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

Compositional Construction of Control Barrier Functions for Networks of Continuous-Time Stochastic Systems ⋆

Ameneh Nejati *, **Sadegh Soudjani** **, **Majid Zamani** ***

* *Department of Electrical and Computer Engineering, Technical University of Munich, Germany (e-mail: amy.nejati@tum.de)*
** *School of Computing, Newcastle University, Newcastle upon Tyne, United Kingdom (e-mail: Sadegh.Soudjani@newcastle.ac.uk)*
*** *Department of Computer Science, University of Colorado Boulder, USA,*
Department of Computer Science, Ludwig Maximilian University of Munich, Germany (e-mail: majid.zamani@colorado.edu)

Abstract: In this paper, we propose a compositional framework for the construction of control barrier functions for networks of continuous-time stochastic control systems. The proposed scheme is based on a notion of so-called *pseudo-barrier functions* computed for subsystems, using which one can synthesize state-feedback controllers for interconnected systems enforcing safety specifications over a finite-time horizon. Particularly, we first leverage sufficient small-gain type conditions to compositionally construct control barrier functions for interconnected systems based on the corresponding pseudo-barrier functions computed for subsystems. Then, using the constructed control barrier functions, we quantify upper bounds on exit probabilities - the probability that an interconnected system reaches certain *unsafe* regions - in a finite-time horizon. We employ a systematic technique based on the sum-of-squares optimization program to search for pseudo-barrier functions of subsystems while synthesizing safety controllers. We demonstrate our proposed results by applying them to a temperature regulation in a network of 1000 rooms.

Keywords: Compositional Control Barrier Functions, Continuous-Time Stochastic Systems, Small-Gain Conditions, Networks of Stochastic Systems.

1. INTRODUCTION

Motivations. Large-scale continuous-time stochastic systems are important modeling frameworks characterizing many real-life engineering systems. They received considerable attentions among both control theorists and computer scientists in the past decade. Automated policy synthesis for this type of complex stochastic systems against some high-level properties, *e.g.,* those expressed as linear temporal logic (LTL) formulae (Pnueli, 1977) is naturally very challenging due to the continuous state sets. In particular, providing automated synthesis of correct-by-design controllers for continuous-time stochastic systems is a crucial task in many safety-critical applications.

Since the closed-form characterization of synthesized policies for continuous-time stochastic systems is not available in general, one potential solution is to approximate original models by simpler ones with finite state sets (finite abstractions). However, the proposed techniques hinge on the discretization of state and input sets and consequently suffer severely from the curse of dimensionality problem. To alleviate this issue, one solution is to consider the large-scale stochastic system as an interconnected system composed of several smaller subsystems, and provide a compositional scheme for the construction of finite abstractions for the given system via finite abstractions of smaller subsystems (Mallik et al., 2019; Soudjani et al., 2017; Lavaei et al., 2018; Lavaei et al., 2019, 2020; Lavaei et al., 2020; Lavaei et al., 2020; Lavaei and Zamani, 2019; Lavaei et al., 2019; Lavaei, 2019; Nejati and Zamani, 2020; Nejati et al., 2020).

Another potential solution to mitigate the computational complexity arising in the analysis of large-scale stochastic systems is to employ *control barrier functions* as a discretization-free approach for the controller synthesis of complex systems. In this respect, discretization-free techniques based on barrier functions for stochastic hybrid systems are initially proposed by Prajna et al. (2007). Stochastic safety verification using barrier certificates for switched diffusion processes and stochastic hybrid systems is respectively proposed by Wisniewski and Bujorianu (2017) and Huang et al. (2017). A verification approach for stochastic switched systems via barrier functions is proposed by Anand et al. (2019). Verification of Markov decision processes using barrier certificates is proposed by Ahmadi et al. (2018). Temporal logic verification of stochastic systems via control barrier certificates is studied

⋆ 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 grant ZA 873/1-1

by Jagtap et al. (2018) with extensions to formal synthesis Jagtap et al. (2019). An adaptive control-based barrier function for a class of stochastic nonlinear systems with full-state constraints is presented by Liu et al. (2018). Control barrier functions for complete and incomplete information stochastic systems are recently proposed by Clark (2019).

Contributions. In this paper, we propose a compositional approach for the construction of control barrier functions for continuous-time stochastic systems. We first compositionally construct control barrier functions for interconnected systems based on so-called pseudo-barrier functions of subsystems by leveraging small-gain conditions. Then, given the constructed control barrier functions, we quantify upper bounds on the probability that interconnected systems reach certain unsafe regions in a finite-time horizon. We finally utilize a systematic technique based on the sum-of-squares optimization program (Parrilo, 2003) to search for pseudo-barrier functions of subsystems. We illustrate the effectiveness of our proposed results by applying them to a temperature regulation in a circular building containing 1000 rooms by compositionally synthesizing safety controllers (together with the corresponding pseudo-barrier functions) regulating the temperature of each room for a bounded-time horizon. Proofs of all statements are omitted in this work due to space limitations.

2. CONTINUOUS-TIME STOCHASTIC CONTROL SYSTEMS

2.1 Notations and Preliminaries

The following notation is utilized throughout the paper. We denote the set of nonnegative integers by $\mathbb{N}_0 := \{0,1,2,\dots\}$ and the set of positive integers by $\mathbb{N} := \{1,2,3,\dots\}$. Symbols $\mathbb{R}$, $\mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote the set of real, positive, and nonnegative real numbers, respectively. We use $\mathbb{R}^n$ to denote an n-dimensional Euclidean space and $\mathbb{R}^{n\times m}$ to denote the space of real matrices with n rows and m columns. We denote by $\mathsf{diag}(a_1,\dots,a_N)$ a diagonal matrix in $\mathbb{R}^{N\times N}$ with diagonal matrix entries $a_1,\dots,a_N$ starting from the upper left corner. Given a matrix $A\in\mathbb{R}^{n\times m}$, $\mathsf{Tr}(A)$ represents the trace of A which is the sum of all its diagonal elements. We employ $x=[x_1;\dots;x_N]$ to denote the corresponding vector of the dimension $\sum_i n_i$, given N vectors $x_i\in\mathbb{R}^{n_i}$, $n_i\in\mathbb{N}_{\geq 1}$, and $i\in\{1,\dots,N\}$. Given a vector $x\in\mathbb{R}^n$, $\|x\|$ denotes the Euclidean norm of x. Given functions $f_i:X_i\to Y_i$, for any $i\in\{1,\dots,N\}$, 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 $(\prod_{i=1}^N f_i)(x_1,\dots,x_N)=[f_1(x_1);\dots;f_N(x_N)]$. The identity matrix in $\mathbb{R}^{n\times n}$ is denoted by $\mathbb{I}_n$. A function $\gamma:\mathbb{R}_{\geq 0}\to\mathbb{R}_{\geq 0}$, is said to be a class $\mathcal{K}$ function if it is continuous, strictly increasing, and $\gamma(0)=0$. A class $\mathcal{K}$ function $\gamma(\cdot)$ is said to be a class $\mathcal{K}_\infty$ if $\gamma(r)\to\infty$ as $r\to\infty$.

We consider a 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, and $\mathbb{P}_\Omega$ is a probability measure that assigns probabilities to events. We assume that triple $(\Omega,\mathcal{F}_\Omega,\mathbb{P}_\Omega)$ is endowed with a filtration $\mathbb{F}=(\mathcal{F}_s)_{s\geq 0}$ satisfying the usual conditions of completeness and right continuity. Moreover, we consider $(\mathbb{W}_s)_{s\geq 0}$ as a b-dimensional $\mathbb{F}$-Brownian motion.

2.2 Continuous-Time Stochastic Control Systems

We consider continuous-time stochastic control systems (ct-SCS) as formalized in the following definition.

Definition 1. A continuous-time stochastic control system (ct-SCS) in this paper is characterized by the tuple

$$\Sigma=(X,U,W,\mathcal{U},\mathcal{W},f,\sigma,Y,h), \tag{1}$$

where

- $X\subseteq\mathbb{R}^n$ is the state set of the system;
- $U\subseteq\mathbb{R}^m$ is the *external* input set of the system;
- $W\subseteq\mathbb{R}^p$ is the *internal* input set of the system;
- $\mathcal{U}$ and $\mathcal{W}$ are respectively subsets of the sets of all $\mathbb{F}$-progressively measurable processes taking values in $\mathbb{R}^m$ and $\mathbb{R}^p$;
- $f:X\times U\times W\to X$ is the drift term which is globally Lipschitz continuous: there exist constants $\mathscr{L}_x,\mathscr{L}_\nu,\mathscr{L}_w\in\mathbb{R}_{\geq 0}$ such that $\|f(x,\nu,w)-f(x',\nu',w')\|\leq\mathscr{L}_x\|x-x'\|+\mathscr{L}_\nu\|\nu-\nu'\|+\mathscr{L}_w\|w-w'\|$ for all $x,x'\in X$, for all $\nu,\nu'\in U$, and for all $w,w'\in W$;
- $\sigma:\mathbb{R}^n\to\mathbb{R}^{n\times\mathsf{b}}$ is the diffusion term which is globally Lipschitz continuous with the Lipschitz constant $\mathscr{L}_\sigma$;
- $Y\subseteq\mathbb{R}^q$ is the output set of the system;
- $h:X\to Y$ is the output map.

A continuous-time stochastic control system Σ satisfies

$$\Sigma:\begin{cases}\mathsf{d}\xi(t)=f(\xi(t),\nu(t),w(t))\,\mathsf{d}t+\sigma(\xi(t))\,\mathsf{d}\mathbb{W}_t,\\ \zeta(t)=h(\xi(t)),\end{cases} \tag{2}$$

$\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.) for any $\nu\in\mathcal{U}$ and any $w\in\mathcal{W}$, where stochastic processes $\xi:\Omega\times\mathbb{R}_{\geq 0}\to X$ and $\zeta:\Omega\times\mathbb{R}_{\geq 0}\to Y$ are called the *solution process* and the *output trajectory* of Σ, respectively. We also employ $\xi_{a\nu w}(t)$ to denote the value of the solution process at time $t\in\mathbb{R}_{\geq 0}$ under input trajectories ν and w from an initial condition $\xi_{a\nu w}(0)=a$ $\mathbb{P}$-a.s., where a is a random variable that is $\mathcal{F}_0$-measurable. We also denote by $\zeta_{a\nu w}$ the *output trajectory* corresponding to the *solution process* $\xi_{a\nu w}$.

Given the ct-SCS in (1), we are interested in Markov policies to control the system.

Definition 2. A Markov policy for the ct-SCS Σ in (1) is the map $\rho:\mathbb{B}(U)\times X\times\mathbb{R}_{\geq 0}\to[0,1]$, with $\mathbb{B}(U)$ being the Borel sigma-algebra on the external input space, such that $\rho(\cdot\,|\,\cdot,t)$ is a universally measurable stochastic kernel for all $t\in\mathbb{R}_{\geq 0}$ (Ross, 2008). For any state $x\in X$ at time t, the input $\nu(t)$ is chosen according to the probability measure $\rho(\cdot\,|\,x,t)$. The class of all such Markov policies is denoted by Π_M. Although we define continuous-time stochastic control systems ct-SCS with outputs, we assume full-state information is available for the sake of controller synthesis. The role of the outputs is mainly for the sake of interconnecting systems as explained in detail in Section 4.

Since the main contribution of this work is to propose a compositional approach for the construction of control barrier functions, we are eventually interested in investigating interconnected systems without having internal

inputs. In this case, the tuple (1) reduces to $(X, U, \mathcal{U}, f, \sigma)$ with $f : X \times U \to X$, and ct-SCS (2) can be re-written as

$$\Sigma : \mathsf{d}\xi(t) = f(\xi(t), \nu(t))\,\mathsf{d}t + \sigma(\xi(t))\,\mathsf{d}\mathbb{W}_t.$$

In the next sections, we propose an approach for the compositional construction of control barrier functions for interconnected ct-SCS. To achieve this, we define notions of control pseudo-barrier and barrier functions for ct-SCS and interconnected versions, respectively.

3. CONTROL PSEUDO-BARRIER AND BARRIER FUNCTIONS

In this section, we first introduce a notion of control pseudo-barrier functions (CPBF) for ct-SCS with both internal and external inputs. We then define a notion of control barrier functions (CBF) for ct-SCS with only external inputs. We leverage the former notion to compositionally construct the latter one for interconnected systems. We mainly employ the latter notion to quantify upper bounds on the probability that the interconnected system reaches certain unsafe regions in a finite-time horizon via Theorem 6.

Definition 3. Consider a ct-SCS $\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, Y, h)$. Let $X_0, X_u \subseteq X$ be initial and unsafe sets of the system, respectively. A twice differentiable function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is called a control pseudo-barrier function (CPBF) for Σ if there exist $\alpha, \kappa \in \mathcal{K}_\infty$, $\rho_{\text{int}} \in \mathcal{K}_\infty \cup \{0\}$, $\gamma, \psi \in \mathbb{R}_{\geq 0}$ and $\lambda \in \mathbb{R}_{>0}$, such that

$$\mathcal{B}(x) \geq \alpha(\|h(x)\|), \quad \forall x \in X, \tag{3}$$
$$\mathcal{B}(x) \leq \gamma, \quad \forall x \in X_0, \tag{4}$$
$$\mathcal{B}(x) \geq \lambda, \quad \forall x \in X_u, \tag{5}$$

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

$$\mathcal{LB}(x) \leq -\kappa(\mathcal{B}(x)) + \rho_{\text{int}}(\|w\|) + \psi, \tag{6}$$

where $\mathcal{LB}$ is the *infinitesimal generator* of the stochastic process acting on the function $\mathcal{B}$ (Oksendal, 2013), as defined in the next remark.

Remark 4. Note that the *infinitesimal generator* $\mathcal{L}$ of the process $\xi(t)$ acting on function $\mathcal{B} : X \to R_{\geq 0}$ is defined as

$$\mathcal{LB}(x) = \partial_x \mathcal{B}(x) f(x, \nu, w) + \frac{1}{2}\mathsf{Tr}(\sigma(x)\sigma(x)^T \partial_{x,x}\mathcal{B}(x)). \tag{7}$$

The employed quantifiers in the condition (6) implicitly imply that one can synthesize *decentralized* controllers for Σ since the control input ν is independent of internal inputs w (state information of other subsystems). However, one can change the sequence of the quantifier in (6) to $\forall x \in X, \forall w \in W, \exists \nu \in U$ in order to design *distributed* control policies. In this latter case, the chance of finding control pseudo-barrier functions gets increased since distributed controllers do not need to be robust against the whole range of the internal input set.

Now we amend the above notion for the interconnected ct-SCS without internal inputs by simply eliminating all the terms related to w. This notion will be utilized in Theorem 6 for quantifying upper bounds on exit probabilities over systems without internal inputs (*e.g.,* interconnected stochastic systems).

Definition 5. Consider the (interconnected) system $\Sigma = (X, U, \mathcal{U}, f, \sigma)$ with initial and unsafe sets $X_0, X_u \subseteq X$. A twice differentiable function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is called a control barrier function (CBF) for Σ if

$$\mathcal{B}(x) \leq \gamma, \quad \forall x \in X_0, \tag{8}$$
$$\mathcal{B}(x) \geq \lambda, \quad \forall x \in X_u, \tag{9}$$

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

$$\mathcal{LB}(x) \leq -\kappa(\mathcal{B}(x)) + \psi, \tag{10}$$

for some $\kappa \in \mathcal{K}_\infty$, $\gamma, \psi \in \mathbb{R}_{\geq 0}$, and $\lambda \in \mathbb{R}_{>0}$ with $\lambda > \gamma$.

The next theorem shows the usefulness of CBF to quantify upper bounds on the exit probability of (interconnected) systems without having internal inputs.

Theorem 6. Let $\Sigma = (X, U, \mathcal{U}, f, \sigma)$ be an (interconnected) ct-SCS without internal inputs. Suppose $\mathcal{B}$ is a CBF for Σ as in Definition 5, and there exists a constant $\hat{\kappa} \in \mathbb{R}_{>0}$ 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 Σ starts from any initial state $\xi(0) = x_0 \in X_0$ and reaches X_u under the policy $\nu(\cdot)$ within a finite-time horizon $[0, T_d] \subseteq \mathbb{R}_{\geq 0}$ is formally quantified as

$$\mathbb{P}^{x_0}_{\nu}\Big\{\sup_{0\leq t\leq T_d} \mathcal{B}(\xi(t)) \geq \lambda \mid \xi(0) = x_0\Big\} \leq \delta, \tag{11}$$

$$\delta := \begin{cases} 1 - (1 - \frac{\gamma}{\lambda})e^{-\frac{\psi T_d}{\lambda}}, & \text{if } \lambda \geq \frac{\psi}{\hat{\kappa}}, \\ \frac{\hat{\kappa}\gamma + (e^{\hat{\kappa}T_d} - 1)\psi}{\hat{\kappa}\lambda e^{\hat{\kappa}T_d}}, & \text{if } \lambda \leq \frac{\psi}{\hat{\kappa}}. \end{cases}$$

Remark 7. In Section 5, we reformulate the conditions of Definition 5 to an optimization problem such that one can minimize the values of γ and ψ in order to acquire an upper bound in the finite-time horizon that is as tight as possible.

In the next section, we analyze networks of stochastic control subsystems and show under which conditions one can construct a CBF of an interconnected system using its CPBF of subsystems.

4. COMPOSITIONAL CONSTRUCTION OF CBF

In this section, we provide a compositional framework for the construction of control barrier functions for interconnected systems Σ. Suppose we are given control subsystems $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, Y_i, h_i), i \in \{1, \ldots, N\}$, where their internal inputs and outputs are partitioned as

$$w_i = [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}],$$
$$y_i = [y_{i1}; \ldots; y_{iN}], \tag{12}$$

and their output spaces and functions are of the form

$$Y_i = \prod_{j=1}^{N} Y_{ij}, \quad h_i(x_i) = [h_{i1}(x_i); \ldots; h_{iN}(x_i)], \tag{13}$$

with $h_{ii}(x_i) = x_i$ (*i.e.,* full state information of subsystems). 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. For the interconnection, if there is a connection from Σ_j to Σ_i, we assume that w_{ij} is equal to y_{ji}. Otherwise, we put the connecting output function identically zero, *i.e.,* $h_{ji} \equiv 0$. An example of the interconnection of two stochastic subsystems Σ_1 and Σ_2 is illustrated in Figure 1.

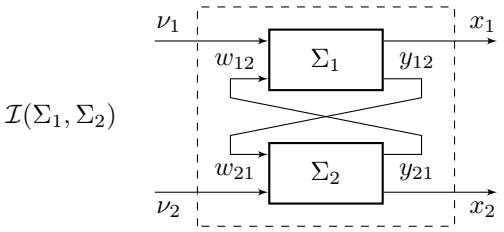

Fig. 1. Interconnection of two stochastic subsystems Σ_1 and Σ_2.

Now we define the interconnected stochastic control systems.

Definition 8. Consider $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, Y_i, h_i)$, $i \in \{1, \ldots, N\}$, with the input-output configuration as in (12) and (13). The interconnection of Σ_i, $\forall i \in \{1, \ldots, N\}$, is the interconnected stochastic control system $\Sigma = (X, U, \mathcal{U}, f, \sigma)$, denoted by $\mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$, such that $X := \prod_{i=1}^N X_i$, (with $X_0 := \prod_{i=1}^N X_{0_i}$, $X_u := \prod_{i=1}^N X_{u_i}$), $U := \prod_{i=1}^N U_i$, $f := \prod_{i=1}^N f_i$, and $\sigma := [\sigma_1(x_1); \cdots; \sigma_N(x_N)]$, subject to the following constraint:

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

Assume that for control subsystems $\Sigma_i, i \in \{1, \ldots, N\}$, there exist CPBF $\mathcal{B}_i$ as defined in Definition 3 with functions $\alpha_i, \kappa_i \in \mathcal{K}_\infty$, $\rho_{\text{int}i} \in \mathcal{K}_\infty \cup \{0\}$, and constants $\gamma_i, \psi_i \in \mathbb{R}_{\geq 0}$ and $\lambda_i \in \mathbb{R}_{>0}$. In order to establish the main compositionality result of the paper, we raise the following small-gain type assumption.

Assumption 9. Assume that for any $i, j \in \{1, \cdots, N\}$, $i \neq j$, there exist $\mathcal{K}_\infty$ functions $\hat{\gamma}_i$ and constants $\hat{\lambda}_i \in \mathbb{R}_{>0}$ and $\hat{\delta}_{ij} \in \mathbb{R}_{\geq 0}$ such that for any $s \in \mathbb{R}_{\geq 0}$:

$$\kappa_i(s) \geq \hat{\lambda}_i \hat{\gamma}_i(s), \tag{14}$$

$$h_{ji} \equiv 0 \implies \hat{\delta}_{ij} = 0, \tag{15}$$

$$h_{ji} \not\equiv 0 \implies \rho_{\text{int}i}((N-1)\alpha_j^{-1}(s)) \leq \hat{\delta}_{ij} \hat{\gamma}_j(s), \tag{16}$$

where α_j, κ_i, and $\rho_{\text{int}i}$, represent the corresponding $\mathcal{K}_\infty$ functions related to $\mathcal{B}_i$ appearing in Definition 3.

Before presenting the next main theorem, we define $\Lambda := \mathsf{diag}(\hat{\lambda}_1, \ldots, \hat{\lambda}_N)$, $\Delta := \{\hat{\delta}_{ij}\}$, where $\hat{\delta}_{ii} = 0$ $\forall i \in \{1, \cdots, N\}$, and $\Gamma(s) := [\hat{\gamma}_1(s_1); \ldots; \hat{\gamma}_N(s_N)]$, where $s = [s_1; \ldots; s_N]$. In the next theorem, we leverage the small-gain Assumption 9 to compute compositionally a control barrier function for the interconnected system Σ as in Definition 5.

Theorem 10. Consider the interconnected stochastic control system $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems Σ_i. Suppose that each control subsystem Σ_i admits a CPBF $\mathcal{B}_i$ as defined in Definition 3 with initial and unsafe sets X_{0_i} and X_{u_i}, respectively. If Assumption 9 holds and there exists a vector $\mu \in \mathbb{R}^N_{>0}$ such that

$$\mu^T(-\Lambda + \Delta) < 0, \tag{17}$$

$$\sum_{i=1}^N \mu_i \lambda_i > \sum_{i=1}^N \mu_i \gamma_i, \tag{18}$$

then

$$\mathcal{B}(x) := \sum_{i=1}^N \mu_i \mathcal{B}_i(x_i) \tag{19}$$

is a CBF for the interconnected system $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ with the initial and unsafe sets $X_0 := \prod_{i=1}^N X_{0_i}$, $X_u := \prod_{i=1}^N X_{u_i}$, respectively.

Remark 11. Note that a vector $\mu \in \mathbb{R}^N_{>0}$ satisfying compositionality condition (17) exists if and only if the spectral radius of $\Lambda^{-1}\Delta$ is strictly less than one (Dashkovskiy et al., 2011). In this case if Δ is irreducible, μ can be chosen as the left eigenvector of $-\Lambda + \Delta$ corresponding to the largest eigenvalue, which is real and negative by the Perron-Frobenius theorem (Axelsson, 1994).

Remark 12. Note that the condition (18) in general is not very restrictive since constants μ_i in (19) play a considerable role in rescaling CPBF for subsystems while normalizing the effect of internal gains of other subsystems. One can expect that the inequality (18) holds in many applications due to this rescaling.

5. COMPUTATION OF CPBF

In this section, we reformulate the proposed conditions in Definition 3 as a sum-of-squares (SOS) optimization problem (Parrilo, 2003) and provide a systematic approach for computing CPBF and corresponding control policies for subsystems Σ_i. The SOS technique relies on the fact that a polynomial is non-negative if it can be written as a sum of squares of different polynomials. In order to utilize an SOS optimization, we raise the following assumption.

Assumption 13. Subsystem Σ_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 $W_i \subseteq \mathbb{R}^{p_i}$. Moreover, the drift term $f_i : X_i \times U_i \times W_i \to X_i$ is a polynomial function of the state x_i and external and internal inputs ν_i, w_i. Furthermore, the diffusion term $\sigma_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i \times \mathsf{b}_i}$ is a polynomial function of the state x_i.

Under Assumption 13, the following lemma provides a set of sufficient conditions for the existence of a CPBF required in Definition 3, which can be solved as an SOS optimization problem.

Lemma 14. Suppose Assumption 13 holds and sets X_0, X_u, X, W can be defined by vectors of polynomial inequalities $X_{0_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{0_i}(x_i) \geq 0\}$, $X_{u_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{1_i}(x_i) \geq 0\}$, $X_i = \{x_i \in \mathbb{R}^{n_i} \mid g_i(x_i) \geq 0\}$, and $W_i = \{w_i \in \mathbb{R}^{p_i} \mid g_{w_i}(w_i) \geq 0\}$, where the inequalities are defined element-wise. Suppose there exists a sum-of-squares polynomial $\mathcal{B}_i(x_i)$, constants $\gamma_i, \psi_i \in \mathbb{R}_{\geq 0}$, $\lambda_i \in \mathbb{R}_{>0}$, functions $\alpha_i, \kappa_i \in \mathcal{K}_\infty$, $\rho_{\text{int}i} \in \mathcal{K}_\infty \cup \{0\}$, polynomials $l_{\nu_{j_i}}(x)$ corresponding to the j^{th} input in $\nu_i = (\nu_{1_i}, \nu_{2_i}, \ldots, \nu_{m_i}) \in U_i \subseteq \mathbb{R}^{m_i}$, and vectors of sum-of-squares polynomials $l_{0_i}(x_i)$, $l_{1_i}(x_i)$, $l_i(x_i)$, $\hat{l}_i(x_i)$, and $l_{w_i}(x_i)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:

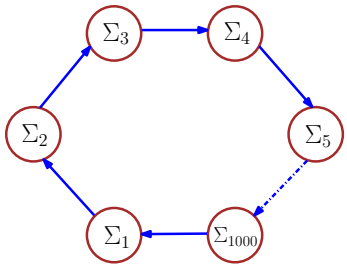

Fig. 2. A circular building in a network of 1000 rooms.

$$\mathcal{B}_i(x_i) - l_i^T(x_i)g_i(x_i) - \alpha_i(\|h_i(x_i)\|), \tag{20}$$
$$-\mathcal{B}_i(x_i) - l_{0_i}^T(x_i)g_{0_i}(x_i) + \gamma_i, \tag{21}$$
$$\mathcal{B}_i(x_i) - l_{1_i}^T(x_i)g_{1_i}(x_i) - \lambda_i, \tag{22}$$
$$-\mathcal{L}\mathcal{B}_i(x_i) - \kappa_i(\mathcal{B}_i(x_i)) + \rho_{\text{int}i}(\|w_i\|) + \psi_i$$
$$-\sum_{j=1}^{m_i}(\nu_{j_i} - l_{\nu_{j_i}}(x_i)) - \hat{l}_i^T(x_i)g_i(x_i) - l_{w_i}^T(w_i)g_{w_i}(w_i). \tag{23}$$

Then, $\mathcal{B}_i(x_i)$ satisfies conditions (3)-(6) in Definition 3 and $\nu_i = [l_{\nu_{1_i}}(x_i); \ldots; l_{\nu_{m_i}}(x_i)]$, $i \in \{1, \ldots, N\}$, is the corresponding safety controller.

Remark 15. Note that the function $\kappa_i(\cdot)$ in (23) can cause nonlinearity on unknown parameters of $\mathcal{B}_i$. A possible way to avoid this issue is to consider a linear function $\kappa_i(r) = \hat{\kappa}_i r, \forall r \in \mathbb{R}_{\geq 0}$, with some constant $\hat{\kappa}_i \in \mathbb{R}_{>0}$ as appeared in Theorem 6. Then one can employ bisection method to minimize the value of $\hat{\kappa}_i$.

Remark 16. Note that for computing the sum-of-squares polynomial $\mathcal{B}_i(x_i)$ fulfilling reformulated conditions (20)-(23), one can readily employ existing software tools available in the literature such as SOSTOOLS (Papachristodoulou et al., 2013) together with a semidefinite programming (SDP) solver such as SeDuMi (Sturm, 1999).

6. CASE STUDY

To illustrate the effectiveness of the proposed results, we apply our approaches to the temperature regulation in a network of 1000 rooms, each equipped with a heater and connected circularly as depicted in Figure 2. We compute CPBF of each room while compositionally synthesizing safety controllers to regulate the temperature of each room in a comfort zone for a bounded-time horizon.

The model of this case study is adapted from (Girard et al., 2016) by including stochasticity in the model. The evolution of the temperature $T(\cdot)$ can be described by the interconnected stochastic differential equation

$$\Sigma : \mathsf{d}T(t) = (AT(t) + \theta T_h \nu(t) + \beta T_E)\mathsf{d}t + G\mathsf{d}\mathbb{W}_t, \tag{24}$$

where A is a matrix with diagonal elements $\bar{a}_{ii} = -2\eta - \beta - \theta\nu_i(t)$, $i \in \{1, \ldots, n\}$, off-diagonal elements $\bar{a}_{i,i+1} = \bar{a}_{i+1,i} = \bar{a}_{1,n} = \bar{a}_{n,1} = \eta$, $i \in \{1, \ldots, n-1\}$, and all other elements are identically zero. Parameters $\eta = 0.05$, $\beta = 0.005$, and $\theta = 0.01$ 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. Moreover, $G = 0.1\mathbb{I}_n$, $T_E = [T_{e_1}; \ldots; T_{e_n}]$, $\nu(t) = [\nu_1(t); \ldots; \nu_n(t)]$, and $T(t) = [T_1(t); \ldots; T_n(t)]$. Outside temperatures are the same for all rooms: $T_{ei} = -1\,^\circ\mathsf{C}$, $\forall i \in \{1, \ldots, n\}$, and the heater temperature is $T_h = 50\,^\circ\mathsf{C}$. Now by considering the individual rooms as Σ_i described by

$$\Sigma_i : \begin{cases} \mathsf{d}T_i(t) = (\bar{a}_{ii}T_i(t) + \theta T_h \nu_i(t) + \eta w_i(t) + \beta T_{e_i})\mathsf{d}t + 0.1\mathsf{d}\mathbb{W}_{t_i}, \\ \zeta_i(t) = T_i(t), \end{cases}$$

one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ where $w_i(t) = \zeta_{i\pm1}(t)$ (with $\zeta_0 = \zeta_n$ and $\zeta_{n+1} = \zeta_1$). Note that for the sake of a simpler illustration of the results, we assume that all subsystems are homogeneous.

The regions of interest in this example are $X_i \in [1, 50], X_{0_i} \in [19, 21], X_{u_i} = [1, 17] \cup [23, 50], \forall i \in \{1, \ldots, n\}$. The main goal is to find a CBF for the interconnected system, during which a safety controller is synthesized for Σ maintaining the temperature of rooms in a comfort zone $[17, 23]^{1000}$. The idea here is to search for CPBF and accordingly design local controllers for subsystems Σ_i. Consequently, the controller for the interconnected system Σ is simply a vector such that its ith component is the controller for the subsystem Σ_i. We employ the software tool SOSTOOLS and the SDP solver SeDuMi to compute CPBF as described in Section 5. According to Lemma 14, we compute CPBF of an order 2 as $\mathcal{B}_i(T_i) = 0.1469T_i^2 - 5.8788T_i + 58.8027$ and the corresponding safety controller of an order 2 as $\nu_i(T_i) = 0.0017T_i^2 - 0.08201T_i + 1.3857$ for all $i \in \{1, \ldots, n\}$. Moreover, the corresponding constants and functions in Definition 3 satisfying conditions (3)-(6) are quantified as $\gamma_i = 0.16, \lambda_i = 1.3, \kappa_i(s) = 0.01s, \psi_i = 10^{-4}, \alpha_i(s) = 45 \times 10^{-6}s, \rho_{\text{int}i}(s) = 4.4955 \times 10^{-9}s, \forall s \in \mathbb{R}_{\geq 0}$.

We now proceed with Theorem 10 to construct a CBF for the interconnected system using CPBF of subsystems. One can readily verify that the small-gain Assumption 9 holds with $\hat{\gamma}_i(s) = s, \forall s \in \mathbb{R}_{\geq 0}, \hat{\lambda}_i = 0.01, \hat{\delta}_{ij} = 9.99 \times 10^{-5}$. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, n\}$, one can readily show that the spectral radius of $\Lambda^{-1}\Delta$ is 0.9996 which is strictly less that one (cf. Remark 11), and consequently the compositionality condition (17) is satisfied. Moreover, the compositionality condition (18) is also met since $\lambda_i > \gamma_i, \forall i \in \{1, \ldots, n\}$. Then by employing the results of Theorem 10, one can conclude that $\mathcal{B}(T) = \sum_{i=1}^{1000}(0.1469T_i^2 - 5.8788x_i + 58.8027)$ is a CBF for the interconnected system Σ with $\gamma = 160, \lambda = 1300, \kappa(s) = 0.0098s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = 0.1$. Accordingly, $\nu(T) = [0.0017T_1^2 - 0.08201T_1 + 1.3857; \ldots; 0.0017T_{1000}^2 - 0.08201T_{1000} + 1.3857]$ is the overall safety controller for the interconnected system.

By employing Theorem 6, one can guarantee that the temperature of the interconnected system Σ starting from initial conditions $x_0 \in [19, 21]^{1000}$ remains in the safe set $[17, 23]^{1000}$ during the finite-time horizon $T_d = 10$ with a probability at least 88%, *i.e.,*

$$\mathbb{P}_\nu^{x_0}\Big\{\mathcal{B}(\xi(t)) < \lambda \mid \xi(0) = x_0, \forall t \in [0, 10]\Big\} \geq 0.88\,. \tag{25}$$

Closed-loop state trajectories of a representative room with 10 different noise realizations are illustrated in Figure 3. As illustrated, one out of 10 trajectories violates the safety specification, which is in accordance with the theoretical guarantee in (25).

REFERENCES

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.

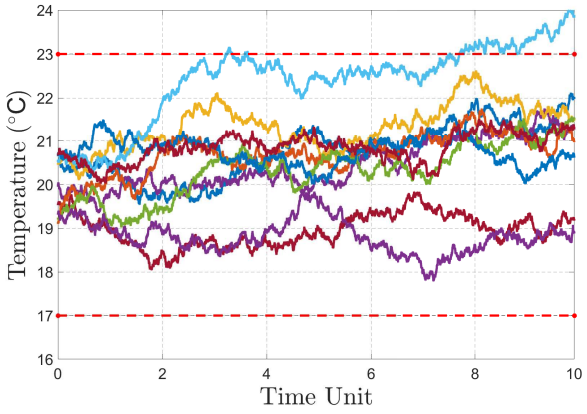

Fig. 3. Closed loop state trajectories of a representative room with 10 noise realizations in a network of 1000 rooms.

Anand, M., Jagtap, P., and Zamani, M. (2019). Verification of switched stochastic systems via barrier certificates. In *Proceedings of the 58th IEEE Conference on Decision and Control, to appear*.

Axelsson, O. (1994). Iterative solution methods. cambridge univ. *Press, Cambridge*.

Clark, A. (2019). Control barrier functions for complete and incomplete information stochastic systems. In *2019 American Control Conference (ACC)*, 2928–2935.

Dashkovskiy, S., Ito, H., and Wirth, F. (2011). On a small gain theorem for ISS networks in dissipative Lyapunov form. *European Journal of Control*, 17(4), 357–365.

Girard, A., Gössler, G., and Mouelhi, S. (2016). Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control*, 61(6), 1537–1549.

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. (2019). Formal synthesis of stochastic systems via control barrier certificates. *arXiv: 1905.04585*.

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. (2019). Compositional construction of infinite abstractions for networks of stochastic control systems. *Automatica*, 107, 125–137.

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. (2019). 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.

Liu, Y.J., Lu, S., Tong, S., Chen, X., Chen, C.P., and Li, D.J. (2018). Adaptive control-based barrier lyapunov functions for a class of stochastic nonlinear systems with full state constraints. *Automatica*, 87, 83–93.

Mallik, K., Schmuck, A., Soudjani, S., and Majumdar, R. (2019). Compositional synthesis of finite-state abstractions. *IEEE Transactions on Automatic Control*, 64(6), 2629–2636.

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*.

Oksendal, B. (2013). *Stochastic differential equations: an introduction with applications*. Springer Science & Business Media.

Papachristodoulou, A., Anderson, J., Valmorbida, G., Prajna, S., Seiler, P., and Parrilo, P. (2013). SOSTOOLS version 3.00 sum of squares optimization toolbox for MATLAB. *arXiv:1310.4716*.

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

Pnueli, A. (1977). The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, 46–57.

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.

Ross, K. (2008). Stochastic control in continuous time. *Lecture Notes on Continuous Time Stochastic Control*, P33–P37.

Soudjani, S., Abate, A., and Majumdar, R. (2017). Dynamic Bayesian networks for formal verification of structured stochastic processes. *Acta Informatica*, 54(2), 217–242.

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.

Wisniewski, R. and Bujorianu, M.L. (2017). Stochastic safety analysis of stochastic hybrid systems. In *Proceedings of the 56th IEEE Conference on Decision and Control*, 2390–2395.