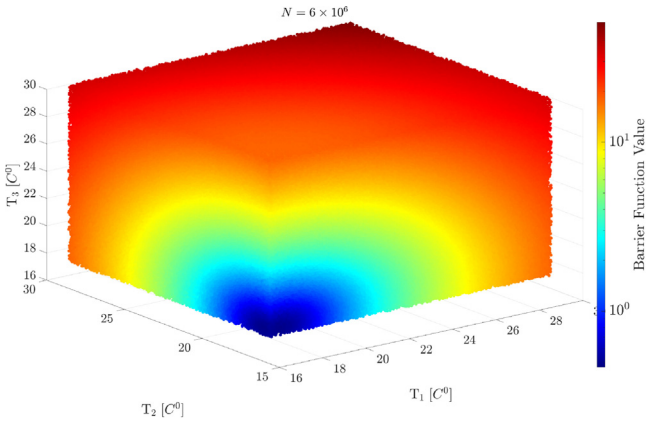

Fig. 4. Scatter plotting of the barrier certificate indicating portions of the state set where the inequalities in (3.4) are enforced for 6×10^6 sampled data.

Since $\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_x G^{-1}(\epsilon) = -0.066 \leq 0$, according to Theorem 4.4, one can conclude:

$$\mathbb{P}_w(\mathcal{S} \models_3 \Psi) \geq 1 - \rho = 0.80,$$

with a confidence of at least $1 - 3\beta - \beta_s = 0.99$. The barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is as follows:

$$\begin{aligned}
\hat{\mathrm{B}}(b, T_1, T_2, T_3 \mid \mathcal{D}) =& 0.112T_1^2 + 0.112T_2^2 + 0.112T_3^2 \\
& - 0.004T_1T_2 - 0.005T_1T_3 - 0.002T_2T_3 \\
& - 3.761T_1 - 3.815T_2 - 3.803T_3 + 99.93.
\end{aligned} \tag{7.3}$$

The computed optimal values for c and λ are 0.627 and 14.872, respectively. The scatter plot of the obtained barrier certificate is illustrated in Fig. 4. As can be seen in this figure, the barrier certificate has less values in the initial set while it has larger values in the unsafe region.

We remark that the conservatism of our approach is originating from two sources. (a) The first one is that we are using barrier certificates for computing the lower bound. A barrier certificate with a fixed template (polynomial of a certain degree) gives a lower bound that could have a gap with the best lower bound on the safety probability. (b) Our sampling approach requires making the optimization more conservative to account for going from robust programs over continuous (uncountable) domains to a scenario program with finite number of samples. If one assumes that the model is known in this case study, the synthesized barrier certificate has the parameters $c = 0.9767$ and $\lambda = 31.51$. This gives the lower bound 0.875 on the safety probability. Therefore, our approach provides a more conservative lower bound 0.80 since it assumes no knowledge of the model.

7.2. Lane keeping system

Lane keeping assist system is a future development of the modern lane departure warning system embedded in the current vehicles. This system usually assists the driver through electronic assistance with the steering force. The characteristics of this support depends on the distance of the vehicle from the edge of the lane among other factors such as uncertainties (Verband der Automobilindustrie, 2020). One of the key challenges in such assisting systems is verifying the obtained performance which can be defined as a safety problem.

In this subsection, it is supposed that the model of the vehicle and the distribution of noise are unknown, and one only has

access to a finite number of samples. This unknown system is characterized by a simplified kinematic single-track model of BMW320i which is adapted from the work by Althoff, Koschi, and Manzinger (2017) by discretization of the model and adding noise to imitate the uncertainties.

The nonlinear stochastic difference equation is as follows:

$$\mathcal{S}: \begin{aligned} x(t+1) &= x(t) + \tau_s v\ \cos(\psi(t) + \mathrm{b}) + w_1(t) \\ y(t+1) &= y(t) + \tau_s v\ \sin(\psi(t) + \mathrm{b}) + w_2(t) \\ \psi(t+1) &= \psi(t) + \frac{\tau_s v}{l_r} \sin(\mathrm{b}) + w_3(t), \end{aligned} \tag{7.4}$$

where $\mathrm{b} = \frac{l_r}{l_r+l_f} \tan^{-1}(\delta_f)$ with $\delta_f = 5$ degrees as the steering angle. Parameters $l_r = 1.384$ and $l_f = 1.384$ are the distances between the center of gravity of the vehicle to the rear and front axles, respectively. Variables x, y, and ψ denote horizontal movement, vertical movement, and the heading angle, respectively. This system is considered to be affected by zero-mean additive noises w_1, w_2, and w_3 which are related to uncertainties of position x, position y, and the heading angle ψ with standard deviation of 0.01, 0.01, and 0.001 respectively. Other parameters are the sampling time ($\tau_s = 0.1$ s), and the velocity ($v = 5$ m/s).

The state set is considered as $X = [1, 10] \times [-7, 7] \times [-0.05, 0.05]$. The regions of interest are $X_{in} = [1, 2] \times [-0.5, 0.5] \times [-0.005, 0.005]$, $X_{u_1} = [1, 10] \times [-7, -6] \times [-0.05, 0.05]$, and $X_{u_2} = [1, 10] \times [6, 7] \times [-0.05, 0.05]$. Now, the goal is to verify if the vehicle does not enter the unsafe regions of the lane for the time horizon of $\mathcal{H} = 3$ or equivalently 0.3 s with a desired confidence of 90%.

We consider a barrier certificate of degree $k = 2$ in the polynomial form as $[x; y; \psi]^T \mathrm{P}[x; y; \psi] = b_0x^2 + b_1y^2 + b_2\psi^2 + b_3xy + b_4x\psi + b_5y\psi + b_6x + b_7y + b_8\psi + b_9$, where the matrix P is as in (7.2).

We follow Algorithm 1 to find the barrier certificate and providing a probabilistic guarantee on the safety of stochastic system. First, the desired confidence parameters β and β_s are chosen as $\frac{.095}{3}$ and 0.005, respectively. We also select the empirical approximation error $\delta = 0.02$. The desired lower bound of safety probability is selected as $1 - \rho = 0.80$. The Lipschitz constant is computed as $\mathrm{L}_x = 10$ according to Remark 4.13. By enforcing $\hat{M} = 0.006$, the required number of samples for the approximation of the expected value in (3.4) is $\hat{N} = 3000$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with an arbitrary sample number $N = 6 \times 10^6$ and $\hat{N}$ which gives us the optimal value $\mathcal{K}^*(\mathcal{D}) = -0.4518$. The computation time is about 5 min. For those values of samples N and β, ϵ is computed as 3.41×10^{-6}. Using Corollary 4.5, $G^{-1}(\epsilon)$ is computed as $2.92\epsilon^{\frac{1}{3}}$.

Since $\mathcal{K}^*(\mathcal{D}) + 2.92\ \mathrm{L}_x\epsilon^{\frac{1}{3}} = -0.01 \leq 0$, according to Theorem 4.4, one can deduce that

$$\mathbb{P}_w(\mathcal{S} \models_3 \Psi) \geq 1 - \rho = 0.80,$$

with a confidence of at least $1 - 3\beta - \beta_s = 90\%$. The barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is represented as:

$$\begin{aligned} \hat{\mathrm{B}}(b, x, y, \psi \mid \mathcal{D}) =& 0.39y^2 + 0.15\psi^2 + 0.009x\psi \\ &- 0.007y\psi - 0.015\psi + 0.452. \end{aligned} \tag{7.5}$$

The optimal values of c and λ are 0.57 and 14.04, respectively. The exact value of the coefficients are reported in the Appendix.

The surface plot of the barrier certificate $\mathrm{B}(x, y, \psi) = \hat{\mathrm{B}}(b, x, y, \psi \mid \mathcal{D})$ with respect to x and y for a fixed value of $\psi = 0$ is depicted in Fig. 5. The blue transparent planes separate unsafe region on y, while the lower and upper red transparent planes demonstrate the thresholds in constraints (2.3) and (2.4), respectively. Satisfaction of the first and second condition of barrier certificate in Definition 2.4 can be observed in Fig. 5. The satisfaction of the third condition is illustrated in Fig. 6.

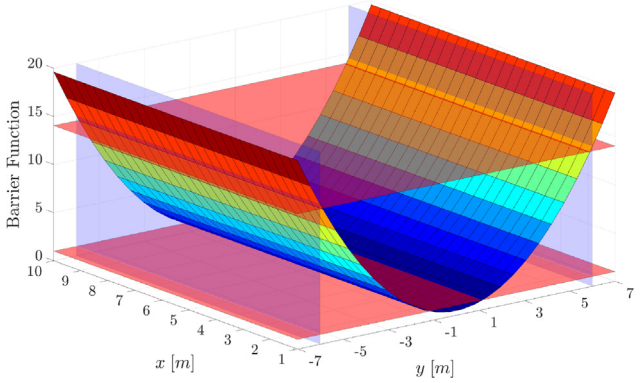

Fig. 5. Surface plot of the barrier certificate $\mathrm{B}(x, y, \psi)$ with respect to x and y for fixed $\psi = 0$. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

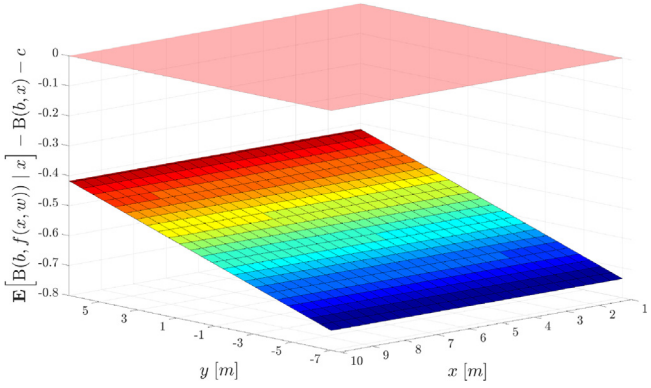

Fig. 6. Satisfaction of the third condition in Definition 2.4 (for $\psi = 0$) $\mathrm{B}(x, y, \psi)$ based on collected data.

7.3. Synthesizing a temperature controller

Consider a temperature regulation problem for a room using a heater characterized by

$$\begin{aligned} \mathcal{S}:\ \mathrm{T}(t+1) =& \mathrm{T}(t) + \tau_s\big(\alpha_e(T_e - \mathrm{T}(t)) + \\ & \alpha_h(T_h - \mathrm{T})u(t)\big) + w(t), \end{aligned} \tag{7.6}$$

where $w(t)$ is a zero-mean Gaussian noise with standard deviation of 0.05. Parameters are $T_e = 15$, $T_h = 45$, $\alpha_e = 8 \times 10^{-3}$, $\alpha_h = 3.6 \times 10^{-3}$, and $\tau_s = 5$. Regions of interest are defined as $X_{in} = [22\ ^\circ\mathrm{C}, 23\ ^\circ\mathrm{C}]$, $X_{u_1} = [27\ ^\circ\mathrm{C}, 28\ ^\circ\mathrm{C}]$, $X_{u_2} = [16.5\ ^\circ\mathrm{C}, 17.5\ ^\circ\mathrm{C}]$, and $X = [16.5\ ^\circ\mathrm{C}, 28\ ^\circ\mathrm{C}]$. The input region is $[0, 1]$. We assume that the model of the system and the distribution of the noise are unknown. The main goal is to design a controller that forces the temperature to remain in the comfort zone $[17.5, 27]$ for the time horizon $\mathcal{H} = 60$, which is equivalent to 300 min, with a priori confidence of 95%.

Let us fix a control barrier certificate with degree $k = 4$ in the polynomial form as $T^T\mathrm{P}T = b_0T^4 + b_1T^3 + b_2T^2 + b_3T + b_4$ with $b_0, b_1, b_2, b_3, b_4 \in \mathbb{R}$. The structure of the controller is considered to be a polynomial of degree $k' = 4$ as $u(p^1, T) = T^T\mathrm{P}_uT = p_0T^4 + p_1T^3 + p_2T^2 + p_3T + p_4$. Matrices P and P_u can be represented

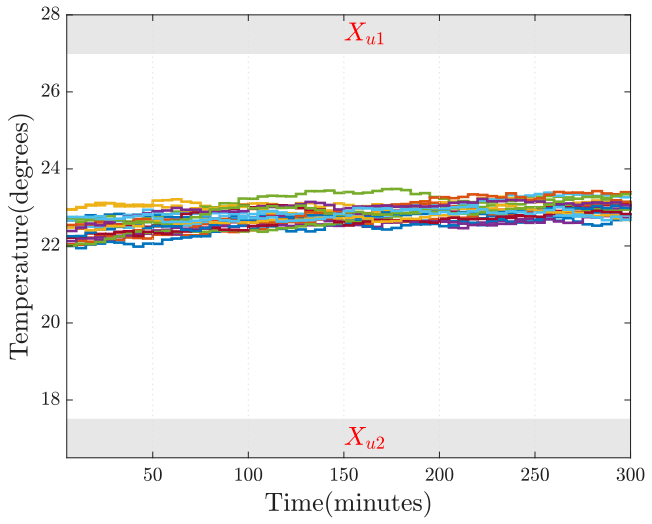

Fig. 7. The temperature trajectories of 15 different realizations of noise for three different initial temperature in the range $[22°, 23°]$.

as:

$$\mathrm{P} = \begin{bmatrix} b_0 & \frac{b_1}{2} & \frac{b_2}{3} \\ \frac{b_1}{2} & \frac{b_2}{3} & \frac{b_3}{2} \\ \frac{b_2}{3} & \frac{b_3}{2} & b_4 \end{bmatrix}, \mathrm{P}_u = \begin{bmatrix} p_0 & \frac{p_1}{2} & \frac{p_2}{3} \\ \frac{p_1}{2} & \frac{p_2}{3} & \frac{p_3}{2} \\ \frac{p_2}{3} & \frac{p_3}{2} & p_4 \end{bmatrix}. \tag{7.7}$$

According to Algorithm 2, we first choose the desired confidences β and β_s as $\frac{0.005}{3}$ and 0.045 respectively. We also select the approximation error $\delta = 2$. The Lipschitz constant $\mathrm{L}_{x,u}$ is computed as 12 according to Remark 4.13. By considering $\hat{M} = 1.5 \times 10^5$, the required number of samples for the approximation of the expected value in (3.4) is $\hat{N} = 833330$. Now, we solve the scenario problem $\mathrm{SCP}_{N,\hat{N}}$ with the selected number of samples $N = 1.5 \times 10^6$ and $\hat{N}$ which gives us the optimal value $\mathcal{K}^*(\mathcal{D}) = -0.41$. The computation time is about 2 min. For $N = 1.5 \times 10^6$ and $\beta = \frac{0.005}{3}$, value of ϵ is computed as 1.7424×10^{-5}. Using Corollary 5.9, $G^{-1}(\epsilon)$ is computed as $4.91\epsilon^{\frac{1}{2}}$.

Since $\mathcal{K}^*(\mathcal{D}) + \mathrm{L}_{x,u} G^{-1}(\epsilon) = -0.164 \leq 0$, one has

$$\mathbb{P}_w^{\mathrm{p}}(\mathcal{S} \models_{60} \Psi) \geq 1 - \rho = 0.80,$$

with a confidence of at least $1 - 3\beta - \beta_s = 95\%$. The computed values for λ and c are 4817 and 16.04, respectively. The control barrier certificate constructed from solving $\mathrm{SCP}_{N,\hat{N}}$ is:

$$\hat{\mathrm{B}}(b, T \mid \mathcal{D}) = 11.89\, T^4 - 1.07 \times 10^3\, T^3 + 3.61 \times 10^4\, T^2 - 5.42 \times 10^5 + 3.05 \times 10^6.$$

The obtained controller is:

$$\mathscr{P}_1(p^1, T \mid \mathcal{D}) = 1.45 \times 10^{-5} T^3 + 0.012 T^2 + 0.355.$$

The temperature trajectories for 15 different realizations of noise from three different initial temperature in the range $[22°, 23°]$ is illustrated in Fig. 7. As can be seen, the temperature in the collected trajectories do not enter the unsafe set, which is in gray color. We also ran the system to get 10^4 trajectories, all of them remain safe. This confirms the theoretical lower bound computed by our approach.

The conservativeness of our approach in terms of the safety bound $(1 - \rho)$ and the number of samples is shown in Table 1. The values are reported for increasing number of samples and two safety thresholds with $\rho \in \{0.1, 0.2\}$. As can be seen from the table, increasing the number of samples makes ϵ smaller and reduces the term $\mathrm{L}_{x,u} G^{-1}(\epsilon)$ used in (5.12). In contrast, the values of $\mathcal{K}^*(\mathcal{D})$ become larger. This creates a tradeoff between the two terms in (5.12). Note that the condition of having a negative value for $\mathrm{L}_{x,u} G^{-1}(\epsilon) + \mathcal{K}^*(\mathcal{D})$, thus guaranteeing safety with probability $(1-\rho)$, is only satisfied in the last two row of the table for $\rho = 0.2$ (indicated in blue color). Also, notice that the satisfaction of (5.12) for a higher desired safety probability requires larger number of samples.

8. Conclusion

We proposed a formal verification and synthesis procedure for discrete-time continuous-space stochastic systems with unknown dynamics against safety specifications. Our approach is based on the notion of barrier certificate and uses sampled trajectories of the unknown system. We first casted the computation of the barrier certificate as a robust convex program (RCP) and approximated its solution with a scenario convex program (SCP) by replacing the unknown dynamics with the sampled trajectories. We then established that the optimal solution of the SCP gives a feasible solution for the RCP with a given confidence, and formulated a lower bound on the required number of samples. Our approach provided a lower bound on the safety probability of the stochastic unknown system when the number of sampled data is larger than a specific lower bound that depends on the desired confidence. We extended the results to a class of non-convex barrier-based safety problems and showed the applicability of our proposed approach using three case studies.

Appendix A. Lipschitz continuity of the max function

Lemma A.1. *The maximum of Lipschitz continuous functions $f_i : X \to \mathbb{R}$, $i = 1, 2, \ldots, m$, is a Lipschitz continuous function. The Lipschitz constant of the maximum is the sum of the Lipschitz constants of f_i.*

Proof. Suppose that two Lipschitz continuous functions f_1 and f_2 have Lipschitz constants L_1 and L_2, respectively. One can rewrite $g = \max(f_1, f_2)$ as:

$$g = \max(f_1, f_2) = \frac{f_1 + f_2 + |f_1 - f_2|}{2}.$$

Then, we can use triangle inequality to show that

$$\begin{aligned} |g(x) - g(y)| &\leq \frac{1}{2}[|f_1(x) - f_1(y)| + |f_2(x) - f_2(y)| + \\ &\quad \big||f_1(x) - f_2(x)| - |f_1(y) - f_2(y)|\big|] \\ &\leq \frac{1}{2}[L_1\|x - y\| + L_2\|x - y\| + |f_1(x) - f_1(y)| + \\ &\quad |f_2(x) - f_2(y)|] \leq \frac{1}{2}[L_1\|x - y\| + L_2\|x - y\| + \\ &\quad L_1\|x - y\| + L_2\|x - y\|] = (L_1 + L_2)\|x - y\|. \end{aligned}$$

Therefore, $\max(f_1, f_2)$ is also a Lipschitz continuous function with Lipschitz constant $L_1 + L_2$. This argument can be extended inductively to the maximum of every number of functions. □

Lemma A.2. *For any two analytic functions $f_1 : X \to \mathbb{R}$ and $f_2 : X \to \mathbb{R}$ with a compact domain X, $L := \max(L_1, L_2)$ is a Lipschitz constant of $\max(f_1, f_2)$.*

Proof. Note that

$$g(x) = \max(f_1(x), f_2(x)) = \begin{cases} f_1(x) & \text{if } f_1(x) - f_2(x) \geq 0 \\ f_2(x) & \text{if } f_1(x) - f_2(x) \leq 0. \end{cases}$$

Table 1
Conservativeness of the proposed approach.

Number of samples	Computed ϵ	$L_{x,u}G^{-1}(\epsilon)$	$\mathcal{K}^*_{\rho=0.2}(\mathcal{D})$	$\mathcal{K}^*_{\rho=0.1}(\mathcal{D})$	$\mathcal{K}^*_{\rho=0.2}(\mathcal{D})+L_{x,u}G^{-1}(\epsilon)$	$\mathcal{K}^*_{\rho=0.1}(\mathcal{D})+L_{x,u}G^{-1}(\epsilon)$
10^3	0.026	9.5	−0.48	−0.45	9.02	9.05
10^4	0.003	3	−0.42	0.09	2.58	3.09
10^5	2.61×10^{-4}	0.952	−0.43	1.37	0.522	2.32
1.5×10^6	1.74×10^{-5}	0.246	−0.41	2.08	−0.164	2.33
3×10^6	8.71×10^{-6}	0.174	−0.35	2.09	−0.176	2.26

The function f_1-f_2 is also analytic, thus has a finite number of zeros in a compact domain. Let us denote the finite set of zeros as Z. We first show this for one-dimensional compact domains $X\subset\mathbb{R}$. Take two points $x,y\in X$ such that $x<y$, and define $Z\cap[x,y]=\{z_1,z_2,\dots,z_m\}$ such that $z_i<z_{i+1}$ for any $i=1,2,\dots,m-1$. Then we have

$$\begin{aligned}|g(y)-g(x)| = |&f_{i_y}(y)-f_{i_m}(z_m)+f_{i_m}(z_m)-f_{i_{m-1}}(z_{m-1})+\cdots\\ &+f_{i_2}(z_2)-f_{i_1}(z_1)+f_{i_1}(z_1)\\ &-f_{i_x}(x)|,\end{aligned}$$

for some appropriate choices of $i_x,i_y,i_1,\dots,i_m$ all from the set $\{1,2\}$. Since $g(z_j)=f_1(z_j)-f_2(z_j)=0$, we can set the index of f to symbol that belongs to the set $\{1,2\}$ when the function is evaluated at any z_j. Then, we have

$$\begin{aligned}&|g(y)-g(x)|\\ &=|f_{i_y}(y)-f_{i_y}(z_m)+f_{i_m}(z_m)-f_{i_m}(z_{m-1})+\cdots+\\ &f_{i_2}(z_2)-f_{i_2}(z_1)+f_{i_x}(z_1)-f_{i_x}(x)|\le\\ &|f_{i_y}(y)-f_{i_y}(z_m)|+|f_{i_m}(z_m)-f_{i_m}(z_{m-1})|+\cdots+\\ &|f_{i_2}(z_2)-f_{i_2}(z_1)|+|f_{i_x}(z_1)-f_{i_x}(x)|\\ &\le L_{i_y}(y-z_m)+L_{i_m}(z_m-z_{m-1})+\cdots+\\ &L_{i_2}(z_2-z_1)+L_{i_x}(z_1-x)\\ &L(y-z_m)+L(z_m-z_{m-1})+\cdots+L(z_2-z_1)+L(z_1-x)\\ &=L(y-x),\end{aligned}$$

where $L=\max(L_1,L_2)=\max(L_{i_y},L_{i_x},L_{i_1},\dots,L_{i_m})$. This concludes the proof for one-dimensional case.

We now prove the statement for multi-dimensional case. Take two points $x,y\in X\subset\mathbb{R}^n$ with $x=(x_1,\dots,x_n)$ and $y=(y_1,\dots,y_n)$. The functions f_1,f_2 have Lipschitz constants L_1,L_2, which means

$$|f_i(y_1,\dots,y_n)-f_i(x_1,\dots,x_n)|\le L_i\|(y_1-x_1,\dots,y_n-x_n)\|,\quad i\in\{1,2\}. \tag{A.1}$$

Define the line segment that connects these two points as $D:=\{\lambda y+(1-\lambda)x\mid\lambda\in[0,1]\}$. Let us know restrict the domain of the function g to D and define:

$$\begin{aligned}&h:[0,1]\to\mathbb{R},\quad h(\lambda):=g(\lambda y+(1-\lambda)x)=\\ &\max(f_1(\lambda y+(1-\lambda)x),f_2(\lambda y+(1-\lambda)x)).\end{aligned}$$

We can now apply the first part of the proof to get:

$$|h(1)-h(0)|\le L'|1-0|, \tag{A.2}$$

where L' is the maximum of the Lipschitz constants of $f_1(\lambda y+(1-\lambda)x)$ and $f_2(\lambda y+(1-\lambda)x)$ with respect to λ. To get these Lipschitz constants, we use (A.1):

$$\begin{aligned}&|f_i(\lambda_1 y+(1-\lambda_1)x)-f_i(\lambda_2 y+(1-\lambda_2)x)|\le\\ &L_i\|(\lambda_1-\lambda_2)(y-x)\|=L_i|\lambda_1-\lambda_2|\,\|y-x\|\\ &=(L_i\|y-x\|)\,|\lambda_1-\lambda_2|\end{aligned}$$

Therefore, the Lipschitz constants of $f_1(\lambda y+(1-\lambda)x)$ for a given x,y with respect to λ is $L_i\|y-x\|$. Replacing definitions in (A.2), we have

$$|g(y)-g(x)|\le L'=\max(L_1\|y-x\|,L_2\|y-x\|)=\|y-x\|\max(L_1,L_2).$$

This completes the proof. □

Appendix B. Proof of Corollary 4.5

The probability distribution from which x_i is sampled must satisfy Assumption 4.2. This assumption requires having a strictly increasing function $G:\mathbb{R}_0^+\to[0,1]$ that satisfies

$$\mathbb{P}[\mathrm{b}(x,r)]\ge G(r),\qquad\forall x\in X.$$

Since we assume that samples are collected uniformly, $\mathbb{P}[\mathrm{b}(x,r)]$ for every small ball centered at every $x\in X$ with radius $r=\epsilon$ can be computed by dividing the volume of this ball by the whole state set volume. Given that one needs to find the maximum ball that is valid for $\forall x\in X$, and some points x lie on the border of the hyper-rectangular state set, the maximum ball is a semi-hypersphere in general, whose volume can be computed as $\frac{1}{2^n}\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\epsilon^n$ with the Gamma function defined as $\Gamma(k)=1\times2\times3\dots\times(k-1)$ and $\Gamma(k+\frac12)=\frac12\times\frac32\times\cdots(k-\frac32)(k-\frac12)\pi^{\frac12}$ for all positive integers. Dividing this value by the whole state set volume, which is $\prod_{i=1}^n\eta_x(i)$ for $\eta_x(i)$ as the length of the edges in each direction, gives us $G(\epsilon)$.

Appendix C. Proof of Corollary 4.6

The proof is similar to the proof of Corollary 4.5 in Appendix B. Here, the centered ball with the maximum volume is the intersection of the whole state set sphere and the small ball $r=\epsilon$ centered at any point on the border of the state set sphere. The volume of this intersection, which is the volume of two separate caps, can be computed as:

$$V_n^{cap}(\tilde r,\mathrm{c}_1)+V_{\mathrm{n}}^{\mathrm{cap}}(\epsilon,\mathrm{c}_2),$$

where

$$V_n^{cap}(\tilde r,\mathrm{c}_1)=\frac12\frac{\pi^{\frac{\mathrm{n}}{2}}}{\Gamma(\frac{\mathrm{n}}{2}+1)}\tilde r^{\mathrm{n}}\mathrm{I}(1-\frac{\mathrm{c}_1^2}{\tilde r^2};\frac{\mathrm{n}+1}{2},\frac12),$$

and

$$V_n^{cap}(\epsilon,\mathrm{c}_2)=\frac12\frac{\pi^{\frac{\mathrm{n}}{2}}}{\Gamma(\frac{\mathrm{n}}{2}+1)}\epsilon^{\mathrm{n}}\mathrm{I}(1-\frac{\mathrm{c}_2^2}{\epsilon^2};\frac{\mathrm{n}+1}{2},\frac12),$$

for $\mathrm{c}_1=\frac{2\tilde r^2-\epsilon^2}{2\tilde r}$, and $\mathrm{c}_2=\frac{\epsilon^2}{2\tilde r}$. By dividing the intersection volume by the volume of the whole hypersphere state set, which is

$$V_n(\tilde r)=\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)}\tilde r^n,$$

one can compute $G(\epsilon)$ as in Corollary 4.6.

Appendix D. Coefficients of the computed barrier certificates in floating point format with 16 digits.

In the above table, the values in first two columns from top to the bottom are $\{b_0,\dots,b_9\}$ in respective case studies. The values in the third column from top to the bottom are $\{b_0,\dots,b_4\}$ in the last case study (see Table D.1).

Table D.1
Computed coefficient values for the BCs in the case studies.

Temperature verification for 3 rooms	Lane keeping System	Synthesizing a Controller
$1.118824712343290 \times 10^{-1}$	$2.200050812923097 \times 10^{-4}$	$1.189325015407815 \times 10$
$1.121295401333170 \times 10^{-1}$	$3.901846347425760 \times 10^{-1}$	$-1.070392322770013 \times 10^{3}$
$1.122576531449860 \times 10^{-1}$	$1.480240596483330 \times 10^{-1}$	$3.612276124685787 \times 10^{4}$
$-3.751401155407000 \times 10^{-3}$	$-2.825312554914731 \times 10^{-4}$	$-5.417521260597183 \times 10^{5}$
$-4.728480781000000 \times 10^{-3}$	$9.905388481691000 \times 10^{-3}$	$3.046603167514221 \times 10^{6}$
$-2.284303936564000 \times 10^{-3}$	$-6.672383448890000 \times 10^{-3}$	–
$-3.761231117922648 \times 10^{0}$	$-6.918249590565419 \times 10^{-4}$	–
$-3.815332731044874 \times 10^{0}$	$4.678025224577894 \times 10^{-4}$	–
$-3.803570830339135 \times 10^{0}$	$-1.539512818952500 \times 10^{-2}$	–
$9.993049903406006 \times 10$	$4.518033593474370 \times 10^{-1}$	–

References

Abate, Alessandro, Ahmed, Daniele, Giacobbe, Mirco, & Peruffo, Andrea (2020). Formal synthesis of Lyapunov neural networks. *IEEE Control Systems Letters*, *5*(3), 773–778.

Althoff, Matthias, Koschi, Markus, & Manzinger, Stefanie (2017). CommonRoad: Composable benchmarks for motion planning on roads. In *2017 IEEE intelligent vehicles symposium (IV)* (pp. 719–726). IEEE.

Andersen, Erling D., & Andersen, Knud D. (2000). The MOSEK interior point optimizer for linear programming: an implementation of the homogeneous algorithm. In *High performance optimization* (pp. 197–232). Springer.

Baier, Christel, & Katoen, Joost-Pieter (2008). *Principles of model checking*. MIT Press.

Belta, Calin, Yordanov, Boyan, & Gol, Ebru Aydin (2017). *Formal methods for discrete-time dynamical systems, Vol. 15*. Springer.

Berberich, Julian, Köhler, Johannes, Muller, Matthias A., & Allgower, Frank (2020). Data-driven model predictive control with stability and robustness guarantees. *IEEE Transactions on Automatic Control*.

Borrmann, Urs, Wang, Li, Ames, Aaron D., & Egerstedt, Magnus (2015). Control barrier certificates for safe swarm behavior. *IFAC-PapersOnLine*, *48*(27), 68–73.

Calafiore, Giuseppe C., & Campi, Marco C. (2006). The scenario approach to robust control design. *IEEE Transactions on Automatic Control*, *51*(5), 742–753.

Clark, Andrew (2021). Control barrier functions for stochastic systems. *Automatica*, *130*, Article 109688.

Coulson, Jeremy, Lygeros, John, & Dörfler, Florian (2020). Distributionally robust chance constrained data-enabled predictive control. arXiv:2006.01702.

Dawson, Charles, Qin, Zengyi, Gao, Sicun, & Fan, Chuchu (2022). Safe nonlinear control using robust neural lyapunov-barrier functions. In *Conference on robot learning* (pp. 1724–1735). PMLR.

Esfahani, Peyman Mohajerin, Sutter, Tobias, & Lygeros, John (2014). Performance bounds for the scenario approach and an extension to a class of non-convex programs. *IEEE Transactions on Automatic Control*, *60*(1), 46–58.

Girard, Antoine (2005). Reachability of uncertain linear systems using zonotopes. In *International workshop on hybrid systems: Computation and control* (pp. 291–305). Springer.

Girard, Antoine, Gössler, Gregor, & Mouelhi, Sebti (2016). Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control*, *61*(6), 1537–1549.

Grant, Michael, & Boyd, Stephen (2014). CVX: Matlab software for disciplined convex programming, version 2.1. http://cvxr.com/cvx.

Han, Shuo, Topcu, Ufuk, & Pappas, George J. (2015). A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems. In *54th IEEE conference on decision and control (CDC)* (pp. 2049–2054).

Hernández, M. A. (2001). Chebyshev's approximation algorithms and applications. *Computers & Mathematics with Applications*, *41*(3–4), 433–445.

Jagtap, Pushpak, Pappas, George J., & Zamani, Majid (2020). Control barrier functions for unknown nonlinear systems using Gaussian processes. arXiv:2010.05818.

Jagtap, Pushpak, Soudjani, Sadegh, & Zamani, Majid (2020). Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, *66*(7), 3097–3110.

Kanamori, Takafumi, & Takeda, Akiko (2012). Worst-case violation of sampled convex programs for optimization with uncertainty. *Journal of Optimization Theory and Applications*, *152*(1), 171–197.

Kenanian, Joris, Balkan, Ayca, Jungers, Raphael M., & Tabuada, Paulo (2019). Data driven stability analysis of black-box switched linear systems. *Automatica*, *109*, Article 108533.

Kesten, Yonit, Pnueli, Amir, & Raviv, Lion (1998). Algorithmic verification of linear temporal logic specifications. In *International colloquium on automata, languages, and programming* (pp. 1–16). Springer.

Kushner, Harold J. (1967). *Stochastic stability and control: Technical report*, Providence RI: Brown Univ.

Lahijanian, M., Andersson, S. B., & Belta, C. (2015). Formal verification and synthesis for discrete-time stochastic systems. *IEEE Transactions on Automatic Control*, *60*(8), 2031–2045.

Majumdar, Rupak, Mallik, Kaushik, & Soudjani, Sadegh (2020). Symbolic controller synthesis for Büchi specifications on stochastic systems. In *Proceedings of the 23rd international conference on hybrid systems: Computation and control* (pp. 1–11).

Majumdar, Rupak, Salamati, Mahmoud, & Soudjani, Sadegh (2023). Neural abstraction-based controller synthesis and deployment. *ACM Transactions on Embedded Computing Systems*, *22*(5s), 1–25.

Murali, Vishnu, Trivedi, Ashutosh, & Zamani, Majid (2022). A scenario approach for synthesizing k-inductive barrier certificates. *IEEE Control Systems Letters*, *6*, 3247–3252.

Nejati, Ameneh, Lavaei, Abolfazl, Jagtap, Pushpak, Soudjani, Sadegh, & Zamani, Majid (2021). Formal verification of unknown discrete- and continuous-time systems:A data-driven approach. submitted for publication.

Niu, Luyao, Zhang, Hongchao, & Clark, Andrew (2021). Safety-critical control synthesis for unknown sampled-data systems via control barrier functions. In *2021 60th IEEE conference on decision and control (CDC)* (pp. 6806–6813). IEEE.

Plambeck, Swantje, Fey, Görschwin, & Schyga (2022). Decision tree models of continuous systems. In *27th international conference on emerging technologies and factory automation (ETFA)*. IEEE.

Prajna, Stephen, & Jadbabaie, Ali (2004). Safety verification of hybrid systems using barrier certificates. In *International workshop on hybrid systems: Computation and control* (pp. 477–492). Springer.

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

Robey, Alexander, Hu, Haimin, Lindemann, Lars, Zhang, Hanwen, Dimarogonas, Dimos V., Tu, Stephen, et al. (2020). Learning control barrier functions from expert demonstrations. arXiv:2004.03315.

Robey, Alexander, Lindemann, Lars, Tu, Stephen, & Matni, Nikolai (2021). Learning robust hybrid control barrier functions for uncertain systems. *IFAC-PapersOnLine*, *54*(5), 1–6.

Sadraddini, Sadra, & Belta, Calin (2018). Formal guarantees in data-driven model identification and control synthesis. In *Proceedings of the 21st international conference on hybrid systems: Computation and control (Part of CPS week)* (pp. 147–156).

Salamati, Ali, Soudjani, Sadegh, & Zamani, Majid (2020). Data-driven verification under signal temporal logic constraints. In *21st IFAC world congress*.

Sloth, Christoffer, Pappas, George J., & Wisniewski, Rafael (2012). Compositional safety analysis using barrier certificates. In *Proceedings of the 15th ACM international conference on hybrid systems: Computation and control* (pp. 15–24).

Soudjani, Sadegh, & Abate, Alessandro (2013). Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes. *SIAM Journal on Applied Dynamical Systems*, *12*(2), 921–956.

Soudjani, Sadegh, Abate, Alessandro, & Majumdar, Rupak (2015). Dynamic Bayesian networks as formal abstractions of structured stochastic processes. In *26th international conference on concurrency theory* (pp. 169–183). Schloss Dagstuhl.

Soudjani, Sadegh, Gevaerts, Caspar, & Abate, Alessandro (2015). FAUST 2: Formal abstractions of uncountable-state stochastic processes. In *21st international conference on tools and algorithms for the construction and analysis of systems (TACAS 2015)*. Newcastle University.

Soudjani, Sadegh, & Majumdar, Rupak (2018). Concentration of measure for chance-constrained optimization. *IFAC-PapersOnLine*, *51*(16), 277–282.

Svoreňová, Mária, Křetínský, Jan, Chmelík, Martin, Chatterjee, Krishnendu, Černá, Ivana, & Belta, Calin (2017). Temporal logic control for stochastic linear systems using abstraction refinement of probabilistic games. *Nonlinear Analysis. Hybrid Systems*, *23*, 230–253.

Swikir, Abdalla, & Zamani, Majid (2019). Compositional synthesis of symbolic models for networks of switched systems. *IEEE Control Systems Letters*, *3*(4), 1056–1061.

Tabuada, Paulo (2009). *Verification and control of hybrid systems: A symbolic approach*. Springer.

Tabuada, Paulo, & Fraile, Lucas (2020). Data-driven stabilization of SISO feedback linearizable systems. arXiv preprint arXiv:2003.14240.

Verband der Automobilindustrie (2020). Lane keeping assist systems. https://www.vda.de/en/topics/safety-and-standards/lkas/lane-keeping-assist-systems.html.

Wang, Li, Ames, Aaron D., & Egerstedt, Magnus (2017). Safety barrier certificates for collisions-free multirobot systems. *IEEE Transactions on Robotics*, *33*(3), 661–674.

Wang, Zheming, & Jungers, Raphaël M. (2019). Data-driven computation of invariant sets of discrete time-invariant black-box systems. arXiv:1907.12075.

Wijesuriya, Viraj Brian, & Abate, Alessandro (2019). Bayes-adaptive planning for data-efficient verification of uncertain Markov decision processes. In *International conference on quantitative evaluation of systems* (pp. 91–108). Springer.

Wood, G. R., & Zhang, B. P. (1996). Estimation of the Lipschitz constant of a function. *Journal of Global Optimization*, *8*(1), 91–103.

Yang, Zhengfeng, Wu, Min, & Lin, Wang (2020). An efficient framework for barrier certificate generation of uncertain nonlinear hybrid systems. *Nonlinear Analysis. Hybrid Systems*, *36*, Article 100837.

Zamani, Majid, & Arcak, Murat (2018). Compositional abstraction for networks of control systems: A dissipativity approach. *IEEE Transactions on Control of Network Systems*, *5*(3), 1003–1015.

Zamani, Majid, Esfahani, Peyman Mohajerin, Majumdar, Rupak, Abate, Alessandro, & Lygeros, John (2014). Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, *59*(12), 3135–3150.

Zamani, Majid, Tkachev, Ilya, & Abate, Alessandro (2017). Towards scalable synthesis of stochastic control systems. *Discrete Event Dynamic Systems*, *27*(2), 341–369.

Zhang, Lijun, She, Zhikun, Ratschan, Stefan, Hermanns, Holger, & Hahn, Ernst Moritz (2010). Safety verification for probabilistic hybrid systems. In *International conference on computer aided verification* (pp. 196–211). Springer.

Ali Salamati is a senior consultant at Autonomous Reply in Munich, Germany. His Ph.D. research focused on machine learning, artificial intelligence, model-based, and data-driven methods for ensuring the safety and performance of cyber–physical systems, including autonomous systems. During his Ph.D., he received the ADHS Best Repeatability Prize in 2021 for developing the code for the conference version of the current paper. He earned his bachelor's degree in electronics from Shiraz University and his master's degree in control engineering from K.N. Toosi University of Technology.

From an industrial perspective, his experience includes conducting engineering tests to determine subsystem parameters and constructing overall models in more than 30 major power plants. He also has experience of leading teams of engineering scientists and technicians and dealing with regulatory authorities. Furthermore, he designed and built an advanced battery management system for the National Energy Research Institute (NRI), with applications in electric vehicles. In this project, he served as the project manager and lead engineer.

Abolfazl Lavaei is an Assistant Professor in the School of Computing at Newcastle University, United Kingdom. Between January 2021 and July 2022, he was a Postdoctoral Associate in the Institute for Dynamic Systems and Control at ETH Zurich, Switzerland. He was also a Postdoctoral Researcher in the Department of Computer Science at LMU Munich, Germany, between November 2019 and January 2021. He received the Ph.D. degree in Electrical Engineering from the Technical University of Munich (TUM), Germany, in 2019. He obtained the M.Sc. degree in Aerospace Engineering with specialization in Flight Dynamics and Control from the University of Tehran, Iran, in 2014. His line of research focuses mainly on theoretical and practical aspects of "formal verification, learning and control of large-scale stochastic cyber–physical systems" with application to "autonomous systems". He is the recipient of several international awards in the acknowledgment of his work including ADHS Best Repeatability Prize 2021, HSCC Best Demo/Poster Awards 2020 and 2022, IFAC Young Author Award Finalist 2019, and Best Graduate Student Award 2014 at University of Tehran.

His research interests revolve around the intersection of Control Theory, Computer Science, Artificial Intelligence and Data Science.

Sadegh Soudjani is an Associate Professor in the School of Computing at Newcastle University, United Kingdom, and a Group Leader at the Max Planck Institute for Software Systems, Germany. He is also the Director of the AMBER Group at Newcastle University. He received the B.Sc. degrees in mathematics and electrical engineering, and the M.Sc. degree in control engineering from the University of Tehran, Tehran, Iran, in 2007 and 2009, respectively. He received the Ph.D. degree in Systems and Control in November 2014 from the Delft Center for Systems and Control at the Delft University of Technology, Delft, the Netherlands. Before joining Newcastle University, he was a postdoctoral researcher at the department of Computer Science, University of Oxford, United Kingdom, and at the Max Planck Institute for Software Systems, Germany. He is the recipient of the DISC Best Ph.D. Thesis Award in 2015, QEST Best Paper Award in 2018, Newcastle Teaching Award in 2020, New Investigator Award from the UK EPSRC Research Council in 2021, and the ERC Consolidator Grant in 2023.

His research interests are formal model-based and data-driven synthesis, abstraction, and verification of complex dynamical systems with application in Cyber–Physical Systems, particularly involving smart grids and energy networks.

Majid Zamani is an Associate Professor in the Computer Science Department at the University of Colorado Boulder, USA. He also holds a guest professorship in the Computer Science Department at the Ludwig Maximilian University of Munich. He earned a B.Sc. degree in Electrical Engineering in 2005 from Isfahan University of Technology, Iran, and completed an M.Sc. degree in Electrical Engineering in 2007 from Sharif University of Technology, Iran. In 2012, he received an MA degree in Mathematics and a Ph.D. degree in Electrical Engineering from the University of California, Los Angeles, USA. Between September 2012 and December 2013, he conducted postdoctoral research at the Delft Center for Systems and Control, Delft University of Technology, Netherlands From May 2014 to January 2019, he was an Assistant Professor in the Department of Electrical and Computer Engineering at the Technical University of Munich, Germany. Additionally, from December 2013 to April 2014, he held an Assistant Professor position in the Design Engineering Department at Delft University of Technology, Netherlands. He received the NSF Career award in 2022 and ERC starting grant award from the European Research Council in 2018.

His research interests span verification and control of hybrid systems, embedded control software synthesis, networked control systems, and incremental properties of nonlinear control systems.