Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Compositional Construction of Control Barrier Certificates for Large-Scale Interconnected Stochastic Systems ⋆

Mahathi Anand[1] *, **Abolfazl Lavaei**[1] *, **Majid Zamani** *,**

* *Department of Computer Science, Ludwig Maximilian University of Munich, Germany (e-mails: mahathi.anand@sosy.ifi.lmu.de, lavaei@lmu.de)*
** *Department of Computer Science, University of Colorado Boulder, USA (e-mail: majid.zamani@colorado.edu)*

[1] Both authors have contributed equally.

Abstract: This paper proposes a compositional approach for constructing control barrier certificates of large-scale interconnected discrete-time stochastic control systems. The proposed compositional methodology is based on a notion of *control sub-barrier certificates* enabling one to construct control barrier certificates of interconnected systems by leveraging some small-gain type conditions. The main goal is to synthesize control policies satisfying safety properties for interconnected systems utilizing those control sub-barrier certificates of subsystems while providing upper bounds on the probability that interconnected systems reach unsafe regions in finite-time horizons. A sum-of-squares optimization problem is formulated for searching control sub-barrier certificates and corresponding local control policies satisfying safety specifications. The proposed compositional approaches are illustrated on a temperature regulation in a circular building containing 1000 rooms by compositionally synthesizing safety controllers to maintain the temperature of each room in a comfort zone in a bounded-time horizon.

Keywords: Control Barrier Certificates, Large-Scale Interconnected Stochastic Systems, Small-Gain Conditions, Compositionality, Formal Controller Synthesis.

1. INTRODUCTION

Formal verification and synthesis of large-scale stochastic systems against complex logic properties, *e.g.,* those expressed as linear temporal logic (LTL) formulae, have attracted significant attentions in the past few years as a challenging problem (Tabuada, 2009). In particular, not only underlying stochastic dynamics are complex due to their continuous-state sets with high dimensions, but properties of interests are also complicated. Hence, providing formal controller synthesis for such complex systems satisfying high-level specifications is inherently a crucial task.

To deal with analyzing large-scale stochastic systems with continuous-state sets, existing results in the literature have been reliant on utilizing *finite abstractions*. In this regard, probabilistic reachability and safety for discrete-time stochastic hybrid systems are proposed by (Abate et al., 2008). An abstraction framework for formal verification and synthesis of discrete-time stochastic systems is provided by (Lahijanian et al., 2015). Although finite abstraction-based techniques depend on the state set discretization and suffer severely from the state-explosion problem, this issue has been partly mitigated by (Soudjani and Abate, 2013) by utilizing adaptive sequential gridding algorithms and by (Zamani et al., 2017) by proposing an input-set abstraction for incrementally stable stochastic control systems. Another potential solution, proposed in the past few years, for alleviating the computational complexity arising in the analysis of large-scale stochastic systems is to employ compositional techniques for constructing finite abstractions of interconnected systems via abstractions of smaller subsystems (Lavaei et al., 2018; Lavaei and Zamani, 2019a; Lavaei et al., 2019b; Lavaei and Zamani, 2019b; Lavaei et al., 2019a, 2020; Lavaei et al., 2020; Lavaei et al., 2020; Lavaei et al., 2019; Lavaei, 2019; Nejati and Zamani, 2020; Nejati et al., 2020).

More recently, research attentions on verification and synthesis of complex systems have been directed towards *discretization-free* approaches using *control barrier certificates*. In this regard, existing results include safety verifications of continuous-time stochastic hybrid systems (Prajna et al., 2007; Huang et al., 2017; Wisniewski and Bujorianu, 2018). A verification approach for Markov decision processes using barrier certificates is proposed by (Ahmadi et al., 2018). Verification and control for finite-time safety of stochastic systems using barrier functions are discussed by (Santoyo et al., 2019a,b). Recently, verification and synthesis of discrete-time stochastic control systems against logic properties in finite-time horizons via control barrier certificates are presented by (Jagtap et al., 2018), and (Jagtap et al., 2020), respectively.

⋆ This work was supported in part by the H2020 ERC Starting Grant AutoCPS (grant agreement No. 804639) and the German Research Foundation (DFG) through the Research Training Group 2428.

The proposed techniques in the aforementioned literatures involve restricting the type of control barrier certificates to polynomials and searching for corresponding coefficients under some mild assumptions. However, there is no guarantee on the existence of such control barrier certificates. Although small-scale dynamical systems usually admit polynomial barriers of lower orders, the search may be very difficult (if not impossible) in the case of dealing with large-scale interconnected systems. These challenges motivated us to propose a compositional framework for the construction of control barrier certificates for large-scale interconnected stochastic systems.

To do so, we first decompose underlying large-scale stochastic systems into different subsystems of lower dimensions, and search for control sub-barrier certificates of those subsystems together with corresponding local control policies with respect to safety specifications. We then derive sufficient small-gain type conditions to construct control barrier certificate of interconnected systems based on control sub-barrier certificates of subsystems. We utilize the constructed control barrier certificates to provide upper bounds on the probability that interconnected systems reach unsafe regions in finite-time horizons.

To the best of our knowledge, this work is the first to propose compositional construction of control barrier certificates for verification and synthesis of large-scale interconnected *discrete-time stochastic systems*. We provide a systematic approach based on a sum-of-squares optimization problem to search for control sub-barrier certificates and synthesize local control policies for subsystems. We demonstrate the effectiveness of our proposed results by applying them to a temperature regulation in a circular building containing 1000 rooms. We compositionally synthesize safety controllers regulating the temperature of each room in a comfort zone for a bounded-time horizon. Proofs of all statements are omitted in this work due to space limitations.

2. DISCRETE-TIME STOCHASTIC CONTROL SYSTEMS

2.1 Preliminaries

This work considers the probability space $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$, where Ω is the sample space, $\mathcal{F}_\Omega$ is a sigma-algebra on Ω comprising subsets of Ω as events, $\mathbb{P}_\Omega$ is the probability measure that assigns probabilities to those events. The topological space S is a Borel space if it is homeomorphic to a Borel subset of a Polish space, *i.e.*, a separable and completely metrizable space. A Borel sigma-algebra is denoted by $\mathcal{B}(S)$, and can be generated from any Borel space S. The map $f : S \to Y$ is measurable whenever it is Borel measurable.

2.2 Notations

We denote the set of real, positive and non-negative real numbers by $\mathbb{R}, \mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$, respectively. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $x = [x_1; ...; x_N]$ denotes the corresponding vector of dimension $\sum_i n_i$. Given a vector $x \in \mathbb{R}^n$, $\|x\|$ denotes the infinity norm of x. Symbol $\mathbb{I}_n$ denotes the identity matrix in $\mathbb{R}^{n\times n}$. The identity function and composition of functions are denoted by $\mathcal{I}_d$ 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 $(\prod_{i=1}^N f_i)(x_1, \ldots, x_N) = [f_1(x_1); \ldots; f_N(x_N)]$. A function $\varphi : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be a class $\mathcal{K}$ function if it is continuous, strictly increasing, and $\varphi(0) = 0$. A class $\mathcal{K}$ function $\varphi(\cdot)$ belongs to class $\mathcal{K}_\infty$ if $\varphi(s) \to \infty$ as $s \to \infty$.

2.3 Discrete-Time Stochastic Control Systems

In this paper, we focus on discrete-time stochastic control systems (dt-SCS) as presented in the next definition.

Definition 1. A *discrete-time stochastic control system* (dt-SCS) is a tuple

$$\mathfrak{S} = (X, U, W, \varsigma, f, Y, h), \tag{1}$$

where

- $X \subseteq \mathbb{R}^n$ is a Borel space as the state space of the system;
- $U \subseteq \mathbb{R}^m$ is a Borel space as the *external* input space of the system;
- $W \subseteq \mathbb{R}^p$ is a Borel space as the *internal* input space of the system;
- ς is a sequence of independent and identically distributed (i.i.d.) random variables from a sample space Ω to the set $\mathcal{V}_\varsigma$, namely $\varsigma := \{\varsigma(k) : \Omega \to \mathcal{V}_\varsigma,\ k \in \mathbb{N}\}$;
- $f : X \times U \times W \times \mathcal{V}_\varsigma \to X$ is a measurable function characterizing the state evolution of $\mathfrak{S}$;
- $Y \subseteq \mathbb{R}^q$ is a Borel space as the output space of the system;
- $h : X \to Y$ is a measurable function that maps a state $x \in X$ to its output $y = h(x)$.

The evolution of the state of dt-SCS $\mathfrak{S}$ for a given initial state $x(0) \in X$, and external and internal input sequences $\{\nu(k) : \Omega \to U,\ k \in \mathbb{N}\}$ and $\{w(k) : \Omega \to W,\ k \in \mathbb{N}\}$ is described as:

$$\mathfrak{S} : \begin{cases} x(k+1) = f(x(k), \nu(k), w(k), \varsigma(k)), \\ y(k) = h(x(k)), \end{cases} \quad k \in \mathbb{N}. \tag{2}$$

We respectively associate to U and W the sets $\mathcal{U}$ and $\mathcal{W}$ to be collections of sequences $\{\nu(k) : \Omega \to U,\ k \in \mathbb{N}\}$ and $\{w(k) : \Omega \to W,\ k \in \mathbb{N}\}$, in which $\nu(k)$ and $w(k)$ are independent of $\varsigma(t)$ for any $k, t \in \mathbb{N}$ and $t \geq k$. The random sequences $x_{a\nu w} : \Omega \times \mathbb{N} \to X$, and $y_{a\nu w} : \Omega \times \mathbb{N} \to Y$ satisfying (2) for any initial state $a \in X$, $\nu(\cdot) \in \mathcal{U}$, and $w(\cdot) \in \mathcal{W}$ are called respectively the *solution process* and *output trajectory* of $\mathfrak{S}$ under an external input ν, an internal input w, and an initial state a.

We present Markov policies, as defined next, to control the dt-SCS in (1).

Definition 2. For the dt-SCS $\mathfrak{S}$ in (1), a Markov policy is a sequence $\varpi = (\varpi_0, \varpi_1, \varpi_2, \ldots)$ of universally measurable stochastic kernels ϖ_n (Bertsekas and Shreve, 1996), each defined on the input space U given X and such that for all $x_n \in X$, $\varpi_n(U \mid x_n) = 1$. The class of all such Markov policies is denoted by $\Pi_{\mathcal{M}}$.

This paper deals with the controller synthesis for interconnected dt-SCS without internal inputs that can be constructed as a composition of several dt-SCSs with both

internal and external inputs. Such an interconnected dt-SCS can be represented by $\mathfrak{S} = (X, U, \varsigma, f)$ with $f : X \times U \times \mathcal{V}_\varsigma \to X$, and consequently dt-SCS in (2) reduces to

$$\mathfrak{S} : x(k+1) = f(x(k), \nu(k), \varsigma(k)), \quad k \in \mathbb{N}. \tag{3}$$

Note that although we define dt-SCS in (2) with outputs, we assume the full-state information is available for interconnected systems (*i.e.,* its output map is identity). In particular, the role of outputs in (2) is mainly for the sake of interconnecting systems as will be explained in detail in Section 4.

In the next section, in order to quantify upper bounds on the probability that the interconnected system in (3) reaches a certain unsafe region in a finite-time horizon, we introduce notations of control sub-barrier certificates (CSBC) and control barrier certificates (CBC) for respectively dt-SCS (with both internal and external signals) and interconnected dt-SCS (without internal signals).

3. CONTROL (SUB-)BARRIER CERTIFICATES

Definition 3. Consider a dt-SCS $\mathfrak{S} = (X, U, W, \varsigma, f, Y, h)$, and sets $X_0, X_u \subseteq X$ as initial and unsafe sets of the system, respectively. A function $\mathbb{B} : X \to \mathbb{R}_{\geq 0}$ is said to be a control sub-barrier certificate (CSBC) for $\mathfrak{S}$ 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 $\beta \in \mathbb{R}_{>0}$, such that

$$\mathbb{B}(x) \geq \alpha(\|h(x)\|), \qquad \forall x \in X, \tag{4}$$
$$\mathbb{B}(x) \leq \eta, \qquad \forall x \in X_0, \tag{5}$$
$$\mathbb{B}(x) \geq \beta, \qquad \forall x \in X_u, \tag{6}$$

and $\forall x \in X$, $\exists \nu \in U$, $\forall w \in W$, one has

$$\mathbb{E}\Big[\mathbb{B}(x(k+1)) \mid x(k), \nu(k), w(k)\Big] \leq \max\Big\{\kappa(\mathbb{B}(x(k))), \rho(\|w(k)\|), c\Big\}. \tag{7}$$

Now we provide a similar definition but for interconnected dt-SCS without internal inputs which is utilized later for providing probabilistic guarantees on the satisfaction of safety specifications over interconnected systems.

Definition 4. Consider an interconnected dt-SCS $\mathfrak{S} = (X, U, \varsigma, f)$ without internal inputs, and sets $X_0, X_u \subseteq X$ as respectively initial and unsafe sets of the interconnected system. A function $\mathbb{B} : X \to \mathbb{R}_{\geq 0}$ is called a control barrier certificate (CBC) for $\mathfrak{S}$ if

$$\mathbb{B}(x) \leq \eta, \qquad \forall x \in X_0, \tag{8}$$
$$\mathbb{B}(x) \geq \beta, \qquad \forall x \in X_u, \tag{9}$$

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

$$\mathbb{E}\Big[\mathbb{B}(x(k+1)) \mid x(k), \nu(k)\Big] \leq \max\Big\{\kappa(\mathbb{B}(x(k))), c\Big\}, \tag{10}$$

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

Remark 5. Note that we require the condition $\beta > \eta$ in Definition 4 in order to propose meaningful probabilistic bounds using Theorem 6. However, we do not have such a condition in Definition 3 for dt-SCS with internal inputs.

Now we employ Definition 4 and propose an upper bound on the probability that the interconnected system in (3) reaches an unsafe region via the next theorem.

Theorem 6. Let $\mathfrak{S} = (X, U, \varsigma, f)$ be an interconnected dt-SCS without internal inputs. Suppose $\mathbb{B}$ is a CBC for $\mathfrak{S}$ and there exists a constant $0 < \hat{\kappa} < 1$ such that the function $\kappa \in \mathcal{K}_\infty$ in (10) satisfies $\kappa(s) \geq \hat{\kappa} s$, $\forall s \in \mathbb{R}_{\geq 0}$. Then the probability that the solution process of $\mathfrak{S}$ starts from any initial state $a \in X_0$ and reaches X_u under the policy $\nu(\cdot)$ (associated with the CBC $\mathbb{B}$) within the time step $k \in [0, T_d]$ is

$$\mathbb{P}^a_\nu\Big\{\sup_{0 \leq k \leq T_d} \mathbb{B}(x(k)) \geq \beta \mid a\Big\} \leq \delta \tag{11}$$

with

$$\delta = \begin{cases} 1-(1-\frac{\eta}{\beta})(1-\frac{c}{\beta})^{T_d}, & \text{if } \beta \geq \frac{c}{\hat{\kappa}}, \\ (\frac{\eta}{\beta})(1-\hat{\kappa})^{T_d} + (\frac{c}{\hat{\kappa}\beta})(1-(1-\hat{\kappa})^{T_d}), & \text{if } \beta < \frac{c}{\hat{\kappa}}. \end{cases}$$

The proposed results in Theorem 6 provide upper bounds on the probability that interconnected systems reach unsafe regions in *finite-time* horizons. We can generalize the proposed results to *infinite-time* horizon provided that the constant $c \equiv 0$ as in the following corollary.

Corollary 7. Let $\mathfrak{S} = (X, U, \varsigma, f)$ be an interconnected dt-SCS without internal inputs. Suppose $\mathbb{B}$ is a CBC for $\mathfrak{S}$ such that the constant $c \equiv 0$ in (10). Then the probability that the solution process of $\mathfrak{S}$ starts from any initial state $a \in X_0$ and reaches X_u under the policy $\nu(\cdot)$ (associated with the CBC $\mathbb{B}$) within the time step $k \in [0, \infty)$ is

$$\mathbb{P}^a_\nu\Big\{\sup_{0 \leq k < \infty} \mathbb{B}(x(k)) \geq \beta \mid a\Big\} \leq \frac{\eta}{\beta}.$$

The proposed results in Theorem 6 simply provide a lower bound on the probability that the interconnected system satisfies the safety property as

$$\mathbb{P}^a_\nu\Big\{x(k) \notin X_u \text{ for } 0 \leq k \leq T_d \mid a\Big\} \geq 1 - \delta.$$

In the next section, we study networks of stochastic control subsystems and propose compositional conditions under which a CBC of an interconnected system can be constructed via CSBC of subsystems.

4. COMPOSITIONAL CONSTRUCTION OF CBC

4.1 Interconnected Stochastic Control Systems

Suppose we are given control subsystems

$$\mathfrak{S}_i = (X_i, U_i, W_i, \varsigma_i, f_i, Y_i, h_i), \quad i \in \{1, \ldots, N\}, \tag{12}$$

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

$$w_i = [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}], \quad y_i = [y_{i1}; \ldots; y_{iN}], \tag{13}$$

and their output spaces and functions are of the form

$$Y_i = \prod_{j=1}^{N} Y_{ij}, \quad h_i(x_i) = [h_{i1}(x_i); \ldots; h_{iN}(x_i)]. \tag{14}$$

The outputs $y_{ii} = x_i$ are interpreted as *external* ones, whereas the outputs y_{ij} with $i \neq j$ are *internal* ones which are employed to interconnect these stochastic control subsystems. If there exists a connection from $\mathfrak{S}_j$ to $\mathfrak{S}_i$, we assume that w_{ij} is equal to y_{ji}. Otherwise, we put the connecting output function identically zero, *i.e.,* $h_{ji} \equiv 0$.

Now we define the interconnected stochastic control systems.

Definition 8. Consider $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems $\mathfrak{S}_i = (X_i, U_i, W_i, \varsigma_i, f_i, Y_i, h_i)$, $i \in \{1, \ldots, N\}$, with the input-output configuration as in (13) and (14). The interconnection of $\mathfrak{S}_i$, $\forall i \in \{1, \ldots, N\}$, is the interconnected stochastic control system $\mathfrak{S} = (X, U, \varsigma, f)$, denoted by $\mathcal{I}(\mathfrak{S}_1, \ldots, \mathfrak{S}_N)$, such that $X := \prod_{i=1}^{N} X_i$, (with $X_0 := \prod_{i=1}^{N} X_{0_i}$, $X_u := \prod_{i=1}^{N} X_{u_i}$), $U := \prod_{i=1}^{N} U_i$ and $f := \prod_{i=1}^{N} f_i$ subjected to the following constraint:

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

4.2 Compositional CBC for Interconnected Systems

In this subsection, we provide a compositional framework for the construction of CBC for $\mathfrak{S}$ using CSBC of $\mathfrak{S}_i$. Suppose for control subsystems $\mathfrak{S}_i, i \in \{1, \ldots, N\}$, in (12), there exist CSBC $\mathbb{B}_i$ as defined in Definition 3 with functions $\alpha_i, \kappa_i \in \mathcal{K}_\infty$, with $\kappa_i < \mathcal{I}_d$, $\rho_i \in \mathcal{K}_\infty \cup \{0\}$, and constants $\eta_i, c_i \in \mathbb{R}_{\geq 0}$ and $\beta_i \in \mathbb{R}_{>0}$. Now we raise the following small-gain assumption that is essential for the compositional construction of CBC for $\mathfrak{S}$.

Assumption 9. Assume that $\mathcal{K}_\infty$ functions κ_{ij} defined as

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

satisfy

$$\kappa_{i_1 i_2} \circ \kappa_{i_2 i_3} \circ \ldots \circ \kappa_{i_{r-1} i_r} \circ \kappa_{i_r i_1} < \mathcal{I}_d \tag{15}$$

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 $\mathcal{K}_\infty$ functions $\sigma_i > 0$ (Rüffer, 2010, Theorem 5.5), satisfying

$$\max_{i,j} \left\{ \sigma_i^{-1} \circ \kappa_{ij} \circ \sigma_j \right\} < \mathcal{I}_d, \quad i, j = \{1, \ldots, N\}. \tag{16}$$

Remark 10. Note that the small-gain condition (15) is a standard one in investigating the stability of large-scale interconnected systems via ISS Lyapunov functions (Dashkovskiy et al., 2007, 2010). This condition is automatically satisfied if each κ_{ij} is less than identity (*i.e.,* $\kappa_{ij} < \mathcal{I}_d, \forall i, j \in \{1, \ldots, N\}$).

In the next theorem, we show that if Assumption 9 holds and $\max_i \sigma_i^{-1}$ is concave (in order to employ Jensen's inequality), then we can construct a CBC of $\mathfrak{S}$ using CSBC of $\mathfrak{S}_i$.

Theorem 11. Consider the interconnected dt-SCS $\mathfrak{S} = \mathcal{I}(\mathfrak{S}_1, \ldots, \mathfrak{S}_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems $\mathfrak{S}_i$. Suppose that each $\mathfrak{S}_i$ admits a CSBC $\mathbb{B}_i$ as defined in Definition 3. If Assumption 9 holds and

$$\max_i \left\{ \sigma_i^{-1}(\beta_i) \right\} > \max_i \left\{ \sigma_i^{-1}(\eta_i) \right\}, \tag{17}$$

then the function $\mathbb{B}(x)$ defined as

$$\mathbb{B}(x) := \max_i \left\{ \sigma_i^{-1}(\mathbb{B}_i(x_i)) \right\}, \tag{18}$$

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

Remark 12. Note that the condition (17) in general is not very restrictive since functions σ_i in (16) play an important role in rescaling CSBC for subsystems while normalizing the effect of internal gains of other subsystems (cf. (Dashkovskiy et al., 2010) for a similar argument but in the context of stability analysis via ISS Lyapunov functions). Then one can expect that the condition (17) holds in many applications due to this rescaling.

5. COMPUTATION OF CSBC AND CONTROL POLICY

In this section, we provide a systematic approach to search for CSBC and the corresponding control policies for subsystems $\mathfrak{S}_i$. The proposed approach is based on the sum-of-squares (SOS) optimization problem using which one can reformulate conditions (4)-(7) as an SOS optimization problem (Parrilo, 2003), where CSBC is restricted to be non-negative which can be written as a sum of squares of different polynomials. To do so, we need to raise the following assumption.

Assumption 13. The stochastic control subsystem $\mathfrak{S}_i$ has a continuous-state set $X_i \subseteq \mathbb{R}^{n_i}$, and continuous external and internal input sets $U_i \subseteq \mathbb{R}^{m_i}$ and $W_i \subseteq \mathbb{R}^{p_i}$. Its vector field $f_i : X_i \times U_i \times W_i \times \mathcal{V}_{\varsigma_i} \to X_i$ is a polynomial function of the state x_i, the external input ν_i and the internal input w_i.

Under Assumption 13, one can reformulate conditions (4)-(7) as an SOS optimization problem to search for a polynomial CSBC $\mathbb{B}_i$ and a polynomial control policy $\nu_i(\cdot)$. The following lemma provides the SOS formulation.

Lemma 14. Suppose Assumption 13 holds and sets X_{0_i}, X_{u_i}, X_i can be defined by vectors of polynomial inequalities $X_{0_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{0_i}(x_i) \geq 0\}$, $X_{u_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{u_i}(x_i) \geq 0\}$ and $X_i = \{x_i \in \mathbb{R}^{n_i} \mid g_i(x_i) \geq 0\}$, where the inequalities are presented element-wise. Similarly, let the internal input set W_i be defined by vectors of a polynomial inequality $W_i = \{w_i \in \mathbb{R}^{p_i} \mid g_{w_i}(w_i) \geq 0\}$. Suppose for a given control subsystem $\mathfrak{S}_i$, there exists a sum-of-squares polynomial $\mathbb{B}_i(x_i)$, constants $\eta_i, \bar{c}_i \in \mathbb{R}_{\geq 0}$, $\beta_i \in \mathbb{R}_{>0}$, functions $\bar{\rho}_i \in \mathcal{K}_\infty \cup \{0\}$, $\alpha_i, \bar{\kappa}_i \in \mathcal{K}_\infty$, with $\bar{\kappa}_i < \mathcal{I}_d$, vectors of sum-of-squares polynomials $\lambda_{0_i}(x_i), \lambda_{u_i}(x_i), \lambda_i(x_i)$, $\hat{\lambda}_i(x_i)$, $\lambda_{w_i}(w_i)$ and polynomials $\lambda_{\nu_{ji}}(x_i)$ corresponding to the j^{th} input in $\nu_i = (\nu_{1_i}, \nu_{2_i}, ..., \nu_{m_i}) \in U_i \subseteq \mathbb{R}^{m_i}$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:

$$\mathbb{B}_i(x_i) - \lambda_i^T(x_i) g_i(x_i) - \alpha_i(\|h_i(x_i)\|) \tag{19}$$

$$-\mathbb{B}_i(x_i) - \lambda_{0_i}^T(x_i) g_{0_i}(x_i) + \eta_i \tag{20}$$

$$\mathbb{B}_i(x_i) - \lambda_{u_i}^T(x_i) g_{u_i}(x_i) - \beta_i \tag{21}$$

$$-\mathbb{E}\Big[\mathbb{B}_i(f_i(x_i, \nu_i, w_i, \varsigma_i)) \mid x_i, \nu_i, w_i\Big] + \bar{\kappa}_i(\mathbb{B}_i(x_i)) + \bar{\rho}_i(\|w_i\|) + \bar{c}_i - \sum_{j=1}^{m_i} (\nu_{ji} - \lambda_{\nu_{ji}}(x_i)) - \hat{\lambda}_i^T(x_i) g_i(x_i) - \lambda_{w_i}^T(w_i) g_{w_i}(w_i). \tag{22}$$

Then $\mathbb{B}_i(x)$ is a CSBC satisfying conditions (4)-(7) and $\nu_i = [\lambda_{\nu_{1i}}(x_i); \ldots; \lambda_{\nu_{m_i}}(x_i)]$, $i \in \{1, \ldots, N\}$, is the corresponding controller of the subsystem $\mathfrak{S}_i$, where

$$\kappa_i = \mathcal{I}_d - (\mathcal{I}_d - \pi_i) \circ (\mathcal{I}_d - \bar{\kappa}_i),$$
$$\rho_i = (\mathcal{I}_d + \bar{\delta}_i) \circ (\mathcal{I}_d - \bar{\kappa}_i)^{-1} \circ \pi_i^{-1} \circ \bar{\pi}_i \circ \bar{\rho}_i,$$
$$c_i = (\mathcal{I}_d + \bar{\delta}_i^{-1}) \circ (\mathcal{I}_d - \bar{\kappa}_i)^{-1} \circ \pi_i^{-1} \circ \bar{\pi}_i \circ (\bar{\pi}_i - \mathcal{I}_d)^{-1}(\bar{c}_i),$$

with $\bar{\delta}_i, \pi_i, \bar{\pi}_i$ being some arbitrarily chosen $\mathcal{K}_\infty$ functions so that $\mathcal{I}_d - \pi_i \in \mathcal{K}_\infty$, $\bar{\pi}_i - \mathcal{I}_d \in \mathcal{K}_\infty$.

6. ROOM TEMPERATURE NETWORK

We illustrate the effectiveness of the proposed results by applying them to a room temperature network in a circular building containing 1000 rooms. The model of this case study is borrowed from (Meyer et al., 2018) by including the stochasticity in the model as an additive noise. The evolution of the temperature $T(\cdot)$ in the interconnected system is governed by the following dynamics

$$\mathfrak{S}: \quad T(k+1) = AT(k) + \mu T_h \nu(k) + \gamma T_E + 0.6\varsigma(k),$$

where $A \in \mathbb{R}^{n\times n}$ is a matrix with diagonal elements of $\bar{a}_{ii} = (1 - 2\theta - \gamma - \mu\nu_i(k))$, off-diagonal elements $\bar{a}_{i,i+1} = \bar{a}_{i+1,i} = \bar{a}_{1,n} = \bar{a}_{n,1} = \theta$, $i \in \{1,\dots,n-1\}$, and all other elements are identically zero. Parameters $\theta = 0.45$, $\gamma = 0.045$, and $\mu = 0.09$ are conduction factors, respectively, between the rooms $i \pm 1$ and i, the external environment and the room i, and the heater and the room i. Outside temperatures are the same for all rooms: $T_{ei} = -1\,°\mathsf{C}$, $\forall i \in \{1,\dots,n\}$, and the heater temperature is $T_h = 50\,°\mathsf{C}$. Moreover, $T(k) = [T_1(k);\dots;T_n(k)]$, $\varsigma = [\varsigma_1(k);\dots;\varsigma_n(k)]$, $\nu(k) = [\nu_1(k);\dots;\nu_n(k)]$, and $T_E = [T_{e_1};\dots;T_{e_n}]$.

Now by considering the individual rooms as $\mathfrak{S}_i$ represented by

$$\mathfrak{S}_i: \begin{cases} T_i(k+1) = \bar{a}T_i(k) + \mu T_h \nu_i(k) + \theta w_i(k) + \gamma T_{ei}(k) \\ \qquad\qquad + 0.6\varsigma_i(k), \\ y_i(k) = T_i(k), \end{cases}$$

one can readily verify that $\mathfrak{S} = \mathcal{I}(\mathfrak{S}_1,\dots,\mathfrak{S}_N)$ where $w_i(k) = [T_{i-1}(k);T_{i+1}(k)]$ (with $T_0 = T_n$ and $T_{n+1} = T_1$).

The main goal is to find a CBC for the interconnected system such that a safety controller is synthesized for $\mathfrak{S}$ regulating the temperature of each room between 19°C and 21°C and ensuring that it does not go below 17°C or above 23°C. The idea here is to search for CSBC and accordingly design local controllers for subsystems $\mathfrak{S}_i$. Consequently, the controller for the interconnected system $\mathfrak{S}$ would be a vector such that each of its components is the controller for subsystems $\mathfrak{S}_i$.

We employ the software tool SOSTOOLS (Prajna et al., 2002) and the SDP solver SeDuMi (Sturm, 1999) to compute CSBC as described in Section 5. Based on Lemma 14, we compute CSBC of an order 2 as $\mathbb{B}_i(T_i) = 0.1387T_i^2 - 5.5452T_i + 55.42501$ and the corresponding safety controller of an order 2 as $\nu_i(T_i) = 0.0001T_i^2 - 0.0114T_i + 0.5971$, $\forall i \in \{1,\dots,n\}$. Furthermore, the corresponding constants and functions in Definition 3 satisfying conditions (4)-(7) are quantified as $\eta_i = 0.1657, \beta_i = 1.2, c_i = 10^{-4}, \kappa_i(s) = 0.95s, \alpha_i(s) = 4.5\times10^{-5}s^2$, and $\rho_i(s) = 4.3\times10^{-5}s^2, \forall s \in \mathbb{R}_{\geq 0}$.

We now proceed with constructing a CBC for the interconnected system using CSBC of subsystems. We check the small-gain condition (15) that is required for the compositionality result. By taking $\sigma_i(s) = s$, $\forall i \in \{1,\dots,n\}$, the condition (15) and as a result the condition (16) are always satisfied without any restriction on the number of rooms. Moreover, the compositionality condition (17) is also met since $\beta_i > \eta_i, \forall i \in \{1,\dots,n\}$. Then one can conclude

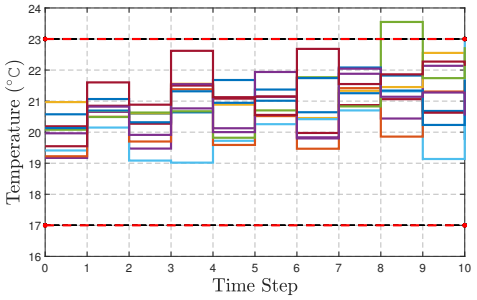

Fig. 1. Closed-loop stage trajectories of a representative room with 10 noise realizations in a network of 1000 rooms.

that $\mathbb{B}(T) = \max_i \left\{0.1387T_i^2 - 5.5452T_i + 55.42501\right\}$ is a CBC for the interconnected system $\mathfrak{S}$. Accordingly, $\nu(T) = [0.0001T_1^2 - 0.0114T_1 + 0.5971;\dots;0.0001T_{1000}^2 - 0.0114T_{1000} + 0.5971]$ is the overall safety controller for the interconnected system and constants and function satisfying conditions (8)-(10) are computed by $\eta = 0.1657, \beta = 1.2, c = 10^{-4}$ and $\kappa(s) = 0.95s, \forall s \in \mathbb{R}_{\geq 0}$.

By employing Theorem 6, one can guarantee that the temperature of the interconnected system $\mathfrak{S}$ starting from the initial set $X_0 = [19,21]^{1000}$ remains in the safe set $[17,23]^{1000}$ during the time horizon $T_d = 10$ with a probability at least 87%, *i.e.*,

$$\mathbb{P}_\nu^a\left\{\mathbb{B}(T(k)) < \beta \mid a,\ \forall k \in [0,10]\right\} \geq 0.87\,. \tag{23}$$

State trajectories of the closed-loop system in a network of 1000 rooms for a representative room with 10 noise realizations are illustrated in Figure 1. As seen, one out of 10 trajectories violates the safety specification, which is in accordance with the theoretical guarantee (23). The computation of CSBC and corresponding control policy for each individual subsystem takes almost 15 seconds with a memory usage of 1.4 MB on a machine with Linux Ubuntu (Intel i7-8665U CPU and a 32 GB of RAM).

7. CONCLUSION

In this paper, we proposed a compositional approach for constructing control barrier certificates of large-scale discrete-time stochastic control systems. We first introduced the notion of control sub-barrier certificates, using which one can construct control barrier certificates of interconnected systems by leveraging some small-gain type conditions. We then proposed upper bounds on the probability that interconnected systems reach unsafe regions in finite-time horizons. We formulated our proposed conditions to a sum-of-squares optimization problem for systematically searching control sub-barrier certificates and corresponding local control policies satisfying safety specifications. We finally illustrated the proposed compositional results on a temperature regulation in a circular building containing 1000 rooms. As a future work, compositional controller barrier certificates for verification and synthesis of more complex LTL properties is under investigation.

REFERENCES

Abate, A., Prandini, M., Lygeros, J., and Sastry, S. (2008). Probabilistic reachability and safety for controlled dis-

crete time stochastic hybrid systems. *Automatica*, 44(11), 2724–2734.

Ahmadi, M., Wu, B., Lin, H., and Topcu, U. (2018). Privacy verification in POMDPs via barrier certificates. In *Proceedings of the 57th IEEE Conference on Decision and Control (CDC)*, 5610–5615.

Bertsekas, D.P. and Shreve, S.E. (1996). *Stochastic Optimal Control: The Discrete-Time Case*. Athena Scientific.

Dashkovskiy, S., Rüffer, B.S., and Wirth, F.R. (2007). An ISS small gain theorem for general networks. *Mathematics of Control, Signals, and Systems (MCSS)*, 19(2), 93–122.

Dashkovskiy, S.N., Rüffer, B.S., and Wirth, F.R. (2010). Small gain theorems for large scale systems and construction of ISS Lyapunov functions. *SIAM Journal on Control and Optimization*, 48(6), 4089–4118.

Huang, C., Chen, X., Lin, W., Yang, Z., and Li, X. (2017). Probabilistic safety verification of stochastic hybrid systems using barrier certificates. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(5s), 186.

Jagtap, P., Soudjani, S., and Zamani, M. (2018). Temporal logic verification of stochastic systems using barrier certificates. In *Proceedings of the International Symposium on Automated Technology for Verification and Analysis*, 177–193.

Jagtap, P., Soudjani, S., and Zamani, M. (2020). Formal synthesis of stochastic systems via control barrier certificates. *Conditionally accepted at the IEEE Transactions on Automatic Control, arXiv:1905.04585*.

Lahijanian, M., Andersson, S.B., and Belta, C. (2015). Formal verification and synthesis for discrete-time stochastic systems. *IEEE Transactions on Automatic Control*, 60(8), 2031–2045.

Lavaei, A. (2019). *Automated Verification and Control of Large-Scale Stochastic Cyber-Physical Systems: Compositional Techniques*. Ph.D. thesis, Technische Universität München, Germany.

Lavaei, A., Soudjani, S., and Zamani, M. (2018). From dissipativity theory to compositional construction of finite Markov decision processes. In *Proceedings of the 21st ACM International Conference on Hybrid Systems: Computation and Control*, 21–30.

Lavaei, A., Soudjani, S., and Zamani, M. (2019). Compositional abstraction-based synthesis of general MDPs via approximate probabilistic relations. *arXiv: 1906.02930*.

Lavaei, A., Soudjani, S., and Zamani, M. (2019a). Compositional construction of infinite abstractions for networks of stochastic control systems. *Automatica*, 107, 125–137.

Lavaei, A., Soudjani, S., and Zamani, M. (2019b). Compositional synthesis of not necessarily stabilizable stochastic systems via finite abstractions. In *Proceedings of the 18th European Control Conference*, 2802–2807.

Lavaei, A., Soudjani, S., and Zamani, M. (2020). Compositional abstraction-based synthesis for networks of stochastic switched systems. *Automatica*, 114.

Lavaei, A., Soudjani, S., and Zamani, M. (2020). Compositional abstraction of large-scale stochastic systems: A relaxed dissipativity approach. *Nonlinear Analysis: Hybrid Systems*, 36.

Lavaei, A., Soudjani, S., and Zamani, M. (2020). Compositional (in)finite abstractions for large-scale interconnected stochastic systems. *IEEE Transactions on Automatic Control, DOI: 10.1109/TAC.2020.2975812*.

Lavaei, A. and Zamani, M. (2019a). Compositional construction of finite MDPs for large-scale stochastic switched systems: A dissipativity approach. *Proceedings of the 15th IFAC Symposium on Large Scale Complex Systems: Theory and Applications*, 52(3), 31–36.

Lavaei, A. and Zamani, M. (2019b). Compositional verification of large-scale stochastic systems via relaxed small-gain conditions. In *Proceedings of the 58th IEEE Conference on Decision and Control*, 2574–2579.

Meyer, P.J., Girard, A., and Witrant, E. (2018). Compositional abstraction and safety synthesis using overlapping symbolic models. *IEEE Transactions on Automatic Control*, 63(6), 1835–1841.

Nejati, A., Soudjani, S., and Zamani, M. (2020). Compositional abstraction-based synthesis for continuous-time stochastic hybrid systems. *European Journal of Control, to appear*.

Nejati, A. and Zamani, M. (2020). Compositional construction of finite MDPs for continuous-time stochastic systems: A dissipativity approach. In *Proceedings of the 21st IFAC World Congress, to appear*.

Parrilo, P.A. (2003). Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming*, 96(2), 293–320.

Prajna, S., Jadbabaie, A., and Pappas, G.J. (2007). A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8), 1415–1428.

Prajna, S., Papachristodoulou, A., and Parrilo, P. (2002). Introducing SOSTOOLS: A general purpose sum of squares programming solver. In *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, volume 1, 741–746. doi:10.1109/CDC.2002.1184594.

Rüffer, B.S. (2010). Monotone inequalities, dynamical systems, and paths in the positive orthant of euclidean n-space. *Positivity*, 14(2), 257–283.

Santoyo, C., Dutreix, M., and Coogan, S. (2019a). A barrier function approach to finite-time stochastic system verification and control. *arXiv:1909.05109*.

Santoyo, C., Dutreix, M., and Coogan, S. (2019b). Verification and control for finite-time safety of stochastic systems via barrier functions. In *2019 IEEE Conference on Control Technology and Applications (CCTA)*, 712–717.

Soudjani, S. and Abate, A. (2013). Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes. *SIAM Journal on Applied Dynamical Systems*, 12(2), 921–956.

Sturm, J.F. (1999). Using sedumi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization methods and software*, 11(1-4), 625–653.

Tabuada, P. (2009). *Verification and Control of Hybrid Systems*. Springer.

Wisniewski, R. and Bujorianu, M.L. (2018). Stochastic safety analysis of stochastic hybrid systems. In *Proceedings of the 57th IEEE Conference on Decision and Control*, 2390–2395.

Zamani, M., Tkachev, I., and Abate, A. (2017). Towards scalable synthesis of stochastic control systems. *Discrete Event Dynamic Systems*, 27(2), 341–369.