Abstract—This article is concerned with a compositional approach for the construction of control barrier certificates for large-scale interconnected stochastic systems while synthesizing hybrid controllers against high-level logic properties. Our proposed methodology involves decomposition of interconnected systems into smaller subsystems and leverages the notion of control sub-barrier certificates of subsystems, enabling one to construct control barrier certificates of interconnected systems by employing some max-type small-gain conditions. The main goal is to synthesize hybrid controllers enforcing complex logic properties, including the ones represented by the accepting language of deterministic finite automata, while providing probabilistic guarantees on the satisfaction of given specifications in bounded-time horizons. To do so, we propose a systematic approach to first decompose high-level specifications into simple reachability tasks by utilizing automata corresponding to the complement of specifications. We then construct control sub-barrier certificates and synthesize local controllers for those simpler tasks and combine them to obtain a hybrid controller that ensures satisfaction of the complex specification with some lower bound on the probability of satisfaction. We finally apply our proposed techniques to a fully-interconnected Kuramoto network composed of 100 nonlinear oscillators.

Index Terms—Compositionality, control barrier certificates, finite-state automata, formal controller synthesis, large-scale stochastic systems, small-gain conditions.

I. INTRODUCTION

Classical control problems can involve checking complex mathematical models against relatively simple properties, such as stability or invariance. On the other hand, the main problem in the formal methods community is to study dynamical models enforcing complex specifications including, but not limited to, safety, reachability, and reach-avoid. In particular, in the past few years, formal verification and synthesis of complex stochastic systems against a wide variety of high-level specifications have gained considerable attentions [1]. Many safety-critical scenarios, such as power networks, air traffic control, and so on, can be modeled by stochastic control systems, and these types of problems are especially challenging when dealing with large-scale systems with continuous state and input sets.

Existing results on the verification and controller synthesis of large-scale stochastic systems have been widely focused on abstraction-based techniques. Such approaches include probabilistic reachability guarantees for discrete-time stochastic hybrid systems via abstraction [2], game-based abstractions for controller synthesis [3] in stochastic hybrid automata, and an abstraction-based framework for the synthesis of bounded Markov decision processes against probabilistic computation tree logic (PCTL) [4]. However, these techniques rely on state-space discretization, and accordingly, computational complexity increases exponentially with the dimension of the state space. This issue has been partially alleviated by using sequential gridding procedures [5] and input-set abstraction for incrementally stable stochastic control systems [6]. As an alternative solution proposed in recent years, one can consider a large-scale system as an interconnection of smaller subsystems and employ compositionality techniques for constructing finite abstractions of interconnected systems based on abstractions of subsystems [7]. More recently, discretization-free approaches via control barrier certificates have been proposed for the verification and synthesis of stochastic systems. Existing results include safety verification of continuous-time stochastic hybrid systems in infinite-time horizons [8], [9]. Such verification in infinite time requires a supermartingale condition that implicitly assumes the system’s stability at its equilibrium point, which is restrictive. In [10], this condition is generalized to the safety verification of stochastic systems in finite-time domains. Controller synthesis for the finite-time safety of stochastic systems using control barrier certificates is discussed in [11]. Systematic verification and synthesis techniques against temporal logic specifications for nonlinear systems are provided in [12], [13] and for Markov decision processes in [14]. Finite-time controller synthesis for discrete-time stochastic control systems using barrier certificates against automata representation of temporal logic properties is proposed in [15].

The proposed techniques in the aforementioned literature involve restricting control barrier certificates to a certain parametric form, such as exponential or polynomial, by searching for their corresponding coefficients under certain assumptions. Although lower-dimensional systems usually admit such simple control barrier certificates and the corresponding search is relatively easy using existing tools, it may be very difficult (if not impossible) in the case of large-scale systems, and therefore, such techniques become computationally intractable.

In order to overcome the aforementioned challenge, we propose a compositional framework for the construction of control barrier certificates for large-scale interconnected stochastic systems. The proposed approach involves decomposing a large-scale stochastic...
system into a number of smaller subsystems of lower dimensions and searching for control sub-barrier certificates for those subsystems together with corresponding local controllers. By leveraging some maximum small-gain conditions, a control barrier certificate and its corresponding controller for the interconnected system can be constructed from control sub-barrier certificates and corresponding local controllers of subsystems. The control barrier certificate is then utilized to establish upper bounds on the probability that interconnected systems reach unsafe regions within finite-time horizons, thereby allowing finite-time verification and synthesis of safety properties.

For synthesizing controllers for more general specifications, we provide a systematic method to decompose a complex property that can be expressed by an acceptance language of a deterministic finite automaton (DFA) into simpler tasks based on the complement automaton of the original specification. Control sub-barrier certificates are then computed for each task along with the corresponding probabilities which can eventually be combined to obtain a lower-bound probability using which the system would satisfy the original specification over a finite-time horizon. Correspondingly, a hybrid controller is achieved for the large-scale interconnected stochastic system that ensures the satisfaction of the given specification. We finally apply our proposed results to a fully-interconnected Kuramoto network with 100 nonlinear oscillators, and synthesize hybrid controllers to ensure satisfaction of a complex specification given by a deterministic finite automaton.

Compositional construction of control barrier certificates via small-gain theorem is presented in [16] but in the context of input-to-state safety properties for non-stochastic interconnected systems with only two subsystems. In comparison, our proposed results are for stochastic large-scale systems without putting any restrictions on the number of subsystems. Moreover, we study here a larger class of logic specifications described by DFA. Compositional construction of control barrier certificates for non-stochastic control systems is also presented in [17] for enforcing specifications that can be described by deterministic Büchi automata (DFA) over infinite-time horizons. In comparison, we deal with stochastic control systems and provide finite-time horizon guarantees for specifications expressed by DFA. Compositional construction of control barrier certificates for large-scale stochastic systems is recently discussed in [18]. Our current work generalizes [18] in two main directions. First and mainly, we do not restrict ourselves to verification and synthesis over simple safety specifications and consider a larger class of specifications that can be accepted by allowing languages of DFA. As our second contribution, this article includes a comprehensive fully-interconnected nonlinear case against complex logic properties expressed by DFA that illustrates the proposed results.

Compositional construction of control barrier functions for large-scale stochastic systems are recently presented in [19] but for continuous-time stochastic systems with a different compositional technique based on sum-type small-gain conditions. Unfortunately, those conditions are conservative as they are all formulated in terms of “almost” linear gains, which means that subsystems should have a (nearly) linear behavior. Due to lack of space, we provide some of the technical discussions and an additional case study in the arXiv version of this article in [20].

II. DISCRETE-TIME STOCHASTIC CONTROL SYSTEMS

A. Preliminaries

We consider the probability space \((\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)\), where \(\Omega\) is the sample space, \(\mathcal{F}_\Omega\) is a sigma-algebra on \(\Omega\) consisting subsets of \(\Omega\) as events, and \(\mathbb{P}_\Omega\) is the probability measure assigning probabilities to those events. Random variables are assumed to be measurable functions of the form \(X : (\Omega, \mathcal{F}_\Omega) \to (S_X, \mathcal{F}_X)\) such that a random variable \(X\) induces a probability measure on its space \((S_X, \mathcal{F}_X)\) as \(\text{Prob}(A) = \mathbb{P}_\Omega(\{X^{-1}(A)\})\) for any \(A \in \mathcal{F}_X\). The probability measure on \((S_X, \mathcal{F}_X)\) is presented directly without explicitly mentioning the underlying probability space or the function \(X\). The topological space \(S\) is a Borel space if it is homeomorphic to a Borel subset of a separable and completely metrizable space. \(\mathcal{B}(S)\) is the Borel sigma-algebra generated from a Borel space \(S\). The map \(f : S \to Y\) is measurable whenever it is Borel measurable.

B. Notations

We denote the set of real, positive, and non-negative real numbers by \(\mathbb{R}, \mathbb{R}_{\geq 0}\), and \(\mathbb{R}_{\geq 0}\), respectively, and \(\mathbb{R}^n\) denotes a real space of dimension \(n\). We use \(\mathbb{N}\) and \(\mathbb{N}_{\geq 1}\) to represent the set of non-negative integers and positive integers, respectively. Given a vector \(x_i \in \mathbb{R}^n\), the corresponding column vector of dimension \(\sum_i n_i\) is denoted by \(x = [x_1; \ldots; x_N]\). For a vector \(x \in \mathbb{R}^n\), an infinity norm of \(x\) is denoted by \(\|x\|\). Symbols \(\mathcal{I}_n\), \(\mathcal{O}_n\), and \(\mathcal{I}_n\) denote the identity matrix in \(\mathbb{R}^{n \times n}\) and the column vectors in \(\mathbb{R}^{n \times 1}\) with all elements equal to zero and one, respectively. The identity function and composition of functions are denoted by \(\mathcal{I}_n\) and symbol \(\circ\), respectively. Given functions \(f_i : X_i \to Y_i\), for any \(i \in \{1, \ldots, N\}\), their Cartesian product \(\prod_{i=1}^{N} f_i : \prod_{i=1}^{N} X_i \to \prod_{i=1}^{N} Y_i\) is defined as \((\prod_{i=1}^{N} f_i)(x_1, \ldots, x_N) = (f_1(x_1); \ldots; f_N(x_N))\). For a set \(S, |S|\) denotes its cardinality. Empty set is denoted by \(\emptyset\). The power set of \(S\) is denoted by \(2^S\). Given a set \(S \subset \mathbb{R}^n\), the complement of \(P\) with respect to \(S\) is given by \(S \setminus P = \{x \in S, x \notin P\}\). A function \(\nu : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}\) is said to be a class \(K\) function if it is continuous, strictly increasing, and \(\nu(0) = 0\). A class \(K\) function \(\nu(\cdot)\) belongs to the class \(\mathcal{K}_\infty\) if \(\nu(s) \to \infty\) as \(s \to \infty\).

C. Discrete-Time Stochastic Control Systems

In this article, we focus on discrete-time stochastic control systems (dt-SCS), as formalized in the following definition.

Definition 1.1: A discrete-time stochastic control system (dt-SCS) is a tuple

\[\mathcal{S} = (X, U, \varsigma, f)\]

where,

1. \(X \subseteq \mathbb{R}^n\) is a Borel set as the state set of the system;
2. \(U \subseteq \mathbb{R}^m\) is a Borel set as the input set of the system;
3. \(\varsigma\) is a sequence of independent and identically distributed (i.i.d.) random variables from a sample space \(\Omega\) to the measurable space \((\mathcal{Y}_\varsigma, \mathcal{F}_\varsigma)\), namely \(\varsigma := \{k\} : \Omega \to \mathcal{Y}_\varsigma, k \in \mathbb{N}\); and
4. \(f : X \times U \times \mathcal{Y}_\varsigma \to X\) is a measurable function that characterizes the state evolution of \(\mathcal{S}\).

The evolution of the state of dt-SCS \(\mathcal{S}\) for a given initial state \(x(0) \in X\), and input sequence \(\{\nu(k) : \Omega \to U, k \in \mathbb{N}\}\) is described by

\[x(k+1) = f(x(k), \nu(k), (k)).\]

A set \(\mathcal{U}\) is associated with \(U\) as a collection of sequences \(\{\nu(k) : \Omega \to U, k \in \mathbb{N}\}\), where \(\nu(k)\) is independent of \(\varsigma(\cdot)\) for any \(k, z \in \mathbb{N}\), and \(z \geq k\). For any initial state \(x \in X\) and \(\nu(\cdot) \in \mathcal{U}\), \(x^{\nu, \varsigma} : \Omega \times \mathbb{N} \to X\) denotes the solution process of \(\mathcal{S}\) under the input sequence \(\nu\) and an initial state \(a\). We now present history-dependent policies to control dt-SCS in (1).
Definition 2.2: For a dt-SCS $\mathcal{S}$ as in (1), a history-dependent policy $\pi = (\pi_0, \pi_1, \ldots)$ is a sequence with functions $\pi_i : G_i \rightarrow U$, where $G_i$ is the set of all $i$-histories $g_i$ that can be defined as $g_i := (x(0), \nu(0), x(1), \nu(1), \ldots, x(i), \nu(i-1), x(i))$. Stationary policies are a subclass of history-dependent policies where $\pi = (\nu, \nu, \ldots), \nu : X \rightarrow U$. Here, the mapping at any time $i$ only depends on the current state $x(i)$ and is not time-variant.

This article is mainly concerned with the controller synthesis for large-scale interconnected dt-SCS as in (1), that can be considered as compositions of several smaller subsystems. These subsystems consist of internal and external inputs, as well as outputs, as defined below.

Definition 2.3: A dt-SCS with internal inputs is a tuple $\mathcal{S} = (X, U, W, \varsigma, f, Y, h)$, where $X, U$, and $W$ are Borel sets as the state set, external input set, and internal input set of the system, respectively. $\varsigma$ is a sequence of i.i.d. random variables from a sample space $\Omega$, $f : X \times U \times W \times V_i \rightarrow X$ is a measurable function characterizing the state evolution of the system, $Y$ is a Borel set as the output set of the system, and $h : X \rightarrow Y$ is a measurable output function that maps states of the system to their outputs $y = h(x)$. Consequently, the dynamics in (2) is extended accordingly to dt-SCS with internal inputs and outputs and is described by

$$\mathcal{S} : \begin{cases} x(k + 1) = f(x(k), \nu(k), w(k), \varsigma(k)), & k \in \mathbb{N}. \\ y(k) = h(x(k)). \end{cases}$$

Moreover, we associate with $W$ a set $\mathcal{W}$ to be a collection of sequences $\{w(k) : \Omega \rightarrow W, k \in \mathbb{N}\}$, where $w(k)$ is independent of $\varsigma(z)$ for any $z, k \in \mathbb{N}$ and $k \geq z$. Now, for any initial state $a \in X$, $\nu'(\cdot) \in U$ and $w'(\cdot) \in \mathcal{W}$, the solution process of $\mathcal{S}$ is denoted by random sequences $x^{a,w'} : \Omega \times \mathbb{N} \rightarrow X$ under an internal input $\nu$, an external input $w$, and an initial state $a$.

Remark 2.4: Note that the main role of outputs in (3) is for the sake of interconnection, which we will see later. More precisely, we assume that the output map of the interconnected system is identity (i.e., the full-state information is available), as appears in (2), mainly for the sake of controller synthesis.

III. CONTROL (SUB-)BARRIER CERTIFICATES

We first define control barrier certificates for interconnected dt-SCS, borrowed from [18], which will later be used to obtain probabilistic guarantees on the satisfaction of specifications over interconnected systems.

**Definition 3.1:** Consider an interconnected dt-SCS $\mathcal{S} = (X, U, \varsigma, f)$ without internal inputs. A function $B : X \rightarrow \mathbb{R}_{\geq 0}$ is called a control barrier certificate (CBC) for $\mathcal{S}$ if

$$B(x) \leq \eta, \quad \forall x \in X_0, \quad B(x) \geq \beta, \quad \forall x \in X_u,$$

and $\forall x \in X, \exists u \in U$, such that

$$\mathbb{E} \left[ B(x(k + 1)) \mid x(k) = x, \nu(k) = u \right] \leq \max \left\{ \kappa(B(x(k))), c \right\},$$

for a function $\kappa \in \mathcal{K}_\infty$, with $\kappa < \mathcal{I}_d$, and constants $\eta, c \in \mathbb{R}_{\geq 0}$ and $\beta \geq \eta$.

A similar definition, borrowed from [18], is applied for dt-SCS with both external and internal inputs.

**Definition 3.2:** Consider a dt-SCS with both internal and external inputs as $\mathcal{S} = (X, U, W, \varsigma, f, Y, h)$, with sets $X_0, X_u \leq X$ as initial and unsafe sets of the system, respectively. A function $B : X \rightarrow \mathbb{R}_{\geq 0}$ is said to be a control sub-barrier certificate (CSBC) for $\mathcal{S}$ if there exist functions $\alpha, \kappa \in \mathcal{K}_\infty$, with $\kappa < \mathcal{I}_d$, $\rho \in \mathcal{K}_\infty \cup \{0\}$, and constants $\eta, c \in \mathbb{R}_{\geq 0}$ and $\beta \in \mathbb{R}_{\geq 0}$, such that

$$B(x) \geq \alpha \left( ||h(x)||^2 \right), \quad \forall x \in X,$$

$$B(x) \leq \eta, \quad \forall x \in X_0,$$

$$B(x) \geq \beta, \quad \forall x \in X_u,$$

and $\forall x \in X, \exists u \in U$, such that $\forall w \in W$, $\mathbb{E} \left[ B(x(k + 1)) \mid x(k) = x, \nu(k) = u, w(k) = w \right] \leq \max \left\{ \kappa(B(x(k))), \rho(||w||^2), c \right\}$.

Remark 3.3: We require condition $\beta > \eta$ in Definition 3.1 for interconnected systems in order to propose meaningful probabilistic bounds on the satisfaction of specifications using Theorem 3.4. However, we do not ask such a condition in Definition 3.2 for dt-SCS with internal inputs since a CSBC does not explicitly provide any probabilistic safety guarantees. In fact, CSBCs as in Definition 3.2 are only utilized to compute CBCs for the interconnected system, which then provide safety guarantees over the interconnected system (cf. Section IV-B).

Now, employing Definition 3.1, we provide a theorem, borrowed from [18], that quantifies an upper bound on the probability that an interconnected dt-SCS reaches an unsafe region in a finite-time horizon.

**Theorem 3.4:** Let $\mathcal{S} = (X, U, \varsigma, f)$ be an interconnected dt-SCS. Suppose $B$ is a CBC for $\mathcal{S}$ and there exists a constant $0 < k < 1$ such that function $\kappa \in \mathcal{K}_\infty$ in (6) satisfies $\kappa(k) \leq \kappa_s$, $\forall s \in \mathbb{R}_{\geq 0}$. Then the probability that the solution process of $\mathcal{S}$ starts from any initial state $a \in X_0$ and reaches an unsafe region $X_u$ under the controller $\nu(\cdot)$ within finite time steps $k \in [0, T_d]$ is lower bounded as

$$\mathbb{P}_a \left\{ \sup_{0 \leq k \leq T_d} B(x(k)) \geq \beta \mid a \right\} \leq \mathcal{X},$$

where,

$$\mathcal{X} = \begin{cases} 1 - \left( 1 - \frac{\eta}{\beta} \right) \left( 1 - \frac{c}{\beta} \right)^{T_d}, & \text{if } \beta \geq \frac{\kappa_s}{1 - \frac{c}{\beta}}, \\ \frac{\eta}{k \kappa_s} \left( \frac{\kappa_s}{k \kappa_s} \right)^{T_d}, & \text{if } \beta < \frac{\kappa_s}{1 - \frac{c}{\beta}}. \end{cases}$$

In the next section, we describe interconnected stochastic control systems as a composition of several stochastic subsystems, and provide compositional conditions under which a CBC of an interconnected system can be constructed from CSBCs of subsystems.

IV. COMPOSITIONAL CONSTRUCTION OF CBC

A. Interconnected Stochastic Control Systems

Suppose we are given $N$ control subsystems

$$\mathcal{S}_i = (X_i, U_i, W_i, \varsigma_i, f_i, Y_i, h_i), \quad i \in \{1, \ldots, N\},$$

where $X_i \in \mathbb{R}^n, U_i \in \mathbb{R}^{m_i}, W_i \in \mathbb{R}^{p_i}$, and $Y_i \in \mathbb{R}^{q_i}$, whose internal inputs and outputs are partitioned as

$$w_i = [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}],$$

$$y_i = [y_{i1}; \ldots; y_{IN}],$$

and their output spaces and functions are of the form

$$Y_i = \prod_{j=1}^{N} Y_{ij}, \quad h_i(x_i) = [h_{i1}(x_i); \ldots; h_{IN}(x_i)].$$

We call outputs $y_{ij} = x_j$ as external ones, whereas outputs $y_{ij}$ with $i \neq j$ are internal ones which are used to interconnect stochastic control subsystems. If there exists a connection from $\mathcal{S}_j$ to $\mathcal{S}_i$, then $w_{ij} = y_{ji}.$
The term “internal” is utilized to refer to those inputs and each subsystem $\subseteq X, U, \varsigma, f$; i.e., $h_{ii}(x_i) = x_i$. In the absence of full-state information, the controller synthesis becomes more challenging since one requires the existence of an estimator with some given accuracy. See [21] for a detailed discussion. Under this assumption, we are able to formulate CSBCs and controllers directly over the actual states of the system.

We now provide a formal definition of interconnected discrete-time stochastic control systems.

**Definition 4.2:** Consider $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems $S_i = (X_i, U_i, W_i, \varsigma_i, f_i, Y_i, h_i), \ i \in \{1, \ldots, N\}$, with the input–output partition as in (13) and (14). The interconnected discrete-time stochastic control system $\mathcal{S} = (X, U, \varsigma, f)$ is composed of $S_i \forall i \in \{1, \ldots, N\}$, denoted by $\mathcal{S}(S_1, \ldots, S_N)$ such that $X := \prod_{i=1}^{N} X_i, U := \prod_{i=1}^{N} U_i, \varsigma := \varsigma_1 \sqcup \cdots \sqcup \varsigma_N$, and $f := \prod_{i=1}^{N} f_i$, subjected to

$$\forall i, j \in \{1, \ldots, N\}, i \neq j : w_{ji} = y_{ij}, \ Y_i \subseteq W_{ji}.$$  

For the sake of better illustrations of the results, we provide our case study as a running example throughout the article.

**Case study:** Consider a Kuramoto oscillator network $\mathcal{S} = 100$ oscillators with a fully-connected topology, as illustrated in Fig. 1. The dynamics of the network is adapted from [22] by adding stochasticity as additive noise and is also presented in Fig. 1. Here, $\theta = \{\theta_1; \ldots; \theta_N\}$ is the phase of oscillators with $\theta_i \in [0, 2\pi] \forall i \in \{1, \ldots, N\}, \Omega = [\Omega_1; \ldots; \Omega_N] = [0; 0.01; 0.01]$ is the natural frequency of oscillators, $K = 0.0012$ is the coupling strength, $\tau = 0.1$ is the sampling time, $\phi(\theta(k)) = [\phi_1(\theta_1(k)); \ldots; \phi_N(\theta_N(k))]$ such that $\phi_1(\theta_1(k)) = \sum_{i \neq 1} \sin(\theta_i(k) - \theta_1(k)), \forall i \in \{1, \ldots, N\}, \nu(k) = [\nu_1(k); \ldots; \nu_N(k)],$ and $\varsigma(k) = [\varsigma_1(k); \ldots; \varsigma_N(k)]$. The dt-SCS is given by $\mathcal{S} = (\mathcal{S}_1, \ldots, \mathcal{S}_N)$, i.e., it can be decomposed as an interconnection of $N$ subsystems $S_i$ whose dynamics are shown in Fig. 1.

**B. Compositional Construction of CBC for Interconnected Systems**

In this subsection, we provide a compositional framework for the construction of CBC for $\mathcal{S}$ using CSBC of $S_i$. For each control subsystem $S_i, i \in \{1, \ldots, N\}$ in (12), suppose there exists CSBC $B_i$ as defined in Definition 3.2 with functions $\alpha_i, \kappa_i : \mathbb{K} \rightarrow \mathbb{K}$, with $\kappa_i \leq \tau_d, \rho_i \in \mathbb{K}_0 \cup \{0\}$, and constants $\eta_i, \varsigma_i \in \mathbb{R}_{\geq 0}$ and $\beta_i \in \mathbb{R}_{\geq 0}$. Now, we present the following small-gain assumption that is essential for the compositional construction of CBC for $\mathcal{S}$.

**Assumption 4.3:** Assume that $K_{\infty}$ functions $\kappa_{ij}$ defined as

$$\kappa_{ij}(s) := \begin{cases} \kappa_i(s), & \text{if } i = j, \\ \rho_i(\alpha_i^{-1}(s)), & \text{if } i \neq j, \end{cases}$$

satisfy

$$\kappa_{ij} \circ \kappa_{ji} \circ \cdots \circ \kappa_{i_{r-1}j_r} \circ \kappa_{i_rj_1} < \tau_d,$$

for all sequences $(i_1, \ldots, i_r) \in \{1, \ldots, N\}^r$ and $r \in \{1, \ldots, N\}$. The small-gain condition (15) implies the existence of $K_{\infty}$ functions $\vartheta_i > 0$ [23, Th. 5.5], satisfying

$$\max_{i,j} \left\{ \vartheta_i^{-1}(\kappa_{ij} \circ \vartheta_j) \right\} < \tau_d, \ i, j \in \{1, \ldots, N\}.$$  

**Remark 4.4:** Note that (15) is a standard small-gain assumption employed for investigating the stability of large-scale interconnected systems via ISS Lyapunov functions [24]. This condition is automatically satisfied if each $\kappa_{ij}$ is less than identity (i.e., $\kappa_{ij} < \tau_d, \forall i, j \in \{1, \ldots, N\}$).

In the next theorem, we show that one can construct a CBC of $\mathcal{S}$ using CSBC of $S_i$ if Assumption 4.3 holds and $\max \vartheta_i^{-1}$ is concave (in order to employ Jensen’s inequality [25]).

**Theorem 4.5:** Consider the interconnected dt-SCS $\mathcal{S} = (\mathcal{S}_1, \ldots, \mathcal{S}_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems $S_i$. Suppose that each $S_i$ admits a CBC $B_i$, as defined in Definition 3.2. If Assumption 4.3 holds and

$$\max_i \left\{ \vartheta_i^{-1}(\kappa_{ij} \circ \vartheta_j) \right\} > \max_i \left\{ \vartheta_i^{-1}(\vartheta_j) \right\},$$

then function $B(x)$ defined as

$$B(x) := \max_i \left\{ \vartheta_i^{-1}(B_i(x_i)) \right\},$$

is a CBC for the interconnected system $\mathcal{S} = (\mathcal{S}_1, \ldots, \mathcal{S}_N)$ provided that $\max \vartheta_i^{-1}$ for $\vartheta_i$ as in (16) is concave.

**Remark 4.6:** Note that $\vartheta_i$ in (16) plays a significant role in rescaling CSBC for subsystems while normalizing the effect of internal gains of other subsystems (cf. [24] for a similar argument but in the context of stability analysis via ISS Lyapunov functions). This rescaling issue mitigates the conservativeness of condition (17), and hence, this condition is able to be satisfied in many scenarios (cf. case study).

**Remark 4.7:** The compositional construction of CBC for the interconnected system relies on the search for CSBCs of individual subsystems. This can be done using sum-of-squares (SOS) optimization techniques under certain assumptions on dynamics of subsystems as explained in [18], [20]. Alternatively, one can also utilize counterexample guided inductive synthesis (CEGIS) techniques provided in [15], [20].

So far, our discussion has been limited to providing probabilistic safety guarantees for interconnected dt-SCS via CBCs. In the next section, we introduce a more general class of specifications expressed by deterministic finite automata, and provide a systematic method to obtain probabilistic guarantees for the satisfaction of such complex specifications.

**V. Specifications Expressed by DFA**

In this article, we deal with a general class of specifications that can be expressed by deterministic finite automata.

**Definition 5.1:** A deterministic finite automat (DFA) is a tuple $A = (Q, q_0, \Sigma, \delta, F)$, where $Q$ is a finite set of states, $q_0 \in Q$ is the initial state, $\Sigma$ is a finite set of input symbols called alphabet, $\delta : Q \times \Sigma \rightarrow Q$ is the transition function, and $F \subseteq Q$ represents the accepting states.

We consider specifications that can be represented by accepting languages of DFA $A$ as in Definition 5.1 over a set of atomic propositions $AP$, i.e., $\Sigma = 2^{AP}$. For instance, all LTL specifications over finite-time...
horizons (i.e., LTLf) [26] can be represented by DFA, which can be built using existing tools, such as SPOT [27]. Note that specifications represented by DFA are more expressive than LTLf [28].

Remark 5.2: A DFA $A$ is normally constructed over the alphabet $\Sigma = 2^{AP}$. However, without loss of generality, we work here with the set of atomic propositions $AP$ as the alphabet rather than its power set $2^{AP}$, i.e., $\Sigma = AP$.

Let $\delta(q, \sigma)$ denote a state in the DFA that can be reached from state $q \in Q$ in the presence of a symbol $\sigma$. A finite word or trace $(\sigma_0, \sigma_1, \ldots, \sigma_{n-1}) \in \Sigma^*$ is accepted by the DFA if there exists a finite state run $q_i = (q_0, q_1, \ldots, q_n) \in Q^{n+1}$ such that $q_{i+1} = \delta(q_i, \sigma_i)$ for all $0 \leq i < n$ and $q_0 \in F$. The accepting language of DFA $A$ is denoted by $L(A)$, which is the set of all finite words accepted by $A$. The complement of a DFA is simply acquired by interchanging its accepting and non-accepting states.

Definition 5.3: For an interconnected dt-SCS $\mathcal{S} = (X, U, \varsigma, f)$ and a DFA $A = (Q, q_0, AP, \delta, F)$, consider a labeling function $L : X \rightarrow AP$. For a finite state sequence $x_M = (x(0), x(1), \ldots, x(M-1)) \in X^M$ of length $M \in \mathbb{N}$, the corresponding finite word over $AP$ is given by $L(x) := (\sigma_0, \sigma_1, \ldots, \sigma_{M-1}) \in \mathcal{AP}^M$, where $\sigma_i = L(x(i))$ for all $i \in \{0, 1, \ldots, M-1\}$.

We now define the probability with which the solution processes of the interconnected system satisfy a specification over a time horizon $M$.

Definition 5.4: Consider an interconnected dt-SCS $\mathcal{S} = (X, U, \varsigma, f)$ and a DFA $A = (Q, q_0, AP, \delta, F)$, a specification given by the accepting language of a DFA $M = (Q, q_0, \mathcal{AP}, \delta, F)$ and a labeling function $L : X \rightarrow \mathcal{AP}$. Then, the probability with which the solution process $x_M$ of $\mathcal{S}$ of length $M \in \mathbb{N}$ started from an initial condition $x(0) = 0$ under the controller $\nu(\cdot)$, satisfies the specification expressed by $A$ is denoted by $\mathbb{P}_\nu^M[L(x_M) = A]$.

We now state the synthesis problem considered in the article.

Problem 5.5: Given an interconnected dt-SCS $\mathcal{S} = (X, U, \varsigma, f)$, a desired specification admitted by the accepting language of the DFA $A = (Q, q_0, \mathcal{AP}, \delta, F)$ over a set of atomic propositions $\mathcal{AP} = \{p_0, p_1, \ldots, p_r\}, R \subseteq \mathbb{N}$, and a labeling function $L : X \rightarrow \mathcal{AP}$, compute a controller $\nu(\cdot)$ and a constant $\varepsilon \in [0, 1]$ such that $\mathbb{P}_\nu^M[L(x_M) = A] \geq \varepsilon$.

To solve this problem, we utilize a DFA representing the complement of the complex specification and decompose it into simpler reachability tasks. For these tasks, we aim to find suitable CBCs, as in Definition 3.1, along with controllers for the interconnected dt-SCS. However, finding CBCs could be computationally expensive. To circumvent this complexity, we consider the interconnected dt-SCS $\mathcal{S} = (X, U, \varsigma, f)$ as an interconnected network of $N$ subsystems $\mathcal{G}_i = (X_i, U_i, \varsigma_i, f_i, Y_i, h_i), i \in \{1, \ldots, N\}$, as explained in Section IV.

Let $X_0$ and $X_\infty$ be two sets as introduced in Definition 3.1 that are connected to atomic propositions $AP$ through some labeling function $L : X \rightarrow \mathcal{AP}$. We assume that those sets can be decomposed as $X_0 = \bigcup_{i=1}^N X_{o_i}$ and $X_\infty = \bigcup_{i=1}^N X_{\infty_i}$. By doing so, one can simply compute a CSBC for each subsystem separately and utilize Theorem 4.5 to obtain a CBC for the interconnected system. Similarly, it is assumed that atomic propositions in the set $AP$ can also be decomposed accordingly. This implies that sets $X_0$ and $X_\infty, i \in \{1, \ldots, N\}$, are also connected to the corresponding decomposed structure of $AP$.

Case study (continued): For the Kuramoto network $\mathcal{E}$ in Fig. 1, we consider the following regions of interest: $X^0 = \{[0, 1]_i, X^1 = \{[23, 25]_i \} \} \mathcal{N}, X^2 = \{[14, 25]_i \} \mathcal{N}, X^3 = \{[0, 16]_i \} \mathcal{N}, X^4 = \{[21, 25]_i, X^5 = \{[23, 25]_i \} \mathcal{N},$ and $X^6 = X_\mathcal{N}(X^0 \cup X^1 \cup X^2 \cup X^3 \cup X^4 \cup X^5)$. Each region is associated with an element of the atomic proposition given by $AP = \{p_0, p_1, p_2, p_3, p_4, p_5, p_6\}$ such that the labeling function $L(x_i) = p_i$ for all $x_i \in X^i, i \in \{0, 1, \ldots, 6\}$. The main goal is to compute a controller such that if the system starts from $X^1$, it must always stay away from $X^0$ and $X^2$, and if it starts from $X^4$, it must always stay away from $X^3$ and $X^5$ within the time horizon $[0, T_d] \subseteq \mathbb{N}$, with $T_d = 7$. This can be represented as an LTLf specification given by $(p_1 \land \neg(p_0 \lor p_2)) \lor (p_4 \land \neg(p_3 \lor p_5))$ associated with $T_d = 7$, or as the language of a DFA, whose complement DFA $A^c$ is, as shown in Fig. 2.

VI. SEQUENTIAL REACHABILITY DECOMPOSITION

In this subsection, we describe the sequential reachability decomposition, in which we divide a complex specification into simpler reachability tasks by utilizing the automaton representing the complement of the specification. This was initially proposed in [15] for a monolithic system. For the sake of completeness, we provide a short description of the procedure in this section and refer interested readers to the arXiv version [20] for detailed information.

For a DFA $A$ representing the desired specification, we first construct a complement DFA $A^c = (Q, q_0, \mathcal{AP}, \delta, F)$ with $F = \mathcal{Q}\backslash F$. The procedure then involves identifying all accepting state runs of $A^c$ of the length at most $M + 1$, with $M \in \mathbb{N}$ being the time horizon. Let $\mathcal{R}_M, M \in \mathbb{N}$, be the set of all finite accepting state runs of at most length $M + 1$ excluding self-loops, where

$\mathcal{R}_M := \{q = (q_0, q_1, \ldots, q_m) \in Q^{m+1} | m \leq M, q_m \in F, q_i \neq q_{i+1}, \forall i < m\}.$

Now, for each $p \in \mathcal{AP}$, we define $\mathcal{R}_M^p$ as

$\mathcal{R}_M^p := \{q = (q_0, q_1, \ldots, q_m) \in \mathcal{R}_M | \sigma(q_0, q_1) = p \in \mathcal{AP}\}.$

We consider any $q = (q_0, q_1, \ldots, q_m) \in \mathcal{R}_M^p$ and define the set $P^p(q)$ of all state runs augmented with a horizon as

$P^p(q) := \{(q_i, q_{i+1}, q_{i+2}) | 0 \leq l \leq m - 2\}$, (19)

to decompose our specification into sequential reachabilities. The horizon $T_h(q, q_{i+l}) = M + 2 - |q|$ for $q_{i+l} \in Q_{\mathcal{P}}$, and 1 otherwise. We define $P^p(M) = \bigcup_{p \in \mathcal{AP}} \bigcup_{q \in \mathcal{R}_M^p} P^p(q)$ as the set of all reachability elements arising from different accepting state runs of a length less than or equal to $M + 1$.

Remark 6.1: The self-loops play a pivotal role in the computation of the time horizon $T_h(q, q_{i+l})$ for any reachability element $\nu = (q, q_1, q_2, q_3) \in P^p(q)$. This is crucial to account for the number of time steps that the solution process can remain in the self-loop $q_{i+l} \in Q_{\mathcal{P}}$ before reaching $q_{i+l+2}$ [15].

Remark 6.2: Note that $P^p(q) = \emptyset$ for those accepting state runs whose length is 2. Any such sequences begin from a subset of the state space that already violates the desired specification, and the outcome
is accordingly a trivial zero probability for the satisfaction of the specification.

For each reachability task, we construct an appropriate CBC along with a corresponding controller to obtain an upper bound on the probability that the interconnected system $\mathcal{S}$ reaches unsafe regions in finite-time horizons. We raise the following lemma to compute CBCs and reachability probabilities.

**Lemma 6.3:** For an accepting state run $q \in R^p_{M}$ for some $M \in \mathbb{N}$ and some $p \in A\mathcal{P}$, consider the reachability element $\vartheta = (q, q', q'', T_h) \in \mathbb{P}^p(q)$. If there exists a CBC and a controller $\nu(\cdot)$ such that conditions (4)–(6) hold with $X_0 = L^{-1}(\sigma(q, q'))$ and $X_u = L^{-1}(\sigma(q', q''))$, then the upper bound on the probability that a solution process of $dt$-SCS starts from an initial state $a \in X_0$ under the controller $\nu(\cdot)$ and reaches $X_u$ within the finite-time horizon $[0, T_h)$ is obtained from (11) and is denoted by $\mathbf{x}_{\vartheta T_h}$.

Having the CBCs and the corresponding probabilities for all individual reachability elements, we combine them to obtain an upper bound on the probability of violation of the specification given by the accepting language of $\mathcal{A}$. Consequently, we quantify a lower bound on the probability of satisfaction together with a controller that ensures the satisfaction of the desired specification.

**Case study (continued):** We decompose $\mathcal{A}^c$ in Fig. 2 into simple reachability problems. We consider accepting state runs without self-loops with $M = 7$. Then, we get $R_M = \{(q_0, q_3), (q_0, q_1, q_3), (q_0, q_2, q_3)\}$. Consequently, we have $\mathbb{P}^p_r(q_0, q_3) = \{(q_0, q_1, q_3, 6)\}$ and $\mathbb{P}^p_r(q_0, q_2, q_3) = \{(q_0, q_2, q_3, 6)\}$. Following Remark 6.2, $\mathbf{q} = (q_0, q_3)$ admits a trivial probability that can be neglected. We need to find control barrier certificates and corresponding controllers for the remaining two reachability elements, namely, $\vartheta_1 = (q_0, q_1, q_3, 6)$ and $\vartheta_2 = (q_0, q_2, q_3, 6)$.

**VII. CONTROLLER AND PROBABILITY COMPUTATION**

**A. Controller Structure**

Ideally, one has to compute the CBC and a suitable controller for each element of $\mathbb{P}^p_M(\mathcal{A}^c)$. However, it is ambiguous when utilizing the controller in the closed loop at those states of automaton where there is more than one edge emanating from the state, i.e., the region corresponding to the atomic proposition on the edge employs two controllers simultaneously. To resolve this, we combine the two reachability problems into one by replacing $X_0$ in Lemma 6.3 with the union of regions corresponding to atomic propositions of all outgoing edges. This results in a common CBC and controller for different reachability elements. In other words, we partition $\mathbb{P}^p_M(\mathcal{A}^c)$ and combine the reachability elements with the same CBC and controller and place them in a single partition set. Consequently, we obtain a switching controller since multiple locations in the automaton $\mathcal{A}^c$ admit different controllers. This procedure has been adapted from [15] and is omitted here due to lack of space. However, we refer the interested readers to the arXiv version [20] for additional information on the controller structure and switching DFA construction.

**B. Probability Computation**

For each individual reachability element given by $\vartheta = (q, q', q'', T_h) \in \mathbb{P}^p_M(\mathcal{A}^c)$, we first compute upper bounds on reachability probabilities and then combine them to provide an upper bound on the probability that the specification represented by the language of DFA $\mathcal{A}$ is violated, which is provided by the following theorem.

**Theorem 7.1:** For a specification given by the accepting language of DFA $\mathcal{A}$, let $\mathcal{A}^c$ represent the complement of $\mathcal{A}$. For $\mathcal{A}^c$, let $R^p_M$ be the set of all accepting state runs of the length of at most $M + 1$ and $\mathbb{P}^p(q)$ be the set of state runs of length 3 augmented with the horizon $T_h$, for $p \in A\mathcal{P}$. Then, the probability that the solution processes of $dt$-SCS starting from any initial state $a \in L^{-1}(p)$ satisfy the specification represented by $\mathcal{A}^c$ under the switching controller within the time horizon $[0, M] \subseteq \mathbb{N}$ is upper bounded by

$$
\mathbb{P}^p_p \{ L(x_M) \models \mathcal{A}^c \} \leq \sum_{q \in R^p_M} \prod_{\theta \in \mathbb{P}^p(q)} \{ \nu_{\mathcal{S} T_h}(\vartheta) \models (q, q', q'', T_h) \}
$$

where $\mathbf{x}_{\vartheta T_h}$ is obtained using Lemma 6.3 and is the upper bound on the probability that solution processes of the system $\mathcal{S}$ start from $X_0 := L^{-1}(\sigma(q, q'))$ and reach $X_u := L^{-1}(\sigma(q', q''))$ within the time horizon $[0, T_h) \subseteq \mathbb{N}$.

**Remark 7.2:** If no CBC is found for a certain element $\vartheta \in \mathbb{P}^p(q)$, the corresponding probability $\mathbf{x}_{\vartheta T_h}$ for that element should be replaced by a trivial probability bound 1 in (20). To obtain a non-trivial probability of satisfaction, CBC should be found for at least one element.

**Remark 7.3:** The proposed bounds in (20) can be improved by minimizing $\eta_c$ for some fixed $\beta$, for each reachability element $\vartheta$. Since CBC of $\mathcal{S}$ is obtained compositionally via (18), these parameters depend on $\eta_c, c_i$ for some fixed $\beta_i$ for all subsystems $\mathcal{S}_i$, $i \in \{1, \ldots, N\}$. The bound is then improved by minimizing $\eta_c, c_i$ for all $i$, via the bisection method [15]. Note that (18) allows for CSBCs of some subsystems to compensate the undesirable parameters of CSBCs of other subsystems as long as condition (17) holds.

We raise the following corollary to compute the lower bound on the probability that the interconnected system $\mathcal{S}$ satisfies the desired specification represented by the DFA $\mathcal{A}$.

**Corollary 7.4:** The probability that the solution processes of $\mathcal{S}$ start from any initial state $a \in L^{-1}(p)$ and satisfy the specification given by the accepting language of DFA $\mathcal{A}$ over a finite-time horizon $[0, M] \subseteq \mathbb{N}$ is lower bounded by

$$
\mathbb{P}^p_p \{ L(x_M) \models \mathcal{A} \} \geq 1 - \sum_{q \in R^p_M} \prod_{\theta \in \mathbb{P}^p(q)} \{ \nu_{\mathcal{S} T_h}(\vartheta) \models (q, q', q'', T_h) \} 
$$

**Case study (continued):** We compute CSBCs and the corresponding local controllers for reachability elements $\vartheta_1$ and $\vartheta_2$ by utilizing SOSTOOLS [29] and semi-definite programming (SDP) solver SeDuMi [30]. Since dynamics of $\mathcal{S}$ are not polynomial and SOS algorithm is only applicable to systems with polynomial dynamics [20], we approximate our dynamics by taking an upper bound on the term $B_s(f_1, \nu, \nu_1, \nu_1, \nu_1)$ by replacing $\sin(\cdot)$ by either 1 or −1 accordingly.

The CSBC, local controller and other parameters satisfying conditions (7)–(10) for the reachable elements $\vartheta_1$ and $\vartheta_2$ are shown in Table I. For both elements, one can see that Assumption 4.3 is satisfied. Therefore, by utilizing Theorem 4.5, we compute CBC and controller for the interconnected system, and also obtain the parameters satisfying (4)–(6). Then, by Lemma 6.3, we correspondingly obtain upper bounds for reaching states corresponding to $p_0 \vee p_2$ and $p_0 \vee p_3$ from $p_1$ and $p_2$, respectively. These values are reported in Table II. The switching mechanism for controllers is obtained, as described in section VII-A. Now, by employing Theorem 7.1 and Corollary 7.4, we obtain the lower bound on the probability that the solution processes of the interconnected system $\mathcal{S}$ start from an initial state $a \in X^1$ and satisfy the specification represented by the language of DFA $\mathcal{A}$ within the time horizon $T_d = 7$ as $\mathbb{P}^p_p \{ L(x_T) \models \mathcal{A} \} \geq 0.94$. Similarly, for the solution processes of the interconnected system $\mathcal{S}$ starting from $a \in X^4$, we acquire $\mathbb{P}^p_p \{ L(x_T) \models \mathcal{A} \} \geq 0.9$. Fig. 3 shows the evolution of solution processes within the time horizon $T_d = 7$ when starting from initial
TABLE I
CSBC, CONTROLLER, AND PARAMETERS OBTAINED FOR REACHABILITY ELEMENTS $\vartheta$ FOR ALL $1 \leq I \leq N$ SUBSYSTEMS

| $I$   | $B_i(\vartheta_i)$ | $\nu_i(\vartheta_i)$ | $\eta_i$ | $\beta_i$ | $c_i$ | $\alpha_i(s)$ | $\kappa_i(s)$ | $\rho_i(s)$ | $\varphi_i(s)$ |
|------|-------------------------|------------------------|---------|----------|-------|---------------|---------------|-----------|-------------|
| 1    | $0.0001361\theta_1^2 - 0.0001877\theta_1^3 + 0.0001361\theta_1^4$ | $0.02$ | $1.2$ | $0.0083$ | $4.7 \times 10^{-7}$ | $0.997s$ | $4.49 \times 10^{-7}$ s |
| 2    | $0.0004904\theta_2^2 - 0.03395\theta_2^3 + 0.00107\theta_2^4 - 3.205\theta_2 + 1.827$ | $0.017$ | $1$ | $0.0162$ | $4.5 \times 10^{-8}$ | $0.998s$ | $4.49 \times 10^{-8}$ s |

TABLE II
CBC, CONTROLLER, AND PROBABILISTIC GUARANTEES OBTAINED FOR REACHABILITY ELEMENTS $\vartheta$ FOR THE INTERCONNECTED SYSTEM

| $I$   | $B(\vartheta)$ | $\nu_i(\vartheta)$ | $\eta$ | $\beta$ | $c$ | $\kappa(s)$ | $\rho\gamma_{\infty}$ |
|------|----------------|-----------------|-------|--------|---|-----------|------------------|
| 1    | $0.0001361\theta_1^2 - 0.0001877\theta_1^3 + 0.0001361\theta_1^4$ | $0.02$ | $1.2$ | $0.0083$ | $4.7 \times 10^{-7}$ | $0.997s$ | $4.49 \times 10^{-7}$ s |
| 2    | $0.0004904\theta_2^2 - 0.03395\theta_2^3 + 0.00107\theta_2^4 - 3.205\theta_2 + 1.827$ | $0.017$ | $1$ | $0.0162$ | $4.5 \times 10^{-8}$ | $0.998s$ | $4.49 \times 10^{-8}$ s |

Hence $B(x)$ is a CBC for the interconnected system $\mathcal{S}$, which completes the proof.

APPENDIX

Proof: (Theorem 3.4) According to the condition (5), $X_u \subseteq \{x \in X \mid B(x) \geq \beta\}$. Then, we have $P^\eta_k\{x(k) \in X_u \text{ for } 0 \leq k < T_d \mid a\} \leq P^\eta_{\sup_{0 \leq k < T_d}}B(x(k)) \geq \beta \mid a\}$. The proposed bounds in (11) follows directly by applying [31, Th. 3, Ch. III] due to the inequality $\kappa(s) \leq \kappa, \forall s \in \mathbb{R}_{\geq 0}$ and employing respectively conditions (6) and (4).

Proof: (Theorem 4.5) We first show that conditions (4) and (5) in Definition 3.1 hold. For any $x : [x_1; \ldots; x_N] \in X_0 = \prod_{i=1}^N X_0$, and from (8), we have $B(x) = \max\{g_i^{-1}(B_i(\vartheta_i))\} \leq \max\{g_i^{-1}(\eta_i)\} = \eta$, and similarly for any $x : [x_1; \ldots; x_N] \in \prod_{i=1}^N X_0$, and from (9), one has $B(x) = \max\{g_i^{-1}(B_i(\vartheta_i))\} \geq \max\{g_i^{-1}(\vartheta_i)\} = \beta$, satisfying conditions (4) and (5) with $\eta = \max\{g_i^{-1}(\eta_i)\}$ and $\beta = \max\{g_i^{-1}(\vartheta_i)\}$. Now, we show that the condition (6) holds, as well. Let $\kappa(s) = \max_j\{g_i^{-1} \circ \kappa_j \circ g_j(s)\}$. It follows from (16) that $\kappa < T_d$. Moreover, $\beta > \eta$ according to (17). Since $\max\{g_i^{-1}\}$ is concave, one can readily acquire the chain of inequalities in (21) using Jensen’s inequality, and by defining the constant $c := \max\{g_i^{-1}(c_i)\}$.
REFERENCES

[1] P. Tabuada, *Verification and Control of Hybrid Systems*. Berlin, Germany: Springer, 2009.

[2] A. Abate, M. Prandini, J. Lygeros, and S. Sastry, “Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems,” *Automatica*, vol. 44, no. 11, pp. 2724–2734, 2008.

[3] E. M. Hahn, G. Norman, D. Parker, B. Wachter, and L. Zhang, “Game-based abstraction and controller synthesis for probabilistic hybrid systems,” in *Proc. 8th Int. Conf. Quantitative Eval. Syst.*, 2011, pp. 69–78.

[4] M. Lahijanian, S. B. Andersson, and C. Belta, “Formal verification and synthesis for discrete-time stochastic systems,” *IEEE Trans. Autom. Control*, vol. 60, no. 8, pp. 2031–2045, Aug. 2015.

[5] S. Soudjani and A. Abate, “Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes,” *SIAM J. Appl. Dynamical Syst.*, vol. 12, no. 2, pp. 921–956, 2013.

[6] M. Zamani, I. Tkachev, and A. Abate, “Towards scalable synthesis of stochastic control systems,” *Discrete Event Dynamic Syst.*, vol. 27, no. 2, pp. 341–369, 2017.

[7] A. Lavaei, “Automated verification and control of large-scale stochastic cyber-physical systems: Compositional techniques,” Ph.D. dissertation, Dept. Electrical Engineering, Technische Universität München, Munich, Germany, 2019.

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

[9] R. Wisniewski and M. L. Bujorianu, “Stochastic safety analysis of stochastic hybrid systems,” in *Proc. 57th IEEE Conf. Decis. Control*, 2018, pp. 2390–2395.

[10] J. Steinhardt and R. Tedrake, “Finite-time regional verification of stochastic non-linear systems,” *Int. J. Robot. Res.*, vol. 31, no. 7, pp. 901–923, 2012.

[11] C. Santoyo, M. Dutreix, and S. Coogan, “Verification and control for finite-time safety of stochastic systems via barrier functions,” in *Proc. IEEE Conf. Control Technol. Appl.*, 2019, pp. 712–717.

[12] 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.

[13] L. Lindemann and D. V. Dimarogonas, “Control barrier functions for signal temporal logic tasks,” *IEEE Control Syst. Lett.*, vol. 3, no. 1, pp. 96–101, Jan. 2019.

[14] M. Ahmadi, A. Singletary, J. W. Burdick, and A. D. Ames, “Barrier functions for multiagent-pomdps with DTL specifications,” in *Proc. 59th IEEE Conf. Decis. Control*, 2020, pp. 1380–1385.

[15] 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.

[16] Z. Lyu, X. Xu, and Y. Hong, “Small-gain theorem for safety verification of interconnected systems,” *Automatica*, vol. 139, 2022, Art. no. 110178.

[17] P. Jagtap, A. Swikir, and M. Zamani, “Compositional construction of control barrier functions for interconnected control systems,” in *Proc. 23rd Int. Conf. Hybrid Systems: Computation Control*, 2020, pp. 1–11.

[18] M. Anand, A. Lavaei, and M. Zamani, “Compositional construction of control barrier certificates for large-scale interconnected stochastic systems,” in *Proc. 21st IFAC World Conf.*, 2020, pp. 1862–1867.

[19] A. Nejati, S. Soudjani, and M. Zamani, “Compositional construction of control barrier functions for continuous-time stochastic hybrid systems,” *Automatica*, 2022, arXiv:2012.07296v2.

[20] M. Anand, A. Lavaei, and M. Zamani, “From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems,” 2022, arXiv:2101.06916v2.

[21] N. Jahanshahi, P. Jagtap, and M. Zamani, “Synthesis of partially observed jump-diffusion systems via control barrier functions,” *IEEE Control Syst. Lett.*, vol. 5, no. 1, pp. 253–258, Jan. 2021.

[22] P. Skardal and A. Arenas, “Control of coupled oscillator networks with application to microgrid technologies,” *Sci. Adv.*, vol. 1, no. 7, 2015, Art. no. e1500339.

[23] B. S. Rüffer, “Monotone inequalities, dynamical systems, and paths in the positive orthant of euclidean n-space,” *Positivity*, vol. 14, no. 2, pp. 257–283, 2010.

[24] S. N. Dashkovskiy, B. S. Rüffer, and F. R. Wirth, “Small gain theorems for large scale systems and construction of ISS Lyapunov functions,” *SIAM J. Control Optim.*, vol. 48, no. 6, pp. 4089–4118, 2010.

[25] D. Chandler and J. Percus, “Introduction to modern statistical mechanics,” *Phys. Today*, vol. 41, 1988.

[26] G. Di Giacomo and M. Y. Vardi, “Synthesis for LTL and LDL on finite traces,” in *Proc. 24th Int. Conf. Artif. Intell.*, 2015, pp. 1558–1564.

[27] A. Duret-Lutz, A. Lewkozwicz, A. Fauchille, T. Michaud, E. Renault, and L. Xu, “Spot 2.0—A framework for LTL and ω-automata manipulation,” in *Proc. 14th Int. Symp. Automated Technol. Verification Anal.*, 2016, pp. 122–129.

[28] G. De Giacomo and M. Y. Vardi, “Synthesis for LTL and LDL on finite traces,” in *Proc. 24th Int. Conf. Artif. Intell.*, 2015, pp. 1558–1564.

[29] S. Prajna, A. Papachristodoulou, and P. Parrilo, “Introducing SOSTOOLS: A general purpose sum of squares programming solver,” in *Proc. 41st IEEE Conf. Decis. Control*, 2002, vol. 1, pp. 741–746.

[30] J. F. Sturm, “Using sedumi 1.02, A MATLAB toolbox for optimization over symmetric cones,” *Optim. Methods Softw.*, vol. 11, no. 1–4, pp. 625–653, 1999.

[31] H. J. Kushner, *Stochastic Stability and Control*. Mathematics in Science and Engineering. Amsterdam, The Netherlands: Elsevier Science, 1967.