Compositional Construction of Infinite Abstractions for Networks of Stochastic Control Systems

Abolfazl Lavaei [a,1], Sadegh Soudjani [b], Majid Zamani [c,d]

[a] *Department of Electrical and Computer Engineering, Technical University of Munich, Germany*

[b] *School of Computing, Newcastle University, United Kingdom*

[c] *Department of Computer Science, University of Colorado Boulder, USA*

[d] *Department of Computer Science, Ludwig Maximilian University of Munich, Germany*

Abstract

This paper is concerned with a compositional approach for constructing infinite abstractions of interconnected discrete-time stochastic control systems. The proposed approach uses the interconnection matrix and joint dissipativity-type properties of subsystems and their abstractions described by new notions of so-called stochastic storage functions. The interconnected abstraction framework is based on new notions of so-called stochastic simulation functions, constructed compositionally using stochastic storage functions of components. Using stochastic simulation functions, one can quantify the distance between original interconnected stochastic systems and interconnected abstractions in the probabilistic setting. Accordingly, one can leverage the proposed results to perform analysis and synthesis over abstract interconnected systems, and then carry the results back over concrete ones. In the first part of the paper, we derive dissipativity-type compositional reasoning for the quantification of the distance in probability between the interconnection of stochastic control subsystems and that of their abstractions. Moreover, we focus on a class of discrete-time nonlinear stochastic control systems with independent noises in the abstract and concrete subsystems, and propose a computational scheme to construct abstractions together with their corresponding stochastic storage functions. In the second part of the paper, we consider specifications expressed as syntactically co-safe linear temporal logic formulae and show how a synthesized policy for the abstract system can be refined to a policy for the original system while providing a guarantee on the probability of satisfaction. We demonstrate the effectiveness of the proposed results by constructing an abstraction (totally 3 dimensions) of the interconnection of three discrete-time nonlinear stochastic control subsystems (together 222 dimensions) in a compositional fashion such that the compositionality condition does not require any constraint on the number or gains of the subsystems. We also employ the constructed abstraction as a substitute to synthesize a controller enforcing a syntactically co-safe linear temporal logic specification.

Key words: Networks of stochastic control systems; Infinite abstractions; Compositionality; Dissipativity theory; Formal synthesis; Co-safe linear temporal logic.

---

1 Introduction

Large-scale interconnected systems have received significant attentions in the last few years due to their presence in real life systems including power grids, traffic networks, and so on. Each complex real-world system can be regarded as an interconnected system composed of several subsystems. Since these large-scale networks of systems are inherently difficult to analyze and control, one can develop compositional schemes and employ the abstractions of the given networks as a replacement in the controller design process. In other words, in order to overcome the computational complexity in large-scale interconnected systems, one can abstract the original (concrete) system by a simpler one with potentially a lower dimension. Those abstractions allow us to design controllers for them, and then refine the controllers back to the ones for the concrete complex systems, while provide us with the quantified errors in this controller synthesis detour.

In the past few years, there have been several results on the construction of (in)finite abstractions for stochastic systems. Existing results for *continuous-time* systems include infinite approximation techniques for jump-

---

Email addresses: `lavaei@tum.de` (Abolfazl Lavaei), `sadegh.soudjani@newcastle.ac.uk` (Sadegh Soudjani), `majid.zamani@colorado.edu` (Majid Zamani).

[1] Corresponding author.

diffusion systems (Julius & Pappas 2009), finite bisimilar abstractions for incrementally stable stochastic switched systems (Zamani et al. 2015) and randomly switched stochastic systems (Zamani & Abate 2014), and finite bisimilar abstractions for incrementally stable stochastic control systems without discrete dynamics (Zamani et al. 2014). Recently, compositional construction of infinite abstractions is discussed by Zamani et al. (2017) using small-gain type conditions, and compositional finite bisimilar abstractions are proposed by Mallik et al. (2017) based on a notion of disturbance bisimilarity relations.

For *discrete-time* stochastic models with continuous-state spaces, finite abstractions are initially employed by Abate et al. (2008) for formal synthesis of this class of systems. The algorithms are improved in terms of scalability by Soudjani & Abate (2013) and Soudjani (2014), and implemented in the tool `FAUST` (Soudjani, Gevaerts & Abate 2015). Extension of the techniques to infinite horizon properties is proposed by Tkachev & Abate (2011), and formal abstraction-based policy synthesis is discussed by Tkachev et al. (2013). A new notion of approximate similarity relation is proposed by Haesaert & Soudjani (2018) and Haesaert et al. (2017) that takes into account both deviation in stochastic evolution and in outputs of the two systems. Compositional construction of infinite abstractions (reduced order models) using small-gain type conditions is proposed by Lavaei et al. (2017). Compositional construction of finite abstractions is discussed by Soudjani, Abate & Majumdar (2015), Lavaei et al. (2018*c*), and Lavaei et al. (2018*b*) using dynamic Bayesian networks, dissipativity-type reasoning, and small-gain conditions, respectively, all for discrete-time stochastic control systems. Recently, compositional synthesis of large-scale stochastic systems using a relaxed dissipativity approach is proposed by Lavaei et al. (2019). Compositional (in)finite abstractions for large-scale interconnected stochastic systems using small-gain type conditions are proposed by Lavaei et al. (2018*a*).

In this paper, we provide a compositional approach for the construction of infinite abstractions of interconnected discrete-time stochastic control systems using the interconnection matrix and joint dissipativity-type properties of subsystems and their abstractions. Our abstraction framework is based on a new notion of stochastic simulation functions under which an abstraction, which is itself a discrete-time stochastic control system with potentially a lower dimension, performs as a substitute in the controller design process. The stochastic simulation function is used to quantify the error in probability in this detour controller synthesis scheme. As a consequence, one can leverage our proposed results to synthesize a policy that satisfies a temporal logic property over the abstract interconnected system, and then refine this policy back for the concrete interconnected one.

Our proposed approach differs from the one presented by Lavaei et al. (2017) in three main directions. First and foremost, rather than using small-gain type reasoning, we employ the dissipativity-type compositional reasoning that may not require any constraint on the number or gains of the subsystems for some interconnection topologies (cf. case study). Second, we provide a scheme for the construction of infinite abstractions for a class of discrete-time nonlinear stochastic control systems whereas the construction scheme proposed by Lavaei et al. (2017) only handles linear systems. As our third main contribution, we consider a fragment of linear temporal logic (LTL) known as syntactically co-safe linear temporal logic (scLTL) (Kupferman & Vardi 2001) whereas the results obtained by Lavaei et al. (2017) only deal with finite-horizon invariant. In particular, given such a specification over the concrete system, we construct an epsilon-perturbed specification over the abstract system whose probability of satisfaction gives a lower bound for the probability of satisfaction in the concrete domain.

It should be also noted that we do not put any restriction on the sources of uncertainties in the concrete and abstract systems. Thus our results are more general than the ones obtained by Zamani et al. (2017), where the noises in the concrete and abstract systems are assumed to be the same, which means the abstraction has access to the noise of the concrete system. Finally, we show the effectiveness of dissipativity-type compositional reasoning for large-scale systems by first constructing an abstraction (totally 3 dimensions) of the interconnection of three discrete-time nonlinear stochastic control subsystems (together 222 dimensions) in a compositional fashion. Then, we employ the abstraction as a substitute to synthesize a controller enforcing a syntactically co-safe linear temporal logic specification over the concrete network.

2 Discrete-Time Stochastic Control Systems

2.1 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 random variables introduced in this article are measurable functions of the form $X : (\Omega, \mathcal{F}_\Omega) \rightarrow (S_X, \mathcal{F}_X)$. 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 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 the Euclidean spaces $\mathbb{R}^n$, its Borel subsets endowed with a subspace topology, as well as hybrid spaces. Any Borel space S is assumed to be endowed with a Borel sigma-algebra, which is denoted by $\mathcal{B}(S)$. We say that a map $f : S \to Y$ is measurable whenever it is Borel measurable.

2.2 Notation

The following notation is used throughout the paper. We denote the sets of nonnegative and positive integers by $\mathbb{N} := \{0, 1, 2, \ldots\}$ and $\mathbb{N}_{\geq 1} := \{1, 2, 3, \ldots\}$, respectively. The symbols $\mathbb{R}$, $\mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote the sets of real, positive and nonnegative real numbers, respectively. Given a vector $x \in \mathbb{R}^n$, $\|x\|$ denotes the Euclidean norm of x. 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. 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 vector of dimension $\sum_i n_i$. We denote by $\mathsf{diag}(a_1, \ldots, a_N)$ a diagonal matrix in $\mathbb{R}^{N\times N}$ with diagonal matrix entries $a_1, \ldots, a_N$ starting from the upper left corner. Given functions $f_i : X_i \to Y_i$, for any $i \in \{1, \ldots, N\}$, their Cartesian product $\prod_{i=1}^N f_i : \prod_{i=1}^N X_i \to \prod_{i=1}^N Y_i$ is defined as $(\prod_{i=1}^N f_i)(x_1, \ldots, x_N) = [f_1(x_1); \ldots; f_N(x_N)]$. For any set A, we denote by $\mathsf{A}^{\mathbb{N}}$ the Cartesian product of a countable number of copies of A, i.e., $\mathsf{A}^{\mathbb{N}} = \prod_{k=0}^\infty \mathsf{A}$. 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 γ is said to be a class $\mathcal{K}_\infty$ if $\gamma(r) \to \infty$ as $r \to \infty$.

2.3 Discrete-Time Stochastic Control Systems

We consider stochastic control systems in discrete time (dt-SCS) defined over a general state space and characterized by the tuple

$$\Sigma = (X, U, W, \varsigma, f, Y_1, Y_2, h_1, h_2), \tag{2.1}$$

where X is a Borel space as the state space of the system. We denote by $(X, \mathcal{B}(X))$ the measurable space with $\mathcal{B}(X)$ being the Borel sigma-algebra on the state space. Sets U and W are Borel spaces as the *external* and *internal* input spaces of the system. Notation ς denotes a sequence of independent and identically distributed (i.i.d.) random variables on a set V_ς as

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

The map $f : X \times U \times W \times V_\varsigma \to X$ is a measurable function characterizing the state evolution of the system. Finally, sets Y_1 and Y_2 are Borel spaces as the *external* and *internal* output spaces of the system, respectively. Maps $h_1 : X \to Y_1$ and $h_2 : X \to Y_2$ are measurable functions that map a state $x \in X$ to its external and internal outputs $y_1 = h_1(x)$ and $y_2 = h_2(x)$, respectively.

For the given initial state $x(0) \in X$ and input sequences $\nu(\cdot) : \mathbb{N} \to U$ and $w(\cdot) : \mathbb{N} \to W$, evolution of the state of dt-SCS Σ can be written as

$$\Sigma : \begin{cases} x(k+1) = f(x(k), \nu(k), w(k), \varsigma(k)), \\ y_1(k) = h_1(x(k)), \\ y_2(k) = h_2(x(k)), \end{cases} \quad k \in \mathbb{N}. \tag{2.2}$$

Remark 2.1 *The above definition can be generalized by allowing the set of valid external inputs to depend on the current state and internal input of the system, i.e., to include* $\{U(x, w) \,|\, x \in X, w \in W\}$ *in the definition of dt-SCS, which is a family of non-empty measurable subsets of* U *with the property that*

$$K := \{(x, \nu, w) : x \in X,\ w \in W,\ \nu \in U(x, w)\},$$

is measurable in $X \times U \times W$*. For the succinct presentation of the results, we assume in this paper that the set of valid external inputs is the whole external input space:* $U(x, w) = U$ *for all* $x \in X$ *and* $w \in W$*, but the obtained results are generally applicable.*

Given the dt-SCS in (2.1), we are interested in *Markov policies* to control the system as the following definition.

Definition 2.2 *A Markov policy for the dt-SCS* Σ *in* (2.1) *is a sequence* $\gamma = (\gamma_0, \gamma_1, \gamma_2, \ldots)$ *of universally measurable stochastic kernels* γ_n *(Bertsekas & Shreve 1996), each defined on the input space* U *given* $X \times W$ *and such that for all* $(x_n, w_n) \in X \times W$, $\gamma_n(U|(x_n, w_n)) = 1$*. The class of all such Markov policies is denoted by* Π_M*.*

We associate respectively to U and W the sets $\mathcal{U}$ and $\mathcal{W}$ to be collections of sequences $\{\nu(k) : \Omega \to U,\ k \in \mathbb{N}\}$ and $\{w(k) : \Omega \to W,\ k \in \mathbb{N}\}$, in which $\nu(k)$ and $w(k)$ are independent of $\varsigma(t)$ for any $k, t \in \mathbb{N}$ and $t \geq k$. For any initial state $a \in X$, $\nu(\cdot) \in \mathcal{U}$, and $w(\cdot) \in \mathcal{W}$, the random sequences $x_{a\nu w} : \Omega \times \mathbb{N} \to X$, $y^1_{a\nu w} : \Omega \times \mathbb{N} \to Y_1$ and $y^2_{a\nu w} : \Omega \times \mathbb{N} \to Y_2$ that satisfy (2.2) are respectively called the *solution process* and external and internal *output trajectory* of Σ under external input ν, internal input w, and initial state a.

Remark 2.3 *In this paper, we are ultimately interested in investigating discrete-time stochastic control systems without internal inputs and outputs. In this case, the tuple* (2.1) *reduces to* $(X, U, \varsigma, f, Y, h)$ *and dt-SCS* (2.2) *can be re-written as*

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

The interconnected control systems, defined later, are also a class of control systems without internal signals, resulting from the interconnection of dt-SCSs having both internal and external inputs and outputs.

In the sequel, we assume that the state and output spaces X and Y of Σ are subsets of $\mathbb{R}^n$ and $\mathbb{R}^q$, respectively. System Σ is called finite if X, U, W are finite sets and infinite otherwise.

3 Stochastic Storage and Simulation Functions

In this section, we first introduce a notion of so-called stochastic storage functions for the discrete-time stochastic control systems with both internal and external inputs which is adapted from the notion of storage functions from dissipativity theory (Arcak et al. 2016). We then define a notion of stochastic simulation functions for systems with only external inputs. We use these definitions to quantify closeness of two dt-SCS.

Definition 3.1 *Consider two dt-SCS* $\Sigma = (X, U, W, \varsigma, f, , Y_1, Y_2, h_1, h_2)$ *and* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{W}, \hat{\varsigma}, \hat{f}, Y_1, \hat{Y}_2, \hat{h}_1, \hat{h}_2)$ *with the same external output spaces. A function* $V : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ *is called a stochastic storage function (SStF) from* $\widehat{\Sigma}$ *to* Σ *if there exist* $\alpha \in \mathcal{K}_\infty$, $\kappa \in \mathcal{K}$, $\rho_{\text{ext}} \in \mathcal{K}_\infty \cup \{0\}$, *some matrices* $G, \hat{G}, H$ *of appropriate dimensions, and some symmetric matrix* $\bar{X}$ *of appropriate dimension with conformal block partitions* $\bar{X}^{ij}$, $i, j \in \{1, 2\}$, *such that for any* $x \in X$ *and* $\hat{x} \in \hat{X}$, *one has*

$$\alpha(\|h_1(x) - \hat{h}_1(\hat{x})\|) \leq V(x, \hat{x}), \tag{3.1}$$

and $\forall x \in X$ $\forall \hat{x} \in \hat{X}$ $\forall \hat{\nu} \in \hat{U}$ $\exists \nu \in U$ *such that* $\forall \hat{w} \in \hat{W}$ $\forall w \in W$ *one obtains*

$$\begin{aligned}&\mathbb{E}\Big[V(x(k+1), \hat{x}(k+1)) \,\big|\, x(k) = x, \hat{x}(k) = \hat{x}, w(k) = w, \\ &, \hat{w}(k) = \hat{w}, \nu(k) = \nu, \hat{\nu}(k) = \hat{\nu}\Big] - V(x, \hat{x}) \leq -\kappa(V(x, \hat{x})) \\ &+ \begin{bmatrix} Gw - \hat{G}\hat{w} \\ h_2(x) - H\hat{h}_2(\hat{x}) \end{bmatrix}^T \overbrace{\begin{bmatrix} \bar{X}^{11} & \bar{X}^{12} \\ \bar{X}^{21} & \bar{X}^{22} \end{bmatrix}}^{\bar{X}:=} \begin{bmatrix} Gw - \hat{G}\hat{w} \\ h_2(x) - H\hat{h}_2(\hat{x}) \end{bmatrix} \\ &+ \rho_{\text{ext}}(\|\hat{\nu}\|) + \psi, \end{aligned} \tag{3.2}$$

for some $\psi \in \mathbb{R}_{\geq 0}$.

We use notation $\widehat{\Sigma} \preceq_{\mathcal{S}} \Sigma$ if there exists a stochastic storage function V from $\widehat{\Sigma}$ to Σ, in which $\widehat{\Sigma}$ is considered as an abstraction of the concrete system Σ.

Remark 3.2 *The second condition above implies implicitly existence of a function* $\nu = \nu_{\hat{\nu}}(x, \hat{x}, \hat{\nu})$ *for satisfaction of* (3.2). *This function is called the* interface function *and can be used to refine a synthesized policy* $\hat{\nu}$ *for* $\widehat{\Sigma}$ *to a policy* ν *for* Σ.

For the dt-SCS without internal signals (including interconnected dt-SCS), the above notion reduces to the following definition.

Definition 3.3 *Consider two dt-SCS* $\Sigma = (X, U, \varsigma, f, Y, , h)$ *and* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{\varsigma}, \hat{f}, Y, \hat{h})$ *with the same output spaces. A function* $V : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ *is called a* stochastic simulation function *(SSF) from* $\widehat{\Sigma}$ *to* Σ *if*

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

$$\forall x \in X, \forall \hat{x} \in \hat{X}, \ \ \alpha(\|h(x) - \hat{h}(\hat{x})\|) \leq V(x, \hat{x}), \tag{3.3}$$

- $\forall x \in X, \hat{x} \in \hat{X}, \hat{\nu} \in \hat{U}$, $\exists \nu \in U$ *such that*

$$\begin{aligned}&\mathbb{E}\Big[V(x(k+1), \hat{x}(k+1)) \big| x(k) = x, \hat{x}(k) = \hat{x}, \nu(k) = \nu, \\ &, \hat{\nu}(k) = \hat{\nu}\Big] - V(x, \hat{x}) \leq -\kappa(V(x, \hat{x})) + \rho_{\text{ext}}(\|\hat{\nu}\|) + \psi, \end{aligned} \tag{3.4}$$

for some $\kappa \in \mathcal{K}$, $\rho_{\text{ext}} \in \mathcal{K}_\infty \cup \{0\}$, *and* $\psi \in \mathbb{R}_{\geq 0}$.

Remark 3.4 *Conditions* (3.1),(3.4) *roughly speaking guarantee that if the concrete system and its abstraction start from two close initial conditions, then they remain close (in terms of expectation) after one step (i.e., roughly, if they start close, they will remain close). This type of conditions is closely related to the ones in the notions of (bi)simulation relations (Tabuada 2009).*

In order to show the usefulness of SSF in comparing output trajectories of two dt-SCS in a probabilistic setting, we need the following technical lemma proved by Kushner (1967, Theorem 3, pp. 86) with some slight modifications for the finite-time horizon, and also by Kushner (1967, Theorem 12, pp. 71) for the infinite-time horizon.

Lemma 3.5 *Let* $\Sigma = (X, \varsigma, f, Y, h)$ *be a dt-SCS with the transition map* $f : X \times V_\varsigma \to X$.
i) Finite-time horizon: Assume there exist $V : X \to \mathbb{R}_{\geq 0}$, *and constants* $0 < \hat{\kappa} < 1$ *and* $\hat{\psi} \in \mathbb{R}_{\geq 0}$ *such that*

$$\mathbb{E}\Big[V(x(k+1)) \big| x(k) = x\Big] \leq \hat{\kappa} V(x) + \hat{\psi}.$$

Then for any random variable a *as the initial state of the dt-SCS, the following inequity holds:*

$$\mathbb{P}\left\{\sup_{0 \leq k \leq T_d} V(x) \geq \epsilon \,|\, a\right\} \leq \delta,$$

$$\delta := \begin{cases} 1 - (1 - \frac{V(a)}{\epsilon})(1 - \frac{\hat{\psi}}{\epsilon})^{T_d} & \textit{if } \epsilon \geq \frac{\hat{\psi}}{\hat{\kappa}}, \\ (\frac{V(a)}{\epsilon})(1 - \hat{\kappa})^{T_d} + (\frac{\hat{\psi}}{\hat{\kappa}\epsilon})(1 - (1 - \hat{\kappa})^{T_d}) & \textit{if } \epsilon < \frac{\hat{\psi}}{\hat{\kappa}}. \end{cases}$$

ii) Infinite-time horizon: Assume there exists a nonnegative $V : X \to \mathbb{R}_{\geq 0}$ *such that*

$$\mathbb{E}\Big[V(x(k+1)) \big| x(k) = x\Big] - V(x) \leq 0.$$

Function V *satisfying the above inequality is also called supermartingale. Then for any random variable* a *as the initial state of the dt-SCS, the following inequity holds:*

$$\mathbb{P}\left\{\sup_{0 \leq k < \infty} V(x) \geq \epsilon \,|\, a\right\} \leq \frac{V(a)}{\epsilon}.$$

Now by employing Lemma 3.5, we provide one of the main results of the paper.

Theorem 3.6 *Let* $\Sigma = (X, U, \varsigma, f, Y, h)$ *and* $\widehat{\Sigma} = (\hat{X}, \hat{U}, \hat{\varsigma}, \hat{f}, Y, \hat{h})$ *be two dt-SCS with the same output spaces. Suppose* V *is an SSF from* $\widehat{\Sigma}$ *to* Σ*, and there exists a constant* $0 < \hat{\kappa} < 1$ *such that function* $\kappa \in \mathcal{K}$ *in (3.4) satisfies* $\kappa(r) \geq \hat{\kappa} r$, $\forall r \in \mathbb{R}_{\geq 0}$*. For any random variables* a *and* $\hat{a}$ *as the initial states of the two dt-SCS and any external input trajectory* $\hat{\nu}(\cdot) \in \hat{\mathcal{U}}$ *preserving Markov property for the closed-loop* $\widehat{\Sigma}$*, there exists an input trajectory* $\nu(\cdot) \in \mathcal{U}$ *of* Σ *through the interface function associated with* V *such that the following inequality holds:*

$$\mathbb{P}\left\{\sup_{0\leq k\leq T_d} \|y_{a\nu}(k) - \hat{y}_{\hat{a}\hat{\nu}}(k)\| \geq \epsilon \,|\, [a;\hat{a}]\right\} \leq \delta, \qquad (3.5)$$

$$\delta := \begin{cases} 1-(1-\frac{V(a,\hat{a})}{\alpha(\epsilon)})(1-\frac{\hat{\psi}}{\alpha(\epsilon)})^{T_d} & \text{if } \alpha(\epsilon)\geq\frac{\hat{\psi}}{\hat{\kappa}}, \\ (\frac{V(a,\hat{a})}{\alpha(\epsilon)})(1-\hat{\kappa})^{T_d}+(\frac{\hat{\psi}}{\hat{\kappa}\alpha(\epsilon)})(1-(1-\hat{\kappa})^{T_d}) & \text{if } \alpha(\epsilon)<\frac{\hat{\psi}}{\hat{\kappa}}, \end{cases}$$

provided that there exists a constant $\hat{\psi} \geq 0$ *satisfying* $\hat{\psi} \geq \rho_{\text{ext}}(\|\hat{\nu}\|_\infty) + \psi$.

The proof of Theorem 3.6 is provided in the Appendix. The results shown in Theorem 3.6 provide closeness of output behaviours of two systems in finite-time horizon. We can extend the result to infinite-time horizon using the second part of Lemma 3.5 given that $\widehat{\psi} = 0$ as stated in the following corollary.

Corollary 3.7 *Let* Σ *and* $\widehat{\Sigma}$ *be two dt-SCS without internal inputs and outputs and with the same output spaces. Suppose* V *is an SSF from* $\widehat{\Sigma}$ *to* Σ *such that* $\rho_{\text{ext}}(\cdot) \equiv 0$ *and* $\psi = 0$*. For any random variables* a *and* $\hat{a}$ *as the initial states of the two dt-SCS and any external input trajectory* $\hat{\nu}(\cdot) \in \hat{\mathcal{U}}$ *preserving Markov property for the closed-loop* $\widehat{\Sigma}$*, there exists* $\nu(\cdot) \in \mathcal{U}$ *of* Σ *through the interface function associated with* V *such that the following inequality holds:*

$$\mathbb{P}\left\{\sup_{0\leq k<\infty} \|y_{a\nu}(k) - \hat{y}_{\hat{a}0}(k)\| \geq \epsilon \,|\, [a;\hat{a}]\right\} \leq \frac{V(a,\hat{a})}{\alpha(\epsilon)}.$$

The proof of Corollary 3.7 is provided in the Appendix.

Remark 3.8 *Note that* $\psi = 0$ *is possible mainly if concrete and abstract systems are both continuous-space but possibly with different dimensions and share the same multiplicative noise. Depending on the dynamic, function* $\rho_{\text{ext}}(\cdot)$ *can be identically zero (cf. Section 5 and case study).*

The relation (3.5) lower bounds the probability such that the Euclidean distance between any output trajectory of the abstract model and the corresponding one of the concrete model remains close and is different from the probabilistic version discussed for finite state, discrete-time labeled Markov chains by Desharnais et al. (2008), which hinges on the absolute difference between transition probabilities over sets covering the state space. However, one can still employ the results in Theorem 3.6 and design controllers for abstractions and refine them to concrete systems while providing the probability of satisfaction over the concrete domain, which is discussed in detail later in Section 6.

4 Compositional Abstractions for Interconnected Systems

In this section, we analyze networks of control systems and show how to construct their abstractions together with the corresponding simulation functions by using stochastic storage functions for the subsystems. We first provide a formal definition of interconnection between discrete-time stochastic control subsystems.

Definition 4.1 *Consider* $N \in \mathbb{N}_{\geq 1}$ *stochastic control subsystems* $\Sigma_i = (X_i, U_i, W_i, \varsigma_i, f_i, Y_{1i}, Y_{2i}, h_{1i}, h_{2i})$, $i \in \{1, \ldots, N\}$*, and a static matrix* M *of an appropriate dimension defining the coupling of these subsystems. The interconnection of* Σ_i *for any* $i \in \{1, \ldots, N\}$*, is the interconnected stochastic control system* $\Sigma = (X, U, \varsigma, f, Y, h)$*, denoted by* $\mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$*, such that* $X := \prod_{i=1}^N X_i$, $U := \prod_{i=1}^N U_i$*, function* $f := \prod_{i=1}^N f_i$, $Y := \prod_{i=1}^N Y_{1i}$*, and* $h = \prod_{i=1}^N h_{1i}$*, with the internal variables constrained by:*

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

4.1 Compositional Abstractions of Interconnected Systems

This subsection contains one of the main contributions of the paper. Assume that we are given N stochastic control subsystems $\Sigma_i = (X_i, U_i, W_i, \varsigma_i, f_i, Y_{1i}, Y_{2i}, h_{1i}, h_{2i})$ together with their corresponding abstractions $\widehat{\Sigma}_i = (\hat{X}_i, \hat{U}_i, \hat{W}_i, \hat{\varsigma}_i, \hat{f}_i, Y_{1i}, \hat{Y}_{2i}, \hat{h}_{1i}, \hat{h}_{2i})$ with SStF V_i from $\widehat{\Sigma}_i$ to Σ_i. We use $\alpha_i, \kappa_i, \rho_{\text{ext}i}, H_i, G_i, \hat{G}_i, \bar{X}_i, \bar{X}_i^{11}, \bar{X}_i^{12}, \bar{X}_i^{21}$, and $\bar{X}_i^{22}$ to denote the corresponding functions, matrices, and their corresponding conformal block partitions appearing in Definition 3.1.

In the next theorem, as one of the main results of the paper, we quantify the error between the interconnection of stochastic control subsystems and that of their abstractions in a compositional way.

Theorem 4.2 *Consider interconnected stochastic control system* $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ *induced by* $N \in \mathbb{N}_{\geq 1}$ *stochastic control subsystems* Σ_i *and the coupling matrix* M*. Suppose stochastic control subsystems* $\widehat{\Sigma}_i$ *are abstractions of* Σ_i *with the corresponding SStF* V_i*. If there exist* $\mu_i > 0$, $i \in \{1, \ldots, N\}$*, and the matrix* $\hat{M}$ *of appropriate dimension such that the matrix (in)equalities*

$$\begin{bmatrix} GM \\ \mathbb{I}_{\tilde{q}} \end{bmatrix}^T \bar{X}_{cmp} \begin{bmatrix} GM \\ \mathbb{I}_{\tilde{q}} \end{bmatrix} \preceq 0, \qquad (4.1)$$

$$GMH = \hat{G}\hat{M}, \qquad (4.2)$$

are satisfied, where $\tilde{q} = \sum_{i=1}^{N} q_{2i}$ *and* q_{2i} *are dimensions of internal outputs of subsystems* Σ_i*, and*

$$G := \mathsf{diag}(G_1, \ldots, G_N),\ \hat{G} := \mathsf{diag}(\hat{G}_1, \ldots, \hat{G}_N),$$
$$H := \mathsf{diag}(H_1, \ldots, H_N), \tag{4.3}$$

$$\bar{X}_{cmp} := \begin{bmatrix} \mu_1 \bar{X}_1^{11} & & & \mu_1 \bar{X}_1^{12} & & \\ & \ddots & & & \ddots & \\ & & \mu_N \bar{X}_N^{11} & & & \mu_N \bar{X}_N^{12} \\ \mu_1 \bar{X}_1^{21} & & & \mu_1 \bar{X}_1^{22} & & \\ & \ddots & & & \ddots & \\ & & \mu_N \bar{X}_N^{21} & & & \mu_N \bar{X}_N^{22} \end{bmatrix}, \tag{4.4}$$

then

$$V(x, \hat{x}) := \sum_{i=1}^{N} \mu_i V_i(x_i, \hat{x}_i), \tag{4.5}$$

is a stochastic simulation function from the interconnected control system $\widehat{\Sigma} = \mathcal{I}(\widehat{\Sigma}_1, \ldots, \widehat{\Sigma}_N)$*, with the coupling matrix* $\hat{M}$*, to* Σ*.*

The proof of Theorem 4.2 is provided in the Appendix. Note that matrix $\bar{X}_{cmp}$ in (4.4) has zero matrices in all its empty entries.

Remark 4.3 *Linear matrix inequality (LMI)* (4.1) *with* $G = \mathbb{I}$ *is similar to the LMI studied by Arcak et al. (2016, Chapter 2) for a compositional stability condition based on the dissipativity theory. As discussed by Arcak et al. (2016), the LMI holds independently of the number of subsystems in many physical applications with specific interconnection structures including communication networks, flexible joint robots, power generators, and so on. We refer the interested readers to Arcak et al. (2016) for more details on the satisfaction of this type of LMI.*

Remark 4.4 *One can relax condition* (4.2) *and employ the linear least square approach instead of solving the equality exactly. In this case, an additional error resulting from the least square approach is added to* ψ *in* (10.2) *which is left for future investigations.*

5 Discrete-Time Stochastic Control Systems with Slope Restrictions on Nonlinearity

In this section, we focus on a specific class of discrete-time nonlinear stochastic control systems Σ_{nl} together with *quadratic* stochastic storage functions V, and provide an approach on the construction of their abstractions. In the next subsection, we first formally define the class of discrete-time nonlinear stochastic control systems.

5.1 A Class of Discrete-Time Nonlinear Stochastic Control Systems

The class of discrete-time nonlinear stochastic control systems, considered here, is given by

$$\Sigma_{\mathsf{nl}} : \begin{cases} x(k+1) = Ax(k) + E\varphi(Fx(k)) + B\nu(k) + Dw(k) + R\varsigma(k), \\ y_1(k) = C_1 x(k), \\ y_2(k) = C_2 x(k), \end{cases} \tag{5.1}$$

where the additive noise $\varsigma(k)$ is a sequence of independent random vectors with multivariate standard normal distributions, and $\varphi : \mathbb{R} \to \mathbb{R}$ satisfies the following constraint

$$0 \leq \frac{\varphi(v) - \varphi(w)}{v - w} \leq b, \quad \forall v, w \in \mathbb{R}, v \neq w, \tag{5.2}$$

for some $b \in \mathbb{R}_{>0} \cup \{\infty\}$.

We use the tuple

$$\Sigma_{\mathsf{nl}} = (A, B, C_1, C_2, D, E, F, R, \varphi),$$

to refer to the class of discrete-time nonlinear stochastic control systems of the form (5.1).

If φ in (5.1) is linear including the zero function (i.e. $\varphi \equiv 0$) or E is a zero matrix, one can remove or push the term $E\varphi(Fx)$ to Ax and, hence, the tuple representing the class of discrete-time nonlinear stochastic control systems reduces to the linear one $\Sigma_{\mathsf{l}} = (A, B, C_1, C_2, D, R)$. Therefore, every time we use the tuple $\Sigma_{\mathsf{nl}} = (A, B, C_1, C_2, D, E, F, R, \varphi)$, it implicitly implies that φ is nonlinear and E is nonzero.

Remark 5.1 *Although the lower bound in* (5.2) *is zero, one can also assume* (5.2) *with some nonlinear functions* φ *with a nonzero lower-bound, e.g.,* $a \in \mathbb{R}$*. In this case, one can make a change of coordinate and define a new function* $\tilde{\varphi}(r) := \varphi(r) - ar$ *which satisfies* (5.2) *with* $\tilde{a} = 0$ *and* $\tilde{b} = b - a$*, and rewrite* (5.1) *as*

$$\Sigma_{nl} : \begin{cases} x(k+1) = \tilde{A}x(k) + E\tilde{\varphi}(Fx(k)) + B\nu(k) + Dw(k) + R\varsigma(k), \\ y_1(k) = C_1 x(k), \\ y_2(k) = C_2 x(k), \end{cases}$$

where $\tilde{A} = A + aEF$*.*

In the next subsection, we provide conditions under which a candidate V is an SStF facilitating the construction of an abstraction $\widehat{\Sigma}_{\mathsf{nl}}$.

5.2 Quadratic Stochastic Storage Functions

Here, we employ the following quadratic function

$$V(x, \hat{x}) = (x - P\hat{x})^T \tilde{M} (x - P\hat{x}), \tag{5.3}$$

where P and $\tilde{M} \succ 0$ are some matrices of appropriate dimensions. In order to show that V in (5.3) is an SStF from $\widehat{\Sigma}_{\mathsf{nl}}$ to Σ_{nl}, we require the following key assumption on Σ_{nl}.

Assumption 5.2 *Let* $\Sigma_{\mathsf{nl}}=(A,B,C_1,C_2,D,E,F,R,\varphi)$. *Assume that for some constants* $0<\hat{\kappa}<1$ *and* $\tilde{k}>0$, *there exist matrices* $\tilde{M}\succ 0$, K, L_1, Z, G, $\bar{X}^{11}$, $\bar{X}^{12}$, $\bar{X}^{21}$, *and* $\bar{X}^{22}$ *of appropriate dimensions such that the matrix equality*

$$D=ZG, \tag{5.4}$$

and inequality (5.5) *hold.*

Now, we provide one of the main results of this section showing under which conditions V in (5.3) is an SStF from $\widehat{\Sigma}_{\mathsf{nl}}$ to Σ_{nl}.

Theorem 5.3 *Let* $\Sigma_{\mathsf{nl}}=(A,B,C_1,C_2,D,E,F,R,\varphi)$ *and* $\widehat{\Sigma}_{\mathsf{nl}}=(\hat{A},\hat{B},\hat{C}_1,\hat{C}_2,\hat{D},\hat{E},\hat{F},\hat{R},\varphi)$ *be two stochastic control subsystems with the same external output space dimension. Suppose Assumption 5.2 holds and there exist matrices* P, Q, H, L_2, *and* $\hat{G}$ *such that*

$$
\begin{aligned}
AP &= P\hat{A}-BQ, && \text{(5.6a)}\\
C_1P &= \hat{C}_1, && \text{(5.6b)}\\
\bar{X}^{12}C_2P &= \bar{X}^{12}H\hat{C}_2, && \text{(5.6c)}\\
\bar{X}^{22}C_2P &= \bar{X}^{22}H\hat{C}_2, && \text{(5.6d)}\\
FP &= \hat{F}, && \text{(5.6e)}\\
E &= P\hat{E}-B(L_1-L_2), && \text{(5.6f)}\\
P\hat{D} &= Z\hat{G}, && \text{(5.6g)}
\end{aligned}
$$

hold. Then, function V *defined in* (5.3) *is an SStF from* $\widehat{\Sigma}_{\mathsf{nl}}$ *to* Σ_{nl}.

The proof of Theorem 5.3 is provided in the Appendix. Note that conditions (5.6) hold as long as the geometric conditions V-18 to V-23 in Zamani & Arcak (2018) hold. The functions $\alpha\in\mathcal{K}_\infty$, $\kappa\in\mathcal{K}$, $\rho_{\mathrm{ext}}\in\mathcal{K}_\infty\cup\{0\}$, and the matrix $\bar{X}$ in Definition 3.1 associated with the SStF in (5.3) are $\alpha(s)=\frac{\lambda_{\min}(\tilde{M})}{\lambda_{\max}(C_1^TC_1)}s^2$, $\kappa(s):=(1-\hat{\kappa})s$, $\rho_{\mathrm{ext}}(s):=\tilde{\kappa}\|\sqrt{\tilde{M}}(B\tilde{R}-P\hat{B})\|^2s^2$, $\forall s\in\mathbb{R}_{\geq 0}$, where $\tilde{R}$ is a matrix of appropriate dimension employed in the interface map (10.4), and $\bar{X}=\begin{bmatrix}\bar{X}^{11} & \bar{X}^{12}\\ \bar{X}^{21} & \bar{X}^{22}\end{bmatrix}$. Moreover, positive constant ψ in (3.2) is $\psi=\mathrm{Tr}\big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\big)$.

It is worth mentioning that for any linear system $\Sigma_{\mathsf{l}}=(A,B,C_1,C_2,D,R)$, stabilizability of the pair (A,B) is sufficient to satisfy Assumption 5.2 in where matrices E, F, and L_1 are identically zero (Antsaklis & Michel 2007, Chapter 4).

One can readily verify from the results of Theorem 5.3 that choosing $\hat{R}$ equal to zero results in smaller constant ψ and, hence, more closeness between subsystems and their abstractions. This is not the case when one assumes the noises of the concrete subsystem and its abstraction are the same as in Zamani et al. (2017) and Zamani (2014).

Since the results in Theorem 5.3 do not impose any condition on matrix $\hat{B}$, it can be chosen arbitrarily. As an example, one can choose $\hat{B}=\mathbb{I}_{\hat{n}}$ which makes the abstract system $\widehat{\Sigma}_{\mathsf{nl}}$ fully actuated and, hence, the synthesis problem over it much easier.

Remark 5.4 *Since Theorem 5.3 does not impose any condition on matrix* $\tilde{R}$, *one can choose* $\tilde{R}$ *such that it minimizes function* ρ_{ext} *for* V *as suggested by Girard & Pappas (2009). The following expression for* $\tilde{R}$

$$\tilde{R}=(B^TMB)^{-1}B^TMP\hat{B},$$

minimizes ρ_{ext}.

6 Probability of Satisfaction for Properties Expressed as scLTL

Consider a dt-SCS $\Sigma=(X,U,\varsigma,f,Y,h)$ and a measurable target set $\mathsf{B}\subset Y$. We say that an output trajectory $\{y(k)\}_{k\geq 0}$ reaches a target set B within time interval $[0,T_d]\subset\mathbb{N}$, if there exists a $k\in[0,T_d]$ such that $y(k)\in\mathsf{B}$. This bounded reaching of B is denoted by $\lozenge^{\leq T_d}\{y\in\mathsf{B}\}$ or briefly $\lozenge^{\leq T_d}\mathsf{B}$. For $T_d\to\infty$, we denote the reachability property as $\lozenge\mathsf{B}$, i.e., eventually B. For a dt-SCS Σ with policy γ, we want to compute the probability that an output trajectory reaches B within the time horizon $T_d\in\mathbb{N}$, i.e., $\mathbb{P}(\lozenge^{\leq T_d}\mathsf{B})$. The *reachability probability* is the probability that the target set B is eventually reached and is denoted by $\mathbb{P}(\lozenge\mathsf{B})$.

More complex properties can be described using temporal logic. Consider a set of atomic propositions AP and the alphabet $\mathsf{\Sigma_a}:=2^{AP}$. Let $\omega=\omega(0),\omega(1),\omega(2),\ldots\in\mathsf{\Sigma_a}^{\mathbb{N}}$ be an infinite word, that is, a string composed of letters from $\mathsf{\Sigma_a}$. Of interest are atomic propositions that are relevant to the dt-SCS via a measurable labeling function L from the output space to the alphabet as $\mathsf{L}:Y\to\mathsf{\Sigma_a}$. Output trajectories $\{y(k)\}_{k\geq 0}\in Y^{\mathbb{N}}$ can be readily mapped to the set of infinite words $\mathsf{\Sigma_a}^{\mathbb{N}}$, as

$$\omega=\mathsf{L}(\{y(k)\}_{k\geq 0}):=\{\omega\in\mathsf{\Sigma_a}^{\mathbb{N}}\,|\,\omega(k)=\mathsf{L}(y(k))\}.$$

Consider LTL properties with syntax (Baier et al. 2008)

$$\phi::=\mathrm{true}\,|\,p\,|\,\neg\phi\,|\,\phi_1\wedge\phi_2\,|\,\bigcirc\phi\,|\,\phi_1\,\mathsf{U}\,\phi_2.$$

Let $\omega_k=\omega(k),\omega(k+1),\omega(k+2),\ldots$ be a subsequence (postfix) of ω, then the satisfaction relation between ω and a property ϕ, expressed in LTL, is denoted by $\omega\vDash\phi$ (or equivalently $\omega_0\vDash\phi$). The semantics of the satisfaction relation are defined recursively over ω_k and the syntax of the LTL formula ϕ. An atomic proposition $p\in AP$ is satisfied by ω_k, i.e., $\omega_k\vDash p$, iff $p\in\omega(k)$. Furthermore, $\omega_k\vDash\neg\phi$ if $\omega_k\nvDash\phi$ and we say that $\omega_k\vDash\phi_1\wedge\phi_2$ if $\omega_k\vDash\phi_1$ and $\omega_k\vDash\phi_2$. The next operator $\omega_k\vDash\bigcirc\phi$ holds if the property holds at the next time instance $\omega_{k+1}\vDash\phi$. We denote by $\bigcirc^j$, $j\in\mathbb{N}$, j times composition of the next operator. With a slight abuse of the notation, one has $\bigcirc^0\phi=\phi$ for any property ϕ. The temporal until operator $\omega_k\vDash\phi_1\,\mathsf{U}\,\phi_2$ holds if $\exists i\in\mathbb{N}:$

$$\begin{bmatrix} (A+BK)^T\tilde{M}(A+BK) & (A+BK)^T\tilde{M}Z & (A+BK)^T\tilde{M}(BL_1+E) & (A+BK)^T\tilde{M}(B\tilde{R}-P\hat{B}) \\ * & Z^T\tilde{M}Z & Z^T\tilde{M}(BL_1+E) & Z^T\tilde{M}(B\tilde{R}-P\hat{B}) \\ * & * & (BL_1+E)^T\tilde{M}(BL_1+E) & (BL_1+E)^T\tilde{M}(B\tilde{R}-P\hat{B}) \\ * & * & * & (B\tilde{R}-P\hat{B})^T\tilde{M}(B\tilde{R}-P\hat{B}) \end{bmatrix}$$

$$\preceq \begin{bmatrix} \hat{\kappa}\tilde{M}+C_2^T\bar{X}^{22}C_2 & C_2^T\bar{X}^{21} & -F^T & 0 \\ \bar{X}^{12}C_2 & \bar{X}^{11} & 0 & 0 \\ -F & 0 & \frac{2}{b} & 0 \\ 0 & 0 & 0 & \tilde{k}(B\tilde{R}-P\hat{B})^T\tilde{M}(B\tilde{R}-P\hat{B}) \end{bmatrix} \tag{5.5}$$

$\omega_{k+i} \vDash \phi_2,$ and $\forall j \in \mathbb{N} : 0 \leq j < i, \omega_{k+j} \vDash \phi_1$. Based on these semantics, operators such as disjunction ($\vee$) can also be defined through the negation and conjunction: $\omega_k \vDash \phi_1 \vee \phi_2 \;\Leftrightarrow\; \omega_k \vDash \neg(\neg\phi_1 \wedge \neg\phi_2)$.

Remark 6.1 *Note that in this section, the satisfaction relation* $\vDash$ *changes by varying the labeling functions* L. *In the following, we employ subscript for* $\models$ *to show its dependency on the labeling functions.*

We are interested in a fragment of LTL properties known as syntactically co-safe linear temporal logic (scLTL) (Kupferman & Vardi 2001). This fragment is defined as the following definition.

Definition 6.2 *An scLTL over a set of atomic propositions AP has syntax*

$$\phi ::= \text{true} \,|\, p \,|\, \neg p \,|\, \phi_1 \wedge \phi_2 \,|\, \phi_1 \vee \phi_2 \,|\, \bigcirc\phi \,|\, \phi_1 \,\mathsf{U}\, \phi_2 \,|\, \Diamond\phi,$$

with $p \in AP$.

Even though scLTL formulas are defined over infinite words (as in LTL formulae), their satisfaction is guaranteed in finite time (Kupferman & Vardi 2001). Any infinite word $\omega \in \Sigma_{\mathsf{a}}^{\mathbb{N}}$ satisfying an scLTL formula ϕ has a finite word $\omega_f \in \Sigma_{\mathsf{a}}^{n}$, $n \in \mathbb{N}$, as its prefix such that all infinite words with prefix ω_f also satisfy the formula ϕ. We denote the language of such finite prefixes associated with an scLTL formula ϕ by $\mathcal{L}_f(\phi)$.

In the remainder, we consider scLTL properties since their verification can be performed via a reachability property over a finite state automaton (Kupferman & Vardi 2001, Belta et al. 2017). For this purpose, we introduce a class of models known as Deterministic Finite-state Automata (DFA).

Definition 6.3 *A DFA is a tuple* $\mathcal{A} = (Q_\ell, q_0, \Sigma_{\mathsf{a}}, F_{\mathsf{a}}, \mathsf{t})$, *where* Q_ℓ *is a finite set of locations,* $q_0 \in Q_\ell$ *is the initial location,* Σ_{a} *is a finite set (a.k.a. alphabet),* $F_{\mathsf{a}} \subseteq Q_\ell$ *is a set of accept locations, and* $\mathsf{t} : Q_\ell \times \Sigma_{\mathsf{a}} \to Q_\ell$ *is a transition function.*

A finite word composed of letters of the alphabet, i.e., $\omega_f = (\omega_f(0), \ldots, \omega_f(n)) \in \Sigma_{\mathsf{a}}^{n+1}$, is accepted by a DFA $\mathcal{A}$ if there exists a finite run $q = (q(0), \ldots, q(n+1)) \in Q_\ell^{n+2}$ such that $q(0) = q_0$, $q(i+1) = \mathsf{t}(q(i), \omega_f(i))$ for all $0 \leq i \leq n$, and $q(n+1) \in F_{\mathsf{a}}$. The accepted language of $\mathcal{A}$, denoted $\mathcal{L}(\mathcal{A})$, is the set of all words accepted by $\mathcal{A}$. For every scLTL property ϕ, cf. Definition 6.2, there exists a DFA $\mathcal{A}_\phi$ such that

$$\mathcal{L}_f(\phi) = \mathcal{L}(\mathcal{A}_\phi).$$

As a result, the satisfaction of the property ϕ now becomes equivalent to the reaching of the accept locations in the DFA. We use the DFA $\mathcal{A}$ to specify properties of dt-SCS $\Sigma = (X, U, \varsigma, f, Y, h)$ as follows. Recall that $\mathsf{L} : Y \to \Sigma_{\mathsf{a}}$ is a given measurable function. To each output $y \in Y$, it assigns the letter $\mathsf{L}(y) \in \Sigma_{\mathsf{a}}$. Given a policy γ, we can define the probability that an output trajectory of Σ satisfies an scLTL property ϕ over time horizon $[0, T_d]$, i.e. $\mathbb{P}(\omega_f \in \mathcal{L}(\mathcal{A}_\phi)$ s.t. $|\omega_f| \leq T_d + 1)$, with $|\omega_f|$ denoting the length of ω_f (Desharnais et al. 2008).

The following example provides an automaton associated with a reach-avoid specification.

Example 6.4 *Consider two measurable sets* $\mathsf{A}, \mathsf{B} \subset Y$ *as the safe and target sets, respectively. We present the DFA for the specification* $(\mathsf{A} \,\mathsf{U}\, \mathsf{B})$, *which requires the output trajectories to reach the target set* B *while remaining in the safe set* A. *Note that we do not assume these two sets being disjoint. Consider the set of atomic propositions* $AP = \{\mathsf{A}, \mathsf{B}\}$ *and the alphabet* $\Sigma_{\mathsf{a}} = \{\emptyset, \{\mathsf{A}\}, \{\mathsf{B}\}, \{\mathsf{A}, \mathsf{B}\}\}$. *Define the labeling function as*

$$\mathsf{L}(y) = \begin{cases} \{\mathsf{A}\} =: a & \text{if } y \in \mathsf{A}\backslash\mathsf{B}, \\ \{\mathsf{B}\} =: b & \text{if } y \in \mathsf{B}, \\ \emptyset =: c & \text{if } y \notin \mathsf{A} \cup \mathsf{B}. \end{cases}$$

As can be seen from the above definition of the labeling function L, *it induces a partition over the output space* Y *as*

$$\mathsf{L}^{-1}(a) = \mathsf{A}\backslash\mathsf{B}, \quad \mathsf{L}^{-1}(b) = \mathsf{B}, \quad \mathsf{L}^{-1}(c) = Y\backslash(\mathsf{A} \cup \mathsf{B}).$$

Note that we have indicated the elements of Σ_{a} *with lower-case letters for the ease of notation. The specification* $(\mathsf{A} \,\mathsf{U}\, \mathsf{B})$ *can be equivalently written as* $(a \,\mathsf{U}\, b)$ *with the associated DFA depicted in Figure 1. This DFA has the set of locations* $Q_\ell = \{q_0, q_1, q_2, q_3\}$, *the initial location*

q_0, and accepting location $F_{\mathsf{a}} = \{q_2\}$. Thus output trajectories of a dt-SCS Σ satisfy the specification $(a \,\mathsf{U}\, b)$ if and only if their associated words are accepted by this DFA.

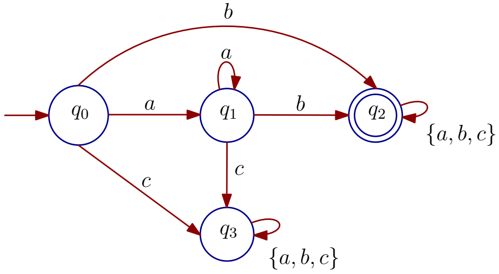

Fig. 1. DFA $\mathcal{A}_\phi$ of the reach-avoid specification $(a \,\mathsf{U}\, b)$.

In the rest of this article, we focus on the computation of probability of $\omega \in \mathcal{L}(\mathcal{A}_\phi)$ over bounded intervals. In other words, we fix a time horizon T_d and compute $\mathbb{P}(\omega(0)\omega(1)\ldots\omega(T_d) \in \mathcal{L}(\mathcal{A}_\phi))$. Suppose Σ and $\widehat{\Sigma}$ are two dt-SCS for which the results of Theorem 3.6 hold. Consider a labeling function L defined on their output space and an scLTL specification ϕ with DFA $\mathcal{A}_\phi$. In the following, we show how to construct a DFA $\mathcal{A}_{\hat{\phi}}$ of another specification $\hat{\phi}$ and a new labeling function L^ϵ such that the satisfaction probability of $\hat{\phi}$ by output trajectories of $\widehat{\Sigma}$ and labeling function L^ϵ gives a lower bounded on the satisfaction probability of ϕ by output trajectories of Σ and labeling function L.

Consider the labeling function $\mathsf{L} : Y \to \Sigma_{\mathsf{a}}$. The new labeling function $\mathsf{L}^\epsilon : Y \to \bar{\Sigma}_{\mathsf{a}}$ is constructed using the ϵ-perturbation of subsets of Y. Define for any Borel measurable set $\mathsf{A} \subset Y$, its ϵ-perturbed version A^ϵ as the largest measurable set satisfying

$$\mathsf{A}^\epsilon \subseteq \{y \in \mathsf{A} \mid \|\bar{y} - y\| \geq \epsilon \text{ for all } \bar{y} \in Y \backslash \mathsf{A}\}.$$

Remark that the set A^ϵ is just the largest measurable set contained in the ϵ-deflated version of A and without loss of generality we assume it is nonempty. Then $\mathsf{L}^\epsilon(y) = \mathsf{L}(y)$ for any $y \in \cup_{a \in \Sigma_{\mathsf{a}}} [\mathsf{L}^{-1}(a)]^\epsilon$, otherwise $\mathsf{L}^\epsilon(y) = \phi_\circ$.

Consider the DFA $\mathcal{A}_\phi = (Q_\ell, q_0, \Sigma_{\mathsf{a}}, F_{\mathsf{a}}, \mathsf{t})$. The new DFA

$$\mathcal{A}_{\hat{\phi}} = (\bar{Q}_\ell, q_0, \bar{\Sigma}_{\mathsf{a}}, F_{\mathsf{a}}, \bar{\mathsf{t}}) \tag{6.1}$$

will be constructed by adding one absorbing location q_{abs} and one letter $\phi_\circ$ as $\bar{Q}_\ell := Q_\ell \cup \{q_{\mathsf{abs}}\}$ and $\bar{\Sigma}_{\mathsf{a}} := \Sigma_{\mathsf{a}} \cup \{\phi_\circ\}$. The initial and accept locations are the same with $\mathcal{A}_\phi$. The transition relation is defined, $\forall q \in \bar{Q}_\ell, \forall a \in \bar{\Sigma}_{\mathsf{a}}$, as

$$\bar{\mathsf{t}}(q, a) := \begin{cases} \mathsf{t}(q, a) & \text{if } q \in Q_\ell, a \in \Sigma_{\mathsf{a}}, \\ q_{\mathsf{abs}} & \text{if } a = \phi_\circ, q \in \bar{Q}_\ell, \\ q_{\mathsf{abs}} & \text{if } q = q_{\mathsf{abs}}, a \in \bar{\Sigma}_{\mathsf{a}}. \end{cases}$$

In other words, we add an absorbing state q_{abs} and all the states will jump to this absorbing state with label $\phi_\circ$. As an example, the modified DFA of the reach-avoid specification in Figure 1 is plotted in Figure 2.

In the next lemma, we employ the new labeling function to relate satisfaction of specifications by output trajectories of two dt-SCS.

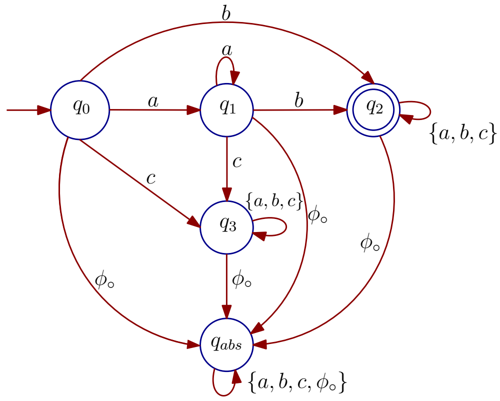

Fig. 2. Modified DFA $\mathcal{A}_{\hat{\phi}}$ of the specification $(a \,\mathsf{U}\, b)$.

Lemma 6.5 *Suppose two observed sequences of output trajectories for two dt-SCS Σ and $\widehat{\Sigma}$ satisfy the inequality*

$$\sup_{0 \leq k \leq T_d} \|y(k) - \hat{y}(k)\| < \epsilon,$$

for some time bound T_d and $\epsilon > 0$. Then $y(\cdot) \vDash_{\mathsf{L}} \phi$ if $\hat{y}(\cdot) \vDash_{\mathsf{L}^\epsilon} \hat{\phi}$ over time interval $[0, T_d]$ with labeling functions L and L^ϵ, and modified specification $\hat{\phi}$ defined in (6.1)*.*

The proof of Lemma 6.5 is provided in the Appendix. Next theorem presents the core result of this section.

Theorem 6.6 *Suppose Σ and $\widehat{\Sigma}$ are two dt-SCS for which inequality* (3.5) *holds with the pair (ϵ, δ) and any time bound T_d. Suppose a specification ϕ and a labeling function L are defined for Σ. The following inequality holds for the labeling function L^ϵ on $\widehat{\Sigma}$ and modified specification $\hat{\phi}$:*

$$\mathbb{P}(\hat{y}(\cdot) \vDash_{\mathsf{L}^\epsilon} \hat{\phi}) - \delta \leq \mathbb{P}(y(\cdot) \vDash_{\mathsf{L}} \phi), \tag{6.2}$$

where the satisfaction is over time interval $[0, T_d]$.

The proof of Theorem 6.6 is provided in the Appendix. In order to get an upper bound for $\mathbb{P}(y(\cdot) \vDash_{\mathsf{L}} \phi)$, we need to define for any Borel measurable set $\mathsf{A} \subset Y$, its $(-\epsilon)$-perturbed version $\mathsf{A}^{-\epsilon}$ as the smallest measurable set satisfying

$$\mathsf{A}^{-\epsilon} \supseteq \{y \in Y \mid \exists \bar{y} \in \mathsf{A} \text{ with } \|\bar{y} - y\| < \epsilon\}.$$

Remark that the set $\mathsf{A}^{-\epsilon}$ is just the smallest measurable set containing the ϵ-inflated version of A.

A new labeling map $\mathsf{L}^{-\epsilon} : Y \to 2^{\Sigma_{\mathsf{a}}}$ is constructed using the $(-\epsilon)-$perturbation of subsets of Y as

$$\mathsf{L}^{-\epsilon}(y) := \left\{a \in \Sigma_{\mathsf{a}} \,|\, y \in [\mathsf{L}^{-1}(a)]^{-\epsilon}\right\}. \tag{6.3}$$

Theorem 6.7 *Suppose Σ and $\widehat{\Sigma}$ are two dt-SCS for which inequality* (3.5) *holds with the pair (ϵ, δ) and any time bound T_d. Suppose a specification ϕ and a labeling function L are defined for Σ. The following inequality holds for the labeling function $\mathsf{L}^{-\epsilon}$ defined in* (6.3) *on $\widehat{\Sigma}$:*

$$\mathbb{P}(y(\cdot) \vDash_{\mathsf{L}} \phi) \leq \mathbb{P}(\hat{y}(\cdot) \vDash_{\mathsf{L}^{-\epsilon}} \phi) + \delta, \tag{6.4}$$

where the satisfaction is over time interval $[0, T_d]$*, and the probability in the right-hand side is computed for having* $\hat{y}(\cdot) \vDash_{\mathsf{L}^{-\epsilon}} \phi$ *for any choice of non-determinism introduced by the labeling map* $\mathsf{L}^{-\epsilon}$*.*

The proof is similar to that of Theorem 6.6, and is omitted here due to lack of space.

In contrast with inequality (6.2), the specification ϕ is the same in both sides of (6.4). The non-determinism originating from $\mathsf{L}^{-\epsilon}$ in the right-hand side of (6.4) can be pushed to the DFA representation of ϕ, by constructing a finite automaton that is non-deterministic.

In the next section, we demonstrate the effectiveness of the proposed results by constructing an abstraction (totally 3 dimensions) of an interconnected system consisting of three nonlinear stochastic control subsystems (together 222 dimensions) in a compositional fashion. We employ the constructed abstraction as a substitute to synthesize a controller enforcing a syntactically co-safe linear temporal logic specification.

7 Case Study

Consider a discrete-time nonlinear stochastic control system Σ_{nl} satisfying

$$\Sigma_{\mathsf{nl}}:\begin{cases} x(k+1) = \bar{G}x(k) + \varphi(x(k)) + \nu(k) + R\varsigma(k),\\ y(k) = Cx(k),\end{cases}$$

for some matrix $\bar{G} = (\mathbb{I}_n - \tau L) \in \mathbb{R}^{n\times n}$ where τL is the Laplacian matrix of an undirected graph with $0 < \tau < 1/\Delta$, where Δ is the maximum degree of the graph (Godsil & Royle 2001). Moreover, $R = \mathsf{diag}(0.007\mathbb{1}_{n_1}\ldots, 0.007\mathbb{1}_{n_N})$, $\varsigma(k) = [\varsigma_1(k); \ldots; \varsigma_N(k)]$, $\varphi(x) = [\mathbb{1}_{n_1}\varphi_1(F_1x_1(k)); \ldots; \mathbb{1}_{n_N}\varphi_N(F_Nx_N(k))]$, where $n = \sum_{i=1}^{N} n_i$, $\varphi_i(x) = sin(x)$, and $F_i = [1; 0; \cdots; 0]^T \in \mathbb{R}^{n_i}$ $\forall i \in \{1, \ldots, N\}$, and C has the block diagonal structure as $C = \mathsf{diag}(C_{11}, \ldots, C_{1N})$, where $C_{1i} \in \mathbb{R}^{q_i \times n_i}, \forall i \in \{1, \ldots, N\}$. We partition x as $x = [x_1; \ldots; x_N]$ and ν as $\nu = [\nu_1; \ldots; \nu_N]$, where $x_i, \nu_i \in \mathbb{R}^{n_i}$. Now, by introducing $\Sigma_{\mathsf{nl}i} = (\mathbb{I}_{n_i}, \mathbb{I}_{n_i}, C_{1i}, \mathbb{I}_{n_i}, \mathbb{I}_{n_i}, \mathbb{1}_{n_i}, F_i, 0.007\mathbb{1}_{n_i}, \varphi_i)$ satisfying

$$\Sigma_{\mathsf{nl}i}:\begin{cases} x_i(k+1) = x_i(k) + \mathbb{1}_{n_i}\varphi_i(F_ix_i(k)) + \nu_i(k) + w_i(k)\\ \qquad\qquad + 0.007\mathbb{1}_{n_i}\varsigma_i(k),\\ y_{1i}(k) = C_{1i}x_i(k),\\ y_{2i}(k) = x_i(k),\end{cases}$$

one can readily verify that $\Sigma_{\mathsf{nl}} = \mathcal{I}(\Sigma_{\mathsf{nl}1}, \ldots, \Sigma_{\mathsf{nl}N})$, where the coupling matrix M is given by $M = -\tau L$. Our goal is to aggregate each x_i into a scalar-valued $\hat{x}_i$, governed by $\widehat{\Sigma}_{\mathsf{nl}i} = (0.5, 1, \hat{C}_{1i}, 1, 1, 0.1, 1, 0, \varphi_i)$ which satisfies:

$$\widehat{\Sigma}_{\mathsf{nl}i}:\begin{cases} \hat{x}_i(k+1) = 0.5\hat{x}_i(k) + 0.1\varphi_i(\hat{x}_i(k)) + \hat{\nu}_i(k) + \hat{w}_i(k),\\ \hat{y}_{1i}(k) = \hat{C}_{1i}\hat{x}_i(k),\\ \hat{y}_{2i}(k) = \hat{x}_i(k),\end{cases}$$

where $\hat{C}_{1i} = C_{1i}\mathbb{1}_{n_i}$. Note that here $\hat{R}_i, \forall i \in \{1, \ldots, N\}$, are considered zero in order to reduce constants ψ_i for each V_i. One can readily verify that, for any $i \in \{1, \ldots, N\}$, conditions (5.4) and (5.5) are satisfied with $\tilde{M}_i = \mathbb{I}_{n_i}$, $\hat{\kappa}_i = 0.95$, $\tilde{\kappa}_i = 1, b_i = 1$, $K_i = (\lambda_i - 1)\mathbb{I}_{n_i}$, $\lambda_i = 0.5$, $Z_i = G_i = \mathbb{I}_{n_i}$, $L_{1i} = -\mathbb{1}_{n_i}$, $\tilde{R} = \mathbb{1}_{n_i}$, $\bar{X}^{11} = \mathbb{I}_{n_i}$, $\bar{X}^{22} = \mathbf{0}_{n_i}$, and $\bar{X}^{12} = \bar{X}^{21} = \lambda_i\mathbb{I}_{n_i}$. Moreover, for any $i \in \{1, \ldots, N\}$, $P_i = \mathbb{1}_{n_i}$ satisfies conditions (5.6) with $Q_i = -0.5\mathbb{1}_{n_i}$, $L_{2i} = -0.1\mathbb{1}_{n_i}$, and $H_i = \hat{G}_i = \mathbb{1}_{n_i}$. Hence, function $V_i(x_i, \hat{x}_i) = (x_i - \mathbb{1}_{n_i}\hat{x}_i)^T(x_i - \mathbb{1}_{n_i}\hat{x}_i)$ is an SStF from $\widehat{\Sigma}_{\mathsf{nl}i}$ to $\Sigma_{\mathsf{nl}i}$ satisfying condition (3.1) with $\alpha_i(s) = \frac{1}{\lambda_{\max}(C_{1i}^TC_{1i})}s^2$ and condition (3.2) with $\kappa_i(s) := 0.05s$, $\rho_{\mathrm{ext}i}(s) = 0$, $\forall s \in \mathbb{R}_{\geq 0}$, $G_i = \mathbb{I}_{n_i}$, $H_i = \mathbb{1}_{n_i}$, and

$$\bar{X}_i = \begin{bmatrix} \mathbb{I}_{n_i} & \lambda_i\mathbb{I}_{n_i}\\ \lambda_i\mathbb{I}_{n_i} & \mathbf{0}_{n_i}\end{bmatrix}, \tag{7.1}$$

where the input ν_i is given via the interface function in (10.4) as

$$\begin{aligned}\nu_i =& (\lambda_i - 1)(x_i - \mathbb{1}_{n_i}\hat{x}_i) - 0.5\mathbb{1}_{n_i}\hat{x}_i + \mathbb{1}_{n_i}\hat{\nu}_i\\ &- \mathbb{1}_{n_i}\varphi_i(F_ix_i) + 0.1\mathbb{1}_{n_i}\varphi_i(F_i\mathbb{1}_{n_i}\hat{x}_i).\end{aligned}$$

Now, we look at $\widehat{\Sigma}_{\mathsf{nl}} = \mathcal{I}(\widehat{\Sigma}_{\mathsf{nl}1}, \ldots, \widehat{\Sigma}_{\mathsf{nl}N})$ with a coupling matrix $\hat{M}$ satisfying condition (4.2) as follows:

$$-\tau L\ \mathsf{diag}(\mathbb{1}_{n_1}, \ldots, \mathbb{1}_{n_N}) = \mathsf{diag}(\mathbb{1}_{n_1}, \ldots, \mathbb{1}_{n_N})\hat{M}. \tag{7.2}$$

Note that the existence of $\hat{M}$ satisfying (7.2) for graph Laplacian τL means that the N subgraphs form an *equitable partition* of the full graph (Godsil & Royle 2001). Although this restricts the choice of a partition in general, for the complete graph any partition is equitable.

Choosing $\mu_1 = \cdots = \mu_N = 1$ and using $\bar{X}_i$ in (7.1), matrix $\bar{X}_{cmp}$ in (4.4) reduces to

$$\bar{X}_{cmp} = \begin{bmatrix} \mathbb{I}_n & \lambda\mathbb{I}_n\\ \lambda\mathbb{I}_n & \mathbf{0}_n\end{bmatrix},$$

where $\lambda = \lambda_1 = \cdots = \lambda_N = 0.5$, and condition (4.1) reduces to

$$\begin{aligned}\begin{bmatrix} -\tau L\\ \mathbb{I}_n\end{bmatrix}^T \bar{X}_{cmp} \begin{bmatrix} -\tau L\\ \mathbb{I}_n\end{bmatrix} &= \tau^2L^TL - \lambda\tau L - \lambda\tau L^T\\ &= \tau L(\tau L - 2\lambda\mathbb{I}_n) \preceq 0,\end{aligned}$$

without requiring any restrictions on the number or gains of the subsystems with $\tau = 0.9/(n-1)$. In order to show the above inequality, we used $\tau L = \tau L^T \succeq 0$ which is always true for Laplacian matrices of undirected graphs. Now, one can readily verify that $V(x, \hat{x}) = \sum_{i=1}^{n}(x_i - \mathbb{1}_{n_i}\hat{x}_i)^T(x_i - \mathbb{1}_{n_i}\hat{x}_i)$ is an SSF from $\widehat{\Sigma}_{\mathsf{nl}}$ to Σ_{nl} satisfying conditions (3.3) and (3.4).

For the sake of simulation, we assume L is the Laplacian matrix of a complete graph. We fix $N = 3$, $n = 222$, $n_i = 74$, and $C_{1i} = [1; 0; \dots; 0]^T$, $i \in \{1, 2, 3\}$. By using inequality (3.5) and starting the interconnected systems Σ_{nl} and $\widehat{\Sigma}_{\mathsf{nl}}$ from initial states $-13\mathbb{1}_{222}$ and $-13\mathbb{1}_3$, respectively, we guarantee that the distance between outputs of Σ_{nl} and $\widehat{\Sigma}_{\mathsf{nl}}$ will not exceed $\epsilon = 1$ during the time horizon $T_d = 10$ with probability at least 90%, i.e.

$$\mathbb{P}\left(\|y_{a\nu}(k) - \hat{y}_{\hat{a}\hat{\nu}}(k)\| \leq 1, \ \forall k \in [0, 10]\right) \geq 0.9.$$

Let us now synthesize a controller for Σ_{nl} via the abstraction $\widehat{\Sigma}_{\mathsf{nl}}$ to enforce the specification, defined by the following scLTL formula (cf. Definition 6.2):

$$\varpi = \bigwedge_{j=0}^{T_d} \bigcirc^j \Big(S \wedge \Big(\bigwedge_{i=1}^{3} (\neg O_i)\Big)\Big) \wedge \Diamond \bar{T}_1 \wedge \Diamond \bar{T}_2, \qquad (7.3)$$

which requires that any output trajectory y of the closed loop system evolves inside the set S, avoids sets O_i, $i \in \{1, 2, 3\}$, indicated with blue boxes in Figure 3, over bounded time interval $[0, T_d]$, and visits each $\bar{T}_i$, $i \in \{1, 2\}$, indicated with red boxes in Figure 3. We want to satisfy ϖ over bounded time interval $[0, 10]$, i.e., $T_d = 10$. We use `SCOTS` (Rungger & Zamani 2016) to synthesize a controller for $\widehat{\Sigma}_{\mathsf{nl}}$ to enforce (7.3). In the synthesis, process we restricted the abstract inputs $\hat{\nu}_1, \hat{\nu}_2, \hat{\nu}_3$ to $[-4, 4]$. We also set the initial states of Σ_{nl} to $x_i = P_i\hat{x}_i$, so that $V_i(x_i, \hat{x}_i) = 0$. A realization of closed-loop output trajectories of Σ_{nl} and $\widehat{\Sigma}_{\mathsf{nl}}$ is illustrated in Figure 3. Also, several realizations of the norm of the error between outputs of Σ_{nl} and $\widehat{\Sigma}_{\mathsf{nl}}$ are illustrated in Figure 4. In order to have some more practical 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_{nl} and $\widehat{\Sigma}_{\mathsf{nl}}$ is always less than or equal to 0.04 with the same probability, (i.e., at least 90%). 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 a formal guarantee on the output trajectories rather than empirical one. Note that it would not have been possible to synthesize a controller using `SCOTS` for the original 222-dimensional system Σ_{nl}, without the 3-dimensional intermediate approximation $\widehat{\Sigma}_{\mathsf{nl}}$. Moreover, we have intentionally dropped the noise of the abstraction and employed SCOTS here to show that if the concrete system possesses some nice stability property and the noises of two systems are additive and independent, it is actually better to construct and employ the non-stochastic abstraction since the non-stochastic abstraction is closer that the stochastic version (as discussed in Section 5).

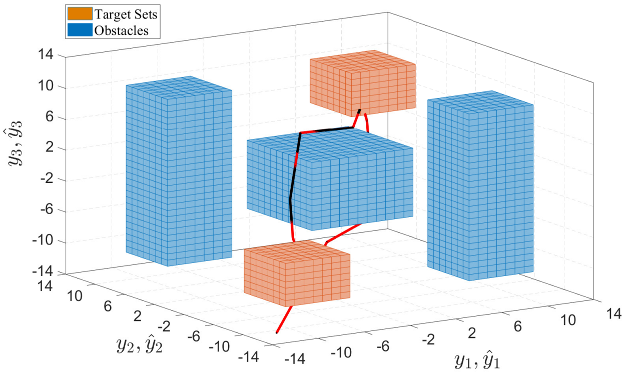

Fig. 3. The specification with closed-loop output trajectories of Σ_{nl} (black one) and $\widehat{\Sigma}_{\mathsf{nl}}$ (red one). The sets S, O_i, $i \in \{1, 2, 3\}$, and $\bar{T}_i$, $i \in \{1, 2\}$ are given by: $S = [-14, 14]^3$, $O_1 = [-10, -6] \times [6, 10] \times [10, 10]$, $O_2 = [-5, 5]^3$, and $O_3 = [6, 10] \times [-10, -6] \times [10, 10]$, $\bar{T}_1 = [-10, -6] \times [-10, -6] \times [-10, -6]$ and $\bar{T}_2 = [6, 10] \times [6, 10] \times [6, 10]$.

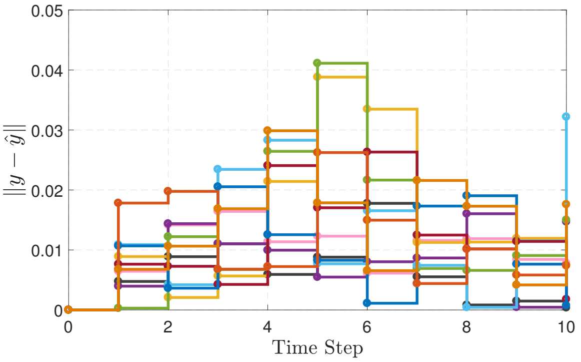

Fig. 4. A few realizations of the norm of the error between the outputs of Σ_{nl} and of $\widehat{\Sigma}_{\mathsf{nl}}$, e.g. $\|y - \hat{y}\|$, for $T_d = 10$.

8 Discussion

In this paper, we provided a compositional approach for infinite abstractions of interconnected discrete-time stochastic control systems, with independent noises in the abstract and concrete domains. To do so, we leveraged the interconnection matrix and joint dissipativity-type properties of subsystems and their abstractions. We introduced new notions of stochastic storage and simulation functions in order to quantify the distance in probability between original stochastic control subsystems and their abstractions and their interconnections, respectively. Using those notions, one can employ the proposed results here to synthesize policies enforcing certain temporal logic properties over abstract systems, and then refine them back to the concrete systems while quantifying the satisfaction errors. We also provided a computational scheme for a class of discrete-time nonlinear stochastic control systems to construct their abstractions together with their corresponding stochastic storage functions. Furthermore, we addressed a fragment of LTL known as syntactically co-safe LTL, and showed how to quantify the probability of satisfaction for such specifications. Finally, we demonstrated the effectiveness of the proposed results by constructing an abstraction (totally 3 dimensions) of the interconnection of three discrete-time nonlinear stochastic control subsystems (together 222 dimensions) in a compositional fashion. We employed the constructed abstraction as a substitute to synthesize a controller enforcing a syntactically co-safe LTL specification.

9 Acknowledgment

This work was supported in part by the H2020 ERC Starting Grant AutoCPS (grant agreement No. 804639) and the German Research Foundation (DFG) through the grant ZA 873/1-1.

References

Abate, A., Prandini, M., Lygeros, J. & Sastry, S. (2008), 'Probabilistic reachability and safety for controlled discrete time stochastic hybrid systems', *Automatica* **44**(11), 2724–2734.

Antsaklis, P. J. & Michel, A. N. (2007), *A linear systems primer*, Vol. 1, Birkhäuser Boston.

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

Baier, C., Katoen, J. P. & Larsen, K. G. (2008), *Principles of model checking*, MIT press.

Belta, C., Yordanov, B. & Gol, E. A. (2017), *Formal Methods for Discrete-Time Dynamical Systems*, Vol. 89 of *Studies in Systems, Decision and Control*, Springer.

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

Desharnais, J., Laviolette, F. & Tracol, M. (2008), Approximate analysis of probabilistic processes: logic, simulation and games, *in* 'Proceedings of the International Conference on Quantitative Evaluation of SysTems (QEST 08)', pp. 264–273.

Girard, A. & Pappas, G. J. (2009), 'Hierarchical control system design using approximate simulation', *Automatica* **45**(2), 566–571.

Godsil, C. & Royle, G. (2001), *Algebraic graph theory*, Graduate Texts in Mathematics, Springe.

Haesaert, S. & Soudjani, S. (2018), 'Robust dynamic programming for temporal logic control of stochastic systems', *CoRR* **abs/1811.11445**.

Haesaert, S., Soudjani, S. & Abate, A. (2017), 'Verification of general Markov decision processes by approximate similarity relations and policy refinement', **55**(4), 2333–2367.

Julius, A. A. & Pappas, G. J. (2009), 'Approximations of stochastic hybrid systems', *IEEE Transactions on Automatic Control* **54**(6), 1193–1203.

Kupferman, O. & Vardi, M. Y. (2001), 'Model checking of safety properties', *Formal Methods in System Design* **19**(3), 291–314.

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

Lavaei, A., Soudjani, S., Majumdar, R. & Zamani, M. (2017), Compositional abstractions of interconnected discrete-time stochastic control systems, *in* 'Proceedings of the 56th IEEE Conference on Decision and Control', pp. 3551–3556.

Lavaei, A., Soudjani, S. & Zamani, M. (2018*a*), 'Compositional (in)finite abstractions for large-scale interconnected stochastic systems', *arXiv: 1808.00893* .

Lavaei, A., Soudjani, S. & Zamani, M. (2018*b*), Compositional synthesis of finite abstractions for continuous-space stochastic control systems: A small-gain approach, *in* 'Proceedings of the 6th IFAC Conference on Analysis and Design of Hybrid Systems', Vol. 51, pp. 265–270.

Lavaei, A., Soudjani, S. & Zamani, M. (2018*c*), 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', pp. 21–30.

Lavaei, A., Soudjani, S. & Zamani, M. (2019), 'Compositional synthesis of large-scale stochastic systems: A relaxed dissipativity approach', *arXiv:1902.01223v2* .

Mallik, K., Soudjani, S., Schmuck, A.-K. & Majumdar, R. (2017), 'Compositional Construction of Finite State Abstractions for Stochastic Control Systems', *arXiv: 1709.09546* .

Rungger, M. & Zamani, M. (2016), SCOTS: A tool for the synthesis of symbolic controllers, *in* 'Proceedings of the 19th ACM International Conference on Hybrid Systems: Computation and Control', pp. 99–104.

Soudjani, S. (2014), Formal Abstractions for Automated Verification and Synthesis of Stochastic Systems, PhD thesis, Technische Universiteit Delft, The Netherlands.

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

Soudjani, S., Abate, A. & Majumdar, R. (2015), Dynamic Bayesian networks as formal abstractions of structured stochastic processes, *in* 'Proceedings of the 26th International Conference on Concurrency Theory', pp. 1–14.

Soudjani, S., Gevaerts, C. & Abate, A. (2015), FAUST^2: Formal abstractions of uncountable-state stochastic processes, *in* 'TACAS'15', Vol. 9035 of *Lecture Notes in Computer Science*, Springer, pp. 272–286.

Tabuada, P. (2009), *Verification and control of hybrid systems: a symbolic approach*, Springer Science & Business Media.

Tkachev, I. & Abate, A. (2011), On infinite-horizon probabilistic properties and stochastic bisimulation functions, *in* 'Proceedings of the 50th IEEE Conference on Decision and Control and European Control

Conference (CDC-ECC)', pp. 526–531.

Tkachev, I., Mereacre, A., Katoen, J. & Abate, A. (2013), 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', pp. 293–302.

Zamani, M. (2014), Compositional approximations of interconnected stochastic hybrid systems, *in* 'Proceedings of the 53rd IEEE Conference on Decision and Control (CDC)', pp. 3395–3400.

Zamani, M. & Abate, A. (2014), 'Approximately bisimilar symbolic models for randomly switched stochastic systems', *Systems & Control Letters* **69**, 38–46.

Zamani, M., Abate, A. & Girard, A. (2015), 'Symbolic models for stochastic switched systems: A discretization and a discretization-free approach', *Automatica* **55**, 183–196.

Zamani, M. & Arcak, M. (2018), 'Compositional abstraction for networks of control systems: A dissipativity approach', *IEEE Transactions on Control of Network Systems* **5**(3), 1003–1015.

Zamani, M., Mohajerin Esfahani, P., Majumdar, R., Abate, A. & Lygeros, J. (2014), 'Symbolic control of stochastic systems via approximately bisimilar finite abstractions', *IEEE Transactions on Automatic Control* **59**(12), 3135–3150.

Zamani, M., Rungger, M. & Mohajerin Esfahani, P. (2017), 'Approximations of stochastic hybrid systems: A compositional approach', *IEEE Transactions on Automatic Control* **62**(6), 2838–2853.

10 Appendix

Proof of Theorem 3.6: Since V is an SSF from $\widehat{\Sigma}$ to Σ, we have

$$\begin{aligned}
&\mathbb{P}\left\{\sup_{0\le k\le T_d}\|y_{a\nu}(k)-\hat{y}_{\hat{a}\hat{\nu}}(k)\|\ge\epsilon \mid [a;\hat{a}]\right\}\\
&=\mathbb{P}\left\{\sup_{0\le k\le T_d}\alpha\left(\|y_{a\nu}(k)-\hat{y}_{\hat{a}\hat{\nu}}(k)\|\right)\ge\alpha(\epsilon) \mid [a;\hat{a}]\right\}\\
&\le\mathbb{P}\left\{\sup_{0\le k\le T_d}V\left(x_{a\nu}(k),\hat{x}_{\hat{a}\hat{\nu}}(k)\right)\ge\alpha(\epsilon) \mid [a;\hat{a}]\right\}.
\end{aligned} \tag{10.1}$$

The equality holds due to α being a $\mathcal{K}_\infty$ function. The inequality is also true due to condition (3.3) on the SSF V. The results follow by applying the first part of Lemma 3.5 to (10.1) with some slight modification and utilizing inequality (3.4). ■

Proof of Corollary 3.7: Since V is an SSF from $\widehat{\Sigma}$ to Σ with $\rho_{\text{ext}}(\cdot)\equiv 0$ and $\psi=0$, for any $x(k)\in X$ and $\hat{x}(k)\in\hat{X}$ and any $\hat{\nu}(k)\in\hat{U}$, there exists $\nu(k)\in U$ such that

$$\begin{aligned}
&\mathbb{E}\Big[V(x(k+1),\hat{x}(k+1) \mid x(k),\hat{x}(k),\nu(k),\hat{\nu}(k)\Big]\\
&\quad - V((x(k),\hat{x}(k)) \le -\kappa(V(x(k),\hat{x}(k)),
\end{aligned}$$

implying that $V\left(x_{a\nu}(k),\hat{x}_{\hat{a}\hat{\nu}}(k)\right)$ is a nonnegative supermartingale (Kushner 1967, Chapter 1) for any initial condition a and $\hat{a}$ and inputs $\nu,\hat{\nu}$. Following the same reasoning as in the proof of Theorem 3.6, we have

$$\begin{aligned}
&\mathbb{P}\left\{\sup_{0\le k<\infty}\|y_{a\nu}(k)-\hat{y}_{\hat{a}\hat{\nu}}(k)\|\ge\epsilon \mid [a;\hat{a}]\right\}\\
=&\mathbb{P}\left\{\sup_{0\le k<\infty}\alpha\Big(\|y_{a\nu}(k)-\hat{y}_{\hat{a}\hat{\nu}}(k)\|\Big)\ge\alpha(\epsilon) \mid [a;\hat{a}]\right\}\\
\le&\mathbb{P}\left\{\sup_{0\le k<\infty}V(x_{a\nu}(k),\hat{x}_{\hat{a}\hat{\nu}}(k))\ge\alpha(\epsilon) \mid [a;\hat{a}]\right\}\le\frac{V(a,\hat{a})}{\alpha(\epsilon)},
\end{aligned}$$

where the last inequality is due to the nonnegative supermartingale property as presented in the second part of Lemma 3.5. ■

Proof of Theorem 4.2: We first show that inequality (3.3) holds 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:

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

with function $\bar{\alpha}:\mathbb{R}_{\ge0}\rightarrow\mathbb{R}_{\ge0}$ defined for all $r\in\mathbb{R}_{\ge0}$ as

$$\bar{\alpha}(r):=\max\left\{\textstyle\sum_{i=1}^{N}\alpha_i^{-1}(s_i) \;\middle|\; s_i\ge0,\ \textstyle\sum_{i=1}^{N}\mu_i s_i=r\right\}.$$

It is not hard to verify that function $\bar{\alpha}(\cdot)$ defined above is a $\mathcal{K}_\infty$ function. By taking the $\mathcal{K}_\infty$ function $\alpha(r):=\bar{\alpha}^{-1}(r)$, $\forall r\in\mathbb{R}_{\ge0}$, one obtains

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

satisfying inequality (3.3). Now we prove that function V in (4.5) satisfies inequality (3.4), as well. Consider any $x=[x_1;\ldots;x_N]\in X$, $\hat{x}=[\hat{x}_1;\ldots;\hat{x}_N]\in\hat{X}$, and $\hat{\nu}=[\hat{\nu}_1;\ldots;\hat{\nu}_N]\in\hat{U}$. For any $i\in\{1,\ldots,N\}$, there exists $\nu_i\in U_i$, consequently, a vector $\nu=[\nu_1;\ldots;\nu_N]\in U$, satisfying (3.2) for each pair of subsystems Σ_i and $\widehat{\Sigma}_i$ with the internal inputs given by $[w_1;\ldots;w_N]=M[h_{21}(x_1);\ldots;h_{2N}(x_N)]$ and $[\hat{w}_1;\ldots;\hat{w}_N]=\hat{M}[\hat{h}_{21}(\hat{x}_1);\ldots;\hat{h}_{2N}(\hat{x}_N)]$. Then we have the chain of inequalities in (10.2) using conditions (4.1) and (4.2), and by defining $\kappa(\cdot),\rho_{\text{ext}}(\cdot),\psi$ as

$$
\begin{aligned}
&\mathbb{E}\Big[\sum_{i=1}^{N}\mu_i V_i(x_i(k+1),\hat{x}_i(k+1))\,\big|\,x(k)=x,\hat{x}(k)=\hat{x},\hat{\nu}(k)=\hat{\nu}\Big]-\sum_{i=1}^{N}\mu_i V_i(x_i,\hat{x}_i)\\
&=\sum_{i=1}^{N}\mu_i\mathbb{E}\Big[V_i(x_i(k+1),\hat{x}_i(k+1))\,\big|\,x_i(k)=x_i,\hat{x}_i(k)=\hat{x}_i,\hat{\nu}_i(k)=\hat{\nu}_i\Big]-\sum_{i=1}^{N}\mu_i V_i(x_i,\hat{x}_i)\\
&\leq\sum_{i=1}^{N}\mu_i\Big(-\kappa_i(V_i(x_i,\hat{x}_i))+\rho_{\text{ext}i}(\|\hat{\nu}_i\|)+\psi_i+\begin{bmatrix}G_iw_i-\hat{G}_i\hat{w}_i\\ h_{2i}(x_i)-H_i\hat{h}_{2i}(\hat{x}_i)\end{bmatrix}^T\begin{bmatrix}\bar{X}_i^{11} & \bar{X}_i^{12}\\ \bar{X}_i^{21} & \bar{X}_i^{22}\end{bmatrix}\begin{bmatrix}G_iw_i-\hat{G}_i\hat{w}_i\\ h_{2i}(x_i)-H_i\hat{h}_{2i}(\hat{x}_i)\end{bmatrix}\Big)\\
&=\sum_{i=1}^{N}-\mu_i\kappa_i(V_i(x_i,\hat{x}_i))+\sum_{i=1}^{N}\mu_i\rho_{\text{ext}i}(\|\hat{\nu}_i\|)+\sum_{i=1}^{N}\mu_i\psi_i\\
&+\begin{bmatrix}G_1w_1-\hat{G}_1\hat{w}_1\\ \vdots\\ G_Nw_N-\hat{G}_N\hat{w}_N\\ h_{21}(x_1)-H_1\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ h_{2N}(x_N)-H_N\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}^T\begin{bmatrix}\mu_1\bar{X}_1^{11} & & \mu_1\bar{X}_1^{12} & \\ & \ddots & & \ddots\\ & \mu_N\bar{X}_N^{11} & & \mu_N\bar{X}_N^{12}\\ \mu_1\bar{X}_1^{21} & & \mu_1\bar{X}_1^{22} & \\ & \ddots & & \ddots\\ & \mu_N\bar{X}_N^{21} & & \mu_N\bar{X}_N^{22}\end{bmatrix}\begin{bmatrix}G_1w_1-\hat{G}_1\hat{w}_1\\ \vdots\\ G_Nw_N-\hat{G}_N\hat{w}_N\\ h_{21}(x_1)-H_1\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ h_{2N}(x_N)-H_N\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}\\
&=\sum_{i=1}^{N}-\mu_i\kappa_i(V_i(x_i,\hat{x}_i))+\sum_{i=1}^{N}\mu_i\rho_{\text{ext}i}(\|\hat{\nu}_i\|)+\sum_{i=1}^{N}\mu_i\psi_i\\
&+\begin{bmatrix}GM\begin{bmatrix}h_{21}(x_1)\\ \vdots\\ h_{2N}(x_N)\end{bmatrix}-\hat{G}\hat{M}\begin{bmatrix}\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ \hat{h}_{2N}(\hat{x}_N)\end{bmatrix}\\ h_{21}(x_1)-H_1\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ h_{2N}(x_N)-H_N\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}^T\bar{X}_{cmp}\begin{bmatrix}GM\begin{bmatrix}h_{21}(x_1)\\ \vdots\\ h_{2N}(x_N)\end{bmatrix}-\hat{G}\hat{M}\begin{bmatrix}\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ \hat{h}_{2N}(\hat{x}_N)\end{bmatrix}\\ h_{21}(x_1)-H_1\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ h_{2N}(x_N)-H_N\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}=\sum_{i=1}^{N}-\mu_i\kappa_i(V_i(x_i,\hat{x}_i))\\
&+\sum_{i=1}^{N}\mu_i\rho_{\text{ext}i}(\|\hat{\nu}_i\|)+\sum_{i=1}^{N}\mu_i\psi_i+\begin{bmatrix}h_{21}(x_1)-H_1\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ h_{2N}(x_N)-H_N\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}^T\begin{bmatrix}GM\\ \mathbb{I}_{\tilde{q}}\end{bmatrix}^T\bar{X}_{cmp}\begin{bmatrix}GM\\ \mathbb{I}_{\tilde{q}}\end{bmatrix}\begin{bmatrix}h_{21}(x_1)-H_1\hat{h}_{21}(\hat{x}_1)\\ \vdots\\ h_{2N}(x_N)-H_N\hat{h}_{2N}(\hat{x}_N)\end{bmatrix}\\
&\leq\sum_{i=1}^{N}-\mu_i\kappa_i(V_i(x_i,\hat{x}_i))+\sum_{i=1}^{N}\mu_i\rho_{\text{ext}i}(\|\hat{\nu}_i\|)+\sum_{i=1}^{N}\mu_i\psi_i\leq-\kappa\left(V\left(x,\hat{x}\right)\right)+\rho_{\text{ext}}(\|\hat{\nu}\|)+\psi.
\end{aligned}
\tag{10.2}
$$

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

Note that κ and ρ_{ext} in (10.2) belong to $\mathcal{K}$ and $\mathcal{K}_\infty\cup\{0\}$, respectively, because of their definitions provided above.

Hence, we conclude that V is an SSF from $\widehat{\Sigma}$ to Σ. ■

Proof of Theorem 5.3: Here, we first show that $\forall x$, $\forall\hat{x}$, $\forall\hat{\nu}$, $\exists\nu$, $\forall\hat{w}$, and $\forall w$, V satisfies $\frac{\lambda_{\min}(\tilde{M})}{\lambda_{\max}(C_1^TC_1)}\|C_1x-\hat{C}_1\hat{x}\|^2\leq V(x,\hat{x})$ and then

---

$$
\begin{aligned}
&\mathbb{E}\Big[V(x(k+1),\hat{x}(k+1)\,|\,x(k)\!=\!x,\hat{x}(k)\!=\!\hat{x},w(k)\!=\!w,\hat{w}(k)\!=\!\hat{w},\hat{\nu}(k)\!=\!\hat{\nu}\Big]-V(x,\hat{x})\\
&\quad=(x-P\hat{x})^T\Big[((A+BK)+\bar{\delta}(BL_1+E)F)^T\tilde{M}((A+BK)+\bar{\delta}(BL_1+E)F)\Big](x-P\hat{x})+2\Big[(x-P\hat{x})^T((A+BK)\\
&\quad+\bar{\delta}(BL_1+E)F)^T\Big]\tilde{M}\Big[Z(Gw-\hat{G}\hat{w})\Big]+2\Big[(x-P\hat{x})^T((A+BK)+\bar{\delta}(BL_1+E)F)^T\Big]\tilde{M}\Big[(B\tilde{R}-P\hat{B})\hat{\nu}\Big]\\
&\quad+2\Big[(Gw-\hat{G}\hat{w})^TZ^T\Big]\tilde{M}\Big[(B\tilde{R}-P\hat{B})\hat{\nu}\Big]+\hat{\nu}^T(B\tilde{R}-P\hat{B})^T\tilde{M}(B\tilde{R}-P\hat{B})\hat{\nu}+(Gw-\hat{G}\hat{w})^TZ^T\tilde{M}Z(Gw-\hat{G}\hat{w})\\
&\quad+\mathrm{Tr}\big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\big)-V(x,\hat{x})=\begin{bmatrix}x-P\hat{x}\\ Gw-\hat{G}\hat{w}\\ \bar{\delta}F(x-P\hat{x})\\ \hat{\nu}\end{bmatrix}^T\\
&\quad\begin{bmatrix}(A+BK)^T\tilde{M}(A+BK) & (A+BK)^T\tilde{M}Z & (A+BK)^T\tilde{M}(BL_1+E) & (A+BK)^T\tilde{M}(B\tilde{R}-P\hat{B})\\ * & Z^T\tilde{M}Z & Z^T\tilde{M}(BL_1+E) & Z^T\tilde{M}(B\tilde{R}-P\hat{B})\\ * & * & (BL_1+E)^T\tilde{M}(BL_1+E) & (BL_1+E)^T\tilde{M}(B\tilde{R}-P\hat{B})\\ * & * & * & (B\tilde{R}-P\hat{B})^T\tilde{M}(B\tilde{R}-P\hat{B})\end{bmatrix}\begin{bmatrix}x-P\hat{x}\\ Gw-\hat{G}\hat{w}\\ \bar{\delta}F(x-P\hat{x})\\ \hat{\nu}\end{bmatrix}\\
&\quad+\mathrm{Tr}\Big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\Big)-V(x,\hat{x})\leq\begin{bmatrix}x-P\hat{x}\\ Gw-\hat{G}\hat{w}\\ \bar{\delta}F(x-P\hat{x})\\ \hat{\nu}\end{bmatrix}^T\begin{bmatrix}\hat{\kappa}\tilde{M}+C_2^T\bar{X}^{22}C_2 & C_2^T\bar{X}^{21} & -F^T & 0\\ \bar{X}^{12}C_2 & \bar{X}^{11} & 0 & 0\\ -F & 0 & \frac{2}{b} & 0\\ 0 & 0 & 0 & \tilde{k}(B\tilde{R}-P\hat{B})^T\tilde{M}(B\tilde{R}-P\hat{B})\end{bmatrix}\\
&\quad\begin{bmatrix}x-P\hat{x}\\ Gw-\hat{G}\hat{w}\\ \bar{\delta}F(x-P\hat{x})\\ \hat{\nu}\end{bmatrix}+\mathrm{Tr}\Big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\Big)-V(x,\hat{x})=-(1-\hat{\kappa})(V(x,\hat{x}))-2\bar{\delta}(1-\frac{\bar{\delta}}{b})(x-P\hat{x})^TF^TF(x-P\hat{x})\\
&\quad+\tilde{k}\|\sqrt{\tilde{M}}(B\tilde{R}-P\hat{B})\nu\|^2+\begin{bmatrix}Gw-\hat{G}\hat{w}\\ C_2x-H\hat{C}_2\hat{x}\end{bmatrix}^T\begin{bmatrix}\bar{X}^{11} & \bar{X}^{12}\\ \bar{X}^{21} & \bar{X}^{22}\end{bmatrix}\begin{bmatrix}Gw-\hat{G}\hat{w}\\ C_2x-H\hat{C}_2\hat{x}\end{bmatrix}+\mathrm{Tr}\Big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\Big)\\
&\quad\leq-(1-\hat{\kappa})(V(x,\hat{x}))+\tilde{k}\|\sqrt{\tilde{M}}(B\tilde{R}-P\hat{B})\|^2\|\hat{\nu}\|^2+\begin{bmatrix}Gw-\hat{G}\hat{w}\\ C_2x-H\hat{C}_2\hat{x}\end{bmatrix}^T\begin{bmatrix}\bar{X}^{11} & \bar{X}^{12}\\ \bar{X}^{21} & \bar{X}^{22}\end{bmatrix}\begin{bmatrix}Gw-\hat{G}\hat{w}\\ C_2x-H\hat{C}_2\hat{x}\end{bmatrix}\\
&\quad+\mathrm{Tr}\Big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\Big). \qquad (10.3)
\end{aligned}
$$

$$
\begin{aligned}
&\mathbb{E}\Big[V(x(k+1),\hat{x}(k+1)\,|\,x(k)=x,\hat{x}(k)=\hat{x},w(k)\!=\!w,\\
&,\hat{w}(k)\!=\!\hat{w},\hat{\nu}(k)\!=\!\hat{\nu}\Big]-V(x,\hat{x})\\
&\leq-(1-\hat{\kappa})(V(x,\hat{x}))+\tilde{k}\|\sqrt{\tilde{M}}(B\tilde{R}-P\hat{B})\|^2\|\hat{\nu}\|^2\\
&+\begin{bmatrix}Gw-\hat{G}\hat{w}\\ h_2(x)-H\hat{h}_2(\hat{x})\end{bmatrix}^T\begin{bmatrix}\bar{X}^{11} & \bar{X}^{12}\\ \bar{X}^{21} & \bar{X}^{22}\end{bmatrix}\begin{bmatrix}Gw-\hat{G}\hat{w}\\ h_2(x)-H\hat{h}_2(\hat{x})\end{bmatrix}\\
&+\mathrm{Tr}\Big(R^T\tilde{M}R+\hat{R}^TP^T\tilde{M}P\hat{R}\Big).
\end{aligned}
$$

According to (5.6b), we have $\|C_1x-\hat{C}_1\hat{x}\|^2=(x-P\hat{x})^TC_1^TC_1(x-P\hat{x})$. Since $\lambda_{\min}(C_1^TC_1)\|x-P\hat{x}\|^2\leq(x-P\hat{x})^TC_1^TC_1(x-P\hat{x})\leq\lambda_{\max}(C_1^TC_1)\|x-P\hat{x}\|^2$, and similarly, $\lambda_{\min}(\tilde{M})\|x-P\hat{x}\|^2\leq(x-P\hat{x})^T\tilde{M}(x-P\hat{x})\leq\lambda_{\max}(\tilde{M})\|x-P\hat{x}\|^2$, it can be readily verified that $\frac{\lambda_{\min}(\tilde{M})}{\lambda_{\max}(C_1^TC_1)}\|C_1x-\hat{C}_1\hat{x}\|^2\leq V(x,\hat{x})$ holds $\forall x$, $\forall\hat{x}$, implying that inequality (3.1) holds with $\alpha(s)=\frac{\lambda_{\min}(\tilde{M})}{\lambda_{\max}(C_1^TC_1)}s^2$ for any $s\in\mathbb{R}_{\geq0}$. We proceed with showing that the inequality (3.2) holds, as well. Given any x, $\hat{x}$, and $\hat{\nu}$, we choose ν via the following *interface* function:

$$
\begin{aligned}
&\nu\!=\!\nu_{\hat{\nu}}(x,\hat{x},\hat{\nu}):=\\
&\quad K(x\!-\!P\hat{x})\!+\!Q\hat{x}\!+\!\tilde{R}\hat{\nu}\!+\!L_1\varphi(Fx)\!-\!L_2\varphi(FP\hat{x}), \qquad (10.4)
\end{aligned}
$$

for some matrix $\tilde{R}$ of appropriate dimension. By employing the equations (5.4), (5.6a), (5.6e), (5.6f) and also the definition of the interface function in (10.4), we simplify

$$\begin{aligned}&Ax+E\varphi(Fx)+B\nu_{\hat{\nu}}(x,\hat{x},\hat{\nu})+Dw\\&\quad-P(\hat{A}\hat{x}+\hat{E}\varphi(\hat{F}\hat{x})+\hat{B}\hat{\nu}+\hat{D}\hat{w})+(R\varsigma-P\hat{R}\hat{\varsigma})\end{aligned}$$

to

$$\begin{aligned}&(A+BK)(x-P\hat{x})+Z(Gw-\hat{G}\hat{w})+(B\tilde{R}-P\hat{B})\hat{\nu}\\&\quad+(BL_1+E)(\varphi(Fx)-\varphi(FP\hat{x}))+(R\varsigma-P\hat{R}\hat{\varsigma}).\end{aligned}\tag{10.5}$$

From the slope restriction (5.2), one obtains

$$\varphi(Fx)-\varphi(FP\hat{x})=\bar{\delta}(Fx-FP\hat{x})=\bar{\delta}F(x-P\hat{x}),\tag{10.6}$$

where $\bar{\delta}$ is a function of x and $\hat{x}$ and takes values in the interval $[0,b]$. Using (10.6), the expression in (10.5) reduces to

$$\begin{aligned}&((A+BK)+\bar{\delta}(BL_1+E)F)(x-P\hat{x})+Z(Gw-\hat{G}\hat{w})\\&\quad+(B\tilde{R}-P\hat{B})\hat{\nu}+(R\varsigma-P\hat{R}\hat{\varsigma}).\end{aligned}$$

Using Cauchy- Schwarz inequality, (5.5), (5.6c), and (5.6d), one can obtain the chain of inequalities in (10.3) in order to acquire an upper bound. Hence, the proposed V in (5.3) is an SStF from $\widehat{\Sigma}_{\mathsf{nl}}$ to Σ_{nl}, which completes the proof. ■

Proof of Lemma 6.5: Suppose $\hat{y}(\cdot)\vDash_{\mathsf{L}^\epsilon}\hat{\phi}$ over time interval $[0,T_d]$. According to the construction of DFA $\mathcal{A}_{\hat{\phi}}$, q_{abs} is an absorbing state and not an accepting state, thus $\mathsf{L}^\epsilon(\hat{y}(k))\neq\phi_\circ$, $\forall k\in[0,T_d]$. Then $\mathsf{L}^\epsilon(\hat{y}(k))\in\Sigma_{\mathsf{a}}$, $\forall k\in[0,T_d]$. Assume $\mathsf{L}^\epsilon(\hat{y}(k))=a$ then $\hat{y}(k)\in[\mathsf{L}^{-1}(a)]^\epsilon$. Since we know that

$$\sup_{0\leq k\leq T_d}\|y(k)-\hat{y}(k)\|<\epsilon,$$

then according to the definition of ϵ-perturbed sets, $y(k)\in\mathsf{L}^{-1}(a)$ which gives $\mathsf{L}(y(k))=a$. Thus $\mathsf{L}(y(\cdot))=\mathsf{L}^\epsilon(\hat{y}(\cdot))$ and having $\hat{y}(\cdot)\vDash_{\mathsf{L}^\epsilon}\hat{\phi}$ guarantees $y(\cdot)\vDash_{\mathsf{L}}\phi$ due to the particular construction of $\hat{\phi}$. ■

Proof of Theorem 6.6: According to Lemma 6.5, $y(\cdot)\nvDash_{\mathsf{L}}\phi$ results in $\hat{y}(\cdot)\nvDash_{\mathsf{L}^\epsilon}\hat{\phi}$ over time interval $[0,T_d]$ or

$$\sup_{0\leq k\leq T_d}\|y(k)-\hat{y}(k)\|\geq\epsilon.$$

Then

$$\begin{aligned}&\mathbb{P}(y(\cdot)\nvDash_{\mathsf{L}}\phi)\leq\mathbb{P}(\hat{y}(\cdot)\nvDash_{\mathsf{L}^\epsilon}\hat{\phi})+\overbrace{\mathbb{P}(\sup_{0\leq k\leq T_d}\|y(k)-\hat{y}(k)\|\geq\epsilon)}^{\leq\delta},\\&\Rightarrow 1-\mathbb{P}(y(\cdot)\vDash_{\mathsf{L}}\phi)\leq 1-\mathbb{P}(\hat{y}(\cdot)\vDash_{\mathsf{L}^\epsilon}\hat{\phi})+\delta,\\&\Rightarrow\mathbb{P}(\hat{y}(\cdot)\vDash_{\mathsf{L}^\epsilon}\hat{\phi})-\delta\leq\mathbb{P}(y(\cdot)\vDash_{\mathsf{L}}\phi),\end{aligned}$$

which completes the proof. ■