Formal Verification of Unknown Discrete- and Continuous-Time Systems: A Data-Driven Approach

Ameneh Nejati, *Student Member, IEEE*, Abolfazl Lavaei, *Senior Member, IEEE*, Pushpak Jagtap, *Member, IEEE*, Sadegh Soudjani, *Member, IEEE*, and Majid Zamani, *Senior Member, IEEE*

***Abstract*—This article is concerned with a formal verification scheme for both discrete- and continuous-time deterministic systems with unknown mathematical models. The main target is to verify the safety of unknown systems based on the construction of barrier certificates via a set of data collected from trajectories of systems while providing an a-priori guaranteed confidence on the safety. In our proposed framework, we first cast the original safety problem as a robust convex program (RCP). Solving the proposed RCP is not tractable in general since the unknown model appears in one of the constraints. Instead, we collect finite numbers of data from trajectories of the system and provide a scenario convex program (SCP) corresponding to the original RCP. We then establish a probabilistic closeness between the optimal value of SCP and that of RCP, and as a result, we formally quantify the safety guarantee of unknown systems based on the number of data points and a required level of confidence. We propose our framework in both discrete-time and continuous-time settings. We illustrate the effectiveness of our proposed results by first applying them to an unknown continuous-time room temperature system. We verify that the temperature of the room maintains in a comfort zone with some desirable confidence by collecting data from trajectories of the system. To show the applicability of our techniques to *higher dimensional* systems with *nonlinear* dynamics, we then apply our results to a continuous-time *nonlinear* jet engine compressor and a discrete-time DC motor.**

***Index Terms*—Data-driven barrier certificates, discrete-time and continuous-time systems, formal safety verification, robust convex program, scenario convex program.**

Manuscript received 9 April 2022; accepted 11 February 2023. Date of publication 10 March 2023; date of current version 26 April 2023. This work was supported in part by the National Science Foundation under Grant CNS-2145184, in part by the UKRI EPSRC New Investigator Award CodeCPS under Grant EP/V043676/1, and in part by the SERB Start-up Research under Grant SRG/2022/001807. Recommended by Senior Editor Tetsuya Iwasaki and Guest Editors George J. Pappas, Anuradha M. Annaswamy, Manfred Morari, Claire J. Tomlin, Rene Vidal, and Melanie N. Zeilinger. *(Corresponding author: Ameneh Nejati.)*

Ameneh Nejati is with the Electrical Engineering Department, Technical University of Munich, Munich, Germany, and also with the Computer Science Department, Ludwig Maximilian University of Munich, 80539 Munich, Germany (e-mail: amy.nejati@tum.de).

Abolfazl Lavaei and Sadegh Soudjani are with the School of Computing, Newcastle University, Newcastle upon Tyne NE4 5TG, U.K. (e-mail: abolfazl.lavaei@newcastle.ac.uk; sadegh.soudjani@newcastle.ac.uk).

Pushpak Jagtap is with the Robert Bosch Center for Cyber-Physical Systems, Indian Institute of Science, Bangalore 560012, India (e-mail: pushpak@iisc.ac.in).

Majid Zamani is with the Computer Science Department, University of Colorado Boulder, Boulder, CO 80309 USA (e-mail: majid.zamani@colorado.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TAC.2023.3255141.

Digital Object Identifier 10.1109/TAC.2023.3255141

I. Introduction

MOTIVATIONS. In the past few years, formal methods have been becoming a promising approach to analyze dynamical systems against high-level logic properties, e.g., those expressed as linear temporal logic (LTL) formulae [1], in a reliable way. Since the closed-form solution of many dynamical systems with continuous state spaces is not available in general, formal analysis of those complex systems is naturally very challenging mainly due to their computational complexity arising from uncountable sets of states and actions, especially in many safety-critical applications.

To mitigate the encountered computational complexity, one potential solution, proposed in the relevant literature, is to approximate original models by simpler ones with finite state sets (i.e., finite abstractions) [2]. However, the major bottleneck of finite-abstraction techniques is their dependency to the state and input discretization parameters and consequently suffering from the curse of dimensionality: the computational complexity exponentially grows as the dimension of the system increases. To alleviate this issue, compositional techniques have been introduced in the past few years to construct finite abstractions of interconnected systems based on abstractions of smaller subsystems [3], [4], [5], [6], [7], [8], [9], [10].

Although the proposed compositional techniques in the setting of finite abstractions can mitigate the effects of the state-explosion problem, the curse of dimensionality may still exist at the subsystem level given the range of state and input sets and their quantization parameters. These challenges motivate the need to employ *barrier certificates* as a discretization-free approach for formal analysis of complex dynamical systems. In particular, barrier certificates are Lyapunov-like functions defined over the state space of the system satisfying a set of inequalities on both the function itself and the one-step transition (or the time derivative along the flow) of the system. In the state

0018-9286 © 2023 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

space, an appropriate level set of a barrier certificate separates an unsafe region from all system trajectories starting from a given set of initial states. Consequently, the existence of such a function provides a formal certificate for the safety of the system [11], [12], [13], [14], [15], [16], [17], [18], [19].

To employ the proposed discretization-based and -free approaches in the abovementioned literature, one needs to know precise models of dynamical systems to construct those finite abstractions or barrier certificates and, hence, the proposed approaches in the relevant literature are not applicable in the settings where the model is unknown. In particular, closed-form mathematical models for many physical systems are either not available or equally complex to be of any practical use, and accordingly, one cannot employ model-based techniques to analyze them. Although there are some results, in the related literature, to solve various analysis and synthesis problems by learning approximate models via identification techniques (see [20], [21], [22], [23], [24], [25], [26]), acquiring an accurate model for complex systems is always very challenging, time-consuming, and expensive. This critical challenge motivated us to develop a direct data-driven approach to bypass the system identification phase and directly construct barrier certificates using data collected from trajectories of systems.

Related literature: In the past few years, there have been some results in the setting of data-driven optimization techniques. *Scenario approach* has been initially introduced in [27] to deal with semi-infinite convex programming for robust control analysis and synthesis problems. The main benefit of the proposed approach is that the solvability of the problem can be obtained through random sampling of constraints provided that a probabilistic relaxation of the worst-case robust paradigm is accepted. As an extension of [27], a random convex program framework is developed in [28] in which the results provide an explicit bound on the upper tail probability of violation. The proposed setup is then generalized to the case of random convex programs with posteriori violated constraints to improve the optimal objective value while maintaining the violation probability under control. A novel framework for establishing a probabilistic bridge from optimal values of scenario convex programs to those of robust convex and chance-constrained programs is initially proposed in [29] in which the uncertainty takes values in a general, possibly infinite-dimensional, metric space. The results are then generalized to a certain class of nonconvex problems that includes binary decision variables.

An approximation bridge from the infinite-dimensional linear programming to tractable finite convex programs is developed in [30] in which the performance of the approximation is quantified explicitly. The proposed results are based on the randomized optimization and first-order methods, leading to priori as well as posteriori performance guarantees. The scenario-based optimization techniques have been also used for the controller design in [31]. The proposed results in [31] only relate optimal values of scenario and chance-constrained programs, and accordingly, provide guarantees over chance-constrained programs. In contrast, we transfer here the safety guarantees over the original robust program (which is the main problem in our setting) but at the cost of taking into account the Lipschitz constant of the system, and consequently, requiring more sampled data. The work in [32] proposes a specification-based simulation metric to synthesize a controller from an abstraction of the system, which is learned from data. In contrast, we propose here a data-driven approach to directly provide a formal guarantee over the safety of unknown systems without performing any system identification.

There have been also some results, proposed in the past few years, in the context of formal analysis of dynamical systems via data-driven approaches. A data-driven stability analysis of black-box linear switched systems is proposed in [33] in which a stability-like guarantee is provided based on both the number of observations and the required level of confidence. As an extension of [33], a data-driven computation of invariant sets of discrete time-invariant black-box systems is proposed in [34]. Under the assumption that the system is asymptotically stable, the maximal invariant set coincides with the domain of attraction. The authors in [35] applied a data-enabled predictive control algorithm to unknown stochastic linear time-invariant systems. In particular, the noise-corrupted input/output data is employed to predict future trajectories and compute optimal control policies. A data-driven verification approach for partially known dynamics with nondeterministic inputs and noisy observations is proposed in [36].

Reinforcement learning schemes to synthesize policies for Markov decision processes (MDPs) with formal guarantees are studied in [37] and [38] for finite state sets and in [39] and [40] for continuous ones. The proposed scheme in [39] enables one to apply model-free, off-the-shelf reinforcement learning algorithms to compute near-optimal strategies for continuous-space MDPs without explicitly constructing their finite abstractions while providing approximate optimality guarantees. The works [41], [42] propose optimization-based frameworks to learn control barrier certificates from data for the systems with *known* dynamics and under the assumption of accessibility of safe trajectories generated by an expert. In contrast to our setting, we develop data-driven approaches to guarantee safety of systems with unknown mathematical dynamics. The work in [43] provides a neural PDE solver-based reachability analysis tool for high-dimensional systems, but without providing any formal guarantee.

Contributions: The main contribution of this work is to provide a data-driven scheme for the construction of barrier certificates for the safety verification of discrete- and continuous-time deterministic systems with unknown mathematical models. In our proposed settings, we first formulate our original safety problem as a robust convex program (RCP). Since the formulated RCP is not tractable due to unknown dynamics, we consider a given set of data collected from the system and provide a scenario convex program (SCP) corresponding to the original RCP. Accordingly, by establishing a probabilistic closeness between the optimal value of SCP and that of RCP, we quantify the safety guarantee of unknown systems based on the number of data and the required level of the safety confidence. In order to establish a probabilistic relation between optimal values of SCP and RCP, we first raise some Lipschitz continuity assumptions over RCP's conditions. We provide some explicit approaches to compute the required Lipschitz constants. To demonstrate the effectiveness

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

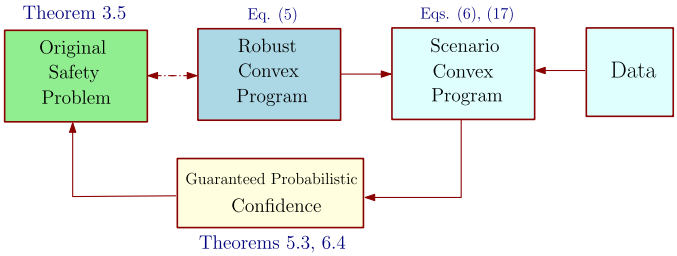

Fig. 1. Graphical representation of the article's structure and contributions.

of the proposed results, we apply our approaches to the following three case studies with unknown dynamics:

i) continuous-time room temperature system;
ii) continuous-time *nonlinear* jet engine compressor;
iii) discrete-time DC motor.

We utilize data collected from trajectories of systems and verify that states of unknown systems stay in some safe sets with an a-priori desired confidence. It should be noted that Lipschitz constant of dynamics and an upper bound on unknown dynamics are the minimal information we need from the system in our data-driven setting. In Appendix A, we present an approach to estimate the Lipschitz constant of dynamics via sampled data. As for an upper bound on unknown dynamics for discrete-time systems, it can be readily computed based on the range of the state set. In the continuous-time setting, to the best of authors' knowledge, there exists no result in the relevant literature to estimate an upper bound for unknown dynamics based on data. In fact, this bound is on the rate of change of the system states and can be chosen conservatively based on the application domain. A graphical representation of the structure of this article and its contributions is illustrated in Fig. 1.

Organization: The rest of this article is organized as follows. Section II is dedicated to *discrete-time* dynamical systems including mathematical notations and the problem description. Section III gives the formal definition of barrier certificates. In Section IV, we reformulate our original problem as an RCP and then present a data-driven scheme for the construction of barrier certificates via collected data by solving the corresponding SCP. We establish a probabilistic closeness between the optimal values of SCP and RCP, and accordingly, provide safety guarantees over unknown systems with an a-priori guaranteed confidence in Section V. Section VI is dedicated to *continuous-time* dynamical systems and their corresponding details. We illustrate the effectiveness of our proposed results by applying them to three (physical) systems with unknown dynamics in Section VII. Finally, Section VIII concludes this article. We provide the proofs of all the statements in the Appendix to increase the readability of our work.

II. Discrete-Time Dynamical Systems

A. Notations

The following notations are utilized throughout this article. Sets of nonnegative and positive integers are denoted by $\mathbb{N} := \{0, 1, 2, \ldots\}$ and $\mathbb{N}_{\geq 1} := \{1, 2, 3, \ldots\}$, respectively. Moreover, symbols $\mathbb{R}$, $\mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote, respectively, sets of real, positive, and nonnegative real numbers. We use $\mathbb{R}^n$ to denote an n-dimensional Euclidean space and $\mathbb{R}^{n\times m}$ to denote the space of real matrices with n rows and m columns. Given any $a \in \mathbb{R}$, $|a|$ denotes the absolute value of a. We denote by $\|x\|$ the Euclidean norm of $x \in \mathbb{R}^n$. For any matrix $P \in \mathbb{R}^{m\times n}$, we have $\|P\| := \sqrt{\lambda_{\max}(P^\top P)}$, where $\lambda_{\max}(\cdot)$ is the maximum eigenvalue. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}_{\geq 1}$, and $i \in \{1, \ldots, N\}$, we use $x = [x_1; \ldots; x_N]$ to denote the corresponding column vector of the dimension $\sum_i n_i$. We denote the indicator function of a subset $\mathcal{A}$ of a set X by $\mathbf{1}_{\mathcal{A}} : X \to \{0, 1\}$, where $\mathbf{1}_{\mathcal{A}}(x) = 1$ if and only if $x \in \mathcal{A}$, and 0 otherwise. We denote the spectral radius of a matrix $P \in \mathbb{R}^{n\times n}$ by $\rho(P)$, which is defined as $\rho(P) = \max\{|\lambda_1|, \ldots, |\lambda_n|\}$, where $\lambda_1, \ldots, \lambda_n$ are eigenvalues of matrix P. Given a probability space $(\mathcal{D}, \mathbb{B}(\mathcal{D}), \mathbb{P})$, we denote by $\mathcal{D}^N$ the N-Cartesian product of set $\mathcal{D}$, and by $\mathbb{P}^N$ its corresponding product measure. We denote the factorial of a nonnegative integer n by $n!$ as the product of all positive integers less than or equal to n, i.e., $n! = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1$. Gamma function is defined as $\Gamma(n) = (n-1)!$ for any positive integer n and $\Gamma(n + \frac{1}{2}) = (n - \frac{1}{2}) \times (n - \frac{3}{2}) \times \cdots \times \frac{1}{2} \times \pi^{\frac{1}{2}}$ for any nonnegative integer n. We also define the regularized incomplete beta function [28] as

$$\mathcal{I} : (c, a, b) \mapsto \mathcal{I}(c, a, b) = \frac{\int_0^c \mathsf{t}^{a-1}(1-\mathsf{t})^{b-1}\mathsf{dt}}{\int_0^1 \mathsf{t}^{a-1}(1-\mathsf{t})^{b-1}\mathsf{dt}} \quad \forall a, b, c \in \mathbb{R}_{>0}.$$

B. Discrete-Time Dynamical Systems

In this work, we consider discrete-time dynamical systems as defined in the following.

Definition 2.1: A discrete-time dynamical system (dt-S) is represented by

$$\Sigma_d : x(k+1) = f(x(k)), \quad k \in \mathbb{N} \tag{1}$$

where $x : \mathbb{N} \to X$ is the *state evolution* of Σ_d, $X \subseteq \mathbb{R}^n$ is the state set of the system, and $f : X \to X$ is a function characterizing the state evolution of the system. We employ $x_{x_0}(k)$ to denote the value of the state evolution at time $k \in \mathbb{N}$ started from an initial condition $x_0 = x(0)$.

In the following section, we provide a formal definition of barrier certificates for dt-S as shown in (1).

III. Barrier Certificates

In this section, we define a notion of barrier certificates for dt-S in (1), adapted from [11], as formalized in the following definition.

Definition 3.1: Consider a dt-S Σ_d, and $X_0, X_u \subseteq X$ as initial and unsafe sets, respectively. A function $\mathcal{B} : X \to \mathbb{R}$ is called a barrier certificate (BC) for Σ_d over a time horizon $[0, \mathcal{T})$ if there exist $c \in \mathbb{R}_{\geq 0}$ and $\gamma, \lambda \in \mathbb{R}$, such that $\gamma + c\mathcal{T} < \lambda$, and

$$\mathcal{B}(x) \leq \gamma, \qquad \forall x \in X_0 \tag{2}$$

$$\mathcal{B}(x) \geq \lambda, \qquad \forall x \in X_u \tag{3}$$

$$\mathcal{B}(f(x)) \leq \mathcal{B}(x) + c, \qquad \forall x \in X. \tag{4}$$

As seen in Definition 3.1, barrier certificates are defined over the state space of the system enforcing a set of inequalities on

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

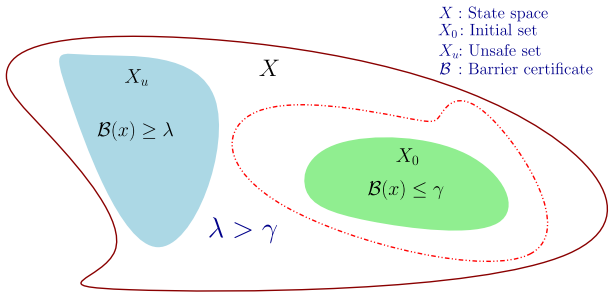

Fig. 2. A barrier certificate for a dynamical system with $c = 0$. The (red) dashed line denotes the level set $\mathcal{B}(x) = \gamma$.

both the function itself [i.e., conditions (2) and (3)] and its one-step transition [i.e., condition (4)]. An appropriate level set of a BC (i.e., γ) separates an unsafe region (i.e., X_u here) from all system trajectories starting from a given set of initial states (i.e., X_0 here). A barrier certificate for discrete-time systems with $c = 0$ is schematically depicted in Fig. 2. It is worth mentioning that one can utilize similar conditions as proposed in Definition 3.1 and synthesize safety controllers for control systems via notions of *control* barrier certificates. We refer the interested readers to [44] for more details.

Remark 3.2: Note that X_0 and X_u should not intersect in order to enforce the safety property in Definition 3.1. In particular, since we enforce $\gamma + c\mathcal{T} < \lambda$, this condition implies that $\gamma < \lambda$, which implicitly implicates that there is no intersection between sets X_0 and X_u based on conditions (2) and (3).

Remark 3.3: Note that since $\gamma + c\mathcal{T} < \lambda$ in Definition 3.1, one can readily see that $\mathcal{T} < \frac{\lambda-\gamma}{c}$, i.e., time horizon $\mathcal{T}$ converges to infinity once c goes to zero.

In the following definition, we present the safety problem for the dt-S Σ_d.

Definition 3.4: Given a safety specification $\varphi = (X_0, X_u, \mathcal{T})$, where $X_0, X_u \subseteq X$ with $X_0 \cap X_u = \emptyset$, and $\mathcal{T} \in \mathbb{N} \cup \{\infty\}$, and a dt-S, Σ_d is called safe within (in)finite time horizon $\mathcal{T}$, denoted by $\Sigma_d \models_{\mathcal{T}} \varphi$, if all trajectories of Σ_d started from the initial set $X_0 \subseteq X$ never reach the unsafe set $X_u \subseteq X$.

We present the following theorem, adapted from [45], to show the usefulness of BC for verifying the safety of dt-S as in Definition 3.4.

Theorem 3.5: Let Σ_d be a dt-S. Suppose $\mathcal{B}$ is a BC for Σ_d as in Definition 3.1. Then, one has $x_{x_0}(k) \notin X_u$, for any $x_0 \in X_0$ and any $k \in [0, \mathcal{T})$, where $\mathcal{T} \leq \frac{\lambda-\gamma}{c}$.

In order to provide a formal guarantee for the safety of the system in (1), knowing the precise map f is essential to check condition (4) in Definition 3.1. In the following section, we assume that we do not have any information about the model (i.e., map f) and develop a data-driven scheme for the construction of BCs using a finite set of data collected from trajectories of the system.

IV. Data-Driven Construction of BC

In this section, we assume that the transition map f in (1) is unknown. Given that the Lipschitz constant of f and an upper bound on unknown f are required in our data-driven setting, we employ the term *(partially) unknown* to refer to this type of models. The main goal is to verify the safety of the unknown system in (1) by constructing a BC using data. In our setting, we take two consecutive data-points from trajectories of the system as the pair of $(x(k), x(k+1))$ and denote it by $(\hat{x}, f(\hat{x}))$. We also fix the structure of BCs as $\mathcal{B}(q, x) = \sum_{j=1}^{z} q_j \bar{p}_j(x)$ with some user-defined (possibly nonlinear) basis functions $\bar{p}_j(x)$ and unknown coefficients $q = [q_1; \ldots; q_z] \in \mathbb{R}^z$. For instance, in the case of polynomial-type BCs, basis functions $\bar{p}_j(x)$ are monomials over x.

In order to enforce conditions (2)–(4) in Definition 3.1, we first cast our problem as the following robust convex program (RCP):

$$\text{RCP}: \begin{cases} \min\limits_{[d;\eta]} & \eta \\ \text{s.t.} & \max_j \{g_j(x,d)\} \leq \eta, j \in \{1,\ldots,4\}, \quad \forall x \in X \\ & d = [\gamma; \lambda; c; q_1; \ldots; q_z] \\ & \eta, \gamma, \lambda \in \mathbb{R},\ c \in \mathbb{R}_{\geq 0} \end{cases} \tag{5}$$

where

$$\begin{aligned} g_1(x,d) &= (\mathcal{B}(q,x) - \gamma)\mathbf{1}_{X_0}(x) \\ g_2(x,d) &= (-\mathcal{B}(q,x) + \lambda)\mathbf{1}_{X_u}(x) \\ g_3(x,d) &= \gamma + c\mathcal{T} - \lambda - \mu \\ g_4(x,d) &= \mathcal{B}(q, f(x)) - \mathcal{B}(q,x) - c \end{aligned}$$

for some $\mu < 0$, and with $\mathbf{1}_{X_0}(x)$ and $\mathbf{1}_{X_u}(x)$ being indicator functions acting on initial and unsafe sets, respectively. Note that we employ $\mu < 0$ in condition g_3 to ensure $\gamma < \lambda$ when $c = 0$. We denote the optimal value of RCP by η_R^*. If $\eta_R^* \leq 0$, a solution to the RCP implies the satisfaction of conditions (2)–(4) in Definition 3.1.

Remark 4.1: Note that we modified conditions (2)–(4) of Definition 3.1 in the RCP in (5) by adding η to their right-hand side. We accordingly defined η as the objective function of the RCP. Later, we provide our solution to the safety verification of the (partially) unknown system by establishing a probabilistic relation between the optimal value of RCP (i.e., η_R^*) and that of its corresponding scenario convex program (SCP), which is defined next.

To solve the proposed RCP in (5), one needs to know the precise map f, which is unknown in our setting. This critical challenge motivated us to develop a direct data-driven approach by proposing a scenario convex program of RCP. Let $(\hat{x}_i)_{i=1}^N$ denote $N \in \mathbb{N}_{\geq 1}$ independent and identically distributed data sampled within X. Instead of solving the RCP in (5), we rather solve the following scenario convex program (SCP):

$$\text{SCP}: \begin{cases} \min\limits_{[d;\eta]} & \eta \\ \text{s.t.} & \max_j\{g_j(x,d), g_4(\hat{x}_i,d)\} \leq \eta, j \in \{1,2,3\} \\ & \forall x \in X, \quad \forall \hat{x}_i \in X, \quad \forall i \in \{1,\ldots,N\} \\ & d = [\gamma; \lambda; c; q_1; \ldots; q_z] \\ & \eta, \gamma, \lambda \in \mathbb{R},\ c \in \mathbb{R}_{\geq 0} \end{cases} \tag{6}$$

where g_1–g_4 are the functions defined in (5). One can readily see that $f(\hat{x}_i)$ in $\mathcal{B}(q, f(\hat{x}_i))$ in g_4 can be substituted by measuring

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

the unknown dt-S after one-step evolution starting from $\hat{x}_i$. We denote the optimal value of SCP by η_N^*.

Remark 4.2: Notice that conditions g_1 and g_2 in SCP (6) should be satisfied for any $x \in X_0, x \in X_u$, respectively. Condition g_4 is the only one which is satisfied based on data since the unknown model is only appeared in g_4.

In the following section, we establish a probabilistic closeness guarantee between the optimal value of SCP (i.e., η_N^*) and that of RCP (i.e., η_R^*), and accordingly, verify the safety of (partially) unknown systems with an a-priori guaranteed confidence bound.

V. Safety Guarantee Over Unknown Systems

In this section, inspired by the fundamental results in [29], we aim at establishing a formal relation between the optimal value of SCP in (6) and that of RCP in (5). Accordingly, we formally quantify the safety guarantee of (partially) unknown systems based on the number of data and a required level of confidence. We state the main problem considered in this article.

Problem 5.1: Consider a (partially) unknown dt-S Σ_d as in Definition 2.1 and a safety specification $\varphi = (X_0, X_u, \mathcal{T})$ as in Definition 3.4. Construct a BC by solving the SCP in (6) based on collected data to provide a formal guarantee on the satisfaction of the safety specification φ within the time horizon $\mathcal{T}$ with an a-priori confidence bound $\beta \in [0,1]$, i.e.,

$$\mathbb{P}^N \{\Sigma_d \models_{\mathcal{T}} \varphi\} \geq 1 - \beta.$$

To address Problem 5.1, we first raise the following assumption.

Assumption 5.2: Suppose $g_4(x,d)$ is Lipschitz continuous with respect to x with the Lipschitz constant $\mathscr{L}_g$.

Under Assumption 5.2, the following theorem, adapted from [29], establishes a bridge between the optimal values of SCP in (6) and that of the original RCP in (5), and accordingly provides a mechanism to verify the safety of the unknown system.

Theorem 5.3: Consider a (partially) unknown dt-S as in (1), and initial and unsafe regions X_0 and X_u, respectively. Let Assumption 5.2 hold. Consider the corresponding SCP in (6) with its associated optimal value η_N^* and solution $d^* = [\gamma^*; \lambda^*; c^*; q_1^*; \ldots; q_z^*]$, with an arbitrary number of samples $N \in \mathbb{N}_{\geq 1}$ and $\beta \in [0,1]$. Then, the following statement holds with a confidence of at least $1-\beta$: if

$$\eta_N^* + \mathscr{L}_g \kappa^{-1}(\varepsilon) \leq 0 \tag{7}$$

with

$$\varepsilon \geq \mathcal{I}^{-1}(1-\beta, \bar{z}, N - \bar{z} + 1) \tag{8}$$

where $\bar{z}$ is the number of decision variables, $\mathcal{I}$ is the regularized incomplete beta function [28], and $\kappa(r) : \mathbb{R}_{\geq 0} \to [0,1]$, which depends on the sampling distribution and the geometry of the uncertainty set X, then the unknown dt-S is safe in the sense of Theorem 3.5 within the time horizon $\frac{\lambda^* - \gamma^*}{c^*}$.

Remark 5.4: As discussed in [29, Prop. 3.8], the function κ in (7) satisfies the following inequity:

$$\kappa(r) \leq \mathbb{P}\left[\mathbb{B}_r(x)\right], \qquad \forall r \in \mathbb{R}_{\geq 0}, \quad \forall x \in X \tag{9}$$

where $\mathbb{B}_r(x) \subset X$ is an open ball centered at x with radius r. In the case of collecting samples with a *uniform* distribution from an n-dimensional *hyper-rectangular* uncertainty set, the function κ in (9) is computed as

$$\kappa(r) = \frac{\text{Vol}(\mathbb{B}_r(x))}{2^n \text{Vol}(X)} = \frac{\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2}+1)} r^n}{2^n \text{Vol}(X)} = \frac{\pi^{\frac{n}{2}} r^n}{2^n \Gamma(\frac{n}{2}+1) \text{Vol}(X)} \tag{10}$$

where $\pi \approx 3.14$, $\text{Vol}(\cdot)$ is the volume of the set, and Γ is the Gamma function. Note that $1/2^n$ in (10) is needed for the computation of $\mathbb{P}[\mathbb{B}_r(x)]$ when the sampled data are located in the corner of the uncertainty set X. If one collects samples with a uniform distribution from a *rectangular uncertainty set* in $\mathbb{R}^2$ with edges of length a and b, the function κ in (10) is reduced to $\kappa(r) = \frac{\pi r^2}{4ab}$ (cf. case studies).

Remark 5.5: In the case of collecting samples with a *uniform* distribution from an n-dimensional *hyper-spherical* uncertainty set with radius $\bar{r}$, the function κ in (9) is computed as

$$\kappa(r) = \frac{\bar{r}^n \int_0^{c_1} \mathsf{t}^{\frac{n-1}{2}} (1-\mathsf{t})^{-\frac{1}{2}} \mathsf{dt} + r^n \int_0^{c_2} \mathsf{t}^{\frac{n-1}{2}} (1-\mathsf{t})^{-\frac{1}{2}} \mathsf{dt}}{2\bar{r}^n \int_0^1 \mathsf{t}^{\frac{n-1}{2}} (1-\mathsf{t})^{-\frac{1}{2}} \mathsf{dt}} \tag{11}$$

where $c_1 = 1 - \frac{(2\bar{r}^2 - r^2)^2}{4\bar{r}^4}$ and $c_2 = 1 - \frac{r^2}{4\bar{r}^2}$. We refer the interested readers to [46] for the computation of κ for other shapes of uncertainty sets with different types of sample distributions.

Remark 5.6: Note that since our dynamical system in this work is nonstochastic, the probabilistic confidence bound in Theorem 5.3 is due to data collected from the system, i.e., by increasing data, the confidence improves. If the unknown system is stochastic, then the provided guarantee consists of two layers of probabilities: the inner layer is regarding the stochasticity in the system and the outer layer is due to data similar to our setting. In this case, one also has a confidence on the probability of satisfaction (see [35]).

Remark 5.7: Note that the minimum number of data in (8) required for solving SCP (6) is exponential with respect to the dimension of unknown systems. However, the main benefit of the results in Theorem 5.3 compared to system identification is that the proposed data-driven technique here is capable of providing safety guarantees for *any type of nonlinear systems, which are Lipschitz continuous*, whereas system identification approaches are mainly tailored to linear or some particular classes of nonlinear systems. In addition, even if one is able to find a model using system identification techniques, one still needs to search for a BC. In this case, one suffers from the computational complexity in both identifying the model as well as searching for a BC based on it. It is worth mentioning that one can leverage the so-called wait-and-judge approach proposed in [47] to reduce the required number of data in (8) for

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

some applications. In particular, the wait-and-judge approach in [47] computes the threshold ε a-posteriori, and accordingly, the worst-case exponential computational complexity will not usually happen in practice.

In order to provide a safety certificate over the original unknown system via Theorem 5.3, we propose Algorithm 1 to describe the required procedure.

Algorithm 1: Safety Guarantee Over (Partially) Unknown dt-S.

1: Select a-priori $N \in \mathbb{N}_{\geq 1}, \beta \in [0,1]$ as desired
2: Compute ε as in (8)
3: Solve the SCP (6) with the desired N and obtain η_N^*
4: If $\eta_N^* + \mathscr{L}_g \kappa^{-1}(\varepsilon) \leq 0$, then the safety of the unknown dynamical system is guaranteed with a confidence of at least $1-\beta$
5: Otherwise, inconclusive: one cannot judge the safety of the system, given parameters N and β

To the best of our knowledge, this work is the first to provide safety verification for dynamical systems with unknown mathematical models using the results in [29]. Providing such a safety certificate using [29] was not straightforward. In particular, there is no objective function involved in searching for BCs in Definition 3.1. In order to utilize the results in [29], we *artificially* defined an objective function based on a value η. We then related the optimal value of RCP (which is unknown) to that of SCP (which can be computed by collecting data) and provided the safety certificate for the unknown system with an a-priori confidence bound as long as $\eta_N^* + \mathscr{L}_g \kappa^{-1}(\varepsilon) \leq 0$.

In order to check condition (7) in Theorem 5.3, one needs to first compute $\mathscr{L}_g$. Although there exists a general approach in [29, Prop. 3.8] to compute the Lipschitz constant $\mathscr{L}_g$, we propose in the following lemma an explicit way to compute $\mathscr{L}_g$ for the choice of quadratic BCs and linear dynamics.

Lemma 5.8: Consider a linear dt-S of the form $x(k+1) = Ax(k)$ with $A \in \mathbb{R}^{n\times n}$. Assume that $\|A\| \leq \mathscr{L}_f$, where $\mathscr{L}_f$ is the Lipschitz constant of the system as in (18). Then, $\mathscr{L}_g$ in Assumption 5.2 for a quadratic BC of the form $x^T P x$, with a symmetric matrix $P \in \mathbb{R}^{n\times n}$, is computed as $\mathscr{L}_g = 2v\rho(P)(\mathscr{L}_f^2 + 1)$, where ρ is the spectral radius, and v is an upper bound on the norm of the state vector, i.e., $\|x\| \leq v$ for any $x \in X$.

Remark 5.9: Note that one needs to know an upper bound for $\rho(P)$ in order to check condition (7) in Theorem 5.3. The pre-assumed upper bound should be then enforced as an additional condition while solving the SCP (6) as mentioned in Step 3 of Algorithm 1. Note also that the required conditions for enforcing $\rho(P) \leq \bar{v}$ may result in nonlinear constraints in SCP (6). To resolve this issue, we enforce those conditions as linear bounds on entries of the matrix P using Gershgorin circle theorem [48] (cf. case studies).

Remark 5.10: If the underlying dynamics are nonlinear in the form of (1), one can still employ a similar reasoning as Lemma 5.8 and compute $\mathscr{L}_g = 2\rho(P)(\mathcal{M}_f \mathscr{L}_f + v)$ by assuming that $\|f(x)\| \leq \mathcal{M}_f$ and $\|\frac{\partial f(x)}{\partial x}\| \leq \mathscr{L}_f$ for any $x \in X$.

In order to compute $\mathscr{L}_g$ as in Lemma 5.8, one needs to know an upper bound for $\|A\|$, which is actually the Lipschitz constant of the dynamic (i.e., $\mathscr{L}_f$) in the linear case. To do so, one can assume the model is fully unknown and estimate the Lipschitz constant of dynamics using a finite number of data collected from trajectories of the system, as described in Appendix A.

In the following sections, we tailor the previous results for continuous-time dynamical systems.

VI. Continuous-Time Dynamical Systems

In this section, we consider a continuous-time dynamical system as formalized in the following definition.

Definition 6.1: A continuous-time dynamical system (ct-S) ia described as

$$\Sigma_c : \dot{x}(t) = f(x(t)) \tag{12}$$

where $x : \mathbb{R}_{\geq 0} \to X$ is the *state trajectory* of Σ_c, $X \subseteq \mathbb{R}^n$ is the state set of the system, and $f : X \to \mathbb{R}^n$ is the vector field. We employ $x_{x_0}(t)$ to denote the value of the state trajectory at time $t \in \mathbb{R}_{\geq 0}$ under the initial condition $x_0 = x(0)$. In order to ensure the existence and uniqueness of the state trajectory, we consider some regularity assumptions on the vector field f as discussed in [49].

We present the notion of barrier certificates for ct-S in (12) in the following definition.

Definition 6.2: Consider a ct-S Σ_c in (12), and $X_0, X_u \subseteq X$ as, respectively, initial and unsafe sets of the system. A continuously differentiable function $\mathcal{B} : X \to \mathbb{R}$ is called a barrier certificate (BC) for Σ_c if there exist $c \in \mathbb{R}_{\geq 0}$ and $\gamma, \lambda \in \mathbb{R}$, with $\gamma + c\mathcal{T} < \lambda$, such that conditions (2), (3) are satisfied, and

$$\mathsf{L}_f \mathcal{B}(x) \leq c, \quad \forall x \in X \tag{13}$$

where $\mathsf{L}_f \mathcal{B}$ is the *Lie derivative* of $\mathcal{B} : X \to \mathbb{R}$ with respect to the vector field f, and is defined as

$$\mathsf{L}_f \mathcal{B}(x) = \partial_x \mathcal{B}(x) f(x). \tag{14}$$

We similarly recast conditions of the BC as the proposed RCP in (5), where

$$g_4(x,d) = \mathsf{L}_f \mathcal{B}(q,x) - c. \tag{15}$$

Similar to the first part of this article, we are interested in employing the proposed SCP in (6) instead of solving the RCP in (5). However, one still needs to know the map f to enforce condition g_4 in (15). Note that condition g_4 in (15) cannot be directly acquired from collected data based on $f(\hat{x}_i)$. To tackle this issue, we approximate the Lie derivative of $\mathcal{B}$ with respect to f (i.e., $\mathsf{L}_f \mathcal{B}(q,x)$) appeared in g_4 as

$$\widehat{\mathsf{L}}_f \mathcal{B}(q,x) := \frac{\mathcal{B}(q,x_\tau) - \mathcal{B}(q,x)}{\tau}, \quad \forall x \in X \tag{16}$$

where x_τ is the solution of the unknown system after $\tau \in \mathbb{R}_{>0}$ units of time starting from x. The proposed approximation in (16) satisfies the following inequality:

$$|\widehat{\mathsf{L}}_f \mathcal{B}(q,x) - \mathsf{L}_f \mathcal{B}(q,x)| \leq \delta, \quad \forall x \in X$$

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

where δ is a positive constant and is formally quantified later in Section VI-A. Now, we propose another version of the SCP (6) as

$$\text{SCP}_\delta: \begin{cases} \min\limits_{[d;\eta]} \quad \eta \\ \text{s.t.} \quad \max\{g_j(x,d), \bar{g}_4(\hat{x}_i,d,\delta)\} \leq \eta, j\in\{1,2,3\} \\ \quad\quad \forall x\in X, \quad \forall \hat{x}_i \in X, \quad \forall i\in\{1,\ldots,N\} \\ \quad\quad d=[\gamma;\lambda;c;q_1;\ldots;q_z] \\ \quad\quad \eta,\gamma,\lambda\in\mathbb{R},\ c,\delta\in\mathbb{R}_{\geq 0} \end{cases} \tag{17}$$

where $\bar{g}_4(\hat{x}_i,d,\delta)=\widehat{\mathsf{L}}_f\mathcal{B}(q,\hat{x}_i)-c+\delta$.

We now state the main problem that we plan to solve in this section.

Problem 6.3: Consider a (partially) unknown ct-S Σ_c as in Definition 6.1 and a safety specification $\varphi=(X_0,X_u,\mathcal{T})$ as in Definition 3.4. Construct a BC by solving the SCP_δ in (17) based on collected data to provide a formal guarantee on the satisfaction of the safety specification φ within the time horizon $\mathcal{T}$ with an a-priori confidence bound $\beta\in[0,1]$, i.e.,

$$\mathbb{P}^N\{\Sigma_c \models_{\mathcal{T}} \varphi\} \geq 1-\beta.$$

To address Problem 6.3, we propose the following theorem, which establishes a bridge between optimal values of SCP_δ in (17) and that of original RCP in (5), and accordingly verifies the safety of the unknown system with an a-priori confidence bound.

Theorem 6.4: Consider a (partially) unknown ct-S as in (12), and initial and unsafe regions X_0 and X_u, respectively. Let Assumption 5.2 hold with g_4 as in (15). Consider the corresponding SCP_δ in (17) with its associated optimal value η_N^* and solution $d^*=[\gamma^*;\lambda^*;c^*;q_1^*;\ldots;q_z^*]$, with an arbitrary number of samples $N\in\mathbb{N}_{\geq 1}$ and $\beta\in[0,1]$. Then, the following statement holds with a confidence of at least $1-\beta$: if

$$\eta_N^*+\mathscr{L}_g\kappa^{-1}(\varepsilon)\leq 0$$

with ε as in (8) and $\kappa(r):\mathbb{R}_{\geq 0}\to[0,1]$, which depends on the sampling distribution and the geometry of the uncertainty set X, then the unknown ct-S in (12) is safe in the sense of Theorem 3.5 (but in the continuous-time setting) within time horizon $\frac{\lambda^*-\gamma^*}{c^*}$.

The proof of Theorem 6.4 is similar to that of Theorem 5.3 and is omitted here.

Similar to Lemma 5.8, we propose in the following lemma, an explicit way to compute $\mathscr{L}_g$ for ct-S for the choice of quadratic BCs and linear dynamics.

Lemma 6.5: For a linear ct-S $\dot{x}(t)=Ax(t)$ with $A\in\mathbb{R}^{n\times n}$, let the matrix A be bounded as $\|A\|\leq\mathscr{L}_f$, where $\mathscr{L}_f$ is the Lipschitz constant of the system as in (18). Then, $\mathscr{L}_g$ for a quadratic BC of the form x^TPx, with a symmetric matrix $P\in\mathbb{R}^{n\times n}$, is computed as $\mathscr{L}_g=4v\rho(P)\mathscr{L}_f$, where ρ is the spectral radius, and v is an upper bound on the norm of the state vector, i.e., $\|x\|\leq v$ for any $x\in X$.

Remark 6.6: If the underlying dynamics are nonlinear in the form of (12), one can still employ a similar reasoning as in Lemma 6.5 and compute the Lipschitz constant as $\mathscr{L}_g=2\rho(P)(\mathcal{M}_f+v\mathscr{L}_f)$ by assuming that $\|f(x)\|\leq\mathcal{M}_f$, and $\|\frac{\partial f(x)}{\partial x}\|\leq\mathscr{L}_f$ for any $x\in X$.

In the following section, we formally approximate the Lie derivative of the system (12), i.e., $\mathsf{L}_f\mathcal{B}(q,x)$, via $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ by providing its quantified closeness as δ.

A. Formal Approximation of Lie Derivative

In order to quantify the formal closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$, we first need to raise the following two assumptions.

Assumption 6.7: Suppose the vector field f and $\partial_x\mathcal{B}(q,x)$ are Lipschitz continuous with Lipschitz constants $\mathscr{L}_f$, $\mathscr{L}_\mathcal{B}\in\mathbb{R}_{\geq 0}$ as, $\forall x,x'\in X$,

$$\begin{aligned}&\|f(x)-f(x')\|\leq\mathscr{L}_f\|x-x'\|\\&\|\partial_x\mathcal{B}(q,x)-\partial_{x'}\mathcal{B}(q,x')\|\leq\mathscr{L}_\mathcal{B}\|x-x'\|.\end{aligned}\tag{18}$$

Assumption 6.8: Suppose the vector field f and $\partial_x\mathcal{B}(q,x)$ are bounded with constants $\mathcal{M}_f,\mathcal{M}_\mathcal{B}\in\mathbb{R}_{>0}$, as

$$\|f(x)\|\leq\mathcal{M}_f,\quad \|\partial_x\mathcal{B}(q,x)\|\leq\mathcal{M}_\mathcal{B}.$$

Remark 6.9: Since the structure of the barrier is considered as a linear combination of known basis functions, one can a-priori select $\mathscr{L}_\mathcal{B}$ and $\mathcal{M}_\mathcal{B}$ as some arbitrary numbers and enforce their corresponding conditions in Assumptions 6.7 and 6.8 as some additional constraints while solving SCP_δ (17) (cf. first two case studies).

We now employ Assumptions 6.7 and 6.8 and propose the next lemma to show that $\mathsf{L}_f\mathcal{B}(q,x)$ is also Lipschitz continuous.

Lemma 6.10: Under Assumptions 6.7 and 6.8, $\mathsf{L}_f\mathcal{B}(q,x)$ is Lipschitz continuous with a Lipschitz constant $\mathscr{L}$ as

$$|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')|\leq\mathscr{L}\|x-x'\|,\quad\forall x,x'\in X$$

where $\mathscr{L}=\mathcal{M}_\mathcal{B}\mathscr{L}_f+\mathcal{M}_f\mathscr{L}_\mathcal{B}$.

Now all the ingredients are ready to formally quantify the closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ as proposed in the following theorem.

Theorem 6.11: Let $\mathsf{L}_f\mathcal{B}(q,x)$ be the Lie derivative of $\mathcal{B}$ with respect to f and $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ be its approximation as in (16). Under Assumptions 6.7, 6.8, and using Lemma 6.10, one has

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)|\leq\frac{1}{2}\tau\mathscr{L}\mathcal{M}_f,\quad\forall x\in X$$

where τ is the sampling time, and $\mathscr{L}=\mathcal{M}_\mathcal{B}\mathscr{L}_f+\mathcal{M}_f\mathscr{L}_\mathcal{B}$.

Remark 6.12: Note that in order to provide a formal closeness between the Lie derivative of $\mathcal{B}$ and its corresponding approximation as in Theorem 6.11, we leverage the continuity properties of the solution process together with the continuity of f and $\mathsf{L}_f\mathcal{B}(q,x)$.

As seen in Theorem 6.11, one can control the closeness error between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,\hat{x}_i)$ by picking a small sampling time τ. This is also better for the precision of the approximation since a smaller sampling time provides a more precise approximation. We employ the following room temperature example to elaborate more on this issue.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

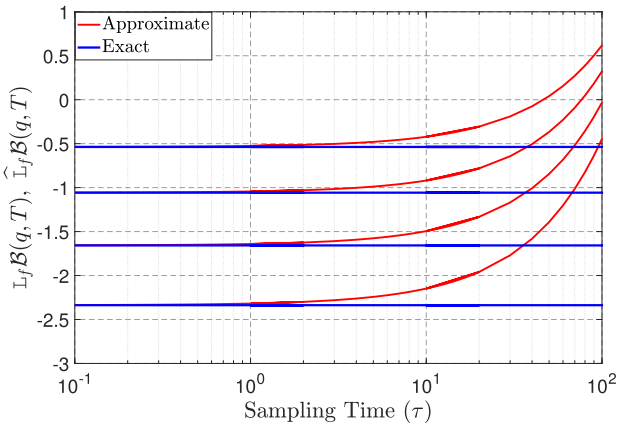

Fig. 3. Exact $\mathsf{L}_f\mathcal{B}(q,T)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ for different ranges of sampling time and four different initial conditions.

Room temperature: Consider a temperature regulation of a room with a model borrowed from [50]. The evolution of the temperature $T(\cdot)$ can be described by the following ct-S:

$$\Sigma_c : \dot{T}(t) = -\theta T(t) + \theta T_e \tag{19}$$

where $\theta = 0.005$ is the conduction factor between the external environment and the room, and $T_e = -20\,^\circ$C, is the outside temperature.

We fix a quadratic BC of the form $\mathcal{B}(q,T) = T^2 + 2\,T - 1$. Accordingly, one has

$$\mathsf{L}_f\mathcal{B}(q,T) = (2\,T + 2)(-\theta T(t) + \theta T_e) \tag{20}$$

which is obviously independent of the sampling time. The approximation of the Lie derivative in our setting based on (16) is $\widehat{\mathsf{L}}_f\mathcal{B}(q,T) = \frac{\mathcal{B}(q,T_\tau)-\mathcal{B}(q,T)}{\tau}$. If the model in (19) is known, its state trajectory is obtained as $Te^{-\theta\tau} - T_e(e^{-\theta\tau} - 1)$. Then, the approximate Lie derivative can be computed as

$$\begin{aligned}\widehat{\mathsf{L}}_f\mathcal{B}(q,T) = \big(&T^2(e^{-2\theta\tau}-1)+2T(e^{-\theta\tau}-1)+T_e^2(e^{-\theta\tau}-1)^2\\ &-2T_e(e^{-\theta\tau}-1)-2T_eTe^{-\theta\tau}(e^{-\theta\tau}-1)\big)/\tau.\end{aligned} \tag{21}$$

It can be readily shown that $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ in (21) converges to $\mathsf{L}_f\mathcal{B}(q,T)$ in (20) if the sampling time τ goes to zero. Since the model in our setting is unknown, we instead collect data and estimate $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ via (16). The exact Lie derivative and its approximation via collected data for different ranges of the sampling time starting from 4 different initial conditions are plotted in Fig. 3. As can be observed, the approximate $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ converges to the exact $\mathsf{L}_f\mathcal{B}(q,T)$ for all initial conditions when the sampling time goes to zero.

Remark 6.13: Although a smaller sampling time provides a smaller closeness error, we do not consider the numerical error originating from finite-precision computations in different computing platforms. In practice, this numerical precision imposes a lower bound over the sampling time and does not allow it to be very small.

In order to provide the closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ as in Theorem 6.11, the Lipschitz constant of the system $\mathscr{L}_f$ is needed (cf. Assumption 6.7). One can assume the model is fully unknown and instead estimate the Lipschitz constant of dynamics from collected data as described in Algorithm 2 in the Appendix with

$$s_i = \frac{\left\|\frac{(\hat{x}_{\tau_i}-\hat{x}_{0_i})-(\hat{y}_{\tau_i}-\hat{y}_{0_i})}{\tau}\right\|}{\|\hat{x}_{0_i}-\hat{y}_{0_i}\|}, \quad \forall i \in \{1,\dots,\bar{N}\}.$$

Remark 6.14: It is worth mentioning that we presented our results in this work for *deterministic* dynamical systems for the sake of providing a clearer presentation. However, our results here can be readily extended to *nondeterministic* dynamical systems with dynamics $x(k+1) = f(x(k), w(k))$ (resp. $\dot{x}(t) = f(x(t), w(t))$), where $w(k) \in W$ (resp. $w(t) \in W$) is a bounded disturbance with $W \subseteq \mathbb{R}^p$ being the disturbance set. In this case, the sample space is expanded to $X \times W$, and accordingly, $\kappa(r)$ in (7) is a function of order $n+p$, where p is the dimension of the disturbance set. In addition, g_4 in Assumption 5.2 should be Lipschitz continuous with respect to both x *and* w, which requires the recomputation of $\mathscr{L}_g$ in Lemma 5.8 and Remark 5.10 (resp. Lemma 6.5 and Remark 6.6 in the continuous-time setting).

VII. Case Studies

To illustrate the effectiveness of our proposed results, we first apply our results to a continuous-time room temperature system in (19). We verify that the temperature of the room with (partially) unknown dynamics maintains in a comfort zone with some desirable confidence by collecting data sampled from trajectories of the system. To show the applicability of our techniques to *higher dimensional* systems with *nonlinear* dynamics, we then apply our results to a continuous-time *nonlinear* jet engine compressor and a discrete-time DC motor. In all three case studies, we collect data from trajectories of unknown systems with a uniform distribution.

A. Continuous-Time Case

Room temperature: Consider the room temperature system in (19). The regions of interest for this example are $X = [17, 20]$, $X_0 = [17, 18]$, and $X_u = [19, 20]$. We assume that the model is unknown to us. The main goal is to construct a BC via data collected from trajectories of the system by solving SCP$_\delta$ (17) and accordingly verify if the temperature of the room stays within the comfort zone [17,19) according to Theorem 6.4 for infinite time horizons, i.e., $c = 0$.

We first fix the structure of our BC as $\mathcal{B}(q,x) = q_1x^2 + q_2x + q_3$. We now follow Algorithm 1 in order to utilize the results of Theorem 5.3. We first fix $N = 1005$ and $\beta = 10^{-7}$, a-priori. Since the Lipschitz constant $\mathscr{L}_f$ is required for computing $\mathscr{L}_g$ according to Lemma 5.8, we employ Algorithm 2 to estimate it from sampled data. By considering $\bar{N} = M = 1000$ and $\alpha = \tau = 0.01$, we get $\mathscr{L}_f = 0.005$ which is exactly equal to the Lipschitz constant of the actual dynamic. We now construct matrix P based on coefficients of the BC. By considering each coefficient of the barrier between $[-0.2, 0.2]$, we ensure that $\rho(P) \leq 0.4$ as discussed in Remark 5.9 and, accordingly, $\mathscr{L}_g = 12$. Given that the number of decision variables affects ε

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

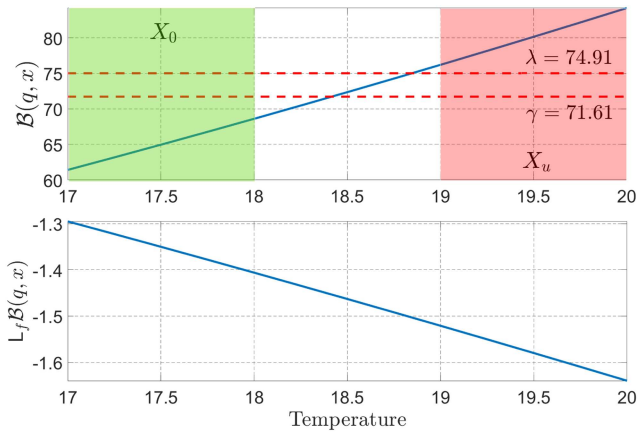

Fig. 4. Barrier certificate of unknown room temperature model. Note that the BC is quadratic and only a small segment of this function between [17, 20] is plotted here.

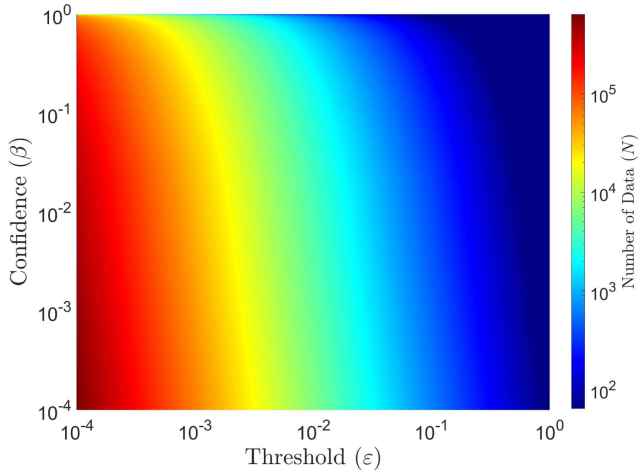

Fig. 5. Required number of data, represented by "color bar," in terms of the threshold ε and the confidence β. Plot is in the logarithmic scale for $\mathscr{L}_g = 12$ and 6 decision variables. The required number of data decreases by increasing either ε or β.

in (8), we fix $c = 0$ a-priori to reduce the number of decision variables to 6. We now compute ε in (8) as $\varepsilon = 0.0278$.

Now we need to compute δ as in Theorem 6.11, which is required for solving the SCP$_\delta$ (17) (i.e., condition $\bar{g}_4$). We assume $\mathcal{M}_f$ is given to us as 0.2. By employing ranges of coefficients of the barrier, we compute $\mathcal{M}_\mathcal{B} \leq 8.2$ and $\mathscr{L}_\mathcal{B} \leq 0.4$. By selecting $\tau = 0.01$, the closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ is computed as $\delta = 1.21 \times 10^{-4}$. Note that considering coefficients of barriers within $[-0.2, 0.2]$ enforces the additional conditions as

$$-0.2 \leq q_1, q_2, q_3 \leq 0.2 \tag{22}$$

that should be enforced in solving SCP$_\delta$ (17) as discussed in Remark 6.9. We now solve the SCP$_\delta$ (17) with $N = 1005, \delta = 1.21 \times 10^{-4}$, and the additional conditions in (22). Coefficients of the BC together with other decision variables of SCP$_\delta$ are computed as

$$\mathcal{B}(q,x) = 0.2x^2 + 0.2x + 0.2$$
$$\eta_N^* = -1.2952, \gamma^* = 71.6191, \lambda^* = 74.9146.$$

We now compute $\kappa(\varepsilon)$ according to Remark 5.4 as $\kappa(\varepsilon) = \frac{\varepsilon}{3}$. Since $\eta_N^* + \mathscr{L}_g\kappa^{-1}(\varepsilon) = -0.2960 \leq 0$, according to Theorem 6.4, one can guarantee that the temperature of the room with unknown dynamics remains in the safe set [17, 19] for an infinite-time horizon with a confidence of at least $1 - \beta = 1 - 10^{-7}$. The constructed BC from data is illustrated in Fig. 4.

In order to have a practical analysis on the required number of collected data in Theorem 5.3, we plotted in Fig. 5 the required number of data in terms of the threshold ε and the confidence β based on (8) for the room temperature problem. As can be observed, the required number of data decreases by increasing either ε or β. However, in practice, one needs to select β as small as possible to provide a reasonable safety confidence (i.e., $1 - \beta$) over the original unknown system. Besides, in order to ensure the safety of the unknown system with some confidence, condition $\eta_N^* + \mathscr{L}_g g^{-1}(\varepsilon) \leq 0$ needs to hold. Consequently, a smaller ε allows for larger optimal value η_N^*, and hence, conditions on the BC become more relaxed but at the cost of solving the SCP$_\delta$ in (17) with a higher number of data as illustrated in Fig. 5.

It is worth mentioning that by increasing the degree of BC, there is a higher chance of satisfying conditions g_1-g_4 but at the cost of considering a bigger ε in (8) given that the number of decision variables $\bar{z}$ also increases.

Jet engine: Consider the following *nonlinear* Moore-Greitzer jet engine model in no-stall mode [51]:

$$\Sigma_c : \begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix}$$

where $x_1 = \Phi - 1, x_2 = \Psi - \Lambda - 2$, with Φ, Ψ, Λ being, respectively, the mass flow, the pressure rise, and a constant. The regions of interest here are $X = [0.1, 1]^2, X_0 = [0.1, 0.5]^2$, and $X_u = [0.7, 1]^2$. We assume that the model is unknown. The main goal is to construct a BC via data collected from trajectories of the system by solving SCP$_\delta$ (17) and accordingly verify that $x(t) \in [0.1, 0.7)^2$ for infinite time horizons, i.e., $c = 0$.

We fix the structure of our BC as $\mathcal{B}(q,x) = q_1x_1 + q_2x_1x_2 + q_3x_2 + q_4$. We also fix $N = 257149$ and $\beta = 0.01$, a-priori. By employing Algorithm 2, we estimate $\mathscr{L}_f = 4.71$. We assume $\mathcal{M}_f$ is given to us as $\mathcal{M}_f = 3.16$. By constructing matrix P and considering each coefficient of the barrier between $[-0.4, 0.4]$, we compute $\rho(P) \leq 0.6$, and accordingly, $\mathscr{L}_g = 8.06$. We fix $\lambda = 3.1$ and $c = 0$ a-priori, to reduce the number of decision variables to 5. We now compute ε in (8) as $\varepsilon = 4.5127 \times 10^{-5}$. Now we need to compute δ as in Theorem 6.11. Considering ranges of coefficients of barriers between $[-0.4, 0.4]$, we compute $\mathcal{M}_\mathcal{B} \leq 1.13$ and $\mathscr{L}_\mathcal{B} \leq 0.8$. By selecting $\tau = 10^{-5}$, the closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ is computed as $\delta = 1.2438 \times 10^{-4}$. We now solve the SCP$_\delta$ (17) with $N = 257149, \delta = 1.2438 \times 10^{-4}$, and the additional conditions $-0.4 \leq q_1, q_2, q_3, q_4 \leq 0.4$. Coefficients of the BC together with decision variables in SCP$_\delta$ are computed as

$$\mathcal{B}(q,x) = 0.4x_1 + 0.4x_1x_2 - 0.0728x_2 + 2.7288$$

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

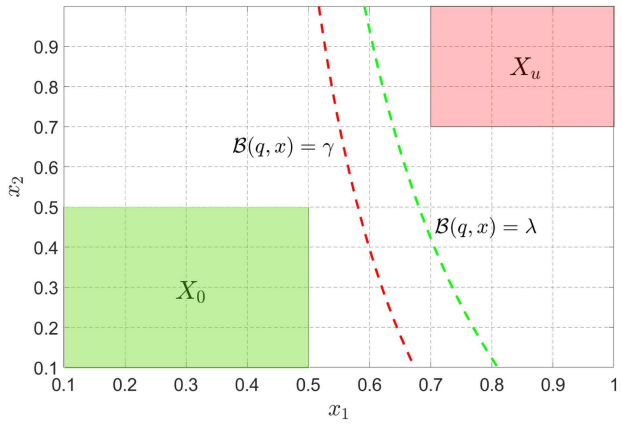

Fig. 6. *Jet engine:* Satisfaction of conditions (2) and (3). Initial set is inside the γ-level set of the BC (i.e., $\mathcal{B}(q,x)=\gamma$) and the unsafe set is outside the λ-level set of the BC (i.e., $\mathcal{B}(q,x)=\lambda$).

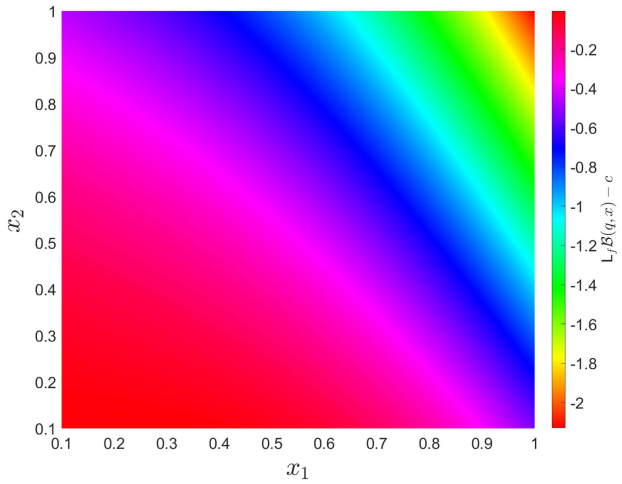

Fig. 7. *Jet engine:* Satisfaction of condition (13). This condition is nonpositive for all ranges of $x_1 \in [0.1, 1]$ and $x_2 \in [0.1, 1]$.

$$\eta_N^* = -0.0552, \gamma^* = 3.0455.$$

We now compute $\kappa(\varepsilon)$ according to Remark 5.4 as $\kappa(\varepsilon) = \frac{\pi}{3.24}\varepsilon^2$. Since $\eta_N^* + \mathscr{L}_g\kappa^{-1}(\varepsilon) = -2 \times 10^{-4} \leq 0$, according to Theorem 6.4, one can guarantee that $x(t) \in [0.1, 0.7)^2$ for all $t \in \mathbb{R}_{\geq 0}$ with a confidence of at least $1 - \beta = 99\%$.

Satisfaction of conditions (2) and (3), and (13) via constructed BC from data is illustrated in Figs. 6 and 7. As observed in Fig. 6, the initial set $X_0 = [0.1, 0.5]^2$ is inside the γ-level set of the BC (i.e., $\mathcal{B}(q,x) = \gamma$) and the unsafe set $X_u = [0.7, 1]^2$ is outside the λ-level set of the BC (i.e., $\mathcal{B}(q,x) = \lambda$). Moreover, in Fig. 7, condition (13) is nonpositive for all ranges of $x_1 \in [0.1, 1]$ and $x_2 \in [0.1, 1]$.

B. Discrete-Time Case

DC motor: Our third case study is a discrete-time dc motor adapted from [52] as follows:

$$x_1(k+1) = x_1(k) + \tau\Big(\frac{-R}{L}x_1(k) - \frac{k_{dc}}{L}x_2(k)\Big)$$

$$x_2(k+1) = x_2(k) + \tau\Big(\frac{k_{dc}}{J}x_1(k) - \frac{b}{J}x_2(k)\Big)$$

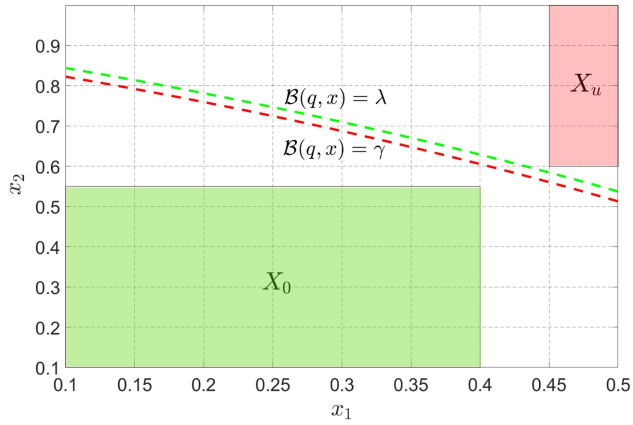

Fig. 8. *DC motor:* Satisfaction of conditions (2) and (3). As seen, the initial set is inside the γ-level set of the BC (i.e., $\mathcal{B}(q,x)=\gamma$) and the unsafe set is outside the λ-level set of the BC (i.e., $\mathcal{B}(q,x)=\lambda$).

where $x_1, x_2, R = 1, L = 0.01$, and $J = 0.01$ are the armature current, the rotational speed of the shaft, the electric resistance, the electric inductance, and the moment of inertia of the rotor, respectively. In addition, $\tau = 0.01, b = 1$, and $K_{\text{dc}} = 0.01$ represent, respectively, the sampling time, the motor torque, and the back electromotive force. The regions of interest here are $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, and $X_u = [0.45, 0.5] \times [0.6, 1]$. We assume that the model is unknown. The main goal is to construct a BC via collected data by solving SCP (6) and accordingly verify that $x \in [0.1, 0.45) \times [0.1, 0.6)$ for infinite time horizons, i.e., $c = 0$.

We fix the structure of our BC as $\mathcal{B}(q,x) = q_1x_1^2 + q_2x_1x_2 + q_3x_2^2 + q_4$. We follow Algorithm 1 in order to utilize the results of Theorem 5.3. We first fix $N = 82821$ and $\beta = 0.01$, a-priori. Now we employ Algorithm 2 and estimate Lipschitz constant of the system as $\mathscr{L}_f \leq 0.014$. By considering each coefficient of the barrier within $[-0.5, 0.5]$, we compute $\rho(P) \leq 0.75$, and accordingly, $\mathscr{L}_g = 1.67$. We fix $c = 0$ a-priori, to reduce the number of decision variables to 7. We now compute ε in (8) as $\varepsilon = 1.76 \times 10^{-4}$. We now solve the SCP (6) with $N = 82821$ and compute coefficients of the BC together with other decision variables as

$$\mathcal{B}(q,x) = 0.5x_1^2 + 0.5x_1x_2 + 0.5x_2^2 + 0.5$$

$$\eta_N^* = -0.0155, \gamma = 0.8882, \lambda = 0.9035.$$

We now compute $\kappa(\varepsilon)$ according to Remark 5.4 as $\kappa(\varepsilon) = \frac{\pi}{1.44}\varepsilon^2$. Since $\eta_N^* + \mathscr{L}_g\kappa^{-1}(\varepsilon) = -5 \times 10^{-4} \leq 0$, according to Theorem 5.3, one can guarantee that $x(k) \in x \in [0.1, 0.45) \times [0.1, 0.6)$ for all $k \in \mathbb{N}$ with a confidence of at least $1 - \beta = 99\%$.

Satisfaction of conditions (2)–(4) via constructed BC from data is illustrated in Figs. 8 and 9.

VIII. Discussion

In this work, we provided a data-driven scheme for the construction of barrier certificates for the safety verification of deterministic dynamical systems with unknown mathematical models in both discrete-time and continuous-time settings. We first cast our original safety problem as an a robust convex program

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

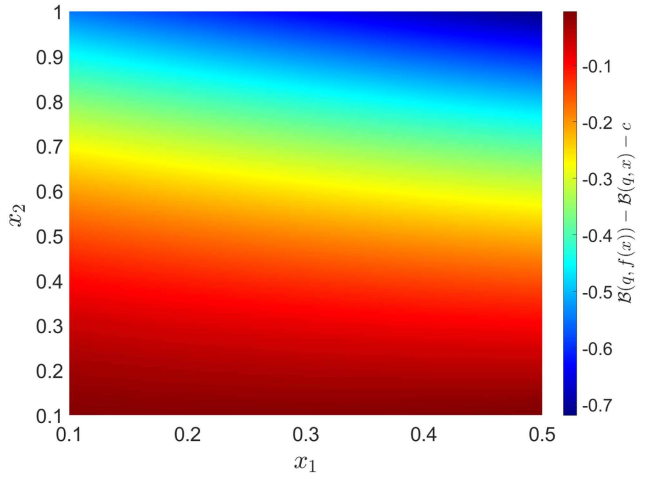

Fig. 9. *DC motor:* Satisfaction of condition (4). As observed, the condition is nonpositive for all ranges of $x_1 \in [0.1, 0.5]$ and $x_2 \in [0.1, 1]$.

(RCP). Since the formulated RCP was not tractable due to having the unknown model in one of the constraints, we provided the corresponding scenario convex program (SCP) of RCP by considering a given set of data collected from trajectories of the unknown system. We then established a probabilistic closeness between the optimal value of SCP and that of RCP. We accordingly verified the safety of the unknown system with an a-priori guaranteed confidence bound. We finally illustrated the effectiveness of our proposed results by applying them to three case studies. Formal *controller synthesis* via data-driven construction of *control* barrier certificates is under investigation as a future work.

APPENDIX

A. Estimation of Lipschitz Constant of Dynamics From Data

In this section, we employ the proposed results in [53] and provide the following algorithm to estimate the Lipschitz constant of dynamics using a finite number of data collected from the system.

By employing Algorithm 2, the following lemma, borrowed from [53], ensures the convergence of the estimated Lipschitz constant to its actual value in the limit.

Lemma 8.1: Let Σ_d be a dt-S with an unknown transition map f. By employing Algorithm 2, the estimated Lipschitz constant $\mathscr{L}_f$ for Σ_d converges to its actual value if and only if α goes to zero and $\bar{N}, M$ go to infinity.

Remark 8.2: Note that we do not consider any confidence bound for the estimation of the Lipschitz constant in the setting of our work. Instead, we pick α very small and $\bar{N}, M$ very big such that one can get a good approximation for the Lipschitz constant. In the case study section, we showed that our estimated value for the Lipschitz constant of the system is almost the same as its actual value.

Algorithm 2: Estimation of Lipschitz Constant of dt-S.

1: Select randomly two initial conditions $\hat{x}_i, \hat{y}_i$, such that $\|\hat{x}_i - \hat{y}_i\| \leq \alpha$ for any $i \in \{1, \ldots, \bar{N}\}$, with $\alpha \in \mathbb{R}_{>0}$ being some arbitrary threshold
2: Compute the slope s_i as,
$$s_i = \frac{\|f(\hat{x}_i) - f(\hat{y}_i)\|}{\|\hat{x}_i - \hat{y}_i\|}, \quad \forall i \in \{1, \ldots, \bar{N}\},$$
where $f(\hat{x}_i)$ and $f(\hat{y}_i)$ are one step evaluations of the system started from initial states x_i and y_i, respectively
3: Compute the maximum slope as $\psi = \max\{s_1, \ldots, s_{\bar{N}}\}$
4: Repeat Steps 1-3 M times and acquire $\psi_1, \ldots, \psi_M$
5: Apply Reverse Weibull distribution [53] to $\psi_1, \ldots, \psi_M$, which gives us so-called location, scale, and shape parameters
6: The obtained *location parameter* is the estimated Lipschitz constant of dt-S.

B. Proofs of Statements

Proof: (Theorem 3.5). According to (4), since $\mathcal{B}(x(k+1)) - \mathcal{B}(x(k)) \leq c$, one can recursively infer that $\mathcal{B}(x(k)) - \mathcal{B}(x(0)) \leq ck$. From (2), we have $\mathcal{B}(x(k)) \leq \gamma + ck$. Now since $\gamma + c\mathcal{T} < \lambda$, one can readily conclude that $\mathcal{B}(x(k)) < \lambda$. From (3), one gets $x(k) \notin X_u$ for any $k \in [0, \mathcal{T})$, which completes the proof. It is clear that if c is equal to zero, one can provide the safety guarantee for an infinite-time horizon. ■

Proof: (Theorem 5.3). We first establish a probabilistic relation between optimal values of RCP and SCP, and then provide safety guarantees over unknown systems via the established relation. Based on [29, Th. 3.6 and Remark 3.9], the probabilistic distance between optimal values of RCP and SCP can be formally lower bounded as[1]

$$\mathbb{P}^N \{0 \leq \eta_R^* - \eta_N^* \leq L_{\text{SP}} h(\varepsilon)\} \geq 1 - \beta \tag{23}$$

where $h(\varepsilon)$ is a uniform level-set bound defined as $h(\varepsilon) = \mathscr{L}_g \kappa^{-1}(\varepsilon)$ [29, Definition 3.1], with $\kappa(r) : \mathbb{R}_{\geq 0} \to [0, 1]$ depending on the sampling distribution and the geometry of the uncertainty set X, and L_{SP} is a Slater constant as defined in [29, eq. (5)]. Equivalently, the inequality in (23) holds for a given N and $\varepsilon \geq \mathcal{I}^{-1}(1-\beta, \bar{z}, N - \bar{z} + 1)$, with $\bar{z}$ being the number of decision variables. Based on [29, Remark 3.5], since the original RCP in (5) can be cast as a min–max optimization problem, the Slater constant L_{SP} can be selected as 1. We refer the interested reader to [29, eq. (5)] for more details on the formal definition of Slater point.

From (23), one can readily conclude that $\eta_N^* \leq \eta_R^* \leq \eta_N^* + \mathscr{L}_g \kappa^{-1}(\varepsilon)$ with a confidence of at least $1 - \beta$. Since $\eta_N^* + \mathscr{L}_g \kappa^{-1}(\varepsilon) \leq 0$ (as the main condition of the theorem), then $\eta_R^* \leq 0$, implying the satisfaction of conditions (2)–(4) in Definition 3.1 and ensuring the safety of the unknown system within the time horizon $\mathcal{T} \leq \frac{\lambda^* - \gamma^*}{c^*}$ with a confidence of at least $1 - \beta$, which completes the proof. ■

Remark 8.3: Note that Slater point is defined based on the concept of Slater condition in optimization theory to ensure

[1]One can readily verify that η_R^* is always bigger than or equal to η_N^* since η_R^* is computed for infinitely many constraints, whereas η_N^* is computed only for finitely many of them.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

the existence of a feasible solution strictly satisfying all the constraints in the optimization problem. In other words, Slater point requires the optimization problem to have at least an optimal point as an interior point of the feasible region. We refer the interested reader to [29, eq. (5)] for more details.

Proof: (Lemma 5.8). For computing the Lipschitz constant of g_4 with respect to x, we have

$$\mathscr{L}_g : \begin{cases} \max\limits_{x\in X} & \|\frac{\partial g_4(x)}{\partial x}\| \\ \text{s.t.} & \|x\| \le v. \end{cases}$$

Accordingly

$$\begin{aligned}\mathscr{L}_g &= \max_{x\in X,\|x\|\le v} \|2(A^TPA-P)x\| \\ &\le \max_{x\in X,\|x\|\le v} \|2(A^TPA-P)\|\|x\| \\ &\le 2v(\|A^TPA\|+\|P\|) \le 2v(\|P\|\|A\|^2+\|P\|) \\ &\le 2v\rho(P)(\mathscr{L}_f^2+1).\end{aligned}$$

Then, $\mathscr{L}_g = 2v\rho(P)(\mathscr{L}_f^2+1)$, which completes the proof. ■

Proof: (Lemma 6.5). For computing the Lipschitz constant of g_4 with respect to x, we have

$$\mathscr{L}_g : \begin{cases} \max\limits_{x\in X} & \|\frac{\partial g_4(x)}{\partial x}\| \\ \text{s.t.} & \|x\| \le v. \end{cases}$$

Accordingly

$$\begin{aligned}\mathscr{L}_g &= \max_{x\in X,\|x\|\le v} \|2(PA+A^TP)x\| \\ &\le \max_{x\in X,\|x\|\le v} \|2(PA+A^TP)\|\|x\| \\ &\le 4v\|P\|\|A\| \le 4v\rho(P)\mathscr{L}_f.\end{aligned}$$

Then, $\mathscr{L}_g = 4v\rho(P)\mathscr{L}_f$, which completes the proof.

Proof: (Lemma 6.10). Using the definition of $\mathsf{L}_f\mathcal{B}(q,x)$ in (14), we have

$$|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')| \le |\partial_x\mathcal{B}(q,x)f(x)-\partial'_x\mathcal{B}(q,x')f(x')|.$$

By employing the following known inequality:

$$|\mathbb{A}^T\mathbb{B}-\mathbb{C}^T\mathbb{D}| \le \|\mathbb{A}\|\|\mathbb{B}-\mathbb{D}\| + \|\mathbb{D}\|\|\mathbb{A}-\mathbb{C}\|$$

for all $\mathbb{A},\mathbb{B},\mathbb{C},\mathbb{D}\in\mathbb{R}^n$, one has

$$\begin{aligned}|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')| &\le \|\partial_x\mathcal{B}(q,x)\|\|f(x)-f(x')\| \\ &+ \|f(x')\|\|\partial_x\mathcal{B}(q,x)-\partial_{x'}\mathcal{B}(q,x')\|.\end{aligned}$$

By employing Assumptions 6.7 and 6.8, one gets

$$\begin{aligned}&|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')| \\ &\quad\le \mathcal{M}_\mathcal{B}\mathscr{L}_f\|x-x'\| + \mathcal{M}_f\mathscr{L}_\mathcal{B}\|x-x'\| \\ &\quad= (\mathcal{M}_\mathcal{B}\mathscr{L}_f+\mathcal{M}_f\mathscr{L}_\mathcal{B})\|x-x'\| = \mathscr{L}\|x-x'\|\end{aligned}$$

which completes the proof. ■

Proof: (Theorem 6.11). Since x_τ is the solution of the model after τ units of time starting from x, one has

$$\mathcal{B}(q,x_\tau) = \mathcal{B}(q,x) + \int_0^\tau \mathsf{L}_f\mathcal{B}(q,x_t)\mathsf{d}t. \tag{24}$$

Considering the approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ as in (16) and by employing (24), one has

$$\widehat{\mathsf{L}}_f\mathcal{B}(q,x) = \frac{1}{\tau}\int_0^\tau \mathsf{L}_f\mathcal{B}(q,x_t)\mathsf{d}t.$$

By subtracting $\mathsf{L}_f\mathcal{B}(q,x)$ from both sides of the equality, we have

$$\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x) \le \frac{1}{\tau}\int_0^\tau (\mathsf{L}_f\mathcal{B}(q,x_t)-\mathsf{L}_f\mathcal{B}(q,x))\,\mathsf{d}t.$$

Consequently

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)| \le \frac{1}{\tau}\int_0^\tau |\mathsf{L}_f\mathcal{B}(q,x_t)-\mathsf{L}_f\mathcal{B}(q,x)|\mathsf{d}t.$$

By employing Lemma 6.10, one gets

$$\begin{aligned}|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)| &\le \frac{1}{\tau}\int_0^\tau \mathscr{L}\|x_t-x\|\mathsf{d}t \\ &= \frac{\mathscr{L}}{\tau}\int_0^\tau \|x_t-x\|\mathsf{d}t.\end{aligned}$$

Now we aim at finding an upper bound for $\|x_t-x\|$. Under the continuity property of the solution process of the system, we have

$$x_t = x + \int_0^t f(x_s)\mathsf{d}s.$$

Then, using Cauchy–Schwarz inequality, one has

$$\begin{aligned}\|x_t-x\| &= \|\int_0^t f(x_s)\mathsf{d}s\| = \left[\int_0^t f(x_s)^T\mathsf{d}s\int_0^t f(x_s)\mathsf{d}s\right]^{\frac{1}{2}} \\ &= \left[\int_0^t\int_0^t f(x_{s_1})^Tf(x_{s_2})\mathsf{d}s_1\mathsf{d}s_2\right]^{\frac{1}{2}} \\ &\le \left[\int_0^t\int_0^t \|f(x_{s_1})\|\|f(x_{s_2})\|\mathsf{d}s_1\mathsf{d}s_2\right]^{\frac{1}{2}}.\end{aligned}$$

Under Assumption 6.8, we obtain

$$\|x_t-x\| \le \int_0^t \mathcal{M}_f\mathsf{d}s = \mathcal{M}_ft.$$

Consequently, one has

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)| \le \frac{\mathscr{L}}{\tau}\int_0^\tau \mathcal{M}_ft\mathsf{d}t = \frac{1}{2}\tau\mathscr{L}\mathcal{M}_f$$

which completes the proof. ■

ACKNOWLEDGMENT

The authors would like to thank P. Mohajerin Esfahani for the fruitful discussions and helpful comments.

REFERENCES

[1] A. Pnueli, "The temporal logic of programs," in *Proc. 18th Annu. Symp. Found. Comput. Sci.*, 1977, pp. 46–57.
[2] A. Lavaei, S. Soudjani, A. Abate, and M. Zamani, "Automated verification and synthesis of stochastic hybrid systems: A survey," *Automatica*, vol. 146, 2022.
[3] E. M. Hahn, A. Hartmanns, H. Hermanns, and J.-P. Katoen, "A compositional modelling and analysis framework for stochastic hybrid systems," *Formal Methods Syst. Des.*, vol. 43, no. 2, pp. 191–232, 2013.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

[4] A. Lavaei, S. Soudjani, and M. Zamani, "Compositional construction of infinite abstractions for networks of stochastic control systems," *Automatica*, vol. 107, pp. 125–137, 2019.

[5] S. Soudjani, A. Abate, and R. Majumdar, "Dynamic Bayesian networks for formal verification of structured stochastic processes," *Acta Informatica*, vol. 54, no. 2, pp. 217–242, 2017.

[6] A. Lavaei, S. Soudjani, and M. Zamani, "Compositional abstraction-based synthesis for networks of stochastic switched systems," *Automatica*, vol. 114, 2020, Art. no. 108827.

[7] K. Mallik, A. Schmuck, S. Soudjani, and R. Majumdar, "Compositional synthesis of finite-state abstractions," *IEEE Trans. Autom. Control*, vol. 64, no. 6, pp. 2629–2636, Jun. 2019.

[8] A. Lavaei, S. Soudjani, and M. Zamani, "Compositional (in)finite abstractions for large-scale interconnected stochastic systems," *IEEE Trans. Autom. Control*, vol. 65, no. 12, pp. 5280–5295, Dec. 2020.

[9] A. Nejati, S. Soudjani, and M. Zamani, "Compositional abstraction-based synthesis for continuous-time stochastic hybrid systems," *Eur. J. Control*, vol. 57, pp. 82–94, 2021.

[10] A. Lavaei and M. Zamani, "From dissipativity theory to compositional synthesis of large-scale stochastic switched systems," *IEEE Trans. Autom. Control*, vol. 67, no. 9, pp. 4422–4437, Sep. 2022.

[11] S. Prajna, A. Jadbabaie, and G. J. Pappas, "A framework for worst-case and stochastic safety verification using barrier certificates," *IEEE Trans. Autom. Control*, vol. 52, no. 8, pp. 1415–1428, Aug. 2007.

[12] R. Wisniewski and M. L. Bujorianu, "Stochastic safety analysis of stochastic hybrid systems," in *Proc. IEEE 56th Conf. Decis. Control*, 2017, pp. 2390–2395.

[13] C. Huang, X. Chen, W. Lin, Z. Yang, and X. Li, "Probabilistic safety verification of stochastic hybrid systems using barrier certificates," *ACM Trans. Embedded Comput. Syst.*, vol. 16, no. 5, pp. 1–19, 2017.

[14] P. Jagtap, S. Soudjani, and M. Zamani, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Trans. Autom. Control*, vol. 66, no. 7, pp. 3097–3110, Jul. 2021.

[15] A. Nejati, S. Soudjani, and M. Zamani, "Compositional construction of control barrier functions for continuous-time stochastic hybrid systems," *Automatica*, vol. 145, 2022, Art. no. 110513.

[16] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *Proc. 18th Eur. Control Conf.*, 2019, pp. 3420–3431.

[17] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 3861–3876, Aug. 2017.

[18] N. Jahanshahi, A. Lavaei, and M. Zamani, "Compositional construction of safety controllers for networks of continuous-space POMDPs," *IEEE Trans. Control Netw. Syst.*, 2022.

[19] A. Nejati, S. Soudjani, and M. Zamani, "Compositional construction of control barrier certificates for large-scale stochastic switched systems," *IEEE Control Syst. Lett.*, vol. 4, no. 4, pp. 845–850, Oct. 2020.

[20] L. Wang, E. A. Theodorou, and M. Egerstedt, "Safe learning of quadrotor dynamics using barrier certificates," in *Proc. Int. Conf. Robot. Autom.*, 2018, pp. 2460–2465.

[21] R. Cheng, G. Orosz, R. M. Murray, and J. W. Burdick, "End-to-end safe reinforcement learning through barrier functions for safety-critical continuous control tasks," in *Proc. AAAI Conf. Artif. Intell.*, 2019, vol. 33, pp. 3387–3395.

[22] S. Sadraddini and C. Belta, "Formal guarantees in data-driven model identification and control synthesis," in *Proc. 21st Int. Conf. Hybrid Syst.: Comput. Control*, 2018, pp. 147–156.

[23] K. Hashimoto, A. Saoud, M. Kishida, T. Ushio, and D. Dimarogonas, "Learning-based safe symbolic abstractions for nonlinear control systems," *Automatica*, vol. 146, 2022.

[24] P. Jagtap, G. J. Pappas, and M. Zamani, "Control barrier functions for unknown nonlinear systems using Gaussian processes," in *Proc. IEEE 59th Conf. Decis. Control*, 2020, pp. 3699–3704.

[25] C. Folkestad, Y. Chen, A. D. Ames, and J. W. Burdick, "Data-driven safety-critical control: Synthesizing control barrier functions with Koopman operators," *IEEE Control Syst. Lett.*, vol. 5, no. 6, pp. 2012–2017, Dec. 2021.

[26] A. Taylor, A. Singletary, Y. Yue, and A. Ames, "Learning for safety-critical control with control barrier functions," in *Proc. Learn. Dyn. Control*, 2020, pp. 708–717.

[27] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE Trans. Autom. Control*, vol. 51, no. 5, pp. 742–753, May 2006.

[28] G. C. Calafiore, "Random convex programs," *SIAM J. Optim.*, vol. 20, no. 6, pp. 3427–3464, 2010.

[29] P. M. Esfahani, T. Sutter, and J. Lygeros, "Performance bounds for the scenario approach and an extension to a class of non-convex programs," *IEEE Trans. Autom. Control*, vol. 60, no. 1, pp. 46–58, Jan. 2015.

[30] P. Mohajerin Esfahani, T. Sutter, D. Kuhn, and J. Lygeros, "From infinite to finite programs: Explicit error bounds with applications to approximate dynamic programming," *SIAM J. Optim.*, vol. 28, no. 3, pp. 1968–1998, 2018.

[31] M. C. Campi, S. Garatti, and M. Prandini, "The scenario approach for systems and control design," *Annu. Rev. Control*, vol. 33, no. 2, pp. 149–157, 2009.

[32] S. Ghosh, S. Bansal, A. Sangiovanni-Vincentelli, S. A. Seshia, and C. Tomlin, "A new simulation metric to determine safe environments and controllers for systems with unknown dynamics," in *Proc. 22nd ACM Int. Conf. Hybrid Syst.: Comput. Control*, 2019, pp. 185–196.

[33] J. Kenanian, A. Balkan, R. M. Jungers, and P. Tabuada, "Data driven stability analysis of black-box switched linear systems," *Automatica*, vol. 109, 2019, Art. no. 108533.

[34] Z. Wang and R. M. Jungers, "Data-driven computation of invariant sets of discrete time-invariant black-box systems," 2019, *arXiv:1907.12075*.

[35] J. Coulson, J. Lygeros, and F. Dörfler, "Regularized and distributionally robust data-enabled predictive control," in *Proc. 58th Conf. Decis. Control*, 2019, pp. 2696–2701.

[36] S. Haesaert, P. M. J. Van den Hof, and A. Abate, "Data-driven property verification of grey-box systems by Bayesian experiment design," in *Proc. Amer. Control Conf.*, 2015, pp. 1800–1805.

[37] M. Hasanbeig, A. Abate, and D. Kroening, "Certified reinforcement learning with logic guidance," 2019, *arXiv:1902.00778*.

[38] E. M. Hahn, M. Perez, S. Schewe, F. Somenzi, A. Trivedi, and D. Wojtczak, "Omega-regular objectives in model-free reinforcement learning," in *Proc. Int. Conf. Tools Algorithms Construction Anal. Syst.*, 2019, pp. 395–412.

[39] A. Lavaei, F. Somenzi, S. Soudjani, A. Trivedi, and M. Zamani, "Formal controller synthesis for continuous-space MDPs via model-free reinforcement learning," in *Proc. 11th ACM/IEEE Int. Conf. Cyber- Phys. Syst.*, 2020, pp. 98–107.

[40] M. Kazemi and S. Soudjani, "Formal policy synthesis for continuous-state systems via reinforcement learning," in *Proc. 16th Int. Conf. Integr. Formal Methods*, 2020, pp. 3–21.

[41] L. Lindemann et al., "Learning hybrid control barrier functions from data," in *Proc. Conf. Robot Learn.*, 2021, pp. 1351–1370.

[42] A. Robey et al., "Learning control barrier functions from expert demonstrations," in *Proc. 59th Conf. Decis. Control*, 2020, pp. 3717–3724.

[43] S. Bansal and C. J. Tomlin, "Deepreach: A deep learning approach to high-dimensional reachability," in *Proc. IEEE Int. Conf. Robot. Autom.*, 2021, pp. 1817–1824.

[44] P. Wieland and F. Allgöwer, "Constructive safety using control barrier functions," *IFAC Proc. Volumes*, vol. 40, no. 12, pp. 462–467, 2007.

[45] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *Proc. 7th Int. Workshop Hybrid Syst.: Comput. Control*, 2004, pp. 477–492.

[46] T. Kanamori and A. Takeda, "Worst-case violation of sampled convex programs for optimization with uncertainty," *J. Optim. Theory Appl.*, vol. 152, no. 1, pp. 171–197, 2012.

[47] A. Salamati and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach," in *Proc. 4th Annu. Learn. Dyn. Control Conf.*, 2022, pp. 441–452.

[48] R. S. Varga, *Geršgorin and His Circles*, vol. 36. Berlin, Germany: Springer, 2010.

[49] E. D. Sontag, *Mathematical Control Theory*, vol. 6, 2nd ed. Berlin, Germany: Springer, 1998.

[50] A. Girard, G. Gössler, and S. Mouelhi, "Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models," *IEEE Trans. Autom. Control*, vol. 61, no. 6, pp. 1537–1549, Jun. 2016.

[51] M. Krstic and P. V. Kokotovic, "Lean backstepping design for a jet engine compressor model," in *Proc. Int. Conf. Control Appl.*, 1995, pp. 1047–1052.

[52] P. A. Adewuyi, "DC motor speed control: A case between PID controller and fuzzy logic controller," *Int. J. Multidisciplinary Sci. Eng.*, vol. 4, no. 4, pp. 36–40, 2013.

[53] G. Wood and B. Zhang, "Estimation of the Lipschitz constant of a function," *J. Glob. Optim.*, vol. 8, no. 1, pp. 91–103, 1996.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.

Ameneh Nejati (Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering. She is currently working toward the Ph.D. degree with the Department of Electrical and Computer Engineering, Technical University of Munich (TUM), Munich, Germany.

She is currently a Research Scientist with Computer Science Department, Ludwig Maximilian University of Munich, Munich, Germany. During her Ph.D. studies since April 2018, she has visited different top-ranked schools outside of Germany including ETH Zurich, Switzerland, Newcastle University, U.K., and the University of Colorado Boulder, CO, USA. Her line of research mainly focuses on developing efficient (data-driven) techniques to design and control highly-reliable autonomous systems while providing mathematical guarantees. Application domain of her research spans a wide range of real-life safety-critical systems including automotive, robotics, transportation systems, energy, healthcare, and so on.

Abolfazl Lavaei (Senior Member, IEEE) received the M.Sc. degree in aerospace engineering with specialization in flight dynamics and control from the University of Tehran (UT), Tehran, Iran, in 2014 and the Ph.D. degree in electrical engineering from the Technical University of Munich (TUM), Munich, Germany, in 2019.

He is currently an Assistant Professor with the School of Computing, Newcastle University, U.K. Between January 2021 and July 2022, he was a Postdoctoral Associate with the Institute for Dynamic Systems and Control, ETH Zurich, Switzerland. He was also a Postdoctoral Researcher with the Department of Computer Science, Ludwig Maximilian University of Munich, Germany, between November 2019 and January 2021. 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. His research interests revolve around the intersection of control theory, computer science, artificial intelligence, and data science.

Dr. Lavaei was 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.

Pushpak Jagtap (Member, IEEE) received the M.Tech. degree in electrical engineering from the Indian Institute of Technology (IIT), Roorkee, India, in 2014 and the Ph.D. degree in electrical and computer engineering from the Technical University of Munich (TUM), Munich, Germany, in 2020.

He is currently an Assistant Professor with the Robert Bosch Center for Cyber-Physical Systems, Indian Institute of Science, Bangalore, India. From 2014 to 2015, he was a Senior Research Fellow (SRF) with the Center of Excellence in Complex and Nonlinear Dynamical Systems, VJTI, Mumbai, India. Before joining the Indian Institute of Science, he was a Postdoctoral Researcher in the Division of Decision and Control Systems with the KTH Royal Institute of Technology, Stockholm, Sweden. He was a Research Assistant with the Software and Computational Systems (SoSy) Lab, Ludwig Maximilian University of Munich, Munich, Germany from July 2019 to June 2020. His research interests include formal synthesis, symbolic models, stochastic systems, nonlinear control systems, and learning-based control.

Dr. Jagtap was the recipient of Google India Research Award in 2021.

Sadegh Soudjani (Members, IEEE) received the B.Sc. degree 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, and the Ph.D. degree in systems and control from the Delft Center for Systems and Control, Delft University of Technology, Delft, The Netherlands, in November 2014.

He is currently an Associate Professor with the School of Computing, Newcastle University, U.K., and a Group Leader with the Max Planck Institute for Software Systems, Saarbrücken, Germany. He is also the Director of the AMBER Group, Newcastle University. Before joining Newcastle University, he was a Postdoctoral Researcher with the Department of Computer Science, University of Oxford, Oxford, U.K., and with the Max Planck Institute for Software Systems. 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.

Dr. Soudjani was 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 U.K. EPSRC Research Council in 2021, and the 4m Award from European Research Council for the project SymAware in 2022.

Majid Zamani (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the Isfahan University of Technology, Isfahan, Iran, in 2005, the M.Sc. degree in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 2007, and the M.A. degree in mathematics and the Ph.D. degree in electrical engineering both in 2012 from the University of California, Los Angeles, Los Angeles, CA, USA.

He is currently an Associate Professor with the Computer Science Department, University of Colorado Boulder, CO, USA. He is also a Guest Professor with the Computer Science Department, Ludwig Maximilian University of Munich, Germany. Between September 2012 and December 2013, he was a Postdoctoral Researcher with the Delft Center for Systems and Control, Delft University of Technology, Delft, The Netherlands. From May 2014 to January 2019, he was an Assistant Professor with the Department of Electrical and Computer Engineering, Technical University of Munich, Germany. From December 2013 to April 2014, he was an Assistant Professor with the Design Engineering Department, Delft University of Technology. His research interests include verification and control of hybrid systems, embedded control software synthesis, networked control systems, and incremental properties of nonlinear control systems.

Dr. Zamani was the recipient of the NSF Career award in 2022 and ERC starting grant award from the European Research Council in 2018.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on May 07,2024 at 20:34:06 UTC from IEEE Xplore. Restrictions apply.