

Data-Driven Safe Controller Synthesis for Deterministic Systems: A Posteriori Method With Validation Tests

Yu Chen, Chao Shang, Xiaolin Huang and Xiang Yin

Abstract—In this work, we investigate the data-driven safe control synthesis problem for unknown dynamic systems. We first formulate the safety synthesis problem as a robust convex program (RCP) based on notion of control barrier function. To resolve the issue of unknown system dynamic, we follow the existing approach by converting the RCP to a scenario convex program (SCP) by randomly collecting finite samples of system trajectory. However, to improve the sample efficiency to achieve a desired confidence bound, we provide a new posteriori method with validation tests. Specifically, after collecting a set of data for the SCP, we further collect another set of independent *validate data* as posterior information to test the obtained solution. We derive a new overall confidence bound for the safety of the controller that connects the original sample data, the support constraints, and the validation data. The efficiency of the proposed approach is illustrated by a case study of room temperature control. We show that, compared with existing methods, the proposed approach can significantly reduce the required number of sample data to achieve a desired confidence bound.

I. INTRODUCTION

With the increasing complexity of engineering cyber-physical systems, ensuring safety has become a top priority in their design. This is particularly important as the consequences of failures or errors in these systems can be severe, ranging from property damage to loss of life. In order to ensure that these systems operate safely and correctly, engineers and developers often turn to *formal methods*. These methods provide a rigorous framework for analyzing and verifying system behavior, and can provide provable guarantees of correctness and safety [1], [2].

In the field of formal synthesis of safe controllers, there has been a significant amount of research conducted in recent years, resulting in the development of various approaches. These approaches can broadly be categorized as either abstraction-based or abstraction-free. Abstraction-based methods involve constructing a finite abstraction of the original system, typically achieved by discretizing the state space [3]–[6]. Symbolic algorithms can then be applied to this abstraction to synthesize a controller, which can subsequently be refined to the original system. However, a significant drawback of this approach is the curse of

dimensionality, which limits its suitability for large-scale systems. On the other hand, abstraction-free approaches for safe control synthesis are becoming increasingly popular, with one widely-used method being control barrier functions (CBF) [7]–[13]. Unlike abstraction-based techniques, CBF can directly synthesize a controller to enforce safety without the need to discretize the state spaces. This approach offers advantages in terms of scalability, making it more feasible for high-dimensional systems.

The aforementioned techniques for safe control synthesis rely on having knowledge of the system model, which can be costly or even impossible for complex systems. To address this issue, recent research has advocated for the use of data-driven approaches. For instance, several techniques have been developed to construct formal abstractions directly from data with confidence guarantees, as described in [14]–[16]. These approaches enable the construction of a finite abstraction of the system directly from data, without requiring a priori knowledge of the system model. Additionally, there are works that combine control barrier functions with collected data to synthesize controllers when the system model is partially or fully unknown; see, e.g., [17]–[20]. These approaches offer promising avenues for safe control synthesis in scenarios where accurate models may be difficult or impossible to obtain.

Recently, there has been a surge of interest in data-driven verification and synthesis for safety, driven in part by the development of the theory *scenario convex programming* [21], [22]. This approach provides a sound method for safety verification or synthesis by connecting the number of sample data to the confidence bound. For instance, for deterministic systems, the safety verification problem has been addressed in [23] for both discrete and continuous-time cases. Additionally, in [24], safety verification for stochastic systems has been investigated, and the results have been extended to the synthesis problem in [25]. Furthermore, the wait-and-judge approach [26] and the repetitive approach [27] have also been used to improve the sample efficiency of the safety verification problem.

In this work, we focus on studying the data-driven control synthesis of unknown discrete-time deterministic systems for safety specifications. Our method also builds upon the tools of control barrier functions and scenario theory. Specifically, we follow the approach in [25] by converting the safety control problem into a robust convex program (RCP) that searches for a control barrier function, ultimately solved by a scenario convex program. However, motivated by the recent results in [28], we introduce a new mechanism called the

This work was supported by the National Natural Science Foundation of China (62061136004, 62173226, 61833012).

Yu Chen, Xiaolin Huang and Xiang Yin are with Department of Automation and Key Laboratory of System Control and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China. {yuchen26, yinxiang, xiaolinhuang}@sjtu.edu.cn. Chao Shang is with the Department of Automation, Beijing National Research Center for Information Science and Technology, Tsinghua University, Beijing 100084, China. c-shang@tssinghua.

validation test for the control synthesis problem. Specifically, our approach requires to collect two different data sets:

- We first collect N data to formulate the scenario convex program in order to obtain a solution;
- Then, we collect N_0 independent *validation data* as *posterior information* to test the obtained solution such that the confidence bound can be further improved.

In contrast to [26] and [27] for the verification problem, where the information of support constraints number and the information of violation frequency in validation data are used independently, here we not only consider the *synthesis* problem, but also use these two posterior information *jointly*. Therefore, our main result is an overall performance bound that connects all three information: the original sample data, support constraints, and validation data, in a uniform manner. We show that, compared with existing methods, the proposed approach can significantly reduce the required number of sample data to achieve a desired confidence bound.

The rest of the paper is organized as follows. In Section II, we provide the necessary preliminaries and formulate the problem. In Section III, we review the existing results on solving data-driven safe control synthesis using scenario convex programs. Our main theoretical contributions are presented in Section IV, where we describe the overall synthesis procedure and derive a new performance bound using posterior information. We demonstrate the sample efficiency of the proposed method in Section V through a room temperature control example. Finally, we conclude the paper in Section VI.

II. PRELIMINARY AND PROBLEM STATEMENT

A. Notations

We denote by \mathbb{R} , $\mathbb{R}_0^+ \mathbb{N} := \{1, 2, 3, \dots\}$ and $\mathbb{N}_0 := \{0, 1, 2, \dots\}$ the set of real numbers, non-negative real numbers, positive integers and non-negative integers, respectively. The indicator function is denoted by $\mathbf{1}_{\mathcal{A}}(X) : X \rightarrow \{0, 1\}$ where $\mathbf{1}_{\mathcal{A}}(x) = 1$ if and only if $x \in \mathcal{A}$. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}$ and $i \in \{1, \dots, N\}$, we denote by $[x_1; \dots; x_n]$ and $[x_1, \dots, x_n]$ the corresponding column and row vectors, respectively. We denote by $\|x\|$ and $\|x\|_\infty$ the Euclidean norm and infinity norm of $x \in \mathbb{R}^n$, respectively. The induced norm of matrix $A \in \mathbb{R}^{m \times n}$ is defined by $\|A\| = \sup_{\|x\|=1} \|Ax\|$.

We consider a probability space with the tuple $(\Delta, \mathcal{F}, \mathbb{P})$ where Δ is the sample space, \mathcal{F} is a σ -algebra on Δ and \mathbb{P} is a probability measure defined over \mathcal{F} . Given $N \in \mathbb{N}$, $\mathbb{N}_0 \ni m \leq n$, and $t \in (0, 1)$, the Beta cumulative probability function is defined as $B_N(t; m) := \sum_{i=0}^m \binom{N}{i} t^i (1-t)^{N-i}$.

B. System Model

We consider a discrete-time dynamical system (dt-DS)

$$\mathbf{S} = (X, U, f),$$

where $X \subseteq \mathbb{R}^n$ is a Borel space representing state space of system, $U \subseteq \mathbb{R}^m$ is a set of control inputs and $f : X \times U \rightarrow X$ is an *unknown* function describing the dynamic of

the system. A (static state-feedback) controller is a mapping $C : X \rightarrow U$ that determines the control input based on the current state. Given a controller C and initial state $x(0) \in X$, the trajectory of the system is defined by

$$\zeta(x(0)) = x(0)x(1) \dots x(n) \dots,$$

where $x(t+1) = f(x(t), C(x(t)))$ for all $t = 0, 1, \dots$. For any $T \in \mathbb{N}$, we denote by $\zeta_T(x(0)) = x(0)x(1) \dots x(T)$ the finite prefix of trajectory $\zeta(x(0))$ of length $T+1$. We denote by \mathbf{S}_C the closed-loop system under control. We assume that the control input set is described as a polytope, i.e.,

$$U = \{u \in \mathbb{R}^m \mid Au \leq B\} \quad (1)$$

where $A \in \mathbb{R}^{r \times m}$, $B \in \mathbb{R}^r$ and $r \in \mathbb{N}$.

Although the dynamic function f is unknown, we assume that we can *simulate* the system by selecting initializing the system at state $x \in X$, applying input $u \in U$ and observing the next state state $x' \in X$ of the system. Such a tuple (x, u, x') is referred to as a data. Suppose that we assign a distribution \mathbb{P} , where $\Delta = X \times U$, to sample N i.i.d. pair (x_i, u_i) . Then the collected dataset \mathcal{D} is

$$\mathcal{D} := \{(x_i, u_i, f(x_i, u_i)) \mid i = 1, \dots, N\} \subseteq X \times U \times X. \quad (2)$$

C. Problem Statement

Given a dt-DS $\mathbf{S} = (X, U, f)$ and a 3-tuple *property*

$$\varphi = (X_0, X_u, T),$$

where $X_0 \subseteq X$ denotes the initial region, $X_u \subseteq X$ denotes the unsafe region, and T denotes the *horizon* of the property. We assume that $X_0 \cap X_u = \emptyset$. We say a trajectory is *safe* if it does not contain an unsafe state in X_u , and we denote the set of safety trajectories w.r.t. φ by

$$\Xi_\varphi = \{x_0 \dots x_T \in X^T \mid \forall i \in 0, \dots, T \text{ s.t } x_i \notin X_u\}.$$

Given controller C , we say that the closed-loop system \mathbf{S}_C satisfies property φ , denoted by $\mathbf{S}_C \models \varphi$ if

$$\forall x(0) \in X_0 : \zeta_T(x(0)) \in \Xi_\varphi.$$

The problem that we solve in this work is stated as follows.

Problem 1: Consider an unknown dt-DS $\mathbf{S} = (X, U, f)$ and a safety property $\varphi = (X_0, X_u, T)$. Using data in the form of (2) to find a controller $C : X \rightarrow U$ such that $\mathbf{S}_C \models \varphi$ with a confidence of $(1 - \beta) \in [0, 1]$, i.e.,

$$\mathbb{P}^N(\mathbf{S}_C \models \varphi) \geq 1 - \beta,$$

where \mathbb{P}^N is the N -cartesian product of distribution \mathbb{P} .

III. SCENARIO APPROACH USING BARRIER CERTIFICATES

The problem described in Problem 1 has already been addressed in the literature by [25]. The basic idea is to use control barrier functions (CBF) as a sufficient condition for ensuring safety properties, and then to solve a convex program to identify candidate CBFs through a scenario approach. We will briefly describe the existing method since our new approach builds upon it.

Definition 1 (control barrier functions): Given a dt-DS $\mathbf{S} = (X, U, f)$ and property $\varphi = (X_0, X_u, T)$, a function $\mathcal{B} : X \rightarrow \mathbb{R}$ is said to be a *control barrier function* (CBF) for \mathbf{S} and φ if there exist constants $\lambda, \gamma \in \mathbb{R}, c \geq 0$, and functions $F_i(x) : X \rightarrow \mathbb{R}, i = 1, \dots, m$ with $[F_1(x); \dots; F_m(x)] \in U$ such that

$$\mathcal{B}(x) < \gamma, \quad \forall x \in X_0, \quad (3)$$

$$\mathcal{B}(x) \geq \lambda, \quad \forall x \in X_u, \quad (4)$$

$$\mathcal{B}(f(x, u)) + \sum_{i=1}^m (u_i - F_i(x)) \leq \mathcal{B}(x) + c, \quad (5)$$

$$\forall x \in X, \forall (u_1, \dots, u_m) \in U,$$

$$\lambda - \gamma \geq cT, \quad (6)$$

As shown in [25], for any dt-DS, if we can find a CBF and its associated parameters, then controller $C : X \rightarrow U$ defined by

$$C(x) = [F_1(x); \dots; F_m(x)], \forall x \in X. \quad (7)$$

ensures the satisfaction of $\mathbf{S}_C \models \varphi$.

To identify a suitable CBF, a commonly adopted approach is to search among candidate polynomial functions. Specifically, a polynomial CBF $\mathcal{B}(q, x)$ with degree $k \in \mathbb{N}$ is of form

$$\mathcal{B}(q, x) = \sum_{a_1=0}^k \dots \sum_{a_n=0}^k q_{a_1, \dots, a_n} (x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}), \quad (8)$$

where q is the vector for all coefficients and for $\sum_{i=1}^n a_i > k$, we have $q_{a_1, \dots, a_n} = 0$. Similarly, for each $i \in \{1, \dots, m\}$, a polynomial function $F_i(p_i, x)$ with degree k_i is of form

$$F_i(p_i, x) = \sum_{a_1=0}^{k_i} \dots \sum_{a_m=0}^{k_i} p_{a_1, \dots, a_m}^i (x_1^{a_1} x_2^{a_2} \dots x_m^{a_m}), \quad (9)$$

where p_i is the vector for all coefficients and for $\sum_{i=m}^n a_i > k_i$, we have $p_{a_1, \dots, a_m}^i = 0$. We define $p = (p_1, \dots, p_m)$ as the overall coefficient vector.

Then by restricting to candidate polynomial functions, one can synthesize a CBF-based controller by solving the following Robust Convex Program (RCP):

$$\text{RCP: } \begin{cases} \min_d K \\ \text{s.t. } \max_{z \in \{1, 2, 3, 4\}} g_z(x, u, d) \leq 0, \forall x \in x, u \in U, \\ d = (K, \lambda, \gamma, c, q, p), \\ K \in \mathbb{R}, c \geq 0, \lambda - \gamma \geq cT \end{cases} \quad (10)$$

where

$$g_1(x, d) = (\mathcal{B}(q, x) - \gamma) \mathbf{1}_{X_0}(x), \quad (11)$$

$$g_2(x, d) = (-\mathcal{B}(q, x) + \lambda) \mathbf{1}_{X_u}(x), \quad (12)$$

$$g_3(x, u, d) = \mathcal{B}(q, f(x, u)) - \mathcal{B}(q, x) \quad (13)$$

$$+ \sum_{i=1}^m (u_i - F_i(p^i, x)) - c - K, \quad (14)$$

$$g_4(x, d) = \max_{i \in \{1, \dots, r\}} (A[F_1(p_1, x); \dots; F_m(p_m, x)] - B)_i. \quad (15)$$

Intuitively, if the optimal value for the above RCP, denoted by K^* , satisfies $K^* < 0$, then we know that $\mathcal{B}(q, x)$ is a valid CBF with associated control functions $F(p, x) = [F(p_1, x); \dots; F(p_m, x)]$. Specifically, $g_1(\cdot) - g_3(\cdot)$ ensure that $\mathcal{B}(q, x)$ satisfies definition of CBF and $g_4(\cdot)$ enforces that the selected control inputs are within the polytope defined in (1). For technical purpose, we further assume that all constraints are Lipschitz continuous with respect to x and u , and we denote by $L > 0$ the Lipschitz constant for all $g_z, z = 1, 2, 3, 4$.

However, the above RCP-based approach can only be used when the dynamic function f is known. When f is unknown, one can make use of the collected dataset \mathcal{D} in (2) to solve the RCP using the *scenario approach*. Specifically, one needs to replace constraint $g_3(x, u, d)$ that should hold for all $x \in X$ and $u \in U$ by a set of N constraints based on the sampled data. This leads to the following Scenario Convex Program (SCP)

$$\text{SCP}_N: \begin{cases} \min_d K \\ \text{s.t. } \max_{z \in \{1, 2, 4\}} \{g_z(x, d), g_3(x_i, u_i, d)\} \leq 0, \\ \forall x \in x, \forall i \in \{1, \dots, N\} \\ d = (K, \lambda, \gamma, c, q, p), \\ K \in \mathbb{R}, c \geq 0, \lambda - \gamma \geq cT \end{cases} \quad (16)$$

For the above SCP_N , we assume that the optimal solution exists and is unique for any possible number N of samples, which is a standard assumption in the literature; see, e.g., [29] for more discussion on this assumption.

Note that the decision variables are same in RCP and SCP_N . In the rest of paper, given a solution \hat{d} , we denote by $\hat{d} \models \mathcal{O}$ if \hat{d} is a feasible solution of \mathcal{O} where \mathcal{O} is a optimization problem.

The following result established in [25] shows how to solve Problem 1 based on SCP_N .

Theorem 1 ([25]): Given dt-DS $\mathbf{S} = (X, U, f)$ with unknown f and safety property $\varphi = (X_0, X_u, T)$. Let $d_N^* = (K_N^*, \lambda^*, \gamma^*, c^*, q^*, p^*)$ the optimal solution to SCP_N and $C(x) = [F_1(p_1^*, x); \dots; F_m(p_m^*, x)]$ be the associated controller. Then we have $\mathbf{S}_C \models \varphi$ with a confidence of at least $1 - \beta$ if, for some $\epsilon \in [0, 1]$, we have

$$N \geq N(\epsilon, \beta) \text{ and } K_N^* + L\mu^{-1}(\epsilon) \leq 0, \quad (17)$$

where

$$N(\epsilon, \beta) := \min \left\{ N \in \mathbb{N} \left| \sum_{i=0}^{Q+P+3} \binom{N}{i} (\epsilon)^i (1-\epsilon)^{N-i} \leq \beta \right. \right\}$$

with Q and P the number of coefficients in the CBF and the total number of coefficients in control functions, respectively, and $\mathcal{U}(r) : \mathbb{R}_0^+ \rightarrow [0, 1]$ is a function related to geometry of $X \times U$ and sampling distribution \mathbb{P} .

Remark 1: The reader is referred to [22] for the general relationship among function $\mathcal{U}(\cdot)$, distribution $\mathbb{P}(\cdot)$ and space $X \times U$. Particularly, if the the sampling distribution \mathbb{P} is uniform over $X \times U$ and $X \times U$ is n -dimensional hyper-rectangular, then function \mathcal{U} is given by [23]

$$\mathcal{U}(r) = \frac{\pi^{\frac{n}{2}} r^n}{2^n \Gamma(\frac{n}{2} + 1) \mathbf{Vol}(X \times U)}$$

where $\Gamma(\frac{n}{2} + 1) = (\frac{n}{2} + 1)!$ when n is even and $\Gamma(\frac{n}{2} + 1) = \frac{n}{2} \times (\frac{n}{2} - 1) \times \dots \times \frac{1}{2}$ otherwise, and $\mathbf{Vol}(\cdot)$ denotes the volume of a set.

IV. MAIN RESULTS USING POSTERIOR INFORMATION

In the previous section, we reviewed existing methods that provide a sound data-driven solution to Problem 1. However, as noted in Remark 1, the number of sample data required to achieve a desired confidence bound is generally exponential with respect to the dimension of the system. Therefore, the question naturally arises: How can we improve the sampling efficiency of the synthesis procedure? To address this issue, we present a more efficient method that leverages additional information.

In the context of SCP, there are two additional posteriori information that are closely related to the performance bound of the program:

- one is the *support constraint* whose removal can improve the optimal value of the SCP;
- the other is the *violation frequency* of a new set of validation data.

As shown in [28], these two posteriori information can be leveraged together to improve the sample efficiency in order to achieve a desired performance bound. In this section, we show how these information can be used in the context of data-driven control synthesis.

First, we review the definition of support constraint.

Definition 2 (Support Constraint, [30]): For a scenario convex program SCP_N and $i \in \{1, \dots, N\}$, constraint $g_3(x_i, u_i, d) \leq 0$ is said to be a *support constraint* if the removal of the constraint improves optimal value of SCP_N .

Intuitively, the number of support constraints characterizes the complexity of SCP_N . As shown in [31], the number of support constraints is upper bounded by the number of decision variables. Furthermore, if the number of support constraints is much smaller than the number of decision variables, the complexity of SCP_N is much lower than we guess in a prior. It means that we can provide the same guarantee by less samples.

The concept of *violate frequency* arises in the *validation test procedure*. Specifically, suppose that we form an

SCP_N from a set \mathcal{D} of N sample data and let d_N^* be the optimal solution to SCP_N . The validation test requires a new set \mathcal{D}' of N_0 independent samples of state-input pair $\{(x'_1, u'_1), \dots, (x'_{N_0}, u'_{N_0})\}$. Then the violation frequency is defined as follows.

Definition 3 (Violation Frequencies, [32]): Let d_N^* be the optimal solution to SCP_N formed by data set \mathcal{D} with N samples. Let \mathcal{D}' be a set of N_0 independent new samples. Then the *violation frequency* with respect to N_0 and d_N^* is defined by

$$R_{N_0} = \sum_{k=1}^{N_0} v(k), \quad (18)$$

where $v(k)$ is the the violation indicator of d_N^* for the k -th sample defined by

$$v(k) = \begin{cases} 0 & g_3(x'_k, u'_k, d_N^*) \leq 0 \\ 1 & \text{otherwise} \end{cases}. \quad (19)$$

Before we provide our main result, we make the following assumption regarding SCP_N .

Assumption 1: (Non-degeneracy [33]) The solution to SCP_N coincides with probability 1 with the solution to the program only defined by support constraints.

The above assumption is a very mild one for convex programs. It effectively rules out situations where the solution of the program with only support constraints lies on the boundaries of other constraints with a non-zero probability.

Now, let d_N^* be the optimal solution of SCP_N with N^* the number of support constraints. The following main result of this paper establishes the connection between the safety of a controlled system and the optimal solution of SCP_N , its number of support constraints and the violation frequency of a new set of data.

Theorem 2: Given dt-DS $\mathbf{S} = (X, U, f)$ with unknown f and safety property $\varphi = (X_0, X_u, T)$. Let $d_N^* = (K_N^*, \lambda^*, \gamma^*, c^*, q^*, p^*)$ the optimal solution to SCP_N formed by a set \mathcal{D} of N data and N^* be the number of support constraints. Let \mathcal{D}' be a collection of N_0 new independent data and R_{N_0} be the violation frequency w.r.t. N_0 and d_N^* . Let $C(x) = [F_1(p_1^*, x); \dots; F_m(p_m^*, x)]$ be controller associated with d_N^* . Then we have $\mathbf{S}_C \models \varphi$ with a confidence of at least $1 - \beta$ if

$$K_N^* + LU^{-1}(1 - \kappa^*) \leq 0, \quad (20)$$

where κ^* is the unique solution of

$$\frac{\beta}{N+1} \sum_{i=N^*}^N \binom{i}{N^*} \kappa^{i-N} - \binom{N}{N^*} B_{N_0}(1 - \kappa; R_{N_0}) = 0. \quad (21)$$

Proof: From RCP we construct a chance constraint program CCP_ϵ for some ϵ as below:

$$\text{CCP}_\epsilon : \begin{cases} \min_d & K \\ \text{s.t.} & \mathbb{P}(g_3(x, u, d) \leq 0) \geq 1 - \epsilon, \\ & \max_{z \in \{1, 2, 4\}} g_z(x, d) \leq 0, \forall x \in X, \\ & d = (K, \lambda, \gamma, c, q, p), \\ & K \in \mathbb{R}, c \geq 0, \lambda - \gamma \geq cT \end{cases} \quad (22)$$

Using Theorem 4 in [28], we know that

$$\mathbb{P}^{N+N_0}(d_N^* \models \text{CCP}_{\epsilon^*}) \geq 1 - \beta \quad (23)$$

where $\epsilon^* = 1 - \kappa^*$. Then we construct a relax version of RCP, denoted by $\text{RCP}_{h(\epsilon^*)}$ as follows:

$$\text{RCP}_{h(\epsilon^*)} : \begin{cases} \min_d & K \\ \text{s.t.} & g_3(x, u, d) \leq h(\epsilon^*), \forall x \in X, \forall u \in U \\ & \max_{z \in \{1,2,4\}} g_z(x, d) \leq 0, \forall x \in X, \\ & d = (K, \lambda, \gamma, c, q, p), \\ & K \in \mathbb{R}, c \geq 0, \lambda - \gamma \geq cT \end{cases} \quad (24)$$

where $h(\cdot)$ is a uniform level-set bound defined in Definition 3.1 of [22]. From result of Lemma 3.2 in [22] and Equation (23), we know that

$$\mathbb{P}^{N+N_0}(d_N^* \models \text{RCP}_{h(\epsilon^*)}) \geq 1 - \beta. \quad (25)$$

We denote by $K_{\text{RCP}_{h(\epsilon^*)}}^*$ the optimal value of objective function of $\text{RCP}_{h(\epsilon^*)}$. Since any feasible solution of $\text{RCP}_{h(\epsilon^*)}$ is larger or equal to $K_{\text{RCP}_{h(\epsilon^*)}}^*$, we have

$$\mathbb{P}^{N+N_0}(K_{\text{RCP}_{h(\epsilon^*)}}^* \leq K_N^*) \geq 1 - \beta. \quad (26)$$

Using Lemma 3.4 in [22], we know that

$$K_{\text{RCP}}^* \leq K_{\text{RCP}_{h(\epsilon^*)}}^* + \mathcal{L}_{sp}h(\epsilon^*)$$

where K_{RCP}^* is optimal of RCP and \mathcal{L}_{sp} is the Slater constant defined in Assumption 3.3 of [22]. As a result, we have

$$\mathbb{P}^{N+N_0}(K_{\text{RCP}}^* \leq K_N^* + \mathcal{L}_{sp}h(\epsilon^*)) \geq 1 - \beta.$$

Because RCP is a min-max problem, according to Remark 3.5 in [22], \mathcal{L}_{sp} can be chosen as 1. Moreover, as statement in Remark 3.8 of [22], $h(\epsilon^*)$ can be computed as $LU^{-1}(\epsilon^*)$ where L is Lipschitz constant of constraints. Thus we have

$$\mathbb{P}^{N+N_0}(K_{\text{RCP}}^* \leq K_N^* + LU^{-1}(\epsilon^*)) \geq 1 - \beta. \quad (27)$$

We define

$$E = \{\mathcal{D} \in \Delta^{N+N_0} | K_{\text{RCP}}^* \leq K_N^* + LU^{-1}(\epsilon^*)\}$$

the set of datasets includes in the event of Equation (27). Let

$$F = \{\mathcal{D} \in \Delta^{N+N_0} | K_N^* + LU^{-1}(\epsilon^*) \leq 0\}.$$

If $E \cap F \neq \emptyset$, we know that $K_{\text{RCP}}^* \leq 0$. Since $K_N^* + LU^{-1}(\epsilon^*) \leq 0$, we know that the selected date set $\mathcal{D} \in F$. From Equation (27) we have

$$\mathbb{P}^{N+N_0}(\mathcal{D} \in E) \geq 1 - \beta.$$

Therefore, $K_{\text{RCP}}^* \leq 0$, i.e., $\mathbf{S}_C \models \varphi$, is true with confidence of at least $1 - \beta$. This completes the proof. ■

Remark 2: Before we proceed further, let us discuss some computational considerations regarding the derived performance bound. First, we can obtain an upper bound of the Lipschitz constant L in Theorem 2 by using the result in Lemma 2 of [25]. Second, in cases where the number of constraints is large, it may be challenging to accurately

count the number of support constraints. However, for convex optimization problems, the support constraint is also an active constraint [34]. Therefore, we can use the number of active constraints in SCP_N as an upper bound for the number of support constraints. Finally, we note that the solution of Equation (21) may not have an analytic expression. Nevertheless, we can use bisection to numerically search for the solution using the procedure in Algorithm 1 of [28].

Algorithm 1: Data-driven system Safe Control Synthesis for Unknown dt-DS

Input: $\mathbf{S} = (X, U, f)$, $\varphi = (X_0, X_u, T)$, $\beta \in [0, 1]$, $L \in \mathbb{R}$, degree $k, k' \in \mathbb{N}$ in (8) and (9).

- 1 Select a probability distribution \mathbb{P} over $X \times U$
- 2 Choose number of samples N and N_0
- 3 Collect N samples
 $\mathcal{D}_1 = \{(x_i, u_i, x'_i) \in X \times U \times X \mid x'_i = f(x_i, u_i)\}$
- 4 Collect N_0 additional samples
 $\mathcal{D}_2 = \{(x_i, u_i, x'_i) \in X \times U \times X \mid x'_i = f(x_i, u_i)\}$
- 5 Solve SCP_N by \mathcal{D}_1 and obtain
 $d^* = (K^*, \lambda^*, c^*, q^*, p^*)$
- 6 Compute the number of support constraints N^*
- 7 Compute violation frequency R_{N_0} by \mathcal{D}_2
- 8 Compute κ^* according to Equation (21)

Output: Controller C defined by Equation (7) has guarantee that $\mathbf{S}_C \models \varphi$ with confidence $1 - \beta$ if $K_N^* + LU^{-1}(1 - \kappa^*) \leq 0$

Now we discuss how to properly select sample numbers N and N_0 to achieve confidence β . For each N , we can solve SCP_N repetitively to estimate optimal objective value \hat{K}_N^* and support constraints number \hat{N}^* in expectation. According to analysis in [28], the expectation of R_{N_0}/N_0 is lower than N^*/N with high confidence. Therefore, we adopt $\hat{R}_{N_0} = N_0 \times \hat{N}^*/N$ as estimated violation frequency.

Since $\mathcal{U}(\cdot)$ is an increasing function, to guarantee Equation (20), we have

$$\kappa^* \geq 1 - \mathcal{U}\left(-\frac{\hat{K}_N^*}{L}\right). \quad (28)$$

We denote by $g_{N, N_0}^\beta(\kappa, N^*, R_{N_0})$ the LHS of Equation (21). From [28] we know that function $g_{N, N_0}^\beta(\cdot)$ is decreasing w.r.t. κ . Therefore, we can pick N and N_0 such that

$$g_{N, N_0}^\beta\left(1 - \mathcal{U}\left(-\frac{\hat{K}_N^*}{L}\right), \hat{N}^*, \hat{R}_{N_0}\right) \geq 0. \quad (29)$$

In summary, given a desired confidence bound β , we can determine the N and N_0 by following steps:

- 1) Pick N and N_0 arbitrary;
- 2) Calculate \hat{K}_N^* , \hat{N}^* , \hat{R}_{N_0} as discussion above;
- 3) If Equation (29) holds, then choose the current N and N_0 ; otherwise increase N and N_0 and return to step 2).

It is important to note that while following the steps outlined above to select values for N and N_0 , it is possible that condition (20) may not be satisfied. In such cases, we

must independently sample a new set of $N + N_0$ data and solve a new instance of SCP_N . In order to reduce the time required, we can over-approximate K_N^* and N^* to obtain a more conservative bound. The overall steps involved in this process are summarized in Algorithm 1.

V. CASE STUDY OF ROOM TEMPERATURE CONTROL

To illustrate the efficiency of the proposed approach, we adopt the room temperature control problem from [25]. Specifically, we control room with a heater whose dynamic function is given by

$$\mathbf{S} : x(t+1) = x(t) + \tau_s(\alpha_e(T_e - x(t)) + \alpha_h(T_h - x(t))u(t)),$$

where $T_e = 15$, $T_h = 45$, $\alpha_e = 8 \times 10^{-3}$, $\alpha_h = 3.6 \times 10^{-3}$ and $\tau_s = 5$. We define $X_0 = [24, 25]$, $X_u = [22.5, 23] \cup [26, 26.5]$, $X = [22.5, 26.5]$, $U = [0, 1]$ and $T = 5$. We assume that the dynamic of system is unknown and the objective is to synthesize a controller under which the room temporal $x(t)$ in a comfortable region between 23° and 26° within time horizon $T = 5$ with confidence of 95%.

For both CBF and controller function, we consider candidate polynomial functions with degree $k = k_1 = 4$. Then the CBF and controller function are in the form of

$$\mathcal{B}(q, x) = \mathbf{x}\mathbf{Q}\mathbf{x}^\top \text{ and } C(p, \mathbf{T}) = \mathbf{x}\mathbb{P}\mathbf{x}^\top,$$

where $\mathbf{x} = [1, x, x^2]$ is a row vector and

$$\mathbf{Q} = \begin{bmatrix} q_0 & \frac{q_1}{2} & \frac{q_2}{3} \\ \frac{q_1}{2} & \frac{q_2}{3} & \frac{q_3}{2} \\ \frac{q_2}{3} & \frac{q_3}{2} & q_4 \end{bmatrix}, \mathbb{P} = \begin{bmatrix} p_0 & \frac{p_1}{2} & \frac{p_2}{3} \\ \frac{p_1}{2} & \frac{p_2}{3} & \frac{p_3}{2} \\ \frac{p_2}{3} & \frac{p_3}{2} & p_4 \end{bmatrix} \quad (30)$$

are two coefficient matrices. By enforcing $\|\mathbf{Q}\| \leq 0.1$ and $\|\mathbb{P}\| \leq 0.05$, the Lipschitz constant L can be upper bounded by 11.63. We choose uniform distribution to sample state-input pairs. Since the state-input space is a 2-dimensional rectangular, function $\mathcal{U}(r)$ is computed by $\mathcal{U}(r) = \frac{\pi}{16}r^2$.

Results by Existing Method: First, we use the results of [25] as stated in Theorem 1 to solve the data-driven control synthesis problem. Let $\beta = 0.05$. By choosing $\epsilon = 7.492 \times 10^{-6}$, we have $LU^{-1}(\epsilon) = 0.07$. Therefore, the minimum number of samples needed for the scenario convex program to ensure the confidence bound is $N = 2733296$. We then solve the SCP_N with acquired samples and obtain the optimal objective value $K_N^* = -0.1486$. Since $K_N^* + LU^{-1}(\epsilon) = -0.0786 \leq 0$, we know that $\mathbf{S}_C \models \varphi$ is ensured with a confidence of at least $1 - \beta = 95\%$.

Results by Our Method: Now we consider the posteriori method proposed in this paper. We also select $\beta = 0.05$. Note that there is no need to fix ϵ in a priori. Here, we choose $N = 140000$ to form the SCP and choose $N_0 = 70000$ for the validation test. Then we solve SCP_N and obtain $K_N^* = -0.149$, $\lambda^* = -68.14$, $\gamma^* = -69.64$ and $c^* = 0.2998$. We use number of active constraints, which is 1, to upper bound the number of support constraints. In the validation test, the violation frequency is 0, which essentially means that the solution to the SCP is already good enough to deserve higher confidence bound. The solution of Equation (21) is $\kappa^* = 0.9999723$. Since $K_N^* + LU^{-1}(1 - \kappa^*) = -0.011 \leq 0$, we

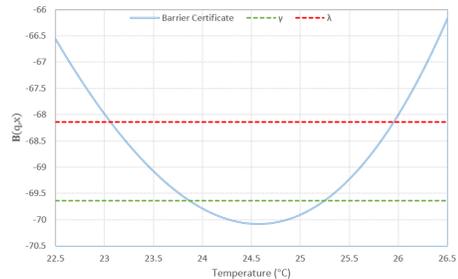


Fig. 1: Computed $\mathcal{B}(x)$ of SCP_N . The green and red dashed line represents solution γ^* and λ^* , respectively.

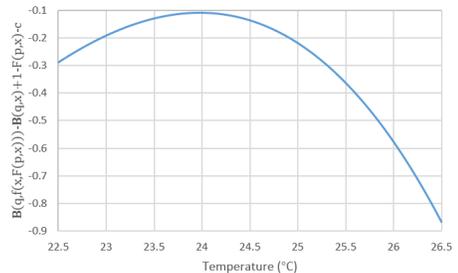


Fig. 2: Satisfaction of condition 5 of computed $\mathcal{B}(x)$ and $C(x)$.

know that $\mathbf{S}_C \models \varphi$ is ensured with a confidence of at least $1 - \beta = 95\%$. The CBF computed from SCP_N is

$$\mathcal{B}(x) = 1.948 \times 10^{-3}x + 0.2395x^2 - 3.841 \times 10^{-2}x^3 + 9.740 \times 10^{-4}x^4$$

and the obtained controller is

$$C(x) = 1.208 \times 10^{-5} + 9.768 \times 10^{-2}x - 3.438 \times 10^{-3}x^2 + 2.418 \times 10^{-5}x^3 + 4.594 \times 10^{-7}x^4.$$

The constructed $\mathcal{B}(x)$ is shown in Figure 1. From Figure 1 we know that conditions (3) and (4) are satisfied. Since we know the underlying dynamic of system \mathbf{S} , we also draw constraint $g_3(\cdot)$ in Figure 2, which shows that condition (5) is also satisfied. Therefore, $\mathcal{B}(x)$ is indeed a CBF and $\mathbf{S}_C \models \varphi$, i.e., controlled system is safe.

In the above example, we get zero violation frequency for the experiment. To further show the average performance, we run Algorithm 1 for 100 times with $N = 140000$ and $N_0 = 70000$. The number of active constraint is always 1. We record R_{N_0} in the 100 runs in Table I. As Table I, $R_{N_0} = 0$ has the highest occurrence frequency. It has been shown in [35] that we have high confidence that R_{N_0}/N_0 can not be much higher than N^*/N , where N^* is number of support constraints. Since $N^* \leq 1$ mostly in SCP_N , we know that R_{N_0} cannot much higher than 0.5 with high confidence. Therefore, the outcome of Table I is consistent with the result in [35]. Moreover, the expected number of samples N_e needed for our method is $N_e = (N + N_0)/0.42 = 500000$.

TABLE I: Record of R_{N_0} for 100 runs of Algorithm 1

R_{N_0}	0	1	2	3	6
frequency	42	34	17	5	2

According to the above experiments, our approach uses a significantly smaller sample size compared to the method proposed in [25]. This is mainly because the number of support constraints is much lower than the number of decision variables. This observation suggests that the complexity of the SCP is considerably lower than we initially assumed. Moreover, the frequency of violations is low in most cases, indicating that our solution provides the desired level of confidence. Collectively, these findings highlight the effectiveness of our approach in addressing the SCP with a reduced sample size while ensuring the same level of confidence.

VI. CONCLUSION

In this work, we presented a new approach for synthesizing safety controllers for unknown dynamic systems using data. Our method involves solving a scenario convex program formed by the data, followed by a validity test to improve confidence. To achieve this, we derived a new overall performance bound that combines the information from the original sample data, support constraints, and violation frequency. Our experiments demonstrated that our approach is more sample-efficient than existing methods. In this work, we only consider deterministic dynamic systems. In the future, we plan to extend our results to the stochastic case.

REFERENCES

- [1] P. Tabuada, *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.
- [2] C. Belta, B. Yordanov, and E. A. Gol, *Formal methods for discrete-time dynamical systems*, vol. 15. Springer, 2017.
- [3] A. Girard, G. Pola, and P. Tabuada, "Approximately bisimilar symbolic models for incrementally stable switched systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 116–126, 2010.
- [4] M. Zamani, P. M. Esfahani, R. Majumdar, A. Abate, and J. Lygeros, "Symbolic control of stochastic systems via approximately bisimilar finite abstractions," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3135–3150, 2014.
- [5] A. Lavaei, S. Soudjani, A. Abate, and M. Zamani, "Automated verification and synthesis of stochastic hybrid systems: A survey," *Automatica*, vol. 146, p. 110617, 2022.
- [6] S. Liu, A. Trivedi, X. Yin, and M. Zamani, "Secure-by-construction synthesis of cyber-physical systems," *Annual Reviews in Control*, 2022.
- [7] A. D. Ames, X. Xu, J. W. Grizzle, and P. Tabuada, "Control barrier function based quadratic programs for safety critical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3861–3876, 2017.
- [8] L. Wang, A. D. Ames, and M. Egerstedt, "Safety barrier certificates for collisions-free multirobot systems," *IEEE Transactions on Robotics*, vol. 33, no. 3, pp. 661–674, 2017.
- [9] P. Jagtap, S. Soudjani, and M. Zamani, "Formal synthesis of stochastic systems via control barrier certificates," *IEEE Transactions on Automatic Control*, vol. 66, no. 7, pp. 3097–3110, 2020.
- [10] A. Nejati, S. Soudjani, and M. Zamani, "Compositional construction of control barrier functions for continuous-time stochastic hybrid systems," *Automatica*, vol. 145, p. 110513, 2022.
- [11] W. Xiao, C. Belta, and C. G. Cassandras, "Adaptive control barrier functions," *IEEE Transactions on Automatic Control*, vol. 67, no. 5, pp. 2267–2281, 2022.
- [12] W. Xiao and C. Belta, "High-order control barrier functions," *IEEE Transactions on Automatic Control*, vol. 67, no. 7, pp. 3655–3662, 2022.
- [13] S. Yang, S. Chen, V. M. Preciado, and R. Mangharam, "Differentiable safe controller design through control barrier functions," *IEEE Control Systems Letters*, 2022.
- [14] A. Makdesi, A. Girard, and L. Fribourg, "Data-driven abstraction of monotone systems," in *Learning for Dynamics and Control*, pp. 803–814, PMLR, 2021.
- [15] A. Lavaei, S. Soudjani, E. Frazzoli, and M. Zamani, "Constructing mdp abstractions using data with formal guarantees," *IEEE Control Systems Letters*, vol. 7, pp. 460–465, 2022.
- [16] A. Peruffo and M. Mazo, "Data-driven abstractions with probabilistic guarantees for linear petc systems," *IEEE Control Systems Letters*, vol. 7, pp. 115–120, 2022.
- [17] S. Han, U. Topcu, and G. J. Pappas, "A sublinear algorithm for barrier-certificate-based data-driven model validation of dynamical systems," in *2015 54th IEEE conference on decision and control*, pp. 2049–2054, IEEE, 2015.
- [18] A. Robey, H. Hu, L. Lindemann, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni, "Learning control barrier functions from expert demonstrations," in *2020 59th IEEE Conference on Decision and Control*, pp. 3717–3724, IEEE, 2020.
- [19] P. Jagtap, G. J. Pappas, and M. Zamani, "Control barrier functions for unknown nonlinear systems using gaussian processes," in *2020 59th IEEE Conference on Decision and Control*, pp. 3699–3704, IEEE, 2020.
- [20] L. Lindemann, H. Hu, A. Robey, H. Zhang, D. Dimarogonas, S. Tu, and N. Matni, "Learning hybrid control barrier functions from data," in *Conference on Robot Learning*, pp. 1351–1370, PMLR, 2021.
- [21] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE Transactions on automatic control*, vol. 51, no. 5, pp. 742–753, 2006.
- [22] 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 Transactions on Automatic Control*, vol. 60, no. 1, pp. 46–58, 2015.
- [23] A. Nejati, A. Lavaei, P. Jagtap, S. Soudjani, and M. Zamani, "Formal verification of unknown discrete-and continuous-time systems: A data-driven approach," *IEEE Transactions on Automatic Control*, 2023.
- [24] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems," in *7th IFAC Conference on Analysis and Design of Hybrid Systems*, pp. 7–12, 2021.
- [25] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven verification and synthesis of stochastic systems through barrier certificates," *arXiv preprint arXiv:2111.10330*, 2021.
- [26] A. Salamati and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach," in *Learning for Dynamics and Control Conference*, pp. 441–452, PMLR, 2022.
- [27] A. Salamati and M. Zamani, "Safety verification of stochastic systems: A repetitive scenario approach," *IEEE Control Systems Letters*, vol. 7, pp. 448–453, 2022.
- [28] C. Shang and F. You, "A posteriori probabilistic bounds of convex scenario programs with validation tests," *IEEE Transactions on Automatic Control*, vol. 66, no. 9, pp. 4015–4028, 2021.
- [29] G. Calafiore and M. C. Campi, "Uncertain convex programs: randomized solutions and confidence levels," *Mathematical Programming*, vol. 102, pp. 25–46, 2005.
- [30] M. C. Campi and S. Garatti, "The exact feasibility of randomized solutions of uncertain convex programs," *SIAM Journal on Optimization*, vol. 19, no. 3, pp. 1211–1230, 2008.
- [31] S. Garatti and M. C. Campi, "Risk and complexity in scenario optimization," *Mathematical Programming*, vol. 191, no. 1, pp. 243–279, 2022.
- [32] M. Thulin, "The cost of using exact confidence intervals for a binomial proportion," *Electronic Journal of Statistics*, vol. 8, no. 1, pp. 817 – 840, 2014.
- [33] M. C. Campi and S. Garatti, "Wait-and-judge scenario optimization," *Mathematical Programming*, vol. 167, pp. 155–189, 2018.
- [34] S. Boyd, S. P. Boyd, and L. Vandenberghe, *Convex optimization*. Cambridge university press, 2004.
- [35] S. Garatti and M. C. Campi, "Risk and complexity in scenario optimization," *Mathematical Programming*, 2022.