Co-Büchi Control Barrier Certificates for Stochastic Control Systems

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

***Abstract*—This letter addresses the problem of synthesizing controllers that enforce properties expressed by Universal Co-Büchi Automata (UCA) over stochastic control systems. Our approach introduces a notion of Stochastic Co-Büchi Control Barrier Certificates (SCBC), which, together with their associated controllers, ensure that specific regions in the state set are visited only a limited number of times during the system's evolution. The SCBC is formulated over a hybrid domain that combines the system's state, the UCA's state, and a counter variable that tracks the number of visits to the UCA's accepting states. We require the SCBC to satisfy a supermartingale condition, thereby, enforcing the property expressed by the UCA on the stochastic control system without any restriction over the time horizon. Additionally, we propose a method for constructing SCBCs and corresponding controllers that guarantee the enforcement of UCA properties over stochastic control systems with formal probabilistic guarantee. The practical applicability of our approach is demonstrated through a case study involving a stochastic three-tank system, whose dynamics is both nonlinear and influenced by noise.**

***Index Terms*—Stochastic systems, stochastic co-Büchi barrier certificates, universal co-Büchi automata.**

I. Introduction

In RECENT years, formal methods have emerged as essential tools in the autonomous and hybrid systems community. They have been offering rigorous frameworks for analyzing complex dynamical systems, often modeled as stochastic processes. These processes are integral to a wide range of applications in science and engineering. They are used to model dynamical systems influenced by stochastic disturbances, where ensuring their correctness is paramount, particularly in safety-critical applications. However, achieving formal guarantees of correctness in such systems presents a significant challenge, especially for processes with continuous state sets. The requirement of interest for these systems is often specified through temporal logic specifications, which are best described using linear temporal logic (LTL) formulae or, more broadly, ω-regular properties [1], and automata-based languages [2].

In the past decade, numerous results have been proposed using abstraction-based methods for synthesizing correct-by-construction controllers for stochastic and non-stochastic control systems [3]. Notable examples of such efforts include the results presented in [4], [5], [6], [7], [8], [9], and references therein. However, these techniques depend on discretizing the state and input sets, which leads to the curse of dimensionality, *i.e.,* the computational complexity grows exponentially with the system's dimension.

The use of barrier certificates [10] offers an alternative method for formal verification and controller synthesis of (stochastic) dynamical systems, one that does not rely on discretization. Barrier certificates, similar to Lyapunov functions, use level sets to distinguish between unsafe regions and the reachable states of the system starting from a given initial set. The existence of such a certificate provides a (probabilistic) safety guarantee for the system. In the context of automata-theoretic verification, the central challenge is to determine whether a set of states can be visited only a finite number of times. This issue can be addressed by establishing a safety-like condition that ensures the number of times the system can visit a specific region is bounded by a fixed hyperparameter. Recent results, as discussed in [11], build on bounded synthesis methods [12], [13], [14], [15] and introduce an abstraction-free technique for automata-theoretic verification of discrete-time non-stochastic dynamical systems. This method introduces notions of co-Büchi barrier certificates, which offer sufficient conditions to verify systems against ω-regular properties defined by universal co-Büchi automata (UCA). For a detailed explanation of the differences between traditional barrier certificates and co-Büchi barrier certificates, we refer the interested readers to [11].

Contributions: In this letter, we introduce an abstraction-free approach for automata-theoretic controller synthesis of discrete-time stochastic control systems with finite input sets. This method is centered on a notion of Stochastic Co-Büchi Barrier Certificates (SCBC). An SCBC is a real-valued function defined over the product of a stochastic control system and a deterministic UCA, with conditions that ensure the UCA's accepting states are visited only a finite number of times. The certificate includes a counter that tracks how often an accepting state is reached. We propose a method for constructing SCBCs, inspired by the counterexample-guided inductive

Received 13 September 2024; revised 30 October 2024; accepted 12 November 2024. Date of publication 14 November 2024; date of current version 27 November 2024. This work was supported by NSF under Grant CNS-2145184, Grant CNS-2111688, and Grant CNS-2039062. Recommended by Senior Editor S. Dey. *(Corresponding author: Daniel Ajeleye.)*

The authors are with the Department of Computer Science, University of Colorado Boulder, Boulder, CO 80309 USA (e-mail: daniel.ajeleye@colorado.edu; majid.zamani@colorado.edu).

Digital Object Identifier 10.1109/LCSYS.2024.3498897

2475-1456 © 2024 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on April 21,2025 at 17:31:25 UTC from IEEE Xplore. Restrictions apply.

synthesis (CEGIS) approach, and we use satisfiability modulo theories (SMT) solvers to identify a suitable SCBC candidate. Once identified, the system can be rendered to satisfy properties expressed by UCA with particular probability lower bounds. We then use the SCBC to synthesize controllers that ensure a stochastic control system visits the accepting states of the UCA only a finite number of times. The effectiveness of our approach is demonstrated using a stochastic three-tank system.

Related Work: In recent years, considerable attentions have been directed towards the formal analysis of stochastic control systems with respect to ω-regular properties using abstraction-free approaches. The results in [16], [17], [18], [19] focus on verifying systems with continuous state sets against automata specifications. A common aspect of these works is their use of barrier certificates to divide the automaton into state triplets, and can be used for the verification of systems whose traces do not reach the automaton's accepting state at all (similar to safety verification) [11]. In contrast, our approach provides a systematic method for synthesizing controllers ensuring that the traces of stochastic control systems visit the accepting states of deterministic UCAs a finite number of times with some probability lower bounds.

A very recent work in [20] tackled the verification and synthesis of controllers of stochastic models with respect to the properties expressed by Streett automata, leveraging the so-called Streett supermartingales. Our work differentiates itself from theirs in two key aspects. First, while [20] guarantees almost sure satisfaction, our approach provides a probabilistic guarantee for satisfaction of properties expressed by deterministic UCA. Achieving an almost sure guarantee is challenging for most stochastic models unless there is a bounded support assumption on the noise or existence of absorbing sets. Secondly, the Streett martingales formulation in [20] involves a notion of Post$(\cdot)$ function that integrates the Streett supermartingales over a probability distribution. In contrast, our approach uses the expectation of the SCBC, which is generally much more straightforward to compute.

Our method systematically synthesizes controllers that enforce deterministic UCA properties over nonlinear discrete-time stochastic control systems, differing from the approach in [21], [22], [23], which synthesize controllers that enforce similar properties over non-stochastic control systems. Moreover, while the work in [11], [24], [25] focuses on verification of non-stochastic dynamical systems using barrier certificates, our approach is tailored to constructing SCBCs and synthesizing controllers that enforce deterministic UCA properties over stochastic control systems.

Organization: The remainder of this letter is structured as follows. Section II provides the required notation and notion of so-called ζ-Universal co-Büchi automata ($\zeta - UCA$), with a formal definition of discrete-time stochastic control systems (dt-SCS), and the main problem studied. In Section III, we formalize the notions of SCBCs and their corresponding controllers. The section also describes a proposed method for constructing SCBCs. Our approach is illustrated over a nonlinear stochastic control system in Section IV. We conclude this letter with brief discussion in Section V.

II. Preliminaries and Definitions

A. Notation

The symbols $\cup$, $\cap$ and $\setminus$ represent, respectively, the union, the intersection and the difference of sets. Notations $\mathbb{Z}$, $\mathbb{R}_{\geq 0}$ and $\mathbb{R}$ denote the sets of integers, non-negative real and real numbers, respectively. For any $n \in \mathbb{Z}$, $\mathbb{Z}_{\geq n} = \{i \in \mathbb{Z} \mid i \geq n\}$. For integers $s, t \in \mathbb{Z}$ where $s < t$, the intervals $[s; t]$ and $(s; t)$ represent, respectively, the closed and open intervals in $\mathbb{Z}$. Similarly, for reals $s, t \in \mathbb{R}$ where $s < t$, the intervals $[s, t]$ and (s, t) represent the corresponding closed and open intervals in $\mathbb{R}$. For any nonempty set Q, $\mathcal{C}_d(Q)$ indicates the cardinality of Q, while Q^ω denotes the set of infinite sequences derived from Q, formally expressed as $Q^\omega := \{\langle w_i \rangle_{i=0}^{\infty} \mid w_i \in Q \ \forall i \in \mathbb{Z}_{\geq 0}\}$.

In a given probability space $(\mathcal{G}, \mathbb{B}(\mathcal{G}), \mathbb{P}_\mathcal{G})$, $\mathcal{G}$ refers to the sample space, $\mathbb{B}(\mathcal{G})$ is a σ-algebra on $\mathcal{G}$ containing subsets of events, and $\mathbb{P}_\mathcal{G}$ is the probability measure that assigns probabilities to these events. We treat random variables as measurable functions (*i.e.,* Borel measurable) of the form $\varpi : (\mathcal{G}, \mathbb{B}(\mathcal{G})) \rightarrow (S_\varpi, \mathbb{B}(\varpi))$, where $(\mathcal{G}, \mathbb{B}(\mathcal{G}))$ and $(S_\varpi, \mathbb{B}(\varpi))$ are measurable spaces. For any $Y \in \mathbb{B}(\varpi)$, the random variable ϖ induces a probability measure on $(S_\varpi, \mathbb{B}(\varpi))$ given by $\text{Prob}[Y] = \mathbb{P}_\mathcal{G}[\varpi^{-1}(Y)]$. For the subsequent discussions in this letter, we often omit the explicit reference to the underlying probability space and the function ϖ when referring to the probability measure on $(S_\varpi, \mathbb{B}(\varpi))$.

B. Universal Co-Büchi Automaton

In line with the definition provided in [14], we introduce a variation of a *deterministic* universal co-Büchi automaton, where the acceptance criterion is defined by allowing at most ζ visits to the accepting states, for some $\zeta \in \mathbb{Z}_{\geq 0}$.

Definition 1: Given $\zeta \in \mathbb{Z}_{\geq 0}$, a deterministic ζ-Universal Co-Büchi Automaton (ζ-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;
- $\varrho : Q \times \Delta \rightrightarrows Q$ 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 (accepting) final set of states.

The acceptance condition of $\mathcal{A}$ requires that Q_F be visited no more than ζ 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 defined as an infinite sequence of states, $\mathbf{q} = \langle q_i \rangle_{i=0}^{\infty} \in Q^\omega$, where $q_0 \in Q_0$ and $q_{i+1} = \varrho(q_i, \varsigma_i) \ \forall i \in \mathbb{Z}_{\geq 0}$. The word $\mathbf{v} \in \Delta^\omega$ is said to be accepted by $\mathcal{A}$ if, for every run $\mathbf{q} = \langle q_i \rangle_{i=0}^{\infty} \in Q^\omega$ of $\mathcal{A}$ over $\mathbf{v}$, one has $\mathcal{C}_d(\{i \mid q_i \in Q_F\}) \leq \zeta$. In other words, every run of $\mathcal{A}$ over $\mathbf{v}$ visits some of the accepting states at most ζ times. The language of a ζ-UCA $\mathcal{A}$, denoted by $\mathcal{L}(\mathcal{A})$, is defined as the set of all words that are accepted by $\mathcal{A}$.

C. Discrete-Time Stochastic Control Systems

Here, we formalize discrete-time stochastic control systems with continuous state sets. This class of systems has been widely used in various engineering and financial contexts [26], [27].

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on April 21,2025 at 17:31:25 UTC from IEEE Xplore. Restrictions apply.

Definition 2: A discrete-time stochastic control system (dt-SCS) is a tuple $\Xi = (X, U, X_0, \Lambda, \varpi, f)$, where

- $X \subseteq \mathbb{R}^n$ is the state set of the system such that $\mathbb{B}(X)$ is a Borel σ-algebra on X and $(X, \mathbb{B}(X))$ is a measurable space;
- $U = \{u_j \in \mathbb{R}^m \mid j \in [1; N]\}$ with $N \in \mathbb{Z}_{\geq 1}$, is the finite input set;
- $X_0 \subseteq X$ is the set of initial states and Λ is the uncertainty set, which is not necessarily bounded;
- ϖ is a sequence of independent and identically distributed (*i.i.d.*) random variables from a sample space $\mathcal{G}$ to the set Λ, *i.e.,* $\varpi := \{\varpi_k : \mathcal{G} \to \Lambda \mid k \in \mathbb{Z}_{\geq 0}\}$;
- $f : X \times U \times \Lambda \to X$ is a measurable state transition function.

For any initial state $x_0 \in X_0$ and an input sequence $\{u(k) : \mathcal{G} \to U \mid k \in \mathbb{Z}_{\geq 0}\}$, we describe the evolution of the state of dt-SCS Ξ for a given time step $k \in \mathbb{Z}_{\geq 0}$ as follows:

$$x(k+1) \ = f(x(k), u(k), \varpi(k)). \tag{1}$$

Furthermore, we denote the state trajectory of dt-SCS Ξ, given an input trajectory $u(\cdot)$, noise $\varpi(\cdot)$ and an initial state $x_0 \in X_0$ by $x_{x_0,u,\varpi} = \langle x_k \rangle_{k=0}^{\infty} \in X^{\omega}$, where $x_{x_0,u,\varpi}(k) = x_k$ and $x_{k+1} = f(x_k, u(k), \varpi(k)),\ \forall k \in \mathbb{Z}_{\geq 0}$. We introduce a labeling function $L : X \to \Delta$ that maps each state of the dt-SCS to a symbol in a finite alphabet Δ. This labeling function captures the regions visited along the trajectories of the dt-SCS and connects the dt-SCS to the ζ-UCA. This concept extends to sequences, allowing us to map a state sequence $\langle x_k \rangle_{k=0}^{\infty} \in X^{\omega}$ to a sequence of symbols $\langle L(x_k) \rangle_{k=0}^{\infty} \in \Delta^{\omega}$. Consequently, we can assign different labels from Δ to regions within X.

Given a ζ-UCA $\mathcal{A}$ and a dt-SCS Ξ, we use Ξ_{μ} to denote Ξ equipped with a controller $\mu : X \times Q \times [0; \zeta] \to U$, while $\mathbb{P}\mathrm{r}[\Xi_{\mu} \models \mathcal{A}]$ denotes the probability for which Ξ_{μ} satisfies a property defined by $\mathcal{A}$. In this letter, our main objective is to synthesize controllers $\mu : X \times Q \times [0; \zeta] \to U$, which guarantee that $\mathbb{P}\mathrm{r}[\Xi_{\mu} \models \mathcal{A}]$ has a potentially tight lower bound. We now proceed to formalize the main problem that we aim to address in this letter.

Problem 1: Consider a dt-SCS Ξ and a ζ-UCA $\mathcal{A}$ as in Definition 2 and 1, respectively. Given a labeling function L, design a controller $\mu : X \times Q \times [0; \zeta] \to U$ and find a constant $0 \leq \delta < 1$, such that Ξ equipped with μ satisfies the property specified by $\mathcal{A}$ with a probability of at least $1 - \delta$, *i.e.,*

$$\mathbb{P}\mathrm{r}\big[\Xi_{\mu} \models \mathcal{A}\big] \geq 1 - \delta.$$

III. Stochastic Co-Büchi Control Barrier Certificates

Consider a dt-SCS $\Xi = (X, U, X_0, \Lambda, \varpi, f)$ and a ζ-UCA $\mathcal{A} = (Q, \Delta, \varrho, Q_0, Q_F)$, as in Definitions 2 and 1, respectively. Let $L : X \to \Delta$ be a labeling map. We define the probability that Ξ satisfies a property specified by $\mathcal{A}$ as the probability measure of the set $\{\langle x_k \rangle_{k=0}^{\infty} \in X^{\omega} \mid \langle L(x_k) \rangle_{k=0}^{\infty} \in \mathcal{L}(\mathcal{A})\}$. The objective of this letter is to provide a lower bound on this probability. To formalize this, we introduce a notion of stochastic co-Büchi barrier certificates. These certificates include a counter variable integrated into the state set to keep track of the number of times the augmented state $(x, q) \in X \times Q$ appears in $X \times Q_F$.

Definition 3: Consider a dt-SCS Ξ and a ζ-UCA $\mathcal{A}$ as described in Definitions 2 and 1, respectively, with $L : X \to \Delta$ serving as a labeling function. A function $\mathcal{S} : X \times Q \times \mathbb{Z}_{\geq 0} \to \mathbb{R}$ is called a stochastic co-Büchi barrier certificate (SCBC) for Ξ with respect to the property defined by $\mathcal{A}$ if there exist $\lambda, \gamma \in \mathbb{R}$ such that $\lambda > \gamma$ and

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

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

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

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

$$\min_{u \in U} \Big\{ \mathbb{E}\big[\mathcal{S}\big(f(x, u, \varpi), q^{+}, \ell^{+}\big) \mid x, q, \ell, u\big] \Big\} \leq \mathcal{S}(x, q, \ell), \tag{5}$$

where $\mathbb{E}[\,\cdot\,]$ represents expectation,

$$q^{+} := \varrho(q, L(x)), \tag{6}$$

$$\text{and } \ell^{+} := \begin{cases} \ell & \text{if } q^{+} \notin Q_F \\ \ell + 1 & \text{otherwise.} \end{cases} \tag{7}$$

Note that condition (5) for an SCBC is a supermartingale-type condition. This ensures that the SCBCs are non-increasing in expectation at each time step, which can be utilized to establish lower bounds for the satisfaction probability $\mathbb{P}\mathrm{r}[\Xi_{\mu} \models \mathcal{A}]$ over infinite time horizons. In addition, one can design a controller $\mu{:}X \times Q \times [0; \zeta] \to U$ based on the SCBC $\mathcal{S}$ as follows:

$$\mu(x, q, \ell) \in \Big\{ u \in U \ \Big|\ \mathbb{E}\big[\mathcal{S}\big(f(x, u, \varpi), q^{+}, \ell^{+}\big) \mid x, q, \ell, u\big] \leq \mathcal{S}(x, q, \ell) \Big\}, \tag{8}$$

where q^{+} and ℓ^{+} are defined in (6) and (7), respectively.

Remark 1: Note that the controller given in equation (8), enforces the specification defined by a ζ-UCA over a dt-SCS and operates within the augmented state set $X \times Q \times [0; \zeta]$. Hence, this controller is history-dependent (*i.e.,* with memory), meaning it takes into account the state of the dt-SCS, ζ-UCA, and the counter variable.

The following theorem illustrates the effectiveness of SCBCs in synthesizing controllers for the specifications expressed by ζ-UCA.

Theorem 1: Consider a dt-SCS Ξ and a ζ-UCA $\mathcal{A}$ according to Definition 2 and 1, respectively. Given a labeling map L, suppose that $\mathcal{S} : X \times Q \times \mathbb{Z}_{\geq 0} \to \mathbb{R}$ is an SCBC for Ξ and $\mathcal{A}$ as in Definition 3. Then, for any initial conditions $x_0 \in X_0$, $q_0 \in Q_0$,

$$\text{and } \ell_0 = \begin{cases} 0 & \text{if } q_0 \notin Q_F \\ 1 & \text{otherwise,} \end{cases} \tag{9}$$

one obtains

$$\mathbb{P}\mathrm{r}\Big[\Xi_{\mu} \models \mathcal{A} \mid x_0, q_0, \ell_0\Big] \geq 1 - \frac{\gamma}{\lambda}, \tag{10}$$

where the controller $\mu : X \times Q \times [0; \zeta] \to U$ is defined in (8).

Proof: Since $\mathcal{S}$ is an SCBC, it follows from condition (4) that for any (x, q, ℓ) where $x \in X$, $q \in Q_F$, and $\ell \geq \zeta + 1$,

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on April 21,2025 at 17:31:25 UTC from IEEE Xplore. Restrictions apply.

one has $\mathcal{S}(x, q, \ell) > \lambda$. Therefore, for every state trajectory $\langle x_k\rangle_{k=0}^{\infty}$ of Ξ with initial conditions $x_0 \in X_0$, $q_0 \in Q_0$, and ℓ_0 as in (9), one obtains the following chain of (in)equalities:

$$\begin{aligned}
1 &- \mathbb{Pr}\big[\Xi_\mu \models \mathcal{A} \mid x_0, q_0, \ell_0\big] \\
&= \mathbb{Pr}\big[\langle L(x_k)\rangle_{k=0}^{\infty} \notin \mathcal{L}(\mathcal{A}) \mid x_0, q_0, \ell_0\big] \\
&= \mathbb{Pr}\big[\langle (x_k, q_k, \ell_k)\rangle_{k=0}^{\infty} \text{ where} \\
&\qquad q_k \in Q_F \text{ and } \ell_k \geq \zeta + 1 \mid x_0, q_0, \ell_0\big] \\
&\leq \mathbb{Pr}\Big[\sup_{k\in\mathbb{Z}_{\geq 0}} \mathcal{S}(x_k, q_k, \ell_k) > \lambda \text{ where} \\
&\qquad q_k \in Q_F \text{ and } \ell_k \geq \zeta + 1 \;\Big|\; x_0, q_0, \ell_0\Big] \\
&\text{(applying Ville's maximal inequality [28] and using (5))} \\
&\leq \frac{1}{\lambda}\mathcal{S}(x_0, q_0, \ell_0) \leq \frac{\gamma}{\lambda} \text{ (obtained by using (2), (3) and (9))},
\end{aligned}$$

which establish the proposed bound in (10). ■

In this letter, we develop a controller to address Problem 1 by leveraging the concept of SCBCs. Theorem 1 provides a lower bound for the probability that a dt-SCS Ξ satisfies the property expressed by a ζ-UCA $\mathcal{A}$. Consequently, solving Problem 1 reduces to finding an appropriate SCBC, which can then be used to synthesize the corresponding controllers.

Although various tools from the literature may be used to search for an SCBC, we provide a brief overview of how to implement one of such method, for the sake of completeness. Specifically, we consider employing the Counterexample Guided Inductive Synthesis (CEGIS) approach [29], which utilizes Satisfiability Modulo Theory (SMT) solvers for this purpose.

In the search for an SCBC as defined in Definition 3 using the CEGIS approach, we start by fixing a template for a candidate SCBC as follows:

$$\mathcal{S}(x, q, \ell) = \sum_{i=1}^{d} p^i(q, \ell)\psi^i(x), \tag{11}$$

where $p^i(q, \ell) \in \mathbb{R}$ are unknown coefficients and ψ^i are some user-defined (nonlinear) functions, which can be, for instance, some monomials over state variables, if one desires polynomial SCBCs. Note that if d and $x \in X$ are fixed in (11), the only decision variables in $\mathcal{S}$ are the coefficients $p^i(q, \ell) \in \mathbb{R}$. To determine these coefficients, we construct a finite set of states $\mathcal{D} = \{x_i \in X \mid i \in [1; M]\}$, where $M \in \mathbb{Z}_{\geq 1}$. We then encode the SCBC constraints for each $x \in \mathcal{D}$ into an SMT-query using the sequence of conjunctions described below.

$$\bigwedge_{(x,q)\in(X_0\cap\mathcal{D})\times(Q_0\setminus Q_F)} \Big(\mathcal{S}(x, q, 0) \leq \gamma\Big), \tag{12}$$

$$\bigwedge_{(x,q)\in(X_0\cap\mathcal{D})\times(Q_0\cap Q_F)} \Big(\mathcal{S}(x, q, 1) \leq \gamma\Big), \tag{13}$$

$$\bigwedge_{(x,q)\in\mathcal{D}\times Q_F} \Big(\mathcal{S}(x, q, \zeta + 1) > \lambda\Big), \tag{14}$$

$$\big(\gamma < \lambda\big), \tag{15}$$

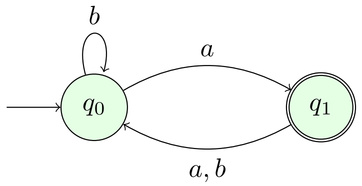

Fig. 1. A ζ-UCA specifying that the dt-SCS visits a state with label a only finitely often.

$$\bigwedge_{\substack{(x,q)\in\mathcal{D}\times Q,\\ \ell\in[0;\zeta]}} \Bigg(\bigvee_{u\in U} \Big(\mathbb{E}\big[\mathcal{S}\big(f(x, u, \varpi), q^+, \ell^+\big) \mid x, q, \ell, u\big] \leq \mathcal{S}(x, q, \ell)\Big)\Bigg), \tag{16}$$

where q^+ and ℓ^+ are defined in (6) and (7), respectively. We compute a candidate SCBC by determining the coefficients $p^i(q, \ell)$, and constants λ and γ, such that the query expressed in (12) to (16) is satisfied. Depending on the nature of the transition function f appearing in (16), this query may be solved using linear real arithmetic theory with Z3 [30] if f is linear, or nonlinear real arithmetic theory with dReal [31] if f is nonlinear. After obtaining a candidate SCBC, we check whether there exists a state $\hat{x} \in X$ where any of the condition (12) to (16) fails. If such a counterexample $\hat{x}$ is found, we repeat the process with the expanded set $\mathcal{D} \cup \{\hat{x}\}$. If no counterexample is identified, the computed candidate is rendered to be a valid SCBC. Upon identifying an SCBC, a lower bound on the satisfaction probability of ζ-UCA by the dt-SCS is calculated as described in Theorem 1.

IV. Case Study

We demonstrate the effectiveness of our approach by designing a controller that ensures that a dt-SCS satisfies a property defined by a ζ-UCA with some probability lower bound, using SCBCs. Our methodology is applied to a stochastic three-tank system arranged in a cascade configuration, with dynamics adopted from [32], and evaluated against a property specified by a ζ-UCA $\mathcal{A} = (Q, \Delta, \varrho, Q_0, Q_F)$ as in Definition 1. In this case, $Q = \{q_0, q_1\}$, $\Delta = \{a, b\}$, $Q_0 = \{q_0\}$, and $Q_F = \{q_1\}$. The transitions between the states of $\mathcal{A}$ are governed by the edges of the graph depicted in Fig. 1, which define the transition function ϱ.

The stochastic three-tank system is discretized with a sampling time $\tau = 2$ seconds and is influenced by additive Gaussian noise $\varpi_i(\cdot)$, for $i \in [1; 3]$, with zero mean and variance of 0.01. The system is modeled by a dt-SCS, where the state evolves as:

$$\begin{aligned}
x_1(k+1) &= \Big[\sqrt{\beta^2 + x_1(k) + \tau u} - \beta\Big]^2 + 0.01\varpi_1(k), \\
x_i(k+1) &= \Big[\sqrt{\beta^2 + x_i(k) + \tau\sqrt{x_{i-1}(k+1)}} - \beta\Big]^2 \\
&\quad + 0.01\varpi_i(k),
\end{aligned} \tag{17}$$

where $\beta = 0.5\tau$ and $i \in \{2, 3\}$. For each $i \in [1; 3]$, the state $x_i(k)$ represents the level of fluid in the i-th tank at time $k \in$

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on April 21,2025 at 17:31:25 UTC from IEEE Xplore. Restrictions apply.

$\mathbb{Z}_{\geq 0}$, while $\sqrt{x_i(k)}$ corresponds to the outflow rate of the same tank. The inflow rate u into the first tank takes values from the set of control inputs $U = \{0, 1.5, 4.5, 7.5, 9\}$. The set of states is defined as $X = [0, 100]^3$, with initial states $X_0 = [0, 6]^2 \times [60, 66]$. Additionally, a labelling function $L : X \to \Delta$ is defined as follows:

$$L(x) = \begin{cases} a \ \forall x \in X \setminus (10, 60)^3, \\ b \ \forall x \in (10, 60)^3. \end{cases} \tag{18}$$

Based on the ζ-UCA depicted in Fig. 1, our objective is to systematically construct an SCBC that addresses Problem 1 by designing a controller $\mu : X \times Q \times [0; \zeta]$, ensuring that the dt-SCS in (17) satisfies the specification expressed by the ζ-UCA $\mathcal{A}$ in Fig. 1 with some probability lower bound. We select $\zeta = 8$; therefore, we aim to design a controller μ that ensures with some probability lower bound that (17) visits the region labeled by a no more than eight times during its evolution. The SCBC is obtained using the CEGIS approach described in the previous section. Hence, as in (11), we fix the SCBCs' structures as piecewise quadratic polynomials $\mathcal{S}_{q,\ell}(x) := \mathcal{S}(x, q, \ell) = \sum_{i=1}^{10} p^i(q, \ell)\psi^i(x) \quad \forall x \in X, \ \forall q \in Q$, and $\forall \ell \in [0; 9]$, where basis functions $\langle \psi^i(x) \rangle_{i=1}^{10} = \langle 1, x_1, x_2, x_3, x_1^2, x_1x_2, x_1x_3, x_2^2, x_2x_3, x_3^2 \rangle$. We reformulate the constraint (5) in query (16) into a bilinear form using equation (13) from [21], replacing the original min-max constraint. Then by leveraging the dReal SMT solver, we compute the SCBC coefficients along with other decision variables in the query, yielding the following results: $\lambda = 70$, $\gamma = 1$, and

$$p^i(q, \ell) = \begin{cases} 2.05842 & \text{if } (q, \ell, i) \in \Upsilon_1, \\ 0.21722 & \text{if } (q, \ell, i) \in \Upsilon_2, \\ 2.1 \times 10^{-3} & \text{if } (q, \ell, i) \in \Upsilon_3, \\ -2.6 \times 10^{-3} & \text{if } (q, \ell, i) \in \Upsilon_4, \\ 100 & \text{if } (q, \ell, i) \in \Upsilon_5, \\ -1.39896 & \text{if } (q, \ell, i) \in \Upsilon_6 \\ 30.38227 & \text{if } (q, \ell, i) \in \Upsilon_7, \\ 0 & \text{if } (q, \ell, i) \in \{q_1\} \times \{9\} \times [2; 10], \end{cases}$$

where:

$$\Upsilon_1 = \Big\{\{q_0\} \times \{\{(0, 1)\} \cup \{\{7\} \times \{3, 5, 8, 10\}\} \cup \{\{8\} \times \{3, 7, 8, 10\}\}\}\Big\} \cup \Big\{\{q_1\} \times \Big\{\{1, 2\} \times \{1\}\Big\}\Big\},$$

$$\Upsilon_2 = \Big\{\{q_0\} \times \Big\{\Big\{\{0\} \times [2; 10]\Big\} \cup \Big\{\{1\} \times \{2, 3, 4, 5, 7, 10\}\Big\} \cup \Big\{(5, 3)\Big\} \cup [2; 4]^2 \cup \Big\{\{5, 7\} \times \{6, 9\}\Big\}\Big\}\Big\} \cup \Big\{\{q_1\} \times \Big\{\Big\{\{1, 2\} \times [2; 4]\Big\} \cup \Big\{[3; 8] \times [2; 10]\Big\}\Big\}\Big\},$$

$$\Upsilon_3 = \Big\{\{q_0\} \times \Big\{\Big\{(6, 3), (6, 7), (7, 7), (8, 5)\Big\} \cup \Big\{\{1\} \times \{6, 8, 9\}\Big\} \cup \Big\{\{2\} \times [5; 10]\Big\} \cup \Big\{\{3\} \times \{5, 7, 8, 10\}\Big\} \cup \Big\{[4; 6] \times \{5, 8, 10\}\Big\}\Big\}\Big\} \cup \Big\{\{q_1\} \times \Big\{\{1, 2\} \times [5; 10]\Big\}\Big\},$$

$$\Upsilon_4 = \Big\{q_0\Big\} \times \Big\{\Big\{\{3, 6, 8\} \times \{6\}\Big\} \cup \Big\{\{4\} \times \{6, 7, 9\}\Big\} \cup \Big\{(5, 7)\Big\}\Big\},$$

$$\Upsilon_5 = \Big\{\{q_0\} \times \Big\{\Big\{[6; 9] \times \{1\}\Big\} \cup \Big\{\{9\} \times [2; 10]\Big\}\Big\}\Big\} \cup \Big\{\{q_1\} \times \Big\{\Big\{\{0\} \times [1; 10]\Big\} \cup \Big\{(9, 1)\Big\}\Big\}\Big\},$$

$$\Upsilon_6 = \Big\{q_0\Big\} \times \Big\{\Big\{\{5, 7\} \times \{2, 4\}\Big\} \cup \Big\{\{6, 8\} \times \{2, 4, 9\}\Big\}\Big\},$$

$$\Upsilon_7 = \Big\{\{q_0, q_1\} \times [1; 9] \times \{1\}\Big\}.$$

According to Theorem 1, the identified SCBC allows us to deploy a controller $\mu(x, q, \ell)$ for any $(x, q, \ell) \in X \times Q \times [0; 8]$ (cf. Fig. 3), ensuring that the specification expressed by $\mathcal{A}$ is enforced over the system in (17) with a satisfaction probability of at least 98.57%. Using the derived SCBC, we performed 10000 simulations on the closed-loop three-tank dt-SCS (17). Out of these simulations, 138 failed to meet the specification set by $\mathcal{A}$, resulting in 9862 successful sequences of the closed-loop states. Importantly, none of these 9862 sequences experienced the three tanks entering the region labeled a more than 8 times. This outcome yields an empirical satisfaction probability of 98.62%, consistent with the minimum threshold specified in Theorem 1. Fig. 2 displays 1000 of these 9862 successful closed-loop state sequences, while Fig. 3 shows the dt-SCS (17) synthesized controller from one of the 9862 successful cases. The entire SCBC construction process was implemented in Python on a 64GB RAM MacBook Pro with a 3.2 GHz processor, taking 220.34 seconds to complete. Moreover, by employing a predetermined SCBC template in this case, a quadratic polynomial we present Figure 4, which illustrates how the lower bound of the satisfaction probability changes with respect to the maximum number of visits, ζ, to region a. It is evident that as ζ grows, the lower bound of the probability of satisfaction also increases.

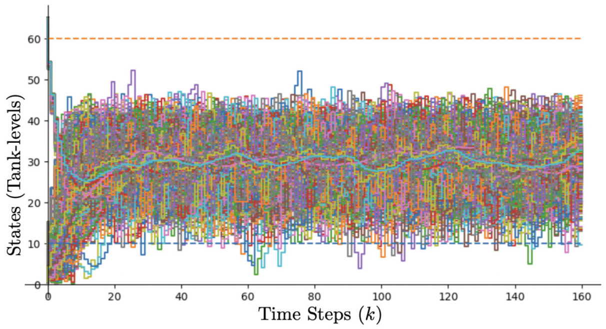

Fig. 2. One thousand closed-loop state trajectories from initial state $[x_1(0); x_2(0); x_3(0)] = [5; 0.5; 65]$ for the stochastic three-tank dt-SCS (17).

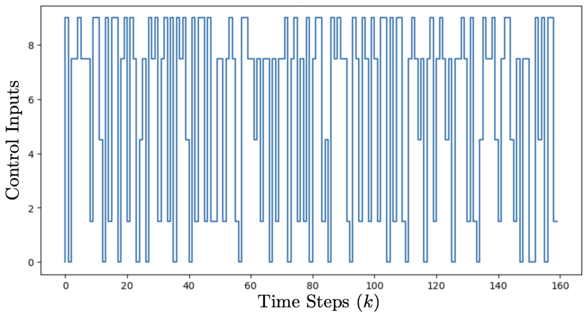

Fig. 3. An input trajectory synthesized for the stochastic three-tank dt-SCS (17) using (8).

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on April 21,2025 at 17:31:25 UTC from IEEE Xplore. Restrictions apply.

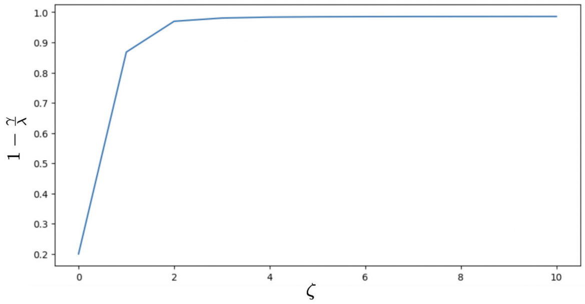

Fig. 4. The lower bound on the probability of satisfaction of ζ-UCA in Figure 1, based on a fixed quadratic SCBC template, with respect to the maximum number of visits ζ to region *a*.

V. Conclusion

In this letter, the main goal was to design a controller that ensures the satisfaction of a ζ-UCA property over a discrete-time stochastic control system. We achieved this by constructing an SCBC and using supermartingale theory to provide a lower bound on the probability of satisfaction. We discussed a method for computing the SCBC and demonstrated the effectiveness of our approach with a stochastic three-tank system. However, the CEGIS approach, although suitable for computing SCBCs, may present challenges due to its iterative nature and the lack of guaranteed termination, making it difficult to analyze its computational complexity. Future work could explore improvements inspired by recent findings [33] to achieve tighter lower bounds for the probability of satisfaction using SCBCs. Moreover, leveraging compositional strategies, including divide-and-conquer techniques for calculating SCBCs, will enhance scalability to tackle large-scale interconnected dt-SCSs.

References

[1] C. Baier and J.-P. Katoen, *Principles of Model Checking*. Cambridge, MA, USA: MIT Press, 2008.

[2] C. Belta, B. Yordanov, and E. A. Gol, *Formal Methods for Discrete-Time Dynamical Systems*, vol. 89. Cham, Switzerland: Springer, 2017,

[3] P. Tabuada, *Verification and Control of Hybrid Systems: A Symbolic Approach*. New York, NY, USA: Springer, 2009.

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

[5] N. Cauchi, L. Laurenti, M. Lahijanian, A. Abate, M. Kwiatkowska, and L. Cardelli, "Efficiency through uncertainty: Scalable formal synthesis for stochastic hybrid systems," in *Proc. 22nd ACM Int. Conf. Hybrid Syst., Comput. Control*, 2019, pp. 240–251.

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

[7] A. Nejati, S. Soudjani, and M. Zamani, "Abstraction-based synthesis of continuous-time stochastic control systems," in *Proc. 18th Eur. Control Conf. (ECC)*, 2019, pp. 1–6.

[8] D. Ajeleye and M. Zamani, "Data-driven construction of finite abstractions for interconnected systems: A compositional approach," 2024, *arXiv:2408.08497*.

[9] A. Lavaei, S. E. Z. Soudjani, R. Majumdar, and M. Zamani, "Compositional abstractions of interconnected discrete-time stochastic control systems," in *Proc. IEEE 56th Annu. Conf. Decision Control (CDC)*, 2017, pp. 3551–3556.

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

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

[12] A. Bohy, V. Bruyère, E. Filiot, N. Jin, and J.-F. Raskin, "Acacia+, a tool for LTL synthesis," in *Proc. 24th Int. Conf. Comput. Aided Verif.*, 2012, pp. 652–657.

[13] E. Filiot, N. Jin, and J.-F. Raskin, "An antichain algorithm for LTL realizability," in *Proc. 21st Int. Conf. Comput. Aided Verif.*, 2009, pp. 263–277.

[14] E. Filiot, N. Jin, and J.-F. Raskin, "Antichains and compositional algorithms for LTL synthesis," *Formal Methods Syst. Design*, vol. 39, pp. 261–296, Dec. 2011.

[15] S. Schewe and B. Finkbeiner, "Bounded synthesis," in *Proc. Int. Symp. Autom. Technol. Verif. Anal.*, 2007, pp. 474–488.

[16] T. Wongpiromsarn, U. Topcu, and A. Lamperski, "Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems," *IEEE Trans. Autom. Control*, vol. 61, no. 11, pp. 3344–3355, Nov. 2016.

[17] M. Anand, A. Lavaei, and M. Zamani, "From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems," *IEEE Trans. Autom. Control*, vol. 67, no. 10, pp. 5638–5645, Oct. 2022.

[18] P. Jagtap, S. Soudjani, and M. Zamani, "Temporal logic verification of stochastic systems using barrier certificates," in *Proc. Int. Symp. Autom. Technol. Verif. Anal.*, 2018, pp. 177–193.

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

[20] A. Abate, M. Giacobbe, and D. Roy, "Stochastic omega-regular verification and control with supermartingales," in *Proc. Int. Conf. Comput. Aided Verif.*, 2024, pp. 395–419.

[21] D. Ajeleye and M. Zamani, "Data-driven controller synthesis via co-Büchi barrier certificates with formal guarantees," *IEEE Control Syst. Lett.*, vol. 8, pp. 958–963, 2024.

[22] M. Anand, A. Lavaei, and M. Zamani, "Compositional synthesis of control barrier certificates for networks of stochastic systems against ω-regular specifications," *Nonlinear Anal., Hybrid Syst.*, vol. 51, Feb. 2024, Art. no. 101427.

[23] P. Jagtap, A. Swikir, and M. Zamani, "Compositional construction of control barrier functions for interconnected control systems," in *Proc. 23rd Int. Conf. Hybrid Syst., Comput. Control*, 2020, pp. 1–11.

[24] 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 Trans. Autom. Control*, vol. 68, no. 5, pp. 3011–3024, May 2023.

[25] 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.

[26] I. V. Evstigneev and V. Arkin, *Stochastic Models of Control and Economic Dynamics*. London, U.K.: Academic, 1987.

[27] D. Bertsekas and S. E. Shreve, *Stochastic Optimal Control: The Discrete-Time Case*, vol. 5. Nashua, NH, USA: Athena Sci., 1996,

[28] J. Ville, *Etude Critique de la Notion de Collectif*. Paris, France: Gauthier-Villars, 1939.

[29] A. Solar-Lezama, *Program Synthesis by Sketching*. Univ. California, Berkeley, CA, USA, 2008.

[30] L. De Moura and N. Bjørner, "Z3: An efficient SMT solver," in *Proc. Int. Conf. Tools Algorithms Constr. Anal. Syst.*, 2008, pp. 337–340.

[31] S. Gao, S. Kong, and E. M. Clarke, "dReal: An SMT solver for nonlinear theories over the reals," in *Proc. Int. Conf. Autom. Deduc.*, 2013, pp. 208–214.

[32] 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 *Proc. 22nd IEEE Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, 2017, pp. 1–4.

[33] M. Black, G. Fainekos, B. Hoxha, D. Prokhorov, and D. Panagou, "Safety under uncertainty: Tight bounds with risk-aware control barrier functions," in *Proc. IEEE Int. Conf. Robot. Autom. (ICRA)*, 2023, pp. 12686–12692.

Authorized licensed use limited to: UNIVERSITY OF COLORADO. Downloaded on April 21,2025 at 17:31:25 UTC from IEEE Xplore. Restrictions apply.