2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Data-Driven Synthesis of Safety Controllers for Partially-Observable Systems with Unknown Models

Niloofar Jahanshahi and Majid Zamani

Abstract— **This paper is concerned with the formal synthesis of safety controllers for partially-observable discrete-time control systems with unknown mathematical models. Given a state estimator with *unknown* dynamics but a *known* upper bound on the estimation error, we propose a data-driven approach to compute controllers that render the partially-observable systems with unknown dynamics safe. Our proposed method is based on the construction of control barrier certificates, where we first formulate the barrier-based safety problem as a robust program (RP). The proposed RP is not tractable since the unknown model of the estimator appears in one of its constraints. To tackle this issue, we collect a set of data from the black-box system and its estimator and replace the original RP with a scenario program (SP). Due to the existence of a max-min constraint in the SP, we construct an analogous scenario program, denoted by SP$^{\alpha}$, in which the max-min constraint is replaced with a single inequality constraint. The control barrier certificates together with their corresponding controllers can then be computed by solving SP$^{\alpha}$ via the collected data. By connecting the feasible solutions of SP$^{\alpha}$ and SP, the safety of the partially-observable system equipped with the synthesized controller can be guaranteed with 100% confidence. We show the effectiveness of our results by synthesizing a safety controller for a partially-observable Van der Pol oscillator with unknown dynamics.**

Index Terms— **Partial-information, Data-driven synthesis, Control barrier certificates, Discrete-time control systems.**

I. Introduction

Safety is of significant importance in many control applications such as autonomous vehicles, drones, aircraft, robots, and advanced manufacturing. For this reason, formal synthesis of controllers ensuring safety properties has received significant attention in the past decade. In this regard, control barrier certificates have shown great promises as a reliable method to synthesize safety controllers for complex dynamical systems [1]. These functions are defined over the state space of the system and have to satisfy a set of inequalities defined over the function itself and one step transition of the system. The existence of such a function provides a controller together with the guarantee on the satisfaction of the safety specification. Since in many real-life applications, all the system's states are not observable, some recent work has investigated controller synthesis problems via control barrier certificates for systems with partial-information. Using state estimators, the results in [2] and [3] provide controllers ensuring safety for infinite time horizon by assuming a priori knowledge of the control barrier certificates and having an unbounded input set. The results in [4]–[6] provide finite-time horizon guarantees together with a lower bound on the probability of safety satisfaction by constructing the barrier certificate over the estimated states. The common prerequisite of all of the above-mentioned literatures is knowing the precise mathematical model of the system. However, obtaining an accurate model for many physical systems can be very challenging and computationally expensive. Moreover, the acquired mathematical model might be too complicated to be of any use. To this end, recent studies have made significant progress in exploring the application of data-driven approaches to construct control barrier functions. In particular, scenario-based approaches have been employed to tackle the challenges posed by semi-infinite programming in control analysis and synthesis problems. In this regard, the results in [7] and [8] utilize optimization-based methods to deal with data-driven safety verification of deterministic systems through barrier certificates by leveraging performance bounds for scenario programs [9]. The extension of [8] to stochastic systems is provided in [10]. Using barrier certificates, the results in [11] and [12] propose a so-called wait-and-judge approach to provide an out-of-sample performance guarantee for verifying the safety of stochastic systems with unknown dynamics. While the aforementioned results show promise, it is important to note that they are limited to systems with complete state information. However, in many practical scenarios, it is not possible to measure all the states of a system, which introduces additional challenges. To address this issue, in [13], a specific data-driven approach is proposed for the safety controller synthesis of partially-observable polynomial-type systems with unknown dynamics. Using sets of data collected from the output trajectories of the unknown system and the trajectories of its partially-unknown estimator, the control barrier certificates and their corresponding controllers are constructed in [13].

Motivated by the above results and their limitations, in this paper we provide a data-driven procedure for the formal synthesis of safety controllers for partially-observable discrete-time control systems with unknown mathematical models. In comparison to the study presented in [13], this paper introduces two significant contributions. Firstly, while [13] focuses on partially-observable polynomial-type systems with unknown dynamics, where the unknown parameters are the polynomial coefficients, our work encompasses a broader class of partially-observable systems with unknown models. Secondly, in [13], the results rely on estimators with partially

This work was supported in part by the NSF under grants CNS-2145184, CNS-1952223, and A22-0123-S003 and the German Research Foundation (DFG) through the Research Training Group 2428.

N. Jahanshahi is with the Computer Science Department, LMU Munich, Germany. Email: niloofar.jahanshahi@lmu.de

M. Zamani is with the Computer Science Department, University of Colorado Boulder, USA. Email: majid.zamani@colorado.edu

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

unknown dynamics, requiring knowledge of the estimator gain. In contrast, our approach tackles the scenario where both the system model and the estimator are unknown. The only requirement in our work is the knowledge of the Lipschitz constant of the estimator. In this work, given an estimator with unknown dynamics and a known upper bound on the estimation accuracy, we provide an approach to synthesize safety controllers based on a notion of control barrier certificates. To deal with unknown models, the control barrier certificate is constructed via a set of data collected from the system and its estimator. In our proposed settings, the data-driven synthesis of control barrier certificates is first cast as a robust program (RP). Since the unknown model of the estimator appears in one of the constraints of the proposed RP, we resort to a scenario-based approach and propose a scenario program (SP) corresponding to the original RP. The proposed SP contains a max-min constraint. We replace this max-min constraint with a single inequality constraint by constructing an analogous scenario program, denoted by SP$^\alpha$. Then, by leveraging the collected data, the control barrier certificate along with its controller are obtained by solving the SP$^\alpha$. As a result, by connecting the feasible solutions of the SP and the SP$^\alpha$, we ensure the safety of the unknown partially-observable control system with 100% guarantee.

The rest of the paper is structured as follows. Section II contains the system definition and mathematical notations. Control barrier certificates are formally defined in Section III. In Section IV, we present our data-driven approach to construct control barrier certificates. The case study and conclusion are given in Sections V and VI, respectively.

II. Partially-Observable Discrete-Time Control Systems

A. Notations

The sets of positive integers, non-negative integers, real numbers, non-negative real numbers, and positive real numbers are denoted by $\mathbb{N}, \mathbb{N}_0, \mathbb{R}, \mathbb{R}_0^+$, and $\mathbb{R}^+$, respectively. We donate the indicator function by $1_{\mathscr{A}}(x) : X \rightarrow \{0, 1\}$, where $1_{\mathscr{A}}(x)$ is 1 if and only if $x \in \mathscr{A} \subseteq X$, and 0 otherwise. We use $\mathbb{R}^n$ to denote an n-dimensional Euclidean space. The notation $\|x\|$ is used to indicate the Euclidean norm of any $x \in \mathbb{R}^n$. For a set X, we denote its ϵ-inflated version by X^ϵ, with $\epsilon \in \mathbb{R}^+$, and define it as $X^\epsilon := \{\hat{x} \in X \mid \exists x \in X, \|\hat{x} - x\| \leq \epsilon\}$. Given N vectors $x_i \in \mathbb{R}^{n_i}, n_i \in \mathbb{N}$, and $i \in \{1, \ldots, N\}$, we use $[x_1; \ldots; x_n]$ and $[x_1, \ldots, x_n]$ to denote the corresponding column and row vectors, respectively, with dimension $\sum_i n_i$.

B. Partially-Observable Discrete-Time Control Systems

We consider partially-observable discrete-time control systems as formalized in the following definition.

Definition 2.1: A partially-observable discrete-time control system (PO-dt-CS) in this paper is characterized by the tuple $\mathcal{S} := (X, U, f, Y, h)$, where $X \subseteq \mathbb{R}^n$ and $Y \subseteq \mathbb{R}^p$ are the bounded state and output sets, respectively. The set $U := \{u_1, u_2, \ldots, u_M\}$ is the finite input set, with $u_j \in \mathbb{R}^m, j \in \{1, \ldots, M\}, M \in \mathbb{N}$. The map $f : X \times U \rightarrow X$ is the transition function, which characterizes the state evolution of the system, and $h : X \rightarrow Y$ is the output function that maps a state $x \in X$ to its output $y \in Y$. A PO-dt-CS $\mathcal{S}$ can also be represented by the following difference equations

$$\mathcal{S} : \begin{cases} x(t+1) = f(x(t), u(t)) \\ y(t) = h(x(t)) + \sigma(t), \quad t \in \mathbb{N}_0, \end{cases} \tag{2.1}$$

where $\sigma(t) \in \mathbb{R}^p$ represents the measurement noise and is assumed to be bounded with an unknown bound (*i.e.,* $\|\sigma(t)\| \leq \bar{\sigma}$, where $\bar{\sigma}$ is not known). We employ the notation $x_{x_0 v}(t)$ to denote the state of $\mathcal{S}$ at time t, initialized from x_0 and under input sequence $v : \mathbb{N}_0 \rightarrow U$.

In this paper, we assume that maps f and h are unknown, and we employ the terms *black-box* or *unknown* models to refer to this type of systems. Additionally, we raise the following assumption on the existence of an estimator that estimates the states of PO-dt-CS $\mathcal{S}$ in (2.1) with an upper bound on the estimation error.

Assumption 1: Consider a PO-dt-CS $\mathcal{S} = (X, U, f, Y, h)$. States of $\mathcal{S}$ in (2.1) can be estimated by an estimator $\widehat{\mathcal{S}}$ which is characterized by the tuple $\widehat{\mathcal{S}} := (\widehat{X}, U, \hat{f}, Y)$ and represented as:

$$\widehat{\mathcal{S}} : \hat{x}(t+1) = \hat{f}(\hat{x}(t), u(t), y(t)), \quad t \in \mathbb{N}_0, \tag{2.2}$$

where $\hat{x}(t) \in \widehat{X}$ is the state of the estimator at time t and $X \subseteq \widehat{X}$ is the estimator's state set. Moreover, in this paper, we consider estimators that provide a guaranteed upper bound on the estimation error as follows.

$$\|x(t) - \hat{x}(t)\| \leq \epsilon, \quad \forall t \in \mathbb{N}_0, \tag{2.3}$$

where $\epsilon \in \mathbb{R}^+$ is known.

Remark 2.2: Note that the presence of measurement noise $\sigma(t)$ in (2.1) can have a detrimental effect on the accuracy of the estimator, reflected in ϵ in (2.3). The measurement noise introduces uncertainty and perturbations in the observed data, potentially leading to more deviations between the estimated states and the true states of the system.

For the unknown PO-dt-CS $\mathcal{S}$ in (2.1), one can resort to existing results in the literature including neural-network-based estimators to construct estimators as in (2.2) with an unknown function $\hat{f}$ (cf. [14]–[18]). In the remainder of the paper, we refer to estimators as in (2.2) with unknown functions $\hat{f}$ as *unknown* estimators. In our setting, we compute the estimation accuracy ϵ in (2.3) empirically using data. The results in [19]–[21] offer valuable insights into the practical computation of estimation errors using solely input-output data, eliminating the need for prior knowledge of the system or the dynamics of the estimator. For a quantitative and rigorous computation of the estimation error for neural network based estimators, we kindly refer the interested readers to the results in [22]. Now, we formally define the main synthesis problem to be addressed in this paper.

Problem 2.3: Consider an unknown PO-dt-CS $\mathcal{S}$ in (2.1) together with an unknown estimator $\widehat{\mathcal{S}}$ in (2.2). Let $X_a, X_b \subseteq$

X be some given initial and unsafe sets for $\mathcal{S}$, respectively. Synthesize a safety controller using which the trajectories of $\mathcal{S}$ starting from X_a never reach the unsafe set X_b.

To solve Problem 2.3, we utilize a notion of control barrier certificates, introduced in the next section

III. Control Barrier Certificates

In this section, we define a notion of control barrier certificates (CBCs), adapted from [23].

Definition 3.1: Consider a PO-dt-CS $\mathcal{S} = (X, U, f, Y, h)$ as in (2.1), its estimator $\widehat{\mathcal{S}}$ as in (2.2), with estimation accuracy ϵ as in (2.3), as specified in Assumption 1. Let $X_a, X_b \subseteq X \subseteq \widehat{X}$ be bounded initial and unsafe sets of $\mathcal{S}$, respectively. A function $\mathfrak{B} : \widehat{X} \to \mathbb{R}$ is called a control barrier certificate for $\widehat{\mathcal{S}}$ if there exist constants $\beta_a, \beta_b \in \mathbb{R}$ such that $\beta_a < \beta_b$, and

$$\forall \hat{x} \in X_a, \mathfrak{B}(\hat{x}) \leq \beta_a, \tag{3.1}$$

$$\forall \hat{x} \in X_b^\epsilon, \mathfrak{B}(\hat{x}) \geq \beta_b, \tag{3.2}$$

$$\forall \hat{x} \in \widehat{X}, \forall y \in Y, \min_{u \in U} \mathfrak{B}\big(\hat{f}(\hat{x}, u, y)\big) \leq \mathfrak{B}(\hat{x}), \tag{3.3}$$

with X_b^ϵ being the ϵ-inflated version of X_b.

Remark 3.2: Note that the above definition implicitly associates a set-valued controller

$$\eta : \widehat{X} \times Y \to 2^U, \tag{3.4}$$

to the CBC $\mathfrak{B}$ by selecting control inputs as $\eta(\hat{x}, y) := \{u \in U \mid \mathfrak{B}(\hat{f}(\hat{x}, u, y)) \leq \mathfrak{B}(\hat{x})\}$ for any $\hat{x} \in \widehat{X}$ and $y \in Y$.

Remark 3.3: Note that in order to enforce conditions (3.1)-(3.3), X_a and X_b^ϵ should not intersect. This condition is implicitly enforced by imposing $\beta_a < \beta_b$. By enforcing this inequality, we guarantee that X_a is a safe region.

The following theorem shows how CBCs can be leveraged to make the unknown PO-dt-CS $\mathcal{S}$ in (2.1) safe in the sense that its trajectories starting from X_a never reach X_b.

Theorem 3.4: Let $\mathcal{S}$ be a PO-dt-CS as in (2.1), $\widehat{\mathcal{S}}$ be its corresponding estimator as in (2.2), with estimation accuracy ϵ as in (2.2). Suppose $\mathfrak{B}$ is a CBC for $\widehat{\mathcal{S}}$ as in Definition 3.1 with the corresponding controller $\eta : \hat{X} \times Y \to 2^U$. Then, one gets $x_{x_0 v}(t) \notin X_b$, $\forall x_0 \in X_a$ and $\forall t \in \mathbb{N}_0$, where $v(t) \in \eta(\hat{x}(t), y(t))$, $\forall t \in \mathbb{N}_0$.

Proof: Condition (3.3) indicates that for any $\hat{x} \in \widehat{X}$ and $y \in Y$, there exists $u \in U$ such that $\mathfrak{B}(\hat{f}(\hat{x}, u, y)) \leq \mathfrak{B}(\hat{x})$. From this and (3.1), one can recursively infer that $\mathfrak{B}(\hat{x}(t)) \leq \mathfrak{B}(\hat{x}(0)) \leq \beta_a, \forall \hat{x}(0) \in X_a$, and $\forall t \in \mathbb{N}_0$. Since $\beta_a < \beta_b$, one gets $\mathfrak{B}(\hat{x}(t)) < \beta_b, \forall t \in \mathbb{N}_0$. From (3.2), one obtains $\hat{x}_{\hat{x}_0 v}(t) \notin X_b^\epsilon, \forall \hat{x}_0 \in X_a$ and $\forall t \in \mathbb{N}_0$, where $v(t) \in \eta(\hat{x}(t), y(t))$. Now, by utilizing the fact that $\hat{x}(t)$ estimates $x(t)$ with estimation error ϵ as in (2.3), one can conclude $x_{x_0 v}(t) \notin X_b$, $\forall x_0 \in X_a$ and $\forall t \in \mathbb{N}_0$, which completes the proof. ■

In order to synthesize controllers via CBCs, we fix the structure of control barrier certificates as

$$\mathfrak{B}(q, \hat{x}) = \sum_{\ell=1}^{\mathsf{r}_b} q_\ell b_\ell(\hat{x}), \tag{3.5}$$

with some user-defined nonlinear basis functions $b_\ell, \ell \in \{1, \ldots, \mathsf{r}_b\}$, and unknown coefficients $q = [q_1; \ldots; q_{\mathsf{r}_b}] \in \mathbb{R}^{\mathsf{r}_b}$. For instance, in the case of polynomial-type barrier certificates, basis functions b_ℓ are monomials over $\hat{x}$. Note that knowledge of the map $\hat{f}$ is required in condition (3.3). Since $\hat{f}$ is unknown in our setting, we provide in the next section a data-driven approach to construct CBCs as in Definition 3.1.

IV. Data-Driven Synthesis of CBCs

In this section, given an estimator as in Assumption 1, we propose a method to construct CBCs for the unknown PO-dt-CS $\mathcal{S}$ in (2.1) using data collected from the black-box system and its estimator. To do so, we first raise the following assumption.

Assumption 2: Consider the unknown system $\mathcal{S}$ in (2.1) and its unknown estimator $\widehat{\mathcal{S}}$ in (2.2). We assume one can collect data sets:

$$\begin{aligned} &\mathcal{D}_{\hat{x}} = \Big\{\hat{x}_i \mid i \in \{1, \ldots, N\}\Big\}, \mathcal{D}_y = \Big\{y_k \mid k \in \{1, \ldots, P\}\Big\}, \\ &\mathcal{D} = \Big\{(\hat{x}_i, y_k, u_j, \hat{f}(\hat{x}_i, y_k, u_j)) \mid i \in \{1, \ldots, N\}, \\ &\qquad k \in \{1, \ldots, P\}, j \in \{1, \ldots, M\}\Big\}. \end{aligned} \tag{4.1}$$

To do so, cover sets are constructed over $\widehat{X}$ and Y such that one has $\widehat{X} = \cup_{i=1}^N \widehat{X}_i$ and $Y = \cup_{k=1}^P Y_k$, with $\widehat{X}_i \subseteq \widehat{X}$, $\forall i \in \{1, \ldots, N\}$, and $Y_k \subseteq Y$, $\forall k \in \{1, \ldots, P\}$. Representative points $\hat{x}_i \in \widehat{X}_i$ and $y_k \in Y_k$ are selected for each $\widehat{X}_i$ and Y_k such that

$$\forall \hat{x} \in \widehat{X}, \exists \hat{x}_i, \text{ s.t. } \|\hat{x} - \hat{x}_i\| \leq d_{\hat{x}}, i \in \{1, \ldots, N\}, \tag{4.2}$$

$$\forall y \in Y, \exists y_k, \text{ s.t. } \|y - y_k\| \leq d_y, k \in \{1, \ldots, P\}, \tag{4.3}$$

for some $d_{\hat{x}}, d_y \in \mathbb{R}^+$.

Note that in order to obtain $\hat{f}(\hat{x}_i, y_k, u_j)$ in (4.1), the estimator is initialized from $\hat{x}_i$, inputs y_k and u_j are applied, and the next step of the estimator is observed. Now, we have all the ingredients to construct a CBC as in Definition 3.1 using data. To do so, we first consider a candidate for CBC $\mathfrak{B}(q, \hat{x})$ as in (3.5). We then cast conditions (3.1)-(3.3) as the following robust program (RP):

$$\text{RP:}\begin{cases} \min\limits_{\Theta} \quad \lambda \\ \text{s.t. } \max\Big\{g_1(\hat{x}, \Theta), g_2(\hat{x}, \Theta), g_3(\Theta), \\ \qquad\qquad \min\limits_{u \in U} g_4(\hat{x}, u, y, \Theta)\Big\} \leq \lambda, \\ \forall \hat{x} \in \widehat{X}, \forall y \in Y, \\ \text{with } \Theta := \big[\lambda; \beta_a; \beta_b; q\big] \in \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{\mathsf{r}_b}, \end{cases} \tag{4.4}$$

where

$$g_1(\hat{x}, \Theta) := \mathfrak{B}(q, \hat{x}) 1_{X_a}(\hat{x}) - \beta_a, \tag{4.5a}$$

$$g_2(\hat{x}, \Theta) := -\mathfrak{B}(q, \hat{x}) 1_{X_b^\epsilon}(\hat{x}) + \beta_b, \tag{4.5b}$$

$$g_3(\Theta) := \beta_a - \beta_b, \tag{4.5c}$$

$$g_4(\hat{x}, u, y, \Theta) := \mathfrak{B}(q, \hat{f}(\hat{x}, u, y)) - \mathfrak{B}(q, \hat{x}), \tag{4.5d}$$

where $1_{X_a}(\hat{x})$ and $1_{X_b^\epsilon}(\hat{x})$ are indicator functions acting on initial and inflated unsafe sets, respectively. Observe that the

RP in (4.4) is non-convex due to the minimization over u. We denote an optimal value of RP by $\lambda_R^\star$. If $\lambda_R^\star \leq 0$, then the satisfaction of conditions (4.5a)-(4.5d) implies the satisfaction of conditions (3.1)-(3.3) in Definition 3.1. Finding an optimal solution for the proposed RP (4.4) is hard in general for two reasons. First, there exist infinitely many constraints in the proposed RP since $\hat{x}$ and y belong to continuous sets, *i.e.,* $\hat{x} \in \hat{X}$ and $y \in Y$. The second difficulty is that one needs to know the exact dynamic of the estimator, *i.e.,* $\hat{f}$ appearing in g_4. To tackle these two difficulties, we use the data sets in Assumption 2 and construct the following scenario program (SP) corresponding to the original RP in (4.4):

$$\text{SP:}\begin{cases}\min\limits_{\Theta} \quad \lambda\\ \text{s.t. } \max\Big\{g_1(\hat{x}_i,\Theta), g_2(\hat{x}_i,\Theta), g_3(\Theta),\\ \qquad\qquad \min\limits_{u\in U} g_4(\hat{x}_i,u,y_k,\Theta)\Big\} \leq \lambda,\\ \forall \hat{x}_i \in \mathcal{D}_{\hat{x}}, \forall y_k \in \mathcal{D}_y,\\ \Theta = \big[\eta;\beta_a;\beta_b;q\big] \in \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}^{\mathsf{r}_b},\end{cases} \tag{4.6}$$

in which functions g_1, g_2, g_3, and g_4 are as in (4.5a)-(4.5d), respectively. We denote an optimal value of the proposed SP by $\lambda_S^\star$. Note that there exists a $\max\text{-}\min$ constraint in (4.6). Solving the SP with this max-min constraint is equivalent to solving a collection of optimization problems, where the size of the collection grows exponentially with respect to $N \times P$. To overcome this challenge, we use the results in [24] and replace the $\max\text{-}\min$ constraint in (4.6) with a single inequality constraint via the following proposition.

Proposition 4.1: The max-min constraint in (4.6), *i.e.,*

$$\max_{\hat{x}_i \in \mathcal{D}_{\hat{x}}, y_k \in \mathcal{D}_y} \ \min_{u_j \in U} g_4(\hat{x}_i, u_j, y_k, \Theta) \leq 0,$$

is satisfied *if and only if* there exists $\alpha^{i,k} = [\alpha_1^{i,k}, \ldots, \alpha_M^{i,k}], \forall i \in \{1,\ldots,N\}$ and $\forall k \in \{1,\ldots,P\}$, such that

$$\forall \hat{x}_i \in \mathcal{D}_{\hat{x}}, \forall y_k \in \mathcal{D}_y, \sum_{j=1}^{M} \alpha_j^{i,k} g_4(\hat{x}_i, u_j, y_k, \Theta) \leq 0, \tag{4.7}$$

with $\sum_{j=1}^{M} \alpha_j^{i,k} = 1, \alpha_j^{i,k} \in \mathbb{R}_{\geq 0}$, where $i \in \{1,\ldots,N\}, j \in \{1,\ldots,M\}$, and $k \in \{1,\ldots,P\}$.

Proposition 4.1 enables us to construct the following scenario program, denoted by SP$^\alpha$, associated with the SP in (4.6):

$$\text{SP}^\alpha\text{:}\begin{cases}\min\limits_{\widetilde{\Theta}} \quad \lambda\\ \text{s.t. } \max\Big\{g_1(\hat{x}_i,\Theta), g_2(\hat{x}_i,\Theta), g_3(\Theta),\\ \qquad\qquad g_4^\alpha(\hat{x}_i,u_1,\ldots,u_M,y_k,\widetilde{\Theta})\Big\} \leq \lambda,\\ \forall \hat{x}_i \in \mathcal{D}_{\hat{x}}, \forall y_k, \mathcal{D}_y,\\ \widetilde{\Theta} := \big[\Theta;\alpha\big]\\ \qquad = \big[\lambda;\beta_a;\beta_b;q;\alpha\big] \in \mathbb{R}\times\mathbb{R}\times\mathbb{R}\times\mathbb{R}^{\mathsf{r}_b}\times(\mathbb{R}_0^+)^{N\times M\times P},\\ \text{with } \alpha = [\alpha_1^{1,1};\ldots;\alpha_M^{N,P}],\end{cases} \tag{4.8}$$

where functions g_1, g_2, and g_3 are as in (4.5a)-(4.5c), respectively, and

$$g_4^\alpha(\hat{x}_i,u_1,\ldots,u_M,y_k,\widetilde{\Theta}) := \sum_{j=1}^{M} \alpha_j^{i,k}\Big(\mathfrak{B}(q,\hat{f}(\hat{x}_i,u_j,y_k)) - \mathfrak{B}(q,\hat{x}_i)\Big),$$
$$\text{with} \sum_{j=1}^{M} \alpha_j^{i,k} = 1, \alpha_j^{i,k} \in \mathbb{R}_0^+, \forall i \in \{1,\ldots,N\}, \forall k \in \{1,\ldots,P\}. \tag{4.9}$$

As a consequence of Proposition 4.1, feasible solutions of SP and SP$^\alpha$ are equivalent in the following sense.

Corollary 4.2: Consider optimization problems SP and SP$^\alpha$ in (4.6) and (4.8), respectively. Then, $\Theta^\star$ is a feasible solution of SP if and only if $\widetilde{\Theta}^\star$ is a feasible solution of SP$^\alpha$.

The proof is a simple consequence of Proposition 4.1 and is omitted here.

Next, we show that the CBC obtained using an optimal solution of the SP$^\alpha$ in (4.8) is a valid CBC for the unknown PO-dt-CS $\mathcal{S}$ in (2.1). To this end, we first propose the following assumption.

Assumption 3: Function $\mathfrak{B}(q,\hat{x})$ in (4.5a) is Lipschitz continuous with respect to $\hat{x}$ with Lipschitz constant $L_1^{\hat{x}}$. Moreover, function $g_4(\hat{x},u_j,y)$ in (4.5d), $j \in \{1,\ldots,M\}$, is also Lipschitz continuous with respect to $\hat{x}$ and y with Lipschitz constants $L_{4,j}^{\hat{x}}$ and $L_{4,j}^{y}$, respectively. We denote the maximum of all these Lipschitz constants with respect to $\hat{x}$ and y by $L_{\max}^{\hat{x}}$ and $L_{\max}^{y}$, *i.e.,* $L_{\max}^{\hat{x}} := \max\{L_1^{\hat{x}}, L_{4,1}^{\hat{x}}, \ldots, L_{4,M}^{\hat{x}}\}$ and $L_{\max}^{y} := \max\limits_{j} L_{4,j}^{y}$.

Note that one can use the estimation technique in [25] to approximate the Lipschitz constants. Moreover, the Lipschitz constants are estimated after $\Theta^\star$ is obtained by solving the SP$^\alpha$ in (4.8). We now propose the main result of the paper.

Theorem 4.3: Let $\mathcal{S}$ in (2.1) be an unknown PO-dt-CS, $\widehat{\mathcal{S}}$ in (2.2) its unknown estimator, and X_a and X_b its initial and unsafe regions, respectively. Suppose Assumptions 2-3 hold. Consider SP$^\alpha$ in (4.8) with its associated optimal solution $\lambda_S^\star$. If the following condition is satisfied

$$L_{\max}^{\hat{x}} d_{\hat{x}} + L_{\max}^{y} d_y + \lambda_S^\star \leq 0, \tag{4.10}$$

with $L_{\max}^{\hat{x}}$ and $L_{\max}^{y}$ as in Assumption 3, $d_{\hat{x}}$ and d_y as in (4.2) and (4.3), respectively, then the PO-dt-CS $\mathcal{S}$ is safe in the sense of Theorem 3.4.

Proof: Here, we show that $\mathfrak{B}(q^\star,\hat{x})$, where $q^\star$ is a feasible solution of SP$^\alpha$, is a CBC satisfying conditions (3.1)-(3.3). Now, since $\lambda_S^\star$ is a feasible solution of SP$^\alpha$ in (4.8), according to Corollary 4.2, it is also a feasible solution of SP in (4.6). Hence, the following conditions hold for all $k \in \{1,\ldots,P\}$ and all $i \in \{1,\ldots,N\}$:

$$g_1(\hat{x}_i,\Theta) \leq \lambda_S^\star, \quad \forall \hat{x}_i \in \mathcal{D}_{\hat{x}}, \tag{4.11}$$

$$g_2(\hat{x}_i,\Theta) \leq \lambda_S^\star, \quad \forall \hat{x}_i \in \mathcal{D}_{\hat{x}}, \tag{4.12}$$

$$g_3(\Theta) \leq \lambda_S^\star, \tag{4.13}$$

$$\min_{u\in U} g_4(\hat{x}_i,u,y_k,\Theta) \leq \lambda_S^\star, \forall \hat{x}_i \in \mathcal{D}_{\hat{x}}, \forall y_k \in \mathcal{D}_y. \tag{4.14}$$

Now consider inequality (4.14). One can readily see from (4.14) that for any $\hat{x}_i$ and any y_k, there exists a choice of $u \in U$, namely $u^\star_{ik}$, such that

$$g_4(\hat{x}_i, u^\star_{ik}, y_k, \Theta) \leq \lambda^\star_S. \tag{4.15}$$

Now, for any $\hat{x} \in \widehat{X}$ and $y \in Y$, there exists, respectively, $\hat{x}_i \in \mathcal{D}_{\hat{x}}$ and $y_k \in \mathcal{D}_y$, $i \in \{1, \ldots, N\}$, $k \in \{1, \ldots, P\}$ such that

$$\begin{aligned} & g_4(\hat{x}, u^\star_{ik}, y, \Theta) - g_4(\hat{x}_i, u^\star_{ik}, y_k, \Theta) \\ & \leq L^{\hat{x}}_{\max}\|\hat{x} - \hat{x}_i\| + L^{y}_{\max}\|y - y_k\| \\ & \leq L^{\hat{x}}_{\max} d_{\hat{x}} + L^{y}_{\max} d_y, \end{aligned} \tag{4.16}$$

where the first inequality follows from the Lipschitz continuity of g_4 with respect to $\hat{x}$ and y in Assumption 3. The second one follows from (4.2) and (4.3) in Assumption 2. Now from (4.10), (4.15), and (4.16), one gets that for all $\hat{x} \in X$ and all $y \in Y$, there exists $u \in U$ such that

$$\min_{u \in U} g_4(\hat{x}, u, y, \Theta) \leq L^{\hat{x}}_{\max} d_{\hat{x}} + L^{y}_{\max} d_y + \lambda^\star_S \leq 0.$$

Hence, $\mathfrak{B}(q^\star, \hat{x})$ satisfies (3.3). Similarly, one can show that $g_z(\hat{x}, \Theta) \leq 0$ where $z \in \{1, 2, 3\}$ as in (4.5a)-(4.5c) if (4.11)-(4.13) hold, respectively. This implies that conditions (3.1) and (3.2) in Definition 3.1 are also satisfied, and therefore, the safety of the PO-dt-CS $\mathcal{S}$ is ensured in the sense of Theorem 3.4. This completes the proof. ■

If (4.10) holds, then the set-valued controller η in (3.4) can be constructed as follows.

Corollary 4.4: Let $\mathfrak{B}$ be a CBC obtained by solving SP$^\alpha$ in (4.8), and $\lambda^\star_S$ be an optimal solution of SP$^\alpha$ such that (4.10) holds. For any $\hat{x} \in \widehat{X}$ and any $y \in Y$, the set-valued controller $\eta : \widehat{X} \times Y \to 2^U$ in (3.4) is constructed as follows:

$$\begin{aligned} \eta(\hat{x}, y) := \big\{ & u \in U \mid \mathfrak{B}(\hat{f}(\hat{x}_i, u, y_k)) - \mathfrak{B}(\hat{x}_i) \leq \lambda^\star_S, \\ & \text{with } \|\hat{x} - \hat{x}_i\| \leq d_{\hat{x}}, \|y - y_k\| \leq d_y, \\ & \exists i \in \{1, \ldots, N\}, \exists k \in \{1, \ldots, P\} \big\}. \end{aligned} \tag{4.17}$$

For the sake of completeness, we present the steps required for utilizing Theorem 4.3 in Algorithm 1.

Algorithm 1 Data-driven safety controller synthesis for unknown PO-dt-CSs

Inputs: N, P, $d_{\hat{x}}$, d_y, and r_b

1: We construct data sets $\mathcal{D}_{\hat{x}}, \mathcal{D}_y$, and $\mathcal{D}$ as in Assumption 2.

2: We solve SP$^\alpha$ using V-K iteration via the acquired data from step 1 and obtain $\lambda^\star_S$.

3: We estimate the Lipschitz constants of function g_4 with respect to $\hat{x}$ and y and consider the largest to be $L^{\hat{x}}_{\max}$ and $L^{y}_{\max}$, respectively.

Outputs: If condition (4.10) is satisfied, then the set-valued controller η in (4.17) associated with the obtained CBC makes the PO-dt-CS safe.

Remark 4.5: Note that here, we do not provide a rigorous method for choosing N and P. However, what might help in the satisfaction of (4.10) is having a smaller $\lambda^\star_S$, as well as smaller values for $d_{\hat{x}}$ and d_y. Unfortunately, these two factors move in opposite directions, leading to a trade-off between reducing $\lambda^\star_S$ and decreasing $d_{\hat{x}}$ and d_y. When we reduce $d_{\hat{x}}$ and d_y, it results in a larger $\lambda^\star_S$. Conversely, to achieve a smaller $\lambda^\star_S$, we must accept larger values for $d_{\hat{x}}$ and d_y.

V. Numerical Example

In this section, we provide a case study in order to illustrate our results. We consider a van der Pol oscillator, adopted from [26], as follows.

$$\mathcal{S} : \begin{cases} x_1(t+1) = x_1(t) + 0.01x_2(t), \\ x_2(t+1) = x_2(t) + 0.01\big(- 1.6x_1^2(t)x_2(t) - x_1(t) \\ \qquad\qquad 1.6x_2(t) + u(t)\big), \\ y(t) = x_2(t) + \sigma(t), \end{cases}$$

where $u \in U := \{0, 0.1, \ldots, 9.5\}$, and $\sigma(t)$ follows a uniform distribution defined over the interval $[0, 0.5]$. The regions of interest are $X_a := [0.9, 1.4] \times [-0.3, 0.3]$, $X_b := [0, 2] \times [-3, -2]$, and $X := [0, 2] \times [-3, 3]$. We assume that the model is unknown. For system $\mathcal{S}$, we design a neural-networks-based estimator as in (2.2) with $\widehat{X} = X^\epsilon$ as the estimator's state set. Furthermore, we compute the estimation accuracy $\epsilon = 0.134$ empirically via data using the results of [20]. Let us fix the structure of our control barrier certificate as $\mathfrak{B}(q, \hat{x}) = [\hat{x}_1^2; \hat{x}_2^2; \hat{x}_1\hat{x}_2; \hat{x}_1; \hat{x}_2; 1]^\top P_q [\hat{x}_1^2; \hat{x}_2^2; \hat{x}_1\hat{x}_2; \hat{x}_1; \hat{x}_2; 1]$. To utilize the results of Theorem 4.3, we fix $N = 900$ and $P = 30$. Then, with $M = 96$, we collect data sets in the form of Assumption 2. By constructing 900 and 30 cover sets for $\widehat{X}$ and Y, respectively, we get $d_{\hat{x}} = 0.0667$ and $d_y = 0.2$. We now have all the ingredients to solve SP$^\alpha$. Note that $g_4^\alpha(\hat{x}_i, u_1, \ldots, u_M, y_k, \widetilde{\Theta})$ in SP$^\alpha$ (4.8) contains a bilinearity between the decision variables $\alpha_j^{i,k}$ and q, *i.e.*, the coefficients of the CBC. In order to tackle this bilinearity, we make use of the idea of V-K iteration [27]. To do so, we first fix the template of the CBC by restricting the degree of the polynomial. Then, the bilinear programming problem can be replaced with a linear programming problem by taking an initial guess for variables $\alpha_j^{i,k} \in \mathbb{R}_0^+$, such that $\sum_{j=1}^M \alpha_j^{i,k} = 1, \forall i \in \{1, \ldots, N\}$ and $\forall k \in \{1, \ldots, P\}$. We use $\alpha_j^{i,k} = \frac{1}{M}$ as the initial guess [24]. The coefficients of the candidate CBC, as well as β_a, β_b, and λ can then be found by solving the acquired linear programming problem using a solver such as MOSEK [28]. We now consider the coefficients of the CBC to be fixed and solve a linear programming problem over the variables $\alpha_j^{i,k}, \beta_a, \beta_b$, and λ. By solving the SP$^\alpha$, we obtain $\beta_a = 10.26$, $\beta_b = 20.35$, and $\lambda^\star_S = -0.0936$. Finally, we estimate the Lipschitz constants as $L^{\hat{x}}_{\max} = 1.009$ and $L^{y}_{\max} = 0.0897$. Then, we get $L^{\hat{x}}_{\max} d_{\hat{x}} + L^{y}_{\max} d_y + \lambda^\star_S = -0.0083 \leq 0$ satisfying (4.10). To simulate the system, we randomly select 10 initial states from the initial state set and simulate the system and its estimator for 500 time steps. Closed-loop state trajectories of the system are illustrated in Figure 1. As observed in Figure 1, the initial set X_a and the

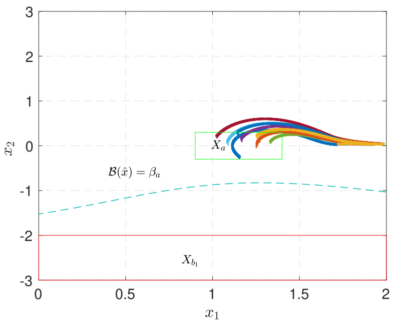

Fig. 1. A few realizations of the closed-loop trajectories of the van der Pol oscillator. The green dash line shows the β_a level set of $\mathfrak{B}$.

ϵ-inflated version of the unsafe set X_b is separated through the β_a-level set of the CBC. This visualization demonstrates that the synthesized controller, which is based on estimated states, effectively prevents the system trajectories starting from X_a from entering X_b.

VI. Conclusion

In this work, we have presented a data-driven approach for the synthesis of safety controllers in partially-observable discrete-time control systems with unknown dynamics. Our method revolves around the construction of control barrier certificates (CBCs) specifically for the estimator. We assume that the dynamics of the estimator are unknown, but we have knowledge of an upper bound on the estimation accuracy. By leveraging a scenario program (SP$^\alpha$), which can be solved using a finite amount of data collected from the system and its estimator, we compute the CBCs. A key aspect of our approach is the inclusion of a condition on the feasible solutions obtained from SP$^\alpha$. This condition plays a crucial role in ensuring the safety of the unknown system. By satisfying this condition, we provide a rigorous safety guarantee for the partially-observable system with unknown dynamics. Finally, we demonstrated the effectiveness of our approach via a case study.

References

[1] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada, "Control barrier functions: Theory and applications," in *2019 18th European control conference (ECC)*. IEEE, 2019, pp. 3420–3431.

[2] A. Clark, "Control barrier functions for complete and incomplete information stochastic systems," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 2928–2935.

[3] ——, "Control barrier functions for stochastic systems," *Automatica*, vol. 130, p. 109688, 2021.

[4] N. Jahanshahi, A. Lavaei, and M. Zamani, "Compositional construction of safety controllers for networks of continuous-space pomdps," *arXiv preprint arXiv:2103.05906*, 2021.

[5] N. Jahanshahi, P. Jagtap, and M. Zamani, "Synthesis of stochastic systems with partial information via control barrier functions," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 2441–2446, 2020.

[6] ——, "Synthesis of partially observed jump-diffusion systems via control barrier functions," *IEEE Control Systems Letters*, vol. 5, no. 1, pp. 253–258, 2020.

[7] N. Noroozi, A. Salamati, and M. Zamani, "Data-driven safety verification of discrete-time networks: a compositional approach," *IEEE Control Systems Letters*, vol. 6, pp. 2210–2215, 2021.

[8] A. Lavaei, A. Nejati, P. Jagtap, and M. Zamani, "Formal safety verification of unknown continuous-time systems: a data-driven approach," in *Proceedings of the 24th International Conference on Hybrid Systems: Computation and Control*, 2021, pp. 1–2.

[9] 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, 2014.

[10] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems," *7th IFAC Conference on Analysis and Design of Hybrid Systems*, 2021.

[11] 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*. PMLR, 2022, pp. 441–452.

[12] ——, "Safety verification of stochastic systems: A repetitive scenario approach," *IEEE Control Systems Letters*, vol. 7, pp. 448–453, 2022.

[13] N. Jahanshahi and M. Zamani, "Synthesis of controllers for partially-observable systems: A data-driven approach," *IFAC-PapersOnLine*, 2023.

[14] H. A. Talebi, F. Abdollahi, R. V. Patel, and K. Khorasani, *Neural network-based state estimation of nonlinear systems: application to fault detection and isolation*. Springer, 2009, vol. 395.

[15] Y. Weng, R. Negi, and M. D. Ilić, "Historical data-driven state estimation for electric power systems," in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2013, pp. 97–102.

[16] N. Yadaiah and G. Sowmya, "Neural network based state estimation of dynamical systems," in *The 2006 IEEE international joint conference on neural network proceedings*. IEEE, 2006, pp. 1042–1049.

[17] D. Georges, "Machine learning for receding horizon observer design: Application to traffic density estimation," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 616–621, 2020.

[18] T. Breiten and K. Kunisch, "Neural network based nonlinear observers," *Systems & Control Letters*, vol. 148, p. 104829, 2021.

[19] R. Zhan and J. Wan, "Neural network-aided adaptive unscented kalman filter for nonlinear state estimation," *IEEE Signal Processing Letters*, vol. 13, no. 7, pp. 445–448, 2006.

[20] A. Quattrini Li, A. Coskun, S. M. Doherty, S. Ghasemlou, A. S. Jagtap, M. Modasshir, S. Rahman, A. Singh, M. Xanthidis, J. M. O'Kane *et al.*, "Experimental comparison of open source vision-based state estimation algorithms," in *2016 International Symposium on Experimental Robotics*. Springer, 2017, pp. 775–786.

[21] J. Wilson and L. Zorzetto, "A generalised approach to process state estimation using hybrid artificial neural network/mechanistic models," *Computers & chemical engineering*, vol. 21, no. 9, pp. 951–963, 1997.

[22] M. Marchi, J. Bunton, B. Gharesifard, and P. Tabuada, "Safety and stability guarantees for control loops with deep learning perception," *IEEE Control Systems Letters*, 2021.

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

[24] C. Kirjner-Neto and E. Polak, "On the conversion of optimization problems with max-min constraints to standard optimization problems," *SIAM Journal on Optimization*, vol. 8, no. 4, pp. 887–915, 1998.

[25] G. Wood and B. Zhang, "Estimation of the lipschitz constant of a function," *Journal of Global Optimization*, vol. 8, no. 1, pp. 91–103, 1996.

[26] A. Clark, "A semi-algebraic framework for verification and synthesis of control barrier functions," *arXiv preprint arXiv:2209.00081*, 2022.

[27] A. Hassibi, S. P. Boyd, and J. P. How, "Control of asynchronous dynamical systems with rate constraints on events," in *Proceedings of the 38th IEEE Conference on Decision and Control*, vol. 2. IEEE, 1999, pp. 1345–1351.

[28] M. ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 9.3*, 2022. [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html