IEEE Control Systems Letters paper presented at
2024 IEEE 63rd Conference on Decision and Control (CDC)
December 16-19, 2024. MiCo, Milan, Italy

Data-Driven Controller Synthesis via Co-Büchi Barrier Certificates with Formal Guarantees

Daniel Ajeleye, *Graduate Student Member, IEEE*, and Majid Zamani, *Senior Member, IEEE*

***Abstract*— In this paper, we introduce a data-driven framework for synthesizing controllers that enforce properties expressed by so-called ℓ universal co-Büchi automata (ℓ-UCA) over control systems with finite input sets and unknown mathematical models. The proposed framework leverages the notion of co-Büchi control barrier certificates (CBC). These certificates, together with their corresponding controllers, guarantee that a region in the state set is visited finitely often as the system evolves, limiting visits to at most ℓ times. The CBC is defined over a domain that augments the system and the ℓ-UCA, incorporating a counter variable to track the number of visits to the accepting states of ℓ-UCA. However, constructing these CBCs typically requires precise knowledge of the dynamics of the system, which is often unavailable in real-world applications. Therefore, we propose a data-driven scheme where we initially formulate the CBC conditions as a robust optimization program (ROP). Since the unknown model appears in some of the ROP constraints, we employ sampled data points collected from the system's trajectories to formulate a scenario optimization program (SOP) associated with the ROP. By solving the corresponding SOP, we construct CBCs and controllers that enforce ℓ-UCA properties for the unknown system with a formal correctness guarantee. The efficacy of our data-driven approach is demonstrated by applying it to a three-tank system whose dynamics is assumed to be unknown.**

I. Introduction

In the last two decades, formal methods have gained considerable attention in the hybrid systems community. They offer formal analyses for complex dynamical systems. However, it remains highly challenging to provide formal verification and controller synthesis frameworks for complex systems to enforce high-level logic properties. These properties, such as those formally expressed as temporal logic formulae or languages specified by automata [1], require significant efforts to ensure their satisfaction. Challenges include the continuity of state sets, the handling of complex logic requirements, and the absence of closed-form mathematical models in numerous real-world applications.

To address these challenges, there is a growing focus on employing data-driven abstraction-based methods to synthesize controllers that are correct-by-construction for systems with (partially) unknown dynamics [2]. Examples of such efforts include the results in [3]–[6], which predominantly utilize discretization-based approaches. The proposed schemes in those results provide formally correct controllers for ω-regular properties.

This work was supported by the NSF CAREER grant CNS-2145184, CNS-2111688, and CNS-2039062.

D. Ajeleye and M. Zamani are with the Department of Computer Science, University of Colorado Boulder, USA. Email: {daniel.ajeleye,majid.zamani}@colorado.edu.

An alternative approach, which is discretization free, initially proposed in [7], involves utilizing barrier certificates as an abstraction-free method for formally verifying and synthesizing controllers for dynamical systems. Barrier certificates are similar to Lyapunov functions, with level sets that separate an unsafe region from the trajectories of the system originating from a given initial set. Consequently, the existence of such a function offers a (probabilistic) safety guarantee for the concrete system. However, in the automata-theoretic verification approach, the primary concern is determining whether a set of states can be visited only finitely often. Recent results in [8], inspired by bounded synthesis methods [9], [10], introduce an abstraction-free method for automata-theoretic verification of discrete-time dynamical systems. This approach introduces the notion of co-Büchi barrier certificates (CBC), which provide sufficient conditions to verify systems against ω-regular properties described by universal co-Büchi automata (UCA).

A co-Büchi barrier certificate is a real-valued function defined over the product of a system and an automaton, whose conditions ensure that the accepting states of the automaton are visited only finitely often. This certificate incorporates a counter value, which tracks the number of times an accepting state is visited. The search for this certificate is based on a preselected upper bound on the number of visits. Upon a successful search, the system can be verified to meet the specification represented by the automaton. Unfortunately, the framework for constructing CBCs, as described in [8], requires precise models for the corresponding analyzes. Consequently, these techniques cannot be employed when the system model is unknown, which is often the case in real-world applications. In this paper, we introduce a novel data-driven technique for constructing CBCs, without performing any system identification, as done in [11], [12].

Contributions. The main goal of this paper is to introduce a data-driven technique for constructing CBCs and synthesizing controllers to ensure that an unknown system satisfies an ω-regular property described by an ℓ-UCA in which ℓ bounds the number of visits to the accepting states of the automaton. We consider systems with finite input sets and unknown mathematical models. We begin by formulating the conditions of CBC as a robust optimization program (ROP). Since the unknown model appears in some of the ROP's constraints, we utilize sampled data points collected from the system's trajectories to formulate a scenario optimization program (SOP) associated with the ROP. By solving the resulting SOP, we construct CBCs together with controllers that formally guarantee the enforcement of the ℓ-UCA prop-

erties for the unknown system.

Related Work. In recent years, limited studies have explored the formal analysis of unknown dynamical systems using data-driven and abstraction-free approaches. Our method is applicable to all classes of nonlinear discrete-time control systems, unlike the approach in [13], which is tailored solely to nonlinear polynomial-type systems. While the findings in [14], [15] concentrate on data-driven methods for unknown dynamical systems using control barrier certificates with certain probabilistic confidence levels, our approach is designed to construct CBCs with a confidence level of 1 using noise-free data. Additionally, we assume that an accurate upper bound for the system's Lipschitz constant is available. The methods in [13]–[16] provide control barrier certificates and controllers to ensure that the trajectories of an unknown system originating from a given set never reach an unsafe region. Our approach distinguishes itself by developing a systematic data-driven framework to construct CBCs. It generalizes classic barrier certificates to ensure that the trajectories of an unknown system visit a specified region at most a fixed number of times. This enhancement broadens the applicability of barrier certificates for ω-regular properties, providing a more general framework for system analysis and design. We direct interested readers to [8] for a comprehensive understanding of the differences between CBC and traditional barrier certificates.

II. Preliminaries and Definitions

A. Notation

Symbols $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ represent sets of real and non-negative real numbers, respectively. Notation $\cap$, $\cup$, and $\setminus$ indicate, respectively, set intersection, union and set difference. The symbol $\mathbb{N}$ denotes the set of natural numbers including 0 and for any $n \in \mathbb{N}$, $\mathbb{N}_{\geq n} = \{i \in \mathbb{N} \mid i \geq n\}$. In the case where $a, b \in \mathbb{N}$ and $a < b$, we employ the notations $(a; b)$, and $[a; b]$ to represent, respectively, the open and closed intervals in $\mathbb{N}$. Similarly, for $a, b \in \mathbb{R}$ and $a < b$, we use (a, b), and $[a, b]$ to represent the corresponding intervals in $\mathbb{R}$. For any non-empty set Q, notation $\mathcal{C}_d(Q)$ depicts the cardinality of Q, while Q^ω indicates the set of infinite-length sequences from Q, *i.e.,* $Q^\omega := \{\langle w_i \rangle_{i=0}^{\infty} \mid w_i \in Q \ \forall i \in \mathbb{N}\}$. We denote the indicator function of $A \subseteq Q$ by $\mathbf{1}_A : Q \to \{0, 1\}$, where $\mathbf{1}_A(x) = 1$ if and only if $x \in A$, and 0 otherwise. Given K vectors $v_l \in \mathbb{R}^{k_l}$, $k_l \in \mathbb{N}$, and $l \in [1; K]$, we use $v = [v_1; \ldots; v_K]$ to denote the corresponding column vector of dimension $\sum_l k_l$. Assuming $c \in \mathbb{R}^n$, $\|c\|$ means the infinity norm of c. For any $B \subseteq \mathbb{R}^n$ and $\varepsilon > 0$, notation $\Phi_\varepsilon(\tilde{b})$ is interpreted as $\{b \in B \mid \|b - \tilde{b}\| \leq \varepsilon\}$. Therefore, we create a partition of B into cells $\Phi_\varepsilon(\tilde{b})$ such that $B \subseteq \bigcup_{\tilde{b} \in [B]_\varepsilon} \Phi_\varepsilon(\tilde{b})$, where $[B]_\varepsilon$ denotes a finite set of representative points picked from those partition sets.

B. Universal Co-Büchi Automaton

Here, in accordance with the definition outlined in [9], we first introduce a variation of a *deterministic* universal co-Büchi automaton, whose acceptance criterion encompasses an atmost ℓ visitation to the accepting states for some $\ell \in \mathbb{N}$.

Definition 2.1: Given $\ell \in \mathbb{N}$, a deterministic ℓ-Universal Co-Büchi Automaton (ℓ-UCA) $\mathcal{A}$ is a tuple $(Q, \Delta, \varrho, Q_0, Q_F)$, where: Q is a finite set of states, Δ is a finite alphabet, $\varrho : Q \times \Delta \to Q$ is a transition map, where $\mathcal{C}_d(\varrho(q, \varsigma)) \leq 1 \ \forall q \in Q$ and $\forall \varsigma \in \Delta$, and $Q_0, Q_F \subseteq Q$, respectively, denotes the initial and final (accepting) set of states, where the acceptance condition is that Q_F is visited at most ℓ times. Consider a *word* $\mathbf{v} = \langle \varsigma_i \rangle_{i=0}^{\infty} \in \Delta^\omega$. A *run* of $\mathcal{A}$ over $\mathbf{v}$ is an infinite sequence of states, $\mathbf{q} = \langle q_i \rangle_{i=0}^{\infty} \in Q^\omega$, where $q_0 \in Q_0$ and $q_{i+1} = \varrho(q_i, \varsigma_i) \ \forall i \in \mathbb{N}$. Therefore, we say the word $\mathbf{v} \in \Delta^\omega$ is accepted by $\mathcal{A}$ if for every run $\mathbf{q}$ of $\mathcal{A}$ over $\mathbf{v}$, it holds that $\mathcal{C}_d(\{q_i \in Q \mid \mathbf{q} = \langle q_i \rangle_{i=0}^{\infty} \in Q^\omega\} \cap Q_F) \leq \ell$. In essence, every run of $\mathcal{A}$ over $\mathbf{v}$ visits some accepting states at most ℓ times. We define the language of a ℓ-UCA $\mathcal{A}$, denoted by $\mathcal{L}(\mathcal{A})$, as the collection of words accepted by it.

Note that to consider non-deterministic ℓ-UCA, one requires to deal with deterministic Rabin or Streett automata [17]. Due to space limitations, we focuses on deterministic ℓ-UCA here.

C. Discrete-Time Control Systems

In this paper, we define the underlying model as discrete-time control systems.

Definition 2.2: A discrete-time control system (dt-CS) Ξ is represented as a tuple (X, X_0, U, f), where:

- $X \subseteq \mathbb{R}^n$ is the state set and $X_0 \subseteq X$ denotes the set of initial states;
- $U = \{u_i \in \mathbb{R}^m \mid i \in [1; M]\}$ with $M \in \mathbb{N}_{\geq 1}$, is the finite input set;
- $f : X \times U \to X$ is the transition function, whereby for an input signal $\nu : \mathbb{N} \to U$, the state evolves as

$$x(t+1) = f(x(t), \nu(t)), \ \forall t \in \mathbb{N}. \tag{1}$$

Furthermore, we denote the state trajectory of dt-CS Ξ, under the input trajectory $\nu(\cdot)$, and starting from $x_0 \in X_0$ by $x_{x_0,\nu} = \langle x_t \rangle_{t=0}^{\infty} \in X^\omega$, such that $x_{x_0,\nu}(t) = x_t$ and $x_{t+1} = f(x_t, \nu(t)), \ \forall t \in \mathbb{N}$. We introduce a labeling function, denoted as $L : X \to \Delta$, which assigns a symbol from a finite alphabet Δ to each state of the dt-CS. This concept naturally extends to sequences, allowing us to map a sequence $\langle x_t \rangle_{t=0}^{\infty} \in X^\omega$ to a sequence of symbols $\langle L(x_t) \rangle_{t=0}^{\infty} \in \Delta^\omega$. Consequently, we have the flexibility to assign different labels from Δ to regions within X.

We assume that the map f in (1) is *unknown* throughout this work. Our primary objective is to synthesize controllers for a dt-CS with unknown f to guarantee that it adheres to a property defined by a given ℓ-UCA. We will formalize this objective in the next subsection.

D. Co-Büchi Control Barrier Certificates

Consider a dt-CS $\Xi = (X, X_0, U, f)$ and an ℓ-UCA $\mathcal{A} = (Q, \Delta, \varrho, Q_0, Q_F)$ as in Definitions 2.2 and 2.1, respectively. Let $L : X \to \Delta$ be a labeling function. A state sequence $\mathbf{x} = \langle x_i \rangle_{i=0}^{\infty} \in X^\omega$ of Ξ is accepted by the ℓ-UCA $\mathcal{A}$ if the augmented state sequence $\hat{\mathbf{x}} = \langle (x_i, q_i) \rangle_{i=0}^{\infty} \in (X \times Q)^\omega$ has at most ℓ-states in $X \times Q_F$, where $(x_0, q_0) \in X_0 \times Q_0$. If

so, we say that dt-CS Ξ satisfies $\mathcal{A}$. To establish this, we employ the notion of co-Büchi barrier certificate [8], which is defined next. Here, a counter variable is appended to the state space, which tracks the number of times an augmented state $(x, q) \in X \times Q$ has appeared in $X \times Q_F$.

Definition 2.3: Consider a dt-CS Ξ and an ℓ-UCA $\mathcal{A}$ as in Definitions 2.2 and 2.1, respectively, with $L : X \to \Delta$ being a labeling function. For any $(q, r) \in Q \times \mathbb{N}$, characterized function $\mathcal{B}_{q,r} : X \to \mathbb{R}$ is a co-Büchi barrier certificate (CBC) for Ξ over the property specified by $\mathcal{A}$ if there exists $\lambda, \gamma \in \mathbb{R}$ such that $\lambda > \gamma$ and

$$\mathcal{B}_{q,0}(x) \leq \gamma, \ \forall x \in X_0, q \in Q_0 \setminus Q_F, \tag{2}$$

$$\mathcal{B}_{q,1}(x) \leq \gamma, \ \forall x \in X_0, q \in Q_0 \cap Q_F, \tag{3}$$

$$\mathcal{B}_{q,\ell+1}(x) > \lambda, \ \forall x \in X, q \in Q_F, \tag{4}$$

and for all states $x \in X$, $q \in Q$, counter values $r \in [0; \ell]$, one has

$$\min_{u \in U} \big\{\mathcal{B}_{q',r'}(f(x,u))\big\} \leq \mathcal{B}_{q,r}(x), \tag{5}$$

$$\text{where } q' = \varrho(q, L(x)) \text{ and } r' = \begin{cases} r & \text{if } q' \notin Q_F \\ r+1 & \text{otherwise,} \end{cases} \tag{6}$$

Note that for any $(q, r) \in Q \times [0; \ell]$, one can develop a set-valued controller $\kappa_{q,r} : X \rightrightarrows U$ built on the CBC $\mathcal{B}_{q,r}$ as follows:

$$\kappa_{q,r}(x) = \big\{u \in U \mid \mathcal{B}_{q',r'}(f(x,u)) \leq \mathcal{B}_{q,r}(x)\big\}, \tag{7}$$

where q' and r' are defined as in (6).

Remark 2.4: Given equation (7), the controller is enforcing the specifications outlined by an ℓ-UCA over a dt-CS and operates within the augmented space $X \times Q \times [0; \ell]$. This controller is history-dependent, relying on the state of the dt-CS, ℓ-UCA, and the counter variable.

Although the underlying dynamics of dt-CS are deemed unknown, its trajectories are accessible. For a suitable grid parameter $\varepsilon > 0$, these trajectories are sampled as $N \times M$ data points in a set

$$\mathcal{D}_{N,\varepsilon} = \big\{(\tilde{x}_i, u_j, f(\tilde{x}_i, u_j)) \,|\, \tilde{x}_i \in [X]_\varepsilon \text{ and } u_j \in U, \ \forall i \in [1; N],\, j \in [1; M]\big\}. \tag{8}$$

Noted that $f(\tilde{x}_i, u_j)$ in (8) is the one time step transition of the unknown dt-CS starting from $\tilde{x}_i$ under input u_j.

In Section III, we elaborate on how the controller $\kappa_{q,r}$ is designed relying on the data set $\mathcal{D}_{N,\varepsilon}$ for any $(q, r) \in Q \times [0; \ell]$. Next, we proceed to formalize the major problem that we aim to address in this paper.

Problem 2.5: Suppose Ξ is a dt-CS with map f being unknown and let $\mathcal{A}$ be an ℓ-UCA as in Definition 2.2 and 2.1, respectively. Given a labeling function L, develop a data-driven approach based on the data set $\mathcal{D}_{N,\varepsilon}$ to design a controller κ, so that for all state trajectory $\langle x_t \rangle_{t=0}^{\infty}$ of Ξ, we have $\langle L(x_t) \rangle_{t=0}^{\infty} \in \mathcal{L}(\mathcal{A})$.

In this paper, we derive a controller to address Problem 2.5 by utilizing the concept of CBCs. Inspired by [8, Theorem 6], the following theorem illustrates the effectiveness of CBCs, as outlined in Definition 2.3, in meeting the specifications set forth by an ℓ-UCA.

Theorem 2.6: Consider a dt-CS Ξ and an ℓ-UCA $\mathcal{A}$ with a given labeling map L. For any $(q, r) \in Q \times [0; \ell+1]$, suppose that $\mathcal{B}_{q,r}$ is a CBC for Ξ and $\mathcal{A}$ as in Definition 2.3. Then the augmented state sequence $\langle (x_i, q_i) \rangle_{i=0}^{\infty} \in (X \times Q)^\omega$ visits $X \times Q_F$ at most ℓ times.

Proof: We establish the proof by contradiction. Suppose there exists an augmented state sequence $\hat{\mathbf{x}} = \langle (x_i, q_i) \rangle_{i=0}^{\infty} \in (X \times Q)^\omega$ that visits $X \times Q_F$ more than ℓ times, where $x_{t+1} = f(x_t, \nu(t))$ and $q_{t+1} = \varrho(q_t, L(x_t)), \ \forall t \in \mathbb{N}$. Let $t' \in \mathbb{N}_{\geq 1}$ be the first index when $\hat{\mathbf{x}}$ visits $X \times Q_F$ for the $(\ell+1)$th time. Based on this assumption, we can infer that for every trajectory $x_{x_0,\nu}(s)$ of Ξ, where $s < t'$ and $\nu(s) \in \kappa(x(s))$, it visits $X \times Q_F$ at most $\ell_s \leq \ell$ times. Thus, proceeding inductively on s results in (2) or (3) achieving $\mathcal{B}_{q_s,\ell_s}(x_s) \leq \gamma$. Now, we apply (5) for $x_{t'}$ and $x_{t'-1}$, to recursively show that $\mathcal{B}_{q_{t'},\ell+1}(x_{t'}) \leq \mathcal{B}_{q_{t'-1},\ell}(x_{t'-1}) \leq \gamma$. Therefore, condition (4) yields $\lambda < \mathcal{B}_{q_{t'},\ell+1}(x_{t'}) \leq \gamma$, which contradicts condition $\gamma < \lambda$ and thus ends the proof. ■

III. Data-Driven Construction of CBC

Here, our focus is on constructing CBC using data acquired from the trajectories of the system, as in (8). Within our data-driven framework and for any $(q, r) \in Q \times [0; \ell+1]$, we fix the CBC structure as $\mathcal{B}_{q,r}(c, x) = \sum_{j=1}^{k} c_{q,r}^j \varphi^j(x)$ with user-defined (possibly nonlinear) basis functions $\varphi^j(x)$ and $p := k \times \mathcal{C}_d(Q) \times (\ell+1)$ unknown coefficients, which are stacked in a vector $c \in \mathbb{R}^p$. It is noteworthy that the basis functions φ^j can assume any arbitrary form. For instance, they can take the form of monomials over x if a polynomial-type CBC is desired.

Designing a controller that solves Problem 2.5 involves simply constructing a CBC as in Definition 2.3. Therefore, to achieve this objective, we frame the search for the CBC as the next robust optimization program (ROP):

$$\begin{cases} \min\limits_{d} \quad \eta, \\ \textbf{s.t.} \ \max\{\gamma - \lambda, g_s(x,d)\} \leq \eta, \ \forall s \in [1;3] \text{ and} \\ \qquad \forall x \in X, \ \forall q \in Q, \ \forall r \in [0; \ell] \\ \qquad \text{with } q' \text{ and } r' \text{ defined in (6),} \\ \qquad \min\limits_{u \in U} \big\{\mathcal{B}_{q',r'}(c, f(x,u))\big\} - \mathcal{B}_{q,r}(c,x) \leq \eta, \qquad \text{(9a)} \\ \qquad c \in \mathbb{R}^p \text{ and } d = [\eta; \gamma; \lambda; c] \in \mathbb{R}^{p+3}, \qquad \text{(9b)} \end{cases}$$

where $\forall x \in X$, $\forall q \in Q$:

$$\begin{aligned} g_1(x,d) &= (\mathcal{B}_{q,0}(c,x) - \gamma)\mathbf{1}_{X_0}(x)\mathbf{1}_{Q_0 \setminus Q_F}(q), \\ g_2(x,d) &= (\mathcal{B}_{q,1}(c,x) - \gamma)\mathbf{1}_{X_0}(x)\mathbf{1}_{Q_0 \cap Q_F}(q), \\ g_3(x,d) &= (-\mathcal{B}_{q,\ell+1}(c,x) + \lambda)\mathbf{1}_{Q_F}(q). \end{aligned} \tag{10}$$

It is evident that if $\eta \leq 0$, a solution to the ROP in (9) guarantees the fulfillment of conditions (2)-(5) as outlined in Definition 2.3. However, solving the ROP presents two significant challenges. Firstly, the ROP involves infinitely many constraints due to the continuous state set of the discrete-time control system (dt-CS), where $x \in X \subseteq \mathbb{R}^n$. Secondly, solving the ROP requires knowledge of the map f, which remains unknown in our work. To overcome these challenges, we propose a data-driven approach to construct

CBCs without directly solving the ROP. Utilizing the sampled data in (8), we introduce a subsequent optimization problem associated with the ROP, which is called scenario optimization program (SOP):

$$\begin{cases} \min\limits_{d} \quad \eta, \\ \textbf{s.t.} \ \max\{\gamma-\lambda, g_s(\tilde{x}_i,d)\}\leq \eta,\ \forall s\in[1;3] \text{ and} \\ \qquad \forall i\in[1;N],\ \forall q\in Q,\ \forall r\in[0;\ell] \\ \qquad \text{with } q' \text{ and } r' \text{ defined in (6)}, \\ \qquad \min\limits_{u\in U}\left\{\mathcal{B}_{q',r'}(c,f(\tilde{x}_i,u))\right\}-\mathcal{B}_{q,r}(c,\tilde{x}_i)\leq\eta, \quad \text{(11a)} \\ \qquad c\in\mathbb{R}^p \text{ and } d=[\eta;\gamma;\lambda;c]\in\mathbb{R}^{p+3}, \quad \text{(11b)} \end{cases}$$

where g_1, g_2, and g_3 are the functions defined in (10). Note that conditions (11a) can be reformulated as max-min constraints:

$$\max_{\substack{i\in[1;N],\\ q\in Q\setminus Q_F,\\ r\in[0;\ell]}}\left[\min_{u\in U}\left\{\mathcal{B}_{q',r'}(c,f(\tilde{x}_i,u))\right\}-\mathcal{B}_{q,r}(c,\tilde{x}_i)\right]\leq\eta. \tag{12}$$

Typically, an optimization problem with max-min constraints can be equivalently represented as a series of optimization problems with inequality constraints. Handling such a problem may pose computational challenges due to the extensive collection involved. Therefore, we adopt the strategy proposed in [18], converting this condition into a nonlinear programming problem. The condition is then expressed as a single inequality constraint, defined as follows, for all $q\in Q$, $i\in[1;N]$, and $r\in[0;\ell]$:

$$\sum_{j=1}^{M}\rho_j\big(\mathcal{B}_{q',r'}(c,f(\tilde{x}_i,u_j))-\mathcal{B}_{q,r}(c,\tilde{x}_i)\big)\leq\eta, \tag{13}$$

where $\sum_{j=1}^{M}\rho_j=1$ such that $\rho_j\in\mathbb{R}_{\geq 0}$. One can employ [18, Proposition 2.1] to demonstrate the equivalence between the conditions in (13) and the max-min constraints in (12). Consequently, the vector of decision variables of SOP (11) as in (11b) becomes $d=[\eta;\gamma;\lambda;c;\rho_1;\ldots;\rho_M]\in\mathbb{R}^{M+p+3}$. One can readily utilize available software tools to solve the resulting optimization problem. In the next section, we establish a formal relation between a feasible solution of SOP in (11) and that of ROP in (9).

IV. Satisfaction Guarantee

In this section, we unveil a result, which establishes that a solution to the SOP in (11) constructs a CBC for an unknown dt-CS, and accordingly provides a controller that enforces the satisfaction of the specification expressed by a given ℓ-UCA over an unknown dt-CS. To achieve this, we first introduce the ensuing assumption.

Assumption 1: Suppose that for all $(q,r)\in Q\times[0;\ell]$, $\mathcal{B}_{q',r'}(c,f(x,u))-\mathcal{B}_{q,r}(c,x)$ and $\mathcal{B}_{q,r}(c,x)$ are Lipschitz continous with respect to x with Lipschitz constants $\mathscr{L}_a$ and $\mathscr{L}_b$, respectively, for any input $u\in U$ where q' and r' are defined in (6).

Remark 4.1: Note that the methods proposed in [19], particularly [16, Algorithm 1], offer a technique for estimating the Lipschitz constants $\mathscr{L}_a$ and $\mathscr{L}_b$ utilizing a finite dataset from an unknown system. However, for the scope of this work, we assume that accurate upper bounds for these constants are known. Additionally, we presume that the data sampled from system trajectories are noise-free. Consequently, we are able to present our main results (cf. Theorem 4.3) with a 100% correctness guarantee.

Remark 4.2: To gather data points in (8) for a given parameter ε, the number of samples N can be determined by the relation: $Vol(X)=N\varepsilon^n$, where $Vol(\cdot)$ denotes the volume of a set. Consequently, the required number of samples grows exponentially with the dimension of the system. Moreover, selecting a smaller ε results in more sampled data, thus increasing the number of constraints in the SOP, and extending the time required to solve the SOP. It is also worth noting that the number of constraints in SOP (11) using (13) are at most of the order of N, for a fixed number of CBC basis functions. Therefore, the complexity of solving the problem is polynomial in $N\ell\mathcal{C}_d(Q)\mathcal{C}_d(\Delta)$.

In accordance with Assumption 1, the following result introduces a data-driven approach for constructing a CBC with a 100% correctness guarantee.

Theorem 4.3: Given an unknown dt-CS as in (1), an ℓ-UCA $\mathcal{A}$ as in Definition 2.1 and let Assumption 1 hold. Suppose that SOP (11) is solved using the data set $\mathcal{D}_{N,\varepsilon}$ in (8), resulting in an optimal solution $d^*=[\eta_S^*;\gamma^*;\lambda^*;c^*]$ in (11b). If

$$\mathscr{L}\varepsilon+\eta_S^*\leq 0, \tag{14}$$

with $\mathscr{L}=\max\{\mathscr{L}_a,\mathscr{L}_b\}$, then for all $(q,r)\in Q\times[0;\ell]$, functions $\mathcal{B}_{q,r}$ constructed by solving SOP in (11) are CBC for the unknown dt-CS.

Proof: We show that under condition (14), the constructed $\mathcal{B}_{q,r}$ via solving SOP in (11) ensures that dt-CS satisfies the property expressed by ℓ-UCA $\mathcal{A}$, in the sense of Theorem 2.6. One can easily verify that (14) implies $\eta_S^*\leq 0$. Therefore, condition $\gamma^*<\lambda^*$ is always satisfied. Note that for every $x\in X$, there is a data point $\tilde{x}_i$ such that $x\in\Phi_\varepsilon(\tilde{x}_i)$. Thus, $\forall i\in[1;N]$, $\forall x\in X_0$ and $\forall q\in Q_0\setminus Q_F$, one gets

$$\begin{aligned}\mathcal{B}_{q,0}(c^*,x)-\gamma^*&=\mathcal{B}_{q,0}(c^*,x)-\mathcal{B}_{q,0}(c^*,\tilde{x}_i)+\mathcal{B}_{q,0}(c^*,\tilde{x}_i)\\&\quad-\gamma^*\leq\mathscr{L}_b\|x-\tilde{x}_i\|+\eta_S^*\leq\mathscr{L}\varepsilon+\eta_S^*\leq 0.\end{aligned}$$

The same line of reasoning as described above can be employed to establish that

$$\begin{aligned}\mathcal{B}_{q,1}(c^*,x)-\gamma^*\leq 0 \quad \forall x\in X_0,\ q\in Q_0\cap Q_F \text{ and}\\ -\mathcal{B}_{q,\ell+1}(c^*,x)+\lambda^*\leq 0 \quad \forall x\in X,\ q\in Q_F.\end{aligned}$$

Furthermore, it can be readily observed from (11a), that for all $\tilde{x}_i$, $i\in[1;N]$, there is a $u\in U$, denoted as u^*, such that $\forall(q,r)\in Q\times[0;\ell]$ with $q'=\varrho(q,L(x_i))$, the following conditions hold:

- if $q'\notin Q_F$ then $\mathcal{B}_{q',r}(c^*,f(\tilde{x}_i,u^*))\leq\mathcal{B}_{q,r}(c^*,\tilde{x}_i)$;
- if $q'\in Q_F$ then $\mathcal{B}_{q',r+1}(c^*,f(\tilde{x}_i,u^*))\leq\mathcal{B}_{q,r}(c^*,\tilde{x}_i)$.

Therefore, for all $x \in X$ and $\forall i \in [1;N]$, one has:

$$\begin{aligned}\mathcal{B}_{q',r}(c^*, f(x,u^*)) - \mathcal{B}_{q,r}(c^*,x) = \mathcal{B}_{q',r}(c^*, f(x,u^*)) - \\ \mathcal{B}_{q,r}(c^*,x) - \big(\mathcal{B}_{q',r}(c^*, f(\tilde{x}_i,u^*)) - \mathcal{B}_{q,r}(c^*,\tilde{x}_i)\big) + \\ \big(\mathcal{B}_{q',r}(c^*, f(\tilde{x}_i,u^*)) - \mathcal{B}_{q,r}(c^*,\tilde{x}_i)\big) \leq \mathscr{L}_a\|x-\tilde{x}_i\| + \eta_S^* \\ \leq \mathscr{L}\varepsilon + \eta_S^* \leq 0 \quad \text{if } q' \notin Q_F.\end{aligned}$$

Similarly, the above argument can be leveraged to show that

$$\mathcal{B}_{q',r+1}(c^*, f(x,u^*)) - \mathcal{B}_{q,r}(c^*,x) \leq 0 \ \text{ whenever } q \in Q_F.$$

Therefore, for any $(q,r) \in Q \times [0;\ell]$, the function $\mathcal{B}_{q,r}$ derived by solving SOP in (11) serves as a CBC for unknown dt-CS in (1), thereby concluding the proof. ∎

Whenever condition (14) of Theorem 4.3 holds, there is a set-valued controller $\kappa_{q,r}$ as defined in (7), guaranteeing the fulfillment of the ℓ-UCA property by the unknown dt-CS as in Theorem 2.6. Specifically, we mold the set-valued map $\kappa_{q,r}$ for any $(q,r) \in Q \times [0;\ell]$, and any $x \in X$, $i \in [1;N]$ with q' and r' defined in (6), as follows:

$$\begin{aligned}\kappa_{q,r}(x) := \big\{u \in U \mid \mathcal{B}_{q',r'}(f(\tilde{x}_i,u)) - \mathcal{B}_{q,r}(\tilde{x}_i) \\ \leq \eta_S^*, \ \text{such that } x \in \Phi_\varepsilon(\tilde{x}_i)\big\}.\end{aligned} \tag{15}$$

It is worth noting that the non-emptiness of data set (8) and the solvability of SOP in (11) imply that the set-valued controller $\kappa_{q,r}$ is also not empty.

Remark 4.4: Note that nearly all data-driven approaches aimed at validating the satisfaction of properties by unknown systems with a formal correctness guarantee (*e.g.,* [14]–[16]), similar to our method, encounter a sample complexity bottleneck-*i.e.,* the required data volume to provide guarantees grows exponentially with the system's dimension. This challenge was also evident in our work.

Remark 4.5: We assume the labeling map L is such that there always exists a choice of ε where $L(x) = L(x_i)$ whenever $x \in \Phi_\varepsilon(x_i)$ for all $i \in [1;N]$. This ensures the satisfaction of Assumption 1 when $\mathcal{B}_{q,r}$ and f are Lipschitz continuous. Furthermore, in an effort to potentially reduce the required number of samples, one might consider initiating sample collection with a larger value of ε when addressing the SOP in (11). If the condition (14) is not satisfied with the chosen (possibly larger) ε, it becomes necessary to opt for a smaller ε and re-address the SOP.

The set-valued map $\kappa_{q,r}$ in (15), which enforces the ℓ-UCA property, can be utilized during runtime as follows: for any state measurement $x \in X$, one can identify the ε-closest data point $\tilde{x}_i$, where $i \in [1;N]$, such that $x \in \Phi_\varepsilon(\tilde{x}_i)$. Consequently, control inputs valid for $\tilde{x}_i$ are also valid for x.

V. Case Study

Here, the effectiveness of our data-driven results is demonstrated on applying them to a three-tank model whose dynamics is assumed to be unknown, with respect to the properties outlined by an ℓ-UCA. We consider ℓ-UCA $\mathcal{A} = (Q, \Delta, \varrho, Q_0, Q_F)$ as in Definition 2.1, where $Q = \{q_0, q_1\}$, $\Delta = \{a, b\}$, and $Q_0 = Q_F = \{q_0\}$. The transitions between states are specified by the edges of the graph depicted in

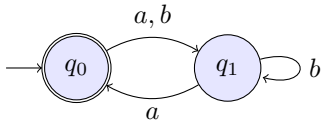

Fig. 1: This ℓ-UCA specifies that the system to be in a state with label a only finitely often.

Fig. 1, which define the transition function ϱ. We consider a three-tank system arranged in a cascade configuration, with its model adopted from [20]. The system is discretized with a sampling time $\tau = 10s$ and is modeled by a dt-CS, where the state evolves as follows:

$$\begin{aligned}x_1(t+1) &= \left[\sqrt{\left(\frac{\tau}{2}\right)^2 + x_1(t) + \tau\nu(t)} - \frac{\tau}{2}\right]^2 \\ x_i(t+1) &= \left[\sqrt{\left(\frac{\tau}{2}\right)^2 + x_i(t) + \tau\sqrt{x_{i-1}(t+1)}} - \frac{\tau}{2}\right]^2,\end{aligned} \tag{16}$$

where $i \in \{2,3\}$. For any $i \in [1;3]$, the state $x_i(t)$ and $\sqrt{x_i(t)}$ denote, respectively, the level of fluid and the outflow rate of the i-th tank at time $t \in \mathbb{N}$. The inflow rate $\nu(t)$ into the first tank takes values from the set of control inputs $U = \{0, 1.5, 4.5, 7.5, 9\}$. We consider the set of states $X = [0,100]^3$, initial states $X_0 = [0,6]^2 \times [60,66]$, and a labelling function $L : X \to \Delta$ defined as:

$$L(x) = b \ \ \forall x \in (10,60)^3 \text{ and } L(x) = a \ \ \forall x \in X \backslash (10,60)^3. \tag{17}$$

Based on the ℓ-UCA depicted in Fig. 1, our objective is to systematically develop a data-driven CBC and its corresponding controller. Our aim is to regulate the fluid levels in the tanks, ensuring that as they evolve from a point in X_0, they reach the region labeled a finitely often. This approach could be practically beneficial for preventing both the emptying and overflowing of the tanks simultaneously. We consider the model in (16) to be unknown to us. However, we employ the model solely to collect samples as in (8), with the number of samples $N = 64000$ and the discretization parameter $\varepsilon = 2.5$. Our primary objective is to construct a CBC by solving SOP in (11) while synthesizing a controller $\kappa_{q,r}$ for any $(q,r) \in Q \times [0;\ell]$ in which the unknown dt-CS satisfies the specification expressed by the ℓ-UCA $\mathcal{A}$ in Fig. 2. We select $\ell = 10$; therefore, we aim for a controller $\kappa_{q,r}$ that ensures that (16) visits the region with label a at most 10 times as it evolves. We fix the CBC structure as piecewise quadratic functions $\mathcal{B}_{q,r}(x) = \sum_{j=1}^{10} c_{q,r}^j \varphi^j(x) \ \ \forall x \in X$, $\forall q \in Q$ and $\forall r \in [0;\ell+1]$, where basis functions $\langle \varphi^j(x) \rangle_{j=1}^{10} = \langle 1, x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2x_3, x_2^2, x_3^2 \rangle$. We solve SOP in (11) using the acquired data set $\mathcal{D}_{64000,5}$ and compute the CBC coefficients together with other decision variables in the SOP, which are presented as follows: $\lambda^* = 3.301$, $\gamma^* = -10$, $\eta_S^* = -13.2995$, and

$$c_{q,r}^j = \begin{cases} 0.1 & \text{if } (q,r,j) \in \Omega_1, \\ -0.1 & \text{if } (q,r,j) \in \Omega_2, \\ 0.07797 & \text{if } (q,r,j) \in \{q_1\} \times \{1,3,6\} \times \{5\}, \\ 0.0838 & \text{if } (q,r,j) \in \{q_1\} \times \{2\} \times \{9\}, \\ 0.0829 & \text{if } (q,r,j) \in \{q_1\} \times \{7\} \times \{9\}, \end{cases}$$

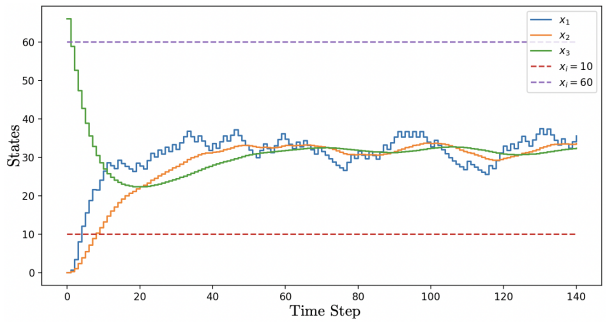

Fig. 2: A closed-loop state trajectory from initial state $[x_1(0); x_2(0); x_3(0)] = [0; 0; 66]$ for unknown three-tank system (16).

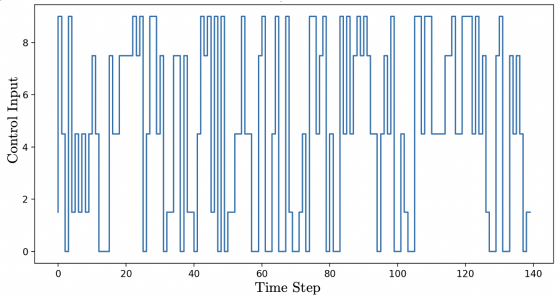

Fig. 3: An input trajectory synthesized for the unknown three-tank system during 140 time steps using (15).

where $\Omega_1 = \big(\{q_0\} \times [0;11] \times [1;10]\big) \cup \big(\{q_1\} \times \{0,4,5,8,9,10\} \times [2;10]\big) \cup \big(\{q_1\} \times \{1,3,6\} \times ([2;10] \setminus \{5\})\big) \cup \big(\{q_1\} \times \{2,7\} \times ([2;10] \setminus \{9\})\big)$ and $\Omega_2 = \big(\{q_1\} \times [0;10] \times \{1\}\big) \cup \big(\{q_1\} \times \{11\} \times [1;10]\big)$. Due to the structure of the CBC, we use [15, Lemma 5.4] to obtain $\mathscr{L} = 5.315$. Since $\mathscr{L}\varepsilon + \eta_S^* = -1211.64 \times 10^{-5} < 0$, in accordance with Theorem 4.3, it is assured that a controller $\kappa_{q,r}$ exists for any $(q, r) \in Q \times [0; \ell]$ that enforces the specification expressed by $\mathcal{A}$ over the system in (16).

Fig. 2 illustrates the closed-loop trajectory of the unknown three-tank system regulated by the synthesized controller. It also demonstrates that the CBC constructed from the data satisfies the conditions highlighted in Definition 2.3. It can be observed that none of the three tanks visits the region with label a more than 10 times. The synthesized controller is constructed according to (15), which is then applied to the unknown dt-CS as depicted in Fig. 3. The implementation for constructing the data-driven CBC has been carried out using the `GUROBI` solver [21] under Python on a 64GB RAM (3.2 GHz) MacBook Pro. The whole computation took 2.2 minutes.

VI. Conclusion

In this paper, the primary goal was to develop a data-driven approach to construct CBC using available data. The aim is to ensure the satisfaction of an ℓ-UCA property by a discrete-time control system with unknown dynamics. To achieve this goal, we leveraged data collected from the trajectories of unknown systems to implement a scenario optimization program (SOP). The successful solution of the SOP enabled us to establish a CBC along with its respective controller, which enforces an ℓ-UCA property with formal guarantees. The effectiveness of our data-driven approach was demonstrated using a three-tank system. However, the scalability challenge posed in this work is outlined in Remark 4.4. Possible strategies to alleviate this computational burden include employing compositional approaches such as divide and conquer tactics or adapting parallelization across SOP. These methods remain areas for future exploration.

References

[1] C. Belta, B. Yordanov, and E. A. Gol, *Formal methods for discrete-time dynamical systems*. Springer, 2017, vol. 89.

[2] P. Tabuada, *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[3] D. Ajeleye, A. Lavaei, and M. Zamani, "Data-driven controller synthesis via finite abstractions with formal guarantees," *IEEE Control Systems Letters*, vol. 7, pp. 3453–3458, 2023.

[4] A. Makdesi, A. Girard, and L. Fribourg, "Efficient data-driven abstraction of monotone systems with disturbances," *IFAC-PapersOnLine*, vol. 54, no. 5, pp. 49–54, 2021.

[5] A. Devonport, A. Saoud, and M. Arcak, "Symbolic abstractions from data: A pac learning approach," in *2021 60th IEEE Conference on Decision and Control (CDC)*. IEEE, 2021, pp. 599–604.

[6] M. Kazemi, R. Majumdar, M. Salamati, S. Soudjani, and B. Wooding, "Data-driven abstraction-based control synthesis," *Nonlinear Analysis: Hybrid Systems*, vol. 52, p. 101467, 2024.

[7] S. Prajna and A. Jadbabaie, "Safety verification of hybrid systems using barrier certificates," in *International Workshop on Hybrid Systems: Computation and Control*. Springer, 2004, pp. 477–492.

[8] V. Murali, A. Trivedi, and M. Zamani, "Co-buchi barrier certificates for discrete-time dynamical systems," *arXiv preprint arXiv:2311.07695*, 2023.

[9] E. Filiot, N. Jin, and J.-F. Raskin, "Antichains and compositional algorithms for ltl synthesis," *Formal Methods in System Design*, vol. 39, pp. 261–296, 2011.

[10] S. Schewe and B. Finkbeiner, "Bounded synthesis," in *International symposium on automated technology for verification and analysis*. Springer, 2007, pp. 474–488.

[11] L. Wang, E. A. Theodorou, and M. Egerstedt, "Safe learning of quadrotor dynamics using barrier certificates," in *2018 IEEE International Conference on Robotics and Automation (ICRA)*. IEEE, 2018, pp. 2460–2465.

[12] 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*. PMLR, 2021, pp. 1351–1370.

[13] A. Nejati, B. Zhong, M. Caccamo, and M. Zamani, "Data-driven controller synthesis of unknown nonlinear polynomial systems via control barrier certificates," in *Learning for Dynamics and Control Conference*. PMLR, 2022, pp. 763–776.

[14] 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.

[15] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani, "Data-driven safety verification of stochastic systems via barrier certificates," *IFAC-PapersOnLine*, vol. 54, no. 5, pp. 7–12, 2021.

[16] A. Nejati and M. Zamani, "Data-driven synthesis of safety controllers via multiple control barrier certificates," *IEEE Control Systems Letters*, 2023.

[17] C. Baier and J.-P. Katoen, *Principles of model checking*. MIT press, 2008.

[18] 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.

[19] G. Wood and B. Zhang, "Estimation of the lipschitz constant of a function," *Journal of Global Optimization*, vol. 8, pp. 91–103, 1996.

[20] M. A. Capcha, W. Ipanaqué, and R. De Keyser, "Comparison of model-based and non-model-based strategies for nonlinear control of a three-tank system," in *2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2017, pp. 1–4.

[21] L. Gurobi Optimization, "Gurobi optimizer reference manual," 2021.