Technische Universität München
TUM School of Computation, Information and Technology

Formal Verification and Control of Stochastic Hybrid Systems: Model-based and Data-driven Techniques

Ameneh Nejati

Vollständiger Abdruck der von der TUM School of Computation, Information and Technology der Technischen Universität München zur Erlangung des akademischen Grades einer

Doktorin der Ingenieurwissenschaften (Dr.-Ing.)

genehmigten Dissertation.

Vorsitz: Prof. Dr.-Ing. Thomas Eibert

Prüfer*innen der Dissertation:

1. Prof. Dr.-Ing. Martin Buss
2. Prof. Dr. Majid Zamani
3. Prof. Dr. Murat Arcak

Die Dissertation wurde am 13.01.2023 bei der Technischen Universität München eingereicht und durch die TUM School of Computation, Information and Technology am 19.06.2023 angenommen.

To my beloved "***Abolfazl***"

Acknowledgments

This dissertation is the outcome of my doctoral research conducted at the School of Computation, Information, and Technology, Technical University of Munich (TUM). In this concise acknowledgment, I would like to seize the opportunity to express my sincere gratitude to the individuals who provided unwavering support throughout my Ph.D. journey.

I am deeply grateful to my Ph.D. advisor, Prof. Majid Zamani, for his continuous support, encouragement, and invaluable guidance throughout my doctoral studies. His consistent mentorship and generous advice have been instrumental in making my research endeavors fruitful and worthwhile. I would also like to extend my sincere appreciation to my co-advisor, Prof. Sadegh Soudjani, for his generous support and guidance during my doctoral journey. Furthermore, I would like to express my gratitude to Prof. Martin Buss for warmly welcoming me to the Chair of Automatic Control Engineering at the Technical University of Munich. I would also like to acknowledge and extend my thanks to all the members of the HyConSys Lab. Our fruitful discussions and enjoyable times have greatly enriched my research experience.

Most importantly, I would like to express my heartfelt appreciation to my beloved *Mom and Dad*. I am eternally grateful to them for their unwavering love, support, and invaluable advice throughout my life. Last but not least, I am forever grateful to my lovely spouse, *Abolfazl*; his boundless patience and unconditional love have been a constant source of strength during my Ph.D. studies. I am profoundly grateful for his endless support throughout this challenging and rewarding period.

Ameneh Nejati
Munich, October 2022

Abstract

This dissertation is motivated by the challenges arising in the formal verification and control of (unknown) continuous-time stochastic hybrid systems (SHS). Over the past two decades, stochastic SHS have gained significant attention as a beneficial modeling framework for a wide range of engineering systems with safety-critical applications including automotive, robotics, transportation systems, energy, healthcare, and critical infrastructures. Most SHS are heterogeneous in nature: discrete dynamics model computation parts including hardware and software, and continuous dynamics model control systems. Developing a formal verification and control framework for these complex systems to enforce some high-level logic specifications, *e.g.,* those expressed as linear temporal logic (LTL) formulae, is inherently very challenging. This is primarily due to (i) the tight interaction between physical and cyber components, (ii) the stochastic nature of dynamics, (iii) the large dimension of state and input sets, (iv) the complexity of logic requirements, and (v) the absence of mathematical closed-form models in some real-world applications.

To address the aforementioned challenges, one potential solution is to employ finite abstractions as approximate descriptions of continuous-space systems in which each finite state represents a collection of continuous states of the original system. These constructed finite abstractions can then serve as suitable substitutes for original systems in the controller synthesis procedure. By ensuring that the probabilistic distance between output trajectories of the original systems and their finite abstractions remains within a guaranteed error bound, one can guarantee that the original systems also satisfy the desired property of interest as finite abstractions with a quantified probabilistic error. The first part of this dissertation focuses on the construction of finite abstractions for continuous-time SHS. Given that abstraction-based techniques involve the discretization of state and input sets, they are susceptible to the *curse of dimensionality.* To mitigate this issue, we also develop *compositional* abstractions-based techniques for formal analysis of continuous-time SHS. These techniques are based on small-gain and dissipativity approaches, which enable more efficient and scalable analysis despite the challenges posed by the curse of dimensionality.

Another promising approach for the formal analysis of SHS is to employ control barrier certificates (CBC), as a *discretization-free* technique. Intuitively speaking, barrier certificates are Lyapunov-like functions defined over the state space of the system, aiming to enforce a set of inequalities on both the function itself and the infinitesimal generator along the system's flow or one-step transition. An appropriate level set of a barrier certificate can separate an unsafe region from all system trajectories starting from a given set of initial conditions. Consequently, the existence of such a function offers a formal

probabilistic certificate for system safety. On the downside, finding CBC for complex dynamical systems is computationally very expensive, particularly for complex dynamical systems with high dimensions. Motivated by this critical difficulty, the second part of the dissertation is dedicated to develop *compositional techniques* in the context of control barrier certificates for formal verification and controller synthesis of large-scale SHS to enforce high-level logic properties, expressed by LTL formulae. By leveraging the compositional approach, we aim to tackle the computational complexity and scalability issues that arise when dealing with control barrier certificates for complex systems.

Although SHS have become increasingly prevalent in different real-world applications in recent years, closed-form mathematical models for these complex systems are either unavailable or equally complex to be practically useful. Consequently, model-based techniques cannot be employed to analyze and design such complex unknown systems. Existing literature includes *indirect data-driven* techniques that offer analysis frameworks for unknown dynamical systems by learning approximate models through identification approaches. However, obtaining an accurate mathematical model is always challenging, time-consuming, and expensive, particularly when dealing with complex dynamics, as is often the case in many real-world applications. As a result, *direct data-driven* techniques have recently garnered significant attention for the formal analysis of unknown SHS, bypassing the system identification phase altogether. Since guaranteeing safety and reliability of physical systems based on data is currently very challenging, which is of paramount importance in many safety-critical applications, the final part of this dissertation focuses on the verification and synthesis of SHS using *direct data-driven* techniques with *formal guarantees*.

To showcase the effectiveness of the proposed findings, we apply the techniques developed in this dissertation to various real-world physical applications. These applications encompass a wide range of systems, including room temperature networks, Kuramoto oscillators, Moore-Greitzer jet engine, and DC motor. Through these real-world case studies, we can assess the effectiveness and robustness of the proposed approaches and their potential for addressing the challenges posed by different physical systems.

Zusammenfassung

Bei der Formalen Verifikation und Regelung von (unbekannten) zeitkontinuierlichen stochastischen Hybridsystemen (SHS) ergeben sich zahlreiche Herausforderungen, die in dieser Dissertation behandelt werden. In den letzten zwei Jahrzehnten haben SHS beachtliche Aufmerksamkeit erhalten, da sie sich besonders zur Modellierung zahlreicher technischer Systeme eignen. Dazu zählen sicherheitskritische Anwendungen, z.B. in den Bereichen Automobil, Robotik, Transportsysteme, Energie, Gesundheitswesen und kritische Infrastrukturen. SHS sind heterogener Natur: Diskrete Berechnungselemente einschließlich Hardware und Software, und kontinuierliche Regelungssysteme. Die Entwicklung eines Frameworks zur formalen Verifikation und Regelung komplexer Systeme dieser Art zur Einhaltung logischer high-level Spezifikationen, z.B. in Form von Formeln der linearen temporalen Logik (LTL), stellt eine große Herausforderung dar. Dies beruht insbesondere auf (i) der engen Interaktion zwischen physischen und Cyber-Komponenten, (ii) der stochastischen Dynamik, (iii) der hohen Dimension der Zustands- und Eingangsgrößen, (iv) der Verarbeitung komplexer logischer Anforderungen und (v) dem Mangel geschlossener mathematischer Modelle für zahlreiche reale Anwendungen.

Ein möglicher Lösungsansatz zur Bewältigung der oben genannten Herausforderungen ist die Verwendung endlicher Abstraktionen zur näherungsweisen Beschreibung kontinuierlicher Systeme. Dabei repräsentiert jeder diskrete Zustand eine Menge kontinuierlicher Zustände des Ursprungssystems. Zur Reglersynthese können die ursprünglichen Systeme durch die endlichen Abstraktionen ersetzt werden. Da der probabilistische Abstand zwischen den Ausgangstrajektorien der Originalsysteme und ihrer endlichen Abstraktionen innerhalb einer garantierten Fehlergrenze liegt, kann sichergestellt werden, dass die Originalsysteme die gewünschte Eigenschaft ebenso erfüllen wie die endlichen Abstraktionen. Dabei ist der probabilistische Fehler quantifizierbar. Der erste Teil dieser Arbeit widmet sich der Konstruktion endlicher Abstraktionen für zeitkontinuierliche SHS. Da abstraktionsbasierte Ansätze auf der Diskretisierung des Zustands- und Eingangsraums beruhen und folglich erheblich unter dem Fluch der Dimensionalität leiden, entwickeln wir zudem kompositionelle abstraktionsbasierte Ansätze für die formale Analyse von zeitkontinuierlichen SHS, die auf Small-Gain- und Dissipativitätsansätzen basieren.

Ein weiterer vielversprechender Ansatz für die formale Analyse von SHS ist die Verwendung sogenannter Control Barrier Certificates (CBC) als diskretisierungsfreie Lösung. Intuitiv gesprochen, sind Barrier Certificates Lyapunov-ähnliche Funktionen, die über den Zustandsraum des Systems definiert werden und eine Reihe von Ungleichheiten sowohl für die Funktion selbst als auch für den infinitesimalen Generator entlang des Flusses (oder des schrittweisen Übergangs) des Systems vorgeben. Eine geeignete Lev-

elmenge eines Barrier Certificates kann eine unsichere Region von allen Systemtrajektorien abgrenzen, die von einer gegebenen Menge von Anfangsbedingungen ausgehen. Die Existenz einer solchen Funktion stellt somit ein formales probabilistisches Zertifikat für die Sicherheit des Systems dar. Der Nachteil ist, dass die Identifizierung von CBC für komplexe dynamische Systeme sehr rechenintensiv ist, insbesondere wenn die Dimension der zugrundeliegenden Systeme hoch ist. Aus diesem Grund widmet sich der zweite Teil dieser Arbeit der Entwicklung kompositioneller Methoden im Kontext von Control Barrier Certificates für die formale Verifikation und Synthese von Reglern für hochdimensionale SHS und logische high-level Eigenschaften.

Obwohl SHS in den letzten Jahren durch diverse praktische Anwendungen allgegenwärtig geworden sind, stehen geschlossene mathematische Modelle für diese komplexen Systeme entweder nicht zur Verfügung oder sind so komplex, dass sie keinen praktischen Nutzen haben. Folglich können modellbasierte Methoden nicht für die Analyse und den Entwurf dieser Art komplexer unbekannter Systeme eingesetzt werden. In der Literatur werden indirekte datengetriebene Ansätze beschrieben, die die Analyse unbekannter dynamischer Systeme durch das Lernen näherungsweiser Modelle mit Hilfe von Identifikationsverfahren ermöglichen. Allerdings ist die Ermittlung eines genauen Modells immer äußerst schwierig, zeitaufwändig und teuer, insbesondere wenn die zugrundeliegende Dynamik zu komplex ist, was bei vielen realen Anwendungen der Fall ist. Kürzlich haben direkte datengetriebene Ansätze, die die Identifikation des Systems umgehen, erhebliche Aufmerksamkeit für die formale Analyse von unbekannten SHS erhalten. Da die Gewährleistung des sicheren und zuverlässigen Betriebs physischer Systeme auf der Grundlage von Daten derzeit eine große Herausforderung darstellt, besonders für sicherheitskritische Anwendungen, konzentriert sich der letzte Teil dieser Arbeit auf die Verifikation und Synthese von SHS mittels direkter datengesteuerter Methoden mit formalen Garantien.

Um die Leistungsfähigkeit der entwickelten Methoden zu demonstrieren, wenden wir sie auf verschiedene realistische physische Anwendungen an, darunter Raumtemperaturnetzwerke, Kuramoto-Oszillatoren, Moore-Greitzer-Düsentriebwerke und Gleichstrommotoren.

Publications by the Author during Ph.D.

Journal Papers

1. **A. Nejati**, A. Lavaei, P. Jagtap, S. Soudjani, and M. Zamani, "Formal Verification of Unknown Discrete- and Continuous-Time Systems: A Data-Driven Approach", *IEEE Transactions on Automatic Control (TAC)* ***(Special Issue on Learning and Control)***, vol. 68, no. 5, pp. 3011-3024, 2023.

2. **A. Nejati**, S. Soudjani, and M. Zamani, "Compositional Construction of Control Barrier Functions for Continuous-Time Stochastic Hybrid Systems", *Automatica*, vol. 145, 2022.

3. **A. Nejati**, S. Soudjani, and M. Zamani, "Compositional Abstraction-based Synthesis for Continuous-Time Stochastic Hybrid Systems", *European Journal of Control*, vol. 57, pp. 82–94, 2021.

4. **A. Nejati** and M. Zamani, "From Dissipativity Theory to Compositional Construction of Control Barrier Certificates", *Leibniz Transactions on Embedded Systems (LITES)* ***(Special Issue on Distributed Hybrid Systems)***, vol. 8, no. 2, 2022.

5. **A. Nejati**, A. Lavaei, S. Soudjani, and M. Zamani, "Estimation of Infinitesimal Generators for Unknown Stochastic Hybrid Systems via Sampling: A Formal Approach", *IEEE Control Systems Letters*, vol. 7, pp. 223-228, 2022.

6. **A. Nejati**, S. Soudjani, and M. Zamani, "Compositional Construction of Control Barrier Certificates for Large-Scale Stochastic Switched Systems", *IEEE Control Systems Letters*, vol. 4, no. 4, pp. 845–850, 2021.

7. **A. Nejati** and M. Zamani, "Data-Driven Synthesis of Safety Controllers via Multiple Control Barrier Certificates", *IEEE Control Systems Letters*, vol. 7, pp. 2497-2502, 2023.

Conference Papers

8. **A. Nejati***, B. Zhong*, M. Caccamo, and M. Zamani, "Data-Driven Controller Synthesis of Unknown Nonlinear Polynomial Systems via Control Barrier Certificates", *Learning for Dynamics and Control Conference (L4DC)* ***(Proceedings of Machine Learning Research)***, pp. 763-776, 2022.

9. **A. Nejati**, A. Lavaei, S. Soudjani, and M. Zamani, "Data-Driven Estimation of Infinitesimal Generators of Stochastic Systems", *7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS)*, vol. 54, no. 5, pp. 277–282, 2021.

10. **A. Nejati** and M. Zamani, "Compositional Construction of Finite MDPs for Continuous-Time Stochastic Systems: A Dissipativity Approach", *21st IFAC World Congress*, vol. 53, no. 2, pp. 1962–1967, 2020.

11. **A. Nejati**, S. Soudjani, and M. Zamani, "Compositional Construction of Control Barrier Functions for Networks of Continuous-Time Stochastic Systems", *21st IFAC World Congress*, vol. 53, no. 2, pp. 1856–1861, 2020.

12. **A. Nejati**, S. Soudjani, and M. Zamani, "Abstraction-based Synthesis of Continuous-Time Stochastic Control Systems", *18th European Control Conference (ECC)*, pp. 3212–3217, 2019.

13. **A. Nejati**, B. Zhong, M. Caccamo, and M. Zamani, "Controller Synthesis for Unknown Polynomial-Type Systems: A Data-Driven Approach", *CPS-IoT Week workshop on Computation-Aware Algorithmic Design for Cyber-Physical Systems*, 2022.

14. A. Lavaei, **A. Nejati**, P. Jagtap, and M. Zamani, "Formal Safety Verification of Unknown Continuous-Time Systems: A Data-Driven Approach", *24th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, 2021.

15. A. Lavaei, **A. Nejati**, S. Soudjani, and M. Zamani, "Estimating Infinitesimal Generators of Stochastic Systems with Formal Error Bounds: A Data-Driven Approach", *24th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, 2021.

Contents

List of Figures

List of Tables

List of Abbreviations

ABC	augmented control barrier certificate
APBC	augmented control pseudo-barrier certificate
BC	barrier certificate
BMI	bilinear matrix inequality
CBC	control barrier certificate
CEGIS	counter-example guided inductive synthesis
CPBC	control pseudo-barrier certificate
CStC	control storage certificate
CTMC	continuous-time Markov chain
ct-S	continuous-time dynamical system
ct-SCS	continuous-time stochastic control system
ct-SHS	continuous-time stochastic hybrid system
ct-SHS-MS	continuous-time stochastic hybrid system with Markovian switching
ct-SS	continuous-time stochastic system
DFA	deterministic finite automata
dt-S	discrete-time dynamical system
dt-SS	discrete-time stochastic switched system
i.i.d.	independent and identically distributed
LQR	linear quadratic regulation
MDP	Markov decision processes
POMDP	partially-observable Markov decision processes
RCP	robust convex program
SCP	scenario convex program
SDP	semidefinite programming
SMT	satisfiability modulo theories
SOS	sum of squares
SPSF	stochastic pseudo-simulation function
SSF	stochastic simulation function
SStF	stochastic storage function

1 Introduction

1.1 Motivations, Research Goals and Original Contributions

Stochastic hybrid systems (SHS) are complex networked models that combine both cyber (computation and communication) and physical components, which tightly interact with each other in a feedback loop. In the past two decades, SHS have received remarkable attentions as a beneficial modeling framework spanning a wide range of engineering systems with real-life safety-critical applications such as automotive, robotics, transportation systems, energy, healthcare, and critical infrastructures, to name a few. Most SHS are of heterogeneous nature: discrete dynamics model computation parts including hardware and software, and continuous dynamics model control systems. Providing formal verification and analysis framework for this type of complex systems to enforce some high-level logic specifications, *e.g.,* those expressed as linear temporal logic (LTL) formulae, is inherently very challenging [Pnu77]. In particular, the ability to handle the interaction between continuous and discrete dynamics under the influence of uncertain factors is a prerequisite to provide a rigorous mathematical framework for the formal verification and synthesis of SHS.

To deal with the above-mentioned difficulties, the verification and policy synthesis for complex SHS are often addressed by methods of (in)finite abstractions. In particular, since the closed-form solution of synthesized policies for SHS is not available in general, a promising approach is to approximate original models by simpler ones with possibly lower dimensional state spaces (*a.k.a.,* infinite abstractions) or with finite state spaces (*a.k.a.,* finite abstractions). Given that the probabilistic distance between output trajectories of original systems and their (in)finite abstractions lives within a guaranteed error bound, one can ensure that original systems also fulfill the intended property with a quantified probabilistic error. The first part of this dissertation is dedicated to the construction of finite abstractions for continuous-time SHS. In order to deal with the *curse of dimensionality* as the main challenge in the construction of finite abstractions, we also develop the *compositional* abstractions-based techniques for formal analysis of continuous-time SHS based on small-gain and dissipativity approaches.

The second part of the dissertation is concerned with developing *compositional techniques* in the context of control barrier certificates (CBC) for formal verification and controller synthesis of large-scale SHS to enforce high-level logic properties. In particular, control barrier certificates have received significant attentions in the past few years as a *discretization-free* approach for formal analysis of SHS. On the downside, finding CBC for complex dynamical systems is computationally very expensive, especially if one is dealing with high-dimensional systems. Then compositional techniques are essential

to alleviate the encountered computational complexity. In our proposed setting, we consider the large-scale SHS as an interconnected system composed of several smaller subsystems, and develop compositional frameworks for the construction of CBC for the complex interconnected SHS using control barrier certificates constructed for smaller subsystems.

In the last part of the dissertation, we develop *data-driven* techniques for the verification and synthesis of SHS while providing *formal guarantees*. In particular, closed-form mathematical models for some complex SHS are either not available or equally complex to be of any practical use. Accordingly, one cannot employ model-based techniques to analyze and design this type of complex unknown systems. Then data-driven techniques have received significant attentions in the past few years for the formal analysis of *unknown* SHS enforcing complex control missions. However, guaranteeing safety and reliability of physical systems based on data is currently very challenging, which is of vital importance in many safety-critical applications. The last part of the dissertation is to develop model-free data-driven verification and synthesis techniques for formal analysis of SHS.

It should be noted that throughout the dissertation, to demonstrate the effectiveness of our results, we apply the proposed techniques to different *real-world* applications including "room temperature networks", "Kuramoto oscillators", "Moore-Greitzer jet engine", and "DC motor".

1.2 Outline of the Dissertation

This dissertation is divided into 6 chapters, the first of which is the current introduction. The rest is structured as follows:

Chapter 2 presents some mathematical notations and preliminaries, and also basic notions from control theory that will be widely employed throughout the dissertation.

Chapter 3 studies compositional (in)finite abstractions with different compositionality techniques including small-gain and dissipativity approaches. The results of this chapter are respectively presented based on [NSZ19, NSZ21, NZ20].

Chapter 4 discusses compositional construction of control barrier certificates to enforce high-level logic properties over SHS. The results of this chapter are respectively presented based on [NSZ20b, NSZ20a, NSZ22, NZ22].

Chapter 5 provides model-free techniques based on data-driven optimization for formal analysis of SHS. The results of this chapter are presented based on [NLSZ21, NLSZ22, NLJ$^+$23, NZCZ22, LNSZ21, LNJZ21].

Chapter 6 summarizes the results of this dissertation and outlines potential directions for the future research.

It should be noted that Chapters 3, 4, 5 follow a common structure for the sake of clarity. In particular, they start with an introduction including a description of the problem addressed, a brief literature review, and a statement of the contributions made. The developed techniques are detailed in subsequent sections, followed by a section

illustrating their efficiency on different case studies. Finally, the chapters are concluded with a summary section.

2 Mathematical Notations, Preliminaries and Basic Notions in Control Theory

2.1 Notations

The following notations are employed throughout the dissertation. The sets of nonnegative and positive integers are denoted by $\mathbb{N} := \{0, 1, 2, \ldots\}$ and $\mathbb{N}_{\geq 1} := \{1, 2, 3, \ldots\}$, respectively. Moreover, the symbols $\mathbb{R}$, $\mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote, respectively, the sets of real, positive and nonnegative real numbers. Given N vectors $x_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}_{\geq 1}$, and $i \in \{1, \ldots, N\}$, we use $x = [x_1; \ldots; x_N]$ to denote the corresponding column vector of dimension $\sum_i n_i$. Given a matrix $P \in \mathbb{R}^{n \times n}$ with diagonal entries $a_1, \ldots, a_n$, we define $\mathsf{Tr}(P) = \sum_{i=1}^{n} a_i$. Given a symmetric matrix P, the minimum and maximum eigenvalues of P are respectively denoted by $\lambda_{\min}(P)$ and $\lambda_{\max}(P)$. We denote by $\|\cdot\|_\infty$ and $\|\cdot\|$ the infinity and Euclidean norms, respectively. For any matrix $P \in \mathbb{R}^{m \times n}$, we have $\|P\| := \sqrt{\lambda_{\max}(P^\top P)}$. We also denote by $\|P\|_F := \sqrt{\mathsf{Tr}(P^\top P)}$ the *Frobenius norm* of any matrix $P \in \mathbb{R}^{m \times n}$. Given any $a \in \mathbb{R}$, $|a|$ denotes the absolute value of a. Symbols $\mathbb{I}_n$, $\mathbf{0}_n$, and $\mathbb{1}_n$ denote the identity matrix in $\mathbb{R}^{n \times n}$ and the column vector in $\mathbb{R}^{n \times 1}$ with all elements equal to zero and one, respectively. The identity function and composition of functions are denoted by $\mathcal{I}_d$ and symbol $\circ$, respectively. We denote the indicator function of a subset $\mathcal{A}$ of a set X by $\mathbf{1}_{\mathcal{A}} : X \to \{0, 1\}$, where $\mathbf{1}_{\mathcal{A}}(x) = 1$ if and only if $x \in \mathcal{A}$, and 0 otherwise.

For any set X we denote by 2^X the power set of X that is the set of all subsets of X. For any set X, $|X|$ and $Int(X)$ represent, respectively, the cardinality and interior of the set. The empty set is denoted by $\emptyset$. Given a set X and $P \subset X$, the complement of P with respect to X is denoted by $X \backslash P = \{x \,|\, x \in X, x \notin P\}$. We denote the disjunction ($\vee$) and conjunction ($\wedge$) of a Boolean function $f(\alpha)$ over an index set Γ by $\bigvee_{\alpha \in \Gamma} f(\alpha)$ and $\bigwedge_{\alpha \in \Gamma} f(\alpha)$, respectively. 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. We denote the spectral radius of a matrix $P \in \mathbb{R}^{n \times n}$ by $\rho_{spc}(P)$ which is defined as $\rho_{spc}(P) = \max\{|\mathsf{eig}_1|, \ldots, |\mathsf{eig}_n|\}$, where $\mathsf{eig}_1, \ldots, \mathsf{eig}_n$ are eigenvalues of matrix P. 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 $(\prod_{i=1}^{N} f_i)(x_1, \ldots, x_N) = [f_1(x_1); \ldots; f_N(x_N)]$. Given a measurable function $f : \mathbb{N} \to \mathbb{R}^n$, the (essential) supremum of f is denoted by $\|f\|_\infty := (\text{ess})\sup\{\|f(k)\|, k \geq 0\}$. 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 denote the factorial of a nonnegative integer n by $n!$ as the product of all positive integers less than or equal to n,

i.e., $n! = n \times (n-1) \times (n-2) \times \cdots \times 3 \times 2 \times 1$. We define the regularized incomplete beta function as [Cal10]

$$\mathcal{I}_r : (c,a,b) \mapsto \mathcal{I}_r(c,a,b) = \frac{\int_0^c \mathsf{t}^{a-1}(1-\mathsf{t})^{b-1}\mathsf{dt}}{\int_0^1 \mathsf{t}^{a-1}(1-\mathsf{t})^{b-1}\mathsf{dt}}, \quad \forall a,b,c \in \mathbb{R}_{>0}.$$

2.2 Preliminaries

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. Given a probability space $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$, we denote the N-Cartesian product set of Ω by Ω^N, and its corresponding product measure by $\mathbb{P}^N$.

We assume that random variables introduced in the dissertation are measurable functions of the form $X : (\Omega, \mathcal{F}_\Omega) \to (S_X, \mathcal{F}_X)$. Any random variable X induces a probability measure on its space $(S_X, \mathcal{F}_X)$ as $Prob\{A\} = \mathbb{P}_\Omega\{X^{-1}(A)\}$ for any $A \in \mathcal{F}_X$. We often directly discuss the probability measure on $(S_X, \mathcal{F}_X)$ without explicitly mentioning the underlying probability space and the function X itself. A topological space $\mathcal{S}$ is called a Borel space if it is homeomorphic to a Borel subset of a Polish space (*i.e.,* a separable and completely metrizable space). Examples of a Borel space are Euclidean spaces $\mathbb{R}^n$, its Borel subsets endowed with a subspace topology as well as hybrid spaces. Any Borel space $\mathcal{S}$ is assumed to be endowed with a Borel sigma-algebra, which is denoted by $\mathbb{B}(\mathcal{S})$. We say that a map $f : \mathcal{S} \to Y$ is measurable whenever it is Borel measurable.

2.3 Continuous-Time Stochastic Hybrid Systems

In this dissertation, we consider stochastic hybrid systems in continuous-time (ct-SHS) defined over a general state space as in the following definition.

Definition 2.3.1. *A continuous-time stochastic hybrid system (ct-SHS) is characterized by the tuple*

$$\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, \rho, Y, h), \tag{2.3.1}$$

where:

- $X \subseteq \mathbb{R}^n$ *is the state space of the system;*
- $U \subseteq \mathbb{R}^{\bar{m}}$ *is the external input space of the system;*
- $W \subseteq \mathbb{R}^{\bar{p}}$ *is the internal input space of the system;*

- $\mathcal{U}$ *and* $\mathcal{W}$ *are subsets of the sets of all* $\mathbb{F}$*-progressively measurable processes (see [KS14] for more details) taking values in* $\mathbb{R}^{\bar{m}}$ *and* $\mathbb{R}^{\bar{p}}$*;*

- $f : X \times U \times W \to X$ *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* $\mathscr{L}_\sigma$*;*

- $\rho : \mathbb{R}^n \to \mathbb{R}^{n\times \mathsf{r}}$ *is the reset term which is globally Lipschitz continuous with the Lipschitz constant* $\mathscr{L}_\rho$*;*

- $Y \subseteq \mathbb{R}^{\bar{q}}$ *is the output space of the system;*

- $h : X \to Y$ *is the output map.*

A continuous-time stochastic hybrid system Σ satisfies

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = f(\xi(t), \nu(t), w(t))\,\mathsf{d}t + \sigma(\xi(t))\,\mathsf{d}\mathbb{W}_t + \rho(\xi(t))\,\mathsf{d}\mathbb{P}_t, \\ \zeta(t) = h(\xi(t)), \end{cases} \tag{2.3.2}$$

$\mathbb{P}$-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 $\xi_{x_0\nu w}(t)$ 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 $\xi_{x_0\nu w}(0) = x_0$ $\mathbb{P}$-a.s., where x_0 is a random variable that is $\mathcal{F}_0$-measurable. We also denote by $\zeta_{x_0\nu w}$ the *output trajectory* corresponding to *solution process* $\xi_{x_0\nu w}$. Here, we assume that the Poisson processes $\mathbb{P}^z_s$, for any $z \in \{1, \ldots, \mathsf{r}\}$, have the rates $\bar{\lambda}_z$. We emphasize that the postulated assumptions on f, σ, and ρ ensure existence, uniqueness, and strong Markov property of the solution process [ØS05].

Remark 2.3.2. *Note that the underlying dynamic considered in* (2.3.2) *is a* class *of stochastic hybrid systems in which the drift and diffusion terms model the continuous part and the Poisson process models the discrete jump of the system. In particular, Brownian motions and Poisson processes introduce natively two different sources of uncertainty: (i) a continuous random walk throughout the state space that is governed by Brownian motions, and (ii) a discrete random jump with an exponential distribution that is modelled by Poisson processes.*

Remark 2.3.3. *In some parts of the dissertation, we consider the class of systems in Definition 2.3.1 but without the reset term* ρ*, and call it continuous-time stochastic control systems (ct-SCS), denoted by*

$$\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, Y, h). \tag{2.3.3}$$

Remark 2.3.4. *In this dissertation, we are ultimately interested in investigating continuous-time stochastic hybrid systems with possibly large-state dimensions but without internal inputs. In this case, the tuple* (2.3.1) *reduces to* $(X, U, \mathcal{U}, f, \sigma, \rho, Y, h)$ *with* $f : X \times U \to X$*, and ct-SHS in* (2.3.2) *can be re-written as*

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

2.4 Markov Policy

Given the ct-SHS in (2.3.1), we are interested in *Markov policies* to control the system defined as follows.

Definition 2.4.1. *A Markov policy for the ct-SHS* Σ *in* (2.3.1) *is a map* $\bar{\rho} : \mathbb{B}(U) \times X \times \mathbb{R}_{\geq 0} \to [0, 1]$*, with* $\mathbb{B}(U)$ *being the Borel sigma-algebra on the external input space, such that* $\bar{\rho}(\cdot \,|\, x, t)$ *is a universally measurable stochastic kernel for all* $t \in \mathbb{R}_{\geq 0}$ *[Ros08]. For any state* $x \in X$ *at time* t*, the input* $\nu(t)$ *is chosen according to the probability measure* $\bar{\rho}(\cdot \,|\, x, t)$*. Stationary policies are a subclass of those Markov policies in which the mapping at any time* t *hinges only on the current state* $x(t)$ *and does not change over time.*

2.5 Continuous-Time Stochastic Hybrid Systems with Markovian Switching

Definition 2.5.1. *A continuous-time stochastic hybrid system with Markovian switching (ct-SHS-MS) is characterized by the tuple*

$$\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho}, Y, h), \tag{2.5.1}$$

where:

- $X \subseteq \mathbb{R}^n$ *is the state set of the system;*
- $U \subseteq \mathbb{R}^{\bar{m}}$ *is the external input set of the system;*
- $W \subseteq \mathbb{R}^{\bar{p}}$ *is the internal input set of the system;*
- $\mathcal{U}$ *and* $\mathcal{W}$ *are, respectively, subsets of sets of* $\mathbb{F}$*-progressively measurable processes taking values in* $\mathbb{R}^{\bar{m}}$ *and* $\mathbb{R}^{\bar{p}}$*;*
- $P = \{1, \ldots, m\}$ *is a finite set of modes;*
- $\mathcal{P}$ *is a subset of* $\bar{\mathcal{S}}(\mathbb{R}_{\geq 0}, P)$ *which denotes the set of piecewise constant functions from* $\mathbb{R}_{\geq 0}$ *to* P*, continuous from the right and with a finite number of discontinuities on every bounded interval of* $\mathbb{R}_{\geq 0}$*;*

- $\hat{f} = \{f_1, \ldots, f_m\}$, $\hat{\sigma} = \{\sigma_1, \ldots, \sigma_m\}$, *and* $\hat{\rho} = \{\rho_1, \ldots, \rho_m\}$ *are, respectively, collections of vector fields, diffusion and reset terms indexed by* p. *For all* $p \in P$, *the vector field* $f_p : X \times U \times W \to X$, *and diffusion and reset terms* $\sigma_p : \mathbb{R}^n \to \mathbb{R}^{n \times b}$, $\rho_p : \mathbb{R}^n \to \mathbb{R}^{n \times r}$ *are assumed to be globally Lipschitz continuous;*

- $Y \subseteq \mathbb{R}^{\bar{q}}$ *is the output set of the system;*

- $h : X \to Y$ *is the output map.*

A continuous-time stochastic hybrid system with Markovian switching Σ satisfies

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = f_{\mathbf{p}(t)}(\xi(t), \nu(t), w(t))\mathsf{d}t + \sigma_{\mathbf{p}(t)}(\xi(t))\mathsf{d}\mathbb{W}_t + \rho_{\mathbf{p}(t)}(\xi(t))\mathsf{d}\mathbb{P}_t, \\ \zeta(t) = h(\xi(t)), \end{cases} \tag{2.5.2}$$

$\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.) for any $\nu \in \mathcal{U}$, $w \in \mathcal{W}$, and switching signal $\mathbf{p}(t) : \mathbb{R}_{\geq 0} \to P$. For any $p \in P$, we use Σ_p to refer to system (2.5.2) with a constant switching signal $\mathbf{p}(t) = p$ for all $t \in \mathbb{R}_{\geq 0}$. We denote the *solution process* and *output trajectory* of Σ_p with, respectively, stochastic processes $\xi^p : \Omega \times \mathbb{R}_{\geq 0} \to X$ and $\zeta^P : \Omega \times \mathbb{R}_{\geq 0} \to Y$. We also employ $\xi^p_{x_0 \nu w}(t)$ to denote the value of the solution process at time $t \in \mathbb{R}_{\geq 0}$ under input trajectories ν and w, and the switching signal p from an initial condition $\xi^p_{x_0 \nu w}(0) = x_0$ $\mathbb{P}$-a.s., where x_0 is a random variable that is $\mathcal{F}_0$-measurable. We also denote by $\zeta^p_{x_0 \nu w}$ the *output trajectory* corresponding to the *solution process* $\xi^p_{x_0 \nu w}$.

Given the switching system in (2.5.2) with $p, p' \in P$, the transition probability between modes at any time instant $t \in \mathbb{R}_{\geq 0}$ is described using the following Markovian switching:

$$\mathbb{P}\Big\{(p, p'), t + \tilde{\delta}\Big\} = \begin{cases} \tilde{\lambda}_{pp'}(\xi^{\mathbf{p}(t)}(t))\,\tilde{\delta}, & \text{if } p \neq p', \\ 1 + \tilde{\lambda}_{pp}(\xi^{\mathbf{p}(t)}(t))\,\tilde{\delta}, & \text{if } p = p', \end{cases}$$

where $\tilde{\delta}$ is the time increment and $\tilde{\lambda}_{pp'} : \mathbb{R}^n \to \mathbb{R}$ is a bounded and Lipschitz continuous function representing transition rates, where, for all $x \in \mathbb{R}^n$, $\tilde{\lambda}_{pp'}(x) \geq 0$ if $p \neq p'$, and $\sum_{p' \in P} \tilde{\lambda}_{pp'}(x) = 0$ for all $p \in P$. The Markovian switching in (2.5.2) implies that the switching between different modes is governed by a continuous-time Markov chain (CTMC) [ASSB00].

Remark 2.5.2. *Stochastic hybrid systems [BLE+06, CL06], in the form of* (2.5.2), *have broad applications in real-life safety-critical systems such as biological networks [MPC+17, IHM09, ABB+15], communication networks [Hes04], power grids [SGS17, DMKFF18], health and epidemiology [OP15, NPP16], air traffic networks [GL04], and manufacturing systems [GAM93], to name a few.*

2.6 Discrete-Time Stochastic Switched Systems

We consider stochastic switched systems in discrete-time (dt-SS) defined formally as follows.

Definition 2.6.1. *A discrete-time stochastic switched system (dt-SS) is characterized by the tuple*

$$\Sigma = (X, W, P, \mathcal{P}, \varsigma, F, Y, h), \tag{2.6.1}$$

where:

- $X \subseteq \mathbb{R}^n$ *is a Borel space as the state set of the system. We denote by* $(X, \mathbb{B}(X))$ *the measurable space with* $\mathbb{B}(X)$ *being the Borel sigma-algebra on the state space;*
- $W \subseteq \mathbb{R}^{\bar{p}}$ *is a Borel space as the internal input set of the system;*
- $P = \{1, \ldots, m\}$ *is a finite set of modes;*
- $\mathcal{P}$ *is a subset of* $\bar{\mathcal{S}}(\mathbb{N}, P)$ *which denotes the set of functions from* $\mathbb{N}$ *to* P*;*
- ς *is a sequence of independent and identically distributed (i.i.d.) random variables from a sample space* Ω *to a set* V_ς*, i.e.,*

$$\varsigma := \{\varsigma(k) : \Omega \to V_\varsigma,\ k \in \mathbb{N}\};$$

- $F = \{f_1, \ldots, f_m\}$ *is a collection of vector fields indexed by* p*. For all* $p \in P$*, the map* $f_p : X \times W \times V_\varsigma \to X$ *is a measurable function characterizing the state evolution of the system in mode* p*;*
- $Y \subseteq \mathbb{R}^{\bar{q}}$ *is a Borel space as the output set of the system;*
- $h : X \to Y$ *is a measurable function as the output map that maps a state* $x \in X$ *to its output* $y = h(x)$*.*

For a given initial state $x(0) \in X$*, an internal input sequence* $w(\cdot) : \mathbb{N} \to W$*, and a switching signal* $\mathbf{p}(k) : \mathbb{N} \to P$*, the evolution of the state of* Σ *is described as*

$$\Sigma : \begin{cases} x(k+1) = f_{\mathbf{p}(k)}(x(k), w(k), \varsigma(k)), \\ y(k) = h(x(k)), \end{cases} \qquad k \in \mathbb{N}. \tag{2.6.2}$$

We assume that the signal $\mathbf{p}$ satisfies a *dwell-time* condition [Mor96] as defined in the next definition.

Definition 2.6.2. *Consider a switching signal* $\mathbf{p} : \mathbb{N} \to P$ *and define its switching time instants as*

$$\mathfrak{S}_{\mathbf{p}} := \{\mathfrak{s}_k : k \in \mathbb{N}_{\geq 1}\}.$$

Then, $\mathbf{p} : \mathbb{N} \to P$ *has dwell-time* $k_d \in \mathbb{N}$ *[Mor96] if elements of* $\mathfrak{S}_{\mathbf{p}}$ *ordered as* $\mathfrak{s}_1 \leq \mathfrak{s}_2 \leq \mathfrak{s}_3 \leq \ldots$ *satisfy* $\mathfrak{s}_1 \geq k_d$ *and* $\mathfrak{s}_{k+1} - \mathfrak{s}_k \geq k_d, \forall k \in \mathbb{N}_{\geq 1}$*.*

3 Discretization-based Techniques based on (In)Finite Abstractions

3.1 Introduction

Construction of (in)finite abstractions was proposed in the past decade as a promising approach to alleviate the complexity of controller synthesis problems, in particular for enforcing complex logical properties. Infinite abstractions are approximated versions of continuous-space systems whose space is still continuous but with lower dimensions. Finite abstractions are abstract descriptions of continuous-space systems in which each discrete state corresponds to a collection of continuous states of the original system. Since the abstractions are finite, algorithmic approaches from computer science are applicable to synthesize controllers enforcing high-level logic specifications. A crucial step is to provide formal guarantees during this approximation phase such that the analysis or synthesis on abstract models can be refined back over original ones. Stochastic simulation functions are then employed as Lyapunov-like functions defined over the Cartesian product of state spaces of two systems to relate output trajectories of abstract systems to those of original ones such that the mismatch between two systems remains within some guaranteed error bounds. This chapter is concerned with the construction of finite abstractions for continuous-time SHS. In order to deal with *curse of dimensionality* problem as the main drawback in the construction of finite abstractions, we also develop *compositional* abstractions-based techniques based on small-gain and dissipativity approaches for formal analysis of continuous-time stochastic SHS.

3.1.1 Related Literature

In the past few years, there have been several results on the construction of finite abstractions for *continuous-time* stochastic systems. Reachability analysis for continuous-time stochastic systems is presented in [LAB$^+$17], which constructs finite-state Markov chain with provable error bounds. Finite bisimilar abstractions for incrementally stable stochastic control systems without discrete dynamics are presented in [ZMEM$^+$14]. Abstraction techniques for randomly switched stochastic systems and incrementally stable stochastic switched systems are discussed in [ZA14] and [ZAG15], respectively. Although original systems in [ZMEM$^+$14, ZAG15, ZA14] are in the stochastic settings, their proposed abstractions are finite labeled transition systems whereas in this chapter we consider finite Markov decision processes (MDPs) as our finite abstractions. An approximation framework for constructing infinite abstractions for jump-diffusion processes

is proposed in [JP09]. Compositional construction of infinite abstractions is discussed in [ZRME17] using small-gain type conditions.

There have been also several results on the construction of (in)finite abstractions for *discrete-time* stochastic systems with continuous-state spaces. In this respect, finite abstractions for formal synthesis of discrete-time stochastic hybrid systems are initially proposed in [APLS08]. A sequential and adaptive gridding approach is proposed in [SA13, Sou14] with dedicated tools FAUST^2 [SGA15], *StocHy* [CA19] and *AMYTISS* [LKSZ20]. Furthermore, formal abstraction-based policy synthesis is discussed in [TMKA13, KSL13]. Compositional construction of (in)finite abstractions using small-gain and dissipativity approaches is presented in [LSZ20d, LSZ19a], respectively. Compositional construction of finite abstractions for discrete-time stochastic control systems is presented in [SAM17] and [LSZ18] using respectively dynamic Bayesian networks and dissipativity properties of subsystems and their abstractions.

A notion of disturbance bisimulation relation is proposed in [MSSM17] for compositional construction of finite abstractions. A notion of approximate simulation relation for stochastic systems is proposed in [HSA17] that is based on lifting probabilistic evolution of systems to a coupled space. This notion is extended in [LSZ20b] for compositional abstraction-based synthesis of general MDPs. This notion enables using both model order reduction and space discretization in a unified framework.Compositional construction of finite abstractions for a class of stochastic hybrid systems, namely stochastic *switched* systems, is proposed in [LSZ20a, LZ22]. Compositional construction of finite abstractions for stochastic systems that are not necessarily stabilizable is presented in [LSZ19b, LZ19, LSZ20c]. Compositional construction of (in)finite abstractions for large-scale discrete-time stochastic systems via different compositionality conditions is widely discussed in [LSAZ22, Lav19].

3.1.2 Contributions

In the first part of this chapter, we develop a scheme for the construction of discrete-time finite-space Markov decision processes (MDPs) from continuous-time stochastic control systems. The proposed framework relies on a relation between the continuous-time system and its discrete-time counterpart employing the notion of *stochastic simulation functions*. This type of relations enables one to compute a probability bound between continuous-time concrete systems and that of their discrete-time (in)finite abstractions. We show that if the original stochastic control system possesses some stability property, the probability bound associated to non-stochastic abstractions is less conservative than that of stochastic ones. In this respect, we first quantify the probabilistic distance between the continuous-time stochastic control systems and that of their discrete-time (finite or infinite) abstractions. We then construct *finite* abstractions together with their corresponding stochastic simulation functions for a particular class of stochastic affine systems. Finally, to demonstrate the effectiveness of the proposed results, we apply our approaches to a temperature regulation in a building of two adjacent rooms and construct a discrete-time abstraction from original continuous-time dynamic. We

employ the constructed discrete-time abstraction as a substitute to synthesize policy regulating the temperature of rooms for a bounded time horizon.

In the second part of the chapter, we propose a *compositional framework* for the construction of discrete-time finite-space MDPs from continuous-time stochastic *hybrid* systems. We leverage sufficient small-gain conditions to provide the compositionality results which rely on the relation between continuous-time subsystems and their discrete-time counterparts based on stochastic simulation functions. We apply our approaches to a temperature regulation in a circular building (presented as a running example) and construct compositionally a discrete-time abstraction of a network containing 1000 rooms.

In the last part of the chapter, we derive dissipativity-type conditions to propose compositionality results for constructing finite MDPs from continuous-time continuous-space stochastic systems. The provided compositionality conditions can enjoy the structure of interconnection topology and be potentially fulfilled independently of the interconnection or gains of subsystems. We then focus on a particular class of stochastic affine systems and construct their finite abstractions together with their corresponding stochastic storage functions. Finally, we illustrate the effectiveness of the proposed techniques by applying them to a temperature regulation in a circular network containing 100 rooms.

3.2 Abstraction-based Synthesis of ct-SCS

In this section, we propose a systematic approach for the construction of discrete-time finite-space MDPs from continuous-time stochastic control systems (ct-SCS) as in Remark 2.3.3 but without internal input sets W. We establish a relation between the continuous-time system and its discrete-time counterpart based on stochastic simulation functions. We then leverage the constructed relation and compute a probability bound between continuous-time concrete systems and that of their discrete-time (in)finite abstractions. We focus on a particular class of stochastic affine systems and construct *finite* abstractions together with their corresponding stochastic simulation functions for this class of systems. We apply our approaches to a temperature regulation in a building of two adjacent rooms and construct a *discrete-time* abstraction from original continuous-time dynamic.

3.2.1 Discrete-Time Finite Abstractions of ct-SCS

Here, we discuss finite abstractions for continuous-time stochastic control systems. To do so, we first need to provide a time-discretized version of ct-SCS defined in Remark 2.3.3. Denote a discrete-time *infinite* abstraction of ct-SCS Σ as

$$\widetilde{\Sigma} = \Big(\tilde{X}, \tilde{U}, \subsetneq, \tilde{f}, \tilde{Y}, \tilde{h}\Big), \tag{3.2.1}$$

where:

- $\tilde{X} \subseteq \mathbb{R}^n$ is a Borel space as the state space of the system. We denote by $(\tilde{X}, \mathbb{B}(\tilde{X}))$ the measurable space with $\mathbb{B}(\tilde{X})$ being the Borel sigma-algebra on the state space;

- $\tilde{U} \subseteq \mathbb{R}^{\bar{m}}$ is a Borel space as the input space of the system;
- ς is a sequence of independent and identically distributed (i.i.d.) random variables from a sample space Ω to the set V_ς,

$$\varsigma := \{\varsigma(k) : \Omega \to V_\varsigma,\ k \in \mathbb{N}\};$$

- $\tilde{f} : \tilde{X} \times \tilde{U} \times V_\varsigma \to \tilde{X}$ is a measurable function characterizing the state evolution of the system;
- $\tilde{Y} \subseteq \mathbb{R}^{\bar{q}}$ is a Borel space as the output space of the system;
- $\tilde{h} : \tilde{X} \to \tilde{Y}$ is a measurable function that maps a state $\tilde{x} \in \tilde{X}$ to its output.

For given initial state $\tilde{a} = \tilde{\xi}(0) \in \tilde{X}$ and input sequence $\tilde{\nu}(\cdot) : \mathbb{N} \to \tilde{U}$, evolution of $\widetilde{\Sigma}$ can be written as

$$\widetilde{\Sigma} : \begin{cases} \tilde{\xi}(k+1) = \tilde{f}(\tilde{\xi}(k), \tilde{\nu}(k), \varsigma(k)), \\ \tilde{\zeta}(k) = \tilde{h}(\tilde{\xi}(k)), \end{cases} \qquad k \in \mathbb{N}. \tag{3.2.2}$$

We associate to $\tilde{U}$ the set $\tilde{\mathcal{U}}$ to be the collection of sequence $\{\tilde{\nu}(k) : \Omega \to \tilde{U},\ k \in \mathbb{N}\}$, in which $\tilde{\nu}(k)$ is independent of $\varsigma(z)$ for any $k, z \in \mathbb{N}$ and $z \geq k$. For any initial state $\tilde{a} \in \tilde{X}$, and $\tilde{\nu}(\cdot) \in \tilde{\mathcal{U}}$, the random sequences $\tilde{\xi}_{\tilde{a}\tilde{\nu}} : \Omega \times \mathbb{N} \to \tilde{X}$, $\tilde{\zeta}_{\tilde{a}\tilde{\nu}} : \Omega \times \mathbb{N} \to \tilde{Y}$ satisfying (3.2.2) are called, respectively, the *solution process* and *output trajectory* of $\widetilde{\Sigma}$ under an input $\tilde{\nu}$, and an initial state $\tilde{a}$.

To control the discrete-time stochastic control system presented in (3.2.2), we are interested in *Markov policies* similar to Definition 2.4.1 but for discrete-time stochastic control systems, as the following definition.

Definition 3.2.1. *A Markov policy for the discrete-time stochastic control system $\widetilde{\Sigma}$ in* (3.2.2) *is a sequence $\bar{\rho} = (\bar{\rho}_0, \bar{\rho}_1, \bar{\rho}_2, \ldots)$ of universally measurable stochastic kernels $\bar{\rho}_n$ [BS96], each defined on the input space $\tilde{U}$ given $\tilde{X}$ such that for all $\tilde{\xi}_n \in \tilde{X}$, $\bar{\rho}_n(\tilde{U}|\tilde{\xi}_n) = 1$. The class of all such Markov policies is denoted by $\Pi_{\bar{\rho}}$.*

Now we are interested in constructing *finite* abstractions of the *discrete-time* stochastic control systems $\widetilde{\Sigma}$ presented in (3.2.2). The abstraction algorithm in this work is based on finite partitions of sets $\tilde{X} = \cup_z \mathsf{X}_z$, and $\tilde{U} = \cup_z \mathsf{U}_z$, and selection of representative points $\hat{\xi}_z \in \mathsf{X}_z$ and $\hat{\nu}_z \in \mathsf{U}_z$ as abstract states and inputs as in the following definition.

Definition 3.2.2. *Given a ct-SCS $\Sigma = (X, U, \mathcal{U}, f, \sigma, Y, h)$, its finite abstraction $\widehat{\Sigma}$ can be represented as*

$$\widehat{\Sigma} = (\hat{X}, \hat{U}, \varsigma, \hat{f}, \hat{Y}, \hat{h}), \tag{3.2.3}$$

where $\hat{X} = \{\hat{\xi}_z, z = 1, \ldots, n_{\hat{\xi}}\}$ and $\hat{U} = \{\hat{\nu}_z, z = 1, \ldots, n_{\hat{\nu}}\}$ are the sets of selected representative points. Function $\hat{f} : \hat{X} \times \hat{U} \times V_\varsigma \to \hat{X}$ is defined as

$$\hat{f}(\hat{\xi}, \hat{\nu}, \varsigma) = \Phi_{\tilde{\xi}}(\tilde{f}(\hat{\xi}, \hat{\nu}, \varsigma)), \tag{3.2.4}$$

where $\Phi_{\tilde{\xi}} : \tilde{X} \to \hat{X}$ *is the map that assigns to any* $\tilde{\xi} \in \tilde{X}$*, the representative point* $\hat{\xi} \in \hat{X}$ *of the corresponding partition set containing* $\tilde{\xi}$*. The output map* $\hat{h}$ *is the same as* $\tilde{h}$ *with its domain restricted to finite state set* $\hat{X}$ *and the output set* $\hat{Y}$ *is just the image of* $\hat{X}$ *under* $\tilde{h}$*. The initial state of* $\widehat{\Sigma}$ *is also selected according to* $\hat{\xi}_0 := \Phi_{\tilde{\xi}}(\tilde{\xi}_0)$ *with* $\tilde{\xi}_0$ *being the initial state of* $\widetilde{\Sigma}$*.*

Abstraction map $\Phi_{\tilde{\xi}}$ presented in (3.2.4) satisfies the inequality

$$\|\Phi_{\tilde{\xi}}(\tilde{\xi}) - \tilde{\xi}\| \leq \delta, \quad \forall \tilde{\xi} \in \tilde{X}, \tag{3.2.5}$$

where δ is the *state* discretization parameter defined as $\delta := \sup\{\|\tilde{\xi} - \tilde{\xi}'\|,\ \tilde{\xi}, \tilde{\xi}' \in \mathsf{X}_z,\ z = 1, 2, \ldots, n_{\tilde{\xi}}\}$.

Remark 3.2.3. *Note that the proposed bound in* (3.2.5) *is valid for any type of norms provided that the state discretization parameter* δ *is defined based on the corresponding norm.*

In the next subsection, we provide an approach for the synthesis of *discrete-time* (finite or infinite) abstractions from ct-SCS. To do so, we first define the notion of sum-type stochastic simulation functions for quantifying the error in probability between original continuous-time stochastic control systems and that of their discrete-time (finite or infinite) abstractions.

3.2.2 sum-Type Stochastic Simulation Functions

Here, we first introduce the notion of sum-type stochastic simulation functions (SSF) for ct-SCS. We then employ this notion to quantify the probabilistic closeness between original continuous-time stochastic control systems and their discrete-time (finite or infinite) abstractions. We slightly abuse the notation and use $\widehat{\Sigma}$ interchangeably in the next definition to refer to both infinite abstractions $\widetilde{\Sigma}$ in (3.2.1) and finite abstractions $\widehat{\Sigma}$ in (3.2.3).

Definition 3.2.4. *Consider ct-SCS* $\Sigma = (X, U, \mathcal{U}, f, \sigma, Y, h)$ *and its (in)finite abstraction* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \varsigma, \hat{f}, \hat{Y}, \hat{h})$*. A function* $\mathcal{V} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ *is called a* sum*-type stochastic simulation function (*sum*-type SSF) from* $\widehat{\Sigma}$ *to* Σ *if*

- $\exists \alpha \in \mathcal{K}_\infty$ *such that*

$$\forall x \in X, \forall \hat{x} \in \hat{X}, \quad \alpha(\|h(x) - \hat{h}(\hat{x})\|) \leq \mathcal{V}(x, \hat{x}), \tag{3.2.6}$$

- $\forall k \in \mathbb{N}$, $\forall \xi := \xi(k\tau) \in X, \forall \hat{\xi} := \hat{\xi}(k) \in \hat{X}$*, and* $\forall \hat{\nu} := \hat{\nu}(k) \in \hat{U}$, $\exists \nu := \nu(k\tau) \in U$ *such that*

$$\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] - \mathcal{V}(\xi, \hat{\xi}) \leq -\kappa \mathcal{V}(\xi, \hat{\xi}) + \rho_{\text{ext}}(\|\hat{\nu}\|) + \psi, \tag{3.2.7}$$

for some chosen sampling time $\tau \in \mathbb{R}_{>0}$*,* $\kappa \in \mathbb{R}_{>0}$*,* $\rho_{\text{ext}} \in \mathcal{K}_\infty$*, and* $\psi \in \mathbb{R}_{>0}$*.*

We write $\widehat{\Sigma} \preceq^{\mathsf{sum}}_{S} \Sigma$ if there exists an SSF $\mathcal{V}$ from $\widehat{\Sigma}$ to Σ, and call the control system $\widehat{\Sigma}$ a *discrete-time* (in)finite abstraction of concrete (original) system Σ. Abstraction $\widehat{\Sigma}$ could be finite or infinite depending on cardinalities of sets $\hat{X}, \hat{U}$.

Remark 3.2.5. *Note that since the concrete system in this work is considered in continuous-time domain, one can employ Dynkin's formula [Dyn65] and establish the following equality:*

$$\begin{aligned}&\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau),\hat{\xi}(k+1)) \,\big|\, \xi(k\tau),\hat{\xi}(k),\nu(k\tau),\hat{\nu}(k)\Big]\\&\quad= \mathbb{E}_{\varsigma}\Big[\mathcal{V}(\xi(k\tau),\hat{\xi}(k+1)) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau} \mathcal{L}\mathcal{V}(\xi(t),\hat{\xi}(k+1))\mathsf{d}t\Big] \,\big|\, \hat{\xi}(k),\hat{\nu}(k)\Big],\end{aligned}$$

where $\mathcal{L}\mathcal{V}$ is the infinitesimal generator of the stochastic process acting on function $\mathcal{V}$ [ZMEM+14], and $\mathbb{E}_{\varsigma}$ is the conditional expectation acting only on the noise of the abstract system.

Condition (3.2.7) roughly speaking guarantees that if the concrete system and its abstraction start from two close initial conditions (guaranteed by condition (3.2.6)), then they remain close (in terms of expectation) after one step. This type of conditions is closely related to the ones in the notions of (bi)simulation relations [Tab09] in the deterministic case.

Condition (3.2.7) also implies implicitly the existence of a function $\nu(t) = \nu_{\hat{\nu}}(\xi(t), \hat{\xi}(k), \hat{\nu}(k)), k\tau \leq t \leq (k+1)\tau$, fulfilling inequality (3.2.7). This function is called an *interface function* and can be employed to refine a synthesized policy $\hat{\nu}$ for $\widehat{\Sigma}$ to a policy ν for Σ.

The next theorem shows how SSF can be used to compare output trajectories of original continuous-time stochastic systems and that of their discrete-time (finite or infinite) abstractions. We borrowed the theorem from [LSMZ17, Theorem 3.3] with a slight modification.

Theorem 3.2.6. *Let $\Sigma = (X, U, \mathcal{U}, f, \sigma, Y, h)$ be a ct-SCS and $\widehat{\Sigma} = (\hat{X}, \hat{U}, \varsigma, \hat{f}, \hat{Y}, \hat{h})$ its* discrete-time *(finite or infinite) abstraction. Suppose $\mathcal{V}$ is an SSF from $\widehat{\Sigma}$ to Σ. For any input trajectory $\hat{\nu}(\cdot) \in \hat{\mathcal{U}}$ that preserves Markov property for the closed-loop $\widehat{\Sigma}$, and for any random variables a and $\hat{a}$ as the initial states of the ct-SCS and its discrete-time abstraction, there exists an input trajectory $\nu(\cdot) \in \mathcal{U}$ of Σ through the interface function associated with $\mathcal{V}$ such that the following inequality holds:*

$$\begin{aligned}&\mathbb{P}\left\{\sup_{0\leq k\leq \mathcal{T}} \|\zeta_{a\nu}(k\tau) - \hat{\zeta}_{\hat{a}\hat{\nu}}(k)\| \geq \varepsilon \,|\, a, \hat{a}\right\} \qquad (3.2.8)\\&\leq \begin{cases} 1-(1-\frac{\mathcal{V}(a,\hat{a})}{\alpha(\varepsilon)})(1-\frac{\hat{\psi}}{\alpha(\varepsilon)})^{\mathcal{T}}, & \text{if } \alpha(\varepsilon) \geq \frac{\hat{\psi}}{1-\kappa},\\ (\frac{\mathcal{V}(a,\hat{a})}{\alpha(\varepsilon)})\kappa^{\mathcal{T}} + (\frac{\hat{\psi}}{(1-\kappa)\alpha(\varepsilon)})(1-\kappa^{\mathcal{T}}), & \text{if } \alpha(\varepsilon) < \frac{\hat{\psi}}{1-\kappa},\end{cases}\end{aligned}$$

where constant $\hat{\psi} \geq 0$ satisfies $\hat{\psi} \geq \rho_{\text{ext}}(\|\hat{\nu}\|_{\infty}) + \psi$.

3.2.3 Construction of Finite Abstraction

In the previous section, $\widehat{\Sigma}$ were considered as general *discrete-time* stochastic control systems without discussing the cardinality of their state sets. In this section, we consider Σ as an infinite ct-SCS and $\widehat{\Sigma}$ as its discrete-time *finite* abstraction constructed as in Subsection 3.2.1. We impose conditions on the infinite ct-SCS Σ enabling us to find an SSF from its finite abstraction $\widehat{\Sigma}$ to Σ. The required conditions are presented for a particular class of continuous-time stochastic affine systems as in the following subsection.

3.2.3.1 Stochastic Affine Systems

Here, we focus on a special class of continuous-time stochastic affine systems Σ and *quadratic* stochastic simulation functions $\mathcal{V}$. First, we formally define this class of systems. Afterwards, we construct their finite MDPs $\widehat{\Sigma}$ as in Subsection 3.2.1, and then provide conditions under which a nominated $\mathcal{V}$ is an SSF from $\widehat{\Sigma}$ to Σ.

The class of continuous-time stochastic affine systems is given by

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = (A\xi(t) + B\nu(t) + \mathbf{b})\mathsf{d}t + G\mathsf{d}W_t, \\ \zeta(t) = C\xi(t), \end{cases} \tag{3.2.9}$$

where $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}, C \in \mathbb{R}^{q\times n}$, $G \in \mathbb{R}^n$, and $\mathbf{b} \in \mathbb{R}^n$. We use the tuple

$$\Sigma = (A, B, C, G, \mathbf{b}),$$

to refer to the class of stochastic affine systems in (3.2.9). The discrete-time *infinite* abstraction of Σ is described by

$$\widetilde{\Sigma} : \begin{cases} \tilde{\xi}(k+1) = \tilde{\xi}(k) + \tilde{\nu}(k) + \tilde{R}\varsigma(k), \\ \tilde{\zeta}(k) = \tilde{C}\tilde{\xi}(k), \end{cases} \qquad k \in \mathbb{N},$$

where $\tilde{R}$ is an arbitrary chosen matrix. Later, we show that $\tilde{R} = \mathbf{0}_n$ results in less approximation errors (cf. Remark 3.2.11). Then we present the discrete-time *finite* abstraction of $\widetilde{\Sigma}$ as

$$\widehat{\Sigma} : \begin{cases} \hat{\xi}(k+1) = \Phi_{\tilde{\xi}}(\hat{\xi}(k) + \hat{\nu}(k) + \tilde{R}\varsigma(k)), \\ \hat{\zeta}(k) = \hat{C}\hat{\xi}(k), \end{cases} \qquad k \in \mathbb{N},$$

where map $\Phi_{\tilde{\xi}} : \tilde{X} \to \hat{X}$ satisfies inequality (3.2.5). Now we nominate the following *quadratic* simulation function

$$\mathcal{V}(x, \hat{x}) = (x - \hat{x})^\top \mathcal{M}(x - \hat{x}), \tag{3.2.10}$$

where $\mathcal{M}$ is a positive-definite matrix of appropriate dimension. In order to show that $\mathcal{V}$ in (3.2.10) is an SSF from $\widehat{\Sigma}$ to Σ, we require the following two key assumptions on Σ.

Assumption 3.2.7. *Assume that there exists a concave function $\gamma \in \mathcal{K}_\infty$ such that $\mathcal{V}$ satisfies*

$$\mathcal{V}(x, x') - \mathcal{V}(x, x'') \leq \gamma(\|x' - x''\|), \tag{3.2.11}$$

for any $x, x', x'' \in X$.

Note that as shown in [ZMEM+14] and by employing the mean value theorem, Assumption 3.2.7 is always satisfied for any differentiable function $\mathcal{V}$ restricted to a compact subset of $X \times X$.

Assumption 3.2.8. *Let $\Sigma = (A, B, C, G, \mathbf{b})$. Assume that for some constant $\tilde{\kappa} \in \mathbb{R}_{>0}$, there exist matrices $\mathcal{M} \succ 0$, K and Q of appropriate dimensions such that the following matrix (in)equalities hold:*

$$(A + BK)^\top \mathcal{M} + \mathcal{M}(A + BK) \leq -\tilde{\kappa}\mathcal{M}, \tag{3.2.12}$$

$$BQ = A. \tag{3.2.13}$$

Note that there exists matrix Q satisfying (3.2.13) if and only if im $A \subseteq$ im B. Now, we provide one of the main results of this section showing that under some conditions $\mathcal{V}$ nominated in (3.2.10) is an SSF from $\widehat{\Sigma}$ to Σ.

Theorem 3.2.9. *Let $\Sigma = (A, B, C, G, \mathbf{b})$ and $\widehat{\Sigma}$ be its finite Markov decision process with discretization parameter δ. Suppose Assumptions 3.2.7 and 3.2.8 hold, and $\hat{C} = \tilde{C} = C$. Then function $\mathcal{V}$ nominated in* (3.2.10) *is an SSF from $\widehat{\Sigma}$ to Σ.*

Proof. We first show that condition (3.2.6) holds. Since $\hat{C} = C$, we have $\|Cx - \hat{C}\hat{x}\|^2 = (x - \hat{x})^\top C^\top C(x - \hat{x})$. Since $\lambda_{\min}(C^\top C)\|x - \hat{x}\|^2 \leq (x - \hat{x})^\top C^\top C(x - \hat{x}) \leq \lambda_{\max}(C^\top C)\|x - \hat{x}\|^2$, and similarly $\lambda_{\min}(\mathcal{M})\|x - \hat{x}\|^2 \leq (x - \hat{x})^\top \mathcal{M}(x - \hat{x}) \leq \lambda_{\max}(\mathcal{M})\|x - \hat{x}\|^2$, it can be readily verified that $\frac{\lambda_{\min}(\mathcal{M})}{\lambda_{\max}(C^\top C)}\|Cx - \hat{C}\hat{x}\|^2 \leq \mathcal{V}(x, \hat{x})$ holds $\forall x \in X$, $\forall \hat{x} \in \hat{X}$, implying that condition (3.2.6) holds with $\alpha(s) = \frac{\lambda_{\min}(\mathcal{M})}{\lambda_{\max}(C^\top C)} s^2$, $\forall s \in \mathbb{R}_{\geq 0}$. We proceed with showing that condition (3.2.7) holds, as well. Using Assumption 3.2.7, we have

$$\begin{aligned}
&\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\Big|\, \xi = \xi(k\tau), \hat{\xi} = \hat{\xi}(k), \nu = \nu(k\tau), \hat{\nu} = \hat{\nu}(k)\Big] - \mathcal{V}(\xi, \hat{\xi}) \\
&= \mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] - \mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] \\
&\quad + \mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] - \mathcal{V}(\xi, \hat{\xi}) \\
&= \mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|) \,\Big|\, \hat{\xi}, \hat{\nu}\Big] - \mathcal{V}(\xi, \hat{\xi}).
\end{aligned}$$

Now by employing Dynkin's formula [Dyn65], one obtains

$$\begin{aligned}
&\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|) \,\Big|\, \hat{\xi}, \hat{\nu}\Big] - \mathcal{V}(\xi, \hat{\xi}) \\
&= \mathbb{E}_\varsigma\Big[\mathcal{V}(\xi, \hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau} \mathcal{L}\mathcal{V}(\xi(t), \hat{\xi})\mathsf{d}t\Big] \,\Big|\, \hat{\xi}, \hat{\nu}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|) \big| \hat{\xi}, \hat{\nu}\Big] - \mathcal{V}(\xi, \hat{\xi}).
\end{aligned}$$

Since the abstract system $\widehat{\Sigma}$ is considered in *discrete-time* domain, then the infinitesimal generator $\mathcal{L}\mathcal{V}(x,\hat{x})$ here is different from the usual one that was employed in [ZMEM+14] and is defined as

$$\mathcal{L}\mathcal{V}(x,\hat{x}) = \partial_x \mathcal{V}(x,\hat{x}) f(x,\nu) + \frac{1}{2}\mathsf{Tr}(\sigma(x)\sigma(x)^\top \partial_{x,x}\mathcal{V}(x,\hat{x})). \tag{3.2.14}$$

Then one has

$$\begin{aligned}
&\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}\mathcal{L}\mathcal{V}(\xi(t),\hat{\xi})\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&\quad=\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2(\xi(t)-\hat{\xi})^\top\mathcal{M}(A\xi(t)+B\nu(t)+\mathbf{b})+G^\top\mathcal{M}G)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\qquad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,|\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi}).
\end{aligned}$$

Given any $\xi(t)$, $\hat{\xi}(k)$, and $\hat{\nu}(k)$, we choose $\nu(t)$ via the following *interface* function:

$$\nu(t) = K(\xi(t)-\hat{\xi}(k)) - Q\hat{\xi}(k) + H\hat{\nu}(k), \tag{3.2.15}$$

where $k\tau \le t \le (k+1)\tau$, and H is a matrix of an appropriate dimension. By employing condition (3.2.13), and the definition of the *interface* function in (3.2.15), we have

$$\begin{aligned}
&\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2(\xi(t)-\hat{\xi})^\top\mathcal{M}(A\xi(t)+B\nu(t)+\mathbf{b})+G^\top\mathcal{M}G)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,|\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&=\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2\,(\xi(t)-\hat{\xi})^\top\mathcal{M}((A+BK)(\xi(t)-\hat{\xi})+BH\hat{\nu}+\mathbf{b})+G^\top\mathcal{M}G)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi}).
\end{aligned}$$

Using Young's inequality [You12] as $ab \le \frac{\pi}{2}a^2 + \frac{1}{2\pi}b^2$, for any $a,b\ge 0$ and any $\pi>0$, by employing Cauchy-Schwarz inequality and using condition (3.2.12), one has

$$\begin{aligned}
&\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2\,(\xi(t)-\hat{\xi})^\top\mathcal{M}((A+BK)(\xi(t)-\hat{\xi})+BH\hat{\nu}+\mathbf{b})+G^\top\mathcal{M}G)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&\le\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(-\tilde{\kappa}\mathcal{V}(\xi(t),\hat{\xi})+\pi\|\sqrt{\mathcal{M}}BH\|^2\|\hat{\nu}\|^2+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+G^\top\mathcal{M}G)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&=\mathbb{E}_\varsigma\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}-\tilde{\kappa}\mathcal{V}(\xi(t),\hat{\xi})\mathsf{d}t+\tau(\pi\|\sqrt{\mathcal{M}}BH\|^2\|\hat{\nu}\|^2+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+G^\top\mathcal{M}G)\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi}).
\end{aligned}$$

Using Grönwall inequality [Gro19], one has

$$\begin{aligned}
&\mathbb{E}_{\varsigma}\Big[\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}-\tilde{\kappa}\mathcal{V}(\xi(t),\hat{\xi})\mathrm{d}t+\tau(\pi\|\sqrt{\mathcal{M}}BH\|^2\|\hat{\nu}\|^2+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+G^\top MG)\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&\leq\mathbb{E}_{\varsigma}\Big[e^{-\tilde{\kappa}\tau}\mathcal{V}(\xi,\hat{\xi})+\mathbb{E}\Big[e^{-\tilde{\kappa}\tau}\tau(\pi\|\sqrt{\mathcal{M}}BH\|^2\|\hat{\nu}\|^2+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+G^\top\mathcal{M}G)\Big]\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&=-(1-e^{-\tilde{\kappa}\tau})\mathcal{V}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau\pi\|\sqrt{\mathcal{M}}BH\|^2\|\hat{\nu}\|^2+e^{-\tilde{\kappa}\tau}\tau(G^\top\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)\\
&\quad+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu}\Big].
\end{aligned}$$

Since function γ defined in Assumption 3.2.7 is *concave*, using Jensen inequality one has

$$\begin{aligned}
\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]&=\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-(\hat{\xi}+\hat{\nu}+\tilde{R}\varsigma)+(\hat{\xi}+\hat{\nu}+\tilde{R}\varsigma)-\hat{\xi}\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]\\
&\leq\mathbb{E}\Big[\gamma(\delta+\|\hat{\nu}+\tilde{R}\varsigma\|)\,\big|\,\hat{\xi},\hat{\nu}\Big]\leq\gamma((1+\varrho)\delta)+\mathbb{E}\Big[\gamma((1+\frac{1}{\varrho})\|\hat{\nu}+\tilde{R}\varsigma\|)\big|\hat{\xi},\hat{\nu}\Big]\\
&\leq\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}\|)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\mathbb{E}\Big[\|\tilde{R}\varsigma\|\,\big|\,\hat{\xi},\hat{\nu}\Big])\\
&=\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}\|)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\mathbb{E}\Big[([\tilde{R}\varsigma]^\top[\tilde{R}\varsigma])^{\frac{1}{2}}\,\big|\,\hat{\xi},\hat{\nu}\Big])\\
&\leq\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}\|)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})(\mathbb{E}\Big[[\tilde{R}\varsigma]^\top[\tilde{R}\varsigma]\,\big|\,\hat{\xi},\hat{\nu}\Big])^{\frac{1}{2}})\\
&=\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}\|)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})}),
\end{aligned}$$

where $\varrho,\varrho'\in\mathbb{R}_{>0}$. Then one can conclude that

$$\begin{aligned}
&\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau),\hat{\xi}(k+1))\,\big|\,\xi,\hat{\xi},\nu,\hat{\nu}\Big]-\mathcal{V}(\xi,\hat{\xi})\\
&\quad\leq-(1-e^{-\tilde{\kappa}\tau})\mathcal{V}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau\pi\|\sqrt{M}BH\|^2\|\hat{\nu}\|^2+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}\|)\\
&\qquad+e^{-\tilde{\kappa}\tau}\tau(G^\top MG+\pi\|\sqrt{M}\mathbf{b}\|^2)+\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})}),
\end{aligned}$$

which completes the proof with $\alpha(s)=\frac{\lambda_{\min}(\mathcal{M})}{\lambda_{\max}(C^\top C)}s^2,\forall s\in\mathbb{R}_{\geq0}$, $\kappa:=1-e^{-\tilde{\kappa}\tau}$, $\rho_{\text{ext}}(s):=e^{-\tilde{\kappa}\tau}\tau\pi\|\sqrt{\mathcal{M}}BH\|^2s^2+\gamma((1+\frac{1}{\varrho})(1+\varrho')s),\forall s\in\mathbb{R}_{\geq0}$, and $\psi=e^{-\tilde{\kappa}\tau}\tau(G^\top\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)+\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})})$. ■

Remark 3.2.10. *Note that if γ is linear, then ρ_{ext} and ψ defined in* (3.2.7) *are reduced to $\rho(s):=e^{-\tilde{\kappa}\tau}\tau\pi\|\sqrt{\mathcal{M}}BH\|^2s^2+\gamma(s),\forall s\in\mathbb{R}_{\geq0}$, and $\psi:=e^{-\tilde{\kappa}\tau}\tau(G^\top\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)+\gamma(\delta)+\gamma(\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})})$.*

Remark 3.2.11. *Note that if the abstraction $\widehat{\Sigma}$ is infinite (i.e., $\widetilde{\Sigma}$), ρ_{ext} and ψ defined in (3.2.7) are reduced to $\rho_{\text{ext}}(s) := e^{-\tilde{\kappa}\tau}\tau\pi\|\sqrt{\mathcal{M}}BH\|^2 s^2 + \gamma((1+\varrho)s), \forall s \in \mathbb{R}_{\geq 0}$, and $\psi := e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2) + \gamma((1+\frac{1}{\varrho})\sqrt{\mathsf{Tr}(\tilde{R}^\top \tilde{R})})$. Moreover, if the abstraction $\widehat{\Sigma}$ is infinite and non-stochastic, ρ_{ext} and ψ are reduced to $\rho_{\text{ext}}(s) := e^{-\tilde{\kappa}\tau}\tau\pi\|\sqrt{\mathcal{M}}BH\|^2 s^2 + \gamma(s), \forall s \in \mathbb{R}_{\geq 0}$, and $\psi := e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)$. This means if the concrete system possesses some stability property and the concrete and abstract systems are, respectively, in continuous-time and discrete-time domain, it is actually better to go to non-stochastic abstractions than stochastic ones since non-stochastic abstractions are closer than stochastic versions (cf. the case study) to concrete systems.*

3.2.4 Case Study

To demonstrate the effectiveness of our proposed approaches, we apply our results to the temperature regulation in a building of two adjacent rooms, each equipped with a heater. The model of this case study is borrowed from [GGM16] with slight modifications and by including stochasticity in the model. We want to first present a *discrete-time* infinite abstraction, and then employ the discrete-time abstraction as a substitute to synthesize policy regulating the temperature of the rooms for a bounded time horizon.

The evolution of the temperature $T(\cdot)$ can be described by the following stochastic differential equation

$$\Sigma\colon \begin{cases} \mathsf{d}T(t) = (AT(t) + \hat{\theta}T_h\nu(t) + \hat{\beta}T_E)\mathsf{d}t + 0.5\mathbb{1}_2\mathsf{d}W_t, \\ \zeta(t) = T(t), \end{cases} \tag{3.2.16}$$

where

$$A = \begin{bmatrix} -2\hat{\eta} - \hat{\beta} & \hat{\eta} \\ \hat{\eta} & -2\hat{\eta} - \hat{\beta} \end{bmatrix},\ T_E = [T_{e_1}; T_{e_2}],\ T(t) = [T_1(t); T_2(t)],\ \nu(t) = [\nu_1(t); \nu_2(t)].$$

Moreover, parameters $\hat{\eta} = 0.05$, $\hat{\beta} = 0.005$, and $\hat{\theta} = 0.01$ are conduction factors, respectively, between the two rooms, between the external environment and each room, and between the heater and each room. Furthermore, parameters $T_{e_i} = -1\,^\circ C$, $i \in \{1, 2\}$, are outside temperatures, $T_h = 50\,^\circ C$ is the heater temperature, and $T_i(t)$, $i \in \{1, 2\}$, are taking values in $[20, 21]$. The discrete-time *infinite* abstraction of Σ is given by

$$\widetilde{\Sigma}\colon \begin{cases} \tilde{T}(k+1) = \tilde{T}(k) + \tilde{\nu}(k), \\ \tilde{\zeta}(k) = \tilde{T}(k), \end{cases} \qquad k \in \mathbb{N},$$

where $\tilde{\nu}(k) = [\tilde{\nu}_1(k); \tilde{\nu}_2(k)]$, and $\tilde{\nu}_i(k)$, $i \in \{1, 2\}$. Then, one can readily verify that conditions (3.2.12)-(3.2.13) are satisfied by

$$K = \begin{bmatrix} -1.808 & -1.734 \\ -1.734 & -1.808 \end{bmatrix},\quad Q = \begin{bmatrix} -0.21 & 0.1 \\ 0.1 & -0.21 \end{bmatrix},\quad \mathcal{M} = \mathbb{I}_2,\quad \tilde{\kappa} = 1.8.$$

By taking $\tau = 0.001$ and $H = 0.1\mathbb{I}_2$, the function $\mathcal{V}(T(k\tau), \tilde{T}(k)) = (T(k\tau) - \tilde{T}(k))^\top (T(k\tau) - \tilde{T}(k))$ is an SSF from $\widetilde{\Sigma}$ to Σ satisfying condition (3.2.6) with $\alpha(s) = s^2$ and condition (3.2.7) with $\kappa = 0.001s$, $\rho_{\text{ext}}(s) = 4.99 \times 10^{-6}s^2 + 2.82s$, $\forall s \in \mathbb{R}_{\geq 0}$, and $\psi = 4.992 \times 10^{-4}$.

Now by taking the initial states of Σ and $\widetilde{\Sigma}$ as $[20.3; 20.7]$, and employing Theorem 3.2.6, one can guarantee that the distance between outputs of Σ and $\widetilde{\Sigma}$ will not exceed $\varepsilon = 0.5$ during the time horizon $\mathcal{T} = 7$ with a probability of at least 88%, *i.e.,*

$$\mathbb{P}(\|\zeta(k\tau) - \tilde{\zeta}(k)\| \leq 0.5,\ \forall k \in [0, 7]) \geq 0.88\,.$$

Let us now synthesize a controller for Σ via its *discrete-time* abstraction $\widetilde{\Sigma}$ such that the controller maintains the temperature of each room in the comfort zone $[20, 21]$. We design a controller for the discrete-time abstract system $\widetilde{\Sigma}$, and then refine the controller back to Σ using an interface function. We employ the tool `SCOTS` [RZ16] to synthesize controllers for $\widetilde{\Sigma}$ keeping the temperature of each room in the safe set $[20, 21]$. Closed-loop state trajectories of two rooms with different noise realizations are illustrated in Figure 3.1. Furthermore, several realizations of the norm of the error between outputs of Σ and $\widetilde{\Sigma}$ are illustrated in Figure 3.2. In order to have some more analysis on the provided probabilistic bound, we also run Monte Carlo simulation of 10000 runs. In this case, one can statistically guarantee that the distance between outputs of Σ and $\widetilde{\Sigma}$ is always less than or equal to 0.19 with the same probability, (*i.e.,* at least 88%). This issue is expected and the reason is due to the conservatism nature of Lyapunov-like techniques (simulation functions), but with the gain of having formal guarantee on the output trajectories rather than empirical ones. Note that we have intentionally dropped the noise of the *discrete-time* abstraction and employed `SCOTS` here to show that if the concrete system possesses some stability property and the two systems are in continuous-time and discrete-time domain, it is actually better to construct and employ the non-stochastic abstractions since non-stochastic abstractions are closer than the stochastic ones (as discussed in Remark 3.2.11) to concrete systems.

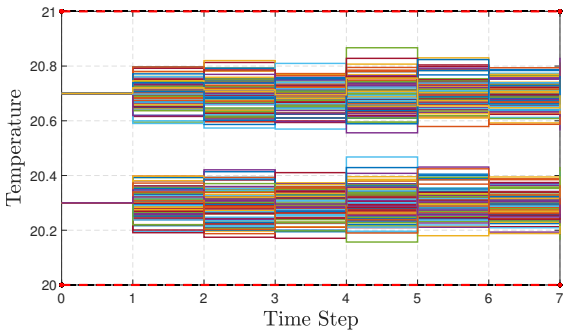

Figure 3.1: Closed-loop state trajectories of two rooms with different noise realizations, for $\mathcal{T} = 7$.

3.3 Compositional Abstraction-based Synthesis of ct-SHS: Small-Gain Approach

In this section, we enlarge the class of models to continuous-time stochastic *hybrid* systems (ct-SHS) as in Definition 2.3.1 by adding Poisson process to the dynamics and pro-

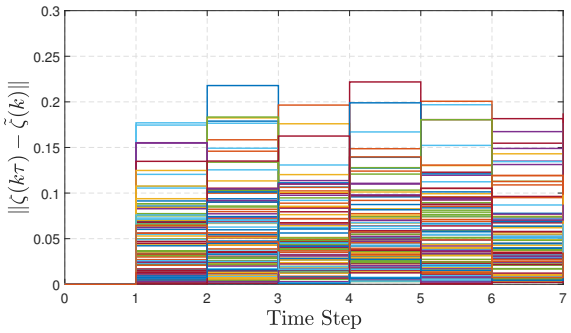

Figure 3.2: Several realizations of the norm of the error between outputs of Σ and of $\widetilde{\Sigma}$, *e.g.*, $\|\zeta(k\tau) - \tilde{\zeta}(k)\|$, for $\mathcal{T} = 7$.

pose a *compositional framework* for the construction of discrete-time finite-space MDPs for this class of systems. We utilize sufficient small-gain conditions to provide the compositionality results which rely on the relation between the continuous-time subsystems and their discrete-time counterparts based on *stochastic simulation functions*. This type of relations enables us to compute a probability bound between the interconnection of continuous-time concrete subsystems and that of their discrete-time (in)finite abstractions. We show that if the original stochastic hybrid system has a stability property, the probability bound associated with non-stochastic abstractions is less conservative than that of stochastic ones. In this respect, we first compositionally quantify the distance between the interconnection of continuous-time stochastic hybrid subsystems and that of their discrete-time (finite or infinite) abstractions in a probabilistic setting. We also generalize our construction scheme to a particular class of *nonlinear* stochastic hybrid systems and construct finite abstractions together with their corresponding stochastic simulation functions for this class of systems. We apply our approaches to a temperature regulation in a circular building (presented as a running example) and construct compositionally a discrete-time abstraction of a network containing 1000 rooms. We employ the constructed discrete-time abstractions as substitutes to compositionally synthesize policies regulating the temperature of each room for a bounded time horizon.

3.3.1 Discrete-Time Finite Abstractions of ct-SHS

Here, the infinite abstraction refers to an approximation of the original system in the discrete-time but continuous-space domain, while the finite abstraction is another approximation in both discrete-time and discrete state set. In order to propose the construction procedure for finite abstractions, we first need to introduce infinite abstractions as time-discretized versions of ct-SHS similar to (3.2.1).

A *discrete-time infinite* abstraction of ct-SHS Σ is denoted by the tuple

$$\widetilde{\Sigma} = \Big(\tilde{X}, \tilde{U}, \tilde{W}, \varsigma, \tilde{f}, \tilde{Y}, \tilde{h}\Big), \tag{3.3.1}$$

where $\tilde{U} \subseteq \mathbb{R}^{\bar{m}}$ and $\tilde{W} \subseteq \mathbb{R}^{\bar{p}}$ are Borel spaces as *external and internal* input spaces of the system, respectively. For given initial state $\tilde{a} = \tilde{x}(0) \in \tilde{X}$ and input sequences $\{\tilde{\nu}(k) : \Omega \to \tilde{U},\ k \in \mathbb{N}\}$ and $\{\tilde{w}(k) : \Omega \to \tilde{W},\ k \in \mathbb{N}\}$, evolution of $\widetilde{\Sigma}$ can be written as

$$\widetilde{\Sigma}\colon \begin{cases} \tilde{\xi}(k+1) = \tilde{f}(\tilde{\xi}(k), \tilde{\nu}(k), \tilde{w}(k), \varsigma(k)), \\ \tilde{\zeta}(k) = \tilde{h}(\tilde{\xi}(k)), \end{cases} \qquad k \in \mathbb{N}. \tag{3.3.2}$$

We associate to $\tilde{U}$ and $\tilde{W}$ the sets $\tilde{\mathcal{U}}$ and $\tilde{\mathcal{W}}$ to be the collections of sequences $\{\tilde{\nu}(k) : \Omega \to \tilde{U},\ k \in \mathbb{N}\}$ and $\{\tilde{w}(k) : \Omega \to \tilde{W},\ k \in \mathbb{N}\}$, in which $\tilde{\nu}(k)$ and $\tilde{w}(k)$ are independent of $\varsigma(z)$ for any $k, z \in \mathbb{N}$ and $z \geq k$. For any initial state $\tilde{a} \in \tilde{X}$, $\tilde{\nu}(\cdot) \in \tilde{\mathcal{U}}$ and $\tilde{w}(\cdot) \in \tilde{\mathcal{W}}$, the random sequences $\tilde{\xi}_{\tilde{a}\tilde{\nu}\tilde{w}} : \Omega \times \mathbb{N} \to \tilde{X}$, $\tilde{\zeta}_{\tilde{a}\tilde{\nu}\tilde{w}} : \Omega \times \mathbb{N} \to \tilde{Y}$ satisfying (3.3.2) are respectively called the *solution process* and *output trajectory* of $\widetilde{\Sigma}$ under an external input $\tilde{\nu}$, an internal input $\tilde{w}$, and an initial state $\tilde{a}$.

A discrete-time infinite abstraction of ct-SHS Σ in (3.3.1) can be *equivalently* represented as an MDP [HSA17]

$$\widetilde{\Sigma} = \Big(\tilde{X}, \tilde{U}, \tilde{W}, \tilde{T}_{\mathsf{x}}, \tilde{Y}, \tilde{h}\Big),$$

where the map $\tilde{T}_{\mathsf{x}} : \mathbb{B}(\tilde{X}) \times \tilde{X} \times \tilde{U} \times \tilde{W} \to [0,1]$, is a conditional stochastic kernel that assigns to any $\tilde{x} \in \tilde{X}$, $\tilde{\nu} \in \tilde{U}$, and $\tilde{w} \in \tilde{W}$, a probability measure $\tilde{T}_{\mathsf{x}}(\cdot|\tilde{x}, \tilde{\nu}, \tilde{w})$ on the measurable space $(\tilde{X}, \mathbb{B}(\tilde{X}))$ so that for any set $\mathcal{A} \in \mathbb{B}(\tilde{X})$,

$$\mathbb{P}(\tilde{x}(k+1) \in \mathcal{A} \,|\, \tilde{x}(k), \tilde{\nu}(k), \tilde{w}(k)) = \int_{\mathcal{A}} \tilde{T}_{\mathsf{x}}(\mathsf{d}\tilde{x}(k+1)|\tilde{x}(k), \tilde{\nu}(k), \tilde{w}(k)).$$

For given inputs $\tilde{\nu}(\cdot), \tilde{w}(\cdot)$, the stochastic kernel $\tilde{T}_{\mathsf{x}}$ captures the evolution of the state of $\widetilde{\Sigma}$ and can be uniquely determined by the pair $(\varsigma, \tilde{f})$ from (3.3.1).

Given the discrete-time stochastic hybrid system presented in (3.3.2), we are interested in a *Markov policies* similar to the one presented in Definition 3.2.1. In particular, the Markov policy here observes the exact values of state $\tilde{\xi}(k) \in \tilde{X}$ and internal input $\tilde{w}(k) \in \tilde{W}$ at time step k, and selects the external input $\tilde{\nu}(k) \in \tilde{U}$ as a sample from the probability measure $\bar{\rho}(\cdot \,|\, \tilde{\xi}(k), \tilde{w}(k))$.

Now we proceed with constructing finite MDPs $\widehat{\Sigma}$ as finite abstractions of the *discrete-time* stochastic hybrid systems $\widetilde{\Sigma}$ presented in (3.3.2). To do so, we assume the state and input sets of $\widetilde{\Sigma}$ are restricted to compact subsets over which we are interested to perform the synthesis. The rest of the state sets can be considered as single absorbing states in both $\widetilde{\Sigma}$ and $\widehat{\Sigma}$. In order to make the notation easier, we assume this procedure is already applied to the system and eliminate the absorbing states from the presentation. Then the abstraction algorithm is based on finite partitions of sets $\tilde{X} = \cup_z \mathsf{X}_z$, $\tilde{U} = \cup_z \mathsf{U}_z$, and $\tilde{W} = \cup_z \mathsf{W}_z$ and selection of representative points $\hat{\xi}_z \in \mathsf{X}_z$, $\hat{\nu}_z \in \mathsf{U}_z$, and $\hat{w}_z \in \mathsf{W}_z$ as abstract states and inputs as in the following definition.

Definition 3.3.1. *Given a ct-SHS $\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, \rho, Y, h)$ with its time-discretized version $\widetilde{\Sigma} = \Big(\tilde{X}, \tilde{U}, \tilde{W}, \varsigma, \tilde{f}, \tilde{Y}, \tilde{h}\Big)$, the finite abstraction $\widehat{\Sigma}$ can be represented as*

$$\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{W}, \varsigma, \hat{f}, \hat{Y}, \hat{h}),$$

where $\hat{X} = \{\hat{\xi}_z, z = 1, \ldots, n_{\tilde{\xi}}\}$, $\hat{U} = \{\hat{\nu}_z, z = 1, \ldots, n_{\tilde{\nu}}\}$, *and* $\hat{W} = \{\hat{w}_z, z = 1, \ldots, n_{\tilde{w}}\}$ *are the sets of selected representative points. Function* $\hat{f} : \hat{X} \times \hat{U} \times \hat{W} \times V_\varsigma \to \hat{X}$ *is defined as*

$$\hat{f}(\hat{\xi}, \hat{\nu}, \hat{w}, \varsigma) = \Phi_{\tilde{\xi}}(\tilde{f}(\hat{\xi}, \hat{\nu}, \hat{w}, \varsigma)), \tag{3.3.3}$$

where the quantization map $\Phi_{\tilde{\xi}} : \tilde{X} \to \hat{X}$ *satisfies inequality* (3.2.5).

Remark 3.3.2. *Note that there is no restriction on discretizing the state, external and internal input sets. However, the size of the state discretization parameter* δ *appears in the formulated error (cf.* (3.3.27)*): one can decrease the error by reducing the state discretization parameter. We also do not have any constraint on the shape of the partition elements in constructing the finite MDPs. For the sake of an easier implementation, one can consider the partition sets as boxes and the center of each box as representative points.*

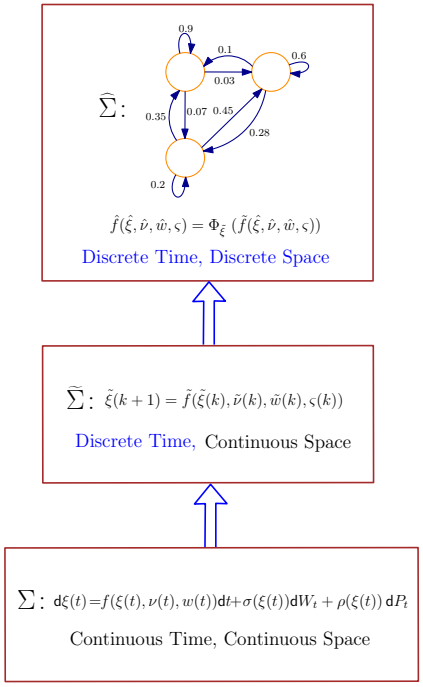

Figure 3.3: A schematic relation between Σ, $\widetilde{\Sigma}$, and $\widehat{\Sigma}$.

A schematic relation between Σ, $\widetilde{\Sigma}$, and $\widehat{\Sigma}$ is depicted in Figure 3.3. In the next subsections, we provide a framework for compositional synthesis of interconnected *discrete-time* (finite or infinite) abstractions from ct-SHS. We define notions of max-type stochastic pseudo-simulation and simulation functions for quantifying the probabilistic error between original *continuous-time* stochastic hybrid systems and that of their *discrete-time* (finite or infinite) abstractions with and without internal signals, respectively.

3.3.2 max-Type Stochastic Pseudo-Simulation and Simulation Functions

Here, we first introduce a notion of max-type stochastic pseudo-simulation functions (SPSF) for ct-SHS with both internal and external inputs. We then define a notion of max-type stochastic simulation functions (SSF) for ct-SHS with only external inputs. We mainly employ these two definitions to quantify the probabilistic closeness of interconnected *continuous-time* stochastic hybrid systems and their *discrete-time* (finite or infinite) abstractions.

Definition 3.3.3. *Consider a ct-SHS* $\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, \rho, Y, h)$ *and its (in)finite abstraction* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{W}, \varsigma, \hat{f}, \hat{Y}, \hat{h})$ *with internal inputs. A function* $\mathcal{S} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ *is called a* max*-type stochastic pseudo-simulation function (*max*-type SPSF) from* $\widehat{\Sigma}$ *to* Σ *if*

- $\exists \alpha \in \mathcal{K}_\infty$ *such that*

$$\forall x \in X, \forall \hat{x} \in \hat{X}, \quad \alpha(\|h(x) - \hat{h}(\hat{x})\|_\infty) \leq \mathcal{S}(x, \hat{x}), \tag{3.3.4}$$

- $\forall k \in \mathbb{N}$, $\forall \xi := \xi(k\tau) \in X, \forall \hat{\xi} := \hat{\xi}(k) \in \hat{X}$, *and* $\forall \hat{\nu} := \hat{\nu}(k) \in \hat{U}$, $\forall w := w(k\tau) \in W$, $\forall \hat{w} := \hat{w}(k) \in \hat{W}$, $\exists \nu := \nu(k\tau) \in U$ *such that*

$$\begin{aligned} &\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}, w, \hat{w}\Big] \\ &\quad \leq \max\Big\{\kappa \mathcal{S}(\xi, \hat{\xi}), \rho_{\text{int}}(\|w - \hat{w}\|_\infty), \rho_{\text{ext}}(\|\hat{\nu}\|_\infty), \psi\Big\}, \end{aligned} \tag{3.3.5}$$

  for some chosen sampling time $\tau \in \mathbb{R}_{>0}$, $0 < \kappa < 1$, $\rho_{\text{ext}}, \rho_{\text{int}} \in \mathcal{K}_\infty$, *and* $\psi \in \mathbb{R}_{>0}$.

We write $\widehat{\Sigma} \preceq^{\mathsf{max}}_{\mathcal{PS}} \Sigma$ if there exists an SPSF $\mathcal{S}$ from $\widehat{\Sigma}$ to Σ, and call the hybrid system $\widehat{\Sigma}$ a *discrete-time* (in)finite abstraction of concrete (original) system Σ. Abstraction $\widehat{\Sigma}$ could be finite or infinite depending on cardinalities of sets $\hat{X}, \hat{U}, \hat{W}$.

Remark 3.3.4. *Note that the above definition does not put any restriction on the state set of abstract systems; therefore, it can also be employed to establish a stochastic pseudo-simulation function from infinite abstractions* $\widetilde{\Sigma}$ *presented in* (3.3.1) *to* Σ *(cf. the running example).*

Now, we adapt the above notion to the interconnected ct-SHS without internal inputs by omitting all the terms related to $w, \hat{w}$ which is utilized in Theorem 3.2.6 for relating interconnected systems.

Definition 3.3.5. *Consider a ct-SHS* $\Sigma = (X, U, \mathcal{U}, f, \sigma, \rho, Y, h)$ *and its finite abstraction* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \varsigma, \hat{f}, \hat{Y}, \hat{h})$ *without internal inputs. A function* $\mathcal{V} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ *is called a* max*-type stochastic simulation function (*max*-type SSF) from* $\widehat{\Sigma}$ *to* Σ *if*

- $\exists \alpha \in \mathcal{K}_\infty$ *such that*

$$\forall x \in X, \forall \hat{x} \in \hat{X}, \quad \alpha(\|h(x) - \hat{h}(\hat{x})\|_\infty) \leq \mathcal{V}(x, \hat{x}), \tag{3.3.6}$$

- $\forall k \in \mathbb{N}$, $\forall \xi := \xi(k\tau) \in X, \forall \hat{\xi} := \hat{\xi}(k) \in \hat{X}$, *and* $\forall \hat{\nu} := \hat{\nu}(k) \in \hat{U}$, $\exists \nu := \nu(k\tau) \in U$ *such that*

$$\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] \leq \max\Big\{\kappa\mathcal{V}(\xi, \hat{\xi}), \rho_{\text{ext}}(\|\hat{\nu}\|_\infty), \psi\Big\}, \quad (3.3.7)$$

for some chosen sampling time $\tau \in \mathbb{R}_{>0}$, $0 < \kappa < 1$, $\rho_{\text{ext}} \in \mathcal{K}_\infty$, *and* $\psi \in \mathbb{R}_{>0}$.

We write $\widehat{\Sigma} \preceq_{\mathcal{S}}^{\mathsf{max}} \Sigma$ if there exists an SSF $\mathcal{V}$ from $\widehat{\Sigma}$ to Σ, and call the hybrid system $\widehat{\Sigma}$ a *discrete-time* (in)finite abstraction of concrete (original) system Σ.

One can utilize Theorem 3.2.6 to compare output trajectories of original interconnected *continuous-time* stochastic hybrid systems and that of their *discrete-time* (finite or infinite) abstractions. This theorem holds for the setting here since the max-type SSF in (3.3.7) implies the sum-type SSF in (3.2.7).

3.3.3 Compositional Abstractions for Interconnected ct-SHS

In this subsection, we analyze networks of stochastic hybrid subsystems

$$\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, \rho_i, Y_i, h_i), \qquad i \in \{1, \ldots, N\}, \quad (3.3.8)$$

and discuss how to construct their finite abstractions together with a max-type SSF based on corresponding SPSF of their subsystems.

3.3.3.1 Interconnected Stochastic Hybrid Systems

We consider a collection of stochastic hybrid subsystems Σ_i as in (3.3.8) where their internal inputs and outputs are partitioned as

$$\begin{aligned} w_i &= [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}], \\ y_i &= [y_{i1}; \ldots; y_{iN}], \end{aligned} \quad (3.3.9)$$

and their output spaces and functions are of the form

$$Y_i = \prod_{j=1}^{N} Y_{ij}, \quad h_i(x_i) = [h_{i1}(x_i); \ldots; h_{iN}(x_i)]. \quad (3.3.10)$$

The outputs y_{ii} are interpreted as *external* ones, whereas the outputs y_{ij} with $i \neq j$ are *internal* ones which are employed to interconnect these stochastic hybrid 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.,* $h_{ji} \equiv 0$. Now we define the *concrete* interconnected stochastic hybrid systems.

Definition 3.3.6. *Consider* $N \in \mathbb{N}_{\geq 1}$ *stochastic hybrid subsystems* $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, \rho_i, Y_i, h_i)$, $i \in \{1, \ldots, N\}$, *with the input-output configuration as in* (3.3.9) *and* (3.3.10). *The interconnection of* Σ_i *for any* $i \in \{1, \ldots, N\}$, *is the concrete interconnected stochastic hybrid system* $\Sigma = (X, U, \mathcal{U}, f, \sigma, \rho, Y, h)$, *denoted by* $\mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$, *such that*

$X := \prod_{i=1}^{N} X_i$, $U := \prod_{i=1}^{N} U_i$, $f := \prod_{i=1}^{N} f_i$, $\sigma := \mathsf{blkdiag}(\sigma_1(x_1), \ldots, \sigma_N(x_N))$, $\rho := \mathsf{blkdiag}(\rho_1(x_1), \ldots, \rho_N(x_N))$, $Y := \prod_{i=1}^{N} Y_{ii}$, *and* $h = \prod_{i=1}^{N} h_{ii}$, *subject to the following interconnection constraint:*

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

Remark 3.3.7. *Note that we employ the term "internal" for inputs and outputs of subsystems that are affecting each other in the interconnection topology: internal output of a subsystem affects internal input of another subsystem. We utilize the term "external" for inputs and outputs that are not used for the sake of constructing the interconnection. Properties of the interconnected system are specified over the external outputs. The main goal is to synthesize external inputs to satisfy desired properties over external outputs.*

An example of the interconnection of two concrete stochastic hybrid subsystems Σ_1 and Σ_2 is illustrated in Figure 3.4.

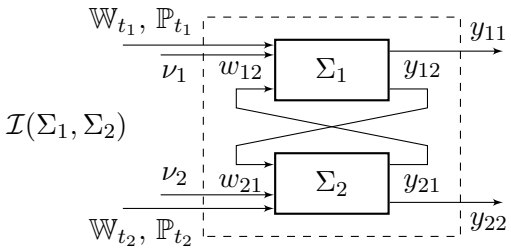

Figure 3.4: Interconnection of two *concrete* stochastic hybrid subsystems Σ_1 and Σ_2.

For the sake of better illustration of the results, we provide our case study as a running example throughout this section.

Running Example. Consider a network of $n = 1000$ rooms each equipped with a heater and connected circularly as depicted in Figure 3.5. The model of this case study is adapted from [GGM16] by including nonlinearity and stochasticity in the model. The evolution of the temperature $T(\cdot)$ can be described by the interconnected stochastic

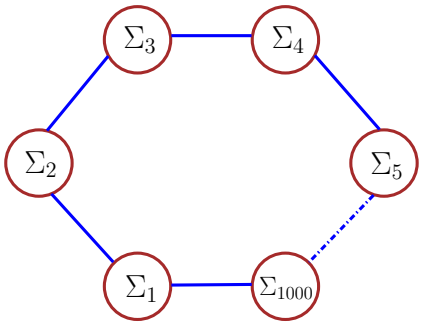

Figure 3.5: A circular building in a network of 1000 rooms.

differential equation

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

where A is a matrix with diagonal elements $a_{ii} = -2\hat{\eta}-\hat{\beta}$, $i \in \{1,\dots,n\}$, off-diagonal elements $\bar{a}_{i,i+1} = \bar{a}_{i+1,i} = \bar{a}_{1,n} = \bar{a}_{n,1} = \hat{\eta}$, $i \in \{1,\dots,n-1\}$, and all other elements are identically zero, $G = 0.5\mathbb{I}_n$, $R = 0.2\mathbb{I}_n$, and $\varphi(\xi(t)) = [0.5\varphi_1(0.5\xi_1(t));\dots;0.5\varphi_n(0.5\xi_n(t))]$ with $\varphi_i(x) = sin(x)$, $\forall i \in \{1,\dots,n\}$. Parameters $\hat{\eta} = 0.05$, $\hat{\beta} = 0.005$, and $\hat{\theta} = 0.01$ 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, $T_E = [T_{e_1};\dots;T_{e_n}]$, $\nu(t) = [\nu_1(t);\dots;\nu_n(t)]$, and $T(t) = [T_1(t);\dots;T_n(t)]$, where $T_i(t)$ is taking values in the set $[20, 21]$, for all $i \in \{1,\dots,n\}$. Outside temperatures are the same for all rooms: $T_{ei} = -1\,^\circ C$, $\forall i \in \{1,\dots,n\}$, and the heater temperature is $T_h = 50\,^\circ C$.

By considering the individual rooms as Σ_i described by

$$\Sigma_i\colon \begin{cases} \mathsf{d}T_i(t) = (a_{ii}T_i(t)+\hat{\theta}T_h\nu_i(t)+\hat{\eta}w_i(t)+\hat{\beta}T_{e_i}+0.5\varphi_i(0.5\xi_i(t)))\mathsf{d}t+0.5\mathsf{d}\mathbb{W}_{t_i} + 0.2\mathsf{d}\mathbb{P}_{t_i}, \\ \zeta_i(t) = T_i(t), \end{cases}$$

one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1,\dots,\Sigma_N)$ where $w_i(t) = [\zeta_{i-1}(t);\zeta_{i+1}(t)]$ (with $\zeta_0 = \zeta_n$, $\zeta_{n+1} = \zeta_1$). ■

3.3.3.2 Compositional Abstractions of Interconnected Hybrid Systems

In this subsection, we consider $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, \rho_i, Y_i, h_i)$ as an original ct-SHS and $\widehat{\Sigma}$ as its discrete-time finite abstraction given by the tuple $\widehat{\Sigma}_i = (\hat{X}_i, \hat{U}_i, \hat{W}_i, \varsigma_i, \hat{f}_i, \hat{Y}_i, \hat{h}_i)$ with the input-output configuration similar to (3.3.9) and (3.3.10), where $\hat{W}_i \subseteq W_i$ and $\hat{Y}_i \subseteq Y_i$. In order to present the compositionality results of the paper, we assume there exist max-type SPSF $\mathcal{S}_i$ from $\widehat{\Sigma}_i$ to Σ_i satisfying conditions (3.3.4), (3.3.5) in Definition 3.3.3 with the corresponding functions and constants denoted by α_i, $\rho_{\text{int}i}$, $\rho_{\text{ext}i}$, κ_i, and ψ_i. Since we construct our finite MDPs $\widehat{\Sigma}_i$ from time-discretized versions of original systems (*i.e.,* from $\widetilde{\Sigma}_i$), we define here the abstraction map $\Phi_{\tilde{w}_{ji}}$ on $\tilde{W}_{ji}$ that assigns to any $\tilde{w}_{ji} \in \tilde{W}_{ji}$ representative point $\hat{w}_{ji} \in \hat{W}_{ji}$ of the corresponding partition set containing $\tilde{w}_{ji}$. The mentioned map satisfies

$$\|\Phi_{\tilde{w}_{ji}}(\tilde{w}_{ji}) - \tilde{w}_{ji}\|_\infty \leq \bar{\mu}_{ji}, \quad \forall \tilde{w}_{ji} \in \tilde{W}_{ji}, \tag{3.3.11}$$

where $\bar{\mu}_{ji}$ is an *internal input* discretization parameter defined similar to δ in (3.2.5). Now we define a notion of interconnection applicable to discrete-time finite abstractions. Note that condition (3.3.11) helps us to freely take quantization parameters of internal input sets at the cost of having an additional error term formulated in ψ in (3.3.15). We now define the *abstract* interconnected stochastic hybrid systems.

Definition 3.3.8. *Consider $N \in \mathbb{N}_{\geq 1}$ finite stochastic hybrid subsystems $\widehat{\Sigma}_i = (\hat{X}_i,\hat{U}_i,\hat{W}_i, \varsigma_i, \hat{f}_i, \hat{Y}_i, \hat{h}_i)$, $i \in \{1,\dots,N\}$. The interconnection of $\widehat{\Sigma}_i$ is the finite interconnected stochastic hybrid system $\widehat{\Sigma} = (\hat{X}, \hat{U}, \varsigma, \hat{f}, \hat{Y}, \hat{h})$, denoted by $\widehat{\mathcal{I}}(\widehat{\Sigma}_1,\dots,\widehat{\Sigma}_N)$, such that*

$\hat{X} := \prod_{i=1}^{N} \hat{X}_i$, $\hat{U} := \prod_{i=1}^{N} \hat{U}_i$, $\varsigma := [\varsigma_1, \ldots, \varsigma_N]$, $\hat{f} := \prod_{i=1}^{N} \hat{f}_i$, $\hat{Y} := \prod_{i=1}^{N} \hat{Y}_{ii}$, *and* $\hat{h} = \prod_{i=1}^{N} \hat{h}_{ii}$, *subject to the following constraint:*

$$\forall i, j \in \{1, \ldots, N\}, i \neq j : \hat{w}_{ji} = \Phi_{\tilde{w}_{ji}}(\hat{y}_{ij}), \quad \Phi_{\tilde{w}_{ji}}(\hat{Y}_{ij}) \subseteq \hat{W}_{ji}.$$

We now raise the following small-gain assumption that is essential for the compositionality result in this chapter.

Assumption 3.3.9. *Assume that there exist $\mathcal{K}_\infty$ functions $\tilde{\delta}_f, \bar{\lambda}$ such that $(\bar{\lambda} - \mathcal{I}_d) \in \mathcal{K}_\infty$ and $\mathcal{K}_\infty$ functions κ_{ij} defined as*

$$\kappa_{ij}(s) := \begin{cases} \kappa_i s & \text{if } i = j, \\ (\mathcal{I}_d + \tilde{\delta}_f) \circ \rho_{\text{int}i} \circ \bar{\lambda} \circ \alpha_j^{-1}(s) & \text{if } i \neq j, \end{cases}$$

satisfy

$$\kappa_{i_1 i_2} \circ \kappa_{i_2 i_3} \circ \cdots \circ \kappa_{i_{r-1} i_r} \circ \kappa_{i_r i_1} < \mathcal{I}_d \tag{3.3.12}$$

for all sequences $(i_1, \ldots, i_r) \in \{1, \ldots, N\}^r$ and $r \in \{1, \ldots, N\}$.

The small-gain condition (3.3.12) *implies the existence of $\mathcal{K}_\infty$ functions $\bar{\sigma}_i$ [Rüf10, Theorem 5.5], satisfying*

$$\max_{i,j} \left\{ \bar{\sigma}_i^{-1} \circ \kappa_{ij} \circ \bar{\sigma}_j \right\} < \mathcal{I}_d, \quad i, j = \{1, \ldots, N\}. \tag{3.3.13}$$

Remark 3.3.10. *Remark that the small-gain condition* (3.3.12) *is a standard one in studying the stability of large-scale interconnected systems via input-to-state stable Lyapunov functions [DRW07, DRW10]. This condition is automatically satisfied if each κ_{ii} is less than identity ($\kappa_{ii} < \mathcal{I}_d, \forall i \in \{1, \ldots, N\}$). Since this condition should be satisfied for all possible sequences $(i_1, \ldots, i_r) \in \{1, \ldots, N\}^r, r \in \{1, \ldots, N\}$, it allows some subsystems to compensate the undesirable effects of other subsystems in the interconnected network such that this condition is satisfied.*

In the next theorem, we employ small-gain Assumption 3.3.9 to quantify the error between the interconnection of continuous-time stochastic hybrid subsystems and that of their discrete-time abstractions in a compositional manner.

Theorem 3.3.11. *Consider an interconnected ct-SHS $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ continuous-time stochastic hybrid subsystems Σ_i. Suppose that each Σ_i admits a discrete-time abstraction $\widehat{\Sigma}_i$ together with a* max*-type SPSF $\mathcal{S}_i$. If Assumption 3.3.9 holds and $\max_i \bar{\sigma}_i^{-1}$ for $\bar{\sigma}_i$ as in* (3.3.13) *is concave, then function $\mathcal{V}(x, \hat{x})$ defined as*

$$\mathcal{V}(x, \hat{x}) := \max_i \{ \bar{\sigma}_i^{-1}(\mathcal{S}_i(x_i, \hat{x}_i)) \}, \tag{3.3.14}$$

is a max*-type SSF from $\widehat{\Sigma} = \widehat{\mathcal{I}}(\widehat{\Sigma}_1, \ldots, \widehat{\Sigma}_N)$ to $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$.*

Proof. We first show that SSF $\mathcal{V}$ in (3.3.14) satisfies condition (3.3.6) for some $\mathcal{K}_\infty$ function α. For any $x=[x_1;\ldots;x_N]\in X$ and $\hat{x}=[\hat{x}_1;\ldots;\hat{x}_N]\in\hat{X}$, one gets:

$$\begin{aligned}\|h(x)-\hat{h}(\hat{x})\|_\infty &= \max_i\{\|h_{ii}(x_i)-\hat{h}_{ii}(\hat{x}_i)\|_\infty\}\leq \max_i\{\|h_i(x_i)-\hat{h}_i(\hat{x}_i)\|_\infty\}\\ &\leq \max_i\{\alpha_i^{-1}(\mathcal{S}_i(x_i,\hat{x}_i))\}=\beta\ (\max_i\{\bar{\sigma}_i^{-1}(\mathcal{S}_i(x_i,\hat{x}_i))\})=\beta(\mathcal{V}(x,\hat{x}))\end{aligned}$$

where $\beta(s)=\max_i\left\{\alpha_i^{-1}\circ\bar{\sigma}_i(s)\right\}$ for all $s\in\mathbb{R}_{\geq 0}$, which is a $\mathcal{K}_\infty$ function and (3.3.6) holds with $\alpha=\beta^{-1}$.

We continue with showing (3.3.7), as well. Let $\kappa(s)=\max_{i,j}\{\bar{\sigma}_i^{-1}\circ\kappa_{ij}\circ\bar{\sigma}_j(s)\}$. It follows from (3.3.13) that $\kappa<\mathcal{I}_d$. Since $\max_i\bar{\sigma}_i^{-1}$ is concave, one can readily acquire the chain of inequalities in (3.3.15) using Jensen's inequality, condition (3.3.11), and by defining $\rho_{\text{ext}}(\cdot)$, and ψ as

$$\begin{aligned}\rho_{\text{ext}}(s)&:=\big\{\max_i\{\bar{\sigma}_i^{-1}\circ\rho_{\text{ext}i}(s_i)\},\quad\text{s.t.}\quad s_i\geq 0,\ \|[s_1;\ldots;s_N]\|_\infty=s\big\},\\ \psi&:=\max_i\bar{\sigma}_i^{-1}(\Lambda_i),\end{aligned}$$

where $\Lambda_i:=(\mathcal{I}_d+\tilde{\delta}_f^{-1})\circ(\rho_{\text{int}i}\circ\bar{\lambda}\circ(\bar{\lambda}-\mathcal{I}_d)^{-1}(\max_{j,j\neq i}\{\bar{\mu}_{ji}\})+\psi_i)$. Hence, $\mathcal{V}$ is a max-type from $\widehat{\Sigma}$ to Σ, which completes the proof. ■

Remark 3.3.12. *Note that to show Theorem 3.3.11, we employed the following inequalities:*

$$\begin{cases}\rho_{\text{int}}(a+b)\leq\rho_{\text{int}}\circ\bar{\lambda}(a)+\rho_{\text{int}}\circ\bar{\lambda}\circ(\bar{\lambda}-\mathcal{I}_d)^{-1}(b),\\ a+b\leq\max\{(\mathcal{I}_d+\tilde{\delta}_f)(a),(\mathcal{I}_d+\tilde{\delta}_f^{-1})(b)\},\end{cases}$$

for any $a,b\in\mathbb{R}_{\geq 0}$, where $\rho_{\text{int}},\tilde{\delta}_f,\bar{\lambda},(\bar{\lambda}-\mathcal{I}_d)\in\mathcal{K}_\infty$.

The results of Theorem 3.3.11 are schematically depicted in Figure 3.6. As illustrated, if there exists a max-type SPSF $\mathcal{S}_i(x_i,\hat{x}_i)$ between each original subsystem and its corresponding finite MDP, one can construct a max-type SSF $\mathcal{V}(x,\hat{x})$ as proposed in (3.3.14) between the interconnected original system and its interconnected finite abstraction provided that the small-gain condition (3.3.12) is satisfied.

3.3.4 Construction of max-type SPSF

Here, we impose conditions on the infinite ct-SHS Σ enabling us to establish a max-type SPSF from its finite abstraction $\widehat{\Sigma}$ to Σ. The required conditions are presented for a particular class of continuous-time nonlinear stochastic hybrid systems as in the next subsection.

3.3.4.1 A Class of Nonlinear Stochastic Hybrid Systems

We focus on a special class of continuous-time nonlinear stochastic hybrid systems Σ and *quadratic* pseudo-stochastic simulation functions $\mathcal{S}$. We formally define this class of

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau),\hat{\xi}(k+1)) \,\big|\, \xi,\hat{\xi},\nu,\hat{\nu}\Big]=\mathbb{E}\Big[\max_i\Big\{\bar{\sigma}_i^{-1}(\mathcal{S}_i(\xi_i((k+1)\tau),\hat{\xi}_i(k+1)))\Big\} \,\big|\, \xi,\hat{\xi},\nu,\hat{\nu}\Big]\\
&\quad\leq \max_i\Big\{\bar{\sigma}_i^{-1}(\mathbb{E}\Big[\mathcal{S}_i(\xi_i((k+1)\tau),\hat{\xi}_i(k+1)) \,\big|\, \xi,\hat{\xi},\nu,\hat{\nu}\Big])\Big\}\\
&\quad= \max_i\Big\{\bar{\sigma}_i^{-1}(\mathbb{E}\Big[\mathcal{S}_i(\xi_i((k+1)\tau),\hat{\xi}_i(k+1)) \,\big|\, \xi_i,\hat{\xi}_i,\nu_i,\hat{\nu}_i\Big])\Big\}\\
&\quad\leq \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),\rho_{\mathrm{int}i}(\|w_i-\hat{w}_i\|_\infty),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\psi_i\})\Big\}\\
&\quad= \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),\rho_{\mathrm{int}i}(\max_{j,j\neq i}\{\|w_{ij}-\hat{w}_{ij}\|_\infty\}),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\psi_i\})\Big\}\\
&\quad= \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),\rho_{\mathrm{int}i}(\max_{j,j\neq i}\{\|y_{ji}-\hat{y}_{ji}+\hat{y}_{ji}-\Phi_{\tilde{w}_{ij}}(\hat{y}_{ji})\|_\infty\}),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\\
&\qquad\quad \psi_i\})\Big\}\\
&\quad\leq \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),\rho_{\mathrm{int}i}(\max_{j,j\neq i}\{\|h_j(x_j)-\hat{h}_j(\hat{x}_j)\|_\infty+\|\hat{y}_{ji}-\Phi_{\tilde{w}_{ij}}(\hat{y}_{ji})\|_\infty\}),\\
&\qquad\quad \rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\psi_i\})\Big\}\\
&\quad\leq \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),\rho_{\mathrm{int}i}(\max_{j,j\neq i}\{\alpha_j^{-1}(\mathcal{S}_j(x_j,\hat{x}_j))+\bar{\mu}_{ji}\}),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\psi_i\})\Big\}\\
&\quad\leq \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),\rho_{\mathrm{int}i}\circ\bar{\lambda}(\max_{j,j\neq i}\{\alpha_j^{-1}(\mathcal{S}_j(x_j,\hat{x}_j))\})\\
&\qquad\quad +\rho_{\mathrm{int}i}\circ\bar{\lambda}\circ(\bar{\lambda}-\mathcal{I}_d)^{-1}(\max_{j,j\neq i}\{\bar{\mu}_{ji}\}),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\psi_i\})\Big\}\\
&\quad\leq \max_i\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i(\mathcal{S}_i(x_i,\hat{x}_i)),(\mathcal{I}_d+\tilde{\delta}_f)\circ\rho_{\mathrm{int}i}\circ\bar{\lambda}(\max_{j,j\neq i}\{\alpha_j^{-1}(\mathcal{S}_j(x_j,\hat{x}_j))\}),\\
&\qquad\quad \rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\Lambda_i\})\Big\}\\
&\quad= \max_{i,j}\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}(\mathcal{S}_j(x_j,\hat{x}_j)),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\Lambda_i\})\Big\}\\
&\quad= \max_{i,j}\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}\circ\bar{\sigma}_j\circ\bar{\sigma}_j^{-1}(\mathcal{S}_j(x_j,\hat{x}_j)),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\Lambda_i\})\Big\}\\
&\quad= \max_{i,j}\Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}\circ\bar{\sigma}_j(\mathcal{V}(x,\hat{x})),\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|_\infty),\Lambda_i\})\Big\}\\
&\quad= \max\{\kappa(\mathcal{V}(x,\hat{x})),\rho_{\mathrm{ext}}(\|\hat{\nu}\|_\infty),\psi\}. \qquad (3.3.15)
\end{aligned}
$$

systems and then construct their finite abstractions $\widehat{\Sigma}$ as discussed in Subsection 3.3.1 by providing conditions under which a nominated $\mathcal{S}$ is a max-type SPSF from $\widehat{\Sigma}$ to Σ.

The class of continuous-time nonlinear stochastic hybrid systems is defined as

$$
\Sigma:\begin{cases}\mathsf{d}\xi(t)=(A\xi(t)+B\nu(t)+Dw(t)+E\varphi(F\xi(t))+\mathbf{b})\,\mathsf{d}t+G\mathsf{d}\mathbb{W}_t+\sum_{z=1}^{\mathsf{r}}R_z\mathsf{d}\mathbb{P}_t^z,\\ \zeta(t)=C\xi(t),\end{cases} \qquad (3.3.16)
$$

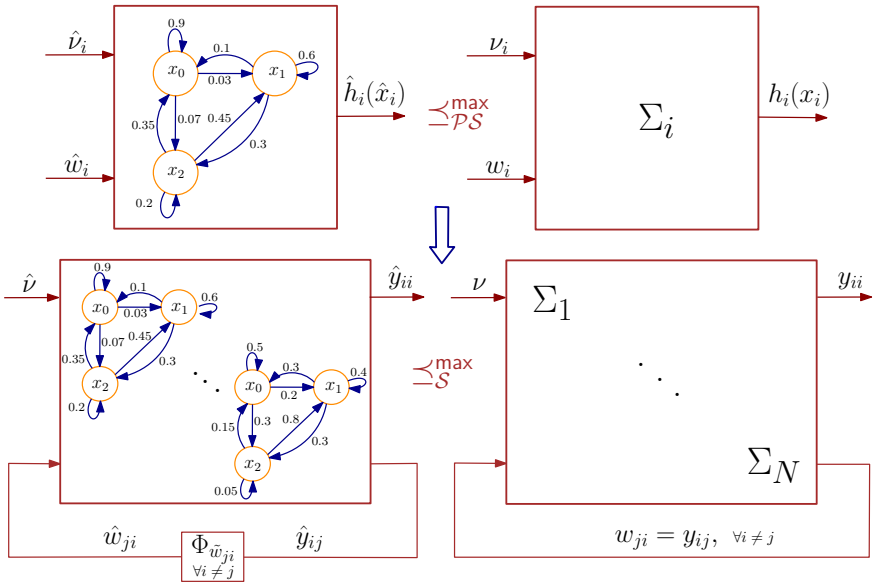

Figure 3.6: Compositionality results given that small-gain condition (3.3.12) is satisfied.

where $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times \bar{m}}, C \in \mathbb{R}^{\bar{q}\times n}$, $D \in \mathbb{R}^{n\times \bar{p}}$, $E \in \mathbb{R}^{n\times 1}$, $F \in \mathbb{R}^{1\times n}$, $G \in \mathbb{R}^{n\times 1}$, $\mathbf{b} \in \mathbb{R}^{n\times 1}$, and $R_i \in \mathbb{R}^{n\times 1}, \forall z \in [1; \cdots; \mathsf{r}]$. We use the tuple

$$\Sigma = (A, B, C, D, E, F, G, \mathbf{b}, R, \varphi, \bar{\lambda}),$$

where $R = \{R_1, \ldots, R_{\mathsf{r}}\}, \bar{\lambda} = \{\bar{\lambda}_1, \ldots, \bar{\lambda}_{\mathsf{r}}\}$ with $\bar{\lambda}_z$ as the rates of Poisson processes $\mathbb{P}^z_t$, to refer to the class of stochastic hybrid systems in (3.3.16). The *discrete-time infinite* abstraction of Σ is described by

$$\widetilde{\Sigma}\colon \begin{cases} \tilde{\xi}(k+1) = \tilde{\xi}(k) + \tilde{\nu}(k) + \tilde{D}\,\tilde{w}(k) + \tilde{R}\varsigma(k), \\ \tilde{\zeta}(k) = \tilde{C}\tilde{\xi}(k), \end{cases} \quad k \in \mathbb{N}, \tag{3.3.17}$$

where $\tilde{D}$ and $\tilde{R}$ are arbitrarily chosen. Our goal here is to use $\widetilde{\Sigma}$ as the time-discretized version of Σ in order to establish a max-type SPSF from $\widehat{\Sigma}$ to Σ via $\widetilde{\Sigma}$ while finding the best approximation error. Later, we show that $\tilde{R} = \mathbf{0}_n$ and $\tilde{D} = \mathbf{0}_{n\times\bar{p}}$ result in the least approximation error (cf. Remark 3.3.17).

Running Example (continued). The discrete-time *infinite* abstraction of Σ_i is given by

$$\widetilde{\Sigma}_i : \begin{cases} \tilde{T}_i(k+1) = \tilde{T}_i(k) + \tilde{\nu}_i(k), \\ \tilde{\zeta}_i(k) = \tilde{T}_i(k), \end{cases} \quad k \in \mathbb{N}.$$

Note that, as discussed in Remark 3.3.17, we consider here $\tilde{R}_i = \tilde{D}_i = 0$ in order to have the smallest constants ψ_i for each $\mathcal{S}_i$ (which results in smaller probabilistic error).

We present the discrete-time *finite* abstraction of $\widetilde{\Sigma}$ as

$$\widehat{\Sigma}\colon \begin{cases} \hat{\xi}(k+1) = \Phi_{\tilde{\xi}}(\hat{\xi}(k) + \hat{\nu}(k) + \tilde{D}\,\hat{w}(k) + \tilde{R}\varsigma(k)), \\ \hat{\zeta}(k) = \hat{C}\hat{\xi}(k), \end{cases} \qquad k \in \mathbb{N}, \tag{3.3.18}$$

where map $\Phi_{\tilde{\xi}} : \tilde{X} \to \hat{X}$ satisfies condition (3.2.5). Now we nominate the following quadratic simulation function

$$\mathcal{S}(x, \hat{x}) = (x - \bar{P}\hat{x})^\top \mathcal{M}(x - \bar{P}\hat{x}), \tag{3.3.19}$$

where $\bar{P}$ is a square matrix and $\mathcal{M}$ is a positive-definite matrix of an appropriate dimension. In order to show that the nominated $\mathcal{S}$ in (3.3.19) is a max-type SPSF from $\widehat{\Sigma}$ to Σ, we require Assumption 3.2.7 and the following key assumption.

Assumption 3.3.13. *Let $\Sigma = (A, B, C, D, E, F, G, \mathbf{b}, R, \varphi, \bar{\lambda})$. Assume that for some constant $\tilde{\kappa} \in \mathbb{R}_{>0}$, there exist matrices $M \succ 0$, K, $\bar{P}$, Q, L and H of appropriate dimensions such that the following matrix (in)equalities hold:*

$$(A + BK)^\top \mathcal{M} + \mathcal{M}(A + BK) \preceq -\tilde{\kappa}\mathcal{M}, \tag{3.3.20}$$
$$A\bar{P} = BQ, \tag{3.3.21}$$
$$E = BL, \tag{3.3.22}$$
$$D = BH. \tag{3.3.23}$$

Note that there exist matrices Q, L, and H satisfying conditions (3.3.21), (3.3.22), and (3.3.23) if and only if $\operatorname{im} A\bar{P} \subseteq \operatorname{im} B$, $\operatorname{im} E \subseteq \operatorname{im} B$, and $\operatorname{im} D \subseteq \operatorname{im} B$, respectively. Now, we provide another main results of this section showing that under Assumptions 3.2.7 and 3.3.13, function $\mathcal{S}$ in (3.3.19) is a max-type SPSF from $\widehat{\Sigma}$ to Σ.

Theorem 3.3.14. *Let $\Sigma = (A, B, C, D, E, F, G, \mathbf{b}, R, \varphi, \bar{\lambda})$ and $\widehat{\Sigma}$ be its discrete-time finite abstraction with the discretization parameter δ. Suppose Assumptions 3.2.7 and 3.3.13 hold, and $\hat{C} = \tilde{C} = C\bar{P}$. Then function $\mathcal{S}$ in* (3.3.19) *is a* max*-type SPSF from $\widehat{\Sigma}$ to Σ.*

Proof. Since $\hat{C} = C\bar{P}$, we have $\|Cx - \hat{C}\hat{x}\|_\infty^2 \leq n\lambda_{\max}(C^\top C)\|x - \bar{P}\hat{x}\|^2$, and similarly $\lambda_{\min}(M)\|x - \bar{P}\hat{x}\|^2 \leq (x - \bar{P}\hat{x})^\top \mathcal{M}(x - \bar{P}\hat{x})$. One can readily verify that $\frac{\lambda_{\min}(M)}{n\lambda_{\max}(C^\top C)}\|Cx - \hat{C}\hat{x}\|_\infty^2 \leq \mathcal{S}(x, \hat{x})$ holds $\forall x$, $\forall \hat{x}$, implying that condition (3.3.4) holds with $\alpha(s) = \frac{\lambda_{\min}(\mathcal{M})}{n\lambda_{\max}(C^\top C)}\, s^2$ for any $s \in \mathbb{R}_{\geq 0}$. We proceed with showing that condition (3.3.5) holds, as well. Using Assumption 3.2.7, we have

$$\begin{aligned}
&\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\Big|\, \xi{=}\xi(k\tau), \hat{\xi}{=}\hat{\xi}(k), \nu{=}\nu(k\tau), \hat{\nu}{=}\hat{\nu}(k), w{=}w(k\tau), \hat{w}{=}\hat{w}(k)\Big] \\
&\quad = \mathbb{E}\Big[\mathcal{S}(\xi((k{+}1)\tau), \hat{\xi}(k{+}1)) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}, w, \hat{w}\Big] - \mathbb{E}\Big[\mathcal{S}(\xi((k{+}1)\tau), \hat{\xi}) \Big| \xi, \hat{\xi}, \nu, \hat{\nu}, w, \hat{w}\Big] \\
&\qquad + \mathbb{E}\Big[\mathcal{S}(\xi((k{+}1)\tau), \hat{\xi}) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}, w, \hat{w}\Big] \\
&\quad \leq \mathbb{E}\Big[\mathcal{S}(\xi((k{+}1)\tau), \hat{\xi}) \,\Big|\, \xi, \hat{\xi}, \nu, \hat{\nu}, w, \hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|_\infty) \,\Big|\, \hat{\xi}, \hat{\nu}, \hat{w}\Big].
\end{aligned}$$

Now by employing Dynkin's formula [Dyn65], one obtains

$$\begin{aligned}&\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi})\,\big|\,\xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_\infty)\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\&\quad=\mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}\mathcal{LS}(\xi(t),\hat{\xi})\mathsf{d}t\Big]\big|\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_\infty)\big|\hat{\xi},\hat{\nu},\hat{w}\Big].\end{aligned}$$

Since the *infinitesimal generator* $\mathcal{LS}$ acting on function $\mathcal{S}$ is defined as

$$\begin{aligned}\mathcal{LS}(\xi,\hat{\xi})=\partial_\xi\mathcal{S}(\xi,\hat{\xi})f(\xi,\nu,w)+\frac{1}{2}\mathsf{Tr}(\sigma(\xi)\sigma(\xi)^\top\partial_{\xi,\xi}\mathcal{S}(\xi,\hat{\xi}))\\+\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j(\mathcal{S}(\xi+\rho(\xi)e_j^{\mathsf{r}},\hat{\xi})-\mathcal{S}(\xi,\hat{\xi})),\end{aligned}\tag{3.3.24}$$

where e_j^{r} denotes an r-dimensional vector with 1 on the j-th entry and 0 elsewhere, and

$$\partial_\xi\mathcal{S}(\xi,\hat{\xi})=2(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M},\quad\partial_{\xi,\xi}\mathcal{S}(\xi,\hat{\xi})=2\mathcal{M},$$

then one has

$$\begin{aligned}&\mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}\mathcal{LS}(\xi(t),\hat{\xi})\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_\infty)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\&\quad=\mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M}(A\xi(t)+E\varphi(F\xi(t))+B\nu(t)+\mathbf{b}+Dw(t))\\&\qquad+G^\top\mathcal{M}G+2(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_zR_z+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_zR_z^\top\mathcal{M}R_z)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\&\qquad+\mathbb{E}\Big[\gamma\left(\|\,\hat{\xi}(k+1)-\hat{\xi}\,\|_\infty\right)\big|\hat{\xi},\hat{\nu},\hat{w}\Big].\end{aligned}$$

Given any $\xi(t)$, $\hat{\xi}(k)$, $w(t)$ and $\hat{w}(k)$, we choose $\nu(t)$ via the following *interface* function:

$$\nu(t)=K(\xi(t)-\bar{P}\hat{\xi}(k))-Q\hat{\xi}(k)-L\varphi(F\xi(t))+H(w(k\tau)-\hat{w}(k))-Hw(t),\tag{3.3.25}$$

where $k\tau\le t\le(k+1)\tau$. By employing conditions (3.3.21), (3.3.22) and (3.3.23) , and the definition of the *interface* function in (3.3.25), we have

$$\begin{aligned}&\mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M}(A\xi(t)+E\varphi(F\xi(t))+B\nu(t)+\mathbf{b}+Dw(t))+G^\top\mathcal{M}G\\&\quad+2(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_zR_z+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_zR_z^\top\mathcal{M}R_z)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_\infty)\,\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\&=\mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2\,(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M}((A+BK)(\xi(t)-\bar{P}\hat{\xi})+\mathbf{b}+D(w-\hat{w}))+G^\top MG\\&\quad+2(\xi(t)-\bar{P}\hat{\xi})^\top\mathcal{M}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_zR_z+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_zR_z^\top\mathcal{M}R_z)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_\infty)\big|\hat{\xi},\hat{\nu},\hat{w}\Big].\end{aligned}$$

Using Young's inequality [You12] as $ab \leq \frac{\pi}{2}a^2 + \frac{1}{2\pi}b^2$, for any $a, b \geq 0$ and any $\pi > 0$, by employing Cauchy-Schwarz inequality and using condition (3.3.20), one has

$$
\begin{aligned}
&\mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2\,(\xi(t)-\bar{P}\hat{\xi})^{\top}\mathcal{M}((A+BK)(\xi(t)-\bar{P}\hat{\xi})+\mathbf{b}+D(w-\hat{w}))+G^{\top}\mathcal{M}G\\
&\quad+2(\xi(t)-\bar{P}\hat{\xi})^{\top}\mathcal{M}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^{\top}\mathcal{M}R_z)\mathsf{d}t\Big]\big|\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_{\infty})\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\leq \mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(-\tilde{\kappa}\mathcal{S}(\xi(t),\hat{\xi})+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\pi\|\sqrt{\mathcal{M}}D\|^2\|w-\hat{w}\|^2+G^{\top}\mathcal{M}G\\
&\quad+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^{\top}\mathcal{M}R_z+\pi\|\sqrt{M}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)\mathsf{d}t\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_{\infty})\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&=\mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}-\tilde{\kappa}\mathcal{S}(\xi(t),\hat{\xi})\,\mathsf{d}t+\tau(\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\pi\|\sqrt{\mathcal{M}}D\|^2\|w-\hat{w}\|^2+G^{\top}MG\\
&\quad+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^{\top}\mathcal{M}R_z+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_{\infty})\big|\hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}
$$

Using Grönwall inequality [Gro19], one has

$$
\begin{aligned}
&\mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}-\tilde{\kappa}\mathcal{S}(\xi(t),\hat{\xi})\mathsf{d}t+\tau(\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\pi\|\sqrt{\mathcal{M}}D\|^2\|w-\hat{w}\|^2+G^{\top}MG\\
&\quad+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^{\top}MR_z+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_{\infty})\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\leq \mathbb{E}_{\varsigma}\Big[e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[e^{-\tilde{\kappa}\tau}\tau(\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+p\pi\|\sqrt{\mathcal{M}}D\|^2\|w-\hat{w}\|_{\infty}^2+G^{\top}\mathcal{M}G+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^{\top}\mathcal{M}R_z\\
&\quad+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)\Big]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_{\infty})\,\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&=e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+p\pi\|\sqrt{\mathcal{M}}D\|^2\|w-\hat{w}\|_{\infty}^2+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^{\top}\mathcal{M}R_z\\
&\quad+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_{\infty})\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}
$$

Since function γ defined in Assumption 3.2.7 is *concave*, using Jensen inequality one has

$$
\begin{aligned}
&\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|_\infty)\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad=\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-(\hat{\xi}+\hat{\nu}+\tilde{D}\hat{w}+\tilde{R}\varsigma)+(\hat{\xi}+\hat{\nu}+\tilde{D}\hat{w}+\tilde{R}\varsigma)-\hat{\xi}\|_\infty)\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad\leq\mathbb{E}\Big[\gamma(\delta+\|\hat{\nu}+\tilde{D}\hat{w}+\tilde{R}\varsigma\|_\infty)\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad\leq\gamma((1+\varrho)\delta)+\mathbb{E}\Big[\gamma((1+\frac{1}{\varrho})\|\hat{\nu}+\tilde{D}\hat{w}+\tilde{R}\varsigma\|_\infty)\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad\leq\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}+\tilde{D}\,\hat{w}\|_\infty)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\mathbb{E}\Big[\|\tilde{R}\varsigma\|_\infty\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big])\\
&\quad\leq\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')\|\hat{\nu}+\tilde{D}\,\hat{w}\|)_\infty+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\mathbb{E}\Big[([\tilde{R}\varsigma]^\top[\tilde{R}\varsigma])^{\frac{1}{2}}\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big])\\
&\quad\leq\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')\|\hat{\nu}\|_\infty)+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\|\tilde{D}\,\|_\infty\,\|\hat{w}\|_\infty)\\
&\quad+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})(\mathbb{E}\Big[[\tilde{R}\varsigma]^\top[\tilde{R}\varsigma]\,\big|\,\hat{\xi},\hat{\nu},\hat{w}\Big])^{\frac{1}{2}})\\
&\quad=\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')\|\hat{\nu}\|_\infty)+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\,\|\tilde{D}\|_\infty\,\|\hat{w}\|_\infty)\\
&\quad+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})}),
\end{aligned}
\tag{3.3.26}
$$

where $\varrho,\varrho',\varrho''\in\mathbb{R}_{>0}$. Then one can conclude that

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}(k+1))\,\big|\,\xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big]\\
&\leq e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')\|\hat{\nu}\|_\infty)+e^{-\tilde{\kappa}\tau}\tau p\pi\|\sqrt{\mathcal{M}}D\|^2\|w-\hat{w}\|_\infty^2\\
&\quad+e^{-\tilde{\kappa}\tau}\tau(G^\top\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^\top\mathcal{M}R_z+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)+\gamma((1+\varrho)\delta)\\
&\quad+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})})+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\,\|\tilde{D}\|_\infty\,\|\hat{w}\|_\infty).
\end{aligned}
\tag{3.3.27}
$$

Using the previous inequality and by employing the similar argument as the one in [SGZ18, Theorem 1], one obtains

$$
\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}(k+1))\,\big|\,\xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big]\leq\max\Big\{\kappa\mathcal{S}(\xi,\hat{\xi}),\rho_{\text{int}}(\|w-\hat{w}\|_\infty),\rho_{\text{ext}}(\|\hat{\nu}\|_\infty),\psi\Big\},
$$

which completes the proof with

$$
\begin{aligned}
\alpha(s) &:= \frac{\lambda_{\min}(\mathcal{M})}{n\lambda_{\max}(C^\top C)}s^2, \quad \forall s \in \mathbb{R}_{\geq 0},\\
\kappa &:= 1-(1-\tilde{\pi})\bar{\kappa},\\
\rho_{\text{ext}}(s) &:= (1+\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')s), \quad \forall s \in \mathbb{R}_{\geq 0},\\
\rho_{\text{int}}(s) &:= (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+\tilde{\varrho}')e^{-\tilde{\kappa}\tau}\tau p\pi\|\sqrt{\mathcal{M}}D\|^2 s^2, \quad \forall s \in \mathbb{R}_{\geq 0},\\
\psi &:= (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+1/\tilde{\varrho}')(e^{-\bar{\kappa}\tau}\tau(G^\top\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^\top\mathcal{M}R_z\\
&\quad +\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2)+\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})})\\
&\quad +\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\,\|\tilde{D}\|_\infty\,\|\hat{w}\|_\infty)),
\end{aligned}
$$

where $\bar{\kappa}=1-e^{-\tilde{\kappa}\tau}$, $0<\tilde{\pi}<1$, and $\tilde{\varrho},\tilde{\varrho}'>0$. ■

Remark 3.3.15. *Note that since the abstract system $\widehat{\Sigma}$ in this chapter is considered in discrete-time domain, then the infinitesimal generator $\mathcal{LS}(x,\hat{x})$ defined in* (3.3.24) *is different from the usual one that was employed in [ZMEM+14].*

Remark 3.3.16. *Note that we nominated the simulation function in the quadratic form as in* (3.3.19) *and obtained the matrix inequality condition* (3.3.20)*. Satisfying this inequality has a necessary and sufficient condition which is stabilizability of the pair (A,B). Alternatively, other forms of simulation functions can be used but the corresponding required conditions need to be obtained according to the definition of the simulation function.*

Running Example (continued). Conditions (3.3.20)-(3.3.23) are satisfied by $\mathcal{M}_i=1,\bar{P}_i=1,Q_i=-0.21,L_i=1,H_i=0.1$. By taking $\tau=0.1,\bar{\lambda}_i=0.5,\pi_i=1,\tilde{\pi}_i=0.99,\tilde{\varrho}_i=0.01,\tilde{\varrho}_i'=1,\varrho_i=0.01$, the function $\mathcal{S}_i(T_i(k\tau),\tilde{T}_i(k))=(T_i(k\tau)-\tilde{T}_i(k))^2$ is a max-type SPSF from $\widehat{\Sigma}_i$ to Σ_i satisfying condition (3.3.4) with $\alpha_i(s)=s^2,\forall s\in\mathbb{R}_{\geq 0}$ and condition (3.3.5) with $\kappa_i=0.99$, $\rho_{\text{ext}i}(s)=2.04s$, $\rho_{\text{int}i}(s)=7.78\times10^{-11}s^2$, $\forall s\in\mathbb{R}_{\geq 0}$, and $\psi_i=1.36\times10^{-8}$. ■

The functions and constants $\alpha, \rho_{\text{ext}}, \rho_{\text{int}} \in \mathcal{K}_\infty$, $0 < \kappa < 1$, and $\psi \in \mathbb{R}_{>0}$ in Definition 3.3.3 associated with $\mathcal{S}$ in (3.3.19) are obtained as

$$
\begin{aligned}
\alpha(s) :=& \frac{\lambda_{\min}(\mathcal{M})}{n\lambda_{\max}(C^\top C)} s^2, \quad \forall s \in \mathbb{R}_{\geq 0},\\
\kappa :=& \, 1-(1-\tilde{\pi})\bar{\kappa},\\
\rho_{\text{ext}}(s) :=& \, (1+\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')s), \quad \forall s \in \mathbb{R}_{\geq 0},\\
\rho_{\text{int}}(s) :=& \, (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+\tilde{\varrho}')e^{-\tilde{\kappa}\tau}\tau p\pi\|\sqrt{\mathcal{M}}D\|^2 s^2, \quad \forall s \in \mathbb{R}_{\geq 0},\\
\psi :=& \, (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+1/\tilde{\varrho}')(e^{-\bar{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2\\
&+\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^\top \mathcal{M} R_z + \pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2) + \gamma((1+\varrho)\delta)\\
&+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})}) + \gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\,\|\tilde{D}\|_\infty\,\|\hat{w}\|_\infty)),
\end{aligned}
$$

where $\bar{\kappa} = 1 - e^{-\tilde{\kappa}\tau}$, and $0 < \tilde{\pi} < 1$ and $\tilde{\varrho}, \tilde{\varrho}', \varrho, \varrho', \varrho'' > 0$ are chosen arbitrarily.

Note that if γ is linear, then ρ_{ext}, and ψ defined in (3.3.5) are reduced to

$$
\begin{aligned}
\rho_{\text{ext}}(s) :=& \, (1+\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})\gamma(s), \quad \forall s \in \mathbb{R}_{\geq 0},\\
\psi :=& \, (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+1/\tilde{\varrho}')(e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2 + \sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z^\top M R_z\\
&+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{\mathsf{r}}\bar{\lambda}_z R_z\|^2) + \gamma(\delta) + \gamma(\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})}) + \gamma(\|\tilde{D}\|_\infty\,\|\hat{w}\|_\infty)).
\end{aligned}
$$

Remark 3.3.17. *Note that for the abstraction $\widetilde{\Sigma}$ in* (3.3.17)*, ρ_{ext}, and ψ defined in* (3.3.5) *are reduced to*

$$
\begin{aligned}
\rho_{\text{ext}}(s) :=& \, (1+\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})\gamma((1+\varrho)(1+\varrho')s), \quad \forall s \in \mathbb{R}_{\geq 0},\\
\psi :=& \, (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+1/\tilde{\varrho}')(e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2 + \sum_{z=1}^{r}\bar{\lambda}_z R_z^\top \mathcal{M} R_z\\
&+\pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{r}\bar{\lambda}_z R_z\|^2) + \gamma((1+\frac{1}{\varrho})\sqrt{\mathsf{Tr}(\tilde{R}^\top\tilde{R})}) + \gamma((1+\varrho)(1+\frac{1}{\varrho'})\,\|\tilde{D}\|_\infty\,\|\hat{w}\|_\infty)).
\end{aligned}
$$

Moreover, if the abstraction $\widetilde{\Sigma}$ is non-stochastic (i.e., $\tilde{R} = \mathbf{0}_n$) with $\tilde{D} = \mathbf{0}_{n\times p}$, then

$$\rho_{\text{ext}}(s) := (1+\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})\gamma(s), \quad \forall s \in \mathbb{R}_{\geq 0},$$
$$\psi := (1+1/\tilde{\varrho})(\frac{1}{\tilde{\pi}\bar{\kappa}})(1+1/\tilde{\varrho}')(e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2 + \sum_{z=1}^{r}\bar{\lambda}_z R_z^\top \mathcal{M} R_z$$
$$+ \pi\|\sqrt{\mathcal{M}}\sum_{z=1}^{r}\bar{\lambda}_z R_z\|^2). \tag{3.3.28}$$

This means if the concrete system has some stability property, it is actually better to go with the non-stochastic infinite abstractions than the stochastic ones since the non-stochastic abstractions are closer than the stochastic versions to the concrete systems (cf. the running example).

Remark 3.3.18. *Note that not having any internal input in the abstract systems in* (3.3.18) *(i.e., $\tilde{D} = \mathbf{0}_{n\times p}$) will actually result in less approximation error. In fact, the smart choice of the interface map in* (3.2.15) *still ensures that output trajectories of abstract systems follow those of the original ones with a quantified probabilistic error bound which gets smaller if $\tilde{D} = \mathbf{0}_{n\times p}$.*

Running Example (continued). Now we proceed with checking the small-gain condition (3.3.12) that is required for the compositionality result. By taking $\bar{\sigma}_i(s) = s$, $\forall i \in \{1,\ldots,n\}$, condition (3.3.12) and as a result condition (3.3.13) are always satisfied. Hence, $\mathcal{V}(T(k\tau),\hat{T}(k)) = \max_i(T_i(k\tau)-\hat{T}_i(k))^2$ is a max-type SSF from $\widetilde{\Sigma}$ to Σ satisfying conditions (3.3.6) and (3.3.7) with $\alpha(s) = s^2, \forall s \in \mathbb{R}_{\geq 0}$, $\kappa = 0.99$, $\rho_{\text{ext}}(s) = 2.04s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = 1.36 \times 10^{-8}$.

By taking the initial states of Σ and $\widetilde{\Sigma}$ as $20.5\mathbb{1}_{1000}$, and utilizing Theorem 3.2.6, one can guarantee that the distance between outputs of Σ and $\widetilde{\Sigma}$ will not exceed $\varepsilon = 0.5$ during the time horizon $\mathcal{T} = 12$ with probability at least 91%, *i.e.,*

$$\mathbb{P}(\|\zeta(k\tau) - \tilde{\zeta}(k)\| \leq 0.5,\ \forall k \in [0,12]) \geq 0.91.$$

We now synthesize a controller for Σ via its *discrete-time* abstraction $\widetilde{\Sigma}$ such that the controller keeps the temperature of each room in a safe set $[20,21]$. The idea here is to design a local controller for the abstract subsystem $\widetilde{\Sigma}_i$, and then refine it back to subsystem Σ_i via the interface function. We employ the software tool `SCOTS` [RZ16] on a machine with Linux Ubuntu (Intel i7@3.6GHz CPU and 16 GB of RAM) to synthesize controllers for $\widetilde{\Sigma}_i$ maintaining the temperature of each room in the comfort zone $[20,21]$. The required memory usage and computation time for synthesizing controllers for each room are respectively 184 MB and 70 seconds. Closed-loop state trajectories of a representative room with different noise realizations in a network of 1000 rooms are illustrated in Figure 3.7. Furthermore, several realizations of the norm of error between outputs of Σ and $\widetilde{\Sigma}$ are illustrated in Figure 3.8. In order to provide more practical analysis on the proposed probabilistic bound, we also run Monte Carlo simulation for

10000 runs. In this case, one can statistically guarantee that the distance between outputs of Σ and $\widetilde{\Sigma}$ is always less than or equal to 0.24 with the same probability (i.e., at least 91%). This issue is expected and the reason is due to the conservative nature of simulation functions, but with the gain of providing formal guarantees on the probabilistic distance between output trajectories rather than empirical ones. Note that we intentionally dropped the noise and instead used `SCOTS` [RZ16]. The reason is because we formally showed that if the concrete system has some stability property and the two systems are in continuous-time and discrete-time domains, it is actually better to construct and employ the non-stochastic abstraction (as discussed in Remark 3.3.17).

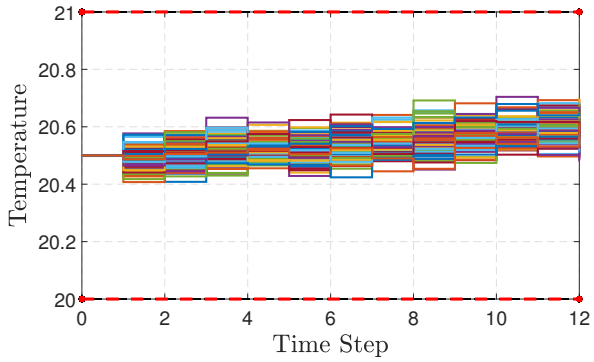

Figure 3.7: Closed loop state trajectories of a representative room with different noise realizations in a network of 1000 rooms, for $\mathcal{T} = 12$.

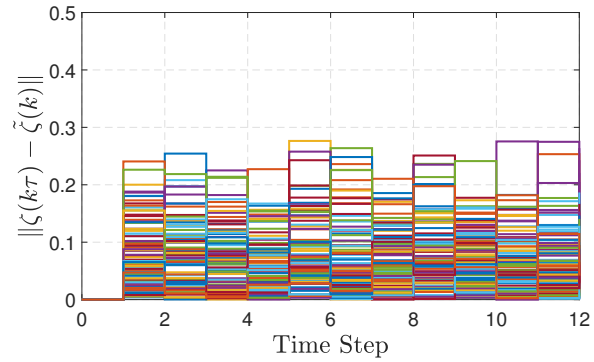

Figure 3.8: Several realizations of the norm of the error between the outputs of Σ and of $\widetilde{\Sigma}$, *i.e.*, $\|\zeta(k\tau) - \tilde{\zeta}(k)\|$, for $\mathcal{T} = 12$.

3.3.5 Analysis on Probabilistic Closeness Guarantee

In order to have a practical analysis on the probabilistic closeness guarantee, we provide Table 3.1 in which we discuss the proposed closeness guarantees for different values of time horizon, closeness precision, diffusion and reset terms. We fixed the employed

Table 3.1: Probabilistic error bound proposed in (3.2.8) based on $\mathcal{T}, \varepsilon, G$ and R.

Time horizon $\mathcal{T}$	5	10	15	20	30	40
Probabilistic closeness	96%	92%	88%	85%	78%	71%
Precision ε	0.1	0.3	0.5	0.7	0.9	1.1
Probabilistic closeness	6%	75%	91%	95%	97%	98%
Diffusion term G	0.1	0.3	0.5	0.7	0.9	1.1
Probabilistic closeness	63%	59%	53%	45%	35%	27%
Reset term R	0.1	0.3	0.5	0.7	0.9	1.1
Probabilistic closeness	75%	68%	53%	37%	23%	12%

parameters in the case study and computed the closeness for different ranges of $\mathcal{T}, G, R, \varepsilon$. We have also fixed $\tau = 0.03$ for computing the probabilistic bound for G, R. As seen, the probabilistic closeness guarantee is improved by either decreasing $\mathcal{T}, G, R$ or increasing ε. Note that constant ψ in (3.2.8) is formulated based on diffusion and reset terms as in (3.3.28).

3.4 Compositional Abstraction-based Synthesis of ct-SCS: Dissipativity Approach

In this section, we provide a compositional scheme based on *dissipativity approach* for the construction of finite MDPs from ct-SCS. We derive dissipativity-type conditions to propose compositionality results which are established based on relations between continuous-time subsystems and that of their abstract counterparts utilizing notions of so-called *stochastic storage functions*. The proposed compositionality approach here can be potentially less conservative than the small-gain one presented in the previous section for some classes of systems. In particular, the dissipativity-type compositional reasoning proposed here can enjoy the structure of the interconnection topology and may not require any constraint on the number or gains of subsystems (cf. Remark 3.5.5 and the case study). Consequently, the proposed approach here can provide a scale-free compositionality condition which is independent of the number of subsystems, compared to the proposed results based on small-gain approach in the previous section.

Here, we consider continuous-time stochastic control systems as in Remark 2.3.3. We slightly abuse the notation and divide the output set and map of the system to Y_1, Y_2 and h_1, h_2, where

- $Y_1 \subseteq \mathbb{R}^{\bar{q}_1}$ is the *external* output set of the system;
- $Y_2 \subseteq \mathbb{R}^{\bar{q}_2}$ 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.

Accordingly, a continuous-time stochastic control system Σ is characterized by

$$\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, Y_1, Y_2, h_1, h_2), \tag{3.4.1}$$

and it satisfies

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = f(\xi(t), \nu(t), w(t))\,\mathsf{d}t + \sigma(\xi(t))\,\mathsf{d}\mathbb{W}_t, \\ \zeta_1(t) = h_1(\xi(t)), \\ \zeta_2(t) = h_2(\xi(t)). \end{cases} \tag{3.4.2}$$

3.4.1 Finite Abstractions of ct-SCS

A *time-discretized* version of ct-SCS Σ is defined by the tuple

$$\widetilde{\Sigma} = \Big(\tilde{X}, \tilde{U}, \tilde{W}, \varsigma, \tilde{f}, \tilde{Y}_1, \tilde{Y}_2, \tilde{h}_1, \tilde{h}_2\Big), \tag{3.4.3}$$

where $\tilde{X}, \tilde{U}, \tilde{W}, \varsigma, \tilde{f}$ are defined as in (3.3.1) and

- $\tilde{Y}_1 \subseteq \mathbb{R}^{\bar{q}_1}$ is a Borel space as the *external* output set;
- $\tilde{Y}_2 \subseteq \mathbb{R}^{\bar{q}_2}$ is a Borel space as the *internal* output set;
- $\tilde{h}_1 : \tilde{X} \to \tilde{Y}_1$ is the *external* output map;
- $\tilde{h}_2 : \tilde{X} \to \tilde{Y}_2$ is the *internal* output map.

The evolution of $\widetilde{\Sigma}$, for given initial state $\tilde{x}(0) \in \tilde{X}$ and input sequences $\{\tilde{\nu}(k) : \Omega \to \tilde{U},\ k \in \mathbb{N}\}$ and $\{\tilde{w}(k) : \Omega \to \tilde{W},\ k \in \mathbb{N}\}$, can be written as

$$\widetilde{\Sigma} : \begin{cases} \tilde{\xi}(k+1) = \tilde{f}(\tilde{\xi}(k), \tilde{\nu}(k), \tilde{w}(k), \varsigma(k)), \\ \tilde{\zeta}_1(k) = \tilde{h}_1(\tilde{\xi}(k)), \\ \tilde{\zeta}_2(k) = \tilde{h}_2(\tilde{\xi}(k)). \end{cases} \qquad k \in \mathbb{N}.$$

The discrete-time stochastic control system $\widetilde{\Sigma}$ can be *equivalently* reformulated as a continuous-time MDP

$$\widetilde{\Sigma} = \Big(\tilde{X}, \tilde{U}, \tilde{W}, \tilde{T}_{\tilde{\mathsf{x}}}, \tilde{Y}_1, \tilde{Y}_2, \tilde{h}_1, \tilde{h}_2\Big),$$

where the map $\tilde{T}_{\tilde{\mathsf{x}}} : \mathbb{B}(\tilde{X}) \times \tilde{X} \times \tilde{U} \times \tilde{W} \to [0, 1]$, is a conditional stochastic kernel.

Given a discrete-time system $\widetilde{\Sigma} = (\tilde{X}, \tilde{U}, \tilde{W},\ \varsigma, \tilde{f}, \tilde{Y}_1, \tilde{Y}_2, \tilde{h}_1, \tilde{h}_2)$, its finite abstraction $\widehat{\Sigma}$ can be characterized as

$$\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{W}, \varsigma, \hat{f}, \hat{Y}_1, \hat{Y}_2, \hat{h}_1, \hat{h}_2),$$

where $\hat{X} = \{\hat{\xi}_z, z = 1, \ldots, n_{\hat{\xi}}\}$, $\hat{U} = \{\hat{\nu}_z, z = 1, \ldots, n_{\tilde{\nu}}\}$, and $\hat{W} = \{\hat{w}_z, z = 1, \ldots, n_{\tilde{w}}\}$ are sets of selected representative points. Function $\hat{f} : \hat{X} \times \hat{U} \times \hat{W} \times V_\varsigma \to \hat{X}$ is defined as (3.3.3).

3.5 Stochastic Storage and sum-Type Simulation Functions

In this section, we first define a notion of stochastic storage functions (SStF) for ct-SCS with both internal and external signals.

Definition 3.5.1. *Consider a ct-SCS* $\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, f, \sigma, Y_1, Y_2, h_1, h_2)$ *and its (in)finite abstraction* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{W}, \varsigma, \hat{f}, \hat{Y}_1, \hat{Y}_2, \hat{h}_1, \hat{h}_2)$*. A function* $\mathcal{S} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ *is called a stochastic storage function (SStF) from* $\widehat{\Sigma}$ *to* Σ *if*

- $\exists \alpha \in \mathcal{K}_\infty$ *such that*

$$\forall x \in X, \forall \hat{x} \in \hat{X}, \quad \alpha(\|h_1(x) - \hat{h}_1(\hat{x})\|) \leq \mathcal{S}(x, \hat{x}), \tag{3.5.1}$$

- $\forall k \in \mathbb{N}$, $\forall \xi := \xi(k\tau) \in X, \forall \hat{\xi} := \hat{\xi}(k) \in \hat{X}$, *and* $\forall \hat{\nu} := \hat{\nu}(k) \in \hat{U}$, $\forall w := w(k\tau) \in W$, $\forall \hat{w} := \hat{w}(k) \in \hat{W}$, $\exists \nu := \nu(k\tau) \in U$ *such that*

$$\begin{aligned} &\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\big|\, \xi, \hat{\xi}, \nu, \hat{\nu}, w, \hat{w}\Big] \\ &\leq \kappa \mathcal{S}(\xi, \hat{\xi}) + \rho_{\text{ext}}(\|\hat{\nu}\|) + \psi + \begin{bmatrix} w - \hat{w} \\ h_2(x) - \hat{h}_2(\hat{x}) \end{bmatrix}^\top \underbrace{\begin{bmatrix} \mathcal{X}^{11} & \mathcal{X}^{12} \\ \mathcal{X}^{21} & \mathcal{X}^{22} \end{bmatrix}}_{\mathcal{X} :=} \begin{bmatrix} w - \hat{w} \\ h_2(x) - \hat{h}_2(\hat{x}) \end{bmatrix}, \end{aligned} \tag{3.5.2}$$

for some chosen sampling time $\tau \in \mathbb{R}_{>0}$, $0 < \kappa < 1$, $\rho_{\text{ext}} \in \mathcal{K}_\infty$, $\psi \in \mathbb{R}_{>0}$, *and a symmetric matrix* $\mathcal{X}$ *with conformal block partitions* $\mathcal{X}^{z,\bar{z}}$, $z, \bar{z} \in \{1, 2\} \in \{1, 2\}$.

We call the control system $\widehat{\Sigma}$ a *discrete-time* (in)finite abstraction of concrete (original) system Σ if there exists an SStF $\mathcal{S}$ from $\widehat{\Sigma}$ to Σ. Abstraction $\widehat{\Sigma}$ could be finite or infinite depending on cardinalities of sets $\hat{X}, \hat{U}, \hat{W}$. Since the above definition does not put any restriction on the state set of abstract systems, it can be also used to define a stochastic storage function from discrete-time system $\widetilde{\Sigma}$ presented in (3.4.3) to Σ (cf. the case study).

We also utilize the notion of sum-type stochastic simulation functions as in Definition 3.2.4 by slightly modifying condition (3.2.7) as

$$\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau), \hat{\xi}(k+1)) \,\big|\, \xi, \hat{\xi}, \nu, \hat{\nu}\Big] \leq \kappa \mathcal{V}(\xi, \hat{\xi}) + \rho_{\text{ext}}(\|\hat{\nu}\|) + \psi, \tag{3.5.3}$$

where $0 < \kappa < 1$. Now by employing Theorem 3.2.6, one can quantify the probabilistic closeness between output trajectories of original interconnected *continuous-time* stochastic systems and that of their *discrete-time* (finite or infinite) abstractions.

3.5.1 Compositionality Results

We first formally define the interconnected stochastic control systems.

Definition 3.5.2. *Consider* $N \in \mathbb{N}_{\geq 1}$ *stochastic control subsystems* $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, Y_{1_i}, Y_{2_i}, h_{1_i}, h_{2_i})$, $i \in \{1, \ldots, N\}$, *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 establish a well-posed interconnection. The interconnection of* Σ_i, $\forall i \in \{1,\dots,N\}$, *is the ct-SCS* $\Sigma = (X, U, \mathcal{U}, f, \sigma, Y, h)$, *denoted by* $\mathcal{I}(\Sigma_1,\dots,\Sigma_N)$, *such that* $X := \prod_{i=1}^{N} X_i$, $U := \prod_{i=1}^{N} U_i$, $f := \prod_{i=1}^{N} f_i$, $\sigma := \mathsf{blkdiag}(\sigma_1(x_1),\dots,\sigma_N(x_N))$, $Y := \prod_{i=1}^{N} Y_{1i}$, *and* $h = \prod_{i=1}^{N} h_{1i}$, *with the internal inputs constrained according to:*

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

Remark 3.5.3. *Note that we do not have any restrictions on the interconnected matrix* M *and its entries can take any values depending on the forms of interconnection topologies.*

We consider $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, f_i, \sigma_i, Y_{1_i}, Y_{2_i}, h_{1_i}, h_{2_i})$ as an original ct-SCS and $\widehat{\Sigma}_i$ as its discrete-time finite abstraction given by the tuple $\widehat{\Sigma}_i = (\hat{X}_i, \hat{U}_i, \hat{W}_i, \varsigma_i, \hat{f}_i, \hat{Y}_{1_i}, \hat{Y}_{2_i}, \hat{h}_{1_i}, \hat{h}_{2_i})$. We also assume that there exist an SStF $\mathcal{S}_i$ from $\widehat{\Sigma}_i$ to Σ_i with the corresponding functions, constants, and matrices denoted by α_i, $\rho_{\text{ext}i}$, κ_i, ψ_i, $\mathcal{X}_i$, $\mathcal{X}_i^{11}$, $\mathcal{X}_i^{12}$, $\mathcal{X}_i^{21}$, and $\mathcal{X}_i^{22}$. In the next theorem, we quantify the error between the interconnection of *continuous-time* stochastic subsystems and that of their *discrete-time* abstractions in a compositional fashion.

Theorem 3.5.4. *Consider an interconnected stochastic control system* $\Sigma = \mathcal{I}(\Sigma_1,\dots,\Sigma_N)$ *induced by* $N \in \mathbb{N}_{\geq 1}$ *stochastic control subsystems* Σ_i *and the coupling matrix* M. *Let each subsystem* Σ_i *admit an abstraction* $\widehat{\Sigma}_i$ *with the corresponding SStF* $\mathcal{S}_i$. *Then*

$$\mathcal{V}(x,\hat{x}) := \sum_{i=1}^{N} \mu_i \mathcal{S}_i(x_i,\hat{x}_i), \tag{3.5.4}$$

is a sum*-type SSF from the interconnected system* $\widehat{\Sigma} = \mathcal{I}(\widehat{\Sigma}_1,\dots,\widehat{\Sigma}_N)$, *with coupling matrix* $\hat{M}$, *to* $\Sigma = \mathcal{I}(\Sigma_1,\dots,\Sigma_N)$ *if there exist* $\mu_i > 0$, $i \in \{1,\dots,N\}$, *and*

$$\begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}} \end{bmatrix}^{\top} \mathcal{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}} \end{bmatrix} \preceq 0, \tag{3.5.5}$$

$$M = \hat{M}, \tag{3.5.6}$$

$$\hat{M}\prod_{i=1}^{N} \hat{Y}_{2i} \subseteq \prod_{i=1}^{N} \hat{W}_i, \tag{3.5.7}$$

where

$$\mathcal{X}_{cmp} := \begin{bmatrix} \mu_1\mathcal{X}_1^{11} & & & \mu_1\mathcal{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\mathcal{X}_N^{11} & & & \mu_N\mathcal{X}_N^{12} \\ \mu_1\mathcal{X}_1^{21} & & & \mu_1\mathcal{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\mathcal{X}_N^{21} & & & \mu_N\mathcal{X}_N^{22} \end{bmatrix}, \tag{3.5.8}$$

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

Proof. We first show that $\mathcal{V}$ in (3.5.4) satisfies condition (3.2.6) for some $\mathcal{K}_\infty$ function α. For any $x = [x_1; \ldots; x_N] \in X$ and $\hat{x} = [\hat{x}_1; \ldots; \hat{x}_N] \in \hat{X}$, one gets:

$$\begin{aligned}\|h(x) - \hat{h}(\hat{x})\| &= \|[h_{11}(x_1); \ldots; h_{1N}(x_N)] - [\hat{h}_{11}(\hat{x}_1); \ldots; \hat{h}_{1N}(\hat{x}_N)]\| \\ &\leq \sum_{i=1}^{N} \|h_{1i}(x_i) - \hat{h}_{1i}(\hat{x}_i)\| \ \leq \sum_{i=1}^{N} \alpha_i^{-1}(\mathcal{S}_i(x_i, \hat{x}_i)) \leq \bar{\alpha}(\mathcal{V}(x, \hat{x})),\end{aligned}$$

with the function $\bar{\alpha} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ defined for all $s \in \mathbb{R}_{\geq 0}$ as

$$\bar{\alpha}(s) := \max\Big\{\textstyle\sum_{i=1}^{N} \alpha_i^{-1}(s_i) \ \big| \ s_i \geq 0, \ \sum_{i=1}^{N} \mu_i s_i = s\Big\}.$$

By taking the $\mathcal{K}_\infty$ function $\alpha(s) := \bar{\alpha}^{-1}(s)$, $\forall s \in \mathbb{R}_{\geq 0}$, one acquires

$$\alpha(\|h(x) - \hat{h}(\hat{x})\|) \leq \mathcal{V}(x, \hat{x}),$$

fulfilling condition (3.2.6).

We continue with showing condition (3.5.3), as well. One can obtain the chain of inequalities in (3.5.9) using conditions (3.5.5) and (3.5.6) and by defining $\kappa(\cdot), \psi, \rho_{\text{ext}}(\cdot)$ as

$$\begin{aligned}\kappa s &:= \max\Big\{ \sum_{i=1}^{N} \mu_i \kappa_i s_i \ \big| \ s_i \geq 0, \ \sum_{i=1}^{N} \mu_i s_i = s\Big\}, \\ \rho_{\text{ext}}(s) &:= \max\Big\{ \sum_{i=1}^{N} \mu_i \rho_{\text{ext}i}(s_i) \ \big| \ s_i \geq 0, \ \|[s_1; \ldots; s_N]\| = s\Big\}, \\ \psi &:= \sum_{i=1}^{N} \mu_i \psi_i.\end{aligned}$$

Hence one can conclude that $\mathcal{V}$ is a sum-type SSF from $\widehat{\Sigma}$ to Σ, which completes the proof. ■

Remark 3.5.5. *Condition* (3.5.5) *is similar to the LMI discussed in [AMP16] as a compositional stability condition based on the dissipativity theory. As shown in [AMP16], this condition holds independently of the number of subsystems in many physical applications with particular interconnection structures, e.g., skew symmetric.*

3.5.2 Construction of SSF for a Class of Affine Systems

Here, we focus on a special class of continuous-time stochastic affine systems and impose conditions enabling us to establish an SStF from its finite abstraction $\widehat{\Sigma}$ to Σ. The model of the system is given by

$$\Sigma : \begin{cases} \mathsf{d}\xi(t) = (A\xi(t) + B\nu(t) + Dw(t) + \mathbf{b})\mathsf{d}t + G\mathsf{d}W_t, \\ \zeta_1(t) = C_1\xi(t), \\ \zeta_2(t) = C_2\xi(t), \end{cases} \tag{3.5.10}$$

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{V}(\xi((k+1)\tau),\hat{\xi}(k+1)) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu}\Big] = \mathbb{E}\Big[\sum_{i=1}^{N}\mu_i\mathcal{S}_i(\xi_i((k+1)\tau),\hat{\xi}_i(k+1)) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu}\Big] \\
&= \sum_{i=1}^{N}\mu_i\mathbb{E}\Big[\mathcal{S}_i(\xi_i((k+1)\tau),\hat{\xi}_i(k+1)) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu}\Big] \\
&= \sum_{i=1}^{N}\mu_i\mathbb{E}\Big[\mathcal{S}_i(\xi_i((k+1)\tau),\hat{\xi}_i(k+1)) \,\Big|\, \xi_i,\hat{\xi}_i,\nu_i,\hat{\nu}_i\Big] \\
&\le \sum_{i=1}^{N}\mu_i\big(\kappa_i\mathcal{S}_i(x_i,\hat{x}_i)+\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|)+\psi_i+\begin{bmatrix} w_i-\hat{w}_i \\ h_{2i}(x_i)-\hat{h}_{2i}(\hat{x}_i)\end{bmatrix}^{\top}\begin{bmatrix}\mathcal{X}_i^{11} & \mathcal{X}_i^{12}\\ \mathcal{X}_i^{21} & \mathcal{X}_i^{22}\end{bmatrix}\begin{bmatrix} w_i-\hat{w}_i \\ h_{2i}(x_i)-\hat{h}_{2i}(\hat{x}_i)\end{bmatrix}\big) \\
&= \sum_{i=1}^{N}\mu_i\kappa_i\mathcal{S}_i(x_i,\hat{x}_i) + \sum_{i=1}^{N}\mu_i\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|) + \sum_{i=1}^{N}\mu_i\psi_i \\
&\quad + \begin{bmatrix} w_1-\hat{w}_1 \\ \vdots \\ w_N-\hat{w}_N \\ h_{21}(x_1)-\hat{h}_{21}(\hat{x}_1) \\ \vdots \\ h_{2N}(x_N)-\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}^{\top} \mathcal{X}_{cmp} \begin{bmatrix} w_1-\hat{w}_1 \\ \vdots \\ w_N-\hat{w}_N \\ h_{21}(x_1)-\hat{h}_{21}(\hat{x}_1) \\ \vdots \\ h_{2N}(x_N)-\hat{h}_{2N}(\hat{x}_N)\end{bmatrix} \\
&= \sum_{i=1}^{N}\mu_i\kappa_i\mathcal{S}_i(x_i,\hat{x}_i) + \sum_{i=1}^{N}\mu_i\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|) + \sum_{i=1}^{N}\mu_i\psi_i \\
&\quad + \begin{bmatrix} M\begin{bmatrix} h_{21}(x_1)\\ \vdots \\ h_{2N}(x_N)\end{bmatrix} - \hat{M}\begin{bmatrix} \hat{h}_{21}(\hat{x}_1)\\ \vdots \\ \hat{h}_{2N}(\hat{x}_N)\end{bmatrix} \\ h_{21}(x_1)-\hat{h}_{21}(\hat{x}_1) \\ \vdots \\ h_{2N}(x_N)-\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}^{\top} \mathcal{X}_{cmp} \begin{bmatrix} M\begin{bmatrix} h_{21}(x_1)\\ \vdots \\ h_{2N}(x_N)\end{bmatrix} - \hat{M}\begin{bmatrix} \hat{h}_{21}(\hat{x}_1)\\ \vdots \\ \hat{h}_{2N}(\hat{x}_N)\end{bmatrix} \\ h_{21}(x_1)-\hat{h}_{21}(\hat{x}_1) \\ \vdots \\ h_{2N}(x_N)-\hat{h}_{2N}(\hat{x}_N)\end{bmatrix} \\
&= \sum_{i=1}^{N}\mu_i\kappa_i\mathcal{S}_i(x_i,\hat{x}_i) + \sum_{i=1}^{N}\mu_i\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|) + \sum_{i=1}^{N}\mu_i\psi_i \\
&\quad + \begin{bmatrix} h_{21}(x_1)-\hat{h}_{21}(\hat{x}_1) \\ \vdots \\ h_{2N}(x_N)-\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}^{\top} \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}}\end{bmatrix}^{\top} \mathcal{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}}\end{bmatrix} \begin{bmatrix} h_{21}(x_1)-\hat{h}_{21}(\hat{x}_1) \\ \vdots \\ h_{2N}(x_N)-\hat{h}_{2N}(\hat{x}_N)\end{bmatrix} \\
&\le \sum_{i=1}^{N}\mu_i\kappa_i\mathcal{S}_i(x_i,\hat{x}_i) + \sum_{i=1}^{N}\mu_i\rho_{\mathrm{ext}i}(\|\hat{\nu}_i\|) + \sum_{i=1}^{N}\mu_i\psi_i \le \kappa\mathcal{V}(x,\hat{x}) + \rho_{\mathrm{ext}}(\|\hat{\nu}\|) + \psi. \quad (3.5.9)
\end{aligned}
$$

where $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times \bar{m}}, D \in \mathbb{R}^{n\times \bar{p}}, C_1 \in \mathbb{R}^{\bar{q}_1\times n}, C_2 \in \mathbb{R}^{\bar{q}_2\times n}$, $G \in \mathbb{R}^n$, and $\mathbf{b} \in \mathbb{R}^n$. We employ the tuple

$$\Sigma = (A, B, C_1, C_2, D, G, \mathbf{b}),$$

to refer to the class of stochastic affine systems in (3.5.10). The *time-discretized* version of Σ is proposed as

$$\widetilde{\Sigma} : \begin{cases} \tilde{\xi}(k+1) = \tilde{\xi}(k) + \tilde{\nu}(k) + \tilde{D}\tilde{w}(k) + \tilde{R}\varsigma(k), \\ \tilde{\zeta}_1(k) = \tilde{C}_1\tilde{\xi}(k), \\ \tilde{\zeta}_2(k) = \tilde{C}_2\tilde{\xi}(k), \end{cases} \quad k \in \mathbb{N}, \tag{3.5.11}$$

where $\tilde{D}$ and $\tilde{R}$ are matrices chosen arbitrarily, and $\tilde{C}_1 = C_1\bar{P}$, $\tilde{C}_2 = C_2\bar{P}$ with $\bar{P}$ as chosen in (3.3.19). Our main target here is to employ $\widetilde{\Sigma}$ as the discrete-time version of Σ in order to establish an SStF from $\widehat{\Sigma}$ to Σ through $\widetilde{\Sigma}$ while quantifying the *best approximation error*. Later, we show that $\tilde{R} = \mathbf{0}_n$ and $\tilde{D} = \mathbf{0}_{n\times\bar{p}}$ result in the least approximation error in our settings. Now, we describe the *finite* abstraction of $\widetilde{\Sigma}$ as

$$\widehat{\Sigma} : \begin{cases} \hat{\xi}(k+1) = \Phi_{\tilde{\xi}}(\hat{\xi}(k) + \hat{\nu}(k) + \tilde{D}\hat{w}(k) + \tilde{R}\varsigma(k)), \\ \hat{\zeta}_1(k) = \hat{C}_1\hat{\xi}(k), \\ \hat{\zeta}_2(k) = \hat{C}_2\hat{\xi}(k), \end{cases} \quad k \in \mathbb{N},$$

where map $\Phi_{\tilde{\xi}} : \tilde{X} \to \hat{X}$ satisfies the inequality (3.2.5). We employ the nominated quadratic function in (3.3.19) and utilize Assumptions 3.2.7 and 3.3.13 (but without condition (3.3.22)) to show the main results of this subsection. We also raise the following main assumption.

Assumption 3.5.6. *Let $\Sigma = (A, B, C_1, C_2, D, G, \mathbf{b})$. Assume that for some constants $\pi > 0$ and $0 < \bar{\kappa} < 1 - e^{-\tilde{\kappa}\tau}$ with a sampling time τ, there exist matrices $\mathcal{X}^{11}$, $\mathcal{X}^{12}$, $\mathcal{X}^{21}$, and $\mathcal{X}^{22}$ of appropriate dimensions such that*

$$\begin{bmatrix} \pi e^{-\tilde{\kappa}\tau}\tau B^\top \mathcal{M} B & 0 \\ 0 & \pi e^{-\tilde{\kappa}\tau}\tau D^\top \mathcal{M} D \end{bmatrix} \preceq \begin{bmatrix} \bar{\kappa}\mathcal{M} + C_2^\top \mathcal{X}^{22} C_2 & C_2^\top \mathcal{X}^{21} \\ \mathcal{X}^{12} C_2 & \mathcal{X}^{11} \end{bmatrix}, \tag{3.5.12}$$

where $\mathcal{M} \succ 0$ is the matrix appeared in (3.3.20).

Remark 3.5.7. *Note that in Assumption 3.5.6, matrices B, D, C_2 are those in the system dynamics, constant and matrix $\tilde{\kappa}, \mathcal{M}$ are the same as those satisfying the condition* (3.3.20)*, and constants and matrices $\pi, \bar{\kappa}, \mathcal{X}^{11}, \mathcal{X}^{12}, \mathcal{X}^{21}, \mathcal{X}^{22}$ are our decision variables to be designed. One can readily satisfy this assumption via semi-definite programing toolboxes and then check the compositionality condition* (3.5.5) *with obtained conformal block partitions $\mathcal{X}^{ij}$, $i, j \in \{1, 2\}$ of subsystems (cf. the case study).*

Now we provide another main result of this section showing that under which conditions $\mathcal{S}$ in (3.3.19) is an SStF from $\widehat{\Sigma}$ to Σ.

Theorem 3.5.8. *Let $\Sigma = (A, B, C_1, C_2, D, G, \mathbf{b})$ and $\widehat{\Sigma}$ be its* finite *MDP with the discretization parameter δ. Suppose Assumptions 3.2.7, 3.3.13 and 3.5.6 hold, $\hat{C}_1 = \tilde{C}_1 = C_1\bar{P}$, and $\hat{C}_2 = \tilde{C}_2 = C_2\bar{P}$. Then the quadratic function $\mathcal{S}$ in* (3.3.19) *is an SStF from $\widehat{\Sigma}$ to Σ.*

Proof. Since $\hat{C}_1 = C_1\bar{P}$, we have $\|C_1x - \hat{C}_1\hat{x}\|^2 = (x - \bar{P}\hat{x})^\top C_1^\top C_1(x - \bar{P}\hat{x})$. Since $\lambda_{\min}(C_1^\top C_1)\|x-\bar{P}\hat{x}\|^2 \leq (x-\bar{P}\hat{x})^\top C_1^\top C_1(x-\bar{P}\hat{x}) \leq \lambda_{\max}(C_1^\top C_1)\|x-\bar{P}\hat{x}\|^2$, and similarly $\lambda_{\min}(\mathcal{M})\|x - \bar{P}\hat{x}\|^2 \leq (x - \bar{P}\hat{x})^\top\mathcal{M}(x - \bar{P}\hat{x}) \leq \lambda_{\max}(\mathcal{M})\|x - \bar{P}\hat{x}\|^2$, it can be readily verified that $\frac{\lambda_{\min}(\mathcal{M})}{\lambda_{\max}(C_1^\top C_1)}\|C_1x - \hat{C}_1\hat{x}\|^2 \leq \mathcal{S}(x,\hat{x})$ holds $\forall x \in X$, $\forall \hat{x} \in \hat{X}$, implying that condition (3.5.1) holds with $\alpha(s) = \frac{\lambda_{\min}(\mathcal{M})}{\lambda_{\max}(C_1^\top C_1)}s^2$, $\forall s \in \mathbb{R}_{\geq 0}$.

We proceed with showing that condition (3.5.2) holds, as well. Using Assumption 3.2.7, we have

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}(k+1)) \,\Big|\, \xi{=}\xi(k\tau), \hat{\xi}{=}\hat{\xi}(k), \nu{=}\nu(k\tau), \hat{\nu}{=}\hat{\nu}(k), w{=}w(k\tau), \hat{w}{=}\hat{w}(k)\Big] \\
&\quad = \mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}(k+1)) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big] - \mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi})\Big|\xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big] \\
&\qquad + \mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big] \\
&\quad \leq \mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|) \,\Big|\, \hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}
$$

Now by employing Dynkin's formula [Dyn65], one obtains

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}) \,\Big|\, \xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|) \,\Big|\, \hat{\xi},\hat{\nu},\hat{w}\Big] \\
&\quad = \mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau} \mathcal{L}\mathcal{S}(\xi(t),\hat{\xi})\mathsf{d}t\Big]\Big|\hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|)\Big|\hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}
$$

Since the *infinitesimal generator* $\mathcal{L}\mathcal{S}$, acting on the function $\mathcal{S}$, is defined as

$$
\mathcal{L}\mathcal{S}(\xi,\hat{\xi}) = \partial_\xi\mathcal{S}(\xi,\hat{\xi})f(\xi,\nu,w) + \frac{1}{2}\mathsf{Tr}(\sigma(\xi)\sigma(\xi)^\top\partial_{\xi,\xi}\mathcal{S}(\xi,\hat{\xi})),
$$

where

$$
\partial_\xi\mathcal{S}(\xi,\hat{\xi}) = 2(\xi(t) - \bar{P}\hat{\xi})^\top\mathcal{M}, \quad \partial_{\xi,\xi}\mathcal{S}(\xi,\hat{\xi}) = 2\mathcal{M},
$$

one has

$$
\begin{aligned}
&\mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau} \mathcal{L}\mathcal{S}(\xi(t),\hat{\xi})\mathsf{d}t\Big] \,\Big|\, \hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1) - \hat{\xi}\|)\Big|\hat{\xi},\hat{\nu},\hat{w}\Big] \\
&\quad = \mathbb{E}_\varsigma\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau} (2(\xi(t) - \bar{P}\hat{\xi})^\top\mathcal{M}(A\xi(t) + B\nu(t) + Dw(t) + \mathbf{b}) \\
&\qquad + G^\top\mathcal{M}G)\mathsf{d}t\Big] \,\Big|\, \hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma\left(\|\,\hat{\xi}(k+1) - \hat{\xi}\,\|\right) \,\Big|\, \hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}
$$

Given any $\xi(t)$, $\hat{\xi}(k)$, $w(t)$ and $\hat{w}(k)$, we choose $\nu(t)$ via the following *interface* function:

$$\nu(t) = K(\xi(t) - \bar{P}\hat{\xi}(k)) - Q\hat{\xi}(k) + (\xi(k\tau) - \bar{P}\hat{\xi}(k)) + H(w(k\tau) - \hat{w}(k)) - Hw(t), \tag{3.5.13}$$

where $k\tau \leq t \leq (k+1)\tau$. By employing conditions (3.3.21), (3.3.23), and the definition of the *interface* function in (3.5.13), we have

$$\begin{aligned}
&\mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2(\xi(t)-\bar{P}\hat{\xi})^{\top}\mathcal{M}(A\xi(t)+B\nu(t)+Dw(t)+\mathbf{b})+G^{\top}\mathcal{M}G)\mathsf{d}t\Big]\,|\,\hat{\xi},\\
&\quad\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&= \mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2\,(\xi(t)-\bar{P}\hat{\xi})^{\top}\mathcal{M}((A+BK)(\xi(t)-\bar{P}\hat{\xi})+B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\\
&\quad+D(w-\hat{w})+\mathbf{b})+G^{\top}\mathcal{M}G)\mathsf{d}t\Big]\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)|\hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}$$

Using Young's inequality [You12] as $ab \leq \frac{\pi}{2}a^2 + \frac{1}{2\pi}b^2$, for any $a, b \geq 0$ and any $\pi > 0$, by employing Cauchy-Schwarz inequality and using condition (3.3.20), one has

$$\begin{aligned}
&\mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(2\,(\xi(t)-\bar{P}\hat{\xi})^{\top}\mathcal{M}((A+BK)(\xi(t)-\bar{P}\hat{\xi})+B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\\
&\quad+D(w-\hat{w})+\mathbf{b})+G^{\top}\mathcal{M}G)\mathsf{d}t\Big]\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\leq \mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}(-\tilde{\kappa}\mathcal{S}(\xi(t),\hat{\xi}) + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2 + \pi\|\sqrt{\mathcal{M}}B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\|^2\\
&\quad+\pi\|\sqrt{\mathcal{M}}D(w-\hat{w})\|^2+G^{\top}\mathcal{M}G)\mathsf{d}t\Big]\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&= \mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi}) + \mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}-\tilde{\kappa}\mathcal{S}(\xi(t),\hat{\xi})\,\mathsf{d}t + \tau(\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2 + \pi\|\sqrt{\mathcal{M}}B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\|^2\\
&\quad+\pi\|\sqrt{\mathcal{M}}D(w-\hat{w})\|^2+G^{\top}\mathcal{M}G)\Big]\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big] + \mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)|\hat{\xi},\hat{\nu},\hat{w}\Big].
\end{aligned}$$

Using Grönwall inequality [Gro19], one has

$$
\begin{aligned}
&\mathbb{E}_{\varsigma}\Big[\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[\int_{k\tau}^{(k+1)\tau}-\tilde{\kappa}\mathcal{S}(\xi(t),\hat{\xi})\mathsf{d}t+\tau(\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\pi\|\sqrt{\mathcal{M}}B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\|^2\\
&\quad+\pi\|\sqrt{\mathcal{M}}D(w-\hat{w})\|^2+G^{\top}\mathcal{M}G)\Big]\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\leq\mathbb{E}_{\varsigma}\Big[e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+\mathbb{E}\Big[e^{-\tilde{\kappa}\tau}\tau(\pi\|\sqrt{\tilde{M}}\mathbf{b}\|^2+\pi\|\sqrt{\mathcal{M}}B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\|^2\\
&\quad+\pi\|\sqrt{\mathcal{M}}D(w-\hat{w})\|^2+G^{\top}\mathcal{M}G)\Big]\,|\,\hat{\xi},\hat{\nu},\hat{w}\Big]+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\,|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&=e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2+\pi\|\sqrt{\mathcal{M}}B(\xi(k\tau)-\bar{P}\hat{\xi}(k))\|^2\\
&\quad+\pi\|\sqrt{\mathcal{M}}D(w-\hat{w})\|^2)+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&=e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad+\begin{bmatrix}\xi-\bar{P}\hat{\xi}\\ w-\hat{w}\end{bmatrix}^{\top}\begin{bmatrix}\pi e^{-\tilde{\kappa}\tau}\tau B^{\top}\mathcal{M}B & 0\\ 0 & \pi e^{-\tilde{\kappa}\tau}\tau D^{\top}\mathcal{M}D\end{bmatrix}\begin{bmatrix}\xi-\bar{P}\hat{\xi}\\ w-\hat{w}\end{bmatrix}.
\end{aligned}
$$

By employing (3.5.12) and since $\hat{C}_2=C_2P$, we have

$$
\begin{aligned}
&e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad+\begin{bmatrix}\xi-\bar{P}\hat{\xi}\\ w-\hat{w}\end{bmatrix}^{\top}\begin{bmatrix}\pi e^{-\tilde{\kappa}\tau}\tau B^{\top}\mathcal{M}B & 0\\ 0 & \pi e^{-\tilde{\kappa}\tau}\tau D^{\top}\mathcal{M}D\end{bmatrix}\begin{bmatrix}\xi-\bar{P}\hat{\xi}\\ w-\hat{w}\end{bmatrix}\\
&\leq e^{-\tilde{\kappa}\tau}\mathcal{S}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad+\begin{bmatrix}\xi-\bar{P}\hat{\xi}\\ w-\hat{w}\end{bmatrix}^{\top}\begin{bmatrix}\bar{\kappa}\mathcal{M}+C_2^{\top}\mathcal{X}^{22}C_2 & C_2^{\top}\mathcal{X}^{21}\\ \mathcal{X}^{12}C_2 & \mathcal{X}^{11}\end{bmatrix}\begin{bmatrix}\xi-\bar{P}\hat{\xi}\\ w-\hat{w}\end{bmatrix}\\
&=(\bar{\kappa}+e^{-\tilde{\kappa}\tau})\mathcal{S}(\xi,\hat{\xi})+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)+\mathbb{E}\Big[\gamma(\|\hat{\xi}(k+1)-\hat{\xi}\|)\big|\hat{\xi},\hat{\nu},\hat{w}\Big]\\
&\quad+\begin{bmatrix}w-\hat{w}\\ C_2\xi-\hat{C}_2\hat{\xi}\end{bmatrix}^{\top}\begin{bmatrix}\mathcal{X}^{11} & \mathcal{X}^{12}\\ \mathcal{X}^{21} & \mathcal{X}^{22}\end{bmatrix}\begin{bmatrix}w-\hat{w}\\ C_2\xi-\hat{C}_2\hat{\xi}\end{bmatrix}.
\end{aligned}
$$

Since the function γ defined in Assumption 3.2.7 is *concave*, using Jensen inequality, one can obtain the chain of inequalities in (3.3.26). Then one can conclude that

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{S}(\xi((k+1)\tau),\hat{\xi}(k+1))\,|\,\xi,\hat{\xi},\nu,\hat{\nu},w,\hat{w}\Big]\\
&\leq(\bar{\kappa}+e^{-\tilde{\kappa}\tau})\mathcal{S}(\xi,\hat{\xi})+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')\|\hat{\nu}\|)+e^{-\tilde{\kappa}\tau}\tau(G^{\top}\mathcal{M}G+\pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2)\\
&\quad+\gamma((1+\varrho)\delta)+\gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^{\top}\tilde{R})})+\gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\,\|\tilde{D}\,\|\,\|\hat{w}\|)\\
&\quad+\begin{bmatrix}w-\hat{w}\\ C_2\xi-\hat{C}_2\hat{\xi}\end{bmatrix}^{\top}\begin{bmatrix}\mathcal{X}^{11} & \mathcal{X}^{12}\\ \mathcal{X}^{21} & \mathcal{X}^{22}\end{bmatrix}\begin{bmatrix}w-\hat{w}\\ C_2\xi-\hat{C}_2\hat{\xi}\end{bmatrix},
\end{aligned}
$$

which completes the proof with

$$\begin{aligned}
\alpha(s) &:= \frac{\lambda_{\min}(\mathcal{M})}{\lambda_{\max}(C_1^\top C_1)} s^2, \quad \forall s \in \mathbb{R}_{\geq 0},\\
\kappa &:= \bar{\kappa} + e^{-\tilde{\kappa}\tau},\\
\rho_{\text{ext}}(s) &:= \gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\varrho'')s), \quad \forall s \in \mathbb{R}_{\geq 0},\\
\psi &:= e^{-\bar{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2) + \gamma((1+\varrho)\delta) + \gamma((1+\frac{1}{\varrho})(1+\frac{1}{\varrho'})\sqrt{\mathsf{Tr}(\tilde{R}^\top \tilde{R})})\\
&\quad + \gamma((1+\frac{1}{\varrho})(1+\varrho')(1+\frac{1}{\varrho''})\,\|\tilde{D}\|\,\|\hat{w}\|).
\end{aligned}$$

■

Remark 3.5.9. *Note that for the discrete-time system $\widetilde{\Sigma}$ in* (3.5.11)*, ρ_{ext}, and ψ defined above are reduced to*

$$\begin{aligned}
\rho_{\text{ext}}(s) &:= \gamma((1+\varrho)(1+\varrho')s), \quad \forall s \in \mathbb{R}_{\geq 0},\\
\psi &:= e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2) + \gamma((1+\frac{1}{\varrho})\sqrt{\mathsf{Tr}(\tilde{R}^\top \tilde{R})}) + \gamma((1+\varrho)(1+\frac{1}{\varrho'})\|\tilde{D}\|\,\|\hat{w}\|).
\end{aligned}$$

Moreover, if the abstraction $\widetilde{\Sigma}$ is non-stochastic (i.e., $\tilde{R} = \mathbf{0}_n$) with $\tilde{D} = \mathbf{0}_{n\times p}$, then

$$\rho_{\text{ext}}(s) := \gamma(s), \forall s \in \mathbb{R}_{\geq 0}, \quad \psi := e^{-\tilde{\kappa}\tau}\tau(G^\top \mathcal{M} G + \pi\|\sqrt{\mathcal{M}}\mathbf{b}\|^2).$$

This simply means if the concrete system satisfies some stability property (cf. (3.3.20)*), it is better to pick non-stochastic discrete-time system rather than stochastic ones since the non-stochastic systems provide smaller approximation errors (cf. the case study).*

3.5.3 Case Study

To illustrate the effectiveness of the proposed results, we apply our approaches to the temperature regulation in a circular network containing 100 rooms and construct compositionally a discrete-time system from its original continuous-time dynamic. We then employ the constructed discrete-time abstractions as substitutes to compositionally synthesize policies regulating the temperature of each room in a comfort zone.

Consider the circular network of $n = 100$ rooms as

$$\Sigma : \begin{cases} \mathsf{d}T(t) = (AT(t) + \hat{\theta}T_h\nu(t) + \hat{\beta}T_E)\,\mathsf{d}t + G\mathsf{d}\mathbb{W}_t,\\ \zeta(t) = T(t), \end{cases} \tag{3.5.14}$$

where A is a matrix with diagonal elements $\bar{a}_{ii} = -2\hat{\eta} - \hat{\beta} - \hat{\theta}\nu_i(t)$, $i \in \{1,\ldots,n\}$, off-diagonal elements $\bar{a}_{i,i+1} = \bar{a}_{i+1,i} = \bar{a}_{1,n} = \bar{a}_{n,1} = \hat{\eta}$, $i \in \{1,\ldots,n-1\}$, and all other elements are identically zero, and $G = 0.5\mathbb{I}_n$. Parameters $\hat{\eta} = 0.05$, $\hat{\beta} = 0.005$, and $\hat{\theta} = 0.01$ are conduction factors. Moreover, $T_E = [T_{e_1};\ldots;T_{e_n}]$, $\nu(t) = [\nu_1(t);\ldots;\nu_n(t)]$, and $T(t) = [T_1(t);\ldots;T_n(t)]$, where $T_i(t)$ is taking values in the set $[20, 21]$, for all

$i \in \{1,\dots,n\}$. Outside temperatures are the same for all rooms: $T_{ei} = -1\,^\circ C$, $\forall i \in \{1,\dots,n\}$, and the heater temperature is $T_h = 50\,^\circ C$. Now by considering the individual rooms as Σ_i described by

$$\Sigma_i : \begin{cases} \mathsf{d}T_i(t) = (\bar{a}_{ii}T_i(t) + \hat{\theta}T_h\nu_i(t) + \hat{\eta}w_i(t) + \hat{\beta}T_{e_i})\,\mathsf{d}t + 0.5\mathsf{d}\mathbb{W}_{t_i}, \\ \zeta_{1_i}(t) = T_i(t), \\ \zeta_{2_i}(t) = T_i(t), \end{cases} \tag{3.5.15}$$

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

$$\widetilde{\Sigma}_i : \begin{cases} \tilde{T}_i(k+1) = \tilde{T}_i(k) + \tilde{\nu}_i(k), \\ \tilde{\zeta}_{1_i}(k) = \tilde{T}_i(k), \\ \tilde{\zeta}_{2_i}(k) = \tilde{T}_i(k), \end{cases} \qquad k \in \mathbb{N}.$$

As discussed in Remark 3.5.9, we consider here $\tilde{R}_i = \tilde{D}_i = 0$ to have the least constants ψ_i for each $\mathcal{S}_i$ (resulting in the least probabilistic error). Then, one can readily verify that conditions (3.3.20),(3.3.21),(3.3.23) are satisfied by $\mathcal{M}_i = 1, \bar{P}_i = 1, Q_i = -0.21, H_i = 0.1$. Condition (3.5.12) is also satisfied by $\tau_i = 0.1, \pi_i = 1, \bar{\kappa}_i = 0.499, \mathcal{X}_i^{11} = e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\eta}^2$, $\mathcal{X}_i^{22} = -\pi_i e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\theta}^2T_h^2$, $\mathcal{X}_i^{12} = \mathcal{X}_i^{21} = 0$. Therefore, $\mathcal{S}_i(T_i(k\tau),\tilde{T}_i(k)) = (T_i(k\tau)-\tilde{T}_i(k))^2$ is an SStF from $\widetilde{\Sigma}_i$ to Σ_i satisfying condition (3.5.1) with $\alpha_i(s) = s^2, \forall s \in \mathbb{R}_{\geq 0}$ and condition (3.5.2) with $\kappa_i = 0.5$, $\rho_{\text{ext}i}(s) = 2s$, $\forall s \in \mathbb{R}_{\geq 0}$, $\psi_i = 1.17 \times 10^{-10}$, and

$$\mathcal{X}_i = \begin{bmatrix} e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\eta}^2 & 0 \\ 0 & -\pi_i e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\theta}^2T_h^2 \end{bmatrix}. \tag{3.5.16}$$

Now we look at $\widetilde{\Sigma} = \mathcal{I}(\widetilde{\Sigma}_1,\dots,\widetilde{\Sigma}_N)$ with a coupling matrix $\tilde{M}$ satisfying condition (3.5.6) as $\tilde{M} = M$. By choosing $\mu_1 = \cdots = \mu_N = 1$ and using $\mathcal{X}_i$ in (3.5.16), matrix $\mathcal{X}_{cmp}$ in (3.5.8) is reduced to

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

and accordingly condition (3.5.5) is reduced to

$$\begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix}^\top \mathcal{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix} = e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\eta}^2M^\top M - \pi_i e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\theta}^2T_h^2\mathbb{I}_n \preceq 0,$$

without requiring any restrictions on the number or gains of subsystems. We used $M = M^\top$, and $4e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\eta}^2 - \pi_i e^{-\tilde{\kappa}_i\tau_i}\tau_i\hat{\theta}^2T_h^2 \preceq 0$ by employing Gershgorin circle theorem [Bel65] to show the above LMI. Hence, $\mathcal{V}(T(k\tau),\tilde{T}(k)) = \sum_{i=1}^{100}(T_i(k\tau)-\tilde{T}_i(k))^2$ is a sum-type SSF from $\widetilde{\Sigma}$ to Σ satisfying conditions (3.2.6) and (3.5.3) with $\alpha(s) = s^2, \forall s \in \mathbb{R}_{\geq 0}$, $\kappa = 0.5$, $\rho_{\text{ext}}(s) = 20s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = 1.17 \times 10^{-8}$.

By taking initial states of Σ and $\widetilde{\Sigma}$ as $20.5\mathbb{1}_{100}$, and employing Theorem 3.2.6, one can guarantee that the distance between outputs of Σ and $\widetilde{\Sigma}$ will not exceed $\varepsilon = 0.5$ during the time horizon $\mathcal{T} = 12$ with a probability of at least 91%, *i.e.,*

$$\mathbb{P}(\|\zeta(k\tau) - \tilde{\zeta}(k)\| \leq 0.5,\ \forall k \in [0, 12]) \geq 0.91.$$

We now synthesize a controller for Σ via its *discrete-time* system $\widetilde{\Sigma}$ such that the controller keeps the temperature of each room in the comfort zone $[20, 21]$. We employ the software tool `SCOTS` [RZ16] to synthesize controllers for $\widetilde{\Sigma}_i$ maintaining the temperature of each room in the safe set $[20, 21]$. Closed-loop state trajectories of a representative room with different noise realizations in a network of 100 rooms are illustrated in Figure 3.9. Furthermore, several realizations of the norm of the error between outputs of Σ and $\widetilde{\Sigma}$ are illustrated in Figure 3.10.

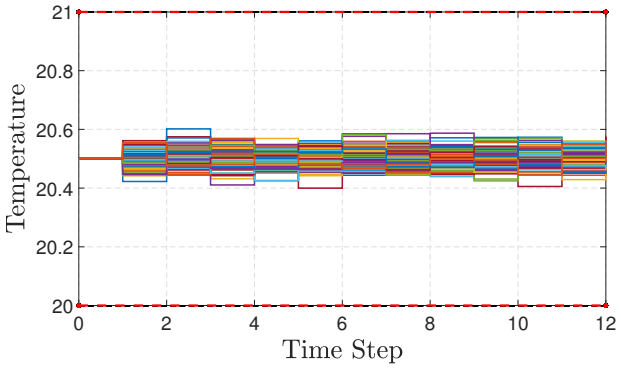

Figure 3.9: Closed-loop state trajectories of a representative room with different noise realizations in a network of 100 rooms, for $\mathcal{T} = 12$.

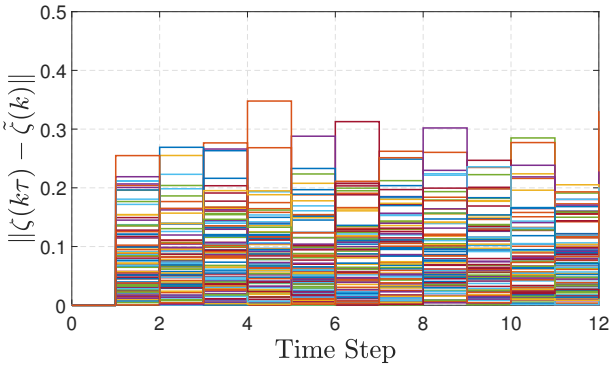

Figure 3.10: Several realizations of the norm of the error between outputs of Σ and of $\widetilde{\Sigma}$, *i.e.,* $\|\zeta(k\tau) - \tilde{\zeta}(k)\|$, for $\mathcal{T} = 12$.

3.6 Summary

In the first part of this chapter, we have proposed a systematic approach for the construction of discrete-time finite-space MDPs from continuous-time stochastic control systems without internal input sets W. We have first established a relation between the continuous-time system and its discrete-time counterpart based on *stochastic simulation functions*. We then leveraged the constructed relation and computed a probability bound between continuous-time concrete systems and that of their discrete-time (in)finite abstractions. We focused on a particular class of stochastic affine systems and constructed *finite* abstractions together with their corresponding stochastic simulation functions for this class of systems.

In the second part of the chapter, we enlarged the class of models to continuous-time stochastic *hybrid* systems with Poisson processes and proposed a *compositional framework* for the construction of discrete-time finite-space MDPs from this class of systems. We utilized sufficient small-gain conditions to provide the compositionality results which rely on the relation between the continuous-time subsystems and their discrete-time counterparts based on stochastic simulation functions. We also generalized our construction scheme to a particular class of *nonlinear* stochastic hybrid systems and constructed finite abstractions together with their corresponding stochastic simulation functions for this class of systems.

Finally, we provided a compositional scheme based on *dissipativity approach* for the construction of finite MDPs from continuous-time stochastic control systems. We derived dissipativity-type conditions to propose compositionality results which are established based on relations between continuous-time subsystems and that of their abstract counterparts utilizing notions of so-called *stochastic storage functions*. We showed that the proposed compositionality condition based on dissipativity reasoning can be potentially less conservative than the small-gain one for some classes of systems. In particular, the dissipativity-type compositional reasoning can enjoy the structure of the interconnection topology and may not require any constraint on the number or gains of subsystems. Consequently, the proposed compositionality condition can be scale-free and independent of the number of subsystems. We applied our approaches to a room temperature system in a circular network.

4 Discretization-free Techniques based on Control Barrier Certificates

4.1 Introduction

Another promising approach for the formal analysis of SHS is to employ control barrier certificates (CBC), as a *discretization-free* approach. Intuitively speaking, barrier certificates are Lyapunov-like functions defined over the state space of the system to enforce a set of inequalities on both the function itself and the infinitesimal generator along the flow (or one-step transition) of the system. An appropriate level set of a barrier certificate can separate an unsafe region from all system trajectories starting from a given set of initial conditions. Consequently, the existence of such a function provides a formal probabilistic certificate for system safety (cf. Figure 4.1). On the downside, finding CBC for complex dynamical systems is computationally very expensive, especially if the dimension of underlying systems is high. Motivated by this main challenge, this chapter is concerned with developing *compositional techniques* in the context of control barrier certificates for formal verification and controller synthesis of large-scale SHS to enforce high-level logic properties. In particular, we consider the large-scale SHS as an interconnected system composed of several smaller subsystems, and develop compositional frameworks for the construction of CBC for the complex interconnected SHS using control barrier certificates of smaller subsystems.

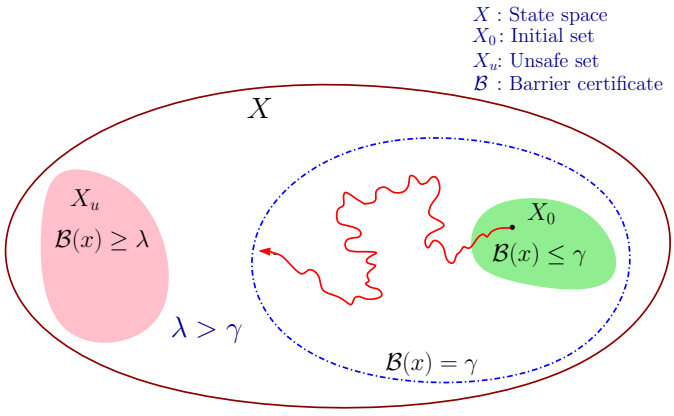

Figure 4.1: A barrier certificate for dynamical systems. The (red) dashed line denotes the initial level set $\mathcal{B}(x) = \gamma$.

4.1.1 Related Literature

In the past few years, there have been some results on the verification and controller synthesis of stochastic systems via control barrier certificates. In this respect, discretization-free techniques based on barrier certificates for stochastic hybrid systems are initially proposed in [PJ04, PJP07]. Stochastic safety verification using barrier certificates for switched diffusion processes and stochastic hybrid systems is, respectively, proposed in [WB17] and [HCL$^+$17]. Formal controller synthesis for stochastic systems via control barrier certificates is proposed in [JSZ20]. A controller synthesis framework for stochastic control systems based on control barrier certificates is also provided in [Cla19]. Verification and control for finite-time safety of stochastic systems via barrier certificates are discussed in [SDC19].

Verification of uncertain partially-observable Markov decision processes (POMDPs) with uncertain transition and/or observation probabilities using barrier certificates is discussed in [ACJT18, ASBA19]. Compositional construction of control barrier certificates for stochastic discrete-time systems is presented in [ALZ20, ALZ22]. An introduction and overview of recent work on control barrier certificates and their application to verify and enforce safety properties in the context of safety-critical controllers are presented in [ACE$^+$19]. Compositional construction of safety controllers for networks of continuous-space POMDPs using control barrier certificates is recently proposed in [JLZ23]. Compositional construction of control barrier certificates for networks of stochastic systems against ω-regular specifications is presented in [ALZ23].

4.1.2 Contributions

In the first part of this chapter, we propose a compositional approach based on small-gain conditions for the construction of control barrier certificates for ct-SCS. The proposed scheme is based on a notion of so-called *pseudo-barrier certificates* 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 certificates for interconnected systems based on the corresponding pseudo-barrier certificates computed for subsystems. Then, using the constructed control barrier certificates, 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 certificates of subsystems while synthesizing safety controllers.

In the second part of the chapter, we enlarge the class of systems to continuous-time stochastic *hybrid* systems by adding Poisson processes to the dynamics and propose a compositional scheme based on dissipativity approaches for the construction of control barrier certificates for this class of models. The proposed compositionality approach here is potentially less conservative than the small-gain one since the dissipativity-type compositional reasoning can enjoy the structure of the interconnection topology and may not require any constraints on the number or gains of the subsystems. Furthermore, the

provided results based on small-gain approaches ask an additional condition (cf. condition (4.2.1)) which is required for the satisfaction of small-gain type compositionality conditions, while dissipativity-type reasoning does not need such an extra condition.

In the third part of the chapter, we generalize the underlying dynamics to stochastic *switching* systems with *Markovian switching signals* and solve the controller synthesis problem for this class of systems with respect to high-level logic properties in a compositional manner. The controller synthesis problem now is more challenging since it deals with two different types of adversarial inputs: (i) internal inputs modeling the effects of other subsystems, and (ii) switching signals which are randomly changing the modes of the system. We also enlarge the class of specifications to those that can be expressed by the accepting language of deterministic finite automata (DFA), whereas previous sections handle only invariance specifications. To do so, we decompose the given complex specification to simple reachability tasks based on automata representing the complements of original finite-state automata and provide upper bounds on probabilities of satisfaction for those reachability tasks by computing their corresponding pseudo-barrier certificates. In addition, we provide an additional approach to compute pseudo-barrier certificates for systems with finite input sets by employing counter-example guided inductive synthesis framework based on the satisfiability modulo theories (SMT) solvers such as Z3 [DMB08], dReal [GAC12] or MathSat [CGSS13].

In the last part of the chapter, we propose a compositional framework for the construction of control barrier certificates for discrete-time stochastic switched systems accepting *multiple* control barrier certificates with some *dwell-time* conditions. Switching signals here are control inputs and the main goal is to synthesize them with a specific dwell-time such that outputs of original systems satisfy some high-level specifications such as safety, reachability, etc. To do so, we first provide an augmented framework for presenting each switched subsystem with several modes with a single system covering all modes (called augmented switched systems) whose output trajectories are exactly the same as those of original switched systems. We then compositionally construct *augmented control barrier certificates* for interconnected augmented systems based on so-called *augmented pseudo-barrier certificates* of subsystems by leveraging some max-type small-gain conditions. Afterwards, given the constructed augmented barrier certificates, we quantify upper bounds on the probability that interconnected systems reach certain unsafe regions in a finite time horizon.

4.2 Compositional Construction of Control Barrier Certificates: Small-Gain Approach

In this section, we propose a compositional technique based on small-gain approaches for the construction of control barrier certificates for continuous-time stochastic control systems. We first compositionally construct control barrier certificates for interconnected systems based on so-called pseudo-barrier certificates of subsystems by leveraging small-gain conditions. Then, given the constructed control barrier certificates, we quantify upper bounds on the probability that interconnected systems reach certain unsafe re-

gions in a finite time horizon. We finally utilize a systematic technique based on the sum-of-squares optimization program [Par03] to search for pseudo-barrier 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 pseudo-barrier certificates) regulating the temperature of each room for a bounded time horizon.

In the next subsections, we define notions of control pseudo-barrier and barrier certificates for ct-SCS and interconnected versions, respectively.

4.2.1 Control Pseudo-Barrier and Barrier Certificates

Here, we first introduce a notion of control pseudo-barrier certificate (CPBC) for ct-SCS with both internal and external inputs. We then define a notion of control barrier certificate (CBC) 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 4.2.6.

Definition 4.2.1. *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 certificate (CPBC) 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*

$$\mathcal{B}(x) \geq \alpha(\|h(x)\|^2), \quad \forall x \in X, \tag{4.2.1}$$
$$\mathcal{B}(x) \leq \gamma, \quad \forall x \in X_0, \tag{4.2.2}$$
$$\mathcal{B}(x) \geq \lambda, \quad \forall x \in X_u, \tag{4.2.3}$$

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

$$\mathcal{LB}(x) \leq -\kappa(\mathcal{B}(x)) + \rho_{\text{int}}(\|w\|^2) + \psi, \tag{4.2.4}$$

where $\mathcal{LB}$ is the infinitesimal generator of the stochastic process acting on $\mathcal{B}$ [Oks13], defined as

$$\mathcal{LB}(x) = \partial_x \mathcal{B}(x) f(x, \nu, w) + \frac{1}{2} \mathsf{Tr}(\sigma(x)\sigma(x)^\top \partial_{x,x} \mathcal{B}(x)). \tag{4.2.5}$$

Remark 4.2.2. *Condition* (4.2.1) *is required for the satisfaction of small-gain type compositionality conditions in Subsection 4.2.2. Although we assume that the full state information is available for interconnected systems, we define ct-SCS in* (2.3.3) *with outputs $y = h(x)$, using which we will introduce the interconnection constraint.*

The employed quantifiers in condition (4.2.4) 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 (4.2.4) 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 certificates 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 4.2.6 for quantifying upper bounds on exit probabilities over systems without internal inputs (*e.g.,* interconnected stochastic systems).

Definition 4.2.3. *Consider an (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 certificate (CBC) for Σ if*

$$\mathcal{B}(x) \leq \gamma, \qquad \forall x \in X_0, \tag{4.2.6}$$

$$\mathcal{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{4.2.7}$$

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

$$\mathcal{L}\mathcal{B}(x) \leq -\kappa(\mathcal{B}(x)) + \psi, \tag{4.2.8}$$

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

Remark 4.2.4. *Note that X_0 and X_u should not intersect in order to enforce the safety property in Definition 4.2.3. In particular, since we enforce $\gamma < \lambda$, this condition implicitly implies that there is no intersection between sets X_0 and X_u based on inequalities* (4.2.6) *and* (4.2.7)*.*

Remark 4.2.5. *Condition* (4.2.8) *ensures that the CBC is decaying up to a nonnegative constant ψ, which captures the magnitude of the stochasticity in the system. In addition, one requires $\gamma < \lambda$ to have a meaningful probabilistic bound using Theorem 4.2.6; however, we only need this condition for the CBC in Definition 4.2.3. One can readily verify that the probabilistic safety guarantee in Theorem 4.2.6 is improved by increasing the distance between γ and λ.*

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

Theorem 4.2.6. *Let $\Sigma = (X, U, \mathcal{U}, f, \sigma)$ be an (interconnected) ct-SCS without internal inputs. Suppose $\mathcal{B}$ is a CBC for Σ as in Definition 4.2.3, and there exists a constant $\hat{\kappa} \in \mathbb{R}_{>0}$ such that the function $\kappa \in \mathcal{K}_\infty$ in* (4.2.8) *satisfies $\kappa(s) \leq \hat{\kappa} s$, $\forall s \in \mathbb{R}_{\geq 0}$. Then the probability that the solution process of Σ staring from any initial state $\xi(0) = x_0 \in X_0$ reaches X_u under the policy $\nu(\cdot)$ within a finite time horizon $[0, \mathcal{T}] \subseteq \mathbb{R}_{\geq 0}$ is formally quantified as*

$$\mathbb{P}_\nu^{x_0}\Big\{\xi(t) \in X_u \text{ for some } 0 \leq t \leq \mathcal{T} \;\Big|\; \xi(0) = x_0\Big\} \leq \begin{cases} 1 - (1 - \frac{\gamma}{\lambda})e^{-\frac{\psi \mathcal{T}}{\lambda}}, & \text{if } \lambda \geq \frac{\psi}{\hat{\kappa}}, \\ \frac{\hat{\kappa}\gamma + (e^{\hat{\kappa}\mathcal{T}} - 1)\psi}{\hat{\kappa}\lambda e^{\hat{\kappa}\mathcal{T}}}, & \text{if } \lambda \leq \frac{\psi}{\hat{\kappa}}. \end{cases} \tag{4.2.9}$$

Proof. Based on condition (4.2.7), we have $X_u \subseteq \{x \in X \mid \mathcal{B}(x) \geq \lambda\}$. Then one has

$$\mathbb{P}_\nu^{x_0}\Big\{\xi(t) \in X_u \text{ for some } 0 \leq t \leq \mathcal{T} \mid \xi(0) = x_0\Big\} \leq \mathbb{P}_\nu^{x_0}\Big\{\sup_{0\leq t\leq \mathcal{T}} \mathcal{B}(\xi(t)) \geq \lambda \mid \xi(0) = x_0\Big\}. \tag{4.2.10}$$

One can acquire the upper bound in (4.2.9) by applying [Kus67, Theorem 1, Chapter III] to (4.2.10) and, respectively, utilizing conditions (4.2.8) and (4.2.6). ■

Remark 4.2.7. *If the function $\kappa(\cdot)$ in* (4.2.8) *is zero, the inequality* (4.2.8) *is reduced to $\mathcal{LB}(x) \leq \psi$, and accordingly, the upper bound in* (4.2.9) *is reduced to $\frac{\gamma+\psi\mathcal{T}}{\lambda}$.*

Remark 4.2.8. *In Section 4.2.3, we reformulate the conditions of Definition 4.2.3 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 subsection, we analyze networks of stochastic control subsystems and show under which conditions one can construct a CBC of an interconnected system using its CPBC of subsystems.

4.2.2 Compositional Construction of CBC

Here, we provide a compositional framework for the construction of control barrier certificates 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 (3.3.9)-(3.3.10). Assume that for control subsystems $\Sigma_i, i \in \{1, \ldots, N\}$, there exist CPBC $\mathcal{B}_i$ as defined in Definition 4.2.1 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 sum-type small-gain assumption.

Assumption 4.2.9. *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 $s \in \mathbb{R}_{\geq 0}$:*

$$\begin{aligned}
&\kappa_i(s) \geq \hat{\lambda}_i \hat{\gamma}_i(s),\\
&h_{ji} \equiv 0 \implies \hat{\delta}_{ij} = 0,\\
&h_{ji} \not\equiv 0 \implies \rho_{\text{int}i}((N-1)\alpha_j^{-1}(s)) \leq \hat{\delta}_{ij}\hat{\gamma}_j(s),
\end{aligned}$$

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 4.2.1.

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 4.2.9 to compute compositionally a control barrier certificate for the interconnected system Σ as in Definition 3.3.6.

Theorem 4.2.10. *Consider the interconnected ct-SCS $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ stochastic control subsystems Σ_i. Suppose that each control subsystem Σ_i admits a CPBC $\mathcal{B}_i$ as defined in Definition 4.2.1 with initial and unsafe sets X_{0_i} and X_{u_i}, respectively. If Assumption 4.2.9 holds and there exists a vector μ with $\mu_i > 0, i \in \{1, \ldots, N\}$, such that*

$$\mu^\top(-\Lambda + \Delta) < 0, \tag{4.2.11}$$

$$\sum_{i=1}^{N} \mu_i \lambda_i > \sum_{i=1}^{N} \mu_i \gamma_i, \tag{4.2.12}$$

then

$$\mathcal{B}(x) := \sum_{i=1}^{N} \mu_i \mathcal{B}_i(x_i) \tag{4.2.13}$$

is a CBC 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.

Proof. We first show that conditions (4.2.6) and (4.2.7) in Definition 4.2.3 hold. For any $x := [x_1; \ldots; x_N] \in X_0 = \prod_{i=1}^{N} X_{0_i}$ and from (4.2.2)

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

and similarly for any $x := [x_1; \ldots; x_N] \in X_u = \prod_{i=1}^{N} X_{u_i}$ and from (4.2.3)

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

satisfying conditions (4.2.6) and (4.2.7) 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 (4.2.12). Now, we show that condition (4.2.8) holds as well. By applying the following inequality

$$\rho_{\text{int}i}(s_1 + \cdots + s_{N-1}) \leq \sum_{i=1}^{N-1} \rho_{\text{int}i}((N-1)s_i),$$

which is valid for any $\rho_{\text{int}i} \in \mathcal{K}_\infty \cup \{0\}$, and any $s_i \in \mathbb{R}_{\geq 0}$, $i \in \{1, \cdots, N\}$, employing condition (4.2.1) and Assumption 4.2.9, one can obtain the chain of inequalities in (4.2.14). By defining

$$\kappa(s) := \min\Big\{ -\mu^\top(-\Lambda + \Delta)\Gamma(\bar{\mathcal{B}}(x)) \,\Big|\, \mu^\top \bar{\mathcal{B}}(x) = s \Big\},$$

$$\psi := \sum_{i=1}^{N} \mu_i \psi_i,$$

where $\bar{\mathcal{B}}(x) = [\mathcal{B}_1(x_1); \ldots; \mathcal{B}_N(x_N)]$, condition (4.2.8) is also satisfied. Then $\mathcal{B}$ is a CBC for Σ, which completes the proof. ■

$$
\begin{aligned}
\mathcal{L}\mathcal{B}(x) = \mathcal{L}\sum_{i=1}^{N}\mu_i\mathcal{B}_i(x_i) = \sum_{i=1}^{N}\mu_i\mathcal{L}\mathcal{B}_i(x_i) &\leq \sum_{i=1}^{N}\mu_i(-\kappa_i(\mathcal{B}_i(x_i)) + \rho_{\text{int}i}(\|w_i\|^2) + \psi_i) \\
&= \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \rho_{\text{int}i}(\sum_{j=1,i\neq j}^{N}\|w_{ij}\|^2) + \psi_i\big) \\
&= \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \rho_{\text{int}i}(\sum_{j=1,i\neq j}^{N}\|y_{ji}\|^2) + \psi_i\big) \\
&\leq \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \sum_{j=1,i\neq j}^{N}\rho_{\text{int}i}((N-1)\|y_{ji}\|^2) + \psi_i\big) \\
&= \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \sum_{j=1,i\neq j}^{N}\rho_{\text{int}i}((N-1)\|h_j(x_j)\|^2) + \psi_i\big) \\
&\leq \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \sum_{j=1,i\neq j}^{N}\rho_{\text{int}i}((N-1)\alpha_j^{-1}(\mathcal{B}_j(x_j))) + \psi_i\big) \\
&\leq \sum_{i=1}^{N}\mu_i\big(-\hat{\lambda}_i\hat{\gamma}_i(\mathcal{B}_i(x_i)) + \sum_{j=1,i\neq j}^{N}\hat{\delta}_{ij}\hat{\gamma}_j(\mathcal{B}_j(x_j)) + \psi_i\big) \\
&= \mu^\top(-\Lambda+\Delta)\Gamma(\mathcal{B}_1(x_1);\ldots;\mathcal{B}_N(x_N)) + \sum_{i=1}^{N}\mu_i\psi_i. \qquad (4.2.14)
\end{aligned}
$$

Remark 4.2.11. *Note that Assumption 4.2.9 is a well-established one in the relevant literature [IDW09, DIW11] studying the stability of large-scale interconnected systems via ISS Lyapunov functions of subsystems. We utilize this standard assumption to construct CBC of networks based on CPBC of their subsystems. The compositionality condition* $\mu^\top(-\Lambda+\Delta) < 0$*, constructed from the parameters in Assumption 4.2.9, is automatically satisfied if the spectral radius of* $\Lambda^{-1}\Delta$ *is strictly less than one [DIW11], denoted by* $\rho_{spc}(\Lambda^{-1}\Delta) < 1$*, which is easy to check. 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 [Axe94].*

Remark 4.2.12. *Condition* (4.2.12) *in general is not very restrictive since constants* μ_i *in* (4.2.13) *play a considerable role in rescaling CPBC for subsystems while normalizing the effect of internal gains of other subsystems (cf. [DRW10] for a similar argument but in the context of stability analysis via ISS Lyapunov functions). One can expect that condition* (4.2.12) *holds in many applications due to this rescaling.*

4.2.3 Computation of CPBC

Here, we reformulate the proposed conditions in Definition 4.2.1 as a sum-of-squares (SOS) optimization problem [Par03] and provide a systematic approach for computing CPBC 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 4.2.13. *Subsystem Σ_i has a continuous state set $X_i \subseteq \mathbb{R}^{n_i}$ and continuous external and internal input sets $U_i \subseteq \mathbb{R}^{\bar{m}_i}$ and $W_i \subseteq \mathbb{R}^{\bar{p}_i}$. 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 output map $h_i : X_i \to Y_i$ and the diffusion term $\sigma_i : \mathbb{R}^{n_i} \to \mathbb{R}^{n_i \times b_i}$ are polynomial functions of the state x_i. We also assume $\mathcal{K}_\infty$ functions α_i and $\rho_{\text{int}i}$ are polynomial.*

Under Assumption 4.2.13, the following lemma provides a set of sufficient conditions for the existence of a CPBC required in Definition 4.2.1, which can be solved as an SOS optimization problem.

Lemma 4.2.14. *Suppose Assumption 4.2.13 holds and sets X_0, X_u, X, W can be defined by vectors of polynomial inequalities $X_{0_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{0_i}(x_i) \geq 0\}$, $X_{u_i} = \{x_i \in \mathbb{R}^{n_i} \mid g_{u_i}(x_i) \geq 0\}$, $X_i = \{x_i \in \mathbb{R}^{n_i} \mid g_i(x_i) \geq 0\}$, $U_i = \{\nu_i \in \mathbb{R}^{\bar{m}_i} \mid g_{\nu_i}(x_i) \geq 0\}$, and $W_i = \{w_i \in \mathbb{R}^{\bar{p}_i} \mid g_{w_i}(x_i) \geq 0\}$, where the inequalities are defined element-wise. Suppose there exist 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 $\nu_i = (\nu_{1_i}, \nu_{2_i}, \ldots, \nu_{\bar{m}_i}) \in U_i \subseteq \mathbb{R}^{\bar{m}_i}$, and vectors of sum-of-squares polynomials $l_{0_i}(x_i)$, $l_{u_i}(x_i)$, $l_i(x_i)$, $\hat{l}_i(x_i, \nu_i, w_i)$, $l_{\nu_i}(x_i, \nu_i, w_i)$, and $l_{w_i}(x_i, \nu_i, w_i)$ of appropriate dimensions such that the following expressions are sum-of-squares polynomials:*

$$\mathcal{B}_i(x_i) - l_i^\top(x_i) g_i(x_i) - \alpha_i(h_i(x_i)^\top h_i(x_i)), \tag{4.2.15}$$

$$-\mathcal{B}_i(x_i) - l_{0_i}^\top(x_i) g_{0_i}(x_i) + \gamma_i, \tag{4.2.16}$$

$$\mathcal{B}_i(x_i) - l_{u_i}^\top(x_i) g_{1_i}(x_i) - \lambda_i, \tag{4.2.17}$$

$$\begin{aligned} -\mathcal{L}\mathcal{B}_i(x_i) - \kappa_i(\mathcal{B}_i(x_i)) + \rho_{\text{int}i}(w_i^\top w_i) + \psi_i - \sum_{j=1}^{\bar{m}_i} (\nu_{j_i} - l_{\nu_{j_i}}(x_i)) \\ - \hat{l}_i^\top(x_i, \nu_i, w_i) g_i(x_i) - l_{\nu_i}^\top(x_i, \nu_i, w_i) g_{\nu_i}(x_i) - l_{w_i}^\top(x_i, \nu_i, w_i) g_{w_i}(x_i). \end{aligned} \tag{4.2.18}$$

Then, $\mathcal{B}_i(x_i)$ satisfies conditions (4.2.1)-(4.2.4) in Definition 4.2.1 and $\nu_i = [l_{\nu_{1_i}}(x_i); \ldots; l_{\nu_{\bar{m}_i}}(x_i)]$, $i \in \{1, \ldots, N\}$, is the corresponding safety controller.

Proof. Since $\mathcal{B}_i(x_i)$ and $l_i(x_i)$ in (4.2.15) are sum-of-squares, we have $0 \leq \mathcal{B}_i(x_i) - l_i^\top(x_i) g_i(x_i) - \alpha_i(\|h_i(x_i)\|^2)$. Since the term $l_i^\top(x_i) g_i(x_i)$ is non-negative over X, the new condition (4.2.15) implies condition (4.2.1) in Definition 4.2.1. Similarly, we can show that (4.2.16) and (4.2.17) imply conditions (4.2.2) and (4.2.3) in Definition 4.2.1. Now

we show that condition (4.2.18) implies (4.5.4), as well. By selecting external inputs $\nu_{ji} = l_{\nu_{ji}}(x_i)$ and since $\hat{l}_i^\top(x_i,\nu_i,w_i)g_i(x_i), l_{\nu_i}^\top(x_i,\nu_i,w_i)g_{\nu_i}(x_i), l_{w_i}^\top(x_i,\nu_i,w_i)$ are all non-negative over the set X, we have $\mathcal{L}\mathcal{B}_i(x_i) \leq -\kappa_i(\mathcal{B}_i(x_i)) + \rho_{\text{int}i}(\|w_i\|) + \psi_i$ which implies that the function $\mathcal{B}_i(x_i)$ is a CPBC, which completes the proof. ■

Remark 4.2.15. *Note that the function $\kappa_i(\cdot)$ in* (4.2.18) *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 constant $\hat{\kappa}_i \in \mathbb{R}_{>0}$ as appeared in Theorem 4.2.6. Then one can employ bisection method to minimize the value of $\hat{\kappa}_i$.*

Remark 4.2.16. *For computing the sum-of-squares polynomial $\mathcal{B}_i(x_i)$ fulfilling reformulated conditions* (4.2.15)-(4.2.18)*, one can readily employ existing software tools available in the literature such as SOSTOOLS [PAV+13] together with a semidefinite programming (SDP) solver such as SeDuMi [Stu99].*

4.2.4 Case Study

To illustrate the effectiveness of the proposed results, we apply our approaches to the temperature regulation in (3.5.14) in a network of 1000 rooms. By considering the individual rooms Σ_i as in (3.5.15), 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 $X_i \in [1, 50], X_{0_i} \in [19.5, 20], X_{u_i} = [1, 17] \cup [23, 50], \forall i \in \{1, \ldots, n\}$. The main goal is to find a CBC 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 CPBC 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 CPBC as described in Subsection 4.2.3. According to Lemma 4.2.14, we compute CPBC of an order 2 as $\mathcal{B}_i(T_i) = 4183T_i^2 - 165400T_i + 1635114$ and the corresponding safety controller of an order 2 as $\nu_i(T_i) = -120T_i + 7000$ for all $i \in \{1, \ldots, n\}$. Moreover, the corresponding constants and functions in Definition 4.2.1 satisfying conditions (4.2.1)-(4.2.4) are quantified as $\gamma_i = 1250, \lambda_i = 23000, \kappa_i(s) = 11 \times 10^{-4}s, \psi_i = 10, \alpha_i(s) = 9s, \rho_{\text{int}i}(s) = 10^{-5}s, \forall s \in \mathbb{R}_{\geq 0}$.

We now proceed with Theorem 4.2.10 to construct a CBC for the interconnected system using CPBC of subsystems. One can readily verify that small-gain Assumption 4.2.9 holds with $\hat{\gamma}_i(s) = s, \forall s \in \mathbb{R}_{\geq 0}, \hat{\lambda}_i = 11 \times 10^{-4}, \hat{\delta}_{ij} = 1.1 \times 10^{-6}$. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, n\}$, one can readily show that the spectral radius of $\Lambda^{-1}\Delta$ is 0.95 which is strictly less that one (cf. Remark 4.2.11), and consequently, the compositionality condition (4.2.11) is satisfied. Moreover, the compositionality condition (4.2.12) is also met since $\lambda_i > \gamma_i, \forall i \in \{1, \ldots, n\}$. Then by employing the results of Theorem 4.2.10, one can conclude that $\mathcal{B}(T) = \sum_{i=1}^{1000}(4183T_i^2 - 165400T_i + 1635114)$ is a CBC for the interconnected system Σ with $\gamma = 125 \times 10^4, \lambda = 23 \times 10^6, \kappa(s) = 11 \times 10^{-4}s, \forall s \in \mathbb{R}_{\geq 0}$,

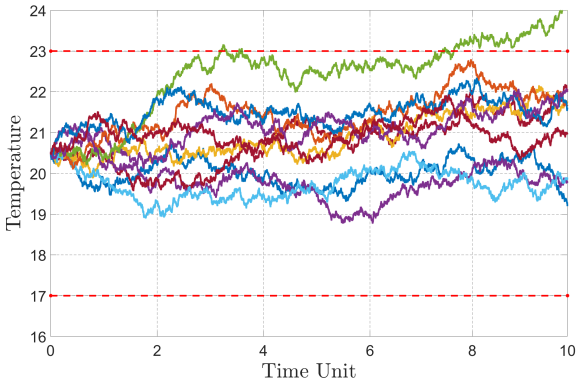

Figure 4.2: Closed-loop state trajectories of a representative room with 10 noise realizations in a network of 1000 rooms.

and $\psi = 10^4$. Accordingly, $\nu(T) = [-1201T_1 + 7000; \ldots; -120T_{1000} + 7000]$ is the overall safety controller for the interconnected system.

By employing Theorem 4.2.6, one can guarantee that the temperature of the interconnected system Σ starting from initial conditions $x_0 \in [19.5, 20]^{1000}$ remains in the safe set $[17, 23]^{1000}$ during the finite time horizon $\mathcal{T} = 10$ with a probability of at least 95%, *i.e.*,

$$\mathbb{P}_{\nu}^{x_0}\Big\{\xi(t) \notin X_u \mid \xi(0) = x_0, \forall t \in [0, 10]\Big\} \geq 0.95\,. \tag{4.2.19}$$

Closed-loop state trajectories of a representative room with 10 different noise realizations are illustrated in Figure 4.2. As illustrated, one out of 10 trajectories violates the safety specification, which is in accordance with the theoretical guarantee in (4.2.19).

4.3 Compositional Construction of Control Barrier Certificates: Dissipativity Approach

In this section, we enlarge the class of systems to continuous-time stochastic *hybrid* systems by adding Poisson processes to the dynamics (cf. Definition 2.3.1) and propose a compositional scheme based on dissipativity approaches for the construction of control barrier certificates for this class of models. The proposed compositionality approach here is potentially less conservative than the small-gain one since the dissipativity-type compositional reasoning can enjoy the structure of the interconnection topology and may not require any constraints on the number or gains of the subsystems. Furthermore, the provided results based on small-gain approaches ask an additional condition (cf. condition (4.2.1)) which is required for the satisfaction of *small-gain* type compositionality conditions, while dissipativity-type reasoning does not need such an extra condition.

4.3.1 Control Storage and Barrier Certificates

In this subsection, we first introduce a notion of control storage certificates (CStC) for ct-SHS with both internal and external signals.

Definition 4.3.1. *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 stochastic control storage certificate (CStC) for* Σ *if there exist* $\kappa \in \mathcal{K}_\infty$, $\gamma, \psi \in \mathbb{R}_{\geq 0}$, $\lambda \in \mathbb{R}_{>0}$, *and a symmetric matrix* $\mathcal{X}$ *with conformal block partitions* $\mathcal{X}^{z\bar{z}}$, $z, \bar{z} \in \{1, 2\}$, *where* $\mathcal{X}^{22} \preceq 0$, *such that*

- $\forall x \in X_0$,

$$\mathcal{B}(x) \leq \gamma, \tag{4.3.1}$$

- $\forall x \in X_u$,

$$\mathcal{B}(x) \geq \lambda, \tag{4.3.2}$$

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

$$\mathcal{LB}(x) \leq -\kappa(\mathcal{B}(x)) + \psi + \begin{bmatrix} w \\ h_2(x) \end{bmatrix}^\top \underbrace{\begin{bmatrix} \mathcal{X}^{11} & \mathcal{X}^{12} \\ \mathcal{X}^{21} & \mathcal{X}^{22} \end{bmatrix}}_{\mathcal{X}:=} \begin{bmatrix} w \\ h_2(x) \end{bmatrix}, \tag{4.3.3}$$

where $\mathcal{LB}$ *is the infinitesimal generator of the stochastic process acting on the function* $\mathcal{B}$ *[Oks13], defined as*

$$\mathcal{LB}(x) = \partial_x \mathcal{B}(x) f(x, \nu, w) + \frac{1}{2} \mathsf{Tr}(\sigma(x)\sigma(x)^\top \partial_{x,x} \mathcal{B}(x)) + \sum_{j=1}^{r} \bar{\lambda}_j (\mathcal{B}(x + \rho(x)\mathsf{e}_j^r) - \mathcal{B}(x)), \tag{4.3.4}$$

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* e_j^r *denotes an* r*-dimensional vector with* 1 *on the* j*-th entry and* 0 *elsewhere.*

Remark 4.3.2. *Note that a stochastic 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* (4.3.3). *This term is interpreted in dissipativity theory as the supply rate of the system [AMP16] 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.* (4.3.5)*).*

Now one can employ the notion of CBC for the interconnected ct-SHS (without internal signals) as in Definition 4.2.3 and quantify upper bounds on the probability that the interconnected system reaches certain unsafe regions in a finite time horizon via Theorem 4.2.6.

Remark 4.3.3. *Note that stochastic storage certificates satisfying conditions* (4.3.1)-(4.3.3) *are not useful on their own to ensure the safety of 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.* (4.3.5),(4.3.6)*). The safety of the system can then be verified via Theorem 4.2.6 only using the constructed control barrier certificate.*

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

4.3.2 Compositional Construction of CBC

Here, we analyze networks of stochastic hybrid subsystems, $i \in \{1, \dots, N\}$,

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

and discuss how to construct a CBC of the interconnected system based on CStC of subsystems using dissipativity-type compositional conditions. We assume that for hybrid subsystems $\Sigma_i, i \in \{1, \dots, N\}$, there exist CStC $\mathcal{B}_i$ as defined in Definition 4.3.1 with the corresponding functions, constant, and matrices denoted by $\kappa_i \in \mathcal{K}_\infty$, $\gamma_i, \psi_i \in \mathbb{R}_{\geq 0}$, $\lambda_i \in \mathbb{R}_{>0}$, $\mathcal{X}_i$, $\mathcal{X}_i^{11}$, $\mathcal{X}_i^{12}$, $\mathcal{X}_i^{21}$, and $\mathcal{X}_i^{22}$. In the next theorem, we compositionally construct a control barrier certificate for the interconnected system Σ as presented in Definition 3.5.2.

Theorem 4.3.4. *Consider an interconnected stochastic hybrid system $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ stochastic hybrid subsystems Σ_i and the coupling matrix M. Suppose that each subsystem Σ_i admits a CStC $\mathcal{B}_i$ as defined in Definition 4.3.1 with the corresponding initial and unsafe sets X_{0_i} and X_{u_i}, respectively. Then*

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

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

$$\begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}} \end{bmatrix}^\top \mathcal{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}} \end{bmatrix} \preceq 0, \tag{4.3.5}$$

$$\sum_{i=1}^{N} \mu_i \lambda_i > \sum_{i=1}^{N} \mu_i \gamma_i, \tag{4.3.6}$$

where $\mathcal{X}_{cmp}$ is defined as (3.5.8) *and $\tilde{q} = \sum_{i=1}^{N} \bar{q}_{2i}$ with $\bar{q}_{2i}$ being dimensions of the* internal *output of subsystems Σ_i.*

Proof. We first show that conditions (4.2.6) and (4.2.7) in Definition 4.2.3 hold. For any $x := [x_1; \ldots; x_N] \in X_0 = \prod_{i=1}^{N} X_{0_i}$ and from (4.3.1)

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

and similarly for any $x := [x_1; \ldots; x_N] \in X_u = \prod_{i=1}^{N} X_{u_i}$ and from (4.3.2)

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

satisfying conditions (4.2.6) and (4.2.7) 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 (4.3.6). Now, we show that condition (4.2.8) holds, as well. One can obtain the chain of inequalities in (4.3.7) using compositionality condition (4.3.5) 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. ■

Remark 4.3.5. *Note that one can utilize Lemma 4.2.14 to reformulate the proposed conditions in Definition 4.3.1 as an SOS optimization problem and provide a systematic approach for computing CStC and corresponding control policies for subsystems Σ_i. In this case, condition* (4.2.18) *in Lemma 4.2.14 is changed to*

$$-\mathcal{L}\mathcal{B}_i(x_i) - \kappa_i(\mathcal{B}_i(x_i)) + \begin{bmatrix} w_i \\ h_{2_i}(x_i) \end{bmatrix}^{\top} \begin{bmatrix} \mathcal{X}_i^{11} & \mathcal{X}_i^{12} \\ \mathcal{X}_i^{21} & \mathcal{X}_i^{22} \end{bmatrix} \begin{bmatrix} w_i \\ h_{2_i}(x_i) \end{bmatrix} + \psi_i - \sum_{j=1}^{\bar{m}_i} (\nu_{j_i} - l_{\nu_{j_i}}(x_i))$$
$$- \hat{l}_i^{\top}(x_i, \nu_i, w_i) g_i(x_i) - l_{\nu_i}^{\top}(x_i, \nu_i, w_i) g_{\nu_i}(x_i) - l_{w_i}^{\top}(x_i, \nu_i, w_i) g_{w_i}(x_i).$$

4.3.3 Case Studies

4.3.3.1 Room Temperature Network

To illustrate the effectiveness of the proposed results, we first apply our approaches to the temperature regulation in (3.5.14) in a network of 1000 rooms by adding a Poisson process to the dynamics. We consider $\hat{\eta} = 0.005$, $\hat{\beta} = 0.06$, $\hat{\theta} = 0.15$, $G = R = 0.1\mathbb{I}_n$, $T_h = 48\,^{\circ}\mathsf{C}$, $T_E = [T_{e_1}; \ldots; T_{e_n}]$ with $T_{ei} = -15\,^{\circ}\mathsf{C}$, $\forall i \in \{1, \ldots, n\}$, $T(t) = [T_1(t); \ldots; T_n(t)]$ and $\nu(t) = [\nu_1(t); \ldots; \nu_n(t)]$. We also consider the rates of Poisson processes as $\bar{\lambda}_i = 0.1, \forall i \in \{1, \ldots, n\}$. Now by considering the individual rooms as in (3.5.15), one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ where the coupling matrix

$$
\begin{aligned}
\mathcal{LB}(x) &= \mathcal{L}\sum_{i=1}^{N}\mu_i\mathcal{B}_i(x_i) = \sum_{i=1}^{N}\mu_i\mathcal{LB}_i(x_i)\\
&\leq \sum_{i=1}^{N}\mu_i\big(-\kappa_i(\mathcal{B}_i(x_i)) + \psi_i + \begin{bmatrix} w_i \\ h_{2_i}(x_i)\end{bmatrix}^\top \begin{bmatrix}\mathcal{X}_i^{11} & \mathcal{X}_i^{12}\\ \mathcal{X}_i^{21} & \mathcal{X}_i^{22}\end{bmatrix}\begin{bmatrix} w_i \\ h_{2_i}(x_i)\end{bmatrix}\big)\\
&= \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i\\
&\quad + \begin{bmatrix} w_1\\ \vdots \\ w_N \\ h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}^\top \begin{bmatrix}\mu_1\mathcal{X}_1^{11} & & & \mu_1\mathcal{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\mathcal{X}_N^{11} & & & \mu_N\mathcal{X}_N^{12}\\ \mu_1\mathcal{X}_1^{21} & & & \mu_1\mathcal{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N\mathcal{X}_N^{21} & & & \mu_N\mathcal{X}_N^{22}\end{bmatrix}\begin{bmatrix} w_1\\ \vdots \\ w_N \\ h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}\\
&= \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i + \begin{bmatrix} M\begin{bmatrix} h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix} \\ h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}^\top \mathcal{X}_{cmp}\begin{bmatrix} M\begin{bmatrix} h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix} \\ h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}\\
&= \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i + \begin{bmatrix} h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}^\top \begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}}\end{bmatrix}^\top \mathcal{X}_{cmp}\begin{bmatrix} M \\ \mathbb{I}_{\tilde{q}}\end{bmatrix}\begin{bmatrix} h_{2_1}(x_1)\\ \vdots \\ h_{2_N}(x_N)\end{bmatrix}\\
&\leq \sum_{i=1}^{N} -\mu_i\kappa_i(\mathcal{B}_i(x_i)) + \sum_{i=1}^{N}\mu_i\psi_i \leq -\kappa(\mathcal{B}(x)) + \psi. \qquad (4.3.7)
\end{aligned}
$$

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 $X_i = [1,50], X_{0_i} = [19.5,20], X_{u_i} = [1,17]\cup[23,50], \forall i \in \{1,\dots,n\}$. 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 $W = [17,23]^{1000}$. We first search for CStC 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 [PAV+13] and the SDP solver SeDuMi [Stu99] to compute CStC as described in Lemma 4.2.14. We compute CStC 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 4.3.1 satisfying conditions (4.3.1)-(4.3.3) 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

$$\mathcal{X}_i = \begin{bmatrix} \hat{\kappa}_i e^{-4} \hat{\eta}^2 & 0 \\ 0 & -\hat{\kappa}_i e^{-4} \theta^2 T_h^2 \end{bmatrix}. \tag{4.3.8}$$

We now proceed with Theorem 4.3.4 to construct a CBC for the interconnected system using CStC of subsystems. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, n\}$, and utilizing $\mathcal{X}_i$ in (4.3.8), the matrix $\mathcal{X}_{cmp}$ in (3.5.8) is reduced to

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

and condition (4.3.5) is reduced to

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

without requiring any restrictions on the number or gains of subsystems. We used $M = M^\top$, and $4\hat{\kappa}_i e^{-4} \hat{\eta}^2 - \hat{\kappa}_i e^{-4} \theta^2 T_h^2 \preceq 0$ by employing Gershgorin circle theorem [Bel65] to show the above LMI. Moreover, the compositionality condition (4.3.6) is also met since $\lambda_i > \gamma_i, \forall i \in \{1, \ldots, n\}$. Then by employing the results of Theorem 4.3.4, one can conclude that $\mathcal{B}(T) = \sum_{i=1}^{1000} (0.3112 T_i^2 - 12.3035 T_i + 121.59906)$ 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 4.2.6, 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 $\mathcal{T} = 10$ with the probability of at least 96%, *i.e.,*

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

Closed-loop state trajectories of a representative room with 10 different noise realizations are illustrated in Figure 4.3.

It is worth highlighting that with the assumption of 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 [WTL15]. 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 Condition. In order to demonstrate the importance of the compositionality condition, we raise the following counter example. Consider a network of two rooms each equipped with a heater and connected circularly as

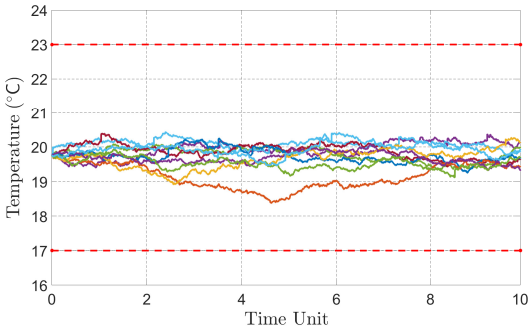

Figure 4.3: Closed-loop state trajectories of a representative room with 10 noise realizations in a network of 1000 rooms.

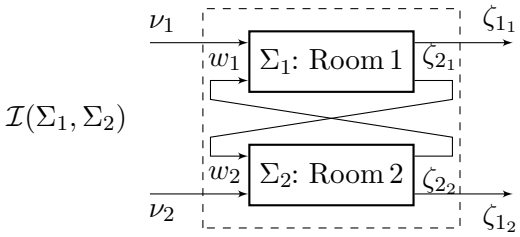

Figure 4.4: Interconnection of two rooms Σ_1 and Σ_2.

illustrated in Figure 4.4, with dynamics as in (3.5.15) 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 CStC 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

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

We now select $\mu_i = 1, \forall i \in \{1, 2\}$, and construct the matrix $\mathcal{X}_{cmp}$ in (3.5.8) as

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

Now we check the compositionality condition in (4.3.5) as

$$\begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix}^\top \mathcal{X}_{cmp} \begin{bmatrix} M \\ \mathbb{I}_n \end{bmatrix} \not\preceq 0,$$

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 (4.2.6)-(4.2.8)) with $\gamma = \gamma_1 + \gamma_2, \lambda = \lambda_1 + \lambda_2, \psi = \psi_1 + \psi_2$. As it can be observed from Figures 4.5-4.7, although conditions (4.2.6),(4.2.7) are satisfied for the overall barrier certificates $\mathcal{B}(T) = \mathcal{B}_1(T_1) + \mathcal{B}_2(T_2)$, condition (4.2.8) is violated since it is positive at some ranges of $X_1 \times X_2$.

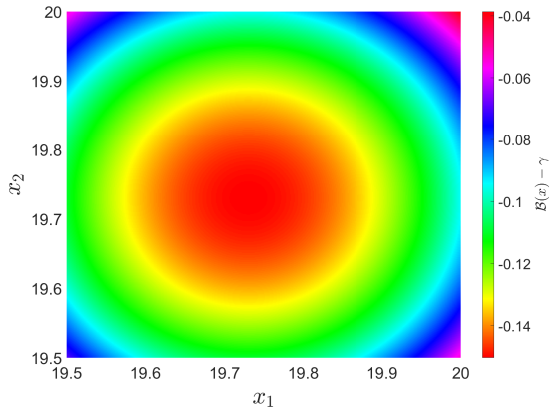

Figure 4.5: Satisfaction of condition (4.2.6). As observed, this condition is negative for all ranges of $x_1 \in X_{0_1}$ and $x_2 \in X_{0_2}$.

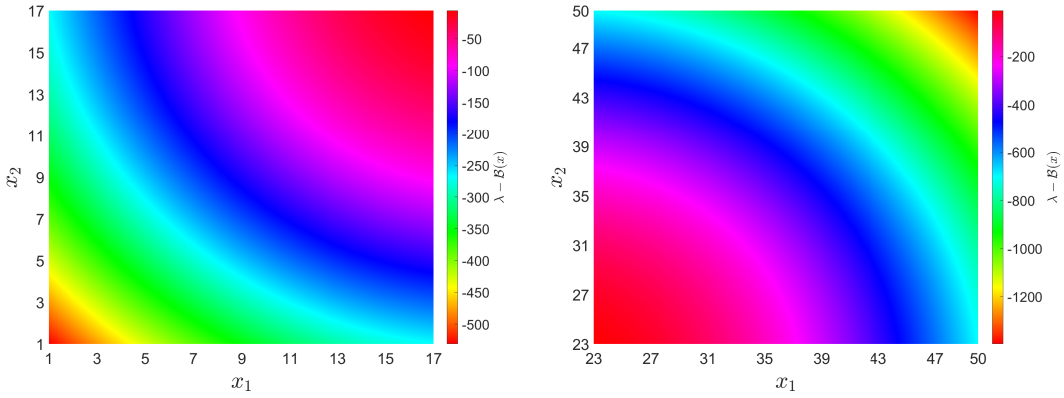

Figure 4.6: Satisfaction of condition (4.2.7). The condition is negative for all ranges of $x_1 \in X_{u_1}$ and $x_2 \in X_{u_2}$.

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.

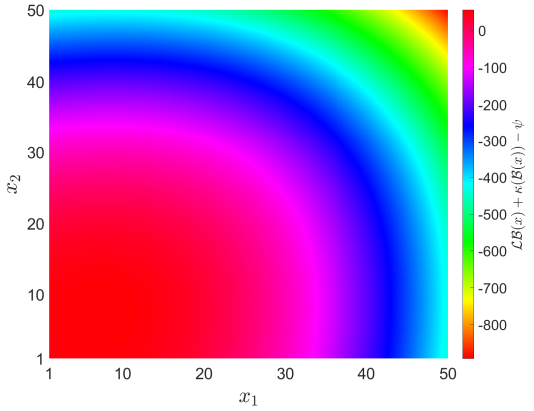

Figure 4.7: Violation of condition (4.2.8). As observed, this condition is positive for some ranges of $x_1 \in X_1$ and $x_2 \in X_2$.

4.3.3.2 Fully-Interconnected Network

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

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

with matrix $\bar{G} = (-I_n - L) \in \mathbb{R}^{n\times n}$, where L is the Laplacian matrix of a complete graph [GR01]:

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

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

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

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 4.2.14, we compute CStC 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 $i \in \{1,\dots,15\}$. The corresponding constants and functions in Definition 4.3.1 satisfying conditions (4.3.1)-(4.3.3) 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

$$\mathcal{X}_i = \begin{bmatrix} 10^{-6} & 10^{-2} \\ 10^{-2} & -5 \times 10^{-4} \end{bmatrix}. \tag{4.3.9}$$

We now proceed with Theorem 4.3.4 to construct a CBC for the interconnected system using CStC of subsystems. By selecting $\mu_i = 1, \forall i \in \{1,\dots,n\}$, and utilizing $\mathcal{X}_i$ in (4.3.9), the matrix $\mathcal{X}_{cmp}$ in (3.5.8) is reduced to

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

and condition (4.3.5) is reduced to

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

which is always satisfied without requiring any restrictions on the number or gains of subsystems. In order to show the above LMI, we used $L = L^\top \succeq 0$ which are always true for Laplacian matrices of undirected graphs. Moreover, the compositionality condition (4.3.6) is also satisfied since $\lambda_i > \gamma_i, \forall i \in \{1,\dots,n\}$. Then by employing Theorem 4.3.4, 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, $\nu(x) = [-5.1465x_1^2 + 60.3564; \dots; -5.1465x_{15}^2 + 60.3564]$ is the overall safety controller for the interconnected system.

By leveraging Theorem 4.2.6, 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 $\mathcal{T} = 10$ with the probability of at least 95%, *i.e.,*

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

Closed-loop state trajectories of a representative subsystem with 10 different noise realizations are illustrated in Figure 4.8.

4.4 Compositional Construction of Control Barrier Certificates for ct-SHS with Markovian Switching

In this section, we generalize the underlying dynamics to stochastic *switching* systems with *Markovian switching signals* as in Definition 2.5.1 and solve the controller synthesis

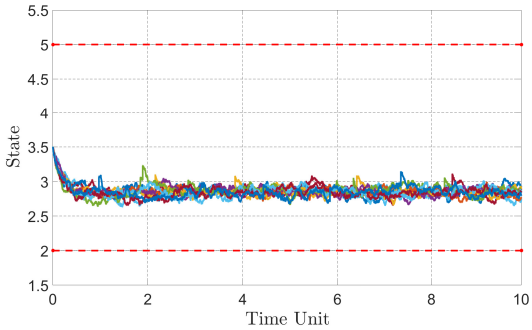

Figure 4.8: Closed-loop state trajectories of a representative subsystem with 10 noise realizations.

problem for this class of systems with respect to high-level logic properties in a compositional manner. The controller synthesis problem now is more challenging since it deals with two different types of adversarial inputs: (i) internal inputs modeling the effects of other subsystems, and (ii) switching signals which are randomly changing the modes of the system. We also enlarge the class of specifications to those that can be expressed by the accepting language of deterministic finite automata (DFA), whereas previous sections handle only invariance specifications. To do so, we decompose the given complex specification to simple reachability tasks based on automata representing the complements of original finite-state automata and provide upper bounds on probabilities of satisfaction for those reachability tasks by computing corresponding pseudo-barrier certificates. In addition, we provide an additional approach to compute pseudo-barrier certificates for systems with finite input sets by employing counter-example guided inductive synthesis framework based on the satisfiability modulo theories (SMT) solvers such as Z3 [DMB08], dReal [GAC12] or MathSat [CGSS13].

Remark 4.4.1. *In this section, we assume that the controller has access to switching modes, which is a standard assumption used in the relevant literature [DST+21]. In particular, it is supposed that there is a mode detection device which is capable of identifying the system mode in real time so that the controller can switch to the matched mode. There are some results, in the context of stability analysis of stochastic switching systems [ZNS19, RX16], which also consider some delay while deploying the synthesized controllers. However, this issue is out of the scope of this section and we leave it to future works (cf. future contributions in Section 6).*

Since the main contribution of this work is to propose a compositional approach for the construction of control barrier certificates, we are eventually interested in investigating interconnected systems without having internal inputs. In this case, the tuple (2.5.1) is reduced to $(X, U, \mathcal{U}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho})$ with $f_p : X \times U \to X$, and ct-SHS-MS (2.5.2) can be re-written as

$$\Sigma : \mathsf{d}\xi(t) = f_{\mathbf{p}(t)}(\xi(t), \nu(t))\,\mathsf{d}t + \sigma_{\mathbf{p}(t)}(\xi(t))\,\mathsf{d}\mathbb{W}_t + \rho_{\mathbf{p}(t)}(\xi(t))\,\mathsf{d}\mathbb{P}_t.$$

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

4.5 Control Pseudo-Barrier and Barrier Certificates for ct-SHS-MS

Here, we first introduce a notion of control pseudo-barrier certificates (CPBC) for ct-SHS-MS with both internal and external inputs. We then define a notion of control barrier certificates (CBC) for ct-SHS-MS with only external inputs. We then 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 4.5.4.

Definition 4.5.1. *Consider a ct-SHS-MS Σ_p, and sets $X_0, X_u \subseteq X$ as initial and unsafe sets of the system, respectively. A twice differentiable function $\mathcal{B}_p : X \to \mathbb{R}_{\geq 0}$ is called a control pseudo-barrier certificate (CPBC) for Σ_p if there exist $\alpha_p, \kappa_p \in \mathcal{K}_\infty$, $\rho_{\text{int}p} \in \mathcal{K}_\infty \cup \{0\}$, and $\gamma_p, \lambda_p, \psi_p \in \mathbb{R}_{\geq 0}$, such that for all $p \in P$,*

$$\mathcal{B}_p(x) \geq \alpha_p(\|h(x)\|^2), \qquad \forall x \in X, \tag{4.5.1}$$
$$\mathcal{B}_p(x) \leq \gamma_p, \qquad \forall x \in X_0, \tag{4.5.2}$$
$$\mathcal{B}_p(x) \geq \lambda_p, \qquad \forall x \in X_u, \tag{4.5.3}$$

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

$$\mathcal{L}\mathcal{B}_p(x) + \sum_{p'=1}^{m} \tilde{\lambda}_{pp'}(x)\mathcal{B}_{p'}(x) \leq -\kappa_p(\mathcal{B}_p(x)) + \rho_{\text{int}p}(\|w\|^2) + \psi_p, \tag{4.5.4}$$

where $\mathcal{L}\mathcal{B}_p$ is the infinitesimal generator of the stochastic process acting on $\mathcal{B}_p$ [Oks13], defined as

$$\mathcal{L}\mathcal{B}_p(x) = \partial_x \mathcal{B}_p(x) f_p(x,\nu,w) + \frac{1}{2}\mathsf{Tr}(\sigma_p(x)\sigma_p(x)^\top \partial_{x,x}\mathcal{B}_p(x)) + \sum_{j=1}^{r} \bar{\lambda}_j(\mathcal{B}_p(x+\rho_p(x)\mathsf{e}_j^r) - \mathcal{B}_p(x)),$$

where e_j^r denotes an r-dimensional vector with 1 on the j-th entry and 0 elsewhere.

Now we adapt the above notion to the interconnected ct-SHS-MS without internal inputs by simply eliminating all terms related to w.

Definition 4.5.2. *Consider an (interconnected) ct-SHS-MS $\Sigma = (X, U, \mathcal{U}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho})$, and $X_0, X_u \subseteq X$ as, respectively, initial and unsafe sets of the interconnected system. A function $\mathcal{B} : X \times P \to \mathbb{R}_{\geq 0}$, that is twice differentiable with respect to x, is called a control barrier certificate (CBC) for Σ if, for all $p \in P$,*

$$\mathcal{B}(x,p) \leq \gamma, \qquad \forall x \in X_0, \tag{4.5.5}$$
$$\mathcal{B}(x,p) \geq \lambda, \qquad \forall x \in X_u, \tag{4.5.6}$$

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

$$\mathcal{L}\mathcal{B}(x,p) + \sum_{p'=1}^{\mathbb{M}} \tilde{\lambda}_{pp'}(x)\mathcal{B}(x,p') \leq -\kappa(\mathcal{B}(x,p)) + \psi, \tag{4.5.7}$$

for some $\kappa \in \mathcal{K}_\infty$, $\gamma, \lambda, \psi \in \mathbb{R}_{\geq 0}$, *with* $\lambda > \gamma$, *and* $\mathbb{M} = \Pi_{i=1}^{N} m_i$, *where* m_i *is the number of modes for each subsystem* Σ_i *as in* (2.5.2).

Remark 4.5.3. *Note that since control barrier certificates provide only sufficient conditions for synthesizing safety controllers and not necessary ones, the initial level-set of CBC, i.e.,* $\mathcal{B}(x,p) = \gamma$ *which is mode-dependent here, is a subset of the maximal winning set. One can always maximize the volume of the initial level-set of CBC, potentially to be close to the maximal winning set, by increasing the degree of CBC but at the cost of having more computational complexity. Remark that due to having unbounded noises in the stochastic setting, the corresponding safety guarantee in Theorem 4.5.4 comes with some probability as opposed to deterministic setting where the safety is guaranteed for all realizations.*

The next theorem shows the usefulness of CBC to quantify upper bounds on probabilities that (interconnected) systems reach certain unsafe regions.

Theorem 4.5.4. *Let* $\Sigma = (X, U, \mathcal{U}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho})$ *be an (interconnected) ct-SHS without internal inputs. Suppose* $\mathcal{B}(x,p)$ *is a CBC for* Σ *as in Definition 4.5.2, and there exists a constant* $\hat{\kappa} \in \mathbb{R}_{>0}$ *such that the function* $\kappa \in \mathcal{K}_\infty$ *in* (4.5.7) *satisfies* $\kappa(s) \leq \hat{\kappa}s$, $\forall s \in \mathbb{R}_{\geq 0}$. *Then the probability that the solution process of* Σ *starting from any initial state* $\xi^p(0) = x_0 \in X_0$ *and any initial mode* p_0 *reaches* X_u *under policy* $\nu(\cdot)$ *within a time horizon* $[0, \mathcal{T}] \subseteq \mathbb{R}_{\geq 0}$ *is formally quantified as*

$$\begin{aligned} &\mathbb{P}_\nu^{x_0}\Big\{\xi^p(t) \in X_u \text{ for some } 0 \leq t \leq \mathcal{T} \mid \xi^p(0) = x_0, p_0\Big\} \leq \bar{\delta}, \\ &\bar{\delta} := \begin{cases} 1 - (1 - \frac{\gamma}{\lambda})e^{-\frac{\psi \mathcal{T}}{\lambda}}, & \text{if } \lambda \geq \frac{\psi}{\hat{\kappa}}, \\ \frac{\hat{\kappa}\gamma + (e^{\hat{\kappa}\mathcal{T}} - 1)\psi}{\hat{\kappa}\lambda e^{\hat{\kappa}\mathcal{T}}}, & \text{if } \lambda \leq \frac{\psi}{\hat{\kappa}}. \end{cases} \end{aligned} \tag{4.5.8}$$

The proof of Theorem 4.5.4 is similar to that of Theorem 4.2.6 based on a direct use of [Kus67, Theorem 1, Chapter III] and is omitted here.

The proposed results in Theorem 4.5.4 provide upper bounds on the probability that interconnected systems reach unsafe regions in *finite time* horizons. We now generalize the proposed results to *infinite time* horizon, as in the next corollary, provided that constant $\psi = 0$

Corollary 4.5.5. *Let* $\Sigma = (X, U, \mathcal{U}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho})$ *be an interconnected ct-SHS without internal inputs. Suppose* $\mathcal{B}(x,p)$ *is a CBC for* Σ *such that* $\psi = 0$ *in* (4.5.7). *Then the probability that the solution process of* Σ *starting from any initial state* $\xi^p(0) = x_0 \in X_0$ *and any initial mode* p_0 *reaches* X_u *under policy* $\nu(\cdot)$ *within a time horizon* $[0, \infty)$ *is formally quantified as*

$$\mathbb{P}_\nu^{x_0}\Big\{\xi^p(t) \in X_u \text{ for some } 0 \leq t < \infty \mid \xi^p(0) = x_0, p_0\Big\} \leq \frac{\gamma}{\lambda}.$$

The proof is similar to that of Theorem 4.2.6 by applying [Kus67, Theorem 12, Chapter II] and is omitted here.

Remark 4.5.6. *Note that CBC $\mathcal{B}(x,p)$ satisfying condition (4.5.7) with $\psi = 0$ is a non-negative supermartingale [Kus67, Chapter I]. Although the supermartingale property on $\mathcal{B}$ allows one to provide probabilistic guarantees for infinite time horizons via Corollary 4.5.5, it is restrictive in the sense that a supermartingale CBC $\mathcal{B}$ may not generally exist [ST12]. Hence, we employ a more general c-martingale type condition in our work that does not require such an assumption at the cost of providing probabilistic guarantees only for finite time horizons.*

4.5.1 Compositional Construction of CBC for ct-SHS-MS

Here, we provide a compositional framework for the construction of CBC for ct-SHS-MS Σ. Suppose we are given N stochastic hybrid subsystems $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, P_i, \mathcal{P}_i, \hat{f}_i, \hat{\sigma}_i, \hat{\rho}_i, Y_i, h_i), i \in \{1, \dots, N\}$, where their internal inputs and outputs are partitioned as (3.3.9)-(3.3.10). Assume that for $\Sigma_{ip_i}, p_i \in \{1, \dots, m_i\}, i \in \{1, \dots, N\}$, there exist CPBC $\mathcal{B}_{ip_i}$ as defined in Definition 4.5.1 with functions $\alpha_{ip_i}, \kappa_{ip_i} \in \mathcal{K}_\infty$, $\rho_{\text{int}ip_i} \in \mathcal{K}_\infty \cup \{0\}$, and constants $\gamma_{ip_i}, \lambda_{ip_i}, \psi_{ip_i} \in \mathbb{R}_{\geq 0}$. One can define the interconnected ct-SHS-MS similar to Definition 3.3.6 with $\hat{f} := \prod_{i=1}^{N} \hat{f}_i$, $\hat{\sigma} := \mathsf{blkdiag}(\hat{\sigma}_1(x_1), \dots, \hat{\sigma}_N(x_N))$, and $\hat{\rho} := \mathsf{blkdiag}(\hat{\rho}_1(x_1), \dots, \hat{\rho}_N(x_N))$. In order to establish the main compositionality result of the section, we raise the following sum-type small-gain assumption for ct-SHS-MS.

Assumption 4.5.7. *Assume that for any $i, j \in \{1, \cdots, N\}$, $i \neq j$, there exist $\mathcal{K}_\infty$ functions $\hat{\gamma}_i$ and constants $\hat{\lambda}_{ip_i} \in \mathbb{R}_{>0}$ and $\hat{\delta}_{ijp_j} \in \mathbb{R}_{\geq 0}$ such that for any $s \in \mathbb{R}_{\geq 0}$:*

$$\kappa_{ip_i}(s) \geq \hat{\lambda}_{ip_i} \hat{\gamma}_i(s), \tag{4.5.9}$$

$$h_{ji} \equiv 0 \implies \hat{\delta}_{ijp_j} = 0,$$

$$h_{ji} \not\equiv 0 \implies \rho_{\text{int}_{ip_i}}((N-1)\alpha_{jp_j}^{-1}(s)) \leq \hat{\delta}_{ijp_j} \hat{\gamma}_j(s), \tag{4.5.10}$$

where α_{jp_j}, κ_{ip_i}, and $\rho_{\text{int}_{ip_i}}$, represent the corresponding $\mathcal{K}_\infty$ functions related to $\mathcal{B}_{ip_i}$ appearing in Definition 4.5.1.

Before presenting the main compositionality theorem, we define $\Lambda := \mathsf{diag}(\hat{\lambda}_1, \dots, \hat{\lambda}_N)$ with $\hat{\lambda}_i = \min_{p_i \in P_i}\{\hat{\lambda}_{ip_i}\}$, $\Delta := \{\hat{\delta}_{ij}\}$ with $\hat{\delta}_{ij} = \max_{p_i \in P_i}\{\delta_{ijp_i}\}$ and $\hat{\delta}_{ii} = 0$, $\forall i \in \{1, \cdots, N\}$, and $\Gamma(s) := [\hat{\gamma}_1(s_1); \dots; \hat{\gamma}_N(s_N)]$, where $s = [s_1; \dots; s_N]$. In the next theorem, we leverage small-gain Assumption 4.5.7 to compositionally compute a control barrier certificate for the interconnected ct-SHS-MS.

Theorem 4.5.8. *Consider an interconnected ct-SHS-MS $\Sigma = \mathcal{I}(\Sigma_1, \dots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ stochastic hybrid subsystems $\Sigma_i = (X_i, U_i, W_i, \mathcal{U}_i, \mathcal{W}_i, P_i, \mathcal{P}_i, \hat{f}_i, \hat{\sigma}_i, \hat{\rho}_i, Y_i, h_i)$. Suppose that each mode Σ_{ip_i} admits a CPBC $\mathcal{B}_{ip_i}$ as defined in Definition 4.5.1 with initial and unsafe sets X_{0_i} and X_{u_i}, respectively. If Assumption 4.5.7 holds and there*

exists a vector μ *with* $\mu_i > 0, i \in \{1, \ldots, N\}$*, such that*

$$\mu^\top(-\Lambda + \Delta) < 0, \tag{4.5.11}$$

$$\sum_{i=1}^{N} \mu_i \min_{p_i \in P_i}\{\lambda_{ip_i}\} > \sum_{i=1}^{N} \mu_i \max_{p_i \in P_i}\{\gamma_{ip_i}\}, \tag{4.5.12}$$

then

$$\mathcal{B}(x, p) := \sum_{i=1}^{N} \mu_i \mathcal{B}_{ip_i}(x_i), \tag{4.5.13}$$

with $p = [p_1; \ldots; p_N], p_i \in \{1, \ldots, m_i\}$*, is a CBC for the interconnected system* $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ *with initial and unsafe sets* $X_0 := \prod_{i=1}^{N} X_{0_i}$*,* $X_u := \prod_{i=1}^{N} X_{u_i}$*, respectively.*

Proof. We first show that conditions (4.5.5) and (4.5.6) in Definition 4.5.2 hold. For any $x := [x_1; \ldots; x_N] \in X_0 = \prod_{i=1}^{N} X_{0_i}$ and from (4.5.2)

$$\mathcal{B}(x, p) = \sum_{i=1}^{N} \mu_i \mathcal{B}_{ip_i}(x_i) \leq \sum_{i=1}^{N} \mu_i \gamma_{ip_i} \leq \sum_{i=1}^{N} \mu_i \max_{p_i \in P_i}\{\gamma_{ip_i}\} = \gamma,$$

and similarly for any $x := [x_1; \ldots; x_N] \in X_u = \prod_{i=1}^{N} X_{u_i}$ and from (4.5.3)

$$\mathcal{B}(x, p) = \sum_{i=1}^{N} \mu_i \mathcal{B}_{ip_i}(x_i) \geq \sum_{i=1}^{N} \mu_i \lambda_{ip_i} \geq \sum_{i=1}^{N} \mu_i \min_{p_i \in P_i}\{\lambda_{ip_i}\} = \lambda,$$

satisfying conditions (4.5.5) and (4.5.6) with $\gamma = \sum_{i=1}^{N} \mu_i \max_{p_i \in P_i}\{\gamma_{ip_i}\}$ and $\lambda = \sum_{i=1}^{N} \mu_i \min_{p_i \in P_i}\{\lambda_{ip_i}\}$. Note that $\lambda > \gamma$ according to (4.5.12). Now, we show that condition (4.5.7) holds, as well. We first compute $\sum_{p'=1}^{\mathbb{M}} \tilde{\lambda}_{pp'}(x)\mathcal{B}(x, p')$ in (4.5.7) based on transition rates of subsystems. To do so, we first compute it for two subsystems with three modes and then extend it to the general case of N subsystems with $\mathbb{M}$ modes. Consider two subsystems Σ_1, Σ_2 with 3 independent modes, *i.e.,* $m_1 = 3, m_2 = 3$. The generator matrix [ASSB00] of Σ_1, Σ_2 are constructed as

$$\tilde{Q}_{\Sigma_1} = \begin{bmatrix} -\tilde{\lambda}_{12_1} - \tilde{\lambda}_{13_1} & \tilde{\lambda}_{12_1} & \tilde{\lambda}_{13_1} \\ \tilde{\lambda}_{21_1} & -\tilde{\lambda}_{21_1} - \tilde{\lambda}_{23_1} & \tilde{\lambda}_{23_1} \\ \tilde{\lambda}_{31_1} & \tilde{\lambda}_{32_1} & -\tilde{\lambda}_{31_1} - \tilde{\lambda}_{32_1} \end{bmatrix},$$

$$\tilde{Q}_{\Sigma_2} = \begin{bmatrix} -\tilde{\lambda}_{12_2} - \tilde{\lambda}_{13_2} & \tilde{\lambda}_{12_2} & \tilde{\lambda}_{13_2} \\ \tilde{\lambda}_{21_2} & -\tilde{\lambda}_{21_2} - \tilde{\lambda}_{23_2} & \tilde{\lambda}_{23_2} \\ \tilde{\lambda}_{31_2} & \tilde{\lambda}_{32_2} & -\tilde{\lambda}_{31_2} - \tilde{\lambda}_{32_2} \end{bmatrix}.$$

Now we construct the generator matrix for the interconnected system $\Sigma = \mathcal{I}(\Sigma_1, \Sigma_2)$ via Table 4.1, in which the first and second elements of the pair $(\cdot, \cdot)$ are corresponding

Table 4.1: Generator matrix of the interconnected system $\Sigma = \mathcal{I}(\Sigma_1, \Sigma_2)$.

$\tilde{Q}_{\mathcal{I}(\Sigma_1,\Sigma_2)}$	$(1,1)$	$(1,2)$	$(1,3)$	$(2,1)$	$(2,2)$	$(2,3)$	$(3,1)$	$(3,2)$	$(3,3)$
$(1,1)$	$*$	$\tilde{\lambda}_{12_2}$	$\tilde{\lambda}_{13_2}$	$\tilde{\lambda}_{12_1}$	0	0	$\tilde{\lambda}_{13_1}$	0	0
$(1,2)$	$\tilde{\lambda}_{21_2}$	$*$	$\tilde{\lambda}_{23_2}$	0	$\tilde{\lambda}_{12_1}$	0	0	$\tilde{\lambda}_{13_1}$	0
$(1,3)$	$\tilde{\lambda}_{31_2}$	$\tilde{\lambda}_{32_2}$	$*$	0	0	$\tilde{\lambda}_{12_1}$	0	0	$\tilde{\lambda}_{13_1}$
$(2,1)$	$\tilde{\lambda}_{21_1}$	0	0	$*$	$\tilde{\lambda}_{12_2}$	$\tilde{\lambda}_{13_2}$	$\tilde{\lambda}_{23_1}$	0	0
$(2,2)$	0	$\tilde{\lambda}_{21_1}$	0	$\tilde{\lambda}_{21_2}$	$*$	$\tilde{\lambda}_{23_2}$	0	$\tilde{\lambda}_{23_1}$	0
$(2,3)$	0	0	$\tilde{\lambda}_{21_1}$	$\tilde{\lambda}_{31_2}$	$\tilde{\lambda}_{32_2}$	$*$	0	0	$\tilde{\lambda}_{23_1}$
$(3,1)$	$\tilde{\lambda}_{31_1}$	0	0	$\tilde{\lambda}_{32_1}$	0	0	$*$	$\tilde{\lambda}_{12_2}$	$\tilde{\lambda}_{13_2}$
$(3,2)$	0	$\tilde{\lambda}_{21_1}$	0	0	$\tilde{\lambda}_{32_1}$	0	$\tilde{\lambda}_{21_2}$	$*$	$\tilde{\lambda}_{23_2}$
$(3,3)$	0	0	$\tilde{\lambda}_{31_1}$	0	0	$\tilde{\lambda}_{32_1}$	$\tilde{\lambda}_{31_2}$	$\tilde{\lambda}_{32_2}$	$*$

to switching modes of the first and second subsystems, respectively. Moreover, diagonal elements "$*$" are the summation of off-diagonals in each row with a negative sign, *i.e.,* summation of each row including "$*$" should be zero. For each state (p_{i_1}, p_{j_2}), we can jump to $(p_{i'_1}, p_{j'_2})$ with $i = i'$ or $j = j'$, *i.e.,* only one of the modes can change [ASSB00]. Then by employing the definition of CBC in (4.5.13) and Table 4.1, one has

$$\begin{aligned}
&\sum_{p'=1}^{9} \tilde{\lambda}_{pp'}(x)\mathcal{B}(x,p') = \sum_{p'_1=1,p'_2=1}^{3} \tilde{\lambda}_{p_1,p_2,p'_1,p'_2}(x) \sum_{i=1}^{2} \mu_i \mathcal{B}_{p'_i}(x_i) \\
&= \sum_{p'_1=1,p'_2=1}^{3} \tilde{\lambda}_{p_1,p_2,p'_1,p'_2}(x)\mu_1\mathcal{B}_{1p'_1}(x_1) + \sum_{p'_1=1,p'_2=1}^{3} \tilde{\lambda}_{p_1,p_2,p'_1,p'_2}(x)\mu_2\mathcal{B}_{2p'_2}(x_2) \\
&= \sum_{p'_1=1}^{3} \mu_1\mathcal{B}_{1p'_1}(x_1) \overbrace{\sum_{p'_2=1}^{3} \tilde{\lambda}_{p_1,p_2,p'_1,p'_2}(x)}^{\tilde{\lambda}_{p_1p'_1}} + \sum_{p'_2=1}^{3} \mu_2\mathcal{B}_{2p'_2}(x_2) \overbrace{\sum_{p'_1=1}^{3} \tilde{\lambda}_{p_1,p_2,p'_1,p'_2}(x)}^{\tilde{\lambda}_{p_2p'_2}} \\
&= \sum_{p'_1=1}^{3} \mu_1\tilde{\lambda}_{p_1p'_1}\mathcal{B}_{1p'_1}(x_1) + \sum_{p'_2=1}^{3} \mu_2\tilde{\lambda}_{p_2p'_2}\mathcal{B}_{2p'_2}(x_2) = \sum_{i=1}^{2}\sum_{p'_i=1}^{3} \mu_i\tilde{\lambda}_{p'_ip_i}(x_i)\mathcal{B}_{ip'_i}(x_i).
\end{aligned}$$

One can readily extend the results to N subsystem, each of which has m_i modes, and conclude that $\sum_{p'=1}^{\mathbb{M}} \tilde{\lambda}_{pp'}(x)\mathcal{B}(x,p') = \sum_{i=1}^{N}\sum_{p'_i=1}^{m_i} \mu_i\tilde{\lambda}_{p_ip'_i}(x_i)\mathcal{B}_{ip'_i}(x_i)$ with $\mathbb{M} = \Pi_{i=1}^{N} m_i$. By applying the following inequality

$$\rho_{\text{int}_{i_{p_i}}}(s_1 + \cdots + s_{N-1}) \leq \sum_{i=1}^{N-1} \rho_{\text{int}_{i_{p_i}}}((N-1)s_i),$$

which is valid for any $\rho_{\text{int}_{i_{p_i}}} \in \mathcal{K}_\infty \cup \{0\}$, and any $s_i \in \mathbb{R}_{\geq 0}$, $i \in \{1, \cdots, N\}$, employing condition (4.5.1) and Assumption 4.5.7, one can obtain the chain of inequalities in

(4.5.14). By defining

$$\kappa(s) := \min\Big\{ -\mu^\top(-\Lambda+\Delta)\Gamma(\bar{\mathcal{B}}(x)) \,\big|\, \mu^\top\bar{\mathcal{B}}(x) = s\Big\},$$
$$\psi := \sum_{i=1}^{N} \mu_i \max_{p_i\in P_i}\{\psi_{ip_i}\},$$

where $\bar{\mathcal{B}}(x) = [\mathcal{B}_{1p_1}(x_1);\ldots;\mathcal{B}_{Np_N}(x_N)]$, condition (4.5.7) is also satisfied. Then $\mathcal{B}$ is a CBC for Σ, which completes the proof. ■

$$\begin{aligned}
&\mathcal{L}\mathcal{B}(x,p) + \sum_{p'=1}^{\mathbb{M}} \tilde{\lambda}_{pp'}(x)\mathcal{B}(x,p') = \mathcal{L}\sum_{i=1}^{N}\mu_i\mathcal{B}_{ip_i}(x_i) + \sum_{i=1}^{N}\sum_{p_i'=1}^{m_i}\mu_i\tilde{\lambda}_{p_ip_i'}(x_i)\mathcal{B}_{ip_i'}(x_i)\\
&= \sum_{i=1}^{N}\mu_i\big(\mathcal{L}\mathcal{B}_{ip_i}(x_i) + \sum_{p_i'=1}^{m_i}\tilde{\lambda}_{p_ip_i'}(x_i)\mathcal{B}_{ip_i'}(x_i)\big) \le \sum_{i=1}^{N}\mu_i\big(-\kappa_{ip_i}(\mathcal{B}_{ip_i}(x_i)) + \rho_{\mathrm{int}_{ip_i}}(\|w_i\|^2) + \psi_{ip_i}\big)\\
&\le \sum_{i=1}^{N}\mu_i\big(-\kappa_{ip_i}(\mathcal{B}_{ip_i}(x_i)) + \rho_{\mathrm{int}_{ip_i}}(\sum_{j=1,i\neq j}^{N}\|w_{ij}\|^2) + \psi_{ip_i}\big)\\
&= \sum_{i=1}^{N}\mu_i\big(-\kappa_{ip_i}(\mathcal{B}_{ip_i}(x_i)) + \rho_{\mathrm{int}_{ip_i}}(\sum_{j=1,i\neq j}^{N}\|y_{ji}\|^2) + \psi_{ip_i}\big)\\
&\le \sum_{i=1}^{N}\mu_i\big(-\kappa_{ip_i}(\mathcal{B}_{ip_i}(x_i)) + \sum_{j=1,i\neq j}^{N}\rho_{\mathrm{int}_{ip_i}}((N-1)\|y_{ji}\|^2) + \psi_{ip_i}\big)\\
&\le \sum_{i=1}^{N}\mu_i\big(-\kappa_{ip_i}(\mathcal{B}_{ip_i}(x_i)) + \sum_{j=1,i\neq j}^{N}\rho_{\mathrm{int}_{ip_i}}((N-1)\|h_j(x_j)\|^2) + \psi_{ip_i}\big)\\
&\le \sum_{i=1}^{N}\mu_i\big(-\kappa_{ip_i}(\mathcal{B}_{ip_i}(x_i)) + \sum_{j=1,i\neq j}^{N}\rho_{\mathrm{int}_{ip_i}}((N-1)\alpha_{jp_j}^{-1}(\mathcal{B}_{jp_j}(x_j))) + \psi_{ip_i}\big)\\
&\le \sum_{i=1}^{N}\mu_i\big(-\hat{\lambda}_{ip_i}\hat{\gamma}_i(\mathcal{B}_{ip_i}(x_i)) + \sum_{j=1,i\neq j}^{N}\hat{\delta}_{ijp_j}\hat{\gamma}_j(\mathcal{B}_{jp_j}(x_j)) + \psi_{ip_i}\big)\\
&= \mu^\top(-\Lambda+\Delta)\Gamma(\mathcal{B}_{1p_1}(x_1);\ldots;\mathcal{B}_{Np_N}(x_N)) + \sum_{i=1}^{N}\mu_i\psi_{ip_i} \le -\kappa(\mathcal{B}(x,p)) + \psi. \qquad (4.5.14)
\end{aligned}$$

Remark 4.5.9. *Note that $\hat{\lambda}_{ip_i}$ and $\hat{\delta}_{ijp_j}$ in Assumption 4.5.7 are used to capture, respectively, the gains of each individual subsystem and its interaction with other subsystems in the interconnection topology, i.e., $\kappa_{ip_i}, \rho_{\mathrm{int}_{ip_i}}$. Those $\hat{\lambda}_{ip_i}$ and $\hat{\delta}_{ijp_j}$ satisfying conditions* (4.5.9)-(4.5.10) *are then utilized for the construction of Λ and Δ, and accordingly, establishing the compositionality condition $\rho_{spc}(\Lambda^{-1}\Delta) < 1$. On the downside, the*

small-gain type requirements inherently condition the spectral radius of the interconnection matrix which, in general, depends on the size of the graph and can be violated as the number of subsystems grows [DK04], [ZA18, Remark 6.1].

4.5.2 Logic Specifications Expressed as DFA

In this subsection, we deal with a class of specifications expressed by the accepting language of deterministic finite automata (DFA), as formalized in the following definition.

Definition 4.5.10. *A deterministic finite automaton (DFA) is a tuple* $\mathcal{A} = \{Q_\ell, q_0, \Sigma_a, F_a, \mathsf{t}\}$*, where* Q_ℓ *is a finite set of locations,* $q_0 \subseteq Q_\ell$ *is the initial location,* Σ_a *is a finite set (a.k.a., alphabet),* $F_a \subseteq Q_\ell$ *is a finite set of accepting locations, and* $\mathsf{t} : Q_\ell \times \Sigma_a \to Q_\ell$ *is a transition function.*

We denote the set of states in the DFA that can be reached from q in the presence of input symbol $\tilde{\sigma}$ by $\mathsf{t}(q, \tilde{\sigma})$. A finite word (*a.k.a.,* trace) $(\tilde{\sigma}_0, \tilde{\sigma}_1, \ldots, \tilde{\sigma}_{k-1}) \in \Sigma_\mathsf{a}^k$ is accepted by the DFA if there exists a finite state run $\mathsf{q} = (q_0, q_1, \ldots, q_k) \in Q_\ell^{k+1}$ such that $q_{i+1} = \mathsf{t}(q_i, \tilde{\sigma}_i)$ for all $0 \leq i < k$ and $q_k \in F_\mathsf{a}$. Accordingly, we denote the set of all finite words accepted by $\mathcal{A}$, *i.e., the language accepted by the DFA* $\mathcal{A}$, by $\mathbb{L}(\mathcal{A})$. We also denote the set of all successor states of a state $q \in Q_\ell$ by $\Delta(q)$. The complement of a DFA is a DFA by simply interchanging accepting and non-accepting states [BK08].

Here, we study specifications represented by accepting languages of DFA $\mathcal{A}$ with symbols defined over a set of atomic propositions $\mathcal{AP}$, *i.e.,* $\Sigma_\mathsf{a} = 2^{\mathcal{AP}}$. Without loss of generality, we work here directly with the set of atomic propositions $\mathcal{AP}$ instead of its power set $2^{\mathcal{AP}}$, *i.e.,* $\Sigma_\mathsf{a} = \mathcal{AP}$. We are interested in LTL specifications in *finite time horizons*, in which the logic operators used in the definition of LTL will also come with a bound on the time horizon (cf. the case study).

We now define how solution processes of the interconnected ct-SHS-MS Σ over a finite-time horizon $\mathcal{T}$ are related to specifications given by the accepting language of DFA $\mathcal{A}$ via a measurable labeling function $\mathsf{L} : X \to \mathcal{AP}$.

Definition 4.5.11. *Consider an interconnected ct-SHS-MS* $\Sigma = (X, U, \mathcal{U}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho})$ *and a specification expressed by DFA* $\mathcal{A} = \{Q_\ell, q_0, \Sigma_a, F_a, \mathsf{t}\}$*. Let* $\mathsf{L} : X \to \mathcal{AP}$ *be a measurable labeling function. A finite sequence* $\tilde{\sigma}_\xi = (\tilde{\sigma}_0, \tilde{\sigma}_1, \ldots, \tilde{\sigma}_{k-1}) \in \mathcal{AP}^k$ *is a finite trace of the solution process* $\xi_{a\varrho}$ *under its corresponding control policy over a finite time horizon* $[0, \mathcal{T}] \subseteq R_{\geq 0}$ *if there exists an associated time sequence* $t_0, t_1, \ldots, t_{k-1}$ *such that* $t_0 = 0$*,* $t_k = \mathcal{T}$*, and for all* $j \in (0, 1, \ldots, k-1)$*,* $t_j \in R_{\geq 0}$ *the following conditions hold:*

- $t_j < t_{j+1}$
- $\xi(t_j) \in \mathsf{L}^{-1}(\tilde{\sigma}_j)$
- *If* $\tilde{\sigma}_j \neq \tilde{\sigma}_{j+1}$*, then for some* $t'_j \in [t_j, t_{j+1}]$*,*

$$\xi(t) \in \begin{cases} \mathsf{L}^{-1}(\tilde{\sigma}_j), & \forall t \in (t_j, t'_j), \\ \mathsf{L}^{-1}(\tilde{\sigma}_{j+1}), & \forall t \in (t'_j, t_{j+1}). \end{cases}$$

In other words,

$$\xi(t'_j) \in \mathsf{L}^{-1}(\tilde{\sigma}_j) \quad or \quad \mathsf{L}^{-1}(\tilde{\sigma}_{j+1}).$$

We now define the probability of satisfaction under which the solution processes of the interconnected system Σ over a finite time horizon $\mathcal{T}$ fulfill a specification expressed by DFA $\mathcal{A}$.

Definition 4.5.12. *Consider an interconnected ct-SHS-MS $\Sigma = (X, U, \mathcal{U}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho})$, a specification given by the accepting language of DFA $\mathcal{A} = \{Q_\ell, q_0, \Sigma_\mathsf{a}, F_\mathsf{a}, \mathsf{t}\}$, and a labeling function $\mathsf{L} : X \to \mathcal{AP}$. Then, $\mathbb{P}^{x_0}_{\varrho}\{\tilde{\sigma}_\xi \models \mathcal{A}\}$ denotes the probability that solution processes $\xi_{a\varrho}$ under the control policy ϱ with initial condition $\xi(0) = x_0$ satisfy the specification expressed by $\mathcal{A}$ over the finite time horizon $\mathcal{T}$.*

Remark 4.5.13. *Note that the set of atomic propositions $\mathcal{AP} = \{\bar{p}_0, \bar{p}_1, \ldots, \bar{p}_z\}$ and the labeling function $\mathsf{L} : X \to \mathcal{AP}$ provide a measurable partition of the state set $X = \cup_{i=1}^{z} X_i$ as $X_i := \mathsf{L}^{-1}(\bar{p}_i)$. Without loss of generality, we assume that $X_i \neq \emptyset$ for any i, since all the atomic propositions $\bar{p}_i$ with $\mathsf{L}^{-1}(\bar{p}_i) = \emptyset$ can be replaced by $(\neg \mathsf{true})$ without affecting the probability of satisfaction.*

Now we state the main problem that we aim to address in this subsection.

Problem 4.5.14. *Consider an interconnected ct-SHS-MS Σ, a specification expressed by the accepting language of DFA $\mathcal{A}$ and a labeling function L. Compute a control policy ϱ such that $\mathbb{P}^{x_0}_{\varrho}\{\tilde{\sigma}_\xi \models \mathcal{A}\} \geq 1 - \bar{\delta}$, for all $x_0 \in X_0$.*

To find a solution to Problem 4.5.14, we compute a control policy that guarantees $\mathbb{P}^{x_0}_{\varrho}\{\tilde{\sigma}_\xi \models \mathcal{A}^c\} \leq \bar{\delta}$ for all $x_0 \in \mathsf{L}^{-1}(\bar{p}_i)$ and some $i \in \{1, 2, \ldots, z\}$, where $\mathcal{A}^c = \{Q_\ell, q_0, \Sigma_\mathsf{a}, \bar{F}_\mathsf{a}, \mathsf{t}\}$ is a DFA which is the complement of DFA $\mathcal{A}$ with $\bar{F}_\mathsf{a} = Q_\ell \backslash F_\mathsf{a}$. Then the lower bound $1 - \bar{\delta}$ can be obviously achieved with the same control policy. Here, we propose our solution to Problem 4.5.14 by providing a method to decompose the complement of given specification into simple reachability problems. The main target now is to find a suitable CBC as in Definition 4.5.2 together with a controller for the interconnected ct-SHS-MS for simple reachability tasks. Since finding a CBC for large-scale complex systems can be computationally intractable, we first search for CPBC and the controller for each subsystem and then leverage compositionality results of Theorem 4.5.8 to acquire the overall CBC and the controller for the given interconnected system for each reachability task. We eventually combine the probabilities of different reachability problems in order to acquire an *overall* lower bound on the probability under which solution processes of the system satisfy the overall specification.

4.5.2.1 Sequential Reachability Decomposition

Here, we describe sequential reachability decomposition using which a complex specification expressed by DFA can be decomposed into simple reachability tasks. We follow a similar approach as the one proposed in [JSZ20, Section 4] but for networks of continuous-time stochastic systems.

For a DFA $\mathcal{A}$ representing the property of interest, we first construct a complement DFA $\mathcal{A}^c$, whose language contains all finite words not included in $\mathbb{L}(\mathcal{A})$. We then specify all accepting state runs of $\mathcal{A}^c$ and denote the set of all finite accepting state runs excluding self-loops by $\mathcal{R}$. The accepting state runs are then partitioned to sets of sequential state runs of length 3, where each of them describes a reachability task.

Let $|\mathsf{q}| = k+1$ be the length of the accepting state run and $\mathcal{R}$ be the set of all finite accepting state runs excluding self-loops, where

$$\mathcal{R} := \{\mathsf{q} = (q_0, q_1, \ldots, q_k) \in Q_\ell^{k+1} \big| q_k \in \bar{F}_\mathsf{a}, q_i \neq q_{i+1}, \forall i < k\}.$$

Note that computation of $\mathcal{R}$ can be efficiently performed by considering the DFA $\mathcal{A}^c$ as a directed graph $\mathcal{D} = (\bar{\mathcal{V}}, \mathcal{E})$, where $\bar{\mathcal{V}} = Q_\ell$ and $\mathcal{E} \subseteq \bar{\mathcal{V}} \times \bar{\mathcal{V}}$ are vertices and edges, respectively, such that $(q, q') \in \mathcal{E}$ if and only if $q' \neq q$ and there exists $\bar{p} \in \mathcal{AP}$ such that $\mathsf{t}(q, \bar{p}) = q'$. For any $(q, q') \in \mathcal{E}$, the atomic proposition corresponding to the edge (q, q') is denoted by $\tilde{\sigma}(q, q')$. It can be readily verified that a finite path starting at a vertex q_0 and terminating at a vertex that $q_k \in \bar{F}_\mathsf{a}$ is an accepting state run q of $\mathcal{A}^c$ without any self-loop belonging to $\mathcal{R}$. Then one can readily compute $\mathcal{R}$ by employing available algorithms for the graph theory such as variants of depth first search algorithm [RN02].

For each $\bar{p} \in \mathcal{AP}$, we define a set $\mathcal{R}^{\bar{p}}$ as

$$\mathcal{R}^{\bar{p}} := \{\mathsf{q} = (q_0, q_1, \ldots, q_k) \in \mathcal{R} \mid \tilde{\sigma}(q_0, q_1) = \bar{p} \in \mathcal{AP}\}.$$

We now utilize the definition of $\mathcal{P}^{\bar{p}}(\mathsf{q})$

$$\mathcal{P}^{\bar{p}}(\mathsf{q}) := \{(q_i, q_{i+1}, q_{i+2}) \,\big|\, 0 \leq i \leq k-2\},$$

which is the set of state runs of length 3, to characterize our problem as a multiple of reachability problems. We accordingly denote the set of all reachability elements arising from different accepting state run sequences by $\mathcal{P}(\mathcal{A}^c) = \bigcup_{\bar{p} \in \mathcal{AP}} \bigcup_{\mathsf{q} \in \mathcal{R}^{\bar{p}}} \mathcal{P}^{\bar{p}}(\mathsf{q})$. Computation of CBC is performed for each individual reachability problem that is obtained from the elements of $\mathcal{P}(\mathcal{A}^c)$.

To give the reader more insight on the sequential reachability decomposition, we present the following running example.

Running Example. Consider the DFA $\mathcal{A}^c$ in Figure 4.9 in which $\mathcal{AP} = \{\bar{p}_0, \bar{p}_1, \bar{p}_2, \bar{p}_3\}$ and $\bar{F}_\mathsf{a} = \{q_3\}$. The set of accepting state runs without self-loops is presented as

$$\mathcal{R} = \{(q_0, q_1, q_2, q_3), (q_0, q_1, q_5, q_3), (q_0, q_4, q_5, q_3), (q_0, q_4, q_3), (q_0, q_3)\}.$$

The sets $\mathcal{R}$ for each $\bar{p} \in \mathcal{AP}$ are denoted by $\mathcal{R}^{\bar{p}}$ and defined as follows:

$$\mathcal{R}^{\bar{p}_0} = \{(q_0, q_1, q_2, q_3), (q_0, q_1, q_5, q_3)\}, \quad \mathcal{R}^{\bar{p}_1} = \{(q_0, q_3)\},$$
$$\mathcal{R}^{\bar{p}_2} = \{(q_0, q_4, q_5, q_3), (q_0, q_4, q_3)\}, \quad \mathcal{R}^{\bar{p}_3} = \{(q_0, q_3)\}.$$

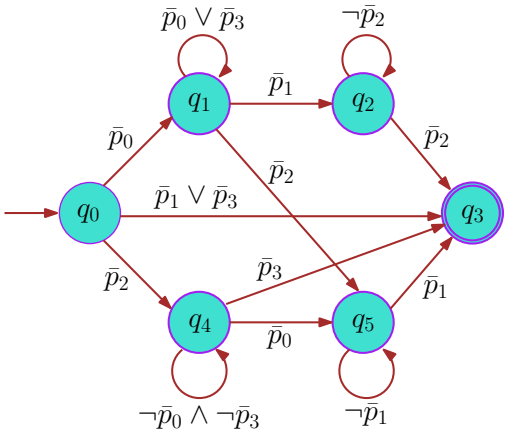

Figure 4.9: DFA $\mathcal{A}^c$ in the running example.

To decompose our complex specification into sequential reachabilities, we consider any $\mathsf{q} \in \mathcal{R}^{\bar{p}}$ and then define $\mathcal{P}^{\bar{p}}(\mathsf{q})$ as a set of all state runs of length 3 as

$$\begin{aligned}
&\mathcal{P}^{\bar{p}_0}(q_0, q_1, q_2, q_3) = \{(q_0, q_1, q_2), (q_1, q_2, q_3)\},\\
&\mathcal{P}^{\bar{p}_0}(q_0, q_1, q_5, q_3) = \{(q_0, q_1, q_5), (q_1, q_5, q_3)\},\\
&\mathcal{P}^{\bar{p}_2}(q_0, q_4, q_5, q_3) = \{(q_0, q_4, q_5), (q_4, q_5, q_3)\},\\
&\mathcal{P}^{\bar{p}_2}(q_0, q_4, q_3) = \{(q_0, q_4, q_3)\},\\
&\mathcal{P}^{\bar{p}_1}(q_0, q_3) = \mathcal{P}^{\bar{p}_3}(q_0, q_3) = \emptyset.
\end{aligned}$$

For every $\mathsf{q} \in \mathcal{R}^{\bar{p}}$, the corresponding finite words $\tilde{\sigma}(\mathsf{q})$ are given by

$$\begin{aligned}
&\tilde{\sigma}(q_0, q_3) = \{(\bar{p}_1 \vee \bar{p}_3)\}, \quad \tilde{\sigma}(q_0, q_4, q_3) = \{(\bar{p}_2, \bar{p}_3)\},\\
&\tilde{\sigma}(q_0, q_1, q_2, q_3) = \{(\bar{p}_0, \bar{p}_1, \bar{p}_2)\},\\
&\tilde{\sigma}(q_0, q_1, q_5, q_3) = \{(\bar{p}_0, \bar{p}_2, \bar{p}_1)\},\\
&\tilde{\sigma}(q_0, q_4, q_5, q_3) = \{(\bar{p}_2, \bar{p}_0, \bar{p}_1)\}.
\end{aligned}$$

■

The following lemma, as a consequence of Theorem 4.5.4, provides the construction of CBC and its corresponding controller from the elements of $\mathcal{P}^{\bar{p}}(\mathsf{q})$ constructed from the DFA $\mathcal{A}^c$.

Lemma 4.5.15. *Consider $(q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})$ for every $\bar{p} \in \mathcal{AP}$ and $\mathsf{q} \in \mathcal{R}^{\bar{p}}$. The probability that the solution process of ct-SHS-MS Σ starting from any initial state $a \in X_0 = \mathsf{L}^{-1}(\tilde{\sigma}(q, q'))$ under the control policy ϱ reaches $X_u = \mathsf{L}^{-1}(\tilde{\sigma}(q', q''))$ in a finite time horizon $\mathcal{T}$ is upper-bounded by $\bar{\delta}$ as in* (4.5.8)*, provided that there exists a CBC and a control policy ϱ such that conditions* (4.5.5)-(4.5.7) *hold.*

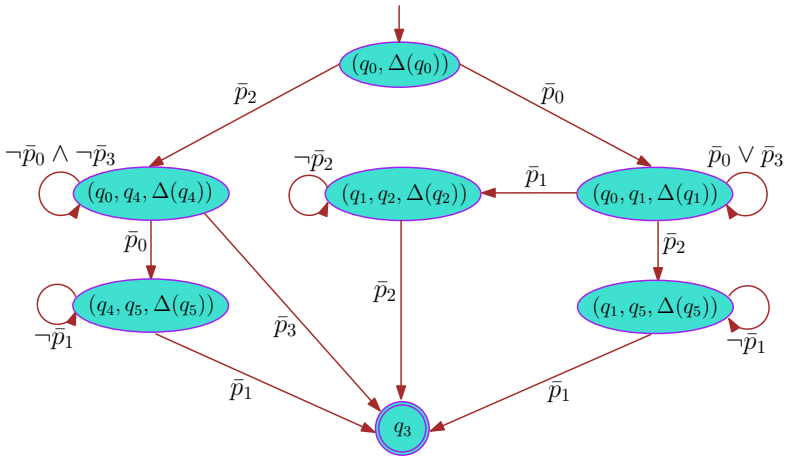

Figure 4.10: DFA $\mathcal{A}_\mathsf{s}$ describing switching mechanism.

4.5.2.2 Control Policy

In this subsection, we follow a similar approach as the one proposed in [JSZ20, Section 5.1] by combining controllers for reachability tasks to compute a hybrid controller enforcing the overall property. In our proposed controller synthesis scheme, one needs to compute a CBC and a suitable controller for each element of $\mathcal{P}(\mathcal{A}^c)$.

Consider the DFA $\mathcal{A}^c$ presented in Figure 4.9. The elements (q_0, q_1, q_2) and (q_0, q_1, q_5) compose two individual reachability problems: one for reaching the region $\mathsf{L}^{-1}(\bar{p}_1)$ and the other one for reaching the region $\mathsf{L}^{-1}(\bar{p}_2)$ both from the same region $\mathsf{L}^{-1}(\bar{p}_0)$. Since there may exist two outgoing transitions from a state of the automaton, one should deal with two different controllers available which may cause ambiguity while applying them in the closed loop. To tackle this problem, we combine the two reachability problems into one by replacing X_u in Lemma 4.5.15 with the union of regions corresponding to the alphabets presenting all the outgoing edges. This technique leads to a *common* CBC and the corresponding controller for different reachability elements in the same partition set. In order to interpret a switching control policy, we first define a DFA $\mathcal{A}_\mathsf{s}$, which includes the switching mechanism. We partition $\mathcal{P}(\mathcal{A}^c)$ and combine the reachability elements with the same CBC and control policy as follows:

$$\bar{\gamma}_{(q,q',\Delta(q'))} := \{(q, q', q'') \in \mathcal{P}(\mathcal{A}^c) \mid q, q', q'' \in Q_\ell, q'' \in \Delta(q')\}.$$

We denote the corresponding CBC and control policy to each partition set $\bar{\gamma}_{(q,q',\Delta(q'))}$ by respectively $\mathcal{B}_{\bar{\gamma}_{(q,q',\Delta(q'))}}(x)$ and $\nu_{\bar{\gamma}_{(q,q',\Delta(q'))}}$. In order to interpret a switching control policy, we first define a DFA $\mathcal{A}_\mathsf{s}$, which includes the switching mechanism as the following definition.

Definition 4.5.16. *Consider the DFA* $\mathcal{A}^c = \{Q_\ell, q_0, \Sigma_a, \bar{F}_a, \mathsf{t}\}$ *with* $\bar{F}_a = Q_\ell \backslash F_a$. *The corresponding DFA for switching mechanism is defined as* $\mathcal{A}_\mathsf{s} = \{Q_{\ell_s}, q_{0_s}, \Sigma_{a_s}, F_{a_s}, \mathsf{t}_\mathsf{s}\}$ *where* $Q_{\ell_s} := q_{0_s} \cup \{(q, q', \Delta(q')) \mid q, q' \in Q_\ell \backslash \bar{F}_a)\} \cup \bar{F}_a$ *is a finite set of locations,* $q_{0_s} :=$

$\{(q, \Delta(q)) \,|\, q = q_0\}$ *is a finite set of initial locations,* $\Sigma_{\mathsf{a}_s} = \Sigma_{\mathsf{a}}$ *is a finite set as the alphabet for switching mechanism, and* $F_{\mathsf{a}_s} = \bar{F}_{\mathsf{a}}$ *is a finite set of accepting locations. Moreover, the transition function* t_s *is defined as*

- $\forall q_s = (q, \Delta(q))) \in q_{0_s}$,
  - $\mathsf{t}_s((q, \Delta(q)), \tilde{\sigma}_{(q,q')}) = (q, q', \Delta(q'))$ *where* $q' \in \Delta(q)$,
- $\forall q_s = (q, q', \Delta(q')) \in Q_{\ell_s} \backslash (q_{0_s} \cup \bar{F}_{\mathsf{a}})$,
  - $\mathsf{t}_s((q, q', \Delta(q')), \tilde{\sigma}_{(q',q'')}) = (q', q'', \Delta(q''))$, *where* $q, q', q'' \in Q_\ell, q'' \in \Delta(q')$ *and* $q'' \notin \bar{F}_{\mathsf{a}}$,
  - $\mathsf{t}_s((q, q', \Delta(q')), \tilde{\sigma}_{(q',q'')}) = q''$ *where* $q, q', q'' \in Q_\ell$, $q'' \in \Delta(q')$ *and* $q'' \in \bar{F}_{\mathsf{a}}$.

The switching control policy for Problem 4.5.14 is formally defined as

$$\varrho(x, q_{\mathsf{s}}) = \nu_{\bar{\gamma}_{q'_{\mathsf{s}}}}(x), \quad \forall (q_{\mathsf{s}}, \mathsf{L}(x), q'_{\mathsf{s}}) \in \mathsf{t}_{\mathsf{s}}.$$

Running Example (continued.) The DFA $\mathcal{A}_{\mathsf{s}} = \{Q_{\ell_{\mathsf{s}}}, q_{0_{\mathsf{s}}}, \Sigma_{\mathsf{a}_{\mathsf{s}}}, F_{\mathsf{a}_{\mathsf{s}}}, \mathsf{t}_{\mathsf{s}}\}$ modeling the switching mechanism between different control policies of the DFA $\mathcal{A}^c$ in Figure 4.9, is represented in Figure 4.10. ■

Now, we propose our solution to compute a lower bound on the probability that the desired specification is satisfied for Problem 4.5.14.

Theorem 4.5.17. *Consider a specification expressed by the accepting language of DFA* $\mathcal{A}$*, and the DFA* $\mathcal{A}^c$ *as its complement. For every* $\bar{p} \in \mathcal{AP}$*, let* $\mathcal{R}^{\bar{p}}$ *be the set of all accepting state runs and* $\mathcal{P}^{\bar{p}}(\mathsf{q})$ *be the set of state runs of length* 3*. Then the probability that the solution process of* Σ *starting from any initial state* $\xi(0) = x_0 \in \mathsf{L}^{-1}(\bar{p})$ *under the corresponding switching control policy satisfying the specification expressed by* $\mathcal{A}^c$ *over the time horizon* $[0, \mathcal{T}] \subseteq \mathbb{R}_{\geq 0}$ *is upper bounded by*

$$\mathbb{P}^{x_0}_{\varrho}\{\tilde{\sigma}_\xi \models \mathcal{A}^c\} \leq \sum_{q \in \mathcal{R}^{\bar{p}}} \prod_{\aleph \in \mathcal{P}^{\bar{p}}(\mathsf{q})} \{\bar{\delta}_\aleph \,|\, \aleph = (q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})\},$$

where $\bar{\delta}_\aleph$ *is computed via* (4.5.8) *and is the upper bound on the probability that solution processes of* Σ *starting from* $X_0 := \mathsf{L}^{-1}(\tilde{\sigma}(q, q'))$ *reach* $X_u := \mathsf{L}^{-1}(\tilde{\sigma}(q', q''))$ *within the time horizon* $[0, \mathcal{T}] \subseteq \mathbb{R}_{\geq 0}$.

Proof. For $\bar{p} \in \mathcal{AP}$, consider an accepting state run $\mathcal{R}^{\bar{p}}$ and $\mathcal{P}^{\bar{p}}(\mathsf{q})$ as the set of state runs of length 3. For $\aleph = (q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})$, one can verify from Lemma 4.5.15 that the upper bound on the probability that the solution process of Σ starts at $X_0 = \mathsf{L}^{-1}(\tilde{\sigma}(q, q'))$ and reaches $X_u = \mathsf{L}^{-1}(\tilde{\sigma}(q', q''))$ within the time horizon $[0, T] \subseteq \mathbb{R}_{\geq 0}$ under the control input $\nu_\aleph$ is given by $\bar{\delta}_\aleph$. Now the upper bound on the probability that the trace of the solution process reaches the accepting state following the path corresponding to q is given by the product of the probability bounds corresponding to all elements $\aleph = (q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})$:

$$\mathbb{P}\{\tilde{\sigma}(\mathsf{q}) \models \mathcal{A}^c\} \leq \prod_{\aleph \in \mathcal{P}^{\bar{p}}(\mathsf{q})} \{\bar{\delta}_\aleph \,|\, \aleph = (q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})\}.$$

Now one can conclude that the final upper bound on the probability for the solution process of Σ starting from any initial state $\xi(0) = x_0 \in \mathsf{L}^{-1}(p)$ to violate the required specification is essentially the summation of probabilities of all possible accepting state runs of $\mathcal{A}^c$, *i.e.*,

$$\mathbb{P}^{x_0}_{\varrho}\{\tilde{\sigma}_\xi \models \mathcal{A}^c\} \leq \sum_{q \in \mathcal{R}^p} \prod_{\aleph \in \mathcal{P}^{\bar{p}}(\mathsf{q})} \{\bar{\delta}_\aleph \,|\, \aleph = (q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})\}.$$

■

Now the probability that solution processes of Σ starting from any initial state $\xi(0) = x_0 \in \mathsf{L}^{-1}(\bar{p})$ under the the same switching controller satisfy the specification represented by the language of DFA $\mathcal{A}$ is lower bounded by

$$\mathbb{P}^{x_0}_{\varrho}\{\tilde{\sigma}_\xi \models \mathcal{A}\} \geq 1 - \sum_{q \in \mathcal{R}^{\bar{p}}} \prod_{\aleph \in \mathcal{P}^{\bar{p}}(\mathsf{q})} \{\bar{\delta}_\aleph \,|\, \aleph = (q, q', q'') \in \mathcal{P}^{\bar{p}}(\mathsf{q})\}.$$

In the next subsection, we provide systematic methods to compute a CPBC and the corresponding controller for each subsystem.

4.5.3 Computation of CPBC and its Controller

One can utilize Lemma 4.2.14 to reformulate the proposed conditions in Definition 4.5.1 as an SOS optimization problem and provide a systematic approach for computing CPBC and corresponding control policies for subsystems Σ_p. Here, we propose another approach for the computation of CPBC based on counter-example guided inductive synthesis (CEGIS) by employing Satisfiability Modulo Theories (SMT) solvers such as Z3 [DMB08], dReal [GAC12] or MathSat [CGSS13]. In order to present this framework, we require the following assumption.

Assumption 4.5.18. *Each Σ_p has a compact state set X, a compact internal input set W and a finite external input set U. Partition sets $X_i = \mathsf{L}^{-1}(\bar{p}_i)$, $\forall i \in \{0, 1, \ldots, z\}$, are bounded semi-algebraic sets.*

Remark 4.5.19. *The assumption of compactness of the state space $X \subseteq \mathbb{R}^n$ can be supported by considering stopped process $\tilde{\xi} : \Omega \times \mathbb{R}_{\geq 0} \to X$ as*

$$\tilde{\xi}(t) = \begin{cases} \xi(t), & \text{for } t < \tau, \\ \xi(\tau), & \text{for } t \geq \tau, \end{cases}$$

where τ is the first time that the solution process ξ of the subsystem exits from the open set $Int(X)$. Note that in most cases, the infinitesimal generator corresponding to $\tilde{\xi}$ is identical to the one corresponding to ξ over the set $Int(X)$, and is equal to zero outside the set [Kus67]. Hence, the results in Theorem 4.5.4 can be employed for any systems with this assumption.

Now we leverage Assumption 4.5.18 and reformulate conditions (4.5.1)-(4.5.4) as a satisfiability problem as the following lemma.

Lemma 4.5.20. *Consider a ct-SHS-MS* $\Sigma = (X, U, W, \mathcal{U}, \mathcal{W}, P, \mathcal{P}, \hat{f}, \hat{\sigma}, \hat{\rho}, Y, h)$*, fulfilling Assumption 4.5.18. Suppose there exists a function* $\mathcal{B}_p(x)$*, constants* $\gamma_p, \lambda_p, \psi_p \in \mathbb{R}_{\geq 0}$*, and functions* $\alpha_p, \kappa_p \in \mathcal{K}_\infty$*,* $\rho_{\text{int}p} \in \mathcal{K}_\infty \cup \{0\}$*, such that the following expression is true:*

$$\bigwedge_{x\in X} \mathcal{B}_p(x) \geq \alpha_p(\|h(x)\|^2) \bigwedge_{x\in X_0} \mathcal{B}_p(x) \leq \gamma_p \bigwedge_{x\in X_u} \mathcal{B}_p(x) \geq \lambda_p$$

$$\bigwedge_{x\in X} \Big(\bigvee_{\nu\in U} \Big(\bigwedge_{w\in W} \mathcal{L}\mathcal{B}_p(x) + \sum_{p'=1}^{\bar{m}} \tilde{\lambda}_{pp'}(x)\mathcal{B}_{p'}(x) \leq -\kappa_p(\mathcal{B}_p(x)) + \rho_{\text{int}p}(\|w\|^2) + \psi_p \Big) \Big).$$

Then $\mathcal{B}_p(x)$ *satisfies conditions* (4.5.1)-(4.5.4) *in Definition 4.5.1, and accordingly, it is a CPBC.*

4.5.4 Case Study

To show the applicability of our approach to *strongly-connected networks* with *nonlinear dynamics* against complex logic properties, we apply our proposed techniques to a *fully-interconnected* Kuramoto network of 100 *nonlinear* oscillators by compositionally synthesizing hybrid controllers regulating the phase of each oscillator in a comfort zone for a bounded time horizon. Kuramoto oscillator has broad applications in real-life systems such as neural networks, smart grids, automated vehicle coordination, and so on. The model of this case study is adapted from [SA15] by including stochasticity in the model. The dynamic for the interconnection of N-oscillators is presented as

$$\Sigma : \mathsf{d}\theta(t) = (\Omega_{\mathbf{p}(t)} + \frac{K}{N}\varphi(\theta(t)) + \nu(t))\mathsf{d}t + G_{\mathbf{p}(t)}\mathsf{d}\mathbb{W}_t + R_{\mathbf{p}(t)}\mathsf{d}\mathbb{P}_t, \tag{4.5.15}$$

where $\theta = [\theta_1; \ldots; \theta_N]$ is the phase of oscillators with $\theta_i \in [0, 2\pi]$, $i = \{1, \ldots, 100\}$, $\Omega = [\Omega_1; \ldots; \Omega_N] = \bar{\Omega}_{p_i}\mathbb{1}_N$ is the natural frequency of oscillators with $\bar{\Omega}_{p_i} = \begin{cases} 0.1, & \text{if } p_i = 1, \\ 0.12, & \text{if } p_i = 2, \end{cases}$ $K = 0.001$ is the coupling strength, $\varphi(\theta) = [\varphi(\theta_1); \ldots; \varphi(\theta_N)]$ such that $\varphi(\theta_i) = \Sigma_{j=1}^{N} \sin(\theta_j - \theta_i), i \in \{1, \ldots, 100\}$. Moreover, $\nu(t) = [\nu_1(t); \ldots; \nu_N(t)]$, $G = \bar{G}_{p_i}\mathbb{I}_n$ with $\bar{G}_{p_i} = \begin{cases} 0.1, & \text{if } p_i = 1, \\ 0.12, & \text{if } p_i = 2, \end{cases}$ and $R = \bar{R}_{p_i}\mathbb{I}_n$ with $\bar{R}_{p_i} = \begin{cases} 0.1, & \text{if } p_i = 1, \\ 0.12, & \text{if } p_i = 2. \end{cases}$ We consider rates of Poisson processes as $\bar{\lambda}_i = 0.1, \forall i \in \{1, \ldots, 100\}$. Now by introducing subsystems $\Sigma_i, i \in \{1, \ldots, 100\}$, described by

$$\Sigma_i : \begin{cases} \mathsf{d}\theta_i(t) = (\bar{\Omega}_{i\mathbf{p}_i(t)} + \frac{K}{N}\sum_{j=1, i\neq j}^{N} \sin(w_{ij}(t) - \theta_i(t)) + \nu_{ip_i}(t))\mathsf{d}t + \bar{G}_{ip_i}\mathsf{d}\mathbb{W}_{t_i} + \bar{R}_{ip_i}\mathsf{d}\mathbb{P}_{t_i}, \\ \zeta_i(t) = \theta_i(t), \end{cases}$$

one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ where $w_{ij}(t) = \theta_j(t)$.

Transition rates for switching between two modes $P = \{1, 2\}$ are given as $\tilde{\lambda}_{11_i} = -0.9, \tilde{\lambda}_{12_i} = 0.9, \tilde{\lambda}_{21_i} = 0.8, \tilde{\lambda}_{22_i} = -0.8, \forall i \in \{1, \ldots, 100\}$. In addition, the regions of interest are $X^0 = [0, \frac{\pi}{16}]^N, X^1 = [\frac{5.8\pi}{12}, \frac{6.2\pi}{12}]^N, X^2 = [\frac{5.7\pi}{6}, \pi]^N, X^3 = [\pi, \frac{6.2\pi}{6}]^N, X^4 = [\frac{17.8\pi}{12}, \frac{18.2\pi}{12}]^N, X^5 = [\frac{11.8\pi}{6}, 2\pi]^N$ and $X^6 = X \backslash (X^0 \cup X^1 \cup X^2 \cup X^3 \cup X^4 \cup X^5)$. Each of these regions is associated with atomic propositions given by $\mathcal{AP} = \{\bar{p}_0, \bar{p}_1, \bar{p}_2, \bar{p}_3, \bar{p}_4, \bar{p}_5, \bar{p}_6\}$

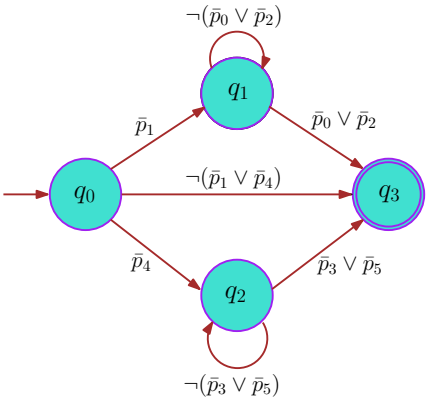

Figure 4.11: DFA $\mathcal{A}^c$ of the complement of specification.

such that the labeling function $\mathsf{L}(x_z) = \bar{p}_z$, $\forall x_z \in X^z, z = \{0, \dots, 6\}$. The objective is to compute a controller such that if the state of the system starts from X^1, it always stays away from X^0 and X^2, and if it starts from X^4, it always stays away from X^3 and X^5 within the time horizon $[0, \mathcal{T}]$. Such a specification can be represented as an LTL specification given by $(\bar{p}_1 \wedge \Box\neg(\bar{p}_0 \vee \bar{p}_2)) \vee (\bar{p}_4 \wedge \Box\neg(\bar{p}_3 \vee \bar{p}_5))$ associated with time horizon $\mathcal{T} = 5$. The specification can also be represented by accepting language $\mathbb{L}(\mathcal{A})$ of a DFA $\mathcal{A}$. Fig. 4.11 represents the complement DFA $\mathcal{A}^c$.

We decompose the complement of our specification into simple reachability tasks. We consider accepting state runs without self-loops with $\mathcal{T} = 5$. The DFA $\mathcal{A}^c$ has three such accepting state runs $\mathcal{R} = \{(q_0, q_3), (q_0, q_1, q_3), (q_0, q_2, q_3)\}$. The sets $\mathcal{P}^{\bar{p}}(\mathsf{q})$ can be obtained for each of these accepting state runs as $\mathcal{P}^{\bar{p}_1}(q_0, q_1, q_3) = \{(q_0, q_1, q_3)\}$, and $\mathcal{P}^{\bar{p}_4}(q_0, q_2, q_3) = \{(q_0, q_2, q_3)\}$. Note that since (q_0, q_3) is a state run of a length 2 and admits the trivial probability, it is not considered. Accordingly, we need to find control policies and control barrier certificates for only two reachability elements. To do so, we utilize the SOS algorithm proposed in Lemma 4.2.14 by employing SOSTOOLS and SDP solver SeDuMi. Note that since the dynamics of the system Σ in (4.5.15) are non-polynomial and SOS algorithm is only specialized for polynomial dynamics, we first make an approximation to our dynamics. In particular, we take an upper bound on the term $\mathcal{LB}_{ip_i}(\theta_i)$ by replacing the $sin(\cdot)$ terms with either 1 or -1.

For the reachability element (q_0, q_1, q_3) with $X_{0_i} = [\frac{5.8\pi}{12}, \frac{6.2\pi}{12}]$ and $X_{u_i} = [0, \frac{\pi}{16}] \cup [\frac{5.7\pi}{6}, \pi], i \in \{1, \dots, 100\}$, we compute CPBC of an order 6 as $\mathcal{B}_{ip_i}(\theta_i) = 85\theta_i^6 - 310\theta_i^5 + 8.9\theta_i^4 - 36\theta_i^3 + 4791\theta_i^2 - 1038\theta_i + 6245$ and the corresponding switching controller $\nu_{ip_i} = -5356\theta_i + 7000$ for $p_i = 1$, and $\mathcal{B}_{ip_i}(\theta_i) = 84\theta_i^6 - 308\theta_i^5 + 2.8\theta_i^4 - 9.5\theta_i^3 + 4756\theta_i^2 - 10400\theta_i + 6286$ together with $\nu_{ip_i} = -4229\theta_i + 5000$ for $p_i = 2, \forall i \in \{1, \dots, 100\}$. Moreover, the corresponding constants and functions in Definition 4.5.1 satisfying conditions (4.5.1)-(4.5.4) are quantified as $\gamma_{ip_i} = 3, \lambda_{ip_i} = 4300, \psi_{ip_i} = 50, \kappa_{ip_i}(s) = 5 \times 10^{-5}s, \alpha_{ip_i}(s) = 0.8\sqrt{s}, \rho_{\text{int}ip_i}(s) = 4 \times 10^{-7}\sqrt{s}, \forall s \in \mathbb{R}_{\geq 0}$ for $p_i = 1$; and $\gamma_{ip_i} = 3.2, \lambda_{ip_i} = 4400, \psi_{ip_i} = 52, \kappa_{ip_i}(s) = 53 \times 10^{-6}s, \alpha_{ip_i}(s) = 0.85\sqrt{s}, \rho_{\text{int}ip_i}(s) = 4.2 \times 10^{-7}\sqrt{s}, \forall s \in \mathbb{R}_{\geq 0}$ for $p_i = 2, \forall i \in \{1, \dots, 100\}$. We now proceed with Theorem 4.5.8 to construct a CBC for the interconnected system using CPBC of subsystems. One can readily verify that the

small-gain Assumption 4.5.7 holds with $\hat{\gamma}_i(s) = s, \forall s \in \mathbb{R}_{\geq 0}, \hat{\lambda}_i = \min_{p_i \in P_i}\{\hat{\lambda}_{ip_i}\} = 5 \times 10^{-5}$, $\hat{\delta}_{ij} = \max_{p_i \in P_i}\{\delta_{ijp_i}\} = 5 \times 10^{-7}$. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, 100\}$, the spectral radius of $\Lambda^{-1}\Delta$ is computed as 0.99 which is strictly less that one (cf. Remark 4.2.11), and consequently the compositionality condition (4.5.11) is satisfied. Moreover, the compositionality condition (4.5.12) is also met since $\min_{p_i \in P_i}\{\lambda_{ip_i}\} > \max_{p_i \in P_i}\{\gamma_{ip_i}\}, \forall i \in \{1, \ldots, 100\}$. Then by employing the results of Theorem 4.5.8, one can conclude that $\mathcal{B}(\theta, p) := \sum_{i=1}^{100} \mathcal{B}_{ip_i}(\theta_i)$ is a CBC for the interconnected system Σ with $\gamma = \sum_{i=1}^{100} \max_{p_i \in P_i}\{\gamma_{ip_i}\} = 320, \lambda = \sum_{i=1}^{100} \min_{p_i \in P_i}\{\lambda_{ip_i}\} = 43 \times 10^4, \kappa(s) = 5 \times 10^{-7}s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = \sum_{i=1}^{100} \max_{p_i \in P_i}\{\psi_{ip_i}\} = 5200$. By employing Theorem 4.5.4, one can guarantee that the state of the interconnected system Σ starts from the initial set $X_0 = X^1$ and never reaches $X_u = X^0 \cup X^2$ during the time horizon $\mathcal{T} = 5$ with the probability of at least 94%, *i.e.,*

$$\mathbb{P}_{\varrho}^{x_0}\{\tilde{\sigma}_\xi \models \mathcal{A}\} \geq 0.94. \tag{4.5.16}$$

Similarly, for the reachability element (q_0, q_2, q_3) with $X_{0_i} = [\frac{17.8\pi}{12}, \frac{18.2\pi}{12}]$ and $X_{u_i} = [\pi, \frac{6.2\pi}{6}] \cup [\frac{11.8\pi}{6}, 2\pi], i \in \{1, \ldots, 100\}$, we compute CPBC of an order 6 as $\mathcal{B}_{ip_i}(\theta_i) = 0.2\theta_i^6 - 0.028\theta_i^5 + 6.7\theta_i^4 - 1.1\theta_i^3 + 20\theta_i^2 - 6365\theta_i + 24559$ and the corresponding hybrid controller $\nu_{ip_i} = -1733\theta_i + 6900$ for $p_i = 1$, and $\mathcal{B}_{ip_i}(\theta_i) = 0.11\theta_i^6 - 0.038\theta_i^5 + 8.7\theta_i^4 - 5.5\theta_i^3 + 21\theta_i^2 - 5801\theta_i + 22215$ together with $\nu_{ip_i} = -1678\theta_i + 21870$ for $p_i = 2, \forall i \in \{1, \ldots, 100\}$. Moreover, the corresponding constants and functions in Definition 4.5.1 satisfying conditions (4.5.1)-(4.5.4) are synthesized as $\gamma_{ip_i} = 300, \lambda_{ip_i} = 5000, \psi_{ip_i} = 64, \kappa_{ip_i}(s) = 5 \times 10^{-5}s, \alpha_{ip_i}(s) = 0.8\sqrt{s}, \rho_{\text{int}ip_i}(s) = 4 \times 10^{-7}\sqrt{s}, \forall s \in \mathbb{R}_{\geq 0}$ for $p_i = 1$; and $\gamma_{ip_i} = 340, \lambda_{ip_i} = 4500, \psi_{ip_i} = 66, \kappa_{ip_i}(s) = 51 \times 10^{-6}s, \alpha_{ip_i}(s) = 0.82\sqrt{s}, \rho_{\text{int}ip_i}(s) = 4.1 \times 10^{-7}\sqrt{s}, \forall s \in \mathbb{R}_{\geq 0}$ for $p_i = 2, \forall i \in \{1, \ldots, 100\}$. We now proceed with Theorem 4.5.8 to construct a CBC for the interconnected system using CPBC of subsystems. One can readily verify that the small-gain Assumption 4.5.7 holds with $\hat{\gamma}_i(s) = s, \forall s \in \mathbb{R}_{\geq 0}, \hat{\lambda}_i = \min_{p_i \in P_i}\{\hat{\lambda}_{ip_i}\} = 5 \times 10^{-5}$, $\hat{\delta}_{ij} = \max_{p_i \in P_i}\{\delta_{ijp_i}\} = 5 \times 10^{-7}$. By selecting $\mu_i = 1, \forall i \in \{1, \ldots, 100\}$, the spectral radius of $\Lambda^{-1}\Delta$ is computed as 0.99 which is strictly less that one, and consequently the compositionality condition (4.5.11) is satisfied. Moreover, the compositionality condition (4.5.12) is also met since $\min_{p_i \in P_i}\{\lambda_{ip_i}\} > \max_{p_i \in P_i}\{\gamma_{ip_i}\}, \forall i \in \{1, \ldots, 100\}$. Then by employing the results of Theorem 4.5.8, one can conclude that $\mathcal{B}(\theta, p) := \sum_{i=1}^{100} \mathcal{B}_{ip_i}(\theta_i)$ is a CBC for the interconnected system Σ with $\gamma = \sum_{i=1}^{100} \max_{p_i \in P_i}\{\gamma_{ip_i}\} = 34000, \lambda = \sum_{i=1}^{100} \min_{p_i \in P_i}\{\lambda_{ip_i}\} = 45 \times 10^4, \kappa(s) = 5 \times 10^{-7}s, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = \sum_{i=1}^{100} \max_{p_i \in P_i}\{\psi_{ip_i}\} = 6400$. By employing Theorem 4.5.4, one can guarantee that the state of the interconnected system Σ starts from the initial set $X_0 = X^4$ and never reaches $X_u = X^3 \cup X^5$ during the time horizon $\mathcal{T} = 5$ with the probability of at least 86%, *i.e.,*

$$\mathbb{P}_{\varrho}^{x_0}\{\tilde{\sigma}_\xi \models \mathcal{A}\} \geq 0.86. \tag{4.5.17}$$

The switching mechanism for controllers is shown in Figure 4.12. Closed-loop state trajectories of a representative oscillator with 10 different noise realizations starting from initial regions X^1 and X^4 are illustrated in Figure 4.13. The required computation time and memory usage for computing the CPBC and its corresponding controller for the

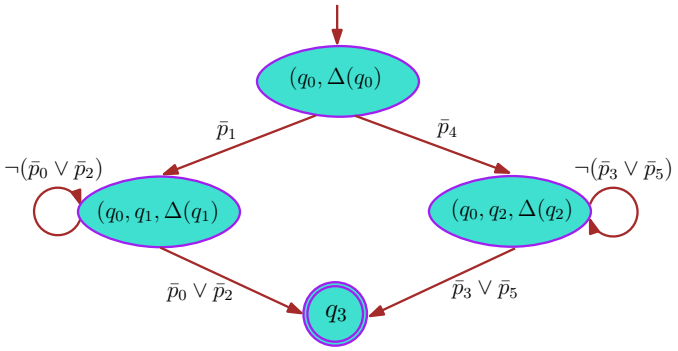

Figure 4.12: Switching mechanism for controllers.

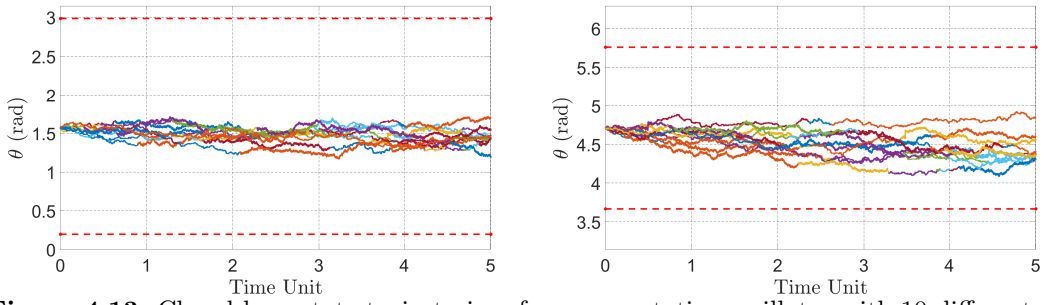

Figure 4.13: Closed-loop state trajectories of a representative oscillator with 10 different noise realizations in a network of 100 oscillators with initial state starting from (left) Region X^1, and (right) Region X^4. Changed colours in each trajectory show that the mode is switched to the other one.

reachability element (q_0, q_1, q_3) are respectively 1.8 minutes and 23 MB, and for the reachability element (q_0, q_2, q_3) are respectively 1.7 minutes and 21 MB on a machine with Windows operating system (Intel i7@3.6GHz CPU and 16 GB of RAM). Note that if one employs our designed controllers and run Monte Carlo simulations on top of the closed-loop system, the empirical probabilities are much better than the ones we proposed in (4.5.16), (4.5.17). However, this issue is expected and the reason is due to the conservatism nature of using polynomial barrier certificates with a fix degree, but with the gain of providing a formal lower bound on the probability of satisfaction for safety specification rather than an empirical one.

4.6 Compositional Construction of Control Barrier Certificates for dt-SS with Dwell-time Conditions

In this section, we propose a compositional framework for the construction of control barrier certificates for discrete-time stochastic switched systems accepting *multiple* control barrier certificates with some *dwell-time* conditions as in Definition 2.6.1. Switching signals here are control inputs and the main goal is to synthesize them with a specific dwell-time such that outputs of original systems satisfy some high-level specifications

such as safety, reachability, etc. To do so, we first provide an augmented framework for presenting each switched subsystem with several modes with a single system covering all modes (called augmented switched systems) whose output trajectories are exactly the same as those of original switched systems. We then compositionally construct *augmented control barrier certificates* for interconnected augmented systems based on so-called *augmented pseudo-barrier certificates* of subsystems by leveraging some max-type small-gain conditions. Given the constructed augmented barrier certificates, we quantify upper bounds on the probability that interconnected systems reach certain unsafe regions in a finite time horizon.

4.6.1 Augmented Stochastic Switched Systems

Here, given a dt-SS Σ, we introduce a notion of augmented dt-SS as in the next definition. Note that this notion is adapted from the definition of labeled transition systems defined in [BK08] and modified to capture the stochastic nature of the system. This provides an alternative description of switched systems enabling us to represent a switched system with a finite set of modes via an augmented system covering the whole modes.

Definition 4.6.1. *Given a dt-SS $\Sigma = (X, P, \mathcal{P}, W, \varsigma, F, Y, h)$, we define the associated augmented dt-SS $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \mathbb{W}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$, where:*

- $\mathbb{X} = X \times P \times \{0, \ldots, k_d - 1\}$ *is the set of states. A state $(x, p, l) \in \mathbb{X}$ means that the current state of Σ is x, the current value of the switching signal is p, and the time elapsed since the latest switching time instant upper bounded by k_d is l;*
- $\mathbb{P} = P$ *is the set of external inputs;*
- $\mathbb{W} = W$ *is the set of internal inputs;*
- ς *is a sequence of i.i.d. random variables;*
- $\mathbb{F} : \mathbb{X} \times \mathbb{P} \times \mathbb{W} \times V_\varsigma \to \mathbb{X}$ *is the one-step transition function given by $(x', p', l') = \mathbb{F}((x, p, l), p, w, \varsigma)$ if and only if $x' = f_p(x, w, \varsigma)$ and the following scenarios hold:*
  - *$l < k_d - 1, p' = p$, and $l' = l + 1$: switching is not allowed because the time elapsed since the latest switch is strictly smaller than the dwell-time;*
  - *$l = k_d - 1, p' = p$, and $l' = k_d - 1$: switching is allowed but no switch occurs;*
  - *$l = k_d - 1, p' \neq p$, and $l' = 0$: switching is allowed and a switch occurs;*
- $\mathbb{Y} = Y$ *is the output set;*
- $\mathbb{H} : \mathbb{X} \to \mathbb{Y}$ *is the output map defined as $\mathbb{H}(x, p, l) = h(x)$.*

We associate to $\mathbb{P}$ and $\mathbb{W}$, respectively, the sets P and W to be collections of sequences $\{p(k) : \Omega \to \mathbb{P},\ k \in \mathbb{N}\}$ and $\{w(k) : \Omega \to \mathbb{W},\ k \in \mathbb{N}\}$, in which $p(k)$ and $w(k)$ are independent of $\varsigma(z)$ for any $k, z \in \mathbb{N}$ and $z \geq k$. We also denote initial conditions of p and l by p_0 and $l_0 = 0$.

Remark 4.6.2. *Note that in the augmented dt-SS $\mathbb{A}(\Sigma)$ in Definition 4.6.1, we added two additional variables p and l to the state tuple of the system Σ, in which l is a counter that depending on its value allows or prevents the system from switching, and p acts as a memory to record the latest mode.*

Proposition 4.6.3. *The output trajectory of the augmented dt-SS $\mathbb{A}(\Sigma)$ in Definition 4.6.1 can be uniquely mapped to an output trajectory of the switched system Σ defined in* (2.6.1)*, and vice versa.*

The proof is similar to that of [LSZ20a, Proposition 2.9] and is omitted here.

In the next subsection, in order to quantify upper bounds on the probability that the interconnected system reaches a certain unsafe region in a finite time horizon, we first introduce notions of augmented control pseudo-barrier and barrier certificates for, respectively, augmented dt-SS (with both internal and external signals) and interconnected augmented dt-SS (without internal signals).

4.6.2 Augmented Control (Pseudo-)Barrier Certificates

Here, we first introduce a notion of augmented control pseudo-barrier certificates for augmented dt-SS with both internal and external inputs.

Definition 4.6.4. *Consider an augmented dt-SS $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \mathbb{W}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$, and initial and unsafe sets $X_0, X_u \subseteq X$ for the dt-SS Σ. Let us define $\mathbb{X}_0 = X_0 \times P \times \{0\}$, $\mathbb{X}_u = X_u \times P \times \{0, \ldots, k_d - 1\}$, as initial and unsafe sets of the augmented system, respectively. A function $\mathcal{B} : \mathbb{X} \to \mathbb{R}_{\geq 0}$ is called an augmented control pseudo-barrier certificate (APBC) for $\mathbb{A}(\Sigma)$ if there exist functions $\alpha \in \mathcal{K}_\infty$, $\rho_{\text{int}} \in \mathcal{K}_\infty \cup \{0\}$, and constants $0 < \kappa < 1$, $\gamma, \psi \in \mathbb{R}_{\geq 0}$ and $\lambda \in \mathbb{R}_{>0}$, such that*

$$\mathcal{B}(x,p,l) \geq \alpha(\|\mathbb{H}(x,p,l)\|_\infty), \qquad \forall (x,p,l) \in \mathbb{X}, \tag{4.6.1}$$

$$\mathcal{B}(x,p,l) \leq \gamma, \qquad \forall (x,p,l) \in \mathbb{X}_0, \tag{4.6.2}$$

$$\mathcal{B}(x,p,l) \geq \lambda, \qquad \forall (x,p,l) \in \mathbb{X}_u, \tag{4.6.3}$$

and $\forall (x,p,l) \in \mathbb{X}$, $\exists p' \in \mathbb{P}$, such that $\forall w \in \mathbb{W}$, one has $(x',p',l') = \mathbb{F}((x,p,l),p,w,\varsigma)$, and

$$\mathbb{E}\Big[\mathcal{B}((x',p',l')) \,\Big|\, x,p,l,w\Big] \leq \max\Big\{\kappa\mathcal{B}(x,p,l), \rho_{\text{int}}(\|w\|_\infty), \psi\Big\}, \tag{4.6.4}$$

where the expectation operator $\mathbb{E}$ is with respect to ς under the one-step transition of the augmented dt-SS $\mathbb{A}(\Sigma)$.

Now, we modify the above notion for augmented dt-SS without internal inputs by eliminating all the terms related to w which will be employed later for providing probabilistic safety certificates over interconnected augmented switched systems.

Definition 4.6.5. *Consider an (interconnected) augmented dt-SS $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$ without internal inputs, with initial and unsafe sets $X_0, X_u \subseteq X$ for the dt-SS Σ. Let us*

define sets $\mathbb{X}_0, \mathbb{X}_u \subseteq \mathbb{X}$ *as, respectively, initial and unsafe sets of the augmented system. A function* $\mathcal{B} : \mathbb{X} \to \mathbb{R}_{\geq 0}$ *is called an augmented control barrier certificate (ABC) for* $\mathbb{A}(\Sigma)$ *if*

$$\mathcal{B}(x,p,l) \leq \gamma, \qquad \forall (x,p,l) \in \mathbb{X}_0, \tag{4.6.5}$$

$$\mathcal{B}(x,p,l) \geq \lambda, \qquad \forall (x,p,l) \in \mathbb{X}_u, \tag{4.6.6}$$

and $\forall (x,p,l) \in \mathbb{X}, \exists p' \in \mathbb{P}$*, such that one has* $(x',p',l') = \mathbb{F}\left((x,p,l),p,\varsigma\right)$*, and*

$$\mathbb{E}\Big[\mathcal{B}((x',p',l')) \,\big|\, x,p,l\Big] \leq \max\Big\{\kappa\mathcal{B}(x,p,l),\psi\Big\}, \tag{4.6.7}$$

for some constants $0 < \kappa < 1$*,* $\gamma, \psi \in \mathbb{R}_{\geq 0}$ *and* $\lambda \in \mathbb{R}_{>0}$ *with* $\gamma < \lambda$*, where the expectation operator* $\mathbb{E}$ *is with respect to* ς *under the one-step transition of the augmented dt-SS* $\mathbb{A}(\Sigma)$*.*

We now employ Definition 4.6.5 and propose an upper bound on the probability that an (interconnected) augmented dt-SS reaches an unsafe region via the next theorem.

Theorem 4.6.6. *Let* $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$ *be an (interconnected) augmented dt-SS without internal inputs. Suppose* $\mathcal{B}$ *is an ABC for* $\mathbb{A}(\Sigma)$*. Then for any random variable* a *as the initial state, any initial mode* p_0*, and* $l_0 = 0$ *as the initial counter, the probability that the interconnected augmented dt-SS reaches an unsafe set* $\mathbb{X}_u$ *within the time step* $k \in [0, \mathcal{T}]$ *is upper bounded by*

$$\mathbb{P}\Big\{\sup_{0\leq k\leq \mathcal{T}} \mathcal{B}(x(k),p(k),l(k)) \geq \lambda \;\big|\; a,p_0,l_0\Big\} \leq \begin{cases} 1-(1-\frac{\gamma}{\lambda})(1-\frac{\psi}{\lambda})^{\mathcal{T}}, & \text{if } \lambda \geq \frac{\psi}{1-\kappa}, \\ (\frac{\gamma}{\lambda})\kappa^{\mathcal{T}} + (\frac{\psi}{(1-\kappa)\lambda})(1-\kappa^{\mathcal{T}}), & \text{if } \lambda < \frac{\psi}{1-\kappa}. \end{cases} \tag{4.6.8}$$

Proof. According to condition (4.6.6), $\mathbb{X}_u \subseteq \{(x,p,l) \in \mathbb{X} \;\big|\; \mathcal{B}(x,p,l) \geq \lambda\}$. Then we have

$$\begin{aligned} &\mathbb{P}\Big\{(x(k),p(k),l(k)) \in \mathbb{X}_u \text{ for } 0 \leq k \leq \mathcal{T} \;\big|\; a,p_0,l_0\Big\} \\ &\quad\leq \mathbb{P}\Big\{\sup_{0\leq k\leq \mathcal{T}} \mathcal{B}(x(k),p(k),l(k)) \geq \lambda \;\big|\; a,p_0,l_0\Big\}. \end{aligned} \tag{4.6.9}$$

The proposed bounds in (4.6.8) follows directly by applying [Kus67, Theorem 3, Chapter III] to (4.6.9) (but adapted to stochastic switched systems) and employing respectively conditions (4.6.7) and (4.6.5). ■

4.6.3 Compositional Construction of ABC

Here, we analyze networks of stochastic switched subsystems by driving a max-type small-gain condition and discuss how to construct an ABC of the augmented dt-SS via the corresponding APBC of subsystems. Suppose we are given N stochastic switched subsystems

$$\Sigma_i = (X_i, P_i, \mathcal{P}_i, W_i, \varsigma_i, F_i, Y_i, h_i),\ i \in \{1,\ldots,N\},$$

where $F_i = \{f_1^i, \ldots, f_{m_i}^i\}$, with its *equivalent* augmented dt-SS $\mathbb{A}(\Sigma_i) = (\mathbb{X}_i, \mathbb{P}_i, \mathbb{W}_i, \varsigma_i, \mathbb{F}_i, \mathbb{Y}_i, \mathbb{H}_i)$, in which their internal inputs and outputs are partitioned as in (3.3.9)-(3.3.10). We now define a notion of the *interconnection* for augmented dt-SS $\mathbb{A}(\Sigma_i) = (\mathbb{X}_i, \mathbb{P}_i, \mathbb{W}_i, \varsigma_i, \mathbb{F}_i, \mathbb{Y}_i, \mathbb{H}_i)$.

Definition 4.6.7. *Consider $N \in \mathbb{N}_{\geq 1}$ augmented dt-SS $\mathbb{A}(\Sigma_i) = (\mathbb{X}_i, \mathbb{P}_i, \mathbb{W}_i, \varsigma_i, \mathbb{F}_i, \mathbb{Y}_i, \mathbb{H}_i)$, with the input-output configuration as in* (3.3.9)-(3.3.10)*. The interconnection of $\mathbb{A}(\Sigma_i)$, $\forall i \in \{1, \ldots, N\}$, is the interconnected augmented dt-SS $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$, denoted by $\mathcal{I}(\mathbb{A}(\Sigma_1), \ldots, \mathbb{A}(\Sigma_N))$, such that $\mathbb{X} := \prod_{i=1}^N \mathbb{X}_i$, $\mathbb{P} := \prod_{i=1}^N \mathbb{P}_i$, $\mathbb{Y} := \prod_{i=1}^N \mathbb{Y}_{ii}$, $\mathbb{H} = \prod_{i=1}^N \mathbb{H}_{ii}$, and the map $\mathbb{F} = \prod_{i=1}^N \mathbb{F}_i$ is the transition function given by $(x', p', l') = \mathbb{F}((x, p, l), p, \varsigma)$ if and only if $x' = f_p(x, w, \varsigma)$, where $f_p = \prod_{i=1}^N f_{p_i}^i$, and the following scenarios hold for any $i \in \{1, \ldots, N\}$:*

- *$l_i < k_{d_i} - 1$, $p_i' = p_i$, and $l_i' = l_i + 1$;*
- *$l_i = k_{d_i} - 1$, $p_i' = p_i$, and $l_i' = k_{d_i} - 1$;*
- *$l_i = k_{d_i} - 1$, $p_i' \neq p_i$, and $l_i' = 0$;*

where $x = [x_1; \ldots; x_N], p = [p_1; \ldots; p_N], l = [l_1; \ldots; l_N], \varsigma = [\varsigma_1; \ldots; \varsigma_N]$, and subjected to the following constraint:

$$\forall i, j \in \{1, \ldots, N\}, i \neq j: \qquad w_{ji} = y_{ij}, \quad \mathbb{Y}_{ij} \subseteq \mathbb{W}_{ji}.$$

Assume for the augmented dt-SS $\mathbb{A}(\Sigma_i) = (\mathbb{X}_i, \mathbb{P}_i, \mathbb{W}_i, \varsigma_i, \mathbb{F}_i, \mathbb{Y}_i, \mathbb{H}_i), i \in \{1, \ldots, N\}$, there exists an APBC $\mathcal{B}_i$ with the corresponding functions and constants denoted by $\alpha_i, \rho_{\text{int}i}, \kappa_i, \gamma_i, \lambda_i$ and ψ_i as in Definition 4.6.4. Now we raise the following max-type small-gain assumption to establish the main compositionality result of the paper.

Assumption 4.6.8. *Assume that $\mathcal{K}_\infty$ functions κ_{ij} defined as*

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

satisfy

$$\kappa_{i_1 i_2} \circ \kappa_{i_2 i_3} \circ \cdots \circ \kappa_{i_{r-1} i_r} \circ \kappa_{i_r i_1} < \mathcal{I}_d, \tag{4.6.10}$$

for all sequences $(i_1, \ldots, i_r) \in \{1, \ldots, N\}^r$ and $r \in \{1, \ldots, N\}$.

The small-gain condition (4.6.10) implies the existence of $\mathcal{K}_\infty$ functions $\bar{\sigma}_i > 0$ [Rüf10, Theorem 5.5] satisfying condition (3.3.13).

In the next theorem, we show that if Assumption 4.6.8 holds and $\max_i \bar{\sigma}_i^{-1}$ is concave (in order to employ Jensen's inequality), then we can construct an ABC of $\mathbb{A}(\Sigma)$ using the APBC of $\mathbb{A}(\Sigma_i)$.

Theorem 4.6.9. *Consider an interconnected augmented dt-SS* $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$ *induced by* $N \in \mathbb{N}_{\geq 1}$ *augmented dt-SS* $\mathbb{A}(\Sigma_i)$*. Suppose that each* $\mathbb{A}(\Sigma_i)$ *admits an APBC* $\mathcal{B}_i$ *as defined in Definition 4.6.4. If Assumption 4.6.8 holds and*

$$\max_i \left\{\bar{\sigma}_i^{-1}(\lambda_i)\right\} > \max_i \left\{\bar{\sigma}_i^{-1}(\gamma_i)\right\}, \tag{4.6.11}$$

then $\mathcal{B}(x, p, l)$ *defined as*

$$\mathcal{B}(x, p, l) := \max_i \left\{\bar{\sigma}_i^{-1}(\mathcal{B}_i(x_i, p_i, l_i))\right\}, \tag{4.6.12}$$

is an ABC for the interconnected augmented dt-SS $\mathcal{I}(\mathbb{A}(\Sigma_1), \ldots, \mathbb{A}(\Sigma_N))$ *provided that* $\max_i \bar{\sigma}_i^{-1}$ *for* $\bar{\sigma}_i$ *as in* (3.3.13) *is concave.*

Proof. We first show that conditions (4.6.5) and (4.6.6) in Definition 4.6.5 hold. For any $(x, p, l) \in \mathbb{X}_0 = \prod_{i=0}^{N} \mathbb{X}_{0_i}$ and from (4.6.2), we have

$$\mathcal{B}(x, p, l) = \max_i \left\{\bar{\sigma}_i^{-1}(\mathcal{B}_i(x_i, p_i, l_i))\right\} \leq \max_i \left\{\bar{\sigma}_i^{-1}(\gamma_i)\right\} = \gamma,$$

and similarly for any $(x, p, l) \in \mathbb{X}_u = \prod_{i=1}^{N} \mathbb{X}_{u_i}$ and from (4.6.3), one has

$$\mathcal{B}(x, p, l) = \max_i \left\{\bar{\sigma}_i^{-1}(\mathcal{B}_i(x_i, p_i, l_i))\right\} \geq \max_i \left\{\bar{\sigma}_i^{-1}(\lambda_i)\right\} = \lambda,$$

satisfying conditions (4.6.5) and (4.6.6) with $\gamma = \max_i \left\{\bar{\sigma}_i^{-1}(\gamma_i)\right\}$ and $\lambda = \max_i \left\{\bar{\sigma}_i^{-1}(\lambda_i)\right\}$.

Now we show that condition (4.6.7) holds, as well. Let $\kappa(s) = \max_{i,j}\{\bar{\sigma}_i^{-1} \circ \kappa_{ij} \circ \bar{\sigma}_j(s)\}$. It follows from (3.3.13) that $\kappa < \mathcal{I}_d$. Moreover, $\lambda > \gamma$ according to (4.6.11). Since $\max_i \bar{\sigma}_i^{-1}$ is concave, one can readily acquire the chain of inequalities in (4.6.13) using Jensen's inequality, and by defining the constant ψ as

$$\psi := \max_i \bar{\sigma}_i^{-1}(\psi_i).$$

Hence $\mathcal{B}(x, p, l)$ is an ABC for the interconnected augmented dt-SS $\mathcal{I}(\mathbb{A}(\Sigma_1), \ldots, \mathbb{A}(\Sigma_N))$, which completes the proof. ■

4.6.4 Construction of APBC

Here, we impose conditions on dt-SS Σ_p enabling us to find an APBC for $\mathbb{A}(\Sigma)$. The APBC for the augmented dt-SS $\mathbb{A}(\Sigma)$ is established under the assumption that the given dt-SS Σ_p has max-type control barrier certificates for all modes as in the following definition.

Definition 4.6.10. *Consider a dt-SS* Σ_p*, and sets* $X_0, X_u \subseteq X$ *as initial and unsafe sets of the given dt-SS, respectively. A function* $\mathcal{B}_p : X \to \mathbb{R}_{\geq 0}$ *is said to be a* max*-type control barrier certificate (*max*-type CBC) for* Σ_p *if there exist functions* $\alpha_p \in \mathcal{K}_\infty$*,*

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{B}(x',p',l') \,\big|\, x,p,l\Big] = \mathbb{E}\Big[\max_i \Big\{\bar{\sigma}_i^{-1}(\mathcal{B}_i(x_i',p_i',l_i'))\Big\} \,\big|\, x,p,l\Big] \\
&\leq \max_i \Big\{\bar{\sigma}_i^{-1}(\mathbb{E}\Big[\mathcal{B}_i(x_i',p_i',l_i') \,\big|\, x,p,l\Big])\Big\} = \max_i \Big\{\bar{\sigma}_i^{-1}(\mathbb{E}\Big[\mathcal{B}_i(x_i',p_i',l_i') \,\big|\, x_i,p_i,l_i\Big])\Big\} \\
&\leq \max_i \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i\mathcal{B}_i(x_i,p_i,l_i), \rho_{\text{int}i}(\|w_i\|_\infty), \psi_i\})\Big\} \\
&= \max_i \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i\mathcal{B}_i(x_i,p_i,l_i), \rho_{\text{int}i}(\max_{j,j\neq i}\{\|w_{ij}\|_\infty\}), \psi_i\})\Big\} \\
&= \max_i \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i\mathcal{B}_i(x_i,p_i,l_i), \rho_{\text{int}i}(\max_{j,j\neq i}\{\|y_{ji}\|_\infty\}), \psi_i\})\Big\} \\
&\leq \max_i \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i\mathcal{B}_i(x_i,p_i,l_i), \rho_{\text{int}i}(\max_{j,j\neq i}\{\|\mathbb{H}_j(x_j,p_j,l_j)\|_\infty\}), \psi_i\})\Big\} \\
&\leq \max_i \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_i\mathcal{B}_i(x_i,p_i,l_i), \rho_{\text{int}i}(\max_{j,j\neq i}\{\alpha_j^{-1}(\mathcal{B}_j(x_j,p_j,l_j))\}), \psi_i\})\Big\} \\
&= \max_{i,j} \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}\mathcal{B}_j(x_j,p_j,l_j), \psi_i\})\Big\} \\
&= \max_{i,j} \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}\circ\bar{\sigma}_j\circ\bar{\sigma}_j^{-1}(\mathcal{B}_j(x_j,p_j,l_j)), \psi_i\})\Big\} \\
&\leq \max_{i,j,z} \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}\circ\sigma_j\circ\bar{\sigma}_z^{-1}(\mathcal{B}_z(x_z,p_z,l_z)), \psi_i\})\Big\} \\
&= \max_{i,j} \Big\{\bar{\sigma}_i^{-1}(\max\{\kappa_{ij}\circ\bar{\sigma}_j(\mathcal{B}(x,p,l)), \psi_i\})\Big\} = \max\Big\{\kappa\mathcal{B}(x,p,l), \psi\Big\}. \qquad (4.6.13)
\end{aligned}
$$

$\rho_{\text{int}p} \in \mathcal{K}_\infty \cup \{0\}$, *and constants* $0 < \kappa_p < 1$, $\gamma_p, \psi_p \in \mathbb{R}_{\geq 0}$ *and* $\lambda_p \in \mathbb{R}_{>0}$, *such that*

$$
\begin{aligned}
&\mathcal{B}_p(x) \geq \alpha_p(\|h(x)\|_\infty), && \forall x \in X, && (4.6.14)\\
&\mathcal{B}_p(x) \leq \gamma_p, && \forall x \in X_0, && (4.6.15)\\
&\mathcal{B}_p(x) \geq \lambda_p, && \forall x \in X_u, && (4.6.16)
\end{aligned}
$$

and $\forall x \in X$, $\forall w \in W$, *one has*

$$
\mathbb{E}\Big[\mathcal{B}_p(x(k+1)) \,\big|\, x,w\Big] \leq \max\Big\{\kappa_p\mathcal{B}_p(x), \rho_{\text{int}p}(\|w\|), \psi_p\Big\}. \qquad (4.6.17)
$$

In order to construct an APBC for the augmented dt-SS $\mathbb{A}(\Sigma)$, we also need to raise the following assumption.

Assumption 4.6.11. *Suppose there exists* $\tilde{\mu} \geq 1$ *such that*

$$
\forall x \in X,\ \forall p,p' \in P, \quad \mathcal{B}_p(x) \leq \tilde{\mu}\mathcal{B}_{p'}(x). \qquad (4.6.18)
$$

Remark 4.6.12. *Assumption 4.6.11 is a standard one in the literature for switched systems accepting multiple Lyapunov functions with dwell-time similar to the one appeared in [Lib03, equation (3.6)].*

Under Definition 4.6.10 and Assumption 4.6.11, the next theorem lays the foundations for constructing an APBC for $\mathbb{A}(\Sigma)$.

Theorem 4.6.13. *Let $\Sigma = (X, P, \mathcal{P}, W, \varsigma, F, Y, h)$ be a switched subsystem with its equivalent augmented system $\mathbb{A}(\Sigma) = (\mathbb{X}, \mathbb{P}, \mathbb{W}, \varsigma, \mathbb{F}, \mathbb{Y}, \mathbb{H})$. Let $\mathcal{B}_p$ be a CBC for Σ_p, $\forall p \in P$, as in Definition 4.6.10. Assume Assumption 4.6.11 holds, and consider $\epsilon > 1$. If $\forall p \in P$, $k_d \geq \epsilon \frac{\ln(\tilde{\mu})}{\ln(1/\kappa_p)} + 1$, then*

$$\mathcal{B}(x, p, l) = \frac{1}{{\kappa_p}^{l/\epsilon}} \mathcal{B}_p(x), \tag{4.6.19}$$

is an APBC for $\mathbb{A}(\Sigma)$.

Proof. For any $(x, p, l) \in \mathbb{X}$, we get

$$\|\mathbb{H}(x, p, l)\|_\infty = \|h(x)\|_\infty \leq \alpha_p^{-1}(\mathcal{B}_p(x)) = \alpha_p^{-1}({\kappa_p}^{l/\epsilon}\, \mathcal{B}((x, p, l))).$$

Since $\frac{1}{\kappa_p^{l/\epsilon}} > 1$, one can conclude that condition (4.6.1) holds with $\alpha(s) = \min_p\{\alpha_p(s)\}$, $\forall s \in \mathbb{R}_{\geq 0}$. Now we show that conditions (4.6.2) and (4.6.3) hold, as well. For any $(x, p, l) \in \mathbb{X}_0$, one has

$$\mathcal{B}(x, p, l) = \frac{1}{{\kappa_p}^{l/\epsilon}} \mathcal{B}_p(x) \leq \frac{1}{{\kappa_p}^{l/\epsilon}} \gamma_p,$$

and similarly for any $(x, p, l) \in \mathbb{X}_u$, one has

$$\mathcal{B}(x, p, l) = \frac{1}{{\kappa_p}^{l/\epsilon}} \mathcal{B}_p(x) \geq \frac{1}{{\kappa_p}^{l/\epsilon}} \lambda_p,$$

satisfying conditions (4.6.2) and (4.6.3) with $\gamma = \max_p\{\frac{1}{{\kappa_p}^{(k_d-1)/\epsilon}} \gamma_p\}$ and $\lambda = \min_p\{\lambda_p\}$ (since $\frac{1}{\kappa_p^{l/\epsilon}} > 1$).

Now we proceed with showing condition (4.6.4), as well. In order to show that $\mathcal{B}(x, p, l)$ in (4.6.19) satisfies (4.6.4), we should consider the three different scenarios as in Definition 4.6.1. For the first scenario ($l < k_d - 1, p' = p$, and $l' = l + 1$), we have:

$$\begin{aligned}
\mathbb{E}\Big[\mathcal{B}(x', p', l') \,\Big|\, x, p, l, w\Big] &= \frac{1}{{\kappa_{p'}}^{l'/\epsilon}} \mathbb{E}\Big[\mathcal{B}_{p'}(x') \,\Big|\, x, p, w\Big] = \frac{1}{{\kappa_p}^{(l+1)/\epsilon}} \mathbb{E}\Big[\mathcal{B}_p(f_p(x, w, \varsigma)) \,\Big|\, x, w\Big] \\
&\leq \frac{1}{{\kappa_p}^{(l+1)/\epsilon}} \max\Big\{\kappa_p \mathcal{B}_p(x(k)), \rho_{\text{int}p}(\|w\|), \psi_p\Big\} \\
&= \max\Big\{{\kappa_p}^{\frac{\epsilon-1}{\epsilon}} \mathcal{B}_p(x, p, l), \frac{1}{\kappa_p^{(l+1)/\epsilon}} \rho_{\text{int}p}(\|w\|), \frac{1}{\kappa_p^{(l+1)/\epsilon}} \psi_p\Big\} \\
&\leq \max\Big\{{\kappa_p}^{\frac{\epsilon-1}{\epsilon}} \mathcal{B}_p(x, p, l), \frac{1}{\kappa_p^{k_d/\epsilon}} \rho_{\text{int}p}(\|w\|), \frac{1}{\kappa_p^{k_d/\epsilon}} \psi_p\Big\};
\end{aligned}$$

Note that the last inequality holds since $l < k_d - 1$, and consequently, $l + 1 < k_d$.

For the second scenario ($l = k_d - 1, p' = p$, and $l' = k_d - 1$), we have:

$$\begin{aligned}\mathbb{E}\Big[\mathcal{B}(x', p', l') \,\big|\, x, p, l, w\Big] &= \frac{1}{{\kappa_{p'}}^{l'/\epsilon}}\mathbb{E}\Big[\mathcal{B}_{p'}(x') \,\big|\, x, p, w\Big] = \frac{1}{{\kappa_p}^{l/\epsilon}}\mathbb{E}\Big[\mathcal{B}_p(f_p(x, w, \varsigma)) \,\big|\, x, w\Big]\\ &\leq \frac{1}{{\kappa_p}^{l/\epsilon}} \max\Big\{\kappa_p \mathcal{B}_p(x(k)), \rho_{\text{int}p}(\|w\|), \psi_p\Big\}\\ &= \max\Big\{\kappa_p \mathcal{B}(x, p, l), \frac{1}{{\kappa_p}^{l/\epsilon}}\rho_{\text{int}p}(\|w\|), \frac{1}{{\kappa_p}^{l/\epsilon}}\psi_p\Big\}\\ &\leq \max\Big\{{\kappa_p}^{\frac{\epsilon-1}{\epsilon}} \mathcal{B}(x, p, l), \frac{1}{\kappa_p^{k_d/\epsilon}}\rho_{\text{int}p}(\|w\|), \frac{1}{\kappa_p^{k_d/\epsilon}}\psi_p\Big\};\end{aligned}$$

Note that the last inequality holds since $\epsilon > 1$, and consequently, $0 < \frac{\epsilon-1}{\epsilon} < 1$.

For the last scenario ($l = k_d - 1, p' \neq p$, and $l' = 0$), using Assumption 4.6.11, we have:

$$\begin{aligned}\mathbb{E}\Big[\mathcal{B}((x', p', l')) \,\big|\, x, p, l, w\Big] &= \frac{1}{{\kappa_{p'}}^{l'/\epsilon}}\mathbb{E}\Big[\mathcal{B}_{p'}(x') \,\big|\, x, p, w\Big] \leq \tilde{\mu}\,\mathbb{E}\Big[\mathcal{B}_p(f_p(x, w, \varsigma)) \,\big|\, x, w\Big]\\ &\leq \tilde{\mu} \max\Big\{\kappa_p \mathcal{B}_p(x(k)), \rho_{\text{int}p}(\|w\|), \psi_p\Big\}\\ &= \tilde{\mu}{\kappa_p}^{(k_d-1)/\epsilon}\frac{1}{{\kappa_p}^{l/\epsilon}} \max\Big\{\kappa_p \mathcal{B}_p(x(k)), \rho_{\text{int}p}(\|w\|), \psi_p\Big\}\\ &= \max\Big\{\tilde{\mu}\kappa_p^{(k_d-1)/\epsilon}\kappa_p \mathcal{B}((x, p, l)), \tilde{\mu}\rho_{\text{int}p}(\|w\|), \tilde{\mu}\psi_p\Big\}\\ &\leq \max\Big\{\kappa_p \mathcal{B}((x, p, l)), \tilde{\mu}\rho_{\text{int}p}(\|w\|), \tilde{\mu}\psi_p\Big\}\\ &\leq \max\Big\{{\kappa_p}^{\frac{\epsilon-1}{\epsilon}} \mathcal{B}((x, p, l)), \frac{1}{\kappa_p^{k_d/\epsilon}}\rho_{\text{int}p}(\|w\|), \frac{1}{\kappa_p^{k_d/\epsilon}}\psi_p\Big\};\end{aligned}$$

Note that the last scenario holds since $\forall p \in P$, $k_d \geq \epsilon\frac{\ln(\tilde{\mu})}{\ln(1/\kappa_p)} + 1$, and equivalently $\forall p \in P$, $\tilde{\mu}\kappa_p^{(k_d-1)/\epsilon} \leq 1$. By defining $\kappa = \max_p\{{\kappa_p}^{\frac{\epsilon-1}{\epsilon}}\}$, $\rho_{\text{int}}(s) = \max_p\{\frac{1}{\kappa_p^{k_d/\epsilon}}\rho_{\text{int}p}(s)\}, \forall s \in \mathbb{R}_{\geq 0}$, and $\psi = \max_p\{\frac{1}{\kappa_p^{k_d/\epsilon}}\psi_p\}$, condition (4.6.4) holds. Hence, $\mathcal{B}(x, p, l)$ is an APBC for $\mathbb{A}(\Sigma)$, which completes the proof. ■

Remark 4.6.14. *Note that if there exists a common CBC $\mathcal{B} : X \to \mathbb{R}_{\geq 0}$ for all switching modes $p \in P$ satisfying conditions of Definition 4.6.10 and Assumption 4.6.11 (with $\tilde{\mu} = 1$), then $\mathcal{B}(x, p, l) = \mathcal{B}(x)$ (cf. the first case study in Subsection 4.6.5.1).*

Remark 4.6.15. *One can use Lemmas 4.2.14 and 4.5.20 to compute* max*-type CBC in Definition 4.6.10 based on, respectively, SOS optimization problem and CEGIS approach.*

4.6.5 Case Study

To demonstrate the effectiveness of the proposed results, we first apply our approaches to the room temperature network in a circular building containing 1000 rooms. We

compositionally synthesize safety controllers to maintain the temperature of each room in a comfort zone in a bounded time horizon. Moreover, to show the applicability of our results to switched systems accepting *multiple* barrier certificates with a *dwell-time* condition, we apply our technique to a circular cascade network of 500 subsystems (totally 1000 dimensions) and provide upper bounds on the probability that the interconnected system reaches some unsafe region in a finite time horizon.

4.6.5.1 Room Temperature Network

The evolution of the temperature $T(\cdot)$ in the interconnected system is governed by the following dynamics:

$$\Sigma\colon \begin{cases} T(k+1) = AT(k) + \hat{\theta}T_h B_{\mathbf{p}(k)} + \hat{\beta}T_E + 0.25\varsigma(k), \\ y(k) = T(k), \end{cases}$$

where $A \in \mathbb{R}^{n\times n}$ is a matrix with diagonal elements given by $\bar{a}_{ii} = (1 - 2\hat{\eta} - \hat{\beta} - \hat{\theta}b_{ip_i})$, off-diagonal elements $\bar{a}_{i,i+1} = \bar{a}_{i+1,i} = \bar{a}_{1,n} = \bar{a}_{n,1} = \hat{\eta}$, $i \in \{1,\dots,n-1\}$, and all other elements are identically zero. Moreover, $\hat{\eta} = 0.005$, $\hat{\beta} = 0.022$, and $\hat{\theta} = 0.05$, $T_{ei} = -1\,^\circ\mathsf{C}$, $T_h = 50\,^\circ\mathsf{C}$, $T(k) = [T_1(k);\dots;T_n(k)]$, $\varsigma = [\varsigma_1(k);\dots;\varsigma_n(k)]$, $T_E = [T_{e_1};\dots;T_{e_n}]$, and $B_p = [b_{1p_1};\dots;b_{np_n}]$, such that

$$b_{ip_i} = \begin{cases} 0, & \text{if} \quad p_i = 1, \\ 0.1, & \text{if} \quad p_i = 2, \\ 0.2, & \text{if} \quad p_i = 3, \\ 0.3, & \text{if} \quad p_i = 4, \\ 0.4, & \text{if} \quad p_i = 5, \\ 0.5, & \text{if} \quad p_i = 6, \\ 0.6, & \text{if} \quad p_i = 7, \end{cases}$$

with the finite set of modes $P_i = \{1,\dots,7\}, i \in \{1,\dots,n\}$. Now by considering the individual rooms as Σ_i represented by

$$\Sigma_i : \begin{cases} T_i(k+1) = \bar{a}_{ii}T_i(k) + \hat{\theta}T_h b_{i\mathbf{p}_i(k)} + \hat{\eta}w_i(k) + \hat{\beta}T_{ei}(k) + 0.25\varsigma_i(k), \\ y_i(k) = T_i(k), \end{cases}$$

one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1,\dots,\Sigma_N)$, equivalently $\Sigma = \mathcal{I}(\mathbb{A}(\Sigma_1),\dots,,\mathbb{A}(\Sigma_N))$, where $w_i(k) = [T_{i-1}(k);T_{i+1}(k)]$ (with $T_0 = T_n$ and $T_{n+1} = T_1$).

The regions of interest in this example are $X_i \in [1,50], X_{0i} \in [19,21], X_{ui} = [1,17] \cup [23,50], \forall i \in \{1,\dots,n\}$. The main goal is to find an ABC for the interconnected system such that a switching signal is synthesized for Σ keeping the temperature of rooms in the comfort zone $[17,23]^{1000}$. Note that in this example $\mathcal{B}_p = \mathcal{B}_{p'}, \forall p,p' \in P$ (*i.e.,* there exists a common barrier certificate with $\tilde{\mu} = 1$). Then $\mathcal{B}(x,p,l) = \mathcal{B}(x)$ as discussed in Remark 4.6.14. We employ the SMT solver Z3 and CEGIS approach to compute an APBC of an order 4 as $\mathcal{B}_i(T_i) = -0.00012T_i^4 + 0.01045T_i^3 - 0.19932T_i^2 - 0.64538T_i +$

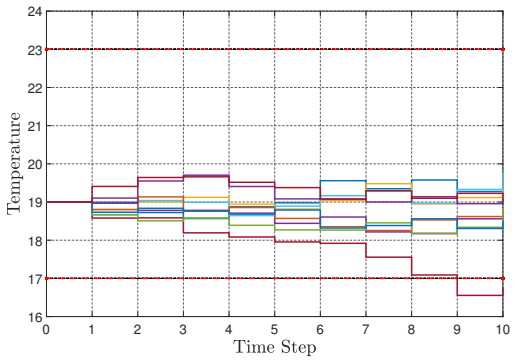

Figure 4.14: Closed-loop state trajectories of a representative room with 10 noise realizations in a network of 1000 rooms.

28.68175. Furthermore, the corresponding constants and functions in Definition 4.6.4 satisfying conditions (4.6.1)-(4.6.4) are quantified as $\gamma_i = 0.16, \lambda_i = 1.2, \psi_i = 7.07 \times 10^{-4}, \kappa_i = 0.99, \alpha_i(s) = 4.5 \times 10^{-5}s^2$, and $\rho_i(s) = 9.3 \times 10^{-6}s^2, \forall s \in \mathbb{R}_{\geq 0}$. Then $\mathcal{B}_i(x_i)$ is an APBC for $\mathbb{A}(\Sigma_i)$,

We now proceed with constructing an ABC for the interconnected system using APBC of subsystems. We check the small-gain condition (4.6.10) that is required for the compositionality result. By taking $\bar{\sigma}_i(s) = s$, $\forall i \in \{1, \ldots, n\}$, condition (4.6.10) and as a result condition (3.3.13) are always satisfied. Moreover, the compositionality condition (4.6.11) is met since $\lambda_i > \gamma_i, \forall i \in \{1, \ldots, n\}$. Then one can conclude that $\mathcal{B}(T) = \max_i \Big\{ -0.00012T_i^4 + 0.01045T_i^3 - 0.19932T_i^2 - 0.64538T_i + 28.68175 \Big\}$ is an ABC for $\mathbb{A}(\Sigma)$ satisfying conditions (4.6.5)-(4.6.7) with $\gamma = 0.16, \lambda = 1.2, \kappa = 0.99$, and $\psi = 7.07 \times 10^{-4}$.

By employing Theorem 4.6.6, one can guarantee that the temperature of the interconnected system Σ starting from the initial condition $a \in [19, 21]^{1000}$ remains in the comfort region $[17, 23]^{1000}$ during the time horizon $\mathcal{T} = 10$ with a probability of at least 87%, *i.e.,*

$$\mathbb{P}\Big\{ \mathcal{B}(T(k)) < 1.2 \;\Big|\; a,\ \forall k \in [0, 10] \Big\} \geq 0.87\,.$$

State trajectories of the closed-loop system in a network of 1000 rooms for a representative room with 10 noise realizations are illustrated in Figure 4.14.

Let us now make a comparison between our results with that of [LSZ20a] which provides a compositional approach for the same class of stochastic switched system but based on finite abstractions. In order to provide a closeness guarantee of at least 87% between state trajectories of the system Σ and those of its finite abstraction in [LSZ20a], one needs to select the state discretization parameter as 0.005, and the required memory usage is accordingly 96.76 GB (cf. [LSZ20a] for more details on computing memory usage based on discretization parameters). In comparison, we needed here only 22.5 MB memory to search for CBC of each subsystem. The computation time in our setting for synthesizing local safety controllers for each subsystem is 5.7 minutes whereas it takes

almost 2865 minutes to only construct finite abstractions for each subsystem using proposed approaches in [LSZ20a]. Note that subsystems in this example are scalar, and the results proposed in [LSZ20a] will suffer from the curse of dimensionality in the case of dealing with higher dimensional subsystems.

4.6.5.2 Switched Systems Accepting Multiple Barrier Certificates with Dwell-Time

In order to show the applicability of our results to switched systems accepting *multiple* barrier certificates with a *dwell-time* condition, we apply our techniques to a circular cascade network of 500 subsystems (totally 1000 dimensions). The model of the system does not have a common barrier certificate because it exhibits unstable behaviors for different switching signals [Lib03] (*i.e.,* if one periodically switches between different modes, the trajectory goes to infinity). The dynamics of the interconnected system are described by

$$\Sigma : \begin{cases} x(k+1) = A_{\mathbf{p}(k)}x(k) + B_{\mathbf{p}(k)} + R\varsigma(k), \\ y(k) = x(k), \end{cases}$$

where

$$A_{\mathbf{p}(k)} = \begin{bmatrix} \bar{A}_{pi} & 0 & \cdots & \cdots & \tilde{A} \\ \tilde{A} & \bar{A}_{pi} & 0 & \cdots & 0 \\ 0 & \tilde{A} & \bar{A}_{pi} & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \tilde{A} & \bar{A}_{pi} \end{bmatrix}_{n\times n},$$

$$\bar{A}_{p_i} = \begin{cases} \begin{bmatrix} 0.05 & 0 \\ 0.9 & 0.03 \end{bmatrix}, & \text{if} \quad p_i = 1, \\ \begin{bmatrix} 0.02 & -1.2 \\ 0 & 0.05 \end{bmatrix}, & \text{if} \quad p_i = 2, \end{cases} \quad \tilde{A} = \begin{bmatrix} 0.01 & 0 \\ 0 & 0.01 \end{bmatrix}.$$

We choose $R = \mathsf{blkdiag}(0.1\mathbb{1}_2, \ldots, 0.1\mathbb{1}_2)$ and fix here $N = 500$. Furthermore, $B_p = [b_{1p_1}; \ldots; b_{Np_N}]$ such that

$$b_{ip_i} = \begin{cases} \begin{bmatrix} -0.9 \\ 0.5 \end{bmatrix}, & \text{if} \quad p_i = 1, \\ \begin{bmatrix} 0.9 \\ -0.2 \end{bmatrix}, & \text{if} \quad p_i = 2. \end{cases}$$

We partition $x(k)$ as $x(k) = [x_1(k); \ldots; x_N(k)]$ and $\varsigma(k)$ as $\varsigma(k) = [\varsigma_1(k); \ldots; \varsigma_N(k)]$, where $x_i(k), \varsigma_i(k) \in \mathbb{R}^2$, *i.e.,* $x_i = [x_{i_1}; x_{i_2}], \varsigma_i = [\varsigma_{i_1}; \varsigma_{i_2}]$. Now, by introducing the individual subsystems Σ_i described as

$$\Sigma_i : \begin{cases} x_i(k+1) = \bar{A}_{\mathbf{p}_i(k)}x_i(k) + \tilde{A}_i w_i(k) + b_{i\mathbf{p}_i(k)} + 0.1\mathbb{1}_2\varsigma_i(k), \\ y_i(k) = x_i(k), \end{cases}$$

where $w_i(k) = y_{i-1}$, $i \in \{1, \ldots, N\}$, with $y_0 = y_N$, one can readily verify that $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$, equivalently $\Sigma = \mathcal{I}(\mathbb{A}(\Sigma_1), \ldots, \mathbb{A}(\Sigma_N))$.

The regions of interest here are $X_i \in [-6,6]^2, X_{0_i} \in [-0.5,0.5]^2, X_{u_i} = [-6,-2]^2 \cup [2,6]^2, \forall i \in \{1,\ldots,N\}$. The main goal is to find an ABC for the interconnected system such that a switching signal is synthesized for Σ regulating the state of subsystems in a safe zone $[-2,2]^{1000}$. We first find a CBC for each mode based on Definitions 4.6.10 using software tool SOSTOOLS [PAV+13] and SDP solver SeDuMi [Stu99]. One can verify that, $\forall i \in \{1,\ldots,N\}$, conditions (4.6.14)-(4.6.17) are satisfied by

$$\begin{aligned}
\text{for } p_i = 1\colon\ & \gamma_{p_i} = 0.15, \lambda_{p_i} = 2.4, \kappa_{p_i} = 0.469, \psi_{p_i} = 5.42 \times 10^{-6},\\
& \alpha_{p_i}(s) = 4 \times 10^{-5} s^2, \rho_{\text{int}p_i}(s) = 2.71 \times 10^{-6} s^2, \forall s \in \mathbb{R}_{\geq 0},\\
\text{for } p_i = 2\colon\ & \gamma_{p_i} = 0.16, \lambda_{p_i} = 2.3, \kappa_{p_i} = 0.498, \psi_{p_i} = 6.88 \times 10^{-6},\\
& \alpha_{p_i}(s) = 5 \times 10^{-5} s^2, \rho_{\text{int}p_i}(s) = 3.44 \times 10^{-6} s^2, \forall s \in \mathbb{R}_{\geq 0},
\end{aligned}$$

with $\mathcal{B}_{1_i}(x_i) = 0.2309x_{i1}^2 + 0.1160x_{i1}x_{i2} + 0.000001x_{i1} + 0.2529x_{i2}^2 - 0.000001x_{i2} + 0.000000002$, $\mathcal{B}_{2_i}(x_i) = 0.2394x_{i1}^2 + 0.1101x_{i1}x_{i2} - 0.000002x_{i1} + 0.2588x_{i2}^2 - 0.000008x_{i2} + 0.000000005$. One can also verify that condition (4.6.18) is met with $\tilde{\mu} = 2$. By taking $\epsilon = 2$, one can get the dwell-time $k_d = 3$. Hence, $\mathcal{B}_i(x_i, p_i, l_i) = \frac{1}{\kappa_{p_i}^{l/2}} \mathcal{B}_i(x_i)$ is an APBC for $\mathbb{A}(\Sigma_i)$ satisfying conditions (4.6.1)-(4.6.4) with $\alpha_i(s) = 4 \times 10^{-5} s^2$, $\forall s \in \mathbb{R}_{\geq 0}, \gamma_i = 0.321, \lambda_i = 2.3, \kappa_i = 0.706$, $\rho_{\text{int}i}(s) = 9.78 \times 10^{-6} s^2$, $\forall s \in \mathbb{R}_{\geq 0}$, and $\psi_i = 1.95 \times 10^{-5}$.

We now proceed with constructing an ABC for the interconnected system using APBC of subsystems. We check the small-gain condition (4.6.10). By taking $\sigma_i(s) = s$, $\forall i \in \{1,\ldots,N\}$, condition (4.6.10) and as a result condition (3.3.13) are always satisfied. Moreover, the compositionality condition (4.6.11) is met since $\lambda_i > \gamma_i, \forall i \in \{1,\ldots,N\}$. Hence, $\mathcal{B}(x,p,l) = \max_i\{\frac{1}{\kappa_{p_i}^{l/2}} \mathcal{B}_i(x_i)\}$ is an ABC for the interconnected $\mathbb{A}(\Sigma)$ satisfying conditions (4.6.5)-(4.6.7) with $\gamma = 0.321, \lambda = 2.3, \kappa = 0.706$, and $\psi = 1.95 \times 10^{-5}$.

By employing Theorem 4.6.6, one can guarantee that the state of the interconnected system Σ starting from the initial condition $a \in [-0.5,0.5]^{1000}$, with any initial mode p_0 and $l_0 = 0$, remains in the safe set $[-2,2]^{1000}$ during the time horizon $\mathcal{T} = 100$ with a probability of at least 86%, *i.e.,*

$$\mathbb{P}\Big\{\mathcal{B}(x(k),p(k),l(k)) < 2.3 \;\Big|\; a, p_0, l_0, \forall k \in [0,100]\Big\} \geq 0.86.$$

4.7 Summary

In the first part of this chapter, we have proposed a compositional approach based on small-gain reasoning for the construction of control barrier certificates for ct-SCS via pseudo-barrier certificates constructed for individual subsystems. We employed a systematic technique based on the sum-of-squares optimization program to search for pseudo-barrier certificates of subsystems while synthesizing safety controllers. Then, utilizing the constructed control barrier certificates, we quantified upper bounds on the probability that an interconnected system reaches certain unsafe regions in a finite time horizon.

In the second part of the chapter, we enlarged the class of systems to continuous-time stochastic *hybrid* systems by adding Poisson processes to the dynamics and proposed a compositional scheme based on dissipativity approaches for the construction of control barrier certificates for this class of models. We showed that the dissipativity-type compositional reasoning can enjoy the structure of the interconnection topology and may not require any constraints on the number or gains of the subsystems. In addition, the provided results based on small-gain approaches ask an additional condition (cf. condition (4.2.1)) which is required for the satisfaction of *small-gain* type compositionality conditions, while dissipativity-type reasoning proposed here does not need such an extra condition.

In the third part of the chapter, we generalized the underlying dynamics to stochastic *switching* systems with *Markovian* switching signals to enforce high-level logic properties in a compositional manner. We also enlarged the class of specifications to those that can be expressed by the accepting language of deterministic finite automata (DFA), whereas previous sections handle only invariance specifications. Furthermore, we provided an additional approach to compute pseudo-barrier certificates for systems with finite input sets by employing counter-example guided inductive synthesis framework based on the satisfiability modulo theories (SMT) solvers such as Z3 [DMB08], dReal [GAC12] or MathSat [CGSS13].

In the last part of the chapter, we proposed a compositional framework for the construction of control barrier certificates for discrete-time stochastic switched systems accepting *multiple* control barrier certificates with some *dwell-time* conditions. We provided an augmented framework for presenting each switched subsystem with several modes with a single system covering all modes whose output trajectories are exactly the same as those of original switched systems. We then compositionally constructed augmented control barrier certificates for interconnected augmented systems based on augmented pseudo-barrier certificates of subsystems by leveraging some max-type small-gain conditions. Given the constructed augmented barrier certificates, we quantified upper bounds on the probability that interconnected systems reach certain unsafe regions in a finite time horizon.

5 Model-free Techniques based on Data-Driven Optimization

5.1 Introduction

Although SHS have been becoming ubiquitous in different real-world safety-critical applications in the past few years, closed-form mathematical models for many complex systems are either not available or equally complex to be of any practical use. Accordingly, one cannot employ model-based techniques, proposed in the previous chapters, to analyze and design this type of complex unknown systems. Although there are some *indirect data-driven* techniques, in the related literature, to solve various analysis and synthesis problems by learning approximate models via identification techniques (see [HW13, and references herein]), acquiring an accurate model for complex systems is always very challenging, time-consuming, and expensive, especially if the underlying dynamics are too complex which is the case in many real-world applications. Then *direct data-driven* techniques have received significant attentions in the past few years for the formal analysis of unknown SHS while bypassing the system identification phase. Since guaranteeing safety and reliability of physical systems based on data is currently very challenging, which is of vital importance in many safety-critical applications, this chapter is concerned with developing *direct data-driven* techniques for the verification and synthesis of SHS while providing *formal guarantees*.

5.1.1 Related Literature

There have been some results in the setting of data-driven optimization techniques. *Scenario approach* has been initially introduced in [CC06] to deal with semi-infinite convex programming for robust control analysis and synthesis problems. The main benefit of the proposed approach is that the solvability of the problem can be obtained through random sampling of constraints provided that a probabilistic relaxation of the worst-case robust paradigm is accepted. As an extension of [CC06], a random convex program framework is developed in [Cal10] in which the results provide an explicit bound on the upper tail probability of violation. The proposed setup is then generalized to the case of random convex programs with posteriori violated constraints to improve the optimal objective value while maintaining the violation probability under control. A novel framework for establishing a probabilistic bridge from optimal values of scenario convex programs to those of robust convex and chance-constrained programs is initially proposed in [MESL14] in which the uncertainty takes values in a general, possibly infinite-dimensional, metric space. The results are then generalized to a certain class of

non-convex problems that includes binary decision variables. An approximation bridge from the infinite-dimensional linear programming to tractable finite convex programs is developed in [MESKL18] in which the performance of the approximation is quantified explicitly. The proposed results are based on the randomized optimization and first-order methods, leading to priori as well as posteriori performance guarantees.

There have been several results on formal analysis and controller synthesis for unknown systems via *indirect* data-driven approaches, *i.e.,* those which leverage system identification techniques followed by model-based controller synthesis approaches. In this regard, a data-driven approach based on Gaussian processes to learn models of quadrotors operating in partially unknown environments is proposed in [WTE18]. A safe reinforcement learning framework for safety-critical control tasks is presented in [COMB19], in which Gaussian processes are employed to model the system dynamics and its uncertainties. A data-driven approach to synthesize controllers enforcing signal temporal logic specifications is studied in [SB18], where a set-valued piece-wise affine model is learned to contain all possible behaviors of an unknown system. A learning-based approach for the construction of symbolic models for nonlinear control systems to enforce safety specifications is proposed in [HSK+20]. A data-driven approach utilizing Gaussian processes to learn unknown control affine nonlinear systems together with a probabilistic bound on the accuracy of the learned model is presented in [JPZ20]. An optimization-based framework for learning control laws from data to enforce safety properties is studied in [LHR+20].

There have also been some results in recent years on the formal analysis of unknown systems via *direct* data-driven approaches, *i.e.,* those that bypass the system identification phase and directly employ system measurements for the verification and control analysis. A data-driven approach for stability analysis of black-box linear switched systems is proposed in [KBJT19], in which a stability-like guarantee is provided based on both the number of observations and the required level of confidence. As an extension of [KBJT19], a data-driven computation of invariant sets for discrete time-invariant black-box systems is proposed in [WJ19]. A data-enabled predictive control algorithm for unknown stochastic linear systems is presented in [CLD19]. A data-driven verification approach for partially-known dynamics with non-deterministic inputs and noisy observations is proposed in [HVdHA15]. Reinforcement learning schemes to synthesize correct policies for continuous-space Markov decision processes with unknown models are studied in [LSS+20, KS20, LPK+22]. Construction of symbolic models and finite MDPs for unknown dynamical systems using data is proposed in [LF22, LSFZ22], respectively. Data-driven verification and synthesis of stochastic systems via (control) barrier certificates are presented in [SLSZ21, SLSZ23]. A data-driven synthesis of safety controllers via multiple control barrier certificates is recently proposed in [NZ23]. Compositional data-driven approaches for safety verification of large-scale stochastic systems including autonomous vehicles are presented in [LDLCF22, LSF23]. Dara-driven stability certificates of (interconnected) homogeneous nonlinear systems are proposed in [LF22, LA23].

Other *direct* data-driven approaches which are developed on top of *behavioral approaches* [WP97] have been proposed to solve linear quadratic regulation (LQR) problems [DPT19], to design model-reference controllers for linear systems [BDPFT21], and

to stabilize polynomial-type systems [GDPT21], switched linear systems [RDPT21], and linear time-varying systems [NM20]. Recently, data-driven approaches for solving LQR problems and synthesizing robust controllers are proposed in [DPT21, BKSA20, BSA20], in which underlying unknown dynamics are affected by exogenous disturbances. A data-driven technique to learn control laws for nonlinear polynomial-type systems directly from data is proposed in [GDPT20], in which input-output measurements are collected in an experiment over a finite-time period. Nevertheless, none of these approaches consider state and input constraints. Data-driven approaches to synthesize state-feedback controllers making a compact polyhedral set containing the origin robustly invariant are proposed in [BDPT20b, BDPT20a]. These results are conservative in the sense that when there is no controller for the given compact polyhedral set, one might be able to find controllers making subsets of this polytope robustly invariant. In addition, these techniques require an individual constraint for each vertex of the polytope (cf. [BDPT20b, Section 4] and [BDPT20a, Theorems 1, 2]). Consequently, given any arbitrary polytope, the number of vertices grows exponentially with respect to its dimension and the number of hyperplanes in the worst case scenario [Dye83].

5.1.2 Contributions

In the first part of this chapter, we propose a data-driven approach for the formal estimation of infinitesimal generators of continuous-time stochastic systems with unknown dynamics. We first approximate the infinitesimal generator of the solution process via a set of data collected from trajectories of the unknown system. The approximation utilizes both time discretization and sampling from the solution process. Assuming proper continuity assumptions on dynamics of the system, we then quantify the closeness between the infinitesimal generator and its approximation while providing a priori guaranteed confidence bound. We demonstrate that both the time discretization and the number of data play significant roles in providing a reasonable closeness precision. Moreover, for a fixed size of data, variance of the estimation converges to infinity when the time discretization parameter goes to zero. The formulated error bound shows how to pick proper data size and time discretization jointly to prevent this counter-intuitive behavior.

In the second part of the chapter, we enlarge the class of systems to stochastic *hybrid* ones by adding Poisson processes to the dynamics and propose a data-driven approach for the estimation of infinitesimal generator for this class of models. In addition, our data-driven scheme handles stochastic systems with control inputs, while the results of the previous section only deal with stochastic *autonomous* systems.

In the third part of the chapter, we propose a data-driven approach for formal verification of both discrete- and continuous-time systems with unknown dynamics. The main target is to verify the safety of unknown systems based on the construction of barrier certificates via a set of data collected from trajectories of systems while providing an a-priori guaranteed confidence on the safety. In our proposed frameworks, we first cast the original safety problem as a robust convex program (RCP). Solving the proposed RCP is not tractable in general since the unknown model appears in one of the

constraints. Instead, we collect finite numbers of data from trajectories of systems and provide a scenario convex program (SCP) corresponding to the original RCP. We then establish a probabilistic closeness between the optimal value of SCP and that of RCP, and as a result, we formally quantify the safety guarantee of unknown systems based on the number of data and the required level of confidence. We propose our frameworks in both discrete- and continuous-time settings.

In the last part of the chapter, we propose a data-driven approach to *synthesize* safety controllers for continuous-time nonlinear polynomial-type systems with unknown dynamics. The proposed framework is based on notions of control barrier certificates, constructed from data while providing a guaranteed confidence of 1 on the safety of unknown systems. Under a certain rank condition, we synthesize polynomial state-feedback controllers to ensure the safety of the unknown system only via a *single trajectory* collected from it.

5.2 Data-Driven Estimation of Infinitesimal Generators for Stochastic Systems

Infinitesimal generator of a continuous-time stochastic process is a partial differential operator that encodes large amounts of information about the stochastic process. In particular, infinitesimal generator plays a significant role in the analysis of continuous-time stochastic systems including (i) stability verification and controller synthesis via (control) Lyapunov functions (*e.g.,* [TSS14]); (ii) input-to-state stability (ISS) property of continuous-time stochastic systems (*e.g.,* [ZKZ12]); (iii) establishing similarity relations between two continuous-time stochastic systems via stochastic simulation functions (*e.g.,* [JP09, NSZ21]); (iv) incremental stability of continuous-time stochastic control systems (*e.g.,* [ZMEM$^+$14]), and (v) safety verification and controller synthesis of continuous-time stochastic systems via barrier certificates (*e.g.,* [PJP07, SDC19, NSZ20b]), to name a few. Hence, computing the infinitesimal generator is a crucial step in developing an analysis framework for continuous-time stochastic systems.

In this section, we propose a data-driven approach for the estimation of infinitesimal generator of continuous-time stochastic systems with unknown dynamics. To do so, we first approximate the infinitesimal generator of the stochastic system via a set of data collected from trajectories of the unknown system. We then provide a formal scheme to compute the error between the approximated infinitesimal generator and the exact one corresponding to unknown dynamics with the associated confidence bound. We show that both the sampling time and number of data are crucial to provide a reasonable closeness precision. To demonstrate the effectiveness of our proposed results, we apply them to an unknown room temperature problem.

5.2.1 Continuous-Time Stochastic Systems

We consider stochastic systems in continuous-time (ct-SS) defined over a general state space as in the following definition.

Definition 5.2.1. *A continuous-time stochastic system (ct-SS) is characterized by the tuple*

$$\Sigma = (X, f, \sigma), \tag{5.2.1}$$

where:

- $X \subset \mathbb{R}^n$ *is the state space of the system;*
- $f : X \to \mathbb{R}^n$ *is the drift term;*
- $\sigma : \mathbb{R}^n \to \mathbb{R}^{n \times b}$ *is the diffusion term.*

A continuous-time stochastic system Σ *satisfies*

$$\Sigma : \mathsf{d}x(t) = f(x(t))\mathsf{d}t + \sigma(x(t))\mathsf{d}\mathbb{W}_t, \tag{5.2.2}$$

$\mathbb{P}$*-almost surely (*$\mathbb{P}$*-a.s.), where the stochastic process* $x : \Omega \times \mathbb{R}_{\geq 0} \to X$ *is called the* solution process *of* Σ*. We also employ* $x_a(t)$ *to denote the value of the solution process at time* $t \in \mathbb{R}_{\geq 0}$ *under an initial condition* $x_a(0) = a$ $\mathbb{P}$*-a.s., where* a *is a random variable that is* $\mathcal{F}_0$*-measurable.*

In order to ensure the existence and uniqueness of the solution process, we assume that the drift term f is globally Lipschitz continuous: *i.e.,* there exists a constant $\mathscr{L}_f \in \mathbb{R}_{\geq 0}$ such that

$$\|f(x) - f(x')\| \leq \mathscr{L}_f \|x - x'\|, \quad \forall x, x' \in X. \tag{5.2.3}$$

We also assume that the diffusion term σ is globally Lipschitz continuous with the Lipschitz constant $\mathscr{L}_\sigma$. In this section, we assume that the state set X is a compact subset of $\mathbb{R}^n$ over which we are interested to perform our analysis. This is motivated by the boundedness assumptions required for the theoretical results of this work (cf. Assumption 5.2.5).

We define $\mathsf{c}(x) := \sigma(x)\sigma(x)^\top$ as the *infinitesimal covariance* and call $f(x)$ the *infinitesimal mean*. In addition, the *infinitesimal generator* $\mathcal{L}$ of the process $x(t)$ acting on a function $\mathcal{H} : X \to \mathbb{R}$ is defined as

$$\mathcal{L}\mathcal{H}(x) = \partial_x \mathcal{H}(x) f(x) + \frac{1}{2}\mathsf{Tr}(\mathsf{c}(x)\partial_{x,x}\mathcal{H}(x)), \tag{5.2.4}$$

where $\partial_x \mathcal{H}(x) = \left[\frac{\partial \mathcal{H}(x)}{\partial x_i}\right]_i \in \mathbb{R}^{1 \times n}$ and $\partial_{x,x}\mathcal{H}(x) = \left[\frac{\partial^2 \mathcal{H}(x)}{\partial x_i \partial x_j}\right]_{i,j} \in \mathbb{R}^{n \times n}$. One important aspect of the infinitesimal generator is that it can be used to compute the expected value of any function of the solution process $\mathcal{H}(x_\tau)$ via Dynkin's formula [Dyn65] as the following:

$$\mathbb{E}\Big[\mathcal{H}(x_\tau)\Big] = \mathcal{H}(x) + \mathbb{E}_x\Big[\int_0^\tau \mathcal{L}\mathcal{H}(x_t)\mathsf{d}t\Big], \qquad \forall x \in X, \tag{5.2.5}$$

where x_τ is the solution process at time $\tau \in \mathbb{R}_{\geq 0}$ starting from x, and $\mathbb{E}_x$ is the expected value conditioned on x.

In this section, we assume that drift and diffusion terms f, σ in (5.2.1) are both unknown, and we employ the term *unknown* model to refer to this type of systems. The main goal is to provide a formal framework for the estimation of the infinitesimal generator in (5.2.4). To do so, we first approximate the infinitesimal generator $\mathcal{L}$ as

$$\widehat{\mathcal{L}}_1\mathcal{H}(x) := \frac{\mathbb{E}_x\Big[\mathcal{H}(x_\tau)\Big] - \mathcal{H}(x)}{\tau}, \qquad \forall x \in X. \tag{5.2.6}$$

Since there is no closed-form solution for the expected value in (5.2.6), one cannot directly employ (5.2.6) as the approximated value of the infinitesimal generator. Suppose we collect $\hat{\mathcal{N}}$ independent and identically distributed (i.i.d.) sampled data $(x_\tau^i)_{i=1}^{\hat{\mathcal{N}}}$ by extracting $\hat{\mathcal{N}}$ solution processes $x_\tau^i, i \in \{1, \ldots, \hat{\mathcal{N}}\}$, at time τ. We now employ an empirical approximation of the expected value and propose another layer of approximation for the infinitesimal generator $\mathcal{L}$ as

$$\widehat{\mathcal{L}}_2\mathcal{H}(x) := \frac{\frac{1}{\hat{\mathcal{N}}}\sum_{i=1}^{\hat{\mathcal{N}}} \mathcal{H}(x_\tau^i) - \mathcal{H}(x)}{\tau}, \qquad \forall x \in X, \tag{5.2.7}$$

where $\hat{\mathcal{N}} \in \mathbb{N}_{\geq 1}$ is the number of samples required for the computation of the empirical mean.

We now state the main problem that we aim at solving in this section.

Problem 5.2.2. *Consider the infinitesimal generator of the stochastic process in* (5.2.4)*, and its data-driven approximation in* (5.2.7)*. Provide a formal framework to quantify $\tilde{\varepsilon} \in \mathbb{R}_{\geq 0}$ as the distance between the infinitesimal generator and its data-driven approximation with an a-priori confidence $\beta \in (0, 1]$ as*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq \tilde{\varepsilon}\Big\} \geq 1 - \beta, \qquad \forall x \in X. \tag{5.2.8}$$

It should be noted that the confidence β in (5.2.8) is due to the data-driven nature of our proposed estimation algorithm. In particular, one can push the confidence to be close to 1 at the cost of collecting more data. This type of guarantee is very similar to the closeness guarantee provided by Chernoff bound in statistical model checking [LSAZ22, Section 9].

Remark 5.2.3. *Note that the empirical approximation in* (5.2.7) *can be utilized for scenarios in which the infinitesimal generator needs to be computed for finitely-many initial conditions. Examples of such scenarios include safety verification and synthesis of stochastic hybrid systems similar to [SLSZ23] or construction of finite Markov decision processes and establishing similarity relations between two stochastic systems via stochastic simulation functions as in [NSZ21], where dynamics of underlying systems are* unknown*.*

5.2.2 Solution Approach

Here, we first quantify the formal closeness between $\mathcal{L}\mathcal{H}(x)$ and its first approximation $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ as in (5.2.6). We then quantify the distance between $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and its empirical approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ as in (5.2.7). We finally propose our solution for the closeness quantification between $\mathcal{L}\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$. To do so, we need to raise the following two assumptions.

Assumption 5.2.4. *Suppose infinitesimal mean $f(x)$, covariance $\mathsf{c}(x)$, $\partial_x\mathcal{H}(x)$, and $\partial_{x,x}\mathcal{H}(x)$ are all Lipschitz continuous with Lipschitz constants $\mathscr{L}_f$ as in* (5.2.3)*, and $\mathscr{L}_{\mathsf{c}}, \mathscr{L}_{\mathcal{H}_1}, \mathscr{L}_{\mathcal{H}_2} \in \mathbb{R}_{\geq 0}$ as the following, $\forall x, x' \in X$:*

$$\|\mathsf{c}(x) - \mathsf{c}(x')\|_F \leq \mathscr{L}_{\mathsf{c}}\|x - x'\|, \quad \|\partial_x\mathcal{H}(x) - \partial_{x'}\mathcal{H}(x')\| \leq \mathscr{L}_{\mathcal{H}_1}\|x - x'\|,$$
$$\|\partial_{x,x}\mathcal{H}(x) - \partial_{x',x'}\mathcal{H}(x')\|_F \leq \mathscr{L}_{\mathcal{H}_2}\|x - x'\|.$$

Assumption 5.2.5. *Suppose $f(x)$, $\mathsf{c}(x)$, $\partial_x\mathcal{H}(x)$, and $\partial_{x,x}\mathcal{H}(x)$ are all bounded with constants $\mathcal{M}_f$, $\mathcal{M}_{\mathsf{c}}, \mathcal{M}_{\mathcal{H}_1}, \mathcal{M}_{\mathcal{H}_2} \in \mathbb{R}_{\geq 0}$ as, $\forall x \in X$:*

$$\|f(x)\| \leq \mathcal{M}_f, \quad \|\partial_x\mathcal{H}(x)\| \leq \mathcal{M}_{\mathcal{H}_1}, \quad \|\mathsf{c}(x)\|_F \leq \mathcal{M}_{\mathsf{c}}, \quad \|\partial_{x,x}\mathcal{H}(x)\|_F \leq \mathcal{M}_{\mathcal{H}_2}.$$

We now employ Assumptions 5.2.4 and 5.2.5 and propose the next lemma which shows that $\mathcal{L}\mathcal{H}(x)$ is also Lipschitz continuous.

Lemma 5.2.6. *Under Assumptions 5.2.4-5.2.5, $\mathcal{L}\mathcal{H}(x)$ is also Lipschitz continuous with a Lipschitz constant $\mathscr{L}$ as:*

$$|\mathcal{L}\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x')| \leq \mathscr{L}\|x - x'\|, \quad \forall x, x' \in X,$$

where $\mathscr{L} = \mathcal{M}_{\mathcal{H}_1}\mathscr{L}_f + \mathcal{M}_f\mathscr{L}_{\mathcal{H}_1} + \frac{1}{2}(\mathscr{L}_{\mathsf{c}}\mathcal{M}_{\mathcal{H}_2} + \mathcal{M}_{\mathsf{c}}\mathscr{L}_{\mathcal{H}_2})$.

Proof. Using the definition of $\mathcal{L}\mathcal{H}(x)$ in (5.2.4), we have

$$|\mathcal{L}\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x')| \leq |\partial_x\mathcal{H}(x)f(x) - \partial_{x'}\mathcal{H}(x')f(x')| + |\frac{1}{2}\mathsf{Tr}\big(\mathsf{c}(x)\partial_{x,x}\mathcal{H}(x) - \mathsf{c}(x')\partial_{x',x'}\mathcal{H}(x')\big)|. \tag{5.2.9}$$

Using the following known inequality

$$|\mathbb{A}^\top\mathbb{B} - \mathbb{C}^\top\mathbb{D}| \leq \|\mathbb{A}\|\|\mathbb{B} - \mathbb{D}\| + \|\mathbb{D}\|\|\mathbb{A} - \mathbb{C}\|,$$

for all $\mathbb{A}, \mathbb{B}, \mathbb{C}, \mathbb{D} \in \mathbb{R}^n$, and Assumptions 5.2.4 and 5.2.5, the first term in the right-hand side of (5.2.9) is upper bounded by

$$\|\partial_x\mathcal{H}(x)\|\|f(x) - f(x')\| + \|f(x')\|\|\partial_x\mathcal{H}(x) - \partial_{x'}\mathcal{H}(x')\| \leq \mathcal{M}_{\mathcal{H}_1}\mathscr{L}_f\|x - x'\| + \mathcal{M}_f\mathscr{L}_{\mathcal{H}_1}\|x - x'\|.$$

Using the notation $A \odot B$ as the Hadamard product of two matrices A, B, the second term in the right-hand side of (5.2.9) is upper bounded as

$$\begin{aligned}
&\frac{1}{2}\Big|\sum_{i,j}[\mathsf{c}(x)\odot\partial_{x,x}\mathcal{H}(x)]_{i,j}-[\mathsf{c}(x')\odot\partial_{x',x'}\mathcal{H}(x')]_{i,j}\Big|\\
&\leq\frac{1}{2}\sum_{i,j}\Big|[(\mathsf{c}(x)-\mathsf{c}(x'))\odot\partial_{x,x}\mathcal{H}(x)]_{i,j}\Big|+\frac{1}{2}\sum_{i,j}\Big|[\mathsf{c}(x')\odot(\partial_{x,x}\mathcal{H}(x)-\partial_{x',x'}\mathcal{H}(x'))]_{i,j}\Big|\\
&\leq\frac{1}{2}\Big[\sum_{i,j}[\mathsf{c}(x)-\mathsf{c}(x')]_{i,j}^2\sum_{i,j}[\partial_{x,x}\mathcal{H}(x)]_{i,j}^2\Big]^{\frac{1}{2}}+\frac{1}{2}\Big[\sum_{i,j}[\mathsf{c}(x')]_{i,j}^2\sum_{i,j}[\partial_{x,x}\mathcal{H}(x)-\partial_{x',x'}\mathcal{H}(x'))]_{i,j}^2\Big]^{\frac{1}{2}}\\
&=\frac{1}{2}\|\mathsf{c}(x)-\mathsf{c}(x')\|_F\|\partial_{x,x}\mathcal{H}(x)\|_F+\frac{1}{2}\|\mathsf{c}(x')\|_F\|\partial_{x,x}\mathcal{H}(x)-\partial_{x',x'}\mathcal{H}(x'))\|_F\\
&\leq\frac{1}{2}(\mathscr{L}_{\mathsf{c}}\mathcal{M}_{\mathcal{H}_2}+\mathcal{M}_{\mathsf{c}}\mathscr{L}_{\mathcal{H}_2})\|x-x'\|.
\end{aligned}$$

Combining the two upper bounds completes the proof. ■

Now as the first step, we formally quantify the closeness between $\mathcal{L}\mathcal{H}(x)$ and its approximation $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ as proposed in the following theorem.

Theorem 5.2.7. *Let $\mathcal{L}\mathcal{H}(x)$ be the infinitesimal generator of the process $x(t)$ acting on a function $\mathcal{H}$ and $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ be its approximation as in* (5.2.6) *both at state x. Under Assumptions 5.2.4 and 5.2.5 and Lemma 5.2.6, one has*

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x)-\mathcal{L}\mathcal{H}(x)|\leq\tilde{\varepsilon}_1,\qquad\forall x\in X,$$

with

$$\tilde{\varepsilon}_1:=\mathscr{L}\Big(\frac{1}{2}\mathcal{M}_f\tau+\frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\Big),\tag{5.2.10}$$

where $\mathscr{L}=\mathcal{M}_{\mathcal{H}_1}\mathscr{L}_f+\mathcal{M}_f\mathscr{L}_{\mathcal{H}_1}+\frac{1}{2}(\mathscr{L}_{\mathsf{c}}\mathcal{M}_{\mathcal{H}_2}+\mathcal{M}_{\mathsf{c}}\mathscr{L}_{\mathcal{H}_2})$, and $\mathcal{M}_\sigma$ is a constant such that $\|\sigma(x)\|_F\leq\mathcal{M}_\sigma$ for all $x\in X$.

Proof: Using Dynkin's formula in (5.2.5) and by considering the definition of $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ as in (5.2.6), one has

$$\widehat{\mathcal{L}}_1\mathcal{H}(x)=\mathbb{E}\Big[\frac{1}{\tau}\int_0^\tau\mathcal{L}\mathcal{H}(x_t)\mathsf{d}t\Big].$$

By subtracting $\mathcal{L}\mathcal{H}(x)$ from the two sides, we get

$$\widehat{\mathcal{L}}_1\mathcal{H}(x)-\mathcal{L}\mathcal{H}(x)=\mathbb{E}\Big[\frac{1}{\tau}\int_0^\tau\big(\mathcal{L}\mathcal{H}(x_t)-\mathcal{L}\mathcal{H}(x)\big)\mathsf{d}t\Big].$$

Consequently,

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x)-\mathcal{L}\mathcal{H}(x)|\leq\frac{1}{\tau}\int_0^\tau\mathbb{E}\Big[|\mathcal{L}\mathcal{H}(x_t)-\mathcal{L}\mathcal{H}(x)|\Big]\mathsf{d}t.$$

By employing Lemma 5.2.6, we have

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq \frac{\mathscr{L}}{\tau}\int_0^\tau \mathbb{E}\Big[\|x_t - x\|\Big]\mathsf{d}t. \tag{5.2.11}$$

Now we aim at finding an upper bound for $\mathbb{E}\Big[\|x_t - x\|\Big]$. Under the continuity property of the solution process of the system, we have

$$x_t = x + \int_0^t f(x_s)\mathsf{d}s + \int_0^t \sigma(x_s)\mathsf{d}\mathbb{W}_s.$$

Then, one obtains

$$\mathbb{E}\Big[\|x_t - x\|\Big] = \mathbb{E}\Big[\|\int_0^t f(x_s)\mathsf{d}s + \int_0^t \sigma(x_s)\mathsf{d}\mathbb{W}_s\|\Big] \leq \mathbb{E}\Big[\|\int_0^t f(x_s)\mathsf{d}s\| + \|\int_0^t \sigma(x_s)\mathsf{d}\mathbb{W}_s\|\Big].$$

According to Jensen's inequality, we know that for any vector $\mathsf{r} \in \mathbb{R}^n$, $\mathbb{E}[\|\mathsf{r}\|] \leq \sqrt{\mathbb{E}[\mathsf{r}^\top \mathsf{r}]}$. Then,

$$\mathbb{E}\Big[\|x_t - x\|\Big] \leq \Big[\mathbb{E}\int_0^t f(x_s)^\top \mathsf{d}s \int_0^t f(x_s)\mathsf{d}s\Big]^{\frac{1}{2}} + \Big[\mathbb{E}\int_0^t \sigma(x_s)^\top \mathsf{d}\mathbb{W}_s^\top \int_0^t \sigma(x_s)\mathsf{d}\mathbb{W}_s\Big]^{\frac{1}{2}}. \tag{5.2.12}$$

Under Assumption 5.2.5, the first term in the right-hand side of (5.2.12) is upper bounded by

$$\Big[\mathbb{E}\int_0^t \int_0^t \|f(x_{s_1})\|\|f(x_{s_2})\|\mathsf{d}s_1\mathsf{d}s_2\Big]^{\frac{1}{2}} \leq \mathcal{M}_f t. \tag{5.2.13}$$

In addition, using the multivariate version of the Itô isometry property [Oks13] and Assumption 5.2.5, we can bound the second term in the right-hand side of (5.2.12) as

$$\Big[\int_0^t \mathbb{E}\Big[\|\sigma(x_s)\|_F^2\Big]\mathsf{d}s\Big]^{\frac{1}{2}} \leq \mathcal{M}_\sigma\sqrt{t}. \tag{5.2.14}$$

By substituting (5.2.13) and (5.2.14) in (5.2.12), one has

$$\mathbb{E}\Big[\|x_t - x\|\Big] \leq \mathcal{M}_f t + \mathcal{M}_\sigma\sqrt{t}. \tag{5.2.15}$$

Consequently, by substituting (5.2.15) in (5.2.11), we have

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq \frac{\mathscr{L}}{\tau}\int_0^\tau (\mathcal{M}_f t + \mathcal{M}_\sigma\sqrt{t})\mathsf{d}t = \mathscr{L}\Big(\frac{1}{2}\mathcal{M}_f\tau + \frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\Big),$$

which completes the proof. ■

Remark 5.2.8. *Note that $\tilde{\varepsilon}_1$ in Theorem 5.2.7 can be seen as the bias of the estimation. This is due to the fact that $\mathbb{E}[\widehat{\mathcal{L}}_2\mathcal{H}(x)] = \widehat{\mathcal{L}}_1\mathcal{H}(x)$ and*

$$|\mathbb{E}[\widehat{\mathcal{L}}_2\mathcal{H}(x)] - \mathcal{L}\mathcal{H}(x)| \leq \tilde{\varepsilon}_1, \qquad \forall x \in X,$$

which means the expectation of the estimator $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ is away from the true value $\mathcal{L}\mathcal{H}(x)$ by at most $\tilde{\varepsilon}_1$.

Remark 5.2.9. *In order to provide a formal closeness between the infinitesimal generator of the stochastic process and its first approximation as in Theorem 5.2.7, the continuity properties of the solution process together with the continuity of $\mathcal{H}(x)$ and $\mathcal{L}\mathcal{H}(x)$ are required.*

As the second step, to quantify the closeness between $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$, we first formulate a bound on the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ in the next lemma.

Lemma 5.2.10. *Suppose $|\mathcal{H}(x)| \leq \mathcal{M}_{\mathcal{H}}$ for all $x \in X$. Under Assumptions 5.2.4 and 5.2.5 and Lemma 5.2.6, the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ in* (5.2.7) *is bounded by*

$$\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq \frac{1}{\hat{\mathcal{N}}}[\frac{\tilde{\alpha}}{\tau} + \frac{\tilde{\gamma}}{\sqrt{\tau}} + \tilde{\theta}], \tag{5.2.16}$$

with $\tilde{\alpha}$ satisfying

$$|\mathcal{L}\mathcal{H}(x)^2 - 2\mathcal{M}_{\mathcal{H}}\mathcal{L}\mathcal{H}(x)| \leq \tilde{\alpha}, \qquad \forall x \in X,$$

$$\textit{and} \qquad \tilde{\gamma} := \frac{2}{3}\mathcal{M}_\sigma(\bar{\mathscr{L}} + 2\mathcal{M}_{\mathcal{H}}\mathscr{L}), \quad \tilde{\theta} := \frac{1}{2}\mathcal{M}_f(\bar{\mathscr{L}} + 2\mathcal{M}_{\mathcal{H}}\mathscr{L}),$$

where $\bar{\mathscr{L}} := \bar{\mathcal{M}}_{\mathcal{H}_1}\mathscr{L}_f + \mathcal{M}_f\bar{\mathscr{L}}_{\mathcal{H}_1} + \frac{1}{2}(\mathscr{L}_{\mathsf{c}}\bar{\mathcal{M}}_{\mathcal{H}_2} + \mathcal{M}_{\mathsf{c}}\bar{\mathscr{L}}_{\mathcal{H}_2})$, and $\bar{\mathcal{M}}_{\mathcal{H}_1}, \bar{\mathcal{M}}_{\mathcal{H}_2}, \bar{\mathscr{L}}_{\mathcal{H}_1}, \bar{\mathscr{L}}_{\mathcal{H}_2}$ are constants similar to the ones in Assumptions 5.2.4 and 5.2.5 but for $\mathcal{H}(x)^2$.

Proof. We compute the variance of the empirical mean as

$$\begin{aligned}
&\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) = \frac{1}{\tau^2\hat{\mathcal{N}}}\mathsf{Var}(\mathcal{H}(x_\tau^i)) = \frac{1}{\tau^2\hat{\mathcal{N}}}\Big[\mathbb{E}[\mathcal{H}(x_\tau^i)^2] - \mathbb{E}[\mathcal{H}(x_\tau^i)]^2\Big] \\
&= \frac{1}{\tau^2\hat{\mathcal{N}}}\Big[\mathbb{E}[\mathcal{H}(x_\tau^i)^2] - \mathcal{H}(x)^2 - \mathbb{E}[\mathcal{H}(x_\tau^i)]^2 + \mathcal{H}(x)^2\Big] \\
&= \frac{1}{\tau\hat{\mathcal{N}}}\Big[\frac{\mathbb{E}[\mathcal{H}(x_\tau^i)^2] - \mathcal{H}(x)^2}{\tau}\Big] - \frac{1}{\tau\hat{\mathcal{N}}}\frac{[\mathbb{E}[\mathcal{H}(x_\tau^i)] - \mathcal{H}(x)][\mathbb{E}[\mathcal{H}(x_\tau^i)] + \mathcal{H}(x)]}{\tau} \\
&= \frac{1}{\tau\hat{\mathcal{N}}}\widehat{\mathcal{L}}_1\mathcal{H}(x)^2 - \frac{1}{\tau\hat{\mathcal{N}}}\widehat{\mathcal{L}}_1\mathcal{H}(x)(\mathbb{E}[\mathcal{H}(x_\tau^i)] + \mathcal{H}(x)).
\end{aligned}$$

Similar to (5.2.10), one can also quantify the distance between $\widehat{\mathcal{L}}_1\mathcal{H}(x)^2$ and $\mathcal{L}\mathcal{H}(x)^2$ as

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x)^2 - \mathcal{L}\mathcal{H}(x)^2| \leq \bar{\varepsilon}_1, \qquad \forall x \in X,$$

with $\bar{\varepsilon}_1 := \bar{\mathscr{L}}\Big(\frac{1}{2}\mathcal{M}_f\tau + \frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\Big)$ and

$$\bar{\mathscr{L}} := \bar{\mathcal{M}}_{\mathcal{H}_1}\mathscr{L}_f + \mathcal{M}_f\bar{\mathscr{L}}_{\mathcal{H}_1} + \frac{1}{2}(\mathscr{L}_{\mathsf{c}}\bar{\mathcal{M}}_{\mathcal{H}_2} + \mathcal{M}_{\mathsf{c}}\bar{\mathscr{L}}_{\mathcal{H}_2}),$$

where $\bar{\mathcal{M}}_{\mathcal{H}_1}, \bar{\mathcal{M}}_{\mathcal{H}_2}, \bar{\mathscr{L}}_{\mathcal{H}_1}, \bar{\mathscr{L}}_{\mathcal{H}_2}$ are constants similar to the ones in Assumptions 5.2.4, 5.2.5 but for $\mathcal{H}(x)^2$. These constants can be easily obtained using $\mathcal{M}_{\mathcal{H}_1}, \mathcal{M}_{\mathcal{H}_2}, \mathscr{L}_{\mathcal{H}_1}, \mathscr{L}_{\mathcal{H}_2}$.

Then, we have

$$\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq \frac{1}{\tau\hat{\mathcal{N}}}\Big((\mathcal{L}\mathcal{H}(x)^2+\bar{\varepsilon}_1) - (\mathcal{L}\mathcal{H}(x)-\tilde{\varepsilon}_1)2\mathcal{M}_{\mathcal{H}}\Big).$$

Accordingly, one has

$$\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq \frac{\tilde{\alpha}+\tilde{\gamma}\sqrt{\tau}+\tilde{\theta}\tau}{\tau\hat{\mathcal{N}}} = \frac{1}{\hat{\mathcal{N}}}[\frac{\tilde{\alpha}}{\tau}+\frac{\tilde{\gamma}}{\sqrt{\tau}}+\tilde{\theta}],$$

with $\tilde{\alpha}$ satisfying

$$|\mathcal{L}\mathcal{H}(x)^2 - 2\mathcal{M}_{\mathcal{H}}\mathcal{L}\mathcal{H}(x)| \leq \tilde{\alpha}, \qquad \forall x \in X,$$
$$\text{and } \tilde{\gamma} := \frac{2}{3}\mathcal{M}_\sigma(\bar{\mathscr{L}}+2\mathcal{M}_{\mathcal{H}}\mathscr{L}), \quad \tilde{\theta} := \frac{1}{2}\mathcal{M}_f(\bar{\mathscr{L}}+2\mathcal{M}_{\mathcal{H}}\mathscr{L}).$$

Note that $\tilde{\alpha}$ can be computed using parameters of Assumptions 5.2.4 and 5.2.5. This completes the proof. ■

In the next theorem, we employ Chebyshev's inequality [SYM84] and quantify the mismatch between approximated values of the infinitesimal generator in (5.2.6) and (5.2.7) by providing an a-priori confidence bound.

Theorem 5.2.11. *Let $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ be approximations of the infinitesimal generator $\mathcal{L}$ at state x based on expected value and empirical approximation as in* (5.2.6) *and* (5.2.7)*, respectively. For any $0 < \beta \leq 1$, we have*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq \tilde{\varepsilon}_2\Big\} \geq 1-\beta, \qquad \forall x \in X,$$

with

$$\tilde{\varepsilon}_2 := \left[\frac{1}{\beta\hat{\mathcal{N}}}\left(\frac{\tilde{\alpha}}{\tau}+\frac{\tilde{\gamma}}{\sqrt{\tau}}+\tilde{\theta}\right)\right]^{\frac{1}{2}}. \tag{5.2.17}$$

Proof. We know that $\mathbb{E}[\widehat{\mathcal{L}}_2\mathcal{H}(x)] = \widehat{\mathcal{L}}_1\mathcal{H}(x)$. According to Chebyshev's inequality [SYM84], one has

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq \tilde{\varepsilon}_2\Big\} = \mathbb{P}\Big\{|\mathbb{E}[\widehat{\mathcal{L}}_2\mathcal{H}(x)] - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq \tilde{\varepsilon}_2\Big\} \geq 1 - \frac{\underline{\sigma}^2}{\tilde{\varepsilon}_2^2},$$

for any $\tilde{\varepsilon}_2 \in \mathbb{R}_{>0}$, where $\underline{\sigma}^2$ is the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ and can be computed using Lemma 5.2.10:

$$\underline{\sigma}^2 := \mathsf{Var}\left[\frac{1}{\hat{\mathcal{N}}}\sum_{i=1}^{\hat{\mathcal{N}}}\mathcal{H}(x_\tau^i)\right] \leq \frac{1}{\hat{\mathcal{N}}}\left[\frac{\tilde{\alpha}}{\tau}+\frac{\tilde{\gamma}}{\sqrt{\tau}}+\tilde{\theta}\right].$$

Putting $\beta = \underline{\sigma}^2/\tilde{\varepsilon}_2^2$ gives the expression (5.2.17) for $\tilde{\varepsilon}_2$ as a function of β, which completes the proof. ■

By employing Theorems 5.2.7 and 5.2.11, we now propose the next theorem as our solution to Problem 5.2.2.

Theorem 5.2.12. *Let $\mathcal{LH}(x)$ be the infinitesimal generator of the process $x(t)$ acting on the function $\mathcal{H}$ at state x and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ be its approximation via the empirical mean as in* (5.2.7)*. By employing the results of Theorems 5.2.7 and 5.2.11, one has*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{H}(x) - \mathcal{LH}(x)| \leq \tilde{\varepsilon}\Big\} \geq 1-\beta, \qquad \forall x \in X,$$

for any $0 < \beta \leq 1$ with $\tilde{\varepsilon} = \tilde{\varepsilon}_1 + \tilde{\varepsilon}_2$, where $\tilde{\varepsilon}_1$ and $\tilde{\varepsilon}_2$ are defined in (5.2.10) *and* (5.2.17)*, respectively.*

Proof. By defining

$$\begin{aligned}
\mathcal{A}_1 &= \{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{LH}(x)| \leq \tilde{\varepsilon}_1\},\\
\mathcal{A}_2 &= \{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq \tilde{\varepsilon}_2\},\\
\mathcal{A} &= \{|\widehat{\mathcal{L}}_2\mathcal{H}(x) - \mathcal{LH}(x)| \leq \tilde{\varepsilon}\},
\end{aligned}$$

one has $\mathbb{P}\{\bar{\mathcal{A}}_1\} = 0$ and $\mathbb{P}\{\bar{\mathcal{A}}_2\} \leq \beta$, where $\bar{\mathcal{A}}_1$ and $\bar{\mathcal{A}}_2$ are the complement of $\mathcal{A}_1$ and $\mathcal{A}_2$, respectively. We are interested in computing the concurrent occurrence of events $\mathcal{A}_1$ and $\mathcal{A}_2$, namely $\mathbb{P}(\mathcal{A}_1 \cap \mathcal{A}_2)$:

$$\mathbb{P}(\mathcal{A}_1 \cap \mathcal{A}_2) = 1 - \mathbb{P}\big(\bar{\mathcal{A}}_1 \cup \bar{\mathcal{A}}_2\big).$$

Since $\mathbb{P}\big(\bar{\mathcal{A}}_1 \cup \bar{\mathcal{A}}_2\big) \leq \mathbb{P}(\bar{\mathcal{A}}_1) + \mathbb{P}(\bar{\mathcal{A}}_2)$, we have

$$\mathbb{P}(\mathcal{A}_1 \cap \mathcal{A}_2) \geq 1 - \mathbb{P}(\bar{\mathcal{A}}_1) - \mathbb{P}(\bar{\mathcal{A}}_2) \geq 1 - \beta. \tag{5.2.18}$$

Due to the triangle inequality, $\mathcal{A}_1 \cap \mathcal{A}_2 \subseteq \mathcal{A}$, and accordingly, $\mathbb{P}\big(\mathcal{A}_1 \cap \mathcal{A}_2\big) \leq \mathbb{P}\big(\mathcal{A}\big)$. Employing (5.2.18), one has

$$\mathbb{P}\big(\mathcal{A}\big) \geq 1 - \beta,$$

which completes the proof. ■

In the next corollary, we present asymptotic properties of our approximation.

Corollary 5.2.13. *Let $\mathcal{LH}(x)$ be the infinitesimal generator of the process $x(t)$ acting on a function $\mathcal{H}$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ be its empirical approximation as in* (5.2.7) *both at state x. The approximated $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ converges to $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ in the mean-square sense if $\tau\hat{\mathcal{N}}$ goes to infinity ($\widehat{\mathcal{L}}_1\mathcal{H}(x)$ converges to $\mathcal{LH}(x)$ if τ goes to zero).*

Remark 5.2.14. *The variance of the empirical mean in* (5.2.16) *has an inverse relation with both the sampling time and the number of data. On the other hand, $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ converges to $\mathcal{LH}(x)$ if τ goes to zero. This means the overall closeness $\tilde{\varepsilon}$ between the infinitesimal generator $\mathcal{LH}(x)$ and its approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ is improved by increasing the number of data $\hat{\mathcal{N}}$ (which is only appears in $\tilde{\varepsilon}_2$). However, since τ appears in both $\tilde{\varepsilon}_1$ and $\tilde{\varepsilon}_2$, decreasing τ does not necessarily improve $\tilde{\varepsilon}$ and its optimal value should be computed to reach the least error.*

If the underlying dynamic is deterministic, one can control the closeness error between Lie derivative $\mathsf{L}\mathcal{H}(x)$ and its approximation $\widehat{\mathsf{L}}\mathcal{H}(x)$ by picking a small sampling time τ (*i.e.,* the approximated Lie derivative converges to the exact one for all initial conditions when the sampling time goes to *zero*). However, in the stochastic setting as this section, both the sampling time and the number of data play significant roles to provide a reasonable closeness precision: $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ converges to $\mathcal{L}\mathcal{H}(x)$ if $\tau\hat{\mathcal{N}}$ goes to *infinity* (cf. Corollary 5.2.13).

5.2.3 Case Study

To illustrate the effectiveness of the proposed results, we apply our approaches to the following temperature regulation:

$$\Sigma\colon \mathsf{d}x(t) = (-\hat{\eta}x(t) + \hat{\eta}T_e)\mathsf{d}t + \sigma\mathsf{d}\mathbb{W}_t,$$

where $\hat{\eta} = 0.001$, $T_e = 8\,^\circ C$, and $\sigma = 0.2$. The temperature of the system varies between $1^\circ\mathsf{C}$ and $5^\circ\mathsf{C}$, *i.e.,* $x \in [1, 5]$.

We fix a quadratic function $\mathcal{H}(x) = x^2$ and aim at computing parameters of Assumptions 5.2.4-5.2.5. Then one has $\mathscr{L}_{\mathcal{H}_1} = 2, \mathscr{L}_{\mathcal{H}_2} = 0, \mathcal{M}_{\mathcal{H}_1} = 10, \mathcal{M}_{\mathcal{H}_2} = 2$. We also assume that $\mathscr{L}_f, \mathcal{M}_f, \mathcal{M}_\sigma, \mathcal{M}_\mathsf{c}, \mathscr{L}_\mathsf{c}$ are given as $\mathscr{L}_f = 0.001, \mathcal{M}_f = 0.007, \mathcal{M}_\sigma = 0.2, \mathcal{M}_\mathsf{c} = 0.04$, and $\mathscr{L}_\mathsf{c} = 0$. We fix $\tau = 1$. Then according to Theorem 5.2.7, one can guarantee that the closeness between $\mathcal{L}\mathcal{H}(x)$ and its first approximation $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ can be bounded by $\tilde{\varepsilon}_1 = 0.0033$, *i.e.,*

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq 0.0033, \qquad \forall x \in X.$$

We now proceed with computing an upper bound for the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ according to Lemma 5.2.10. By selecting $\hat{\mathcal{N}} = 10^7$ and $\mathcal{M}_\mathcal{H} = 25$, one has $\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq 4.8 \times 10^{-7}$. Now according to Theorem 5.2.11, by taking $\beta = 0.01$, we compute the closeness between $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ as $\tilde{\varepsilon}_2 = 0.007$ with a confidence of at least 99%, *i.e.,*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq 0.007\Big\} \geq 0.99, \qquad \forall x \in X.$$

According to Theorem 5.2.12, we formally quantify the closeness between the infinitesimal generator $\mathcal{L}\mathcal{H}(x)$ and its approximation via the empirical mean $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ as $\tilde{\varepsilon} = 0.0103$ with a confidence of at least 99%, *i.e.,*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq 0.0103\Big\} \geq 0.99, \qquad \forall x \in X.$$

In order to have a practical analysis on the proposed closeness bound in Theorem 5.2.12, we fix $\beta = 0.01$ (*i.e.,* confidence is 99%) and plot the closeness $\tilde{\varepsilon}$ based on different ranges of the sampling time τ and number of data $\hat{\mathcal{N}}$ in Figure 5.1. As seen, the closeness $\tilde{\varepsilon}$ between the infinitesimal generator $\mathcal{L}\mathcal{H}(x)$ and its data-driven approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ is improved by increasing the number of data $\hat{\mathcal{N}}$. However, since $\tilde{\varepsilon} = \tilde{\varepsilon}_1 + \tilde{\varepsilon}_2$ and the sampling time τ appears in both $\tilde{\varepsilon}_1$ in (5.2.10) and $\tilde{\varepsilon}_2$ in (5.2.17), the closeness $\tilde{\varepsilon}$ is not

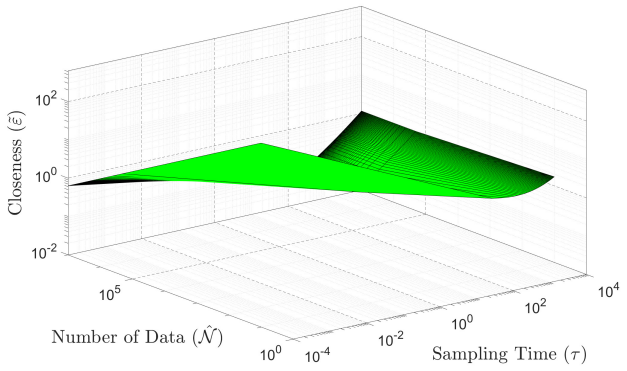

Figure 5.1: Closeness $\tilde{\varepsilon}$ based on different ranges of the sampling time τ and number of data $\hat{\mathcal{N}}$. Plot is in the logarithmic scale.

monotonic for a given confidence $1-\beta$. In other words, decreasing τ does not always improve $\tilde{\varepsilon}$ and its optimal value should be computed to reach the least error.

In order to show that the asymptotic properties of our approximation according to Corollary 5.2.13, we assume that we know the model and compute $\mathcal{LH}(x)$ as

$$\mathcal{LH}(x) = 2x(-\hat{\eta}x + \hat{\eta}T_e) + 0.04,$$

which is clearly independent of the sampling time. We now compute $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ based on (5.2.7). In Figure 5.2, we plot the difference between the exact $\mathcal{LH}(x)$ and its approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ for the same initial condition $x_1(0) = 0.07$ but for different ranges of the sampling time. We compute $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ 500 times with different numbers of data and plot only the maximum of computed values. As can be observed, for the small sampling time (*e.g.,* 10^{-4}), the number of data should be large enough such that $\hat{\mathcal{N}}\tau$ remains large enough, and accordingly, one can provide a reasonable closeness precision between $\mathcal{LH}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$.

5.3 Data-Driven Estimation of Infinitesimal Generators for ct-SHS

In this section, we enlarge the class of models to contentious-time stochastic *hybrid* systems by adding Poisson processes to the dynamics and propose a data-driven approach for the estimation of infinitesimal generator for this class of models. In addition, our data-driven scheme handles stochastic systems with control inputs, while the results of the previous section only deal with stochastic *autonomous* systems. We consider continuous-time stochastic hybrid systems as in Definition 2.3.1 but without internal inputs w and denote it by the tuple $\Sigma = (X, U, \mathcal{U}, f, \sigma, \rho)$ satisfying

$$\Sigma\colon \mathsf{d}x(t) = f(x(t), \nu(t))\mathsf{d}t + \sigma(x(t))\mathsf{d}\mathbb{W}_t + \rho(x(t))\mathsf{d}\mathbb{P}_t, \tag{5.3.1}$$

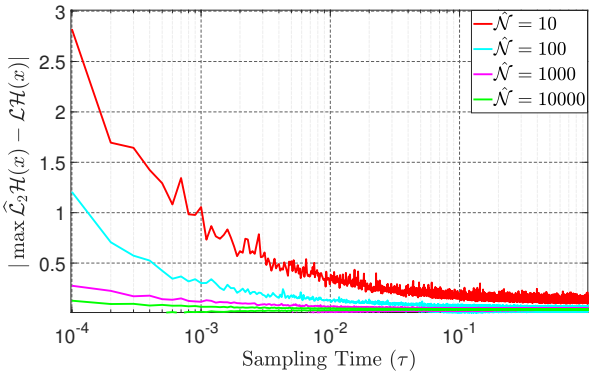

Figure 5.2: Difference between the exact analytical $\mathcal{L}\mathcal{H}(x)$ and its approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ for the same initial condition $x = 0.07$ but different ranges of the sampling time. Plots are in the logarithmic scale in horizontal axis. The computation of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ is repeated 500 times with different numbers of data and only the maximum of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ is plotted.

$\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.) for any $\nu \in \mathcal{U}$, where the stochastic process $x : \Omega \times \mathbb{R}_{\geq 0} \to X$ is called the *solution process* of Σ. Here, we assume that Poisson processes $\mathbb{P}_s^z$, for any $z \in \{1, \ldots, \mathsf{r}\}$, have rates $\bar{\lambda}_z$.

To ensure the existence, uniqueness, and strong Markov property of the solution process [ØS05], we assume that the drift, diffusion, and reset terms are all globally Lipschitz continuous (cf. Assumption 5.3.1). We perform our analysis over X and U which are assumed to be compact subsets of $\mathbb{R}^n$ and $\mathbb{R}^{\bar{m}}$, respectively. This is motivated by boundedness assumptions required for our theoretical results (cf. Assumption 5.3.2).

We study the *infinitesimal generator* $\mathcal{L}$ of the process $x(t)$ acting on a twice continuously-differentiable function $\mathcal{H} : X \to \mathbb{R}$, defined as [Oks13].

$$\begin{aligned}\mathcal{L}\mathcal{H}(x) = \; & \partial_x \mathcal{H}(x) f(x,\nu) + \frac{1}{2}\mathsf{Tr}(\mathsf{c}(x)\partial_{x,x}\mathcal{H}(x)) \\ & + \sum_{j=1}^{\mathsf{r}} \bar{\lambda}_j (\, \mathcal{H}(x + \rho(x)\mathsf{e}_j^{\mathsf{r}}) - \mathcal{H}(x)), \end{aligned} \tag{5.3.2}$$

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

Here, we develop a data-driven scheme to formally quantify $\tilde{\varepsilon} \in \mathbb{R}_{\geq 0}$ as the distance between the infinitesimal generator of ct-SHS in (5.3.2) and its data-driven approximation in (5.2.7) with a priori confidence $\beta \in (0, 1]$ as in (5.2.8). To do so, we first need to raise the following two assumptions.

Assumption 5.3.1. *Suppose $f, \sigma, \rho, \nu(t), \mathsf{c}(x), \mathcal{H}(x), \partial_x\mathcal{H}(x)$, and $\partial_{x,x}\mathcal{H}(x)$ are all Lipschitz continuous with, respectively, Lipschitz constants $\mathscr{L}_f, \mathscr{L}_\nu, \mathscr{L}_\sigma, \mathscr{L}_\rho, \bar{\mathscr{L}}_\nu, \mathscr{L}_{\mathsf{c}}, \mathscr{L}_{\mathcal{H}}, \mathscr{L}_{\mathcal{H}_1}$,*

$\mathscr{L}_{\mathcal{H}_2} \in \mathbb{R}_{\geq 0}$ as the following, $\forall x, x' \in X$, $\forall \nu, \nu' \in U$, $\forall t, t' \in \mathbb{R}_{\geq 0}$:

$$\begin{aligned}
&\|f(x,\nu) - f(x',\nu')\| \leq \mathscr{L}_f \|x - x'\| + \mathscr{L}_\nu \|\nu - \nu'\|,\\
&\|\sigma(x) - \sigma(x')\|_F \leq \mathscr{L}_\sigma \|x - x'\|, \quad \|\rho(x) - \rho(x')\|_F \leq \mathscr{L}_\rho \|x - x'\|,\\
&\|\nu(t) - \nu(t')\| \leq \bar{\mathscr{L}}_\nu |t - t'|, \quad \|\mathsf{c}(x) - \mathsf{c}(x')\|_F \leq \mathscr{L}_\mathsf{c} \|x - x'\|,\\
&|\mathcal{H}(x) - \mathcal{H}(x')| \leq \mathscr{L}_\mathcal{H} \|x - x'\|, \quad \|\partial_x \mathcal{H}(x) - \partial_{x'} \mathcal{H}(x')\| \leq \mathscr{L}_{\mathcal{H}_1} \|x - x'\|,\\
&\|\partial_{x,x} \mathcal{H}(x) - \partial_{x',x'} \mathcal{H}(x')\|_F \leq \mathscr{L}_{\mathcal{H}_2} \|x - x'\|.
\end{aligned}$$

Assumption 5.3.2. *Suppose $f(x)$, $\mathsf{c}(x)$, $\sigma(x)$, $\rho(x)$, $\mathcal{H}(x)$, $\partial_x \mathcal{H}(x)$, and $\partial_{x,x} \mathcal{H}(x)$ are all bounded with constants $\mathcal{M}_f$, $\mathcal{M}_\mathsf{c}, \mathcal{M}_\sigma, \mathcal{M}_\rho, \mathcal{M}_\mathcal{H}, \mathcal{M}_{\mathcal{H}_1}, \mathcal{M}_{\mathcal{H}_2} \in \mathbb{R}_{\geq 0}$ as, $\forall x \in X, \forall \nu \in U$:*

$$\begin{aligned}
&\|f(x,\nu)\| \leq \mathcal{M}_f, \|\mathsf{c}(x)\|_F \leq \mathcal{M}_\mathsf{c}, \|\sigma(x)\|_F \leq \mathcal{M}_\sigma, \|\rho(x)\|_F \leq \mathcal{M}_\rho,\\
&|\mathcal{H}(x)| \leq \mathcal{M}_\mathcal{H}, \ \|\partial_x \mathcal{H}(x)\| \leq \mathcal{M}_{\mathcal{H}_1}, \ \|\partial_{x,x} \mathcal{H}(x)\|_F \leq \mathcal{M}_{\mathcal{H}_2}.
\end{aligned}$$

By leveraging Assumptions 5.3.1-5.3.2, we propose next result showing that $\mathcal{LH}(x)$ is also Lipschitz continuous.

Lemma 5.3.3. *Under Assumptions 5.3.1-5.3.2, $\mathcal{LH}(x)$ is Lipschitz continuous with Lipschitz constants $\mathscr{L}_1, \mathscr{L}_2 \in \mathbb{R}_{\geq 0}$:*

$$|\mathcal{LH}(x) - \mathcal{LH}(x')| \leq \mathscr{L}_1 \|x - x'\| + \mathscr{L}_2 \|\nu - \nu'\|,$$

for all $x, x' \in X$ and all $\nu, \nu' \in U$, where

$$\begin{aligned}
\mathscr{L}_1 =& \ \mathcal{M}_{\mathcal{H}_1} \mathscr{L}_f + \mathcal{M}_f \mathscr{L}_{\mathcal{H}_1} + \frac{1}{2}(\mathscr{L}_\mathsf{c} \mathcal{M}_{\mathcal{H}_2} + \mathcal{M}_\mathsf{c} \mathscr{L}_{\mathcal{H}_2}) + \sum_{j=1}^{r} \bar{\lambda}_j (2\mathscr{L}_\mathcal{H} + \mathscr{L}_\mathcal{H} \mathscr{L}_\rho),\\
\mathscr{L}_2 =& \ \mathcal{M}_{\mathcal{H}_1} \mathscr{L}_\nu.
\end{aligned}$$

Proof: Using the definition of $\mathcal{LH}(x)$ in (5.3.2), we have

$$\begin{aligned}
&|\mathcal{LH}(x) - \mathcal{LH}(x')| \leq |\partial_x \mathcal{H}(x) f(x,\nu) - \partial_{x'} \mathcal{H}(x') f(x',\nu')|\\
&+ |\frac{1}{2} \mathsf{Tr}\big(\mathsf{c}(x) \partial_{x,x} \mathcal{H}(x) - \mathsf{c}(x') \partial_{x',x'} \mathcal{H}(x')\big)| + |\sum_{j=1}^{r} \bar{\lambda}_j \big(\mathcal{H}(x + \rho(x) \mathsf{e}_j^r) - (\mathcal{H}(x' + \rho(x') \mathsf{e}_j^r)\big)|\\
&+ |\sum_{j=1}^{r} \bar{\lambda}_j (\mathcal{H}(x) - \mathcal{H}(x'))|. \qquad (5.3.3)
\end{aligned}$$

Using the following inequality

$$|\mathbb{A}^T \mathbb{B} - \mathbb{C}^T \mathbb{D}| \leq \|\mathbb{A}\| \|\mathbb{B} - \mathbb{D}\| + \|\mathbb{D}\| \|\mathbb{A} - \mathbb{C}\|,$$

for all $\mathbb{A}, \mathbb{B}, \mathbb{C}, \mathbb{D} \in \mathbb{R}^n$, and Assumptions 5.3.1-5.3.2, the first term in the right-hand side of (5.3.3) is upper bounded by

$$\begin{aligned}
&\|\partial_x \mathcal{H}(x)\| \|f(x,\nu) - f(x',\nu')\| + \|f(x',\nu')\| \|\partial_x \mathcal{H}(x) - \partial_{x'} \mathcal{H}(x')\|\\
&\leq \mathcal{M}_{\mathcal{H}_1} (\mathscr{L}_f \|x - x'\| + \mathscr{L}_\nu \|\nu - \nu'\|) + \mathcal{M}_f \mathscr{L}_{\mathcal{H}_1} \|x - x'\|.
\end{aligned}$$

Using the notation $\mathbb{A} \odot \mathbb{B}$ as the Hadamard product of two matrices $\mathbb{A}, \mathbb{B}$, the second term in the right-hand side of (5.3.3) is upper bounded as

$$
\begin{aligned}
&\frac{1}{2}\Big|\sum_{i,j}[\mathsf{c}(x)\odot\partial_{x,x}\mathcal{H}(x)]_{i,j}-[\mathsf{c}(x')\odot\partial_{x',x'}\mathcal{H}(x')]_{i,j}\Big|\\
&\leq\frac{1}{2}\sum_{i,j}\Big|[(\mathsf{c}(x)-\mathsf{c}(x'))\odot\partial_{x,x}\mathcal{H}(x)]_{i,j}\Big|+\frac{1}{2}\sum_{i,j}\Big|[\mathsf{c}(x')\odot(\partial_{x,x}\mathcal{H}(x)-\partial_{x',x'}\mathcal{H}(x'))]_{i,j}\Big|\\
&\leq\frac{1}{2}\Big[\sum_{i,j}\Big|[\mathsf{c}(x)-\mathsf{c}(x')]_{i,j}^2\sum_{i,j}[\partial_{x,x}\mathcal{H}(x)]_{i,j}^2\Big]^{\frac{1}{2}}+\frac{1}{2}\Big[\sum_{i,j}[\mathsf{c}(x')]_{i,j}^2\sum_{i,j}[\partial_{x,x}\mathcal{H}(x)-\partial_{x',x'}\mathcal{H}(x')]_{i,j}^2\Big]^{\frac{1}{2}}\\
&=\frac{1}{2}\|\mathsf{c}(x)-\mathsf{c}(x')\|_F\|\partial_{x,x}\mathcal{H}(x)\|_F+\frac{1}{2}\|\mathsf{c}(x')\|_F\|\partial_{x,x}\mathcal{H}(x)-\partial_{x',x'}\mathcal{H}(x'))\|_F\\
&\leq\frac{1}{2}(\mathscr{L}_{\mathsf{c}}\mathcal{M}_{\mathcal{H}_2}+\mathcal{M}_{\mathsf{c}}\mathscr{L}_{\mathcal{H}_2})\|x-x'\|.
\end{aligned}
$$

Since $\mathcal{H}(x)$ is Lipschitz continuous according to Assumption 5.3.1, two last terms in the right-hand side of (5.3.3) are upper bounded as

$$
\begin{aligned}
&\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j\big(\mathscr{L}_{\mathcal{H}}\|x-x'+\rho(x)\mathsf{e}_j^{\mathsf{r}}-\rho(x')\mathsf{e}_j^{\mathsf{r}}\|+\mathscr{L}_{\mathcal{H}}\|x-x'\|\big)\\
&\leq\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j\big(\mathscr{L}_{\mathcal{H}}(\|x-x'\|+\|\rho(x)-\rho(x')\|_F\|\mathsf{e}_j^{\mathsf{r}}\|)+\mathscr{L}_{\mathcal{H}}\|x-x'\|\big)\\
&\leq\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j\big(\mathscr{L}_{\mathcal{H}}(\|x-x'\|+\mathscr{L}_{\rho}\|x-x'\|)+\mathscr{L}_{\mathcal{H}}\|x-x'\|\big)\\
&=\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j\big(2\mathscr{L}_{\mathcal{H}}+\mathscr{L}_{\mathcal{H}}\mathscr{L}_{\rho}\big)\|x-x'\|.
\end{aligned}
$$

Combining the three upper bounds completes the proof. ■

Now as the first step, we formally quantify the closeness between $\mathcal{L}\mathcal{H}(x)$ and its first approximation $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ in the following theorem.

Theorem 5.3.4. *Under Assumptions 5.3.1-5.3.2 and Lemma 5.3.3, one has*

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x)-\mathcal{L}\mathcal{H}(x)|\leq\tilde{\varepsilon}_1,\quad\forall x\in X,$$

where:

$$\tilde{\varepsilon}_1:=\mathscr{L}_1\big(\frac{1}{2}(\mathcal{M}_f+\mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j)\tau+\frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\big)+\frac{\tau}{2}\mathscr{L}_2\bar{\mathscr{L}}_\nu.\tag{5.3.4}$$

Proof: Using Dynkin's formula in (5.2.5) and by considering the definition of $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ in (5.2.6), one has

$$\widehat{\mathcal{L}}_1\mathcal{H}(x)=\mathbb{E}\Big[\frac{1}{\tau}\int_0^\tau\mathcal{L}\mathcal{H}(x(t))\mathsf{d}t\Big],$$

where $x := x(0)$. By subtracting $\mathcal{LH}(x)$ from two sides:

$$\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{LH}(x) = \mathbb{E}\Big[\frac{1}{\tau}\int_0^\tau \big(\mathcal{LH}(x(t)) - \mathcal{LH}(x)\big)\mathsf{d}t\Big].$$

Consequently,

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{LH}(x)| \leq \frac{1}{\tau}\int_0^\tau \mathbb{E}\Big[|\mathcal{LH}(x(t)) - \mathcal{LH}(x)|\Big]\mathsf{d}t.$$

By employing Lemma 5.3.3, one has

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{LH}(x)| \leq \frac{1}{\tau}\int_0^\tau \mathbb{E}\Big[\mathscr{L}_1\|x(t) - x\| + \mathscr{L}_2\|\nu(t) - \nu\|\Big]\mathsf{d}t,$$

with $u := u(0)$. Since $\|\nu(t) - \nu(t')\| \leq \bar{\mathscr{L}_\nu}|t - t'|$:

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{LH}(x)| \leq \frac{\mathscr{L}_1}{\tau}\int_0^\tau \mathbb{E}\Big[\|x(t) - x\|\Big]\mathsf{d}t + \frac{\tau}{2}\mathscr{L}_2\bar{\mathscr{L}_\nu}. \tag{5.3.5}$$

Now we aim at finding an upper bound for $\mathbb{E}\Big[\|x(t)-x\|\Big]$. Under the continuity property of the solution process of the system, we have

$$x(t) = x + \int_0^t f(x(s),\nu(s))\mathsf{d}s + \int_0^t \sigma(x(s))\mathsf{d}\mathbb{W}_s + \sum_{j=1}^{\mathsf{r}}\sum_{i=1}^{\mathbb{P}_t^j}\rho(x_{s_i})\mathsf{e}_j^{\mathsf{r}}, \tag{5.3.6}$$

where $\mathbb{P}_t = [\mathbb{P}_t^1; \cdots; \mathbb{P}_t^{\mathsf{r}}]$ is the Poisson process with r events and x_{s_i} is the solution process of the system that jumps at times s_i. Then, one obtains

$$\begin{aligned}\mathbb{E}\Big[\|x(t) - x\|\Big] &= \mathbb{E}\Big[\|\int_0^t f(x(s),\nu(s))\mathsf{d}s + \int_0^t \sigma(x(s))\mathsf{d}\mathbb{W}_s + \sum_{j=1}^{\mathsf{r}}\sum_{i=1}^{\mathbb{P}_t^j}\rho(x_{s_i})\mathsf{e}_j^{\mathsf{r}}\|\Big] \\ &\leq \mathbb{E}\Big[\|\int_0^t f(x(s),\nu(s))\mathsf{d}s\| + \|\int_0^t \sigma(x(s))\mathsf{d}\mathbb{W}_s\| + |\sum_{j=1}^{\mathsf{r}}\sum_{i=1}^{\mathbb{P}_t^j}\rho(x_{s_i})\mathsf{e}_j^{\mathsf{r}}|\Big].\end{aligned}$$

According to Jensen's inequality, for any vector $\mathsf{r} \in \mathbb{R}^n$, $\mathbb{E}[\|\mathsf{r}\|] \leq \sqrt{\mathbb{E}[\mathsf{r}^T\mathsf{r}]}$. Then,

$$\begin{aligned}\mathbb{E}\Big[\|x(t) - x\|\Big] \leq& \Big[\mathbb{E}\big[\int_0^t f(x(s),\nu(s))^T\mathsf{d}s\int_0^t f(x(s),\nu(s))\mathsf{d}s\big]\Big]^{\frac{1}{2}} \\ &+ \Big[\mathbb{E}\big[\int_0^t \sigma(x(s))^T\mathsf{d}\mathbb{W}_s^T\int_0^t \sigma(x(s))\mathsf{d}\mathbb{W}_s\big]\Big]^{\frac{1}{2}} + \mathbb{E}\Big[\sum_{j=1}^{\mathsf{r}}\sum_{i=1}^{\mathbb{P}_t^j}\|\rho(x_{s_i})\|\|\mathsf{e}_j^{\mathsf{r}}\|\Big].\end{aligned} \tag{5.3.7}$$

Under Assumption 5.3.2, the first term in the right-hand side of (5.3.7) is upper bounded by

$$\Big[\mathbb{E}\big[\int_0^t\int_0^t \|f(x(s_1),\nu(s_1))\|\|f(x(s_2),\nu(s_2))\|\mathsf{d}s_1\mathsf{d}s_2\big]\Big]^{\frac{1}{2}} \leq \mathcal{M}_f t. \tag{5.3.8}$$

In addition, using the multivariate version of the Itô isometry property [Oks13] and Assumption 5.3.2, one can bound the second term in the right-hand side of (5.3.7) as

$$\Big[\int_0^t \mathbb{E}\Big[\|\sigma(x(s))\|_F^2\Big]\mathsf{d}s\Big]^{\frac{1}{2}} \leq \mathcal{M}_\sigma\sqrt{t}. \tag{5.3.9}$$

Moreover,

$$\mathbb{E}\Big[\sum_{j=1}^{\mathsf{r}}\sum_{i=1}^{\mathbb{P}_t^j}\|\rho(x_{s_i})\|\|\mathsf{e}_j^{\mathsf{r}}\|\Big] \leq \mathbb{E}\Big[\sum_{j=1}^{\mathsf{r}}\sum_{i=1}^{\mathbb{P}_t^j}\mathcal{M}_\rho\Big] = \mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\mathbb{E}\big[\mathbb{P}_t^j\big] \leq \mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j t. \tag{5.3.10}$$

By substituting (5.3.8)-(5.3.10) in (5.3.7), one has

$$\mathbb{E}\Big[\|x(t)-x\|\Big] \leq \mathcal{M}_f t + \mathcal{M}_\sigma\sqrt{t} + \mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j t. \tag{5.3.11}$$

Consequently, by substituting (5.3.11) in (5.3.5), one has

$$\begin{aligned}|\widehat{\mathcal{L}}_1\mathcal{H}(x)-\mathcal{L}\mathcal{H}(x)| &\leq \frac{\mathscr{L}_1}{\tau}\int_0^\tau(\mathcal{M}_f t+\mathcal{M}_\sigma\sqrt{t}+\mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j t)\mathsf{d}t + \frac{\tau}{2}\mathscr{L}_2\bar{\mathscr{L}}_\nu\\ &= \mathscr{L}_1\big(\frac{1}{2}(\mathcal{M}_f+\mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j)\tau+\frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\big)+\frac{\tau}{2}\mathscr{L}_2\bar{\mathscr{L}}_\nu,\end{aligned}$$

which completes the proof. ■

Remark 5.3.5. *If input signal ν is piece-wise constant of duration τ instead of being Lipschitz continuous, the error term contributed by ν in our setting will be zero. Accordingly, the bound $\tilde{\varepsilon}_1$ in* (5.3.4) *is reduced to* $\tilde{\varepsilon}_1 := \mathscr{L}_1\big(\frac{1}{2}(\mathcal{M}_f+\mathcal{M}_\rho\sum_{j=1}^{r}\bar{\lambda}_j)\tau+\frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\big)$.

As the second step, we now quantify the closeness between $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$. To do so, we first formulate a bound on the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ in the next theorem.

Theorem 5.3.6. *Under Assumptions 5.3.1-5.3.2 and Lemma 5.3.3, the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ in* (5.2.7) *is bounded by*

$$\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq \frac{1}{\hat{\mathcal{N}}}[\frac{\tilde{\alpha}}{\tau}+\frac{\tilde{\gamma}}{\sqrt{\tau}}+\tilde{\theta}], \tag{5.3.12}$$

for some $\tilde{\alpha},\tilde{\gamma},\tilde{\theta}\in\mathbb{R}_{\geq 0}$.

Proof: Since $(x_\tau^i)_{i=1}^{\hat{\mathcal{N}}}$ is $\hat{\mathcal{N}}$ i.i.d. sampled data by extracting $\hat{\mathcal{N}}$ solution processes $x_\tau^i, i \in \{1, \ldots, \hat{\mathcal{N}}\}$, at time τ from the same initial condition under $\hat{\mathcal{N}}$ different independent noise realizations, we compute the variance of empirical mean as

$$\begin{aligned}
&\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) = \frac{1}{\tau^2\hat{\mathcal{N}}}\mathsf{Var}(\mathcal{H}(x_\tau^i)) = \frac{1}{\tau^2\hat{\mathcal{N}}}\Big[\mathbb{E}[\mathcal{H}(x_\tau^i)^2] - \mathbb{E}[\mathcal{H}(x_\tau^i)]^2\Big] \\
&= \frac{1}{\tau^2\hat{\mathcal{N}}}\Big[\mathbb{E}[\mathcal{H}(x_\tau^i)^2] - \mathcal{H}(x)^2 - \mathbb{E}[\mathcal{H}(x_\tau^i)]^2 + \mathcal{H}(x)^2\Big] \\
&= \frac{1}{\tau\hat{\mathcal{N}}}\Big[\frac{\mathbb{E}[\mathcal{H}(x_\tau^i)^2] - \mathcal{H}(x)^2}{\tau}\Big] - \frac{1}{\tau\hat{\mathcal{N}}}\frac{[\mathbb{E}[\mathcal{H}(x_\tau^i)] - \mathcal{H}(x)][\mathbb{E}[\mathcal{H}(x_\tau^i)] + \mathcal{H}(x)]}{\tau} \\
&= \frac{1}{\tau\hat{\mathcal{N}}}\widehat{\mathcal{L}}_1\mathcal{H}(x)^2 - \frac{1}{\tau\hat{\mathcal{N}}}\widehat{\mathcal{L}}_1\mathcal{H}(x)(\mathbb{E}[\mathcal{H}(x_\tau^i)] + \mathcal{H}(x)).
\end{aligned}$$

Similar to (5.3.4), one can also quantify the distance between $\widehat{\mathcal{L}}_1\mathcal{H}(x)^2$ and $\mathcal{L}\mathcal{H}(x)^2$ as $|\widehat{\mathcal{L}}_1\mathcal{H}(x)^2 - \mathcal{L}\mathcal{H}(x)^2| \leq \bar{\varepsilon}_1$, where

$$\bar{\varepsilon}_1 := \bar{\mathscr{L}}_1\big(\frac{1}{2}(\mathcal{M}_f + \mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j)\tau + \frac{2}{3}\mathcal{M}_\sigma\sqrt{\tau}\big) + \frac{\tau}{2}\bar{\mathscr{L}}_2\bar{\mathscr{L}}_\nu,$$

with

$$\begin{aligned}
\bar{\mathscr{L}}_1 &= \bar{\mathcal{M}}_{\mathcal{H}_1}\mathscr{L}_f + \mathcal{M}_f\bar{\mathscr{L}}_{\mathcal{H}_1} + \frac{1}{2}(\mathscr{L}_{\mathsf{c}}\bar{\mathcal{M}}_{\mathcal{H}_2} + \mathcal{M}_{\mathsf{c}}\bar{\mathscr{L}}_{\mathcal{H}_2}) + \sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j(2\bar{\mathscr{L}}_{\mathcal{H}} + \bar{\mathscr{L}}_{\mathcal{H}}\mathscr{L}_\rho), \\
\bar{\mathscr{L}}_2 &= \bar{\mathcal{M}}_{\mathcal{H}_1}\mathscr{L}_\nu,
\end{aligned}$$

where $\bar{\mathcal{B}}_{\mathcal{H}_1}, \bar{\mathcal{B}}_{\mathcal{H}_2}, \bar{\mathscr{L}}_{\mathcal{H}}, \bar{\mathscr{L}}_{\mathcal{H}_1}, \bar{\mathscr{L}}_{\mathcal{H}_2}$ are constants similar to the ones in Assumptions 5.3.1-5.3.2 but for $\mathcal{H}(x)^2$. These constants can be readily obtained using $\mathcal{M}_{\mathcal{H}_1}, \mathcal{M}_{\mathcal{H}_2}, \mathscr{L}_{\mathcal{H}}, \mathscr{L}_{\mathcal{H}_1}, \mathscr{L}_{\mathcal{H}_2}$. Then,

$$\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq \frac{1}{\tau\hat{\mathcal{N}}}\big((\mathcal{L}\mathcal{H}(x)^2 + \bar{\varepsilon}_1) - (\mathcal{L}\mathcal{H}(x) - \bar{\varepsilon}_1)2\mathcal{M}_{\mathcal{H}}\big).$$

Accordingly, one has

$$\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq \frac{\tilde{\alpha} + \tilde{\gamma}\sqrt{\tau} + \tilde{\theta}\tau}{\tau\hat{\mathcal{N}}} = \frac{1}{\hat{\mathcal{N}}}[\frac{\tilde{\alpha}}{\tau} + \frac{\tilde{\gamma}}{\sqrt{\tau}} + \tilde{\theta}],$$

with $\tilde{\alpha}$ satisfying $|\mathcal{L}\mathcal{H}(x)^2 - 2\mathcal{M}_{\mathcal{H}}\mathcal{L}\mathcal{H}(x)| \leq \tilde{\alpha}, \forall x \in X$, and

$$\begin{aligned}
\tilde{\gamma} &:= \frac{2}{3}\mathcal{M}_\sigma(\bar{\mathscr{L}}_1 + 2\mathcal{M}_{\mathcal{H}}\mathscr{L}_1), \\
\tilde{\theta} &:= \frac{1}{2}((\mathcal{M}_f + \mathcal{M}_\rho\sum_{j=1}^{\mathsf{r}}\bar{\lambda}_j)(\bar{\mathscr{L}}_1 + 2\mathcal{M}_{\mathcal{H}}\mathscr{L}_1) + (\bar{\mathscr{L}}_2\bar{\mathscr{L}}_\nu + 2\mathcal{M}_{\mathcal{H}}\mathscr{L}_2\bar{\mathscr{L}}_\nu)).
\end{aligned}$$

Note that $\tilde{\alpha}$ can be computed using parameters of Assumptions 5.3.1-5.3.2, and this completes the proof. ■

In the next theorem, we employ Chebyshev's inequality [SYM84] and quantify the mismatch between approximated values of the infinitesimal generator in (5.2.6) and (5.2.7) by providing an a-priori confidence bound.

Theorem 5.3.7. *Let $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ be approximations of the infinitesimal generator $\mathcal{L}\mathcal{H}(x)(x)$ based on the expected value and empirical approximation as in* (5.2.6) *and* (5.2.7)*, respectively. For any $\beta \in (0,1]$, we have*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq \tilde{\varepsilon}_2\Big\} \geq 1-\beta, \quad \forall x \in X,$$

with

$$\tilde{\varepsilon}_2 := \big[\frac{1}{\beta\hat{\mathcal{N}}}\big(\frac{\tilde{\alpha}}{\tau} + \frac{\tilde{\gamma}}{\sqrt{\tau}} + \tilde{\theta}\big)\big]^{\frac{1}{2}}. \tag{5.3.13}$$

The proof is similar to that of Theorem 5.2.11 and is omitted here.

By leveraging Theorems 5.3.4 and 5.3.7, we now propose the next theorem as our solution to Problem 5.2.2 for the formal quantification of the closeness between the infinitesimal generator $\mathcal{L}\mathcal{H}(x)$ and its data-driven approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$.

Theorem 5.3.8. *Let $\mathcal{L}\mathcal{H}(x)$ be the infinitesimal generator of the stochastic process $x(t)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ be its approximation via the empirical mean as in* (5.2.7)*. By employing the results of Theorems 5.3.4 and 5.3.7, one has*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq \tilde{\varepsilon}\Big\} \geq 1-\beta, \quad \forall x \in X,$$

for any $\beta \in (0,1]$ with $\tilde{\varepsilon} = \tilde{\varepsilon}_1 + \tilde{\varepsilon}_2$, where $\tilde{\varepsilon}_1$ and $\tilde{\varepsilon}_2$ are defined in (5.3.4) *and* (5.3.13)*, respectively.*

The proof is similar to that of Theorem 5.2.12 and is omitted here.

5.3.1 Case Study: Jet Engine Compressor

To demonstrate the effectiveness of the proposed results, we apply our data-driven approaches to a *nonlinear* jet engine compressor [AT10]:

$$\Sigma : \begin{bmatrix} \mathsf{d}x_1(t) \\ \mathsf{d}x_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) - \nu(t) \end{bmatrix} \mathsf{d}t + \begin{bmatrix} 0.1\mathsf{d}\mathbb{W}_t \\ 0.1\mathsf{d}\mathbb{W}_t \end{bmatrix} + \begin{bmatrix} 0.1\mathsf{d}\mathbb{P}_t \\ 0.1\mathsf{d}\mathbb{P}_t \end{bmatrix},$$

where $x_1 = \bar{\Phi} - 1, x_2 = \bar{\Psi} - \bar{\Lambda} - 2$, with $\bar{\Phi}, \bar{\Psi}, \bar{\Lambda}$ being, respectively, the mass flow, the pressure rise, and a constant. We assume that the model is unknown to us. In addition, the controller is also unknown and we only have its Lipschitz constant as $\bar{\mathscr{L}}_\nu = 1.12$.

We fix $\mathcal{H}(x) = 0.01x_1^2 + 0.02x_1x_2 + 0.01x_2^2$, and compute parameters of Assumptions 5.3.1-5.3.2. Then one has $\mathscr{L}_\mathcal{H} = 0.056, \mathscr{L}_{\mathcal{H}_1} = 0.04, \mathscr{L}_{\mathcal{H}_2} = 0, \mathcal{M}_\mathcal{H} = 0.04, \mathcal{M}_{\mathcal{H}_1} = 0.056, \mathcal{M}_{\mathcal{H}_2} = 0.04$. We also assume that $\mathscr{L}_f = 4.7, \mathscr{L}_u = 1, \mathscr{L}_c = 0, \mathcal{M}_f = 3.08, \mathcal{M}_\mathsf{c} = 0.014, \mathcal{M}_\sigma = 0.14$, and $\mathcal{M}_\rho = 0.14$. We fix $\tau = 0.01$. Then according to Theorem 5.3.4, one can guarantee that the closeness between $\mathcal{L}\mathcal{H}(x)$ and its first approximation $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ can be bounded by $\tilde{\varepsilon}_1 = 0.01$, *i.e.,*

$$|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq 0.01, \quad \forall x \in X.$$

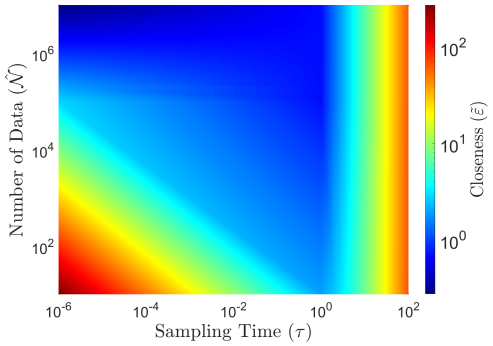

Figure 5.3: Closeness $\tilde{\varepsilon}$, represented by 'colour bar', based on different ranges of the sampling time τ and number of data $\hat{\mathcal{N}}$. As it can be observed, for a fixed number of $\hat{\mathcal{N}}$, the total error $\tilde{\varepsilon}$ first decreases for $\tau \in [10^{-6}, 10^{0}]$ and again increases for $\tau \in [10^{0}, 10^{2}]$.

We now proceed with computing an upper bound for the variance of $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ according to Theorem 5.3.6. By selecting $\hat{\mathcal{N}} = 10^5$, one has $\mathsf{Var}(\widehat{\mathcal{L}}_2\mathcal{H}(x)) \leq 9.5 \times 10^{-6}$. Now according to Theorem 5.3.7, by taking $\beta = 0.01$, we compute the closeness between $\widehat{\mathcal{L}}_1\mathcal{H}(x)$ and $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ as $\tilde{\varepsilon}_2 = 0.03$ with a confidence of at least 99%, *i.e.,*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_1\mathcal{H}(x) - \widehat{\mathcal{L}}_2\mathcal{H}(x)| \leq 0.03\Big\} \geq 0.99, \quad \forall x \in X.$$

According to Theorem 5.3.8, we formally quantify the closeness between the infinitesimal generator $\mathcal{L}\mathcal{H}(x)$ and its approximation via the empirical mean $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ as $\tilde{\varepsilon} = 0.04$ with a confidence of at least 99%, *i.e.,*

$$\mathbb{P}\Big\{|\widehat{\mathcal{L}}_2\mathcal{H}(x) - \mathcal{L}\mathcal{H}(x)| \leq 0.04\Big\} \geq 0.99, \quad \forall x \in X.$$

We fix $\beta = 0.01$ (*i.e.,* confidence is 99%) and plot the closeness $\tilde{\varepsilon}$ based on different ranges of the sampling time τ and number of data $\hat{\mathcal{N}}$ in Fig. 5.3. As it can be observed, the closeness $\tilde{\varepsilon}$ between the infinitesimal generator $\mathcal{L}\mathcal{H}(x)$ and its approximation $\widehat{\mathcal{L}}_2\mathcal{H}(x)$ is improved by increasing the number of data $\hat{\mathcal{N}}$. However, since $\tilde{\varepsilon} = \tilde{\varepsilon}_1 + \tilde{\varepsilon}_2$ and the sampling time τ appears in both $\tilde{\varepsilon}_1$ in (5.3.4) and $\tilde{\varepsilon}_2$ in (5.3.13), the closeness $\tilde{\varepsilon}$ is not monotonic for a given confidence $1 - \beta$.

5.4 Data-Driven Verification of Unknown Discrete- and Continuous-Time Systems

In this section, we provide a data-driven scheme for the construction of barrier certificates for the safety verification of unknown discrete- and continuous-time systems. In our proposed settings, we first formulate our original safety problem as a robust convex program (RCP). Since the formulated RCP is not tractable due to unknown dynamics,

we consider a given set of data collected from the system and provide a scenario convex program (SCP) corresponding to the original RCP. Accordingly, by establishing a probabilistic closeness between the optimal value of SCP and that of RCP, we quantify the safety guarantee of unknown systems based on the number of data and the required level of the safety confidence. In order to establish a probabilistic relation between optimal values of SCP and RCP, we first raise some Lipschitz continuity assumptions over RCP's conditions. We provide some explicit approaches to compute the required Lipschitz constants. To demonstrate the effectiveness of the proposed results, we apply our approaches to three physical systems with unknown dynamics: (i) continuous-time room temperature system, (ii) continuous-time *nonlinear* jet engine compressor, and (iii) discrete-time DC motor. We utilize data collected from trajectories of systems and verify that states of unknown systems stay in some safe sets with an a-priori desired confidence. A graphical representation of the structure of this section and its contributions is illustrated in Fig. 5.4.

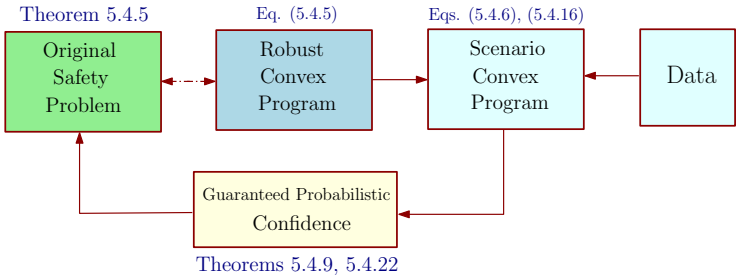

Figure 5.4: A graphical representation of the section's structure and contributions.

In is worth mentioning that scenario-based optimization techniques have been also used for the controller design in [CGP09]. However, the proposed results in [CGP09] only relate optimal values of scenario and chance-constrained programs, and accordingly, provide guarantees over chance-constrained programs. In contrast, we transfer here the safety guarantees over the original robust program (which is the main problem in our setting) but at the cost of taking into account the Lipschitz constant of the system, and consequently, requiring much more sampled data. The work in [GBSV$^+$19] proposes a specification-based simulation metric to synthesize a controller from an abstraction of the system which is learned from data. In contrast, we propose here a data-driven approach to directly provide a formal guarantee over the safety of unknown systems without performing any system identification. The work in [LHR$^+$20, RHL$^+$20] proposes an optimization-based framework to learn control barrier functions from data for the systems with *known* dynamics and under the assumption of accessibility of safe trajectories generated by an expert. Whereas in our setting, we develop data-driven approaches to guarantee safety of systems with (partially) unknown dynamics.

5.4.1 Discrete-Time Dynamical Systems

We consider discrete-time dynamical systems (dt-S) as defined in the following.

Definition 5.4.1. *A discrete-time dynamical system (dt-S) is represented by*

$$\Sigma_d \colon x(k+1) = f(x(k)), \quad k \in \mathbb{N}, \tag{5.4.1}$$

where $x : \mathbb{N} \to X$ is the state evolution *of Σ_d, $X \subseteq \mathbb{R}^n$ is the state set of the system, and $f : X \to \mathbb{R}^n$ is a function characterizing the state evolution of the system. We employ $x_{x_0}(k)$ to denote the value of the state evolution at time $k \in \mathbb{N}$ started from an initial condition $x_0 = x(0)$.*

In the next subsection, we provide a formal definition of barrier certificates for discrete-time dynamical systems as in (5.4.1).

5.4.2 Barrier Certificates (BC)

Definition 5.4.2. *Consider a dt-S Σ_d, and $X_0, X_u \subseteq X$ as initial and unsafe sets, respectively. A function $\mathcal{B} : X \to \mathbb{R}$ is called a barrier certificate (BC) for Σ_d over a time horizon $[0, \mathcal{T})$ if there exist $\psi \in \mathbb{R}_{\geq 0}$ and $\gamma, \lambda \in \mathbb{R}$, such that $\gamma + \psi\mathcal{T} < \lambda$, and*

$$\mathcal{B}(x) \leq \gamma, \qquad \forall x \in X_0, \tag{5.4.2}$$
$$\mathcal{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{5.4.3}$$
$$\mathcal{B}(f(x)) \leq \mathcal{B}(x) + \psi, \qquad \forall x \in X. \tag{5.4.4}$$

Remark 5.4.3. *Note that since $\gamma + \psi\mathcal{T} < \lambda$ in Definition 5.4.2, one can readily see that $\mathcal{T} < \frac{\lambda - \gamma}{\psi}$, i.e., time horizon $\mathcal{T}$ converges to infinity once c goes to zero.*

In the next definition, we present the safety problem for dt-S Σ_d.

Definition 5.4.4. *Given a safety specification $\varphi = (X_0, X_u, \mathcal{T})$, where $X_0, X_u \subseteq X$ and $\mathcal{T} \in \mathbb{N} \cup \{\infty\}$, and a dt-S Σ_d, Σ_d is called safe within (in)finite time horizon $\mathcal{T}$, denoted by $\Sigma_d \models_{\mathcal{T}} \varphi$, if all trajectories of Σ_d started from the initial set $X_0 \subseteq X$ never reach the unsafe set $X_u \subseteq X$.*

We present the next theorem to show the usefulness of BC for verifying the safety of dt-S as in Definition 5.4.4.

Theorem 5.4.5. *Let Σ_d be a dt-S. Suppose $\mathcal{B}$ is a BC for Σ_d as in Definition 5.4.2. Then one has $x_{x_0}(k) \notin X_u$, for any $x_0 \in X_0$ and any $k \in [0, \mathcal{T})$, where $\mathcal{T} \leq \frac{\lambda - \gamma}{\psi}$.*

Proof. According to (5.4.4), since $\mathcal{B}(x(k+1)) - \mathcal{B}(x(k)) \leq \psi$, one can recursively infer that $\mathcal{B}(x(k)) - \mathcal{B}(x(0)) \leq \psi k$. From (5.4.2), we have $\mathcal{B}(x(k)) \leq \gamma + \psi k$. Now since $\gamma + \psi\mathcal{T} < \lambda$, one can readily conclude that $\mathcal{B}(x(k)) < \lambda$. From (5.4.3), one gets $x(k) \notin X_u$ for any $k \in [0, \mathcal{T})$ which completes the proof. It is clear that if ψ is equal to zero, one can provide the safety guarantee for an infinite time horizon. ■

In order to provide a formal guarantee for the safety of the system in (5.4.1), knowing the precise map f is essential to check the condition (5.4.4) in Definition 5.4.2. In the next subsection, we assume that we do not have any information about the model (*i.e.,* map f) and provide a data-driven scheme for the construction of barrier certificates using a finite set of data collected from trajectories of the system.

5.4.3 Data-Driven Construction of BC

Here, we assume that the transition map f in (5.4.1) is unknown, and we employ the term *unknown* model to refer to this type of systems. The main goal is to verify the safety of the unknown system in (5.4.1) by constructing a barrier certificate using data. In our setting, we take two consecutive data-points from trajectories of the system as the pair of $(x(k), x(k+1))$ and denote it by $(\hat{x}, f(\hat{x}))$. We also fix the structure of barrier certificates as $\mathcal{B}(q,x) = \sum_{j=1}^{z} q_j p_j(x)$ with some user-defined (possibly nonlinear) basis functions $p_j(x)$ and unknown coefficients $q = [q_1; \ldots; q_z] \in \mathbb{R}^z$. For instance, in the case of polynomial-type barrier certificates, basis functions $p_j(x)$ are monomials over x.

In order to enforce conditions (5.4.2)-(5.4.4) in Definition 5.4.2, we first cast our problem as the following robust convex program (RCP):

$$\text{RCP}: \begin{cases} \min\limits_{[d;\Phi]} & \Phi, \\ \text{s.t.} & \max_j \left\{ g_j(x,d) \right\} \leq \Phi, j \in \{1,\ldots,4\}, \forall x \in X, \\ & d = [\gamma; \lambda; \psi; q_1; \ldots; q_z],\ \Phi, \gamma, \lambda \in \mathbb{R},\ \psi \in \mathbb{R}_{\geq 0}, \end{cases} \tag{5.4.5}$$

where

$$g_1(x,d) = (\mathcal{B}(q,x) - \gamma)\mathbf{1}_{X_0}(x),\ g_2(x,d) = (-\mathcal{B}(q,x) + \lambda)\mathbf{1}_{X_u}(x),$$
$$g_3(x,d) = \gamma + \psi\mathcal{T} - \lambda - \hat{\mu},\ g_4(x,d) = \mathcal{B}(q,f(x)) - \mathcal{B}(q,x) - \psi,$$

for some $\hat{\mu} < 0$, and with $\mathbf{1}_{X_0}(x)$ and $\mathbf{1}_{X_u}(x)$ being indicator functions acting on initial and unsafe sets, respectively. Note that we employ $\hat{\mu} < 0$ in condition g_3 to ensure $\gamma < \lambda$ when $\psi = 0$. We denote the optimal value of RCP by Φ_R^*. If $\Phi \leq 0$, a solution to the RCP implies the satisfaction of conditions (5.4.2)-(5.4.4) in Definition 5.4.2.

Remark 5.4.6. *Note that we modified conditions* (5.4.2)-(5.4.4) *of Definition 5.4.2 in the RCP in* (5.4.5) *by adding* Φ *to their right-hand side. We accordingly defined* Φ *as the objective function of the RCP. Later, we provide our solution to the safety verification of the unknown system by establishing a probabilistic relation between the optimal value of RCP (i.e.,* Φ_R^**) and that of its corresponding scenario convex program (SCP) which is defined next.*

To solve the proposed RCP (5.4.5), we face two major difficulties. First, the proposed RCP in (5.4.5) has infinitely many constraints since the state of the system lives in a continuous set (*i.e.,* $x \in X$). Besides, one needs to know the precise map f in order to tackle the problem. These challenges motivate us to employ data-driven approaches

and propose a scenario convex program of RCP. Let $(\hat{x}_i)_{i=1}^{\mathcal{N}}$ denote $\mathcal{N}$ independent and identically distributed (i.i.d.) data sampled within X. Instead of solving the RCP in (5.4.5), we rather solve the following scenario convex program (SCP):

$$\text{SCP}: \begin{cases} \min\limits_{[d;\Phi]} & \Phi, \\ \text{s.t.} & \max_j \big\{g_j(x,d), g_4(\hat{x}_i,d)\big\} \leq \eta, j \in \{1,2,3\}, \\ & \forall x \in X, \forall \hat{x}_i \in X, \forall i \in \{1,\ldots,\mathcal{N}\}, \\ & d = [\gamma;\lambda;\psi;q_1;\ldots;q_z],\ \Phi,\gamma,\lambda \in \mathbb{R},\ \psi \in \mathbb{R}_{\geq 0}, \end{cases} \tag{5.4.6}$$

where g_1-g_4 are the functions defined in (5.4.5). One can readily see that (5.4.6) has constraints of the same form as in (5.4.5) only restricted to a finite number of data. Moreover, one can substitute $f(\hat{x}_i)$ in $\mathcal{B}(q, f(\hat{x}_i))$ in g_4 by measuring the unknown dt-S after one-step evolution starting from $\hat{x}_i$. We denote the optimal value of SCP by $\Phi^*_{\mathcal{N}}$. One can readily see that the SCP in (5.4.6) is a linear programming in terms of unknown decision variables.

In the next subsection, we establish a probabilistic closeness guarantee between the optimal value of SCP (*i.e.,* $\Phi^*_{\mathcal{N}}$) and that of RCP (*i.e.,* Φ^*_R), and accordingly, verify the safety of unknown systems with an a-priori guaranteed confidence bound.

5.4.4 Safety Guarantee over Unknown Systems

Here, inspired by the fundamental results in [MESL14], we aim at establishing a formal relation between the optimal value of SCP in (5.4.6) and that of RCP in (5.4.5). Accordingly, we formally quantify the safety guarantee of unknown systems based on the number of data and the required level of confidence. We state the main problem considered in this subsection.

Problem 5.4.7. *Consider a (partially) unknown dt-S Σ_d as in* (5.4.1) *and a safety specification $\varphi = (X_0, X_u, \mathcal{T})$ as in Definition 5.4.4. Construct a barrier certificate by solving the SCP in* (5.4.6) *based on collected data to provide a formal guarantee on the satisfaction of the safety specification φ within the time horizon $\mathcal{T}$ with an a-priori confidence bound $\beta \in [0,1]$, i.e.,*

$$\mathbb{P}^{\mathcal{N}}\big\{\Sigma_d \models_{\mathcal{T}} \varphi\big\} \geq 1-\beta.$$

To address Problem 5.4.7, we first propose the following assumption.

Assumption 5.4.8. *Suppose $g_4(x,d)$ is Lipschitz continuous with respect to x with the Lipschitz constant $\mathscr{L}_g$.*

Under Assumption 5.4.8, the next theorem, inspired by [MESL14], establishes a bridge between the optimal values of SCP in (5.4.6) and that of the original RCP in (5.4.5), and accordingly, provides a mechanism to verify the safety of the unknown system.

Theorem 5.4.9. *Consider a (partially) unknown dt-S as in* (5.4.1)*, and initial and unsafe regions X_0 and X_u, respectively. Let Assumption 5.4.8 hold. Consider the corresponding SCP in* (5.4.6) *with its associated optimal value $\Phi^*_{\mathcal{N}}$ and solution $d^* = [\gamma^*; \lambda^*; \psi^*; q_1^*; \ldots; q_z^*]$, with an arbitrary number of samples $\mathcal{N} \in \mathbb{N}_{\geq 1}$ and $\beta \in [0, 1]$. Then the following statement holds with a confidence of at least $1 - \beta$: if*

$$\Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon) \leq 0, \tag{5.4.7}$$

with

$$\varepsilon \geq \mathcal{I}_r^{-1}(1 - \beta, \bar{z}, \mathcal{N} - \bar{z} + 1)), \tag{5.4.8}$$

where $\bar{z}$ is the number of decision variables, $\mathcal{I}$ is the regularized incomplete beta function [Cal10], and $\hat{g}(r) : \mathbb{R}_{\geq 0} \to [0, 1]$ is a function of order r^n which depends on the sampling distribution and the geometry of the uncertainty set X, then the unknown dt-S is safe in the sense of Theorem 5.4.5 within the time horizon $\frac{\lambda^* - \gamma^*}{\psi^*}$.

Proof. Based on [MESL14, Theorem 3.6 and Proposition 3.8], the probabilistic distance between optimal values of RCP and SCP can be formally lower bounded as*

$$\mathbb{P}^{\mathcal{N}}\Big\{0 \leq \Phi^*_R - \Phi^*_{\mathcal{N}} \leq \mathrm{L_{SP}} \bar{h}(\varepsilon)\Big\} \geq 1 - \beta, \tag{5.4.9}$$

with $\bar{h}(\varepsilon) = \mathscr{L}_g \hat{g}^{-1}(\varepsilon)$, where $\hat{g}(r) : \mathbb{R}_{\geq 0} \to [0, 1]$ is a function of order r^n which depends on the sampling distribution and the geometry of the uncertainty set X, and $\mathrm{L_{SP}}$ is a Slater constant as defined in [MESL14, equation (5)]. Based on [MESL14, Remark 3.5], since the original RCP in (5.4.5) can be casted as a min-max optimization problem, the Slater constant $\mathrm{L_{SP}}$ can be selected as 1. We refer the interested reader to [MESL14, equation (5)] for more details on the formal definition of Slater point.
From (5.4.9), one can readily conclude that $\Phi^*_{\mathcal{N}} \leq \Phi^*_R \leq \Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon)$ with a confidence of at least $1 - \beta$. If $\Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon) \leq 0$, then $\Phi^*_R \leq 0$, implying the satisfaction of conditions (5.4.2)-(5.4.4) in Definition 5.4.2 and ensuring the safety of the unknown system within time horizon $\frac{\lambda^* - \gamma^*}{\psi^*}$ with a confidence of at least $1 - \beta$, which completes the proof. ■

Remark 5.4.10. *As discussed in [MESL14, Proposition 3.8], the function $\hat{g}$ in* (5.4.8) *satisfies the following inequity:*

$$\hat{g}(r) \leq \mathbb{P}\big[\mathbb{B}_r(x)\big], \qquad \forall r \in \mathbb{R}_{\geq 0}, \forall x \in X,$$

where $\mathbb{B}_r(x) \subset X$ is an open ball centered at x with radius r. In the case of collecting samples with a uniform distribution from an n-dimensional hyper-rectangle uncertainty set, the function $\hat{g}$ in (5.4.8) *is computed as*

$$\hat{g}(r) = \frac{\mathsf{Vol}(\mathbb{B}_r(x))}{2^n \mathsf{Vol}(X)} = \frac{\frac{\pi^{\frac{n}{2}}}{\tilde{\Gamma}(\frac{n}{2}+1)} r^n}{2^n \mathsf{Vol}(X)} = \frac{\pi^{\frac{n}{2}} r^n}{2^n \tilde{\Gamma}(\frac{n}{2}+1) \mathsf{Vol}(X)}, \tag{5.4.10}$$

*One can readily verify that Φ^*_R is always bigger than or equal to $\Phi^*_{\mathcal{N}}$ since Φ^*_R is computed for infinitely many constraints, whereas $\Phi^*_{\mathcal{N}}$ is computed only for finitely many of them.

where $\pi \approx 3.14$, $\mathsf{Vol}(\cdot)$ *is the volume of the set/ball, and* $\tilde{\Gamma}$ *is the Gamma function defined as* $\tilde{\Gamma}(n) = (n-1)!$ *for any positive integer* n *and* $\tilde{\Gamma}(n+\frac{1}{2}) = (n-\frac{1}{2})\times(n-\frac{3}{2})\times\cdots\times\frac{1}{2}\times\pi^{\frac{1}{2}}$ *for any non-negative integer* n. *Note that* $1/2^n$ *in* (5.4.10) *is needed for the computation of* $\mathbb{P}\big[\mathbb{B}_r(x)\big]$ *when the sampled data are located in the corner of the uncertainty set* X. *If one collects samples with a uniform distribution from a* rectangle uncertainty set *with side lengths* a *and* b, *the function* $\hat{g}$ *in* (5.4.10) *is reduced to* $\hat{g}(r) = \frac{\pi r^2}{4ab}$ *(cf. case studies).*

Remark 5.4.11. *In the case of collecting samples with a uniform distribution from an* n*-dimensional hyper-sphere uncertainty set with radius* R, *the function* $\hat{g}$ *in* (5.4.15) *is computed as*

$$\hat{g}(r) = \frac{R^n \int_0^{c_1} \mathsf{t}^{\frac{n-1}{2}}(1-\mathsf{t})^{-\frac{1}{2}}\mathsf{dt} + r^n \int_0^{c_2} \mathsf{t}^{\frac{n-1}{2}}(1-\mathsf{t})^{-\frac{1}{2}}\mathsf{dt}}{2R^n \int_0^1 \mathsf{t}^{\frac{n-1}{2}}(1-\mathsf{t})^{-\frac{1}{2}}\mathsf{dt}}, \tag{5.4.11}$$

where $c_1 = 1 - \frac{(2R^2-r^2)^2}{4R^4}, c_2 = 1 - \frac{r^2}{4R^2}$. *We refer the interested readers to [KT12] for the computation of* $\hat{g}$ *for other shapes of uncertainty sets with different types of sample distributions.*

Since our dynamical system in this section is non-stochastic, the probabilistic confidence bound in Theorem 5.4.9 is due to data collected from the system (*i.e.,* by increasing data, the confidence improves). If the unknown system is stochastic, then the provided guarantee consists of two layers of probabilities: the inner layer is regarding the stochasticity in the system and the outer layer is due to data similar to our setting. In this case, one also has a confidence on the probability of satisfaction (see [CLD19]).

It is worth mentioning that the main benefit of the results in Theorem 5.4.9 compared to system identification is that the proposed data-driven technique here is capable of providing safety guarantees for *any type of nonlinear systems which are Lipschitz continuous*, whereas system identification approaches are mainly tailored to linear or some particular classes of nonlinear systems. In addition, even if one is able to find a model using system identification techniques, one still needs to search for a barrier certificate. In this case, one suffers from the computational complexity in both identifying the model as well as searching for a barrier certificate based on it.

In order to provide a safety certificate over the original unknown system via Theorem 5.4.9, we propose Algorithm 1 to describe the required procedure.

Algorithm 1 Safety guarantee over unknown dt-S

1: Select a-priori $\mathcal{N} \in \mathbb{N}_{\geq 1}, \beta \in [0,1]$ as desired
2: Compute ε as in (5.4.8)
3: Solve the SCP (5.4.6) with the desired $\mathcal{N}$ and obtain $\Phi^*_{\mathcal{N}}$
4: If $\Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon) \leq 0$, then the safety of the unknown dynamical system is guaranteed with a confidence of at least $1-\beta$
5: Otherwise, one cannot judge the safety of the system, given parameters ε and β.

To the best of our knowledge, our result is the first to provide safety verification for unknown dynamical systems. Providing such a safety certificate using [MESL14] was not straightforward. In particular, there is no objective function involved in searching for barrier certificates in Definition 5.4.2. In order to utilize the results in [MESL14], we *artificially* defined an objective function based on a value Φ. We then related the optimal value of RCP (which is unknown) to that of SCP (which can be computed by collecting data) and provided the safety certificate for the unknown system with an a-priori confidence bound as long as $\Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon) \leq 0$.

Remark 5.4.12. *Note that our approach provides a much more tractable way of computing barrier certificates than model-based approaches using sum-of-squares (SOS) optimization problem. In particular, our method is not only applicable to polynomial-type dynamics, but also to much more complex (un)known systems in which the RCP problem does not have even any tractable solution.*

In order to check the condition (5.4.7) in Theorem 5.4.9, one needs to first compute $\mathscr{L}_g$. We propose in the next lemma an explicit way to compute $\mathscr{L}_g$ for the choice of quadratic barrier certificates and linear dynamics.

Lemma 5.4.13. *Consider a linear dt-S of the form $x(k+1) = Ax(k)$ with $A \in \mathbb{R}^{n\times n}$. Assume that $\|A\| \leq \mathscr{L}_f \in \mathbb{R}_{\geq 0}$. Then $\mathscr{L}_g$ in Assumption 5.4.8 for a quadratic barrier certificate of the form $x^\top \bar{P} x$, with a symmetric matrix $\bar{P} \in \mathbb{R}^{n\times n}$, is computed as $\mathscr{L}_g = 2\tilde{h}\rho_{spc}(\bar{P})(\mathscr{L}_f^2 + 1)$, where ρ_{spc} is the spectral radius, and $\tilde{h}$ is an upper bound on the norm of the state vector, i.e., $\|x\| \leq \tilde{h} \in \mathbb{R}_{\geq 0}$ for any $x \in X$.*

Proof. For computing the Lipschitz constant of g_4 with respect to x, we have

$$\mathscr{L}_g = \max_{x\in X, \|x\|\leq \tilde{h}} \|\frac{\partial g_4(x)}{\partial x}\|.$$

Accordingly,

$$\begin{aligned}\mathscr{L}_g &= \max_{x\in X,\|x\|\leq\tilde{h}} \|2(A^\top \bar{P}A - \bar{P})x\| \leq \max_{x\in X,\|x\|\leq\tilde{h}} \|2(A^\top \bar{P}A - \bar{P})\|\|x\| \\ &\leq 2\tilde{h}(\|A^\top \bar{P}A\| + \|\bar{P}\|) \leq 2\tilde{h}(\|\bar{P}\|\|A\|^2 + \|\bar{P}\|) \leq 2\tilde{h}\rho_{spc}(\bar{P})(\mathscr{L}_f^2 + 1).\end{aligned}$$

Then $\mathscr{L}_g = 2\tilde{h}\rho_{spc}(\bar{P})(\mathscr{L}_f^2 + 1)$, which completes the proof. ■

Remark 5.4.14. *Note that one needs to know an upper bound for $\rho_{spc}(\bar{P})$ in order to check the condition* (5.4.7) *in Theorem 5.4.9. The pre-assumed upper bound should be then enforced as an additional condition while solving the SCP* (5.4.6) *as mentioned in Step 3 of Algorithm 1. Note that the required conditions for enforcing $\rho_{spc}(\bar{P}) \leq \bar{v} \in \mathbb{R}_{>0}$ may result in nonlinear constraints in SCP* (5.4.6)*. To resolve this issue, we enforce those conditions as linear bounds on entries of matrix $\bar{P}$ using Gershgorin circle theorem [Var10] (cf. case studies).*

Remark 5.4.15. *If the underlying dynamics are nonlinear in the form of* (5.4.1)*, one can still employ a similar reasoning as Lemma 5.4.13 and compute* $\mathscr{L}_g = 2\rho_{spc}(\bar{P})(\mathcal{M}_f\mathscr{L}_f + \tilde{h})$ *by assuming that* $\|f(x)\| \leq \mathcal{M}_f \in \mathbb{R}_{\geq 0}$*, and* $\|\frac{\partial f(x)}{\partial x}\| \leq \mathscr{L}_f \in \mathbb{R}_{\geq 0}$ *for any* $x \in X$*.*

In order to compute $\mathscr{L}_g$ as in Lemma 5.4.13, one needs to know an upper bound for $\|A\|$ which is actually the Lipschitz constant of the dynamic (*i.e.,* $\mathscr{L}_f$) in the linear case. To do so, one can assume the model is fully unknown and estimate the Lipschitz constant of dynamics using a finite number of data collected from trajectories of the system as described in the following subsection.

5.4.4.1 Estimation of Lipschitz Constant of Dynamics from Data

Here, we employ the proposed results in [WZ96] and provide the following algorithm to estimate the Lipschitz constant of dynamics from a finite number of data collected from the system.

Algorithm 2 Estimation of Lipschitz constant of dt-S

1: Select randomly two initial conditions $\hat{x}_i, \hat{y}_i$, such that $\|\hat{x}_i - \hat{y}_i\| \leq \hat{\alpha}$ for any $i \in \{1, \ldots, \bar{\mathcal{N}}\}$, with $\hat{\alpha} \in \mathbb{R}_{>0}$ being some arbitrary threshold
2: Compute the slope s_i as,

$$s_i = \frac{\|f(\hat{x}_i) - f(\hat{y}_i)\|}{\|\hat{x}_i - \hat{y}_i\|}, \quad \forall i \in \{1, \ldots, \bar{\mathcal{N}}\},$$

where $f(\hat{x}_i)$ and $f(\hat{y}_i)$ are one step evaluations of the system started from initial states x_i and y_i, respectively
3: Compute the maximum slope as $\bar{\psi} = \max\{s_1, \ldots, s_{\bar{\mathcal{N}}}\}$
4: Repeat Steps 1-3 $\bar{\mathcal{M}}$ times and acquire $\bar{\psi}_1, \ldots, \bar{\psi}_{\bar{\mathcal{M}}}$
5: Apply Reverse Weibull distribution [WZ96] to $\bar{\psi}_1, \ldots, \bar{\psi}_{\bar{M}}$, which gives us so-called location, scale, and shape parameters
6: The obtained *location parameter* is the estimated Lipschitz constant of dt-S

By employing Algorithm 2, the following lemma, borrowed from [WZ96], ensures the convergence of the estimated Lipschitz constant to its actual value in the limit.

Lemma 5.4.16. *Let* Σ_d *be a dt-S with an unknown transition map* f*. By employing Algorithm 2, the estimated Lipschitz constant* $\mathscr{L}_f$ *for* Σ_d *converges to its actual value if and only if* $\hat{\alpha}$ *goes to zero and* $\bar{\mathcal{N}}, \bar{\mathcal{M}}$ *go to infinity.*

Remark 5.4.17. *Note that we do not consider any confidence bound for the estimation of the Lipschitz constant in the setting of our work. Instead, we pick* $\hat{\alpha}$ *very small and* $\bar{\mathcal{N}}, \bar{\mathcal{M}}$ *very big such that one can get a good approximation for the Lipschitz constant. In the case study section, we show that our estimated value for the Lipschitz constant of the system is almost the same as its actual value.*

In the next subsections, we tailor the previous results for *continuous-time* dynamical systems.

5.4.5 Continuous-Time Dynamical Systems

We consider continuous-time dynamical systems (ct-S) as formalized in the following definition.

Definition 5.4.18. *A continuous-time dynamical system (ct-S) described as*

$$\Sigma_c : \dot{x}(t) = f(x(t)), \tag{5.4.12}$$

where $x : \mathbb{R}_{\geq 0} \to X$ is the state trajectory of Σ_c, $X \subseteq \mathbb{R}^n$ is the state set of the system, and $f : X \to \mathbb{R}^n$ is the vector field. We employ $x_{x_0}(t)$ to denote the value of the state trajectory at time $t \in \mathbb{R}_{\geq 0}$ under the initial condition $x_0 = x(0)$. In order to ensure the existence and uniqueness of the state trajectory, we consider some regularity assumptions on vector field f as discussed in [Son98].

We present the notion of barrier certificates (BC) for ct-S in (5.4.12) in the following definition.

Definition 5.4.19. *Consider a ct-S Σ_c in (5.4.12), and $X_0, X_u \subseteq X$ as, respectively, initial and unsafe sets of the system. A continuously differentiable function $\mathcal{B} : X \to \mathbb{R}$ is called a barrier certificate (BC) for Σ_c if there exist $\psi \in \mathbb{R}_{\geq 0}$ and $\gamma, \lambda \in \mathbb{R}$, with $\gamma + \psi\mathcal{T} < \lambda$, such that conditions (5.4.2), (5.4.3) are satisfied, and*

$$\mathsf{L}_f\mathcal{B}(x) \leq \psi, \qquad \forall x \in X, \tag{5.4.13}$$

where $\mathsf{L}_f\mathcal{B}$ is the Lie derivative of $\mathcal{B} : X \to \mathbb{R}$ with respect to the vector field f, and is defined as

$$\mathsf{L}_f\mathcal{B}(x) = \partial_x\mathcal{B}(x)f(x). \tag{5.4.14}$$

We similarly recast conditions of the barrier certificate as the proposed RCP in (5.4.5), where

$$g_4(x, d) = \mathsf{L}_f\mathcal{B}(q, x) - \psi. \tag{5.4.15}$$

Similar to the first part of this section, we employ the proposed SCP in (5.4.6) instead of solving the RCP in (5.4.5). Although the infinitely many constraints in (5.4.5) are converted to finitely many in SCP (5.4.6) by using the collected data, one still needs to know the map f to enforce condition g_4. Note that condition g_4 in (5.4.15) cannot be directly acquired from collected data based on $f(\hat{x}_i)$. To tackle this issue, inspired by the previous sections, we approximate the Lie derivative of $\mathcal{B}$ with respect to f (*i.e.,* $\mathsf{L}_f\mathcal{B}(q, x)$) appeared in g_4 as

$$\widehat{\mathsf{L}}_f\mathcal{B}(q, x) := \frac{\mathcal{B}(q, x_\tau) - \mathcal{B}(q, x)}{\tau}, \quad \forall x \in X, \tag{5.4.16}$$

where x_τ is the solution of the unknown system after $\tau \in \mathbb{R}_{>0}$ units of time starting from x. The proposed approximation in (5.4.16) satisfies the following inequality

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x) - \mathsf{L}_f\mathcal{B}(q,x)| \leq \tilde{\varepsilon}, \quad \forall x \in X,$$

where $\tilde{\varepsilon}$ is a positive constant and is formally quantified later in Subsection 5.2.2. Now, we propose another version of the SCP (5.4.6) as

$$\mathrm{SCP}_{\tilde{\varepsilon}}\colon \begin{cases} \min\limits_{[d;\Phi]} & \Phi, \\ \text{s.t.} & \max\big\{g_j(\hat{x}_i,d), \bar{g}_4(\hat{x}_i,d,\tilde{\varepsilon})\big\} \leq \Phi, j\in\{1,2,3\},\ \forall i \in \{1,\ldots,\mathcal{N}\}, \\ & d=[\gamma;\lambda;\psi;q_1;\ldots;q_z],\ \Phi,\gamma,\lambda\in\mathbb{R},\ \psi,\tilde{\varepsilon}\in\mathbb{R}_{\geq 0}, \end{cases} \tag{5.4.17}$$

where $\bar{g}_4(\hat{x}_i,d,\tilde{\varepsilon}) = \widehat{\mathsf{L}}_f\mathcal{B}(q,\hat{x}_i) - \psi + \tilde{\varepsilon}$.

We now state the main problem that we plan to solve in this subsection.

Problem 5.4.20. *Consider a (partially) unknown ct-S Σ_c as in* (5.4.12) *and a safety specification $\varphi = (X_0, X_u, \mathcal{T})$ as in Definition 5.4.4. Construct a barrier function by solving the SCP$_{\tilde{\varepsilon}}$ in* (5.4.17) *based on collected data to provide a formal guarantee on the satisfaction of the safety specification φ within the time horizon $\mathcal{T}$ with an a-priori confidence bound $\beta \in [0,1]$, i.e.,*

$$\mathbb{P}^{\mathcal{N}}\big\{\Sigma_c \models_{\mathcal{T}} \varphi\big\} \geq 1-\beta.$$

To address Problem 5.4.20, we propose the next theorem which establishes a bridge between optimal values of SCP$_{\tilde{\varepsilon}}$ in (5.4.17) and that of original RCP in (5.4.5), and accordingly verifies the safety of the unknown system with an a-priori confidence bound.

Theorem 5.4.21. *Consider an unknown ct-S as in* (5.4.12)*, and initial and unsafe regions X_0 and X_u, respectively. Let Assumption 5.4.8 hold with g_4 as in* (5.4.15)*. Consider the corresponding SCP$_{\tilde{\varepsilon}}$ in* (5.4.17) *with its associated optimal value $\Phi^*_{\mathcal{N}}$ and solution $d^* = [\gamma^*;\lambda^*;\psi^*;q_1^*;\ldots;q_z^*]$, with an arbitrary number of samples $\mathcal{N} \in \mathbb{N}_{\geq 1}$ and $\beta \in [0,1]$. Then the following statement holds with a confidence of at least $1-\beta$: if*

$$\Phi^*_{\mathcal{N}} + \mathscr{L}_g\hat{g}^{-1}(\varepsilon) \leq 0,$$

with ε as in (5.4.8)*, and $\hat{g}(r) : \mathbb{R}_{\geq 0} \to [0,1]$ being a function of order r^n which depends on the sampling distribution and the geometry of the uncertainty set X, then the unknown ct-S in* (5.4.12) *is safe in the sense of Theorem 5.4.5 (but in the continuous-time setting) within the time horizon $\frac{\lambda^*-\gamma^*}{\psi^*}$.*

The proof of Theorem 5.4.21 is similar to that of Theorem 5.4.9 and is omitted here.

Similar to Lemma 5.4.13, we propose in the next lemma an explicit way to compute $\mathscr{L}_g$ for ct-S for the choice of quadratic barrier certificates and linear dynamics.

Lemma 5.4.22. *For a linear ct-S $\dot{x}(t) = Ax(t)$ with $A \in \mathbb{R}^{n\times n}$, let the matrix A be bounded as $\|A\| \leq \mathscr{L}_f$, where $\mathscr{L}_f$ is the Lipschitz constant of the system as in* (5.2.3)*.*

Then $\mathscr{L}_g$ for a quadratic barrier certificate of the form $x^\top \bar{P} x$, with a symmetric matrix $\bar{P} \in \mathbb{R}^{n\times n}$, is computed as $\mathscr{L}_g = 4\tilde{h}\rho_{spc}(\bar{P})\mathscr{L}_f$, where ρ_{spc} is the spectral radius, and $\tilde{h}$ is an upper bound on the norm of the state vector, i.e., $\|x\| \leq \tilde{h} \in \mathbb{R}_{\geq 0}$ for any $x \in X$.

Proof. For g_4, we have

$$\mathscr{L}_g : \begin{cases} \max\limits_{x\in X} & \|\frac{\partial g_4(x)}{\partial x}\|, \\ \text{s.t.} & \|x\| \leq \tilde{h}. \end{cases}$$

Accordingly,

$$\begin{aligned} \mathscr{L}_g &= \max_{x\in X, \|x\|\leq \tilde{h}} \|2(\bar{P}A + A^\top \bar{P})x\| \leq \max_{x\in X, \|x\|\leq \tilde{h}} \|2(\bar{P}A + A^\top \bar{P})\|\|x\| \\ &\leq 4\tilde{h}\|\bar{P}\|\|A\| \leq 4\tilde{h}\rho_{spc}(\bar{P})\mathscr{L}_f, \end{aligned}$$

which completes the proof. ■

Remark 5.4.23. *If the underlying dynamics are nonlinear in the form of* (5.4.12)*, one can still employ a similar reasoning as in Lemma 5.4.22 and compute the Lipschitz constant as $\mathscr{L}_g = 2\rho_{spc}(\bar{P})(\mathcal{M}_f + \tilde{h}\mathscr{L}_f)$ by assuming that $\|f(x)\| \leq \mathcal{M}_f \in \mathbb{R}_{\geq 0}$, and $\|\frac{\partial f(x)}{\partial x}\| \leq \mathscr{L}_f \in \mathbb{R}_{\geq 0}$ for any $x \in X$.*

In the next subsection, we formally approximate the Lie derivative of the system (5.4.12) (*i.e.,* $\mathsf{L}_f\mathcal{B}(q,x)$) by $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ by providing its quantified closeness as $\tilde{\varepsilon}$.

5.4.5.1 Formal Approximation of Lie Derivative

In order to quantify the formal closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$, we assume that vector field f and $\partial_x\mathcal{B}(q,x)$ are Lipschitz continuous and bounded as

$$\|f(x) - f(x')\| \leq \mathscr{L}_f\|x - x'\|,\ \|\partial_x\mathcal{B}(q,x) - \partial_{x'}\mathcal{B}(q,x')\| \leq \mathscr{L}_{\mathcal{B}_1}\|x - x'\|, \tag{5.4.18}$$

$$\|f(x)\| \leq \mathcal{M}_f,\ \|\partial_x\mathcal{B}(q,x)\| \leq \mathcal{M}_{\mathcal{B}_1}. \tag{5.4.19}$$

Remark 5.4.24. *Since the structure of the barrier is considered as a linear combination of known basis functions, one can a-priori select $\mathscr{L}_{\mathcal{B}_1}$ and $\mathcal{M}_{\mathcal{B}_1}$ as some arbitrary numbers and enforce their corresponding conditions in* (5.4.18) *and* (5.4.19) *as some additional constraints while solving SCP$_{\tilde{\varepsilon}}$* (5.4.17) *(cf. case studies).*

We now employ (5.4.18),(5.4.19) and propose the next lemma to show that $\mathsf{L}_f\mathcal{B}(q,x)$ is also Lipschitz continuous.

Lemma 5.4.25. *Under conditions* (5.4.18),(5.4.19)*, $\mathsf{L}_f\mathcal{B}(q,x)$ is Lipschitz continuous with a Lipschitz constant $\mathscr{L}$ as:*

$$|\mathsf{L}_f\mathcal{B}(q,x) - \mathsf{L}_f\mathcal{B}(q,x')| \leq \mathscr{L}\|x - x'\|, \quad \forall x, x' \in X,$$

where $\mathscr{L} = \mathcal{M}_{\mathcal{B}_1}\mathscr{L}_f + \mathcal{M}_f\mathscr{L}_{\mathcal{B}_1}$.

Proof. Using the definition of $\mathsf{L}_f\mathcal{B}(q,x)$ in (5.4.14), we have

$$|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')| \leq |\partial_x\mathcal{B}(q,x)f(x)-\partial'_x\mathcal{B}(q,x')f(x')|.$$

By employing the following known inequality

$$|\mathbb{A}^\top\mathbb{B}-\mathbb{C}^\top\mathbb{D}| \leq \|\mathbb{A}\|\|\mathbb{B}-\mathbb{D}\|+\|\mathbb{D}\|\|\mathbb{A}-\mathbb{C}\|,$$

for all $\mathbb{A},\mathbb{B},\mathbb{C},\mathbb{D}\in\mathbb{R}^n$, one has

$$|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')| \leq \|\partial_x\mathcal{B}(q,x)\|\|f(x)-f(x')\|+\|f(x')\|\|\partial_x\mathcal{B}(q,x)-\partial_{x'}\mathcal{B}(q,x')\|.$$

By employing conditions (5.4.18),(5.4.19), one gets

$$\begin{aligned}|\mathsf{L}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x')| &\leq \mathcal{M}_{\mathcal{B}_1}\mathscr{L}_f\|x-x'\|+\mathcal{M}_f\mathscr{L}_{\mathcal{B}_1}\|x-x'\|\\ &=(\mathcal{M}_{\mathcal{B}_1}\mathscr{L}_f+\mathcal{M}_f\mathscr{L}_{\mathcal{B}_1})\|x-x'\|=\mathscr{L}\|x-x'\|,\end{aligned}$$

which completes the proof. ■

Now all the ingredients are ready to formally quantify the closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ as proposed in the following theorem.

Theorem 5.4.26. *Let $\mathsf{L}_f\mathcal{B}(q,x)$ be the Lie derivative of $\mathcal{B}$ with respect to f and $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ be its approximation as in* (5.4.16)*. Under conditions* (5.4.18),(5.4.19)*, and using Lemma 5.4.25, one has*

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)| \leq \frac{1}{2}\tau\mathscr{L}\mathcal{M}_f, \quad \forall x\in X,$$

where τ is the sampling time, and $\mathscr{L}=\mathcal{M}_{\mathcal{B}_1}\mathscr{L}_f+\mathcal{M}_f\mathscr{L}_{\mathcal{B}_1}$.

Proof. Since x_τ is the solution of the model after τ units of time starting from x, one has

$$\mathcal{B}(q,x_\tau)=\mathcal{B}(q,x)+\int_0^\tau \mathsf{L}_f\mathcal{B}(q,x_t)\mathsf{d}t. \tag{5.4.20}$$

Considering the approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ as in (5.4.16) and by employing (5.4.20), one has

$$\widehat{\mathsf{L}}_f\mathcal{B}(q,x)=\frac{1}{\tau}\int_0^\tau \mathsf{L}_f\mathcal{B}(q,x_t)\mathsf{d}t.$$

By subtracting $\mathsf{L}_f\mathcal{B}(q,x)$ from both sides of the equality, we have

$$\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)=\frac{1}{\tau}\int_0^\tau \big(\mathsf{L}_f\mathcal{B}(q,x_t)-\mathsf{L}_f\mathcal{B}(q,x)\big)\mathsf{d}t.$$

Consequently,

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)|\leq\frac{1}{\tau}\int_0^\tau|\mathsf{L}_f\mathcal{B}(q,x_t)-\mathsf{L}_f\mathcal{B}(q,x)|\mathsf{d}t.$$

By employing Lemma 5.4.25, one gets

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)|\leq\frac{1}{\tau}\int_0^\tau\mathscr{L}\|x_t-x\|\mathsf{d}t=\frac{\mathscr{L}}{\tau}\int_0^\tau\|x_t-x\|\mathsf{d}t.$$

Now we aim at finding an upper bound for $\|x_t-x\|$. Under the continuity property of the solution process of the system, we have

$$x_t=x+\int_0^t f(x_s)\mathsf{d}s.$$

Then, using Cauchy–Schwarz inequality, one has

$$\begin{aligned}\|x_t-x\|&=\|\int_0^t f(x_s)\mathsf{d}s\|=\Big[\int_0^t f(x_s)^\top\mathsf{d}s\int_0^t f(x_s)\mathsf{d}s\Big]^{\frac{1}{2}}=\Big[\int_0^t\int_0^t f(x_{s_1})^\top f(x_{s_2})\mathsf{d}s_1\mathsf{d}s_2\Big]^{\frac{1}{2}}\\&\leq\Big[\int_0^t\int_0^t\|f(x_{s_1})\|\|f(x_{s_2})\|\mathsf{d}s_1\mathsf{d}s_2\Big]^{\frac{1}{2}}.\end{aligned}$$

Under condition (5.4.19), we obtain

$$\|x_t-x\|\leq\int_0^t\mathcal{M}_f\mathsf{d}s=\mathcal{M}_f t.$$

Consequently, one has

$$|\widehat{\mathsf{L}}_f\mathcal{B}(q,x)-\mathsf{L}_f\mathcal{B}(q,x)|\leq\frac{\mathscr{L}}{\tau}\int_0^\tau\mathcal{M}_f t\mathsf{d}t=\frac{1}{2}\tau\mathscr{L}\mathcal{M}_f,$$

which completes the proof. ■

As seen in Theorem 5.4.26, one can control the closeness error between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,\hat{x}_i)$ by picking a small sampling time τ. This is also better for the precision of the approximation since a smaller sampling time provides a more precise approximation. We employ the following room temperature example to elaborate more on this issue.

Room temperature. Consider a temperature regulation of a room with a model borrowed from [GGM16]. The evolution of the temperature $T(\cdot)$ can be described by the following ct-S

$$\Sigma_c:\dot{T}(t)=-\hat{\theta}T(t)+\hat{\theta}T_e,\tag{5.4.21}$$

where $\hat{\theta}=0.005$ and $T_e=-20\,^\circ\mathsf{C}$.

We fix a quadratic barrier certificate of the form $\mathcal{B}(q,T)=T^2+2T-1$. Accordingly, one has

$$\mathsf{L}_f\mathcal{B}(q,T)=(2T+2)(-\hat{\theta}T(t)+\hat{\theta}T_e),\tag{5.4.22}$$

which is independent of the sampling time. The approximation of the Lie derivative in our setting based on (5.4.16) is $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)=\frac{\mathcal{B}(q,T_\tau)-\mathcal{B}(q,T)}{\tau}$. If the model in (5.4.21) is

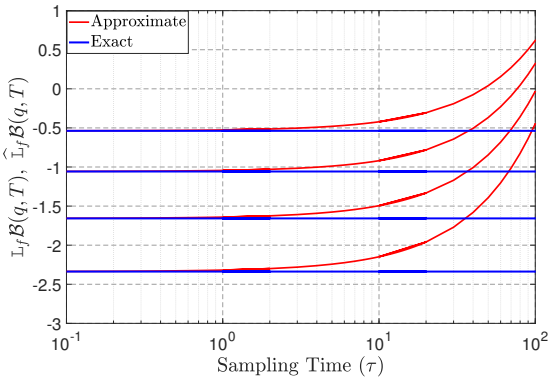

Figure 5.5: Exact $\mathsf{L}_f\mathcal{B}(q,T)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ for different ranges of sampling time and 4 different initial conditions.

known, its state trajectory is obtained as $Te^{-\hat{\theta}\tau} - T_e(e^{-\hat{\theta}\tau} - 1)$. Then the approximate Lie derivative can be computed as

$$\begin{aligned}\widehat{\mathsf{L}}_f\mathcal{B}(q,T) = \big(&T^2(e^{-2\hat{\theta}\tau}-1)+2T(e^{-\hat{\theta}\tau}-1)+T_e^2(e^{-\hat{\theta}\tau}-1)^2\\ &-2T_e(e^{-\hat{\theta}\tau}-1)-2T_eTe^{-\hat{\theta}\tau}(e^{-\hat{\theta}\tau}-1)\big)/\tau. \end{aligned} \tag{5.4.23}$$

It can be readily shown that $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ in (5.4.23) converges to $\mathsf{L}_f\mathcal{B}(q,T)$ in (5.4.22) if the sampling time τ goes to zero. Since the model in our setting is unknown, we instead collect data and estimate $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ via (5.4.16). The exact Lie derivative and its approximation via collected data for different ranges of the sampling time starting from 4 different initial conditions are plotted in Figure 5.5. As can be observed, the approximate $\widehat{\mathsf{L}}_f\mathcal{B}(q,T)$ converges to the exact $\mathsf{L}_f\mathcal{B}(q,T)$ for all initial conditions when the sampling time goes to zero.

Remark 5.4.27. *Although a smaller sampling time provides a smaller closeness error, we do not consider the numerical error originating from finite-precision computations in different computing platforms. In practice, this numerical precision imposes a lower bound over the sampling time and does not allow it to be very small.*

In order to provide the closeness between $\mathsf{L}_f\mathcal{B}(q,x)$ and its approximation $\widehat{\mathsf{L}}_f\mathcal{B}(q,x)$ as in Theorem 5.4.26, the Lipschitz constant of the system $\mathscr{L}_f$ is needed (cf. Assumption 5.2.4). One can assume the model is fully unknown and instead estimate the Lipschitz constant of dynamics from collected data as described in Algorithm 2 with

$$s_i = \frac{\left\| \frac{(\hat{x}_{\tau_i} - \hat{x}_{0_i}) - (\hat{y}_{\tau_i} - \hat{y}_{0_i})}{\tau} \right\|}{\|\hat{x}_{0_i} - \hat{y}_{0_i}\|}, \quad \forall i \in \{1, \dots, \bar{\mathcal{N}}\}.$$

Remark 5.4.28. *It is worth mentioning that we presented our results in this section for deterministic dynamical systems for the sake of providing a clearer presentation. However, our results here can be readily extended to nondeterministic dynamical systems*

with dynamics $x(k+1) = f(x(k), w(k))$ (resp. $\dot{x}(t) = f(x(t), w(t))$), where $w(k) \in W$ (resp. $w(t) \in W$) is a bounded disturbance with $W \subseteq \mathbb{R}^{\bar{p}}$ being the disturbance set. In this case, the sample space is expanded to $X \times W$, and accordingly, $\hat{g}(r)$ is a functions of $r^{n+\bar{p}}$, where $\bar{p}$ is the dimension of the disturbance set. In addition, g_4 in Assumption 5.4.8 should be Lipschitz continuous with respect to both x and *w which requires the re-computation of $\mathscr{L}_g$ in Lemma 5.4.13 and Remark 5.4.15 (resp. Lemma 5.4.22 and Remark 5.4.23 in the continuous-time setting).*

5.4.6 Case Studies

To illustrate the effectiveness of our proposed results, we first apply our results to the *continuous-time* room temperature system in (5.4.21). We verify that the temperature of the room with unknown dynamics maintains in a comfort zone with some desirable confidence by collecting data sampled from trajectories of the system. To show the applicability of our techniques to *higher dimensional* systems with *nonlinear* dynamics, we then apply our results to a continuous-time *nonlinear* jet engine compressor and a *discrete-time* DC motor. In all three case studies, we collect data from trajectories of unknown systems with a uniform distribution.

5.4.6.1 Continuous-Time Case

Room Temperature. Consider the room temperature system in (5.4.21). The regions of interest here are $X = [17, 20], X_0 = [17, 18]$, and $X_u = [19, 20]$. We assume that the model is unknown to us. The main goal is to construct a BC via data collected from trajectories of the system by solving $\text{SCP}_{\tilde{\varepsilon}}$ (5.4.17) and accordingly verify if the temperature of the room stays within the comfort zone $[17, 19]$ according to Theorem 5.4.21.

We first fix the structure of our barrier certificate as $\mathcal{B}(q, x) = q_1 x^2 + q_2 x + q_3$. We now follow Algorithm 1 in order to utilize the results of Theorem 5.4.9. We first fix $\mathcal{N} = 1005$ and $\beta = 10^{-7}$, a-priori. Now we need to compute $\mathscr{L}_g$ which is required for checking the condition (5.4.7) in Theorem 5.4.9. Since the Lipschitz constant $\mathscr{L}_f$ is required for computing $\mathscr{L}_g$ according to Lemma 5.4.13, we employ Algorithm 2 to estimate it from sampled data. By considering $\bar{\mathcal{N}} = \bar{\mathcal{M}} = 1000$ and $\hat{\alpha} = \tau = 0.01$, we get $\mathscr{L}_f = 0.005$ which is exactly equal to the Lipschitz constant of the actual dynamic. We now construct matrix P based on coefficients of the barrier certificate. By considering each coefficient of the barrier between $[-0.2, 0.2]$, we ensure that $\rho_{spc}(P) \leq 0.4$ as discussed in Remark 5.4.14 and, accordingly, $\mathscr{L}_g = 12$. Given that the number of decision variables affects ε in (5.4.8), we fix $\psi = 0$ a-priori to enforce the safety property for an infinite time horizon (decision variables now are reduced to 6). We now compute ε in (5.4.8) as $\varepsilon = 0.0278$.

Now we need to compute $\tilde{\varepsilon}$ as in Theorem 5.4.26 which is required for solving the $\text{SCP}_{\tilde{\varepsilon}}$ (5.4.17) (*i.e.,* condition $\bar{g}_4$). We assume $\mathcal{M}_f$ is given to us as 0.2. By employing ranges of coefficients of the barrier, we compute $\mathcal{M}_{\mathcal{B}_1} \leq 8.2$ and $\mathscr{L}_{\mathcal{B}_1} \leq 0.4$. By selecting $\tau = 0.01$, the closeness between $\mathsf{L}_f\mathcal{B}(q, x)$ and $\widehat{\mathsf{L}}_f\mathcal{B}(q, x)$ is computed as $\tilde{\varepsilon} = 1.21 \times 10^{-4}$. Note that considering coefficients of barriers within $[-0.2, 0.2]$ enforces the additional

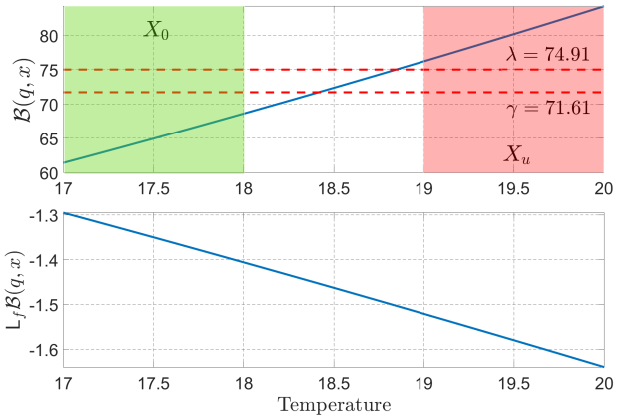

Figure 5.6: Barrier certificate of unknown room temperature model. Note that the barrier certificate is quadratic and only a small segment of this function between $[17, 20]$ is plotted here.

conditions as

$$-0.2 \leq q_1, q_2, q_3 \leq 0.2, \tag{5.4.24}$$

that should be enforced in solving $\text{SCP}_{\tilde{\varepsilon}}$ (5.4.17) as discussed in Remark 5.4.24. We now solve the $\text{SCP}_{\tilde{\varepsilon}}$ (5.4.17) with $\mathcal{N} = 1005, \tilde{\varepsilon} = 1.21 \times 10^{-4}$, and the additional conditions in (5.4.24). Coefficients of the barrier certificate together with other decision variables of $\text{SCP}_{\tilde{\varepsilon}}$ are computed as

$$\mathcal{B}(q,x) = 0.2x^2 + 0.2x + 0.2, \Phi^*_{\mathcal{N}} = -1.2952, \gamma^* = 71.6191, \lambda^* = 74.9146.$$

We now compute $\hat{g}(\varepsilon)$ according to Remark 5.4.10 as $\hat{g}(\varepsilon) = \frac{\varepsilon}{3}$. Since $\Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon) = -0.2960 \leq 0$, according to Theorem 5.4.21, one can guarantee that the temperature of the room with unknown dynamics remains in the safe set $[17, 19]$ for an infinite time horizon with a confidence of at least $1 - \beta = 1 - 10^{-7}$. The constructed barrier certificate from data is illustrated in Figure 5.6.

In order to have a practical analysis on the required number of collected data in Theorem 5.4.9, we plotted in Figure 5.7 the required number of data in terms of the threshold ε and the confidence β based on (5.4.8) for the room temperature problem. As it can be observed, the required number of data decreases by increasing either the threshold ε or the confidence β. However, in practice, one needs to select β as small as possible to provide a reasonable safety confidence (*i.e.,* $1 - \beta$) over the original unknown system. Besides, in order to ensure the safety of the unknown system with some confidence, condition $\Phi^*_{\mathcal{N}} + \mathscr{L}_g \hat{g}^{-1}(\varepsilon) \leq 0$ needs to hold. Consequently, selecting a smaller ε allows for larger optimal value $\Phi^*_{\mathcal{N}}$, and hence, conditions on the barrier certificates become more relaxed but at the cost of solving the $\text{SCP}_{\tilde{\varepsilon}}$ in (5.4.17) with a higher number of data as illustrated in Figure 5.7.

It is worth mentioning that by increasing the degree of BC, there is a higher chance of satisfying conditions g_1-g_4 but at the cost of considering a bigger ε in (5.4.8) given that the number of decision variables $\bar{z}$ also increases.

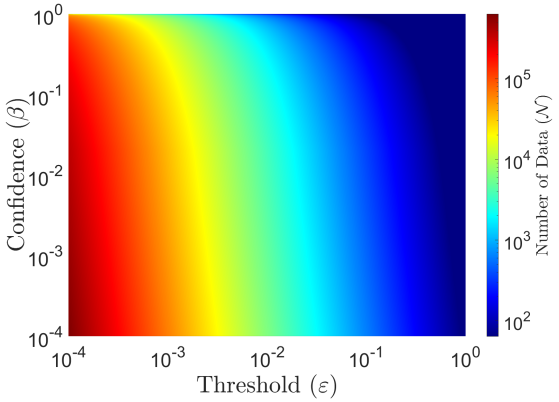

Figure 5.7: Required number of data, represented by 'colour bar', in terms of the threshold ε and the confidence β. Plot is in the logarithmic scale for $\mathscr{L}_g = 12$ and 6 decision variables. The required number of data decreases by increasing either the threshold ε or the confidence β.

Jet Engine. Consider the following *nonlinear* Moore-Greitzer jet engine model in no-stall mode [ZMEAL13]:

$$\Sigma_c : \begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -x_2(t) - \frac{3}{2}x_1^2(t) - \frac{1}{2}x_1^3(t) \\ x_1(t) \end{bmatrix},$$

where $x_1 = \bar{\Phi} - 1, x_2 = \bar{\Psi} - \bar{\Lambda} - 2$, with $\bar{\Phi}, \bar{\Psi}, \bar{\Lambda}$ being, respectively, the mass flow, the pressure rise, and a constant. The regions of interest here are $X = [0.1, 1]^2, X_0 = [0.1, 0.5]^2$, and $X_u = [0.7, 1]^2$. We assume that the model is unknown. The main goal is to construct a BC via data collected from trajectories of the system by solving $\text{SCP}_{\tilde{\varepsilon}}$ (5.4.17) and accordingly verify if $x(t) \in [0.1, 0.7)^2$ for some time t according to Theorem 5.4.21.

We fix the structure of our barrier function as $\mathcal{B}(q, x) = q_1x_1 + q_2x_1x_2 + q_3x_2 + q_4$. We also fix $\mathcal{N} = 257149$ and $\beta = 0.01$, a-priori. By employing Algorithm 2, we estimate $\mathscr{L}_f = 12.083$. We assume $\mathcal{M}_f$ is given to us as $\mathcal{M}_f = 12.1655$. By constructing matrix P and considering each coefficient of the barrier between $[-0.4, 0.4]$, we compute $\rho_{spc}(P) \leq 0.6$, and accordingly, $\mathscr{L}_g = 55.6098$. We fix $\lambda = 3.1$ and $\psi = 0$ a-priori, to reduce the number of decision variables to 5. We now compute ε in (5.4.8) as $\varepsilon = 4.5127 \times 10^{-5}$. Now we need to compute $\tilde{\varepsilon}$ as in Theorem 5.4.26. By considering ranges of coefficients of barriers between $[-0.4, 0.4]$, we compute $\mathcal{M}_{\mathcal{B}_1} \leq 3.3941$ and $\mathscr{L}_{\mathcal{B}_1} \leq 1.2649$. By selecting $\tau = 10^{-5}$, the closeness between $\mathsf{L}_f\mathcal{B}(q, x)$ and $\widehat{\mathsf{L}}_f\mathcal{B}(q, x)$ is computed as $\tilde{\varepsilon} = 3.4306 \times 10^{-4}$. We now solve the $\text{SCP}_{\tilde{\varepsilon}}$ (5.4.17) with $\mathcal{N} = 257149, \tilde{\varepsilon} = 3.4306 \times 10^{-4}$, and the additional conditions $-0.4 \leq q_1, q_2, q_3 \leq 0.4$. Coefficients of the barrier certificate

together with decision variables in $\text{SCP}_{\tilde{\varepsilon}}$ are computed as

$$\mathcal{B}(q,x) = 0.4x_1 + 0.4x_1x_2 - 0.0728x_2 + 2.7288, \Phi^*_{\mathcal{N}} = -0.0552, \gamma^* = 3.0455.$$

We now compute $\hat{g}(\varepsilon)$ according to Remark 5.4.10 as $\hat{g}(\varepsilon) = \frac{\pi}{3.24}\varepsilon^2$. Since $\Phi^*_{\mathcal{N}} + \mathscr{L}_g\hat{g}^{-1}(\varepsilon) = -2 \times 10^{-4} \leq 0$, according to Theorem 5.4.21, one can guarantee that $x(t) \in [0.1, 0.7)^2$ for all $t \in \mathbb{R}_{\geq 0}$ with a confidence of at least $1 - \beta = 99\%$.

Satisfaction of conditions (5.4.2)-(5.4.3) and (5.4.13) via constructed barrier certificate from data is illustrated in Figures 5.8 and 5.9. As observed in Figure 5.8, the initial set $X_0 = [0.1, 0.5]^2$ is inside the γ-level set of the barrier certificate (*i.e.,* $\mathcal{B}(q,x) = \gamma$) and the unsafe set $X_u = [0.7, 1]^2$ is outside the λ-level set of the barrier certificate (*i.e.,* $\mathcal{B}(q,x) = \lambda$). Moreover, in Figure 5.9, condition (5.4.13) is non-positive for all ranges of $x_1 \in [0.1, 1]$ and $x_2 \in [0.1, 1]$.

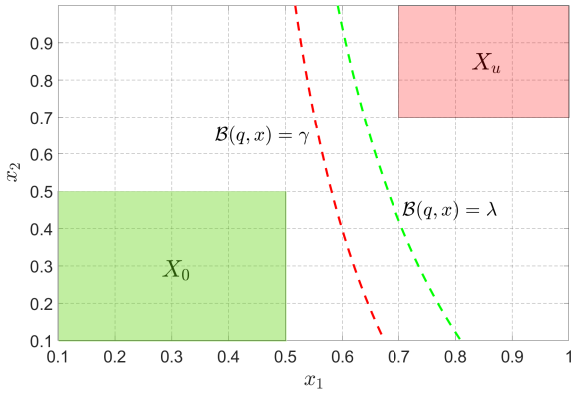

Figure 5.8: Jet engine: Satisfaction of conditions (5.4.2)-(5.4.3). Initial set is inside the γ-level set of the barrier certificate (*i.e.,* $\mathcal{B}(q,x) = \gamma$) and the unsafe set is outside the λ-level set of the barrier certificate (*i.e.,* $\mathcal{B}(q,x) = \lambda$).

5.4.6.2 Discrete-Time Case

DC Motor. Our third case study is a discrete-time DC motor adapted from [Ade13] as follows:

$$x_1(k+1) = x_1(k) + \tau\big(\frac{-\bar{R}}{\bar{L}}x_1(k) - \frac{k_{dc}}{\bar{L}}x_2(k)\big),$$
$$x_2(k+1) = x_2(k) + \tau\big(\frac{k_{dc}}{\bar{J}}x_1(k) - \frac{b}{\bar{J}}x_2(k)\big),$$

where $x_1, x_2, \bar{R} = 1, \bar{L} = 0.5$, and $\bar{J} = 0.01$ are the armature current, the rotational speed of the shaft, the electric resistance, the electric inductance, and the moment of inertia of the rotor, respectively. In addition, $\tau = 0.01, b = 0.1$, and $K_{dc} = 0.01$ which represents both the motor torque and the back electromotive force. The regions of interest here are $X = [0.1, 0.5] \times [0.1, 1]$, $X_0 = [0.1, 0.4] \times [0.1, 0.55]$, and $X_u = [0.45, 0.5] \times [0.6, 1]$. We

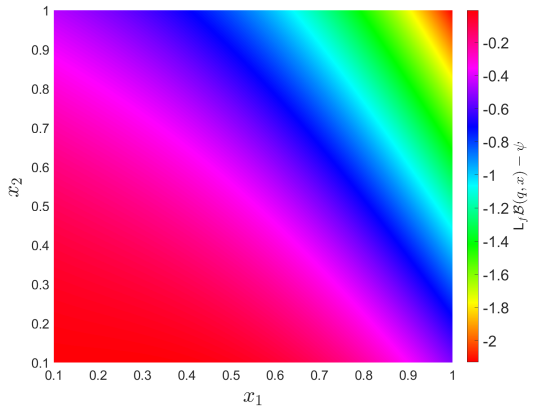

Figure 5.9: Jet engine: Satisfaction of condition (5.4.13). This condition is non-positive for all ranges of $x_1 \in [0.1, 1]$ and $x_2 \in [0.1, 1]$.

assume that the model is unknown. The main goal is to construct a BC via collected data by solving SCP (5.4.6) and accordingly verify if $x \in [0.1, 0.45) \times [0.1, 0.6)$ based on Theorem 5.4.9 for infinite time horizons.

We fix the structure of our barrier function as $\mathcal{B}(q, x) = q_1 x_1^2 + q_2 x_1 x_2 + q_3 x_2^2 + q_4$. We follow Algorithm 1 in order to utilize the results of Theorem 5.4.9. We first fix $\mathcal{N} = 82821$ and $\beta = 0.05$, a-priori. Now we employ Algorithm 2 and estimate Lipschitz constant of the system as $\mathscr{L}_f \leq 1$. Let $\mathcal{M}_f$ be given to us as $\mathcal{M}_f \leq 1$. By constructing matrix P and considering each coefficient of the barrier within $[-0.5, 0.5]$, we compute $\rho_{spc}(P) \leq 1$, and accordingly, $\mathscr{L}_g = 1.67$. We fix $\psi = 0$ a-priori, to reduce the number of decision variables to 7. We now compute ε in (5.4.8) as $\varepsilon = 1.76 \times 10^{-4}$. We then solve the SCP (5.4.6) with $\mathcal{N} = 82821$ and compute coefficients of the barrier certificate together with other decision variables as

$$\mathcal{B}(q, x) = 0.5x_1^2 + 0.5x_1x_2 + 0.5x_2^2 + 0.5, \Phi^*_{\mathcal{N}} = -0.0155, \gamma = 0.8882, \lambda = 0.9035.$$

We now compute $\hat{g}(\varepsilon)$ according to Remark 5.4.10 as $\hat{g}(\varepsilon) = \frac{\pi}{1.44}\varepsilon^2$. Since $\Phi^*_{\mathcal{N}} + \mathscr{L}_g\hat{g}^{-1}(\varepsilon) = -5 \times 10^{-4} \leq 0$, according to Theorem 5.4.9, one can guarantee that $x(k) \in x \in [0.1, 0.45) \times [0.1, 0.6)$ for all $t \in \mathbb{R}_{\geq 0}$ with a confidence of at least $1 - \beta = 95\%$.

Satisfaction of conditions (5.4.2)-(5.4.4) via constructed barrier certificate from data is illustrated in Figures 5.10 and 5.11.

5.5 Data-Driven Controller Synthesis of Unknown Nonlinear Polynomial Systems

In this section, we propose a data-driven approach to *synthesize* safety controllers for continuous-time nonlinear polynomial-type systems with unknown models. In our proposed framework, we leverage *control* barrier certificates constructed from data and

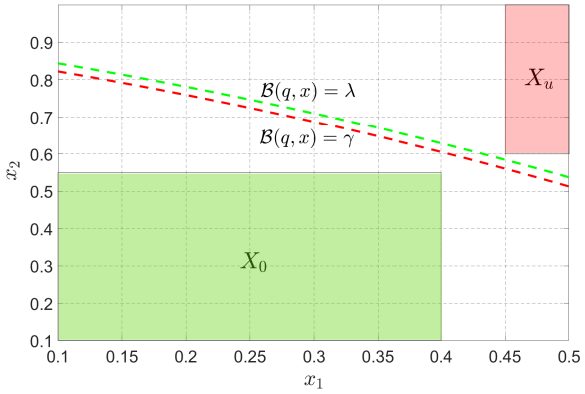

Figure 5.10: DC motor: Satisfaction of conditions (5.4.2)-(5.4.3). As seen, the initial set is inside the γ-level set of the barrier certificate (*i.e.,* $\mathcal{B}(q,x)=\gamma$) and the unsafe set is outside the λ-level set of the barrier certificate (*i.e.,* $\mathcal{B}(q,x)=\lambda$).

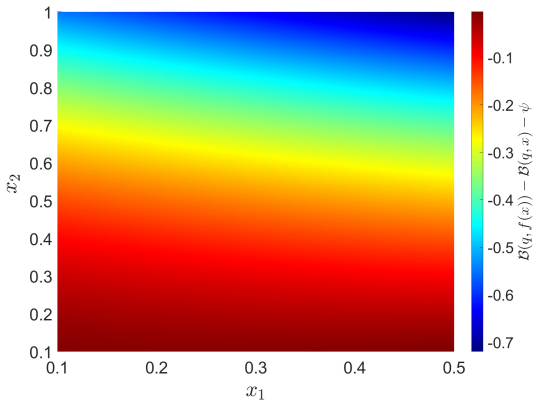

Figure 5.11: DC motor: Satisfaction of condition (5.4.4). As observed, the condition is non-positive for all ranges of $x_1 \in [0.1, 0.5]$ and $x_2 \in [0.1, 1]$.

provide guaranteed *confidence of* 1 on the safety of unknown systems. Under a certain rank condition, which is closely related to the condition of *persistency of excitation* [WRMDM05], we synthesize polynomial-type state-feedback controllers to ensure the safety of unknown systems only by using a *single trajectory* collected from systems. To illustrate the effectiveness of our proposed approaches, we apply them to a nonlinear polynomial system with unknown dynamics.

5.5.1 Continuous-Time Nonlinear Polynomial Systems

Here, we consider continuous-time nonlinear polynomial systems (ct-NPS) as formalized in the following definition.

Definition 5.5.1. *A continuous-time nonlinear polynomial system (ct-NPS) is described by*

$$\Sigma\colon \dot{x} = A\tilde{\mathcal{M}}(x) + B\nu, \tag{5.5.1}$$

where $A \in \mathbb{R}^{n\times\tilde{N}}, B \in \mathbb{R}^{n\times\bar{m}}$, $\tilde{\mathcal{M}}(x) \in \mathbb{R}^{\tilde{N}}$ *is a vector of monomials in state* $x \in X$, *and* $\nu \in U$ *is the control input, with* $X \subset \mathbb{R}^n$ *and* $U \subset \mathbb{R}^{\bar{m}}$ *being the state and input sets, respectively.*

We assume that matrices A, B are both unknown and we employ the term *unknown model* to refer to this type of systems in (5.5.1). With this definition in hand, we now state the main problem that we aim to solve in this section.

Problem 5.5.2. *Consider a ct-NPS in* (5.5.1) *with unknown matrices* A, B, *and an initial and unsafe sets* $X_0, X_u \subset X$, *respectively. Synthesize a matrix polynomial* $\tilde{F}(x)$ *such that controller* $\nu = \tilde{F}(x)\tilde{\mathcal{M}}(x)$ *makes the unknown ct-NPS* (5.5.1) *safe in the sense that its trajectories starting from* X_0 *never reach* X_u.

In order to address Problem 5.5.2, we present a definition of control barrier certificates for ct-NPS in the next subsection.

5.5.2 Control Barrier Certificates (CBC)

Definition 5.5.3. *Consider the ct-NPS* Σ, *and* $X_0, X_u \subseteq X$ *as its initial and unsafe sets, respectively. A function* $\mathcal{B} : X \to \mathbb{R}$ *is called a control barrier certificate (CBC) for* Σ *if there exist* $\gamma, \lambda \in \mathbb{R}_{>0}$, *with* $\lambda > \gamma$, *such that*

$$\mathcal{B}(x) \leq \gamma, \qquad \forall x \in X_0, \tag{5.5.2}$$
$$\mathcal{B}(x) \geq \lambda, \qquad \forall x \in X_u, \tag{5.5.3}$$

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

$$\mathsf{L}\mathcal{B}(x) \leq 0, \tag{5.5.4}$$

where $\mathsf{L}\mathcal{B}$ *is the Lie derivative of* $\mathcal{B} : X \to \mathbb{R}$ *with respect to dynamics as in* (5.5.1), *which is defined as*

$$\mathsf{L}\mathcal{B}(x) = \partial_x\mathcal{B}(x)(A\tilde{\mathcal{M}}(x) + B\nu), \tag{5.5.5}$$

with $\partial_x\mathcal{B}(x) = \left[\frac{\partial\mathcal{B}(x)}{\partial x_i}\right]_i$.

We denote by $x_{x_0\nu}(t)$ the state of Σ reached at time $t \in \mathbb{R}_{\geq 0}$ under an input ν and from an initial condition $x_0 = x(0)$. Inspired by [PJ04], we present the next theorem showing how to use CBC to ensure that the state evolution of Σ starting from any initial state in X_0 will never reach the unsafe region X_u for an infinite time horizon.

Theorem 5.5.4. *Consider a ct-NPS* Σ. *Suppose* $\mathcal{B}$ *is a CBC for* Σ *as in Definition 5.5.3. Then, one gets* $x_{x_0\nu}(t) \notin X_u$ *for any* $x_0 \in X_0$ *and any* $t \in \mathbb{R}_{\geq 0}$, *where the control input* ν *is chosen in a way that* (5.5.4) *holds.*

5.5.3 Data-Driven Synthesis of Safety Controller

Here, we propose our data-driven approach to synthesize safety controllers for unknown ct-NPS in (5.5.1). To do so, we first fix the structure of our CBC to be quadratic in the form of $\mathcal{B}(x) = \tilde{\mathcal{M}}(x)^\top \bar{P} \tilde{\mathcal{M}}(x)$, with $\bar{P} \succ 0$. We then collect input-output data from unknown ct-NPS over the time interval $[t_0, t_0 + (\tilde{T}-1)\tau]$, where $\tilde{T} \in \mathbb{N}_{>0}$ is the number of collected samples, and $\tau \in \mathbb{R}_{>0}$ is the sampling time:

$$\mathcal{U}_{0,\tilde{T}} = [\nu(t_0) \;\; \nu(t_0+\tau) \;\; \dots \;\; \nu(t_0+(\tilde{T}-1)\tau)], \tag{5.5.6}$$

$$\mathcal{X}_{0,\tilde{T}} = [x(t_0) \;\; x(t_0+\tau) \;\; \dots \;\; x(t_0+(\tilde{T}-1)\tau)], \tag{5.5.7}$$

$$\mathcal{X}_{1,\tilde{T}} = [\dot{x}(t_0) \;\; \dot{x}(t_0+\tau) \;\; \dots \;\; \dot{x}(t_0+(\tilde{T}-1)\tau)]. \tag{5.5.8}$$

Remark 5.5.5. *Note that $\mathcal{X}_{1,\tilde{T}}$ contains derivatives of the state at sampling times, which are in general not available as measurements. In order to tackle this issue, one can use appropriate filters for the approximation of derivatives via the available approaches proposed in the relevant literature (e.g., [LMS08, PA15]).*

Inspired by [GDPT20], we present the following lemma to obtain *data-based representation* of closed-loop ct-NPS (5.5.1) with polynomial controllers $\nu = \tilde{F}(x)\tilde{\mathcal{M}}(x)$, where $\tilde{F}(x)$ is a matrix polynomial, which will be synthesized.

Lemma 5.5.6. *Let matrix $\mathcal{Q}(x)$ be a $(\tilde{T} \times \tilde{N})$ matrix polynomial such that*

$$\mathbb{I}_{\tilde{N}} = \mathcal{N}_{0,\tilde{T}} \mathcal{Q}(x),$$

with

$$\tilde{\mathcal{N}}_{0,\tilde{T}} = [\tilde{\mathcal{M}}(x(t_0)) \;\; \tilde{\mathcal{M}}(x(t_0+\tau)) \;\; \dots \;\; \tilde{\mathcal{M}}(x(t_0+(\tilde{T}-1)\tau))]$$

being an $(\tilde{N} \times \tilde{T})$ full row-rank matrix, constructed from the vector $\tilde{\mathcal{M}}(x)$ and samples $\mathcal{X}_{0,\tilde{T}}$. If one sets $\nu = \tilde{F}(x)\tilde{\mathcal{M}}(x) = \mathcal{U}_{0,\tilde{T}}\mathcal{Q}(x)\tilde{\mathcal{M}}(x)$, then the closed-loop system $\dot{x} = A\tilde{\mathcal{M}}(x) + B\nu$ has the following data-based representation:

$$\dot{x} = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)\tilde{\mathcal{M}}(x), \;\; \textit{equivalently,} \;\; A + B\tilde{F} = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x).$$

Proof. Since $\tilde{F}(x) = \mathcal{U}_{0,\tilde{T}}\mathcal{Q}(x)$, the closed-loop ct-NPS can be written as

$$(A + B\tilde{F}(x))\tilde{\mathcal{M}}(x) = [B \;\; A]\begin{bmatrix}\tilde{F}(x) \\ \mathbb{I}_{\tilde{N}}\end{bmatrix}\tilde{\mathcal{M}}(x) = [B \;\; A]\begin{bmatrix}\mathcal{U}_{0,\tilde{T}} \\ \tilde{\mathcal{N}}_{0,\tilde{T}}\end{bmatrix}\mathcal{Q}(x)\tilde{\mathcal{M}}(x) = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)\tilde{\mathcal{M}}(x),$$

with $\mathcal{X}_{1,\tilde{T}} = [B \; A]\begin{bmatrix}\mathcal{U}_{0,\tilde{T}} \\ \tilde{\mathcal{N}}_{0,\tilde{T}}\end{bmatrix}$ and $\mathcal{U}_{0,\tilde{T}}$ as in (5.5.6). Hence, $\dot{x} = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)\tilde{\mathcal{M}}(x)$, equivalently, $A + B\tilde{N}F = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)$ is the data-based representation of the closed-loop ct-NPS, which completes the proof. ■

Remark 5.5.7. *Note that in order to enforce $\tilde{\mathcal{N}}_{0,\tilde{T}}$ to be full row rank, the number of samples $\tilde{T}$ should be at least $\tilde{N}$. Since the matrix $\tilde{\mathcal{N}}_{0,\tilde{T}}$ is constructed from sampled data, this assumption is readily verifiable.*

By employing the data-based representation in Lemma 5.5.6, we propose the following theorem, as the main result of this section, to construct a CBC from data and synthesize the control gain $\tilde{F}(x)$ making the unknown ct-NPS in (5.5.1) safe.

Theorem 5.5.8. *Consider an unknown ct-NPS Σ as in* (5.5.1)*, i.e., $\dot{x} = A\tilde{\mathcal{M}}(x) + B\nu$, with its data-based representation $\dot{x} = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)\tilde{\mathcal{M}}(x)$. Suppose there exists a matrix polynomial $\tilde{\mathcal{H}}(x) \in \mathbb{R}^{\tilde{T}\times\tilde{N}}$ such that*

$$\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x) = \bar{P}^{-1}, \quad \text{with } \bar{P} \succ 0.$$

If the following conditions are satisfied

- $\forall x \in X_0$,

$$\tilde{\mathcal{M}}(x)^\top \big[\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\big]^{-1}\tilde{\mathcal{M}}(x) \leq \gamma, \tag{5.5.9}$$

- $\forall x \in X_u$,

$$\tilde{\mathcal{M}}(x)^\top \big[\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\big]^{-1}\tilde{\mathcal{M}}(x) \geq \lambda, \tag{5.5.10}$$

- $\forall x \in X$,

$$\mathcal{J}(x) := -\Big[\frac{\partial\tilde{\mathcal{M}}}{\partial x}\mathcal{X}_{1,\tilde{T}}\tilde{\mathcal{H}}(x) + \tilde{\mathcal{H}}(x)^\top\mathcal{X}_{1,\tilde{T}}^\top(\frac{\partial\tilde{\mathcal{M}}}{\partial x})^\top\Big] \succeq 0, \tag{5.5.11}$$

then $\mathcal{B}(x) = \tilde{\mathcal{M}}(x)^\top(\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x))^{-1}\tilde{\mathcal{M}}(x)$ is a CBC and $\nu = \mathcal{U}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)(\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x))^{-1}\tilde{\mathcal{M}}(x)$ is its corresponding safety controller for the unknown ct-NPS.

Proof. Since $\mathcal{B}(x) = \tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x)$ and $\bar{P}^{-1} = \tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)$, it is straightforward that conditions (5.5.9)-(5.5.10) imply (5.5.2)-(5.5.3). We now proceed with showing condition (5.5.4), as well. Considering (5.5.4) and (5.5.5), one has

$$\begin{aligned}\mathsf{L}\mathcal{B}(x) &= \tilde{\mathcal{M}}(x)^\top\bar{P}\frac{\partial\tilde{\mathcal{M}}}{\partial x}(A + B\tilde{F}(x))\tilde{\mathcal{M}}(x) + \tilde{\mathcal{M}}(x)^\top(A + B\tilde{F}(x))^\top(\frac{\partial\tilde{\mathcal{M}}}{\partial x})^\top\bar{P}\tilde{\mathcal{M}}(x)\\ &= \tilde{\mathcal{M}}(x)^\top\bar{P}\Big[\frac{\partial\tilde{\mathcal{M}}}{\partial x}(A + B\tilde{F}(x))\bar{P}^{-1} + \bar{P}^{-1}(A + B\tilde{F}(x))^\top(\frac{\partial\tilde{\mathcal{M}}}{\partial x})^\top\Big]\bar{P}\tilde{\mathcal{M}}(x).\end{aligned}$$

Since $\bar{P}^{-1} = \tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)$, then $\bar{P}^{-1}\bar{P} = \mathbb{I}_{\tilde{N}} = \tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\bar{P}$. Since $\mathbb{I}_{\tilde{N}} = \tilde{\mathcal{N}}_{0,\tilde{T}}\mathcal{Q}(x)$, then $\mathcal{Q}(x) = \tilde{\mathcal{H}}(x)\bar{P}$ and, accordingly, $\mathcal{Q}(x)\bar{P}^{-1} = \tilde{\mathcal{H}}(x)$. Since $A + B\tilde{F}(x) = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)$, then

$$(A + B\tilde{F}(x))\bar{P}^{-1} = \mathcal{X}_{1,\tilde{T}}\mathcal{Q}(x)\bar{P}^{-1} = \mathcal{X}_{1,\tilde{T}}\tilde{\mathcal{H}}(x).$$

Therefore,

$$\mathsf{L}\mathcal{B}(x)=\tilde{\mathcal{M}}(x)^\top\bar{P}\Big[\frac{\partial\tilde{\mathcal{M}}}{\partial x}\mathcal{X}_{1,\tilde{T}}\tilde{\mathcal{H}}(x)+\tilde{\mathcal{H}}(x)^\top\mathcal{X}_{1,\tilde{T}}^\top(\frac{\partial\tilde{\mathcal{M}}}{\partial x})^\top\Big]\bar{P}\tilde{\mathcal{M}}(x)=-\tilde{\mathcal{M}}(x)^\top\bar{P}\big[\mathcal{J}(x)\big]\bar{P}\tilde{\mathcal{M}}(x).$$

If $\mathcal{J}(x)\succeq 0$, then $\mathsf{L}\mathcal{B}(x)\preceq 0$ and condition (5.5.4) is satisfied. Consequently,

$$\mathcal{B}(x)=\tilde{\mathcal{M}}(x)^\top(\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x))^{-1}\tilde{\mathcal{M}}(x)$$

is a CBC and

$$\nu=\mathcal{U}_{0,\tilde{T}}\mathcal{Q}(x)\tilde{\mathcal{M}}(x)=\mathcal{U}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)(\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x))^{-1}\tilde{\mathcal{M}}(x)$$

is its corresponding safety controller for the unknown ct-NPS, which completes the proof. ■

Remark 5.5.9. *Note that in practice, in order to satisfy condition* (5.5.11)*, some a-priori information about unknown systems, such as physical considerations, can be useful to get insights on the most appropriate choice of* $\tilde{\mathcal{M}}(x)$*.*

In the remainder of this section, we discuss the implementation of Theorem 5.5.8. Here, we consider the state set X, initial set X_0, and unsafe set X_u as

$$X=\bigcup_{i=1}^{m_x}X_i,\quad\text{with } X_i:=\{x\in\mathbb{R}^n\,\big|\,\tilde{g}_{i_k}(x)\geq 0,k=1,\ldots,\mathsf{k}\},\tag{5.5.12}$$

$$X_0=\bigcup_{i=1}^{m_0}X_{0_i},\ \text{with } X_{0_i}:=\{x\in\mathbb{R}^n\,\big|\,\tilde{f}_{i_k}(x)\geq 0,k=1,\ldots,\mathsf{k}_0\},\tag{5.5.13}$$

$$X_u=\bigcup_{i=1}^{m_1}X_{u_i},\ \text{with } X_{u_i}:=\{x\in\mathbb{R}^n\,\big|\,\tilde{h}_{i_k}(x)\geq 0,k=1,\ldots,\mathsf{k}_1\},\tag{5.5.14}$$

with $\tilde{g}_{ik}(x)$, $\tilde{f}_{ik}(x)$, and $\tilde{h}_{ik}(x)$ being polynomial. The input set U is defined as

$$U:=\{\nu\in\mathbb{R}^{\bar{m}}\,\big|\,b_j^\top\nu\leq 1,\ \text{with } j=1,\ldots,\bar{\mathcal{J}}\},\tag{5.5.15}$$

with $b_j\in\mathbb{R}^{\bar{m}}$ being some constant vectors. Additionally, we raise the following corollary which is required for our implementation results.

Corollary 5.5.10. *Consider a CBC* $\mathcal{B}(x)=\tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x)$ *with* $\bar{P}\succ 0$ *as in Definition 5.5.3 for a ct-NPS* Σ *in* (5.5.1)*, and* $\tilde{\gamma}\in\mathbb{R}_{>0}$*. If* $\tilde{\mathcal{M}}(x(0))^\top\bar{P}\tilde{\mathcal{M}}(x(0))\leq\tilde{\gamma}$*, then* $\tilde{\mathcal{M}}(x(t))^\top\bar{P}\tilde{\mathcal{M}}(x(t))\leq\tilde{\gamma}$ *for all* $t\in\mathbb{R}_{>0}$*.*

Corollary 5.5.10 can readily be verified with the help of non-positiveness of $\mathsf{L}\mathcal{B}(x)$ (5.5.4). By employing Corollary 5.5.10, we are ready to show the next result for computing a CBC and its associated safety controller.

Corollary 5.5.11. *Consider a ct-NPS Σ as in* (5.5.1)*, sets X, X_0, and X_u as in* (5.5.12)-(5.5.14)*, respectively, an input set U as in* (5.5.15)*, and data $\mathcal{U}_{0,\tilde{T}}$, $\mathcal{X}_{1,\tilde{T}}$, and $\tilde{\mathcal{N}}_{0,\tilde{T}}$ as in* (5.5.6)*,* (5.5.8)*, and Lemma 5.5.6, respectively. If there exist a positive definite matrix $\bar{P} \in \mathbb{R}^{\tilde{N}\times\tilde{N}}$, a matrix polynomial $\tilde{\mathcal{H}}(x) \in \mathbb{R}^{\tilde{T}\times\tilde{N}}$, and $\gamma, \lambda \in \mathbb{R}_{>0}$, with $\lambda > \gamma$ such that*

$$-\tilde{\mathcal{M}}(x)^\top \bar{P}\tilde{\mathcal{M}}(x) - \sum_{k=1}^{\mathsf{k}_0}\tilde{\lambda}'_{i_k}(x)\tilde{f}_{i_k}(x) + \gamma, \forall i \in [1, m_0], \forall k \in [1, \mathsf{k}_0], \tag{5.5.16}$$

$$\tilde{\mathcal{M}}(x)^\top \bar{P}\tilde{\mathcal{M}}(x) - \sum_{k=1}^{\mathsf{k}_1}\tilde{\lambda}''_{i_k}(x)\tilde{h}_{i_k}(x) - \lambda, \forall i \in [1, m_1], \forall k \in [1, \mathsf{k}_1], \tag{5.5.17}$$

$$-[\frac{\partial\tilde{\mathcal{M}}}{\partial x}\mathcal{X}_{1,\tilde{T}}\tilde{\mathcal{H}}(x) + \tilde{\mathcal{H}}(x)^\top\mathcal{X}_{1,\tilde{T}}^\top(\frac{\partial\tilde{\mathcal{M}}}{\partial x})^\top] - \sum_{k=1}^{\mathsf{k}}\tilde{\lambda}_{i_k}(x)\tilde{g}_{i_k}(x)\mathbb{I}_N, \forall i \in [1, m_x], \forall k \in [1, \mathsf{k}], \tag{5.5.18}$$

$$1 - b_j^\top\mathcal{U}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\bar{P}\tilde{\mathcal{M}}(x) - \tilde{\lambda}_u(x)\Big(\gamma - \tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x)\Big), \forall j = 1, \ldots, \bar{\mathcal{J}}, \tag{5.5.19}$$

are sum-of-square (SOS), with $\tilde{\lambda}_{i_k}(x)$, $\tilde{\lambda}'_{i_k}(x)$, $\tilde{\lambda}''_{i_k}(x)$, and $\tilde{\lambda}_u(x)$ being SOS polynomials, and $\mathbb{I}_{\tilde{N}} = \bar{P}\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)$, then $\mathcal{B}(x) = \tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x)$ is a CBC for Σ with the corresponding safety controller $\nu = \mathcal{U}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\bar{P}\tilde{\mathcal{M}}(x)$.

Proof. It is straightforward that if (5.5.16) holds, then one has $\tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x) + \sum_{k=1}^{\mathsf{k}_0}\tilde{\lambda}'_{i_k}(x)\tilde{f}_{i_k}(x) \leq \gamma$, $\forall i \in [1, m_0], \forall k \in [1, \mathsf{k}_0]$. Since $\tilde{\lambda}'_{i_k}(x)$ are SOS polynomials, then $\sum_{k=1}^{\mathsf{k}}\tilde{\lambda}_{i_k}(x)\tilde{g}_{i_k}(x)$ are non-negative given the definition of X_0 in (5.5.13). Hence, $\tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x) \leq \gamma$ holds $\forall x \in X_0$, indicating that (5.5.9) holds with $\bar{P} = \big[\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\big]^{-1}$. Similarly, (5.5.17) implies that $\tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x) - \sum_{k=1}^{\mathsf{k}_1}\tilde{\lambda}''_{i_k}(x)\tilde{h}_{i_k}(x) \geq \lambda, \forall i \in [1, m_1], \forall k \in [1, \mathsf{k}_1]$. Since $\tilde{\lambda}''_{i_k}(x)$ are SOS polynomials, one has $\sum_{k=1}^{\mathsf{k}_1}\tilde{\lambda}''_{i_k}(x)\tilde{h}_{i_k}(x) \geq 0$, and accordingly $\tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x) \geq \lambda$ for all $x \in X_u$, indicating that (5.5.10) holds with $\bar{P} = \big[\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\big]^{-1}$. Next, we show that (5.5.18) implies that

$$\mathcal{J}_i(x) := -[\frac{\partial\tilde{\mathcal{M}}}{\partial x}\mathcal{X}_{1,\tilde{T}}\tilde{\mathcal{H}}(x) + \tilde{\mathcal{H}}(x)^\top\mathcal{X}_{1,\tilde{T}}^\top(\frac{\partial\tilde{\mathcal{M}}}{\partial x})^\top] \succeq 0$$

hold for all $x \in X_i$, $i \in [1, m_x]$. First, (5.5.18) is SOS implying that $\mathcal{J}_i(x) - \sum_{k=1}^{\mathsf{k}}\tilde{\lambda}_{i_k}(x)$ $\tilde{g}_{i_k}(x)\mathbb{I}_{\tilde{N}} \succeq 0$. Since $\tilde{\lambda}_{i_k}(x)$ are SOS polynomials for all $k \in [1, \mathsf{k}]$, $\sum_{k=1}^{\mathsf{k}}\tilde{\lambda}_{i_k}(x)\tilde{g}_{i_k}(x)$ are non-negative over X_i. Then, one can readily verify that $\mathcal{J}_i(x) \succeq 0$, $\forall x \in X_i$, and (5.5.11) holds accordingly. Finally, we show that (5.5.19) ensures that $\nu = \mathcal{U}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)\bar{P}\tilde{\mathcal{M}}(x) \in U$ for all $x \in \mathcal{B}_1(x)$ with $\mathcal{B}_1(x) := \{x \in \mathbb{R}^n | \tilde{\mathcal{M}}(x)^\top\bar{P}\tilde{\mathcal{M}}(x) \leq \gamma\}$, and $\mathbb{I}_{\tilde{N}} = \bar{P}\tilde{\mathcal{N}}_{0,\tilde{T}}\tilde{\mathcal{H}}(x)$. Note that we only need to consider the set $\mathcal{B}_1(x)$ instead of the whole state set X since

Corollary 5.5.10 shows that state trajectories of the system stay inside the set $\mathcal{B}_1(x)$. Considering the definition of U as in (5.5.15), $\nu \in U$ requires that

$$b_j^\top \mathcal{U}_{0,\tilde{T}} \tilde{\mathcal{H}}(x) \bar{P} \tilde{\mathcal{M}}(x) \leq 1, \tag{5.5.20}$$

holds $\forall j = 1, \ldots, \bar{\mathcal{J}}$, and $\forall x \in \mathcal{B}_1(x)$. Note that (5.5.19) implies that $b_j^\top \mathcal{U}_{0,\tilde{T}} \tilde{\mathcal{H}}(x) \bar{P} \tilde{\mathcal{M}}(x) + \tilde{\lambda}_u(x)(\gamma - \tilde{\mathcal{M}}(x)^\top \bar{P} \tilde{\mathcal{M}}(x)) \leq 1$. Hence, (5.5.20) holds since $\tilde{\lambda}_u$ is an SOS polynomial. ■

Remark 5.5.12. *One can employ existing software tools in the relevant literature such as SOSTOOLS [PAV+13] together with a semidefinite programming (SDP) solver such as SeDuMi [Stu99] to readily enforce conditions* (5.5.16)-(5.5.19) *over the sets* X_0, X_u,*and* X*, while searching for the matrix polynomial* $\tilde{\mathcal{H}}(x)$ *and matrix* $\bar{P}$*.*

Remark 5.5.13. *Note that condition* (5.5.19) *is a bilinear matrix inequality (BMI) due to having a bilinearity between decision matrices* $\tilde{\mathcal{H}}$ *and* $\bar{P}$*. In order to resolve this problem, one can first obtain a candidate for* $\bar{P}$ *based on* (5.5.16) *and* (5.5.17)*, and then try to search for appropriate* $\tilde{\mathcal{H}}(x)$ *such that* (5.5.18) *and* (5.5.19) *hold. As an alternative approach, one can also use the technique proposed in [HHB99] to linearize the BMI using a first-order perturbation approximation and then solve the linearized version.*

5.5.4 Case Study

Here, we focus on the following nonlinear polynomial system borrowed from [GDPT20]:

$$\begin{aligned} \dot{x}_1 &= x_2, \\ \dot{x}_2 &= x_1^2 + \nu, \end{aligned} \tag{5.5.21}$$

which is of the form of (5.5.1), with

$$A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \tilde{\mathcal{M}}(x) = \begin{bmatrix} x_2 \\ x_1^2 \end{bmatrix},$$

and $n = \tilde{N} = 2$. Here, we consider the state set $X = [-20, 20] \times [-20, 20]$, the initial set $X_0 = [-2.5, 2.5] \times [-2.5, 2.5]$, the unsafe set $X_u = [-20, 20] \times [10, 20] \cup [-20, 0] \times [-20, -10] \cup [3.5, 7] \times [-4, 0]$, and the input set $U = [-30, 30]$. We assume that both matrices A and B are unknown and treat this system as a black-box one.

To collect data, we initialize the system at $x(0) = [2; 3]$ and simulate the system with inputs that are randomly selected from the input set following a uniform distribution. The data are collected with a sampling time $\tau = 0.02s$ as follows:

$$\begin{aligned} \mathcal{U}_{0,5} &= \begin{bmatrix} 0.8134 & 3.6710 & -0.4437 & -1.9421 & -0.7241 \end{bmatrix}, \\ \mathcal{X}_{0,5} &= \begin{bmatrix} 2 & 2.0610 & 2.1246 & 2.1906 & 2.2581 \\ 3 & 3.0987 & 3.2597 & 3.3439 & 3.4040 \end{bmatrix}, \\ \mathcal{X}_{1,5} &= \begin{bmatrix} 3 & 3.0987 & 3.2597 & 3.3439 & 3.4040 \\ 4.8134 & 7.9186 & 4.0701 & 2.8565 & 4.3747 \end{bmatrix}. \end{aligned}$$

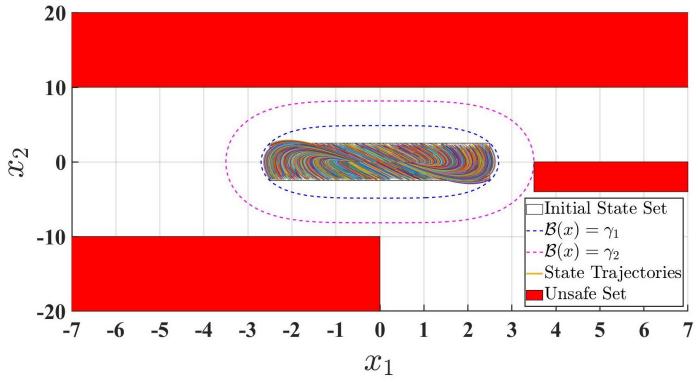

Figure 5.12: Several state trajectories, initial set X_0, unsafe set X_u, and level sets $\tilde{\mathcal{M}}(x)^\top \bar{P}\tilde{\mathcal{M}}(x) = \gamma$ and $\tilde{\mathcal{M}}(x)^\top \bar{P}\tilde{\mathcal{M}}(x) = \lambda$.

Accordingly, one has

$$\tilde{\mathcal{N}}_{0,5} = \begin{bmatrix} 3 & 3.0987 & 3.2597 & 3.3439 & 3.4040 \\ 4 & 4.2476 & 4.5137 & 4.7986 & 5.0988 \end{bmatrix},$$

with $\tilde{\mathcal{N}}_{0,5}$ being defined as in Lemma 5.5.6 with $\tilde{T} = 5$. With the help of Theorem 5.5.8 and Corollary 5.5.11, we obtain

$$\tilde{\mathcal{H}}(x) = \begin{bmatrix} 0.4266 & 0.07214x_1 - 0.3641 \\ -0.2245 & -0.1001x_1 - 0.0333 \\ 0.2831 & 0.0047x_1 - 0.3398 \\ 0.1311 & 0.0097x_1 - 0.3049 \\ -0.5217 & 0.01334x_1 + 0.9762 \end{bmatrix}, \quad \bar{P} = \begin{bmatrix} 5.8938 & 0 \\ 0 & 2.6160 \end{bmatrix},$$

with $\gamma = 139.03$, and $\lambda = 392.56$. The associated safety controller is designed as

$$\nu = -0.8877x_1^3 - x_1^2 - 2.8264x_2. \tag{5.5.22}$$

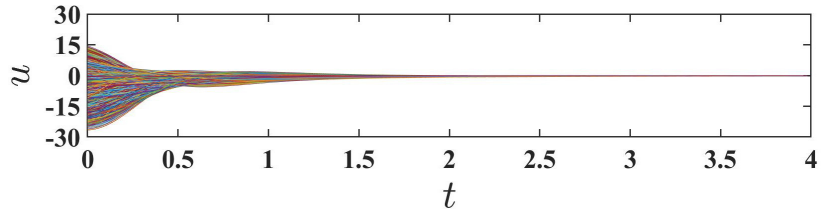

Figure 5.13: Several input trajectories of the system.

For the simulation results, we randomly select 10^5 initial states from the initial state set and simulate the system for 4 seconds, while the controller in (5.5.22) is applied in the closed-loop. We depicted some state and input trajectories in Figures 5.12 and 5.13, respectively. Moreover, we also depicted in Figure 5.12 the initial set X_0, the unsafe set X_u, and the corresponding level sets specified by γ and λ as in Corollary 5.5.11. One can readily see that the system in (5.5.21) is safe and the input constraint is also satisfied.

5.6 Summary

In the first part of this chapter, we proposed a data-driven approach for the estimation of infinitesimal generators of continuous-time stochastic systems with unknown dynamics. We approximated the infinitesimal generator of the solution process via a set of data collected from trajectories of the unknown system. The approximation leverages both time discretization and sampling from the solution process. By assuming proper continuity assumptions on dynamics of the system, we then quantified the closeness between the infinitesimal generator and its approximation while providing an a-priori guaranteed confidence bound.

In the second part of the chapter, we enlarged the class of models to stochastic *hybrid* systems by adding Poisson processes to the dynamics and propose a data-driven approach for the estimation of infinitesimal generator for this class of models. In addition, we developed a data-driven scheme to handle stochastic systems with control inputs, while the results of the previous section only deal with stochastic *autonomous* systems.

In the third part of the chapter, we proposed a data-driven approach for formal verification of both discrete- and continuous-time systems with unknown dynamics. The main target was to verify the safety of unknown systems based on the construction of barrier certificates via a set of data collected from trajectories of systems while providing an a-priori guaranteed confidence on the safety. To do so, we first cast the original safety problem as a robust convex program (RCP) and provided a scenario convex program (SCP) corresponding to the original RCP by collecting finite numbers of data from trajectories of systems. We then established a probabilistic closeness between the optimal value of SCP and that of RCP, and as a result, we formally quantified the safety guarantee of unknown systems based on the number of data and the required level of confidence.

In the last part of the chapter, we proposed a data-driven approach to synthesize safety controllers for continuous-time nonlinear polynomial-type systems with unknown dynamics. The proposed framework was based on notions of control barrier certificates, constructed from data while providing a guaranteed *confidence of* 1 on the safety of unknown systems. Under a certain rank condition, we synthesized polynomial state-feedback controllers to ensure the safety of the unknown system only via a *single trajectory* collected from it.

6 Conclusions and Future Contributions

6.1 Conclusions

This dissertation was concerned with (compositional) techniques for formal analysis and synthesis of (unknown) stochastic hybrid systems. In the first part of the dissertation, we proposed systematic approaches for the construction of finite abstractions for continuous-time stochastic control and hybrid systems. In order to deal with *curse of dimensionality* problem as the main challenge in the construction of finite abstractions, we also provided *compositional abstractions-based techniques* based on small-gain and dissipativity approaches for formal analysis of continuous-time SHS. We showed that the proposed compositionality approach based on dissipativity reasoning can be potentially less conservative than the small-gain one for some classes of systems given that it can enjoy the structure of the interconnection topology and may not require any constraint on the number or gains of subsystems. Consequently, the dissipativity compositionality condition can be scale-free and independent of the number of subsystems compared to the small-gain approach.

In the second part of the dissertation, we developed *compositional techniques* in the context of control barrier certificates (CBC) for formal verification and controller synthesis of large-scale stochastic control and hybrid systems. In particular, control barrier certificates have received significant attentions in the past few years as a *discretization-free* approach for formal analysis of SHS. On the downside, finding CBC for complex dynamical systems is computationally very expensive, especially if one is dealing with high-dimensional systems. Then developing compositional techniques is essential to alleviate this type of computational complexity. In our proposed setting, we considered the large-scale SHS as an interconnected system composed of several smaller subsystems, and provided compositional frameworks for the construction of CBC for the complex interconnected SHS using control barrier certificates of smaller subsystems.

In the last part of the dissertation, we developed *data-driven* techniques for the verification and synthesis of SHS while providing *formal guarantees*. In particular, closed-form mathematical models for some complex SHS are either not available or equally complex to be of any practical use. Accordingly, one cannot employ model-based techniques to analyze and design this type of complex unknown systems. Then data-driven techniques have received significant attentions in the past decade for the formal analysis of *unknown* SHS enforcing complex control missions. However, guaranteeing safety and reliability of physical systems based on data is very challenging, which is of vital importance in many safety-critical applications. The last part of the thesis was dedicated to develop data-driven verification and synthesis techniques for formal analysis of SHS.

6.2 Recommendations for Future Research

In this section, we discuss some interesting topics that could be considered as potential future research lines.

- **Compositional controller synthesis via abstraction-based techniques.** In the third chapter of the dissertation, we widely studied different compositional approaches for the construction of (in)finite abstractions for networks of stochastic control/hybrid systems. One potential direction as a future work is to investigate the compositional controller synthesis for continuous-time stochastic systems. In particular, given a specification over the interconnected system, one can study the formal relation between the probability of satisfactions provided by local controllers for individual subsystems and that of their monolithic ones in the interconnected case.

- **Decomposition of larger classes of LTL properties.** In the third chapter of the thesis, we mainly considered our specifications as the safety. In particular, we considered the overall safety specification as a hyper-rectangle (a.k.a., hyper interval) and decomposed and projected it to different dimensions corresponding to subsystems. We first designed local controllers for abstractions $\widehat{\Sigma}_i$, and then refined them back to subsystems Σ_i using interface functions. Consequently, the controller for the interconnected system Σ is simply constructed by augmenting controllers of subsystems Σ_i. Another direction as the future research line is to consider more complex LTL properties including reachability, reach-avoid, etc., and study how to decompose those high-level specifications in order to provide a compositional synthesis framework for them.

- **Establishing similarity relations for the general setting of continuous-time SHS.** In the third chapter of the dissertation, we focused on a particular class of stochastic *affine* and *nonlinear* systems and constructed finite abstractions together with their corresponding stochastic simulation functions for these classes of models. One interesting open problem is to provide a similarity relation for the *general setting* of continuous-time SHS.

- **Closeness guarantees between sampling times.** In the third chapter of the dissertation, we provided probabilistic closeness guarantees between output trajectories of original continuous-time stochastic systems and that of their discrete-time (finite or infinite) abstractions only at sampling times. Another research direction is to extend our proposed results to provide a closeness between sampling times, as well.

- **Reduce conservatism in controller synthesis via CBC.** In the forth chapter of the dissertation, the way that we synthesized controllers via CBC is somewhat conservative since we added an extra term in (4.2.18) to resolve the bilinearity problem between unknown coefficients of CBC and its controller, which makes

our proposed SOS conservative. One research line is to investigate another approaches to resolve the encountered bilinearity and search for the controller in a less conservative way.

- **Considering delay in controller synthesis of Markovian switching.** In the forth chapter of the dissertation, in order to provide the CBC results for ct-SHS with Markovian switching, we assumed that the controller has access to switching modes. In particular, it is supposed that there is a mode detection device which is capable of identifying the system mode in real time so that the controller can switch to the matched mode. One interesting research direction is to consider also some delay while deploying the synthesized controllers which makes our proposed approach more practical.

- **Reduce sample complexity of the data-driven approach via parallelization.** In the last chapter of the dissertation, in order to provide safety guarantees over unknown original system, the required number of data for solving scenario convex program is exponential with respect to the dimension of the system. One potential research direction is to reduce the sample complexity via developing a parallelization methodology for linear programming of each scenario optimization problem. Such an approach would effectively reduce the computational burden and enhance the efficiency of the analysis.

- **Data-driven controller synthesis for general nonlinear systems.** In the last chapter of the dissertation, we proposed a data-driven approach to synthesize safety controllers for continuous-time nonlinear *polynomial-type* systems with unknown models. Another research direction is to leverage a similar reasoning as we proposed here and develop the data-driven controller synthesis approach for the *general setting* of nonlinear systems.

- **Data-driven analysis for more complex LTL properties.** In the final chapter of the dissertation, we introduced a data-driven approach for analyzing safety specifications in black-box systems. Building upon this work, an intriguing avenue for further research involves applying a similar reasoning framework to develop a data-driven analysis for more complex Linear LTL properties, such as reachability and reach-avoid. This expansion would enable a comprehensive exploration of complex system behaviors, leveraging the power of data-driven techniques to enhance the analysis of such properties.

- **Data-driven construction of finite MDPs.** In the final chapter of the dissertation, we presented novel data-driven approaches for constructing (control) barrier certificates. Extending this line of research, an intersecting direction is to apply similar reasoning techniques to construct finite MDPs using data, particularly for stochastic hybrid systems with unknown characteristics. This research direction holds significant potential for advancing the analysis and control of such systems by leveraging the power of data-driven techniques.

Bibliography

[ABB+15] A. Angius, G. Balbo, M. Beccuti, E. Bibbona, A. Horvath, and R. Sirovich. Approximate analysis of biological systems by hybrid switching jump diffusion. *Theoretical Computer Science*, 587:49–72, 2015.

[ACE+19] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada. Control barrier functions: Theory and applications. In *Proceedings of the 18th European Control Conference (ECC)*, pages 3420–3431, 2019.

[ACJT18] M. Ahmadi, M. Cubuktepe, N. Jansen, and U. Topcu. Verification of uncertain POMDPs using barrier certificates. In *Proceedings of the Annual Allerton Conference on Communication, Control, and Computing*, pages 115–122, 2018.

[Ade13] Philip. A. Adewuyi. DC motor speed control: A case between PID controller and fuzzy logic controller. *international journal of multidisciplinary sciences and engineering*, 4(4):36–40, 2013.

[ALZ20] 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.

[ALZ22] M. Anand, A. Lavaei, and M. Zamani. From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems. *IEEE Transactions on Automatic Control*, 67(10):5638–5645, 2022.

[ALZ23] M. Anand, A. Lavaei, and M. Zamani. Compositional synthesis of control barrier certificates for networks of stochastic systems against ω-regular specifications. *Nonlinear Analysis: Hybrid Systems*, 2023.

[AMP16] M. Arcak, C. Meissen, and A. Packard. *Networks of dissipative systems*. Springer, 2016.

[APLS08] A. Abate, M. Prandini, J. Lygeros, and S. Sastry. Probabilistic reachability and safety for controlled discrete-time stochastic hybrid systems. *Automatica*, 44(11):2724–2734, 2008.

[ASBA19] M. Ahmadi, A. Singletary, J. W. Burdick, and A. D. Ames. Safe policy synthesis in multi-agent POMDPs via discrete-time barrier functions. In *Proceedings of the 58th Conference on Decision and Control (CDC)*, pages 4797–4803, 2019.

[ASSB00] A. Aziz, K. Sanwal, V. Singhal, and R. Brayton. Model-checking continuous-time Markov chains. *ACM Transactions on Computational Logic (TOCL)*, 1(1):162–170, 2000.

[AT10] A. Anta and P. Tabuada. To sample or not to sample: Self-triggered control for nonlinear systems. *IEEE Transactions on automatic control*, 55(9):2030–2042, 2010.

[Axe94] O. Axelsson. Iterative solution methods. Cambridge univ. *Press, Cambridge*, 1994.

[BDPFT21] V. Breschi, C. De Persis, S. Formentin, and P. Tesi. Direct data-driven model-reference control with lyapunov stability guarantees. *arXiv preprint:2103.12663*, 2021.

[BDPT20a] A. Bisoffi, C. De Persis, and P. Tesi. Controller design for robust invariance from noisy data. *arXiv preprint:2007.13181*, 2020.

[BDPT20b] A. Bisoffi, C. De Persis, and P. Tesi. Data-based guarantees of set invariance properties. *IFAC-PapersOnLine*, 53(2):3953–3958, 2020.

[Bel65] H. E. Bell. Gershgorin's theorem and the zeros of polynomials. *The American Mathematical Monthly*, 72(3):292–295, 1965.

[BK08] C. Baier and J.-P. Katoen. *Principles of model checking*. MIT press, 2008.

[BKSA20] J. Berberich, A. Koch, C. W. Scherer, and F. Allgöwer. Robust data-driven state-feedback design. In *American Control Conference (ACC)*, pages 1532–1538. IEEE, 2020.

[BLE+06] H. AP. Blom, J. Lygeros, M. Everdij, S. Loizou, and K. Kyriakopoulos. *Stochastic hybrid systems: theory and safety critical applications*, volume 337. Springer, 2006.

[BS96] D. P. Bertsekas and S. E. Shreve. *Stochastic optimal control: The discrete-time case*. Athena Scientific, 1996.

[BSA20] J. Berberich, C. W. Scherer, and F. Allgöwer. Combining prior knowledge and data for robust controller design. *arXiv preprint:2009.05253*, 2020.

[CA19] N. Cauchi and A. Abate. StocHy: Automated verification and synthesis of stochastic processes. In *Proceedings of the International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 247–264. Springer, 2019.

[Cal10] G. C. Calafiore. Random convex programs. *SIAM Journal on Optimization*, 20(6):3427–3464, 2010.

[CC06] G. C. Calafiore and M. C. Campi. The scenario approach to robust control design. *IEEE Transactions on Automatic Control*, 51(5):742–753, 2006.

[CGP09] M.C. Campi, S. Garatti, and M. Prandini. The scenario approach for systems and control design. *Annual Reviews in Control*, 33(2):149–157, 2009.

[CGSS13] A. Cimatti, A. Griggio, B. J. Schaafsma, and R. Sebastiani. The MathSAT5 SMT Solver. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 93–107, 2013.

[CL06] C. G. Cassandras and J. Lygeros. *Stochastic hybrid systems*. CRC Press, 2006.

[Cla19] A. Clark. Control barrier functions for complete and incomplete information stochastic systems. In *Proceedings of the American Control Conference (ACC)*, pages 2928–2935, 2019.

[CLD19] J. Coulson, J. Lygeros, and F. Dörfler. Regularized and distributionally robust data-enabled predictive control. In *Proceedings of the 58th Conference on Decision and Control (CDC)*, pages 2696–2701, 2019.

[COMB19] R. Cheng, G. Orosz, R. M. Murray, and J. W. Burdick. End-to-end safe reinforcement learning through barrier functions for safety-critical continuous control tasks. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 33, pages 3387–3395, 2019.

[DIW11] S. Dashkovskiy, H. Ito, and F. Wirth. On a small gain theorem for ISS networks in dissipative Lyapunov form. *European Journal of Control*, 17(4):357–365, 2011.

[DK04] K. C. Das and P. Kumar. Some new bounds on the spectral radius of graphs. *Discrete Mathematics*, 281(1-3):149–161, 2004.

[DMB08] L. De Moura and N. Bjørner. Z3: An efficient SMT solver. In *Proceedings of the International conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340, 2008.

[DMKFF18] M. Dabbaghjamanesh, S. Mehraeen, A. Kavousi-Fard, and F. Ferdowsi. A new efficient stochastic energy management technique for interconnected ac microgrids. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*, pages 1–5. IEEE, 2018.

[DPT19] C. De Persis and P. Tesi. Formulas for data-driven control: Stabilization, optimality, and robustness. *IEEE Transactions on Automatic Control*, 65(3):909–924, 2019.

[DPT21] C. De Persis and P. Tesi. Low-complexity learning of linear quadratic regulators from noisy data. *Automatica*, 128:109548, 2021.

[DRW07] S. Dashkovskiy, B. S. Rüffer, and F. R. Wirth. An ISS small gain theorem for general networks. *Mathematics of Control, Signals, and Systems (MCSS)*, 19(2):93–122, 2007.

[DRW10] S. N Dashkovskiy, B. S. Rüffer, and F. R. Wirth. Small gain theorems for large scale systems and construction of ISS Lyapunov functions. *SIAM Journal on Control and Optimization*, 48(6):4089–4118, 2010.

[DST+21] Z. Du, Y. Sattar, D. A. Tarzanagh, L. Balzano, S. Oymak, and N. Ozay. Certainty equivalent quadratic control for Markov jump systems. *arXiv:2105.12358*, 2021.

[Dye83] M. E. Dyer. The complexity of vertex enumeration methods. *Mathematics of Operations Research*, 8(3):381–402, 1983.

[Dyn65] E. B. Dynkin. *Markov processes*. Springer, 1965.

[GAC12] S. Gao, J. Avigad, and E. M. Clarke. δ-complete decision procedures for satisfiability over the reals. In *International Joint Conference on Automated Reasoning*, pages 286–300, 2012.

[GAM93] M. K. Ghosh, A. Arapostathis, and S. I. Marcus. Optimal control of switching diffusions with application to flexible manufacturing systems. *SIAM Journal on Control and Optimization*, 31(5):1183–1204, 1993.

[GBSV+19] Shromona Ghosh, Somil Bansal, Alberto Sangiovanni-Vincentelli, Sanjit A Seshia, and Claire Tomlin. A new simulation metric to determine safe environments and controllers for systems with unknown dynamics. In *Proceedings of the 22nd ACM International Conference on Hybrid Systems: Computation and Control*, pages 185–196, 2019.

[GDPT20] M. Guo, C. De Persis, and P. Tesi. Learning control for polynomial systems using sum of squares relaxations. In *59th IEEE Conference on Decision and Control (CDC)*, pages 2436–2441. IEEE, 2020.

[GDPT21] M. Guo, C. De Persis, and P. Tesi. Data-driven stabilization of nonlinear polynomial systems with noisy data. *IEEE Transactions on Automatic Control*, 2021.

[GGM16] 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.

[GL04] W. Glover and J. Lygeros. A stochastic hybrid model for air traffic control simulation. In *International Workshop on Hybrid Systems: Computation and Control*, pages 372–386. Springer, 2004.

[GR01] C. Godsil and G. Royle. *Algebraic graph theory*. Graduate Texts in Mathematics. Springe, New York, 2001.

[Gro19] T. H. Gronwall. Note on the derivatives with respect to a parameter of the solutions of a system of differential equations. *Annals of Mathematics*, pages 292–296, 1919.

[HCL+17] 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.

[Hes04] J. P. Hespanha. Stochastic hybrid systems: Application to communication networks. In *International Workshop on Hybrid Systems: Computation and Control*, pages 387–401. Springer, 2004.

[HHB99] A. Hassibi, J. How, and S. Boyd. A path-following method for solving bmi problems in control. In *Proceedings of the American control conference*, volume 2, pages 1385–1389, 1999.

[HSA17] S. Haesaert, S. Soudjani, and A. Abate. Verification of general Markov decision processes by approximate similarity relations and policy refinement. *SIAM Journal on Control and Optimization*, 55(4):2333–2367, 2017.

[HSK+20] K. Hashimoto, A. Saoud, M. Kishida, T. Ushio, and D. Dimarogonas. Learning-based safe symbolic abstractions for nonlinear control systems. *arXiv:2004.01879*, 2020.

[HVdHA15] S. Haesaert, P. MJ. Van den Hof, and A. Abate. Data-driven property verification of grey-box systems by Bayesian experiment design. In *Proceedings of the American Control Conference (ACC)*, pages 1800–1805, 2015.

[HW13] Z. Hou and Z. Wang. From model-based control to data-driven control: Survey, classification and perspective. *Information Sciences*, 235:3–35, 2013.

[IDW09] H. Ito, S. Dashkovskiy, and F. Wirth. On a small gain theorem for networks of ISS systems. In *Proceedings of the 48h IEEE Conference on Decision and Control (CDC) held jointly with 28th Chinese Control Conference*, pages 4210–4215, 2009.

[IHM09] S. Intep, D.J. Higham, and X. Mao. Switching and diffusion models for gene regulation networks. *Multiscale Modeling & Simulation*, 8(1):30–45, 2009.

[JLZ23] N. Jahanshahi, A. Lavaei, and M. Zamani. Compositional construction of safety controllers for networks of continuous-space POMDPs. *IEEE Transactions on Control of Network Systems*, 10(1):87–99, 2023.

[JP09] A. A. Julius and G. J. Pappas. Approximations of stochastic hybrid systems. *IEEE Transactions on Automatic Control*, 54(6):1193–1203, 2009.

[JPZ20] P. Jagtap, G. J. Pappas, and M. Zamani. Control barrier functions for unknown nonlinear systems using Gaussian processes. In *Proceedings of the 59th IEEE Conference on Decision and Control*, pages 3699–3704, 2020.

[JSZ20] 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.

[KBJT19] J. Kenanian, A. Balkan, R. M. Jungers, and P. Tabuada. Data-driven stability analysis of black-box switched linear systems. *Automatica*, 109, 2019.

[KS14] I. Karatzas and S. Shreve. *Brownian motion and stochastic calculus*, volume 113. springer, 2014.

[KS20] M. Kazemi and S. Soudjani. Formal policy synthesis for continuous-state systems via reinforcement learning. In *International Conference on Integrated Formal Methods*, pages 3–21. Springer, 2020.

[KSL13] M. Kamgarpour, S. Summers, and J. Lygeros. Control design for specifications on stochastic hybrid systems. In *Proceedings of the 16th International Conference on Hybrid Systems: Computation and Control*, pages 303–312, 2013.

[KT12] T. Kanamori and A. Takeda. Worst-case violation of sampled convex programs for optimization with uncertainty. *Journal of Optimization Theory and Applications*, 152(1):171–197, 2012.

[Kus67] H. J. Kushner. *Stochastic Stability and Control*. Mathematics in Science and Engineering. Elsevier Science, 1967.

[LA23] A. Lavaei and D. Angeli. Data-driven stability certificate of interconnected homogeneous networks via ISS properties. *IEEE Control Systems Letters*, 7:2395–2400, 2023.

[LAB+17] L. Laurenti, A. Abate, L. Bortolussi, L. Cardelli, M. Ceska, and M. Kwiatkowska. Reachability computation for switching diffusions: Finite abstractions with certifiable and tuneable precision. In *Proceedings of the 20th ACM International Conference on Hybrid Systems: Computation and Control*, pages 55–64, 2017.

[Lav19] A. Lavaei. *Automated Verification and Control of Large-Scale Stochastic Cyber-Physical Systems: Compositional Techniques*. PhD thesis, Department of Electrical Engineering, Technische Universität München, Germany, 2019.

[LDLCF22] A. Lavaei, L. Di Lillo, A. Censi, and E. Frazzoli. Formal estimation of collision risks for autonomous vehicles: A compositional data-driven approach. *IEEE Transactions on Control of Network Systems*, 10(1):407–418, 2022.

[LF22] A. Lavaei and E. Frazzoli. Data-driven synthesis of symbolic abstractions with guaranteed confidence. *IEEE Control Systems Letters*, 7:253–258, 2022.

[LHR+20] L. Lindemann, H. Hu, A. Robey, H. Zhang, D. V. Dimarogonas, S. Tu, and N. Matni. Learning hybrid control barrier functions from data. *arXiv:2011.04112*, 2020.

[Lib03] D. Liberzon. *Switching in systems and control*. Springer Science & Business Media, 2003.

[LKSZ20] A. Lavaei, M. Khaled, S. Soudjani, and M. Zamani. AMYTISS: Parallelized automated controller synthesis for large-scale stochastic systems. In *32nd International Conference on Computer Aided Verification (CAV)*, pages 461–474, 2020.

[LMS08] E. K. Larsson, M. Mossberg, and T. Söderström. Estimation of continuous-time stochastic system parameters. In *Identification of continuous-time models from sampled data*, pages 31–66. Springer, 2008.

[LNJZ21] A. Lavaei, A. Nejati, P. Jagtap, and M. Zamani. Formal safety verification of unknown continuous-time systems: A data-driven approach. In *Proceedings of the 24th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, 2021.

[LNSZ21] A. Lavaei, A. Nejati, S. Soudjani, and M. Zamani. Estimating infinitesimal generators of stochastic systems with formal error bounds: A data-driven approach. In *Proceedings of the 24th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, 2021.

[LPK+22] A. Lavaei, M. Perez, M. Kazemi, F. Somenzi, S. Soudjani, A. Trivedi, and M. Zamani. Compositional reinforcement learning for discrete-time stochastic control systems. *arXiv:2208.03485*, 2022.

[LSAZ22] A. Lavaei, S. Soudjani, A. Abate, and M. Zamani. Automated verification and synthesis of stochastic hybrid systems: A survey. *Automatica*, 146, 2022.

[LSF23] A. Lavaei, S. Soudjani, and E. Frazzoli. A compositional dissipativity approach for data-driven safety verification of large-scale dynamical systems. *IEEE Transactions on Automatic Control*, 2023.

[LSFZ22] A. Lavaei, S. Soudjani, E. Frazzoli, and M. Zamani. Constructing MDP abstractions using data with formal guarantees. *IEEE Control Systems Letters*, 7:460–465, 2022.

[LSMZ17] A. Lavaei, S. Soudjani, R. Majumdar, and M. Zamani. Compositional abstractions of interconnected discrete-time stochastic control systems. In *Proceedings of the 56th IEEE Conference on Decision and Control*, pages 3551–3556, 2017.

[LSS+20] A. Lavaei, F. Somenzi, S. Soudjani, A. Trivedi, and M. Zamani. Formal controller synthesis for continuous-space MDPs via model-free reinforcement learning. In *Proceedings of the 11th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, pages 98–107, 2020.

[LSZ18] A. Lavaei, S. Soudjani, and M. Zamani. 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*, pages 21–30, 2018.

[LSZ19a] A. Lavaei, S. Soudjani, and M. Zamani. Compositional construction of infinite abstractions for networks of stochastic control systems. *Automatica*, 107:125–137, 2019.

[LSZ19b] A. Lavaei, S. Soudjani, and M. Zamani. Compositional synthesis of not necessarily stabilizable stochastic systems via finite abstractions. In *Proceedings of the 18th European Control Conference*, pages 2802–2807, 2019.

[LSZ20a] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis for networks of stochastic switched systems. *Automatica*, 114, 2020.

[LSZ20b] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis of general MDPs via approximate probabilistic relations. *Nonlinear Analysis: Hybrid Systems*, 39, 2020.

[LSZ20c] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction of large-scale stochastic systems: A relaxed dissipativity approach. *Nonlinear Analysis: Hybrid Systems*, 36, 2020.

[LSZ20d] 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.

[LZ19] A. Lavaei and M. Zamani. Compositional verification of large-scale stochastic systems via relaxed small-gain conditions. In *Proceedings of the 58th IEEE Conference on Decision and Control*, pages 2574–2579, 2019.

[LZ22] A. Lavaei and M. Zamani. From dissipativity theory to compositional synthesis of large-scale stochastic switched systems. *IEEE Transactions on Automatic Control*, 67(9):4422–4437, 2022.

[MESKL18] P. Mohajerin Esfahani, T. Sutter, D. Kuhn, and J. Lygeros. From infinite to finite programs: Explicit error bounds with applications to approximate dynamic programming. *SIAM journal on optimization*, 28(3):1968–1998, 2018.

[MESL14] P. Mohajerin Esfahani, T. Sutter, and J. Lygeros. Performance bounds for the scenario approach and an extension to a class of non-convex programs. *IEEE Transactions on Automatic Control*, 60(1):46–58, 2014.

[Mor96] A. S. Morse. Supervisory control of families of linear set-point controllers-part i. exact matching. *IEEE transactions on Automatic Control*, 41(10):1413–1431, 1996.

[MPC+17] C. Manes, P. Palumbo, V. Cusimano, M. Vanoni, and L. Alberghina. Modeling biological timing and synchronization mechanisms by means of interconnections of stochastic switches. *IEEE Control Systems Letters*, 2(1):19–24, 2017.

[MSSM17] K. Mallik, S. Soudjani, A. Schmuck, and R. Majumdar. Compositional construction of finite state abstractions for stochastic control systems. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 550–557, Dec 2017.

[NLJ+23] A. Nejati, A. Lavaei, P. Jagtap, S. Soudjani, and M. Zamani. Formal verification of unknown discrete- and continuous-time systems: A data-driven approach. *IEEE Transactions on Automatic Control (TAC), Special Issue on Learning and Control*, 68(5):3011–3024, 2023.

[NLSZ21] A. Nejati, A. Lavaei, S. Soudjani, and M. Zamani. Data-driven estimation of infinitesimal generators of stochastic systems. *Proceedings of the 7th IFAC Conference on Analysis and Design of Hybrid Systems (ADHS)*, 54(5):277–282, 2021.

[NLSZ22] A. Nejati, A. Lavaei, S. Soudjani, and M. Zamani. Estimation of infinitesimal generators for stochastic hybrid systems via sampling: A formal approach. *IEEE Control Systems Letters*, 7:223–228, 2022.

[NM20] B. Nortmann and T. Mylvaganam. Data-driven control of linear time-varying systems. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3939–3944. IEEE, 2020.

[NPP16] C. Nowzari, V. M Preciado, and G. J. Pappas. Analysis and control of epidemics: A survey of spreading processes on complex networks. *IEEE Control Systems Magazine*, 36(1):26–46, 2016.

[NSZ19] A. Nejati, S. Soudjani, and M. Zamani. Abstraction-based synthesis of continuous-time stochastic control systems. In *Proceedings of the 18th European Control Conference*, pages 3212–3217, 2019.

[NSZ20a] 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.

[NSZ20b] 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.

[NSZ21] 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.

[NSZ22] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier functions for continuous-time stochastic hybrid systems. *Automatica*, 145, 2022.

[NZ20] 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.

[NZ22] A. Nejati and M. Zamani. From dissipativity theory to compositional construction of control barrier certificates. *Leibniz Transactions on Embedded Systems (LITES), Special Issue on Distributed Hybrid Systems*, 8(2), 2022.

[NZ23] A. Nejati and M. Zamani. Data-driven synthesis of safety controllers via multiple control barrier certificates. *IEEE Control Systems Letters*, 2023.

[NZCZ22] A. Nejati, B. Zhong, M. Caccamo, and M. Zamani. Data-driven controller synthesis of unknown nonlinear polynomial systems via control barrier certificates. In *Learning for Dynamics and Control Conference (L4DC)*, pages 763–776, 2022.

[Oks13] B. Oksendal. *Stochastic differential equations: an introduction with applications*. Springer Science & Business Media, 2013.

[OP15] M. Ogura and V. M. Preciado. Disease spread over randomly switched large-scale networks. In *2015 American Control Conference (ACC)*, pages 1782–1787. IEEE, 2015.

[ØS05] B. K. Øksendal and A. Sulem. *Applied stochastic control of jump diffusions*, volume 498. Springer, 2005.

[PA15] A. Padoan and A. Astolfi. Towards deterministic subspace identification for autonomous nonlinear systems. In *Proceedings of the 54th IEEE Conference on Decision and Control (CDC)*, pages 127–132, 2015.

[Par03] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical programming*, 96(2):293–320, 2003.

[PAV+13] 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.

[PJ04] S. Prajna and A. Jadbabaie. Safety verification of hybrid systems using barrier certificates. In *Proceedings of the 7th ACM International Conference on Hybrid Systems: Computation and Control (HSCC)*, pages 477–492, 2004.

[PJP07] 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.

[Pnu77] A. Pnueli. The temporal logic of programs. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, pages 46–57, 1977.

[RDPT21] M. Rotulo, C. De Persis, and P. Tesi. Online learning of data-driven controllers for unknown switched linear systems. *arXiv preprint: 2105.11523*, 2021.

[RHL+20] Alexander Robey, Haimin Hu, Lars Lindemann, Hanwen Zhang, Dimos V Dimarogonas, Stephen Tu, and Nikolai Matni. Learning control barrier functions from expert demonstrations. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3717–3724. IEEE, 2020.

[RN02] S. J. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach*. Pearson Education, 2 edition, 2002.

[Ros08] K. Ross. Stochastic control in continuous time. *Lecture Notes on Continuous Time Stochastic Control*, pages P33–P37, 2008.

[Rüf10] B. S. Rüffer. Monotone inequalities, dynamical systems, and paths in the positive orthant of Euclidean n-space. *Positivity*, 14(2):257–283, 2010.

[RX16] W. Ren and J. Xiong. Stability and stabilization of switched stochastic systems under asynchronous switching. *Systems & Control Letters*, 97:184–192, 2016.

[RZ16] M. Rungger and M. Zamani. SCOTS: A tool for the synthesis of symbolic controllers. In *Proceedings of the 19th ACM International Conference on Hybrid Systems: Computation and Control*, pages 99–104, 2016.

[SA13] S. Soudjani and A. Abate. Adaptive and sequential gridding procedures for the abstraction and verification of stochastic processes. *SIAM Journal on Applied Dynamical Systems*, 12(2):921–956, 2013.

[SA15] P. S. Skardal and A. Arenas. Control of coupled oscillator networks with application to microgrid technologies. *Science advances*, 1(7):e1500339, 2015.

[SAM17] S. Soudjani, A. Abate, and R. Majumdar. Dynamic Bayesian networks for formal verification of structured stochastic processes. *Acta Informatica*, 54(2):217–242, Mar 2017.

[SB18] S. Sadraddini and C. Belta. Formal synthesis of control strategies for positive monotone systems. *IEEE Transactions on Automatic Control*, 64(2):480–495, 2018.

[SDC19] C. Santoyo, M. Dutreix, and S.l Coogan. Verification and control for finite-time safety of stochastic systems via barrier functions. In *Proceedings of the IEEE conference on control technology and applications (CCTA)*, pages 712–717, 2019.

[SGA15] S. Soudjani, C. Gevaerts, and A. Abate. FAUST^2: Formal abstractions of uncountable-state stochastic processes. In *TACAS'15*, volume 9035 of *Lecture Notes in Computer Science*, pages 272–286. Springer, 2015.

[SGS17] F. Samadi Gazijahani and J. Salehi. Stochastic multi-objective framework for optimal dynamic planning of interconnected microgrids. *IET Renewable Power Generation*, 11(14):1749–1759, 2017.

[SGZ18] A. Swikir, A. Girard, and M. Zamani. From dissipativity theory to compositional synthesis of symbolic models. In *Proceedings of the 4th Indian Control Conference (ICC)*, pages 30–35, 2018.

[SLSZ21] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani. Data-driven safety verification of stochastic systems via barrier certificates. *IFAC-PapersOnLine*, 54(5):7–12, 2021.

[SLSZ23] A. Salamati, A. Lavaei, S. Soudjani, and M. Zamani. Data-driven verification and synthesis of stochastic systems via barrier certificates. *Automatica*, 2023.

[Son98] E. D. Sontag. *Mathematical control theory*, volume 6. Springer-Verlag, New York, 2nd edition, 1998.

[Sou14] S. Soudjani. *Formal Abstractions for Automated Verification and Synthesis of Stochastic Systems*. PhD thesis, Technische Universiteit Delft, The Netherlands, 2014.

[ST12] J. Steinhardt and R. Tedrake. Finite-time regional verification of stochastic non-linear systems. *The International Journal of Robotics Research*, 31(7):901–923, 2012.

[Stu99] 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.

[SYM84] J. G. Saw, M. C. Yang, and T. C. Mo. Chebyshev inequality with estimated mean and variance. *The American Statistician*, 38(2):130–132, 1984.

[Tab09] P. Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[TMKA13] I. Tkachev, A. Mereacre, Joost-Pieter Katoen, and A. Abate. Quantitative automata-based controller synthesis for non-autonomous stochastic hybrid systems. In *Proceedings of the 16th ACM International Conference on Hybrid Systems: Computation and Control*, pages 293–302, 2013.

[TSS14] A. R. Teel, A. Subbaraman, and A. Sferlazza. Stability analysis for stochastic hybrid systems: A survey. *Automatica*, 50(10):2435–2456, 2014.

[Var10] R. S. Varga. *Geršgorin and his circles*, volume 36. Springer Science & Business Media, 2010.

[WB17] 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.

[WJ19] Z. Wang and R. M. Jungers. Data-driven computation of invariant sets of discrete time-invariant black-box systems. *arXiv:1907.12075*, 2019.

[WP97] J. C. Willems and J. W Polderman. *Introduction to mathematical systems theory: a behavioral approach*, volume 26. Springer Science & Business Media, 1997.

[WRMDM05] J. C. Willems, P. Rapisarda, I. Markovsky, and B. L. M. De Moor. A note on persistency of excitation. *Systems & Control Letters*, 54(4):325–329, 2005.

[WTE18] Li Wang, Evangelos A Theodorou, and Magnus Egerstedt. Safe learning of quadrotor dynamics using barrier certificates. In *Proceedings of the International Conference on Robotics and Automation (ICRA)*, pages 2460–2465, 2018.

[WTL15] 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.

[WZ96] G.R. Wood and B.P. Zhang. Estimation of the Lipschitz constant of a function. *Journal of Global Optimization*, 8(1):91–103, 1996.

[You12] W. H. Young. On classes of summable functions and their Fourier series. *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 87(594):225–229, 1912.

[ZA14] M. Zamani and A. Abate. Approximately bisimilar symbolic models for randomly switched stochastic systems. *Systems & Control Letters*, 69:38–46, 2014.

[ZA18] M. Zamani and M. Arcak. Compositional abstraction for networks of control systems: A dissipativity approach. *IEEE Transactions on Control of Network Systems*, 5(3):1003–1015, 2018.

[ZAG15] M. Zamani, A. Abate, and A. Girard. Symbolic models for stochastic switched systems: A discretization and a discretization-free approach. *Automatica*, 55:183–196, 2015.

[ZKZ12] P. Zhao, Y. Kang, and D. Zhai. On input-to-state stability of stochastic nonlinear systems with markovian jumping parameters. *International journal of control*, 85(4):343–349, 2012.

[ZMEAL13] M. Zamani, P. Mohajerin Esfahani, A. Abate, and J. Lygeros. Symbolic models for stochastic control systems without stability assumptions. In *Proceedings of the European Control Conference (ECC)*, pages 4257–4262, 2013.

[ZMEM+14] M. Zamani, P. Mohajerin Esfahani, R. Majumdar, A. Abate, and J. Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12):3135–3150, 2014.

[ZNS19] L. Zhang, Z. Ning, and Y. Shi. Analysis and synthesis for a class of stochastic switching systems against delayed mode switching: A framework of integrating mode weights. *Automatica*, 99:99–111, 2019.

[ZRME17] M. Zamani, M. Rungger, and P. Mohajerin Esfahani. Approximations of stochastic hybrid systems: A compositional approach. *IEEE Transactions on Automatic Control*, 62(6):2838–2853, 2017.