From Dissipativity Theory to Compositional Construction of Control Barrier Certificates

Ameneh Nejati
Department of Electrical Engineering, Technical University of Munich, Germany
Department of Computer Science, LMU Munich, Germany

Majid Zamani
Department of Computer Science, University of Colorado Boulder, USA
Department of Computer Science, LMU Munich, Germany

Abstract

This paper proposes a compositional framework based on dissipativity approaches to construct control barrier certificates for networks of continuous-time stochastic hybrid systems. The proposed scheme leverages the structure of the interconnection topology and a notion of so-called *control storage certificates* to construct control barrier certificates compositionally. By utilizing those certificates, one can compositionally synthesize state-feedback controllers for interconnected systems enforcing safety specifications over a finite-time horizon. In particular, we leverage dissipativity-type compositionality conditions to construct *control barrier certificates* for interconnected systems based on corresponding control storage certificates computed for subsystems. Using those constructed control barrier certificates, one can quantify upper bounds on probabilities that interconnected systems reach certain *unsafe* regions in finite-time horizons. We employ a systematic technique based on the sum-of-squares optimization program to search for storage certificates of subsystems together with their corresponding safety controllers. We demonstrate our proposed results by applying them to a temperature regulation in a circular building containing 1000 rooms. To show the applicability of our approaches to dense networks, we also apply our proposed techniques to a *fully-interconnected network*.

2012 ACM Subject Classification Computer systems organization → Embedded and cyber-physical systems; Mathematics of computing → Stochastic processes; Theory of computation → Timed and hybrid models

Keywords and Phrases Compositional barrier certificates, Stochastic hybrid systems, Dissipativity theory, Large-scale networks, Formal controller synthesis

Digital Object Identifier 10.4230/LITES.8.2.6

Funding This work was supported in part by the H2020 ERC Starting Grant AutoCPS (grant agreement No. 804639) and the NSF under Grant CNS-2145184.

Received 2020-08-31 **Accepted** 2022-02-11 **Published** 2022-12-07

Editor Alessandro Abate, Uli Fahrenberg, and Martin Fränzle

Special Issue Special Issue on Distributed Hybrid Systems

1 Introduction

Motivations. Formal methods are becoming a promising scheme to design controllers for complex stochastic systems against high-level logic properties, *e.g.,* those expressed as linear temporal logic (LTL) formulae [25]. Since the closed-form characterization of synthesized policies for continuous-time continuous-space stochastic systems is not available in general, formal policy synthesis for those complex systems is naturally very challenging due to their continuous state sets.

To mitigate the encountered computational complexity, one potential direction is to approximate original models by simpler ones with finite state sets (*a.k.a.,* finite Markov decision processes (MDPs)). However, due to discretizing the state and input sets, the finite-abstraction based techniques suffer severely from the curse of dimensionality problem. To alleviate this issue, compositional techniques have been introduced in the past few years to construct finite MDPs of interconnected systems based on constructing finite MDPs of smaller subsystems [11, 12, 13, 14, 15, 16, 19, 20].

Although the proposed compositional frameworks in the setting of finite abstractions can mitigate the effects of the state-explosion problem, the curse of dimensionality may still occur in the level of subsystems given their range of state and input sets. These challenges motivate the need to employ *control barrier certificates* as a discretization-free approach for synthesizing controllers for complex stochastic systems. In this respect, discretization-free techniques based on barrier certificates for stochastic hybrid systems are initially proposed in [26]. Stochastic safety verification using barrier certificates for switched diffusion processes and classes of stochastic hybrid systems is, respectively, proposed in [29] and [8]. Verification of MDPs using barrier certificates is proposed in [1]. Temporal logic synthesis of stochastic systems via control barrier certificates is presented in [9]. Compositional construction of control barrier certificates for *discrete-time* stochastic *control and switched* systems is respectively proposed in [2, 17].

Contributions. This paper proposes a compositional scheme based on dissipativity approaches for the construction of control barrier certificates for a class of continuous-time continuous-space stochastic hybrid systems, namely, jump-diffusion systems. Particularly, we compositionally construct control barrier certificates of interconnected jump-diffusion systems based on so-called *control storage certificates* of subsystems by leveraging dissipativity-type compositionality reasoning. The proposed compositionality condition can enjoy the structure of the interconnection topology and may not require any constraints on the number or even gains of subsystems (cf. Remark 6 and the case study). Using those constructed control barrier certificates, one can quantify upper bounds on probabilities that interconnected systems reach certain unsafe regions in finite-time horizons. We finally utilize a systematic technique based on the sum-of-squares (SOS) optimization program [24] to search for control storage certificates 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 control storage certificates) regulating the temperature of each room in a comfort zone within a bounded-time horizon. We also apply our proposed techniques to a *fully-interconnected network* to show their applicabilities to non-sparse interconnection topologies.

Recent Works. Compositional construction of control barrier certificates for continuous-time stochastic systems is also proposed in [18], but using a different compositionality scheme, namely, based on *small-gain* conditions. Our proposed compositionality approach here is potentially less conservative than the one presented in [18] since the dissipativity-type compositional reasoning, proposed in this work, can enjoy the structure of the interconnection topology and may not require any constraints on the number or gains of the subsystems (cf. Remark 6). Furthermore, the provided results in [18] ask an additional condition (*i.e.,* [18, condition (3)]) which is required for the satisfaction of *small-gain* type compositionality conditions, while we do not need such an extra condition in our setting. Besides, we enlarge the class of systems here to a fragment of continuous-time stochastic *hybrid* ones by adding Poisson processes to the dynamics, whereas the results in [18] only deal with systems described by stochastic differential equations without jumps.

Control barrier functions for stochastic systems in the presence of process and measurement noises are presented in [5]. Although the proposed results in [5] are also for continuous-time stochastic systems, they are only presented in a monolithic framework and dealing only with Brownian motions as sources of the noise. In comparison, we propose here a *compositional* approach for the construction of barrier functions for networks of stochastic systems affected by both Brownian motions and Poisson processes. The results in [5] propose a rather *qualitative* satisfaction of safety specification in which the safety property is either satisfied with the probability 1 or not satisfied. As a result, the proposed approach there is very conservative and the proposed

optimization problem is not going to be feasible for many scenarios depending on different dynamics and safety specifications. In contrast, our work proposes a *quantitative* version of satisfaction in which one can get a lower bound on the probability of satisfaction which is less than one.

2 Continuous-Time Stochastic Hybrid Systems

2.1 Notation and Preliminaries

The following notation is utilized throughout the paper. We denote sets of nonnegative and positive integers by $\mathbb{N}_0 := \{0, 1, 2, \ldots\}$ and $\mathbb{N} := \{1, 2, 3, \ldots\}$, respectively. The symbols $\mathbb{R}$, $\mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote sets 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 $\mathsf{diag}(a_1, \ldots, a_N)$ and $\mathsf{blkdiag}(a_1, \ldots, a_N)$, respectively, a diagonal matrix in $\mathbb{R}^{N\times N}$ with diagonal scalar and matrix entries $a_1, \ldots, a_N$ 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 $x = [x_1; \ldots; x_N]$ to denote the corresponding vector of a dimension $\sum_i n_i$, given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}$, and $i \in \{1, \ldots, N\}$. 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 $i \in \{1, \ldots, N\}$, 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 $(\prod_{i=1}^N f_i)(x_1, \ldots, x_N) = [f_1(x_1); \ldots; f_N(x_N)]$. 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. Let $(\mathbb{W}_s)_{s\geq 0}$ be a b-dimensional $\mathbb{F}$-Brownian motion and $(\mathbb{P}_s)_{s\geq 0}$ be an r-dimensional $\mathbb{F}$-Poisson process. We assume that the Poisson process and Brownian motion are independent of each other. The Poisson process $\mathbb{P}_s = [\mathbb{P}_s^1; \cdots; \mathbb{P}_s^{\mathsf{r}}]$ models r events whose occurrences are assumed to be independent of each other.

2.2 Continuous-Time Stochastic Hybrid Systems

We consider a class of continuous-time stochastic hybrid systems (ct-SHS) as formalized in the following definition.

▶ **Definition 1.** A continuous-time stochastic hybrid system (ct-SHS) in this work is characterized by the tuple

$$\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, \rho, Y_1, Y_2, h_1, h_2), \tag{1}$$

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 sets of all $\mathbb{F}$-progressively measurable processes taking values in $\mathbb{R}^m$ and $\mathbb{R}^p$;
- $f : X \times U \times W \to \mathbb{R}^n$ 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 $\mathscr{L}_\sigma$;

- $\rho : \mathbb{R}^n \to \mathbb{R}^{n\times \mathsf{r}}$ is the reset term which is globally Lipschitz continuous with the Lipschitz constant $\mathscr{L}_\rho$;
- $Y_1 \subseteq \mathbb{R}^{q_1}$ is the *external* output set of the system;
- $Y_2 \subseteq \mathbb{R}^{q_2}$ is the *internal* output set of the system;
- $h_1 : X \to Y_1$ is the *external* output map;
- $h_2 : X \to Y_2$ is the *internal* output map.

A continuous-time stochastic hybrid system Σ satisfies

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = f(\xi(t),\nu(t),w(t))\mathsf{d}t + \sigma(\xi(t))\mathsf{d}\mathbb{W}_t + \rho(\xi(t))\mathsf{d}\mathbb{P}_t, \\ \zeta_1(t) = h_1(\xi(t)), \\ \zeta_2(t) = h_2(\xi(t)), \end{cases} \tag{2}$$

$\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.) for any $\nu \in \mathcal{U}$ and any $w \in \mathcal{W}$, where stochastic processes $\xi : \Omega\times\mathbb{R}_{\geq 0} \to X$, $\zeta_1 : \Omega \times \mathbb{R}_{\geq 0} \to Y_1$, and $\zeta_2 : \Omega \times \mathbb{R}_{\geq 0} \to Y_2$ are, respectively, called the *solution process* and the external and internal *output trajectories* of Σ. We also use $\xi_{a\nu w}(t)$ to denote the value of the solution process at the 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 $\zeta_{1_{a\nu w}}$ and $\zeta_{2_{a\nu w}}$ the external and internal *output trajectories* corresponding to the *solution process* $\xi_{a\nu w}$. Here, we assume that the Poisson processes $\mathbb{P}^{\hat{z}}_s$, for any $\hat{z} \in \{1,\dots,\mathsf{r}\}$, have rates $\bar{\lambda}_{\hat{z}}$. We emphasize that the postulated assumptions on f, σ, and ρ ensure existence, uniqueness, and strong Markov property of the solution process [22].

Given the ct-SHS in (1), we are interested in Markov policies to control the system as defined in the next definition.

▶ **Definition 2.** A Markov policy for the ct-SHS Σ in (1) is a map $\varrho : \mathbb{B}(U) \times X \times \mathbb{R}_{\geq 0} \to [0,1]$, with $\mathbb{B}(U)$ being the Borel sigma-algebra on the external input space, such that $\varrho(\cdot \,|\, \cdot, t)$ is a universally measurable stochastic kernel for all $t \in \mathbb{R}_{\geq 0}$ [27]. For any state $x \in X$ at time t, the input $\nu(t)$ is chosen according to the probability measure $\varrho(\cdot \,|\, x, t)$.

Although we define continuous-time stochastic hybrid systems with outputs, we assume the full-state information is available for the sake of controller synthesis. The role of outputs are mainly for the sake of interconnecting systems as explained in detail in Section 4.

Given the main contribution of this work which is developing a compositional approach for the construction of control barrier certificates, we are ultimately interested in investigating interconnected systems without having internal signals. In this case, the tuple (1) reduces to $(X, U, \mathcal{U}, f, \sigma, \rho, Y, h)$ with $f : X \times U \to \mathbb{R}^n$, and ct-SHS (2) can be re-written as

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

In the next sections, we propose an approach for the compositional construction of control barrier certificates for interconnected ct-SHS. To do so, we define, in the next section, notions of control storage and barrier certificates for ct-SHS and interconnected versions, respectively.

3 Control Storage and Barrier Certificates

In this section, we first introduce a notion of control storage certificates (CSC) for ct-SHS with both internal and external signals. We then define a notion of control barrier certificates (CBC) for ct-SHS with only external signals. We leverage the former notion to compositionally construct the latter one for interconnected systems. We then employ the latter notion to quantify upper bounds on the probability that the interconnected system reaches certain unsafe regions in finite-time horizons.

▶ **Definition 3.** Consider a ct-SHS $\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, \rho, Y_1, Y_2, h_1, h_2)$. Let $X_0, X_1 \subseteq X$ 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 storage certificate (CSC) for Σ if there exist $\kappa \in \mathcal{K}_\infty$, $\gamma, \lambda, \psi \in \mathbb{R}_{\geq 0}$, and a symmetric matrix $\bar{X}$ with conformal block partitions $\bar{X}^{z\bar{z}}$, $z, \bar{z} \in \{1, 2\}$, where $\bar{X}^{22} \preceq 0$, such that

- $\forall x \in X_0$,

$$\mathcal{B}(x) \leq \gamma, \tag{3}$$

- $\forall x \in X_1$,

$$\mathcal{B}(x) \geq \lambda, \tag{4}$$

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

$$\mathcal{L}\mathcal{B}(x) \leq -\kappa(\mathcal{B}(x)) + \psi + \begin{bmatrix} w \\ h_2(x) \end{bmatrix}^T \underbrace{\begin{bmatrix} \bar{X}^{11} & \bar{X}^{12} \\ \bar{X}^{21} & \bar{X}^{22} \end{bmatrix}}_{\bar{X} :=} \begin{bmatrix} w \\ h_2(x) \end{bmatrix}, \tag{5}$$

where $\mathcal{L}\mathcal{B}$ is the *infinitesimal generator* of the stochastic process acting on the function $\mathcal{B}$ [21], as defined in the next remark.

▶ Remark 1. Note that the *infinitesimal generator* $\mathcal{L}$ of the process $\xi(t)$ acting on the function $\mathcal{B} : X \to R_{\geq 0}$ is defined as

$$\mathcal{L}\mathcal{B}(x) = \partial_x \mathcal{B}(x) f(x, \nu, w) + \frac{1}{2} \mathsf{Tr}(\sigma(x)\sigma(x)^T \partial_{x,x} \mathcal{B}(x)) + \sum_{j=1}^{\mathsf{r}} \bar{\lambda}_j (\mathcal{B}(x + \rho(x)\mathsf{e}^{\mathsf{r}}_j) - \mathcal{B}(x)), \tag{6}$$

where $\partial_x \mathcal{B}(x) = \left[\frac{\partial \mathcal{B}(x)}{\partial x_i}\right]_i$ is a row vector, $\partial_{x,x} \mathcal{B}(x) = \left[\frac{\partial^2 \mathcal{B}(x)}{\partial x_i \partial x_j}\right]_{i,j}$, $\bar{\lambda}_j$ is the rate of Poisson process, and $\mathsf{e}^{\mathsf{r}}_j$ denotes an r-dimensional vector with 1 on the j-th entry and 0 elsewhere.

▶ Remark 2. Since the control input ν in condition (5) is independent of internal inputs w (*i.e.,* state information of other subsystems), the employed quantifier in (5) implicitly implies that one can synthesize *decentralized* controllers for Σ . However, one can design *distributed* control policies by changing the sequence of the quantifier in (5) to $\forall x \in X, \forall w \in W, \exists \nu \in U$. In this case, the chance of finding control storage certificates gets increased; however, one needs to measure the state information of other subsystems to deploy the synthesized controllers.

▶ Remark 3. Note that a local storage certificate captures the role of w (*i.e.,* the effect of interaction between subsystems in the interconnected topology) using the quadratic term in the right-hand side of (5). This term is interpreted in dissipativity theory as the supply rate of the system [3] which is initially used to show the stability of a network based on stabilities of its subsystems. Here, we choose this function to be quadratic which results in tractable compositional conditions later in the form of linear matrix inequalities (cf. (13)).

Now we modify the above notion for the interconnected ct-SHS without internal signals. This notion will be utilized in Theorem 5 for quantifying upper bounds on the probability that the interconnected system (without internal signals) reaches certain unsafe regions in a finite-time horizon.

▶ **Definition 4.** Consider the (interconnected) system $\Sigma = (X, U, \mathcal{U}, f, \sigma, \rho, Y, h)$, and $X_0, X_1 \subseteq X$ as respectively initial and unsafe sets of the interconnected system. A twice differentiable function $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ is called a control barrier certificate (CBC) for Σ if

- $\forall x \in X_0$,

$$\mathcal{B}(x) \leq \gamma \tag{7}$$

- $\forall x \in X_1$,

$$\mathcal{B}(x) \geq \lambda \tag{8}$$

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

$$\mathcal{L}\mathcal{B}(x) \leq -\kappa(\mathcal{B}(x)) + \psi, \tag{9}$$

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

▶ Remark 4. Note that stochastic storage certificates satisfying conditions (3)-(5) are not useful on their own to ensure the safety of the corresponding subsystems and the interconnected system as a whole. Stochastic storage certificates are some appropriate tools used to construct overall control barrier certificates given that some compositionality conditions are satisfied (cf. (13),(14)). The safety of the system can then be verified via Theorem 5 only using the constructed control barrier certificate.

The next theorem shows the usefulness of CBC to quantify upper bounds on the probability that the interconnected system reaches certain unsafe regions in a finite-time horizon.

▶ **Theorem 5.** *Let $\Sigma = (X, U, \mathcal{U}, f, \sigma, \rho, Y, h)$ be an (interconnected) ct-SHS without internal signals. Suppose $\mathcal{B}$ is a CBC for Σ as in Definition 4, and there exists a constant $\hat{\kappa} \in \mathbb{R}_{>0}$ such that the function $\kappa \in \mathcal{K}_\infty$ in (9) 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_1 under the policy $\nu(\cdot)$ within a time horizon $[0, T_d] \subseteq \mathbb{R}_{\geq 0}$ is formally quantified as*

$$\mathbb{P}_\nu^{x_0}\Big\{\xi(t) \in X_1 \text{ for some } 0 \leq t \leq T_d \;\Big|\; \xi(0) = x_0\Big\} \leq \begin{cases} 1 - (1 - \frac{\gamma}{\lambda})e^{-\frac{\psi T_d}{\lambda}}, & \text{if } \lambda \geq \frac{\psi}{\hat{\kappa}}, \\ \frac{\hat{\kappa}\gamma + (e^{\hat{\kappa} T_d} - 1)\psi}{\hat{\kappa}\lambda e^{\hat{\kappa} T_d}}, & \text{if } \lambda \leq \frac{\psi}{\hat{\kappa}}. \end{cases} \tag{10}$$

The proof of Theorem 5 is provided in Appendix.

▶ Remark 5. In Section 5, we reformulate conditions of Definition 4 as an optimization problem such that one can minimize values of γ and ψ in order to obtain a better upper bound that is as tight as possible.

In the next section, we analyze networks of stochastic hybrid subsystems and show under which conditions one can construct a CBC of an interconnected system utilizing the corresponding CSC of subsystems.

4 Compositional Construction of CBC

In this section, we analyze networks of stochastic hybrid subsystems, $i \in \{1, \ldots, N\}$,

$$\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, \rho_i, Y_{1_i}, Y_{2_i}, h_{1_i}, h_{2_i}), \tag{11}$$

and discuss how to construct a CBC of the interconnected system based on CSC of subsystems using dissipativity-type compositional conditions. We first formally define the interconnected stochastic hybrid systems.

▶ **Definition 6.** Consider $N \in \mathbb{N}$ stochastic hybrid subsystems $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, \rho_i, Y_{1_i}, Y_{2_i}, h_{1_i}, h_{2_i})$, $i \in \{1, \dots, N\}$, and a matrix M defining the coupling between these subsystems. We require the condition $M \prod_{i=1}^{N} Y_{2i} \subseteq \prod_{i=1}^{N} W_i$ to have a well-posed interconnection. The interconnection of Σ_i, $\forall i \in \{1, \dots, N\}$, is the ct-SHS $\Sigma = (X, U, \mathcal{U}, f, \sigma, Y, h)$, denoted by $\mathcal{I}(\Sigma_1, \dots, \Sigma_N)$, such that $X := \prod_{i=1}^{N} X_i$, $U := \prod_{i=1}^{N} U_i$, $f := \prod_{i=1}^{N} f_i$, $\sigma := \mathsf{blkdiag}(\sigma_1(x_1), \dots, \sigma_N(x_N))$, $\rho := \mathsf{blkdiag}(\rho_1(x_1), \dots, \rho_N(x_N))$, $Y := \prod_{i=1}^{N} Y_{1i}$, and $h = \prod_{i=1}^{N} h_{1i}$, with the internal inputs constrained according to

$$[w_1; \cdots; w_N] = M[h_{21}(x_1); \cdots; h_{2N}(x_N)].$$

We assume that for hybrid subsystems $\Sigma_i, i \in \{1, \dots, N\}$, there exist CSC $\mathcal{B}_i$ as defined in Definition 3 with the corresponding functions, constant, and matrices denoted by $\kappa_i \in \mathcal{K}_\infty$, $\gamma_i, \lambda_i, \psi_i \in \mathbb{R}_{\geq 0}$, $\bar{X}_i$, $\bar{X}_i^{11}$, $\bar{X}_i^{12}$, $\bar{X}_i^{21}$, and $\bar{X}_i^{22}$. In the next theorem, we compositionally construct a control barrier certificate for the interconnected system Σ as in Definition 4.

▶ **Theorem 7.** *Consider an interconnected stochastic hybrid system $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ induced by $N \in \mathbb{N}$ stochastic hybrid subsystems Σ_i and the coupling matrix M. Suppose that each subsystem Σ_i admits a CSC $\mathcal{B}_i$ as defined in Definition 3 with the corresponding initial and unsafe sets X_{0_i} and X_{1_i}, respectively. Then*

$$\mathcal{B}(x) := \sum_{i=1}^{N} \mu_i \mathcal{B}_i(x_i) \tag{12}$$

is a CBC for the interconnected system $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ with the corresponding initial and unsafe sets $X_0 := \prod_{i=1}^{N} X_{0_i}$, $X_1 := \prod_{i=1}^{N} X_{1_i}$, respectively, if there exist $\mu_i > 0$, $i \in \{1, \dots, N\}$, such that

$$\begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}} \end{bmatrix}^T \bar{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}} \end{bmatrix} \preceq 0, \tag{13}$$

$$\sum_{i=1}^{N} \mu_i \lambda_i > \sum_{i=1}^{N} \mu_i \gamma_i, \tag{14}$$

where

$$\bar{X}_{cmp} := \begin{bmatrix} \mu_1 \bar{X}_1^{11} & & & \mu_1 \bar{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N \bar{X}_N^{11} & & & \mu_N \bar{X}_N^{12} \\ \mu_1 \bar{X}_1^{21} & & & \mu_1 \bar{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N \bar{X}_N^{21} & & & \mu_N \bar{X}_N^{22} \end{bmatrix}, \tag{15}$$

and $\tilde{q} = \sum_{i=1}^{N} q_{2i}$ with q_{2i} being dimensions of the internal *output of subsystems Σ_i.*

The proof of Theorem 7 is provided in Appendix.

▶ Remark 6. Condition (13) is similar to the LMI appeared in [3] as a compositional stability condition based on the dissipativity theory. It is shown in [3] that this condition holds independently of the number of subsystems in many physical applications with particular interconnection topologies, *e.g.,* skew symmetric.

▶ Remark 7. Note that the condition (14) in general is not very restrictive since constants μ_i in (12) play a significant role in rescaling CSC for subsystems while normalizing the effect of internal gains of other subsystems. One can expect that condition (14) holds in many applications due to this rescaling.

5 Computation of CSC

In this section, we formulate the proposed conditions in Definition 3 as a sum-of-squares (SOS) optimization problem [24] and provide a systematic approach for computing CSC and corresponding control policies for subsystems Σ_i. The SOS optimization 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 1. 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 $f_i : X_i \times U_i \times W_i \to \mathbb{R}^{n_i}$ is a polynomial function of the state x_i and external and internal inputs ν_i, w_i. Furthermore, diffusion and reset terms $\sigma_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i \times \mathsf{b}_i}$ and $\rho_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i \times \mathsf{r}_i}$ are polynomial functions of the state x_i.

Under Assumption 1, one can reformulate the proposed conditions in Definition 3 as an SOS optimization problem to search for a polynomial CSC $\mathcal{B}_i(\cdot)$, and a polynomial control policy $\nu_i(\cdot)$. The following lemma provides a set of sufficient conditions for the existence of such CSC required in Definition 3, which can be solved now as an SOS optimization problem.

▶ **Lemma 8.** *Suppose Assumption 1 holds and sets $X_{0_i}, X_{1_i}, X_i, U_i, W_i$ can be defined by vectors of polynomial inequalities $X_{0_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{0_i}(x_i) \geq 0\}$, $X_{1_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{1_i}(x_i) \geq 0\}$, $X_i = \{x_i \in \mathbb{R}^{n_i} \mid g_i(x_i) \geq 0\}$, $U_i = \{\nu_i \in \mathbb{R}^{m_i} \mid g_{\nu_i}(\nu_i) \geq 0\}$, 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 exist a sum-of-square polynomial $\mathcal{B}_i(x_i)$, constants $\gamma_i, \lambda_i, \psi_i \in \mathbb{R}_{\geq 0}$, functions $\kappa_i \in \mathcal{K}_\infty$, a symmetric matrix $\bar{X}_i$ with conformal block partitions $\bar{X}_i^{z\bar{z}}$, $z, \bar{z} \in \{1, 2\}$, where $\bar{X}_i^{22} \preceq 0$, polynomials $l_{\nu_{ji}}(x)$ 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 $l_{0_i}(x_i)$, $l_{1_i}(x_i)$, $l_i(x_i, \nu_i, w_i)$, $l_{\nu_i}(x_i, \nu_i, w_i)$, and $l_{w_i}(x_i, \nu_i, w_i)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$-\mathcal{B}_i(x_i) - l_{0_i}^T(x_i) g_{0_i}(x_i) + \gamma_i \tag{16}$$

$$\mathcal{B}_i(x_i) - l_{1_i}^T(x_i) g_{1_i}(x_i) - \lambda_i \tag{17}$$

$$\begin{aligned} &-\mathcal{L}\mathcal{B}_i(x_i) - \kappa_i(\mathcal{B}_i(x_i)) + \begin{bmatrix} w_i \\ h_{2_i}(x_i) \end{bmatrix}^T \begin{bmatrix} \bar{X}_i^{11} & \bar{X}_i^{12} \\ \bar{X}_i^{21} & \bar{X}_i^{22} \end{bmatrix} \begin{bmatrix} w_i \\ h_{2_i}(x_i) \end{bmatrix} \\ &+ \psi_i - \sum_{j=1}^{m_i} (\nu_{ji} - l_{\nu_{ji}}(x_i)) - l_i^T(x_i, \nu_i, w_i) g_i(x_i) - l_{\nu_i}^T(x_i, \nu_i, w_i) g_{\nu_i}(\nu_i) - l_{w_i}^T(x_i, \nu_i, w_i) g_{w_i}(w_i). \end{aligned} \tag{18}$$

Then, $\mathcal{B}_i(x_i)$ satisfies conditions (3)-(5) 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.

The proof of Lemma 8 is provided in Appendix.

▶ Remark 8. Note that function $\kappa_i(\cdot)$ in (18) can cause nonlinearity on unknown parameters of $\mathcal{B}_i$. A possible way to avoid this issue is to consider a linear function $\kappa_i(s) = \hat{\kappa}_i s, \forall s \in \mathbb{R}_{\geq 0}$, with some given constant $\hat{\kappa}_i \in \mathbb{R}_{>0}$. Then one can employ bisection method to minimize the value of $\hat{\kappa}_i$.

▶ Remark 9. Note that for computing the sum-of-squares polynomial $\mathcal{B}_i(x_i)$ fulfilling reformulated conditions (16)-(18), one can readily employ existing software tools available in the literature such as SOSTOOLS [23] together with a semi-definite programming (SDP) solver such as SeDuMi [28].

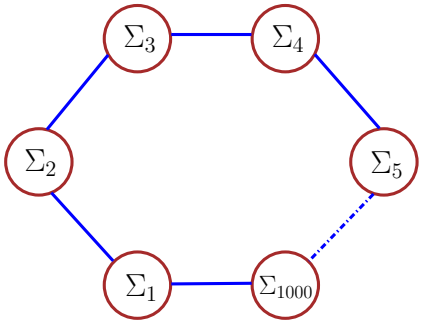

Figure 1 A circular building in a network of 1000 rooms.

6 Case Studies

6.1 Room Temperature Network

To illustrate the effectiveness of the proposed results, we first apply our approaches to a temperature regulation in a network of 1000 rooms, each equipped with a heater and connected circularly as depicted in Figure 1. We compute the CSC 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 borrowed from [6] by including stochasticity in the model. The evolution of the temperature $T(\cdot)$ can be described by the interconnected jump-diffusion

$$\Sigma : \begin{cases} \mathsf{d}T(t) = (AT(t) + \theta T_h \nu(t) + \beta T_E)\mathsf{d}t + G\mathsf{d}\mathbb{W}_t + R\mathsf{d}\mathbb{P}_t, \\ \zeta(t) = T(t), \end{cases}$$

where A is a matrix with diagonal elements $a_{ii} = -2\eta - \beta - \theta\nu_i(t)$, $i \in \{1, \dots, n\}$, off-diagonal elements $a_{i,i+1} = a_{i+1,i} = a_{1,n} = a_{n,1} = \eta$, $i \in \{1, \dots, n-1\}$, and all other elements are identically zero. Parameters $\eta = 0.005$, $\beta = 0.06$, and $\theta = 0.156$ are conduction factors, respectively, between rooms $i \pm 1$ and i, the external environment and the room i, and the heater and the room i. Moreover, $G = R = 0.1\mathbb{I}_n$, $T_E = [T_{e_1}; \dots; T_{e_n}]$, $T(t) = [T_1(t); \dots; T_n(t)]$, and $\nu(t) = [\nu_1(t); \dots; \nu_n(t)]$. Outside temperatures are the same for all rooms: $T_{ei} = -15\,^\circ\mathsf{C}$, $\forall i \in \{1, \dots, n\}$, and the heater temperature is $T_h = 48\,^\circ\mathsf{C}$. We consider the rates of Poisson processes as $\bar{\lambda}_i = 0.1, \forall i \in \{1, \dots, n\}$. Now by considering the individual rooms as Σ_i described by

$$\Sigma_i : \begin{cases} \mathsf{d}T_i(t) = (a_{ii}T_i(t) + \theta T_h \nu_i(t) + \eta w_i(t) + \beta T_{e_i})\mathsf{d}t + 0.1\mathsf{d}\mathbb{W}_{t_i} + 0.1\mathsf{d}\mathbb{P}_{t_i}, \\ \zeta_{1_i}(t) = T_i(t), \\ \zeta_{2_i}(t) = T_i(t), \end{cases} \tag{19}$$

one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ where the coupling matrix M is defined as $m_{i,i+1} = m_{i+1,i} = m_{1,n} = m_{n,1} = 1$, $i \in \{1, \dots, n-1\}$, and all other elements are identically zero.

The regions of interest in this example are $X_i = [1\ 50]$, $X_{0_i} = [19.5\ 20]$, $X_{1_i} = [1\ 17] \cup [23\ 50]$, $\forall i \in \{1, \dots, n\}$. The main goal is to find a CBC for the interconnected system, using which a safety controller is synthesized for Σ maintaining the temperatures of rooms in the comfort zone $W = [17\ 23]^{1000}$. The idea here is to search for CSC 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 subsystem Σ_i. We employ the software tool SOSTOOLS [23] and the SDP solver SeDuMi [28] to compute CSC as described in Section 5. According to Lemma 8, we compute CSC of order 2 as $\mathcal{B}_i(T_i) = 0.3112T_i^2 - 12.3035T_i + 121.59906$

and the corresponding safety controller $\nu_i(T_i) = -0.0120155T_i + 0.7$ for all $i \in \{1, \ldots, n\}$. Moreover, the corresponding constants and functions in Definition 3 satisfying conditions (3)-(5) are quantified as $\gamma_i = 0.08, \lambda_i = 2.7, \kappa_i(s) = \hat{\kappa}_i s, \forall s \in \mathbb{R}_{\geq 0}$ with $\hat{\kappa}_i = 10^{-7}, \psi_i = 5 \times 10^{-3}$, and

$$\bar{X}_i = \begin{bmatrix} \hat{\kappa}_i e^{-4}\eta^2 & 0 \\ 0 & -\hat{\kappa}_i e^{-4}\theta^2 T_h^2 \end{bmatrix}. \tag{20}$$

We now proceed with Theorem 7 to construct a CBC for the interconnected system using CSC of subsystems. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, n\}$, and utilizing $\bar{X}_i$ in (20), the matrix $\bar{X}_{cmp}$ in (15) reduces to

$$\bar{X}_{cmp} = \begin{bmatrix} \hat{\kappa}_i e^{-4}\eta^2 \mathbb{I}_n & 0 \\ 0 & -\hat{\kappa}_i e^{-4}\theta^2 T_h^2 \mathbb{I}_n \end{bmatrix},$$

and condition (13) is reduced to

$$\begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix}^T \bar{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix} = \hat{\kappa}_i e^{-4}\eta^2 M^T M - \hat{\kappa}_i e^{-4}\theta^2 T_h^2 \mathbb{I}_n \preceq 0,$$

without requiring any restrictions on the number or gains of subsystems. We used $M = M^T$, and $4\hat{\kappa}_i e^{-4}\eta^2 - \hat{\kappa}_i e^{-4}\theta^2 T_h^2 \preceq 0$ by employing Gershgorin circle theorem [4] to show the above LMI. Moreover, the compositionality condition (14) is also met since $\lambda_i > \gamma_i, \forall i \in \{1, \ldots, n\}$. Then by employing the results of Theorem 7, one can conclude that $\mathcal{B}(T) = \sum_{i=1}^{1000}(0.3112T_i^2 - 12.3035T_i + 121.59906)$ is a CBC for the interconnected system Σ with $\gamma = 80, \lambda = 2700, \kappa(s) = 10^{-7}s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = 5$. Accordingly, $\nu(T) = [-0.0120155T_1 + 0.7; \ldots; -0.0120155T_{1000} + 0.7]$ is the overall safety controller for the interconnected system.

By employing Theorem 5, one can guarantee that the temperature of the interconnected system Σ starting from initial conditions inside $X_0 = [19.5\ 20]^{1000}$ remains in the safe set $[17\ 23]^{1000}$ during the time horizon $T_d = 10$ with the probability of at least 96%, *i.e.,*

$$\mathbb{P}_\nu^{x_0}\Big\{\xi(t) \notin X_1 \mid \xi(0) = x_0,\ \forall t \in [0, 10]\Big\} \geq 0.96\,. \tag{21}$$

Closed-loop state trajectories of a representative room with 10 different noise realizations are illustrated in Figure 2.

With the assumption that all dynamics and barrier certificates are polynomial types, the computational complexity of using SOS in our setting is linear with respect to the number of subsystems. Whereas, if one is interested in solving the problem in a monolithic manner, the complexity will be polynomial in terms of the number of subsystems [30]. In the worst-case scenario, the computational complexity in the monolithic manner will be exponential in terms of the number of subsystems if the underlying dynamics and barrier certificates are not polynomial.

Importance of Compositionality Conditions. In order to demonstrate the importance of the compositionality conditions, we raise the following counter example. Consider a network of *two rooms* each equipped with a heater and connected circularly, as illustrated in Figure 3, with dynamics as in (19) with $T_{e_i} = -100, \forall i \in \{1, 2\}$. One can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \Sigma_2)$ where the coupling matrix M is defined as $M = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Let regions of interest be the same as before. We compute CSC of order 2 as $\mathcal{B}_i(T_i) = 0.76484T_i^2 - 30.18033T_i + 297.73079$ and its corresponding controller $\nu_i(T_i) = 0.0120155T_i + 0.7$ for all $i \in \{1, 2\}$, with

$$\bar{X}_i = \begin{bmatrix} 4 \times 10^{-4} & 20 \\ 20 & 5 \times 10^{-4} \end{bmatrix}.$$

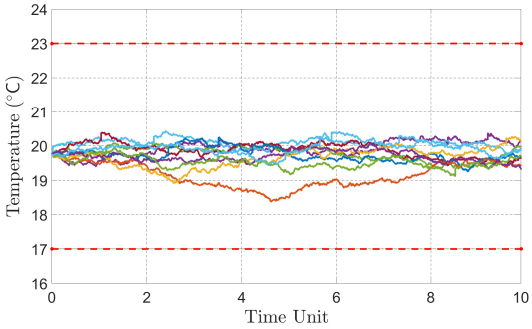

Figure 2 Closed-loop state trajectories of a representative room with 10 noise realizations in a network of 1000 rooms.

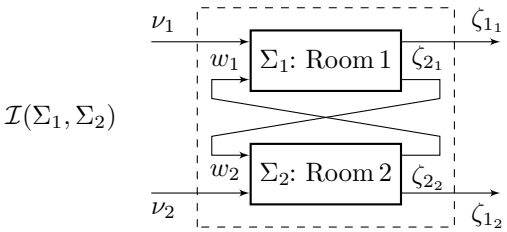

Figure 3 Interconnection of two rooms Σ_1 and Σ_2.

We now select $\mu_i = 1, \forall i \in \{1, 2\}$, and construct the matrix $\bar{X}_{cmp}$ in (15) as

$$\bar{X}_{cmp} = \begin{bmatrix} 4 \times 10^{-4} & 0 & 20 & 0 \\ 0 & 4 \times 10^{-4} & 0 & 20 \\ 20 & 0 & 5 \times 10^{-4} & 0 \\ 0 & 20 & 0 & 5 \times 10^{-4} \end{bmatrix}.$$

Now we check the compositionality condition in (13) as

$$\begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix}^T \bar{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix} \not\succeq 0,$$

with eigenvalues equal to -39.9991 and 40.0009. Since the compositionality condition is violated, one cannot automatically conclude that $\mathcal{B}(T) = \mathcal{B}_1(T_1) + \mathcal{B}_2(T_2)$ is a barrier certificate for the overall system. To show this issue, we employ $\mathcal{B}(T) = 0.76484T_1^2 - 30.18033T_1 + 297.73079 + 0.76484T_2^2 - 30.18033T_2 + 297.73079$ and check the corresponding conditions for the overall barrier certificate (*i.e.,* conditions (7)-(9)) with $\gamma = \gamma_1 + \gamma_2, \lambda = \lambda_1 + \lambda_2, \psi = \psi_1 + \psi_2$. As it can be observed from Figures 4-6, although conditions (7),(8) are satisfied for the overall barrier certificates $\mathcal{B}(T) = \mathcal{B}_1(T_1) + \mathcal{B}_2(T_2)$, condition (9) is violated since it is positive at some ranges of $X_1 \times X_2$.

Then one can readily verify that $\mathcal{B}(T) = \mathcal{B}_1(T_1) + \mathcal{B}_2(T_2)$ is not necessarily a barrier certificate for the overall network ensuring its safety even though all the rooms are the same and storage certificates are input independent.

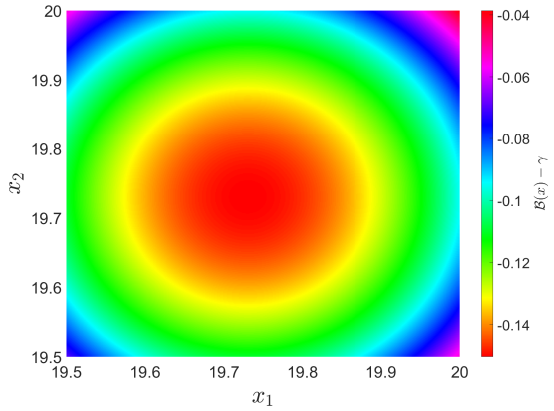

Figure 4 Satisfaction of condition (7). As observed, this condition is negative for all ranges of $x_1 \in X_{0_1}$ and $x_2 \in X_{0_2}$.

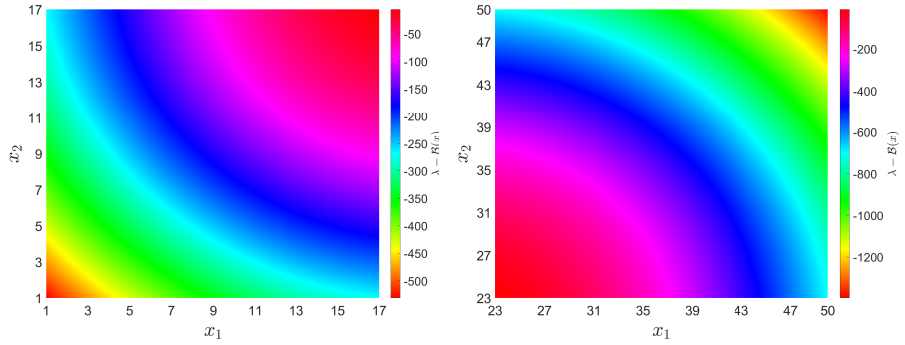

Figure 5 Satisfaction of condition (8). The condition is negative for all ranges of $x_1 \in X_{1_1}$ and $x_2 \in X_{1_2}$.

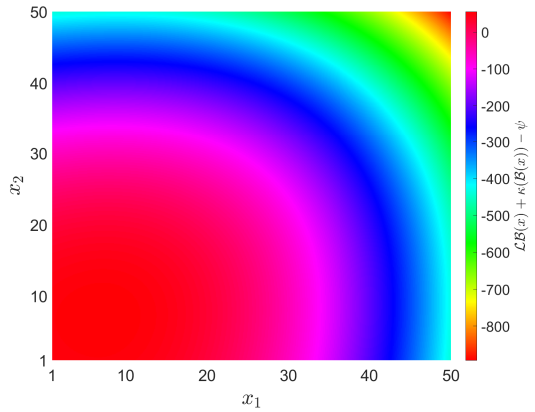

Figure 6 Violation of condition (9). As observed, this condition is positive for some ranges of $x_1 \in X_1$ and $x_2 \in X_2$.

6.2 Fully-Interconnected Network

To show the applicability of our approach to strongly connected networks, we consider interconnected linear ct-SHS

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = (\bar{G}\xi(t) + B\nu(t))\mathsf{d}t + G\mathsf{d}\mathbb{W}_t + R\mathsf{d}\mathbb{P}_t, \\ \zeta(t) = \xi(t), \end{cases}$$

with matrix $\bar{G} = (-I_n - L) \in \mathbb{R}^{n\times n}$, where L is the Laplacian matrix of a complete graph [7]:

$$L = \begin{bmatrix} n-1 & -1 & \cdots & \cdots & -1 \\ -1 & n-1 & -1 & \cdots & -1 \\ -1 & -1 & n-1 & \cdots & -1 \\ \vdots & & \ddots & \ddots & \vdots \\ -1 & \cdots & \cdots & -1 & n-1 \end{bmatrix}_{n\times n}.$$

We partition $\xi(t) = [\xi_1(t); \ldots; \xi_n(t)]$, and $\nu(t) = [\nu_1(t); \ldots; \nu_n(t)]$. Moreover, $B = 0.15\mathbb{I}_n$ and $G = R = 0.1\mathbb{I}_n$. We also consider rates of Poisson processes as $\bar{\lambda}_i = 0.1, \forall i \in \{1, \ldots, n\}$. Now by considering the individual subsystems as

$$\Sigma_i : \begin{cases} \mathsf{d}\xi_i(t) = (-\xi_i(t) + 0.15\nu_i(t) + w_i(t))\mathsf{d}t + 0.1\mathsf{d}\mathbb{W}_{t_i} + 0.1\mathsf{d}\mathbb{P}_{t_i}, \\ \zeta_{1_i}(t) = \xi_i(t), \\ \zeta_{2_i}(t) = \xi_i(t), \end{cases}$$

one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ where the coupling matrix M is defined as $M = -L$.

The regions of interest in this example are $X_i = [2\ 6], X_{0_i} = [2\ 4], X_{1_i} = [5\ 6], \forall i \in \{1, \ldots, n\}$. For the sake of simulation, we fix $n = 15$. The main goal is to find a CBC for the interconnected system and design its corresponding safety controller Σ maintaining the state of the interconnected system in the safe set $W = [2\ 5]^{15}$. According to Lemma 8, we compute CSC of order 4 as $\mathcal{B}_i(x_i) = 0.0002x_i^4 - 0.0024x_i^3 + 0.0109x_i^2 - 0.0207x_i + 0.0146$ and the corresponding safety controller $\nu_i(x_i) = -5.1465x_i^2 + 60.3564$ for all $i \in \{1, \ldots, 15\}$. The corresponding constants and functions in Definition 3 satisfying conditions (3)-(5) are computed as $\gamma_i = 10^{-4}, \lambda_i = 2 \times 10^{-3}, \kappa_i(s) = \hat{\kappa}_i s, \forall s \in \mathbb{R}_{\geq 0}$ with $\hat{\kappa}_i = 10^{-7}, \psi_i = 10^{-6}$, and

$$\bar{X}_i = \begin{bmatrix} 10^{-6} & 10^{-2} \\ 10^{-2} & -5 \times 10^{-4} \end{bmatrix}. \tag{22}$$

We now proceed with Theorem 7 to construct a CBC for the interconnected system using CSC of subsystems. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, n\}$, and utilizing $\bar{X}_i$ in (22), the matrix $\bar{X}_{cmp}$ in (15) is reduced to

$$\bar{X}_{cmp} = \begin{bmatrix} 10^{-6}\mathbb{I}_n & 10^{-2}\mathbb{I}_n \\ 10^{-2}\mathbb{I}_n & -5 \times 10^{-4}\mathbb{I}_n \end{bmatrix},$$

and condition (13) is reduced to

$$\begin{bmatrix} -L \\ \mathbb{I}_n \end{bmatrix}^T \bar{X}_{cmp} \begin{bmatrix} -L \\ \mathbb{I}_n \end{bmatrix} = 10^{-6}L^TL - 10^{-2}(L + L^T) - 5 \times 10^{-4}\mathbb{I}_n \preceq 0,$$

which is always satisfied without requiring any restrictions on the number or gains of subsystems. In order to show the above LMI, we used $L = L^T \succeq 0$ which is always true for Laplacian matrices of undirected graphs. Moreover, the compositionality condition (14) is also satisfied since $\lambda_i > \gamma_i, \forall i \in \{1, \ldots, n\}$. Then by employing Theorem 7, one can conclude that $\mathcal{B}(x) =$

$\sum_{i=1}^{15}(0.0002x_i^4 - 0.0024x_i^3 + 0.0109x_i^2 - 0.0207x_i + 0.0146)$ is a CBC for the interconnected system Σ with $\gamma = 0.0015, \lambda = 0.03, \kappa(s) = 10^{-7}s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = 1.5 \times 10^{-5}$. Accordingly, $\nu(x) = [-5.1465x_1^2 + 60.3564; \ldots; -5.1465x_{15}^2 + 60.3564]$ is the overall safety controller for the interconnected system.

By leveraging Theorem 5, one can guarantee that the state of the interconnected system Σ starting from initial conditions inside $X_0 = [2\ 4]^{15}$ remains in the safe set $[2\ 5]^{15}$ during the time horizon $T_d = 10$ with the probability of at least 95%, *i.e.,*

$$\mathbb{P}_\nu^{x_0}\Big\{\xi(t) \notin X_1 \mid \xi(0) = x_0,\ \forall t \in [0, 10]\Big\} \geq 0.95\,.$$

Closed-loop state trajectories of a representative subsystem with 10 different noise realizations are illustrated in Figure 7.

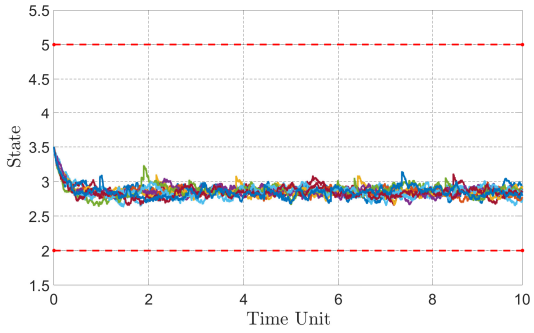

Figure 7 Closed-loop state trajectories of a representative subsystem with 10 noise realizations.

7 Conclusion

In this work, we proposed a compositional scheme based on dissipativity approaches for constructing control barrier certificates of large-scale continuous-time continuous-space stochastic hybrid systems while providing upper bounds on the probability that interconnected systems reach certain unsafe regions in finite-time horizons. The main goal was to synthesize control policies satisfying safety properties for interconnected systems by utilizing control storage certificates of subsystems. We constructed control barrier certificates for interconnected stochastic systems using control storage certificates of subsystems as long as some dissipativity-type compositional conditions hold. We employed a systematic approach based on the sum-of-squares optimization program and computed control storage certificates of subsystems. We illustrated our proposed results on two case studies with circular and fully-interconnected topologies.

References

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

2 M. Anand, A. Lavaei, and M. Zamani. Compositional construction of control barrier certificates for large-scale interconnected stochastic systems. *Proceedings of the 21st IFAC World Congress*, 53(2):1862–1867, 2020.

3 M. Arcak, C. Meissen, and A. Packard. *Networks of dissipative systems*. SpringerBriefs in Electrical and Computer Engineering. Springer, 2016.

4 H. E. Bell. Gershgorin's theorem and the zeros of polynomials. *The American Mathematical Monthly*, 72(3):292–295, 1965.

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

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

7 C. Godsil and G. Royle. *Algebraic graph theory*. Graduate Texts in Mathematics. Springe, 2001.

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

9 P. Jagtap, S. Soudjani, and M. Zamani. Formal synthesis of stochastic systems via control barrier certificates. *IEEE Transactions on Automatic Control*, 66(7):3097–3110, 2020.

10 H. J. Kushner. *Stochastic Stability and Control*. Mathematics in Science and Engineering. Elsevier Science, 1967.

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

12 A. Lavaei, S. Soudjani, A. Abate, and M. Zamani. Automated verification and synthesis of stochastic hybrid systems: A survey. *Automatica*, 2022.

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

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

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

16 A. Lavaei, S. Soudjani, and M. Zamani. Compositional (in)finite abstractions for large-scale interconnected stochastic systems. *IEEE Transactions on Automatic Control*, 65(12):5280–5295, 2020.

17 A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier certificates for large-scale stochastic switched systems. *IEEE Control Systems Letters*, 4(4):845–850, 2020.

18 A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier functions for networks of continuous-time stochastic systems. *Proceedings of the 21st IFAC World Congress*, 53(2):1856–1861, 2020.

19 A. Nejati, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis for continuous-time stochastic hybrid systems. *European Journal of Control*, 57:82–94, 2021.

20 A. Nejati and M. Zamani. Compositional construction of finite MDPs for continuous-time stochastic systems: A dissipativity approach. *Proceedings of the 21st IFAC World Congress*, 53(2):1962–1967, 2020.

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

22 B. K. Øksendal and A. Sulem. *Applied stochastic control of jump diffusions*, volume 498. Springer, 2005.

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

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

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

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

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

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

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

30 T. Wongpiromsarn, U. Topcu, and A. Lamperski. Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems. *IEEE Transactions on Automatic Control*, 61(11):3344–3355, 2015.

8 Appendix

Proof of Theorem 5. Based on condition (8), we have $X_1 \subseteq \{x \in X \mid \mathcal{B}(x) \geq \lambda\}$. Then one has

$$\mathbb{P}_{\nu}^{x_0}\Big\{\xi(t) \in X_1 \text{ for some } 0 \leq t \leq T_d \mid \xi(0) = x_0\Big\} \leq \mathbb{P}_{\nu}^{x_0}\Big\{\sup_{0\leq t\leq T_d} \mathcal{B}(\xi(t)) \geq \lambda \mid \xi(0) = x_0\Big\}. \tag{23}$$

One can acquire the upper bound in (10) by applying [10, Theorem 1, Chapter III] to (23) and respectively utilizing conditions (9) and (7). ◀

Proof of Theorem 7. We first show that conditions (7) and (8) in Definition 4 hold. For any $x := [x_1; \ldots; x_N] \in X_0 = \prod_{i=1}^{N} X_{0_i}$ and from (3)

$$\mathcal{B}(x) = \sum_{i=1}^{N} \mu_i \mathcal{B}_i(x_i) \leq \sum_{i=1}^{N} \mu_i \gamma_i = \gamma,$$

and similarly for any $x := [x_1; \ldots; x_N] \in X_1 = \prod_{i=1}^{N} X_{1_i}$ and from (4)

$$\mathcal{B}(x) = \sum_{i=1}^{N} \mu_i \mathcal{B}_i(x_i) \geq \sum_{i=1}^{N} \mu_i \lambda_i = \lambda,$$

satisfying conditions (7) and (8) with $\gamma = \sum_{i=1}^{N} \mu_i \gamma_i$ and $\lambda = \sum_{i=1}^{N} \mu_i \lambda_i$. Note that $\lambda > \gamma$ according to (14). Now, we show that the condition (9) holds, as well. One can obtain the chain of inequalities in (24) using condition (13) and by defining $\kappa(\cdot), \psi$ as

$$\kappa(s) := \min \Big\{ \sum_{i=1}^{N} \mu_i \kappa_i(s_i) \;\Big|\; s_i \geq 0,\ \sum_{i=1}^{N} \mu_i s_i = s \Big\},$$
$$\psi := \sum_{i=1}^{N} \mu_i \psi_i.$$

Then $\mathcal{B}$ is a CBC for Σ, which completes the proof. ◀

Proof of Lemma 8. Since condition (16) is sum-of-squares, we have $0 \leq \mathcal{B}_i(x_i) - l_{0_i}^T(x_i) g_i(x_i) - \gamma_i$. Since the term $l_{0_i}^T(x_i) g_{0_i}(x_i)$ is non-negative over X_0, the new condition (16) implies the condition (3) in Definition 3. Similarly, one can show that (17) implies condition (4) in Definition 3. Now we show that condition (18) implies (5), as well. By selecting external inputs $\nu_{ji} = l_{\nu_{ji}}(x_i)$ and since terms $l_i^T(x_i, \nu_i, w_i) g_i(x_i), l_{\nu_i}^T(x_i, \nu_i, w_i) g_{\nu_i}(\nu_i), l_{w_i}^T(x_i, \nu_i, w_i) g_{w_i}(w_i)$ are non-negative over the set X, we have

$$\mathcal{L}\mathcal{B}_i(x_i) \leq -\kappa_i(\mathcal{B}_i(x_i)) + \psi_i + \begin{bmatrix} w_i \\ h_{2_i}(x_i) \end{bmatrix}^T \begin{bmatrix} \bar{X}_i^{11} & \bar{X}_i^{12} \\ \bar{X}_i^{21} & \bar{X}_i^{22} \end{bmatrix} \begin{bmatrix} w_i \\ h_{2_i}(x_i) \end{bmatrix},$$

which implies that the function $\mathcal{B}_i(x_i)$ is a CSC and completes the proof. ◀

$$
\begin{aligned}
\mathcal{LB}(x) &= \mathcal{L}\sum_{i=1}^{N}\mu_i\mathcal{B}_i(x_i) = \sum_{i=1}^{N}\mu_i\mathcal{LB}_i(x_i)\\
&\leq \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \psi_i + \begin{bmatrix} w_i \\ h_{2_i}(x_i)\end{bmatrix}^T \begin{bmatrix} \bar{X}_i^{11} & \bar{X}_i^{12} \\ \bar{X}_i^{21} & \bar{X}_i^{22}\end{bmatrix}\begin{bmatrix} w_i \\ h_{2_i}(x_i)\end{bmatrix}\big)\\
&= \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i\\
&\quad + \begin{bmatrix} w_1 \\ \vdots \\ w_N \\ h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}^T \begin{bmatrix} \mu_1\bar{X}_1^{11} & & & \mu_1\bar{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\bar{X}_N^{11} & & & \mu_N\bar{X}_N^{12} \\ \mu_1\bar{X}_1^{21} & & & \mu_1\bar{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\bar{X}_N^{21} & & & \mu_N\bar{X}_N^{22}\end{bmatrix}\begin{bmatrix} w_1 \\ \vdots \\ w_N \\ h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}\\
&= \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i\\
&\quad + \begin{bmatrix} M\begin{bmatrix} h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix} \\ h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}^T \begin{bmatrix} \mu_1\bar{X}_1^{11} & & & \mu_1\bar{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\bar{X}_N^{11} & & & \mu_N\bar{X}_N^{12} \\ \mu_1\bar{X}_1^{21} & & & \mu_1\bar{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\bar{X}_N^{21} & & & \mu_N\bar{X}_N^{22}\end{bmatrix}\begin{bmatrix} M\begin{bmatrix} h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix} \\ h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}\\
&= \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i\\
&\quad + \begin{bmatrix} h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}^T \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}}\end{bmatrix}^T \begin{bmatrix} \mu_1\bar{X}_1^{11} & & & \mu_1\bar{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\bar{X}_N^{11} & & & \mu_N\bar{X}_N^{12} \\ \mu_1\bar{X}_1^{21} & & & \mu_1\bar{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\bar{X}_N^{21} & & & \mu_N\bar{X}_N^{22}\end{bmatrix}\begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}}\end{bmatrix}\begin{bmatrix} h_{2_1}(x_1) \\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}\\
&\leq \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i \leq -\kappa(\mathcal{B}(x)) + \psi. \qquad (24)
\end{aligned}
$$