Automatica 131 (2021) 109745

Contents lists available at ScienceDirect

Automatica

journal homepage: www.elsevier.com/locate/automatica

Brief paper

Compositional synthesis of opacity-preserving finite abstractions for interconnected systems ☆

Siyuan Liu [a,c,*], Majid Zamani [b,c]

[a] Department of Electrical and Computer Engineering, Technical University of Munich, 80333, Germany
[b] Computer Science Department, University of Colorado Boulder, CO 80309, USA
[c] Computer Science Department, LMU Munich, 80539, Germany

ARTICLE INFO

Article history:
Received 31 March 2020
Received in revised form 27 April 2021
Accepted 8 May 2021
Available online 10 June 2021

Keywords:
Large-scale complex systems
Opacity verification
Finite abstractions
Compositionality

ABSTRACT

In this paper, we propose a compositional approach to construct opacity-preserving finite abstractions (a.k.a symbolic models) for networks of discrete-time nonlinear control systems. Particularly, we introduce new notions of simulation functions that characterize the distance between control systems while preserving opacity properties across them. Instead of treating large-scale systems in a monolithic manner, we develop a compositional scheme to construct the finite abstractions together with the overall opacity-preserving simulation functions based on those of the smaller subsystems. For a network of incrementally input-to-state stable control subsystems and under some small-gain type condition, an algorithm for designing local quantization parameters is presented to orderly build the local symbolic models of subsystems. We show that the network of those constructed symbolic models simulates the original network for an a-priori defined abstraction accuracy while preserving its opacity properties.

1. Introduction

In the recent decade, the world has witnessed a rapid increase in applications of cyber–physical systems (CPSs), which are networked systems resulting from intricate interactions of cyber components and physical plants. However, new threats have been continuously affecting the performance and safety of CPSs. One of the major issues is security problems. In particular, the complex interaction between embedded (cyber) software and physical devices may release secret information and expose the system to (cyber) attackers. Therefore, new approaches to analyze or enforce security over safety-critical CPSs have emerged in the past few years (Ashibani & Mahmoud, 2017).

In this paper, we focus on an information-flow security property called *opacity*, which was originally proposed in the realm of computer science for the analysis of cryptographic protocols (Mazaré, 2004) but has not been thoroughly investigated in the domain of CPSs. As a confidentiality property, opacity characterizes the ability of a system to avoid leaking "secret" information in the presence of outside observers with potentially malicious intentions. In discrete-event systems (DESs) literature, different notions of opacity were proposed to capture various types of secret requirements, including state-based notions (Saboori & Hadjicostis, 2007, 2011, 2012, 2013b) and language-based notions (Lin, 2011). Recently, more research on opacity of various classes of discrete systems has been conducted (Saboori & Hadjicostis, 2013a; Tong, Li, Seatzu, & Giua, 2017); see some recent surveys in Jacob, Lesage, and Faure (2016) and Lafortune, Lin, and Hadjicostis (2018) for more details about opacity of DESs. Unfortunately, most of the existing results on opacity are tailored to DESs, where they consider the event-based observation model, i.e., some events of the system are observable or distinguishable while some are not. Whereas in real-world applications, outputs are typically physical signals equipped with some metrics and state space are usually continuous. A recent work (Ramasubramanian, Cleaveland, & Marcus, 2020) extended the notion of opacity to discrete-time (switched) linear systems. However, their definition of opacity is more related to an output reachability property rather than an information-flow one. To the best of our knowledge, most of the existing results on opacity are not suitable for capturing the information-flow security of real-world CPSs.

In this work, we aim at leveraging symbolic techniques to verify opacity for CPSs. In particular, we address this property

☆ This work was supported in part by the German Research Foundation (DFG) through the grant ZA 873/7-1, China Scholarship Council, and the National Science Foundation (NSF), USA under Grant ECCS-2015403. The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Christoforos Hadjicostis under the direction of Editor Christos G. Cassandras.

* Corresponding author at: Department of Electrical and Computer Engineering, Technical University of Munich, 80333, Germany.
E-mail addresses: sy.liu@tum.de (S. Liu), majid.zamani@colorado.edu (M. Zamani).

https://doi.org/10.1016/j.automatica.2021.109745
0005-1098/

by constructing finite abstractions of concrete systems based on some types of opacity-preserving simulation relations between concrete systems and their abstractions. These relations enable us to verify opacity for concrete systems by performing the corresponding analysis over their finite abstractions. Moreover, by following such a detour process, one can leverage (by some adaptation) existing computational tools developed in DESs literature to verify or enforce opacity over CPSs. In recent years, there have been some attempts in the literature to leverage abstraction-based techniques for the verification or enforcement of opacity (Liu, Yin, & Zamani, 2020; Wu & Lin, 2018; Yin, Zamani, & Liu, 2021; Zhang, Yin, & Zamani, 2019). The result in Wu and Lin (2018) introduced an abstract model based on the belief space of the intruder, using which controllers are synthesized to enforce opacity. However, the systems considered there are modeled as transition systems with finite state sets, thus, not suitable for general CPSs. In Zhang et al. (2019), a new formulation of opacity-preserving (bi)simulation relations is proposed, which allows one to verify opacity of an infinite-state transition system by leveraging its associated quotient one. However, the notion of opacity proposed there assumes that the outputs of systems are symbols and exactly distinguishable from each other, thus, is only suitable for systems with purely logical output sets. In Yin et al. (2021), a new notion called *approximate opacity* is proposed to suitably capture the continuity of output spaces of real-world CPSs. Additionally, a new simulation relation, called approximate opacity-preserving simulation relation, was proposed to characterize the closeness of two systems while preserving approximate opacity across them. The recent results in Liu et al. (2020) investigate opacity for discrete-time stochastic control systems using a notion of initial-state opacity-preserving stochastic simulation functions between stochastic control systems and their finite abstractions (finite Markov Decision Processes). Though promising, when confronted with large-scale interconnected systems, the construction of finite abstractions in the aforementioned literatures will suffer severely from the *curse of dimensionality* because the number of discrete states grows exponentially with the dimension of the concrete monolithic state set.

Motivated by the abstraction-based techniques in Liu et al. (2020), Yin et al. (2021), Zhang et al. (2019) and their computational complexity issues, here, we aim at providing a compositional framework to conquer this complexity challenge using a "divide and conquer" strategy. To this purpose, we first introduce new notions of opacity-preserving simulation functions for both subsystems and the entire networks. Based on these notions, we propose a compositional scheme on the construction of abstractions for concrete networks. Rather than dealing with the original large-scale system, our compositional framework allows one to construct opacity-preserving abstractions locally using local opacity-preserving simulation functions, while providing the guarantee that the interconnection of local abstractions simulates the concrete network while preserving opacity across them. By exploiting the interconnection topology of the network, an algorithm is presented to orderly design local quantization parameters with the guarantee of obtaining an overall finite abstraction with any desired precision. Remark that compositional approaches have been investigated recently for controller synthesis of interconnected CPSs, see e.g., Kim, Arcak, and Zamani (2018), Mallik, Schmuck, Soudjani, and Majumdar (2018), Pola, Pepe, and Di Benedetto (2016), Swikir and Zamani (2019) and Tazaki and Imura (2008). Unfortunately, none of those techniques is applicable to the verification or enforcement of opacity mainly because their underlying system relations do not necessarily preserve opacity across related systems (Zhang et al., 2019).

2. Preliminaries

Notation: We denote by $\mathbb{R}$ and $\mathbb{N}$ the set of real numbers and non-negative integers, respectively. These symbols are annotated with subscripts to restrict them in the usual way. The closed and open intervals in $\mathbb{R}$ are denoted by $[a\ b]$ and $]a\ b[$, respectively. For $a, b \in \mathbb{N}$ and $a \leq b$, we use $[a; b]$ and $]a; b[$ to denote the corresponding intervals in $\mathbb{N}$. Given $N \in \mathbb{N}_{\geq 1}$ vectors $x_i \in \mathbb{R}^{n_i}$ with $i \in [1; N]$, $n_i \in \mathbb{N}_{\geq 1}$, and $n = \sum_i n_i$, we denote the concatenated vector in $\mathbb{R}^n$ by $x = [x_1; \ldots; x_N]$ and the infinity norm of x by $\|x\|$. Given $a \in \mathbb{R}$, $|a|$ denotes the absolute value of a. The composition of functions f and g is denoted by $f \circ g$. We use notations $\mathcal{K}$ and $\mathcal{K}_\infty$ to denote the different classes of comparison functions, as follows: $\mathcal{K} = \{\gamma : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} \mid \gamma \text{ is continuous, strictly increasing and} \gamma(0) = 0\}$; $\mathcal{K}_\infty = \{\gamma \in \mathcal{K} \mid \lim_{r\to\infty} \gamma(r) = \infty\}$. We use $\mathcal{I}_d$ to denote identity function and $\text{card}(X)$ the cardinality of a finite set X. The complement of set X w.r.t. Y is defined as $Y \backslash X = \{x : x \in Y, x \notin X\}$. For any set $S \subseteq \mathbb{R}^n$ of the form of finite union of boxes, e.g., $S = \bigcup_{j=1}^{M} S_j$ for some $M \in \mathbb{N}$, where $S_j = \prod_{i=1}^{n} [c_i^j, d_i^j] \subseteq \mathbb{R}^n$ with $c_i^j < d_i^j$, we define $span(S) = \min_{j=1,\ldots,M} \eta_{S_j}$ and $\eta_{S_j} = \min\{|d_1^j - c_1^j|, \ldots, |d_n^j - c_n^j|\}$. Moreover, for a set in the form of $X = \prod_{i=1}^{N} X_i$, where $X_i \subseteq \mathbb{R}^{n_i}$ are of the form of finite union of boxes, and any positive (componentwise) vector $\phi = [\phi_1; \ldots; \phi_N]$ with $\phi_i \leq span(X_i)$, $\forall i \in [1; N]$, we define $[X]_\phi = \prod_{i=1}^{N} [X_i]_{\phi_i}$, where $[X_i]_{\phi_i} = [\mathbb{R}^{n_i}]_{\phi_i} \cap X_i$ and $[\mathbb{R}^{n_i}]_{\phi_i} = \{a \in \mathbb{R}^{n_i} \mid a_j = k_j \phi_i, k_j \in \mathbb{Z}, j = 1, \ldots, n_i\}$. Note that if $\phi = [\eta; \ldots; \eta]$, $0 < \eta \leq span(S)$, we simply use notation $[S]_\eta$ rather than $[S]_\phi$.

2.1. Discrete-time control systems

In this paper we study the class of discrete-time control systems of the following form.

Definition 2.1. A discrete-time control system (dt-CS) Σ is defined by the tuple $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, \mathbb{W}, f, \mathbb{Y}, h)$ where $\mathbb{X}$, $\mathbb{U}$, $\mathbb{W}$ and $\mathbb{Y}$ are the state, external input, internal input, and output set, respectively. We denote by $\mathbb{X}_0, \mathbb{X}_s \subseteq \mathbb{X}$ the set of initial states and secret states, respectively. The set-valued map $f : \mathbb{X} \times \mathbb{U} \times \mathbb{W} \rightrightarrows \mathbb{X}$ is the state transition function, and $h : \mathbb{X} \to \mathbb{Y}$ is the output function. The dt-CS Σ is described by difference inclusions of the form

$$\Sigma : \begin{cases} \mathbf{x}(t+1) \in & f(\mathbf{x}(t), \nu(t), \omega(t)), \\ \mathbf{y}(t) = & h(\mathbf{x}(t)), \end{cases} \tag{2.1}$$

where $\mathbf{x} : \mathbb{N} \to \mathbb{X}$, $\mathbf{y} : \mathbb{N} \to \mathbb{Y}$, $\nu : \mathbb{N} \to \mathbb{U}$, and $\omega : \mathbb{N} \to \mathbb{W}$ are the state, output, external input, and internal input signals, respectively. System $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, \mathbb{W}, f, \mathbb{Y}, h)$ is called deterministic if $\text{card}(f(x, u, w)) \leq 1$ $\forall x \in \mathbb{X}, \forall u \in \mathbb{U}, \forall w \in \mathbb{W}$, and non-deterministic otherwise. System Σ is called finite if $\mathbb{X}$, $\mathbb{U}$, $\mathbb{W}$ are finite sets and infinite otherwise.

Consider $N \in \mathbb{N}_{\geq 1}$ systems Σ_i as in Definition 2.1, $i \in [1; N]$. Assume internal inputs and output maps are partitioned as

$$w_i = [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}], \tag{2.2}$$

$$h_i(x_i) = [h_{i1}(x_i); \ldots; h_{iN}(x_i)], \tag{2.3}$$

with $\mathbb{W}_i = \prod_{j=1, j\neq i}^{N} \mathbb{W}_{ij}$ and $\mathbb{Y}_i = \prod_{j=1}^{N} \mathbb{Y}_{ij}$, $w_{ij} \in \mathbb{W}_{ij}$, $y_{ij} = h_{ij}(x_i) \in \mathbb{Y}_{ij}$. The outputs y_{ii} are considered as external ones, whereas y_{ij} with $i \neq j$ are interpreted as internal ones to construct interconnections between subsystems. In the case that no connection exists between subsystems Σ_i and Σ_j, we simply have $h_{ij} \equiv 0$. Now, we are ready to provide a formal definition of interconnected dt-CSs as follows.

Definition 2.2. Consider $N \in \mathbb{N}_{\geq 1}$ dt-CSs $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, \mathbb{U}_i, \mathbb{W}_i, f_i, \mathbb{Y}_i, h_i)$, $i \in [1; N]$, with the input–output structure given in (2.2)–(2.3). The *concrete* interconnected control system denoted by $\mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ is a tuple $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, f, \mathbb{Y}, h)$, where $\mathbb{X} = \prod_{i=1}^N \mathbb{X}_i$, $\mathbb{X}_0 = \prod_{i=1}^N \mathbb{X}_{0_i}$, $\mathbb{X}_s = \prod_{i=1}^N \mathbb{X}_{s_i}$, $\mathbb{U} = \prod_{i=1}^N \mathbb{U}_i$, $\mathbb{Y} = \prod_{i=1}^N \mathbb{Y}_{ii}$, $f(x, u) = \{[x'_1; \ldots; x'_N] | \ x'_i \in f_i(x_i, u_i, w_i), \forall i \in [1; N]\}$, $h(x) = [h_{11}(x_1); \ldots; h_{NN}(x_N)]$, subject to:

$$y_{ji} = w_{ij}, \ \mathbb{Y}_{ji} \subseteq \mathbb{W}_{ij}, \forall i \in [1; N], j \neq i. \tag{2.4}$$

An interconnected *finite* control system $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{\mathbb{U}}, \hat{f}, \hat{\mathbb{Y}}, \hat{h})$, denoted by $\hat{\Sigma} = \hat{\mathcal{I}}(\hat{\Sigma}_1, \ldots, \hat{\Sigma}_N)$, is composed of $N \in \mathbb{N}_{\geq 1}$ finite dt-CSs $\hat{\Sigma}_i$, subject to:

$$\forall \hat{y}_{ji}, \exists \hat{w}_{ij}, \ \text{s.t.} \ \|\hat{y}_{ji} - \hat{w}_{ij}\| \leq \phi_{ij}, i \in [1; N], j \neq i, \tag{2.5}$$

where ϕ_{ij} is an internal input quantization parameter designed for constructing local finite abstractions (cf. Section 5.1).

Remark 2.3. Note that in the above definition, the interconnection constraint in (2.4) for the concrete network is different from that for the abstract network in (2.5). For networks of finite abstractions, due to possibly different granularities of finite internal input sets $\hat{\mathbb{W}}_{ij}$ and output sets $\hat{\mathbb{Y}}_{ij}$, we introduce parameters ϕ_{ij} in (2.5) for having a well-posed interconnection.

2.2. Approximate opacity for interconnected dt-CSs

Before stating our main results, let us review the notions of approximate opacity proposed in Yin et al. (2021). The adopted notions of secrets are formulated as state-based. In this setting, it is assumed that there exists an intruder that can only observe the outputs of the systems. Using the observed output information, the intruder aims at inferring the secret states of the system. Opacity essentially determines whether or not any trace that reveals secrets of the system is indistinguishable from those, not revealing secrets, to an intruder. The three basic notions of opacity, i.e. approximate initial-state, current-state, and infinite-step opacity, introduced in Yin et al. (2021), are recalled next.

Definition 2.4. Consider an interconnected dt-CS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, f, \mathbb{Y}, h)$ and a constant $\delta \geq 0$. System Σ is

- δ-*approximate initial-state opaque* if for any $x_0 \in \mathbb{X}_0 \cap \mathbb{X}_s$ and finite state run $\{x_0, \ldots, x_n\}$, there exist $x'_0 \in \mathbb{X}_0 \setminus \mathbb{X}_s$ and a finite state run $\{x'_0, \ldots, x'_n\}$ s.t. $\max_{i\in[0;n]} \|h(x_i) - h(x'_i)\| \leq \delta$.
- δ-*approximate current-state opaque* if for any $x_0 \in \mathbb{X}_0$ and finite state run $\{x_0, \ldots, x_n\}$ s.t. $x_n \in \mathbb{X}_s$, there exist $x'_0 \in \mathbb{X}_0$ and a finite state run $\{x'_0, \ldots, x'_n\}$ s.t. $x'_n \in \mathbb{X} \setminus \mathbb{X}_s$ and $\max_{i\in[0;n]} \|h(x_i) - h(x'_i)\| \leq \delta$.
- δ-*approximate infinite-step opaque* if for any $x_0 \in \mathbb{X}_0$ and finite state run $\{x_0, \ldots, x_n\}$ s.t. $x_k \in \mathbb{X}_s$ for some $k \in [0; n]$, there exist $x'_0 \in \mathbb{X}_0$ and a finite state run $\{x'_0, \ldots, x'_n\}$ s.t. $x'_k \in \mathbb{X} \setminus \mathbb{X}_s$ and $\max_{i\in[0;n]} \|h(x_i) - h(x'_i)\| \leq \delta$.

Remark 2.5. Intuitively, the notions of approximate opacity provide a quantitative security guarantee that, if the intruder/observer does not have enough measurement precision, captured by the parameter δ, then the system's secret information cannot be revealed. We assume $X_0 \not\subseteq X_s$ throughout this work, otherwise opacity is trivially violated. Note that we are always interested in verifying opacity of the interconnected systems Σ as in Definition 2.2 rather than subsystems Σ_i introduced in Definition 2.1. The subsystems will be used later in the compositionality results to show opacity of interconnected systems.

3. Opacity-preserving simulation functions

In this section, we introduce new notions of approximate opacity-preserving simulation functions, which will provide us the basis for using abstraction-based technique in verifying approximate opacity for large-scale interconnected systems. First, we introduce a new notion of initial-state opacity-preserving simulation functions.

Definition 3.1. Consider interconnected dt-CSs $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, f, \mathbb{Y}, h)$ and $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{\mathbb{U}}, \hat{f}, \hat{\mathbb{Y}}, \hat{h})$ where $\hat{\mathbb{Y}} \subseteq \mathbb{Y}$. For $\varpi \in \mathbb{R}_{\geq 0}$, function $\tilde{V} : \mathbb{X} \times \hat{\mathbb{X}} \to \mathbb{R}_{\geq 0}$ is an ϖ-approximate initial-state opacity-preserving simulation function (ϖ-InitSOPSF) from Σ to $\hat{\Sigma}$, if there exists a function $\alpha \in \mathcal{K}_\infty$ s.t.

1 (a) $\forall x_0 \in \mathbb{X}_0 \cap \mathbb{X}_s, \exists \hat{x}_0 \in \hat{\mathbb{X}}_0 \cap \hat{\mathbb{X}}_s$, s.t. $\tilde{V}(x_0, \hat{x}_0) \leq \varpi$;
(b) $\forall \hat{x}_0 \in \hat{\mathbb{X}}_0 \setminus \hat{\mathbb{X}}_s, \exists x_0 \in \mathbb{X}_0 \setminus \mathbb{X}_s$, s.t. $\tilde{V}(x_0, \hat{x}_0) \leq \varpi$;
2 $\forall x \in \mathbb{X}, \forall \hat{x} \in \hat{\mathbb{X}}, \alpha(\|h(x) - \hat{h}(\hat{x})\|) \leq \tilde{V}(x, \hat{x})$;
3 $\forall x \in \mathbb{X}, \forall \hat{x} \in \hat{\mathbb{X}}$ s.t. $\tilde{V}(x, \hat{x}) \leq \varpi$, the following hold:

(a) $\forall u \in \mathbb{U}, \forall x_d \in f(x, u), \exists \hat{u} \in \hat{\mathbb{U}}, \exists \hat{x}_d \in \hat{f}(\hat{x}, \hat{u})$, s.t. $\tilde{V}(x_d, \hat{x}_d) \leq \varpi$;
(b) $\forall \hat{u} \in \hat{\mathbb{U}}, \forall \hat{x}_d \in \hat{f}(\hat{x}, \hat{u}), \exists u \in \mathbb{U}, \exists x_d \in f(x, u)$, s.t. $\tilde{V}(x_d, \hat{x}_d) \leq \varpi$.

It is worth noting that the ϖ-InitSOPSF characterizes the distance between two systems in terms of the satisfaction of approximate opacity. This relation considers not only the dynamic, but also the secrets of the system. The usefulness of Definition 3.1 in terms of preservation of approximate opacity across related systems will be shown later in Proposition 3.4.

Next, we introduce a new notion of current-state opacity-preserving simulation functions.

Definition 3.2. Consider interconnected dt-CSs $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, f, \mathbb{Y}, h)$ and $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{\mathbb{U}}, \hat{f}, \hat{\mathbb{Y}}, \hat{h})$ where $\hat{\mathbb{Y}} \subseteq \mathbb{Y}$. For $\varpi \in \mathbb{R}_{\geq 0}$, function $\tilde{V} : \mathbb{X} \times \hat{\mathbb{X}} \to \mathbb{R}_{\geq 0}$ is an ϖ-approximate current-state opacity-preserving simulation function (ϖ-CurSOPSF) from Σ to $\hat{\Sigma}$, if there exists a function $\alpha \in \mathcal{K}_\infty$ such that

1 $\forall x_0 \in \mathbb{X}_0, \exists \hat{x}_0 \in \hat{\mathbb{X}}_0$, s.t. $\tilde{V}(x_0, \hat{x}_0) \leq \varpi$;
2 $\forall x \in \mathbb{X}, \forall \hat{x} \in \hat{\mathbb{X}}, \alpha(\|h(x) - \hat{h}(\hat{x})\|) \leq \tilde{V}(x, \hat{x})$;
3 $\forall x \in \mathbb{X}, \forall \hat{x} \in \hat{\mathbb{X}}$ s.t. $\tilde{V}(x, \hat{x}) \leq \varpi$, the following hold:

(a) $\forall u \in \mathbb{U}, \forall x_d \in f(x, u), \exists \hat{u} \in \hat{\mathbb{U}}, \exists \hat{x}_d \in \hat{f}(\hat{x}, \hat{u})$, s.t. $\tilde{V}(x_d, \hat{x}_d) \leq \varpi$;
(b) $\forall u \in \mathbb{U}, \forall x_d \in f(x, u)$ s.t. $x_d \in \mathbb{X}_s, \exists \hat{u} \in \hat{\mathbb{U}}, \exists \hat{x}_d \in \hat{f}(\hat{x}, \hat{u})$ with $\hat{x}_d \in \hat{\mathbb{X}}_s$, s.t. $\tilde{V}(x_d, \hat{x}_d) \leq \varpi$;
(c) $\forall \hat{u} \in \hat{\mathbb{U}}, \forall \hat{x}_d \in \hat{f}(\hat{x}, \hat{u}), \exists u \in \mathbb{U}, \exists x_d \in f(x, u)$, s.t. $\tilde{V}(x_d, \hat{x}_d) \leq \varpi$;
(d) $\forall \hat{u} \in \hat{\mathbb{U}}, \forall \hat{x}_d \in \hat{f}(\hat{x}, \hat{u})$ s.t. $\hat{x}_d \in \hat{\mathbb{X}} \setminus \hat{\mathbb{X}}_s, \exists u \in \mathbb{U}, \exists x_d \in f(x, u)$ with $x_d \in \mathbb{X} \setminus \mathbb{X}_s$, s.t. $\tilde{V}(x_d, \hat{x}_d) \leq \varpi$.

Similarly, we introduce a new notion of infinite-step opacity-preserving simulation functions by combining the conditions of ϖ-InitSOPSF and ϖ-CurSOPSF.

Definition 3.3. Consider interconnected dt-CSs $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, f, \mathbb{Y}, h)$ and $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{\mathbb{U}}, \hat{f}, \hat{\mathbb{Y}}, \hat{h})$ where $\hat{\mathbb{Y}} \subseteq \mathbb{Y}$. For $\varpi \in \mathbb{R}_{\geq 0}$, function $\tilde{V} : \mathbb{X} \times \hat{\mathbb{X}} \to \mathbb{R}_{\geq 0}$ is an ϖ-approximate infinite-step opacity-preserving simulation function (ϖ-InfSOPSF) from Σ to $\hat{\Sigma}$, if it is both an ϖ-InitSOPSF and an ϖ-CurSOPSF from Σ to $\hat{\Sigma}$.

Note that if there exists an opacity-preserving simulation function from Σ to $\hat{\Sigma}$, and $\hat{\Sigma}$ is finite, $\hat{\Sigma}$ is called a finite abstraction of the concrete network Σ. Now we provide the main result of this section which shows the usefulness of above-defined opacity-preserving simulation functions in terms of preserving approximate opacity across related interconnected systems.

Proposition 3.4. *Consider two interconnected dt-CSs* $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, f, \mathbb{Y}, h)$ *and* $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{\mathbb{U}}, \hat{f}, \hat{\mathbb{Y}}, \hat{h})$*, where* $\hat{\mathbb{Y}} \subseteq \mathbb{Y}$*, and let* $\varepsilon, \delta \in \mathbb{R}_{\geq 0}$ *where* $\varepsilon \leq \frac{\delta}{2}$*. If* Σ *and* $\hat{\Sigma}$ *admit an opacity-preserving simulation function as in Definition 3.1 (resp. Definition 3.2 or Definition 3.3) associated with function* $\alpha \in \mathcal{K}_\infty$ *and constant* ϖ*, then the following implication holds*

$\hat{\Sigma}$ is $(\delta - 2\varepsilon)$-approximate opaque

$\Rightarrow \Sigma$ is δ-approximate opaque,

where $\varepsilon = \alpha^{-1}(\varpi)$.

This proposition can be proved by combining the results in Swikir and Zamani (2019, Proposition 2.4) and Yin et al. (2021, Theorem V.2). The proof is omitted here due to lack of space and can be found in Liu and Zamani (2020). Note that the above implication across two related systems holds for all of the three types of approximate opacity in Definition 2.4. This result provides us a sufficient condition for verifying approximate opacity using abstraction-based techniques.

4. Compositional construction of approximate opacity-preserving simulation functions

In the previous section, we proposed new notions of opacity-preserving simulation functions for interconnected systems using which one can check opacity using their finite abstractions. However, it is known that the construction of finite abstractions and the corresponding simulation functions for large-scale systems generally suffers from the curse of dimensionality. Motivated by this, we present here a compositional approach to establish local simulation functions for interconnected systems by composing those of the subsystems, defined below.

Definition 4.1. Consider subsystems $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, \mathbb{U}_i, \mathbb{W}_i, f_i, \mathbb{Y}_i, h_i)$ and $\hat{\Sigma}_i = (\hat{\mathbb{X}}_i, \hat{\mathbb{X}}_{0_i}, \hat{\mathbb{X}}_{s_i}, \hat{\mathbb{U}}_i, \hat{\mathbb{W}}_i, \hat{f}_i, \hat{\mathbb{Y}}_i, \hat{h}_i)$ where $\hat{\mathbb{W}}_i \subseteq \mathbb{W}_i$ and $\hat{\mathbb{Y}}_i \subseteq \mathbb{Y}_i$. For $\varpi_i \in \mathbb{R}_{\geq 0}$, function $V_i : \mathbb{X}_i \times \hat{\mathbb{X}}_i \to \mathbb{R}_{\geq 0}$ is called a local ϖ_i-InitSOPSF from Σ_i to $\hat{\Sigma}_i$, if there exist a constant $\vartheta_i \in \mathbb{R}_{\geq 0}$, and a function $\alpha_i \in \mathcal{K}_\infty$ such that

1 (a) $\forall x_0 \in \mathbb{X}_{0_i} \cap \mathbb{X}_{s_i}$, $\exists \hat{x}_{0_i} \in \hat{\mathbb{X}}_{0_i} \cap \hat{\mathbb{X}}_{s_i}$, s.t. $V_i(x_{0_i}, \hat{x}_{0_i}) \leq \varpi_i$;
(b) $\forall \hat{x}_0 \in \hat{\mathbb{X}}_{0_i} \setminus \hat{\mathbb{X}}_{s_i}$, $\exists x_{0_i} \in \mathbb{X}_{0_i} \setminus \mathbb{X}_{s_i}$, s.t. $V_i(x_{0_i}, \hat{x}_{0_i}) \leq \varpi_i$;
2 $\forall x_i \in \mathbb{X}_i$, $\forall \hat{x}_i \in \hat{\mathbb{X}}_i$, $\alpha_i(\|h_i(x_i) - \hat{h}_i(\hat{x}_i)\|) \leq V_i(x_i, \hat{x}_i)$;
3 $\forall x_i \in \mathbb{X}_i$, $\forall \hat{x}_i \in \hat{\mathbb{X}}_i$ s.t. $V_i(x_i, \hat{x}_i) \leq \varpi_i$, $\forall w_i \in \mathbb{W}_i$, $\forall \hat{w}_i \in \hat{\mathbb{W}}_i$ s.t. $\|w_i - \hat{w}_i\| \leq \vartheta_i$, the following hold:

(a) $\forall u_i \in \mathbb{U}_i$, $\forall x_{d_i} \in f_i(x_i, u_i, w_i)$, $\exists \hat{u}_i \in \hat{\mathbb{U}}_i$, $\exists \hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$, s.t. $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$;
(b) $\forall \hat{u}_i \in \hat{\mathbb{U}}_i$, $\forall \hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$, $\exists u_i \in \mathbb{U}_i$, $\exists x_{d_i} \in f_i(x_i, u_i, w_i)$, s.t. $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$.

Similarly, we introduce new notions of local ϖ_i-CurSOPSFs and local ϖ_i-InfSOPSFs for subsystems.

Definition 4.2. Consider subsystems $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, \mathbb{U}_i, \mathbb{W}_i, f_i, \mathbb{Y}_i, h_i)$ and $\hat{\Sigma}_i = (\hat{\mathbb{X}}_i, \hat{\mathbb{X}}_{0_i}, \hat{\mathbb{X}}_{s_i}, \hat{\mathbb{U}}_i, \hat{\mathbb{W}}_i, \hat{f}_i, \hat{\mathbb{Y}}_i, \hat{h}_i)$ where $\hat{\mathbb{W}}_i \subseteq \mathbb{W}_i$ and $\hat{\mathbb{Y}}_i \subseteq \mathbb{Y}_i$. For $\varpi_i \in \mathbb{R}_{\geq 0}$, function $V_i : \mathbb{X}_i \times \hat{\mathbb{X}}_i \to \mathbb{R}_{\geq 0}$ is called a local ϖ_i-CurSOPSF from Σ_i to $\hat{\Sigma}_i$, if there exist a constant $\vartheta_i \in \mathbb{R}_{\geq 0}$, and a function $\alpha_i \in \mathcal{K}_\infty$ such that

1 $\forall x_{0_i} \in \mathbb{X}_{0_i}$, $\exists \hat{x}_{0_i} \in \hat{\mathbb{X}}_{0_i}$, s.t. $V_i(x_{0_i}, \hat{x}_{0_i}) \leq \varpi_i$;
2 $\forall x_i \in \mathbb{X}_i$, $\forall \hat{x}_i \in \hat{\mathbb{X}}_i$, $\alpha_i(\|h_i(x_i) - \hat{h}_i(\hat{x}_i)\|) \leq V_i(x_i, \hat{x}_i)$;
3 $\forall x_i \in \mathbb{X}_i$, $\forall \hat{x}_i \in \hat{\mathbb{X}}_i$ s.t. $V_i(x_i, \hat{x}_i) \leq \varpi_i$, $\forall w_i \in \mathbb{W}_i$, $\forall \hat{w}_i \in \hat{\mathbb{W}}_i$ s.t. $\|w_i - \hat{w}_i\| \leq \vartheta_i$, the following hold:

(a) $\forall u_i \in \mathbb{U}_i$, $\forall x_{d_i} \in f_i(x_i, u_i, w_i)$, $\exists \hat{u}_i \in \hat{\mathbb{U}}_i$, $\exists \hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$, s.t. $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$;
(b) $\forall u_i \in \mathbb{U}_i$, $\forall x_{d_i} \in f_i(x_i, u_i, w_i)$ s.t. $x_{d_i} \in \mathbb{X}_{s_i}$, $\exists \hat{u}_i \in \hat{\mathbb{U}}_i$, $\exists \hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$ with $\hat{x}_{d_i} \in \hat{\mathbb{X}}_{s_i}$, s.t. $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$;
(c) $\forall \hat{u}_i \in \hat{\mathbb{U}}_i$, $\forall \hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$, $\exists u_i \in \mathbb{U}_i$, $\exists x_{d_i} \in f_i(x_i, u_i, w_i)$, s.t. $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$;
(d) $\forall \hat{u}_i \in \hat{\mathbb{U}}_i$, $\forall \hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$ s.t. $\hat{x}_{d_i} \in \hat{\mathbb{X}}_i \setminus \hat{\mathbb{X}}_{s_i}$, $\exists u_i \in \mathbb{U}_i$, $\exists x_{d_i} \in f_i(x_i, u_i, w_i)$ with $x_{d_i} \in \mathbb{X}_i \setminus \mathbb{X}_{s_i}$, s.t. $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$.

Definition 4.3. Consider subsystems $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, \mathbb{U}_i, \mathbb{W}_i, f_i, \mathbb{Y}_i, h_i)$ and $\hat{\Sigma}_i = (\hat{\mathbb{X}}_i, \hat{\mathbb{X}}_{0_i}, \hat{\mathbb{X}}_{s_i}, \hat{\mathbb{U}}_i, \hat{\mathbb{W}}_i, \hat{f}_i, \hat{\mathbb{Y}}_i, \hat{h}_i)$ where $\hat{\mathbb{W}}_i \subseteq \mathbb{W}_i$ and $\hat{\mathbb{Y}}_i \subseteq \mathbb{Y}_i$. For $\varpi_i \in \mathbb{R}_{\geq 0}$, a function $V_i : \mathbb{X}_i \times \hat{\mathbb{X}}_i \to \mathbb{R}_{\geq 0}$ is called a local ϖ_i-InfSOPSF from Σ_i to $\hat{\Sigma}_i$, if it is both a local ϖ_i-InitSOPSF and a local ϖ_i-CurSOPSF from Σ_i to $\hat{\Sigma}_i$.

If there exists a local opacity-preserving simulation function from Σ_i to $\hat{\Sigma}_i$, and $\hat{\Sigma}_i$ is finite, $\hat{\Sigma}_i$ is called a local finite abstraction of the concrete subsystem Σ_i. Note that the local simulation functions are mainly proposed for constructing overall simulation functions for networks and are not directly used for deducing the preservation of approximate opacity between subsystems. Next, we show how to compose the above-defined local opacity-preserving simulation functions so that they can be used to quantify the distance between two networks.

Theorem 4.4. *Consider an interconnected dt-CS* $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ *induced by* $N \in \mathbb{N}_{\geq 1}$ *subsystems* Σ_i*. Assume that each* Σ_i *and its abstraction* $\hat{\Sigma}_i$ *admit a local* ϖ_i*-InitSOPSF (resp.* ϖ_i*-CurSOPSF or* ϖ_i*-InfSOPSF)* V_i*. Let* $\varpi = \max_i \varpi_i$*. If*

$$\alpha_j^{-1}(\varpi_j) + \phi_{ij} \leq \vartheta_i, \forall i \in [1; N], \forall j \neq i, \tag{4.1}$$

where ϕ_{ij} *is an internal input quantization parameter for constructing the finite abstractions* $\hat{\Sigma}_i$*, then, function*

$$\tilde{V}(x, \hat{x}) := \max_i \{\frac{\varpi}{\varpi_i} V_i(x_i, \hat{x}_i)\}, \tag{4.2}$$

is an ϖ*-InitSOPSF (resp.* ϖ*-CurSOPSF or* ϖ*-InfSOPSF) from* Σ *to* $\hat{\Sigma} = \hat{\mathcal{I}}(\hat{\Sigma}_1, \ldots, \hat{\Sigma}_N)$.

Proof. First, we show that condition (1a) in Definition 3.1 holds. Consider any $x_0 = [x_{0_1}; \ldots; x_{0_N}] \in \mathbb{X}_0 \cap \mathbb{X}_s$. For any subsystem Σ_i and the corresponding abstraction $\hat{\Sigma}_i$, from the definition of local ϖ_i-InitSOPSF V_i, we have $\forall x_{0_i} \in \mathbb{X}_{0_i} \cap \mathbb{X}_{s_i}$, $\exists \hat{x}_{0_i} \in \hat{\mathbb{X}}_{0_i} \cap \hat{\mathbb{X}}_{s_i}$: $V_i(x_{0_i}, \hat{x}_{0_i}) \leq \varpi_i$. Then, from the definition of $\tilde{V}$ as in (4.2) we get $\tilde{V}(x_0, \hat{x}_0) \leq \varpi$, where $\hat{x}_0 = [\hat{x}_{0_1}; \ldots; \hat{x}_{0_N}] \in \hat{\mathbb{X}}_0 \cap \hat{\mathbb{X}}_s$. Thus, condition (1a) in Definition 3.1 holds. Condition (1b) can be proved in the same way thus is omitted here. Now, we show that condition 2 in Definition 3.1 holds for some $\mathcal{K}_\infty$ function α. Consider any $x = [x_1; \ldots; x_N] \in \mathbb{X}$ and $\hat{x} = [\hat{x}_1; \ldots; \hat{x}_N] \in \hat{\mathbb{X}}$. Then, using condition 2 in Definition 4.1, one gets $\|h(x) - \hat{h}(\hat{x})\| = \max_i\{\|h_{ii}(x_i) - \hat{h}_{ii}(\hat{x}_i)\|\} \leq \max_i\{\|h_i(x_i) - \hat{h}_i(\hat{x}_i)\|\} \leq \max_i\{\alpha_i^{-1}(V_i(x_i, \hat{x}_i))\} \leq \hat{\alpha}(\max_i\{\frac{\varpi}{\varpi_i} V_i(x_i, \hat{x}_i)\})$, where $\hat{\alpha}(s) = \max_i\{\alpha_i^{-1}(s)\}$, $\forall s \in \mathbb{R}_{\geq 0}$. By defining $\alpha = \hat{\alpha}^{-1}$, one obtains $\alpha(\|h(x) - \hat{h}(\hat{x})\|) \leq \tilde{V}(x, \hat{x})$, which satisfies condition 2.

Next, we show that condition 3 holds. Let us consider any $x = [x_1; \ldots; x_N] \in \mathbb{X}$ and $\hat{x} = [\hat{x}_1; \ldots; \hat{x}_N] \in \hat{\mathbb{X}}$ such that $\tilde{V}(x, \hat{x}) \leq \varpi$. It can be seen that from the construction of $\tilde{V}$ in (4.2), we get $V_i(x_i, \hat{x}_i) \leq \varpi_i$ holds, $\forall i \in [1; N]$. For each pair of subsystems Σ_i and $\hat{\Sigma}_i$, the internal inputs satisfy the chain of inequality: $\|w_i - \hat{w}_i\| = \max_{j \neq i}\{\|w_{ij} - \hat{w}_{ij}\|\} = \max_{j \neq i}\{\|y_{ji} - \hat{y}_{ji} + \hat{y}_{ji} - \hat{w}_{ij}\|\} \leq \max_{j \neq i}\{\|y_{ji} - \hat{y}_{ji}\| + \phi_{ij}\} \leq \max_{j \neq i}\{\|h_j(x_j) - \hat{h}_j(\hat{x}_j)\| + \phi_{ij}\} \leq \max_{j \neq i}\{\alpha_j^{-1}(V_j(x_j, \hat{x}_j)) + \phi_{ij}\} \leq \max_{j \neq i}\{\alpha_j^{-1}(\varpi_j) + \phi_{ij}\}$. Using (4.1), one has $\|w_i - \hat{w}_i\| \leq \vartheta_i$. Therefore, by Definition 4.1 for each pair of subsystems Σ_i and $\hat{\Sigma}_i$, one has $\forall u_i \in \mathbb{U}_i$ $\forall x_{d_i} \in f_i(x_i, u_i, w_i)$, there exist $\hat{u}_i \in \hat{\mathbb{U}}_i$ and $\hat{x}_{d_i} \in \hat{f}_i(\hat{x}_i, \hat{u}_i, \hat{w}_i)$ such that $V_i(x_{d_i}, \hat{x}_{d_i}) \leq \varpi_i$.

As a result, we get $\forall u = [u_1; \ldots; u_N] \in \mathbb{U}$, $\forall x_d \in f(x, u)$, there exist $\hat{u} = [\hat{u}_1; \ldots; \hat{u}_N] \in \hat{\mathbb{U}}$ and $\hat{x}_d \in \hat{f}(\hat{x}, \hat{u})$ such that $\tilde{V}(x_d, \hat{x}_d) := \max_i\{\frac{\varpi}{\varpi_i} V_i(x_{d_i}, \hat{x}_{d_i})\} \leq \varpi$. Therefore, condition (3a) in Definition 3.1 is satisfied with $\varpi = \max_i \varpi_i$. The proof of condition (3b) uses the same reasoning as that of (3a) and is omitted here. Therefore, we conclude that $\tilde{V}$ is an ϖ-InitSOPSF from Σ to $\hat{\Sigma}$. In a similar way, one can prove that $\tilde{V}$ is also an ϖ-CurSOPSF (resp. ϖ-InfSOPSF) from Σ to $\hat{\Sigma}$. □

In the sequel, we will impose conditions on the dynamics of the subsystems such that one can establish proper finite abstractions together with their corresponding local opacity-preserving simulation functions for all of the subsystems.

5. Construction of finite abstractions

In this section, we present a method to construct local finite abstractions, together with the corresponding local opacity-preserving simulation functions for the concrete subsystems satisfying certain stability property. We consider each subsystem $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, \mathbb{U}_i, \mathbb{W}_i, f_i, \mathbb{Y}_i, h_i)$ as an infinite, deterministic dt-CS with $\mathbb{X}_{0_i} = \mathbb{X}_i$. We assume the output map h_i of Σ_i satisfies the following general Lipschitz assumption $\|h_i(x_i) - h(x_i')\| \leq \ell(\|x_i - x_i'\|)$, for all $x_i, x_i' \in \mathbb{X}_i$, where $\ell \in \mathcal{K}_\infty$.

5.1. Construction of local finite abstractions

Note that throughout this subsection, we will work on subsystems rather than the overall network. However, we omit index i of subsystems throughout the text for the sake of better readability, e.g., we write Σ instead of Σ_i. The opacity-preserving simulation functions between Σ and its local finite abstraction is established under the assumption that Σ is incrementally input-to-state stable (δ-ISS) (Angeli, 2002) as defined next.

Definition 5.1. System $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, \mathbb{W}, f, \mathbb{Y}, h)$ is δ-ISS if there exist functions $\mathcal{G} : \mathbb{X} \times \mathbb{X} \to \mathbb{R}_{\geq 0}$, $\underline{\alpha}, \overline{\alpha}, \kappa, \rho_{int}, \rho_{ext} \in \mathcal{K}_\infty$, such that $\forall x, x' \in \mathbb{X}$, $\forall u, u' \in \mathbb{U}$, $\forall w, w' \in \mathbb{W}$,

$$\underline{\alpha}(\|x - x'\|) \leq \mathcal{G}(x, x') \leq \overline{\alpha}(\|x - x'\|), \tag{5.1}$$

$$\mathcal{G}(f(x, u, w), f(x', u', w')) - \mathcal{G}(x, x') \leq -\kappa(\mathcal{G}(x, x')) + \rho_{int}(\|w - w'\|) + \rho_{ext}(\|u - u'\|). \tag{5.2}$$

We additionally assume that there exists a function $\hat{\gamma} \in \mathcal{K}_\infty$ such that $\forall x, x', x'' \in \mathbb{X}$,

$$\mathcal{G}(x, x') \leq \mathcal{G}(x, x'') + \hat{\gamma}(\|x' - x''\|), \tag{5.3}$$

for $\mathcal{G}$ defined in Definition 5.1. Note that in most real applications, the state set $\mathbb{X}$ is a compact subset of $\mathbb{R}^n$ and, hence, condition (5.3) is not restrictive.

Now, we construct a local finite abstraction of a δ-ISS dt-CS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, \mathbb{W}, f, \mathbb{Y}, h)$. For the remainder of the paper, we assume that sets $\mathbb{X}$, $\mathbb{X}_s$, $\mathbb{W}$, and $\mathbb{U}$ are of the form of finite unions of boxes. Consider a tuple $q = (\eta, \theta, \mu, \phi)$ of parameters, where $0 \leq \eta \leq \min\{span(\mathbb{X}_s), span(\mathbb{X} \setminus \mathbb{X}_s)\}$ is the state set quantization, $0 \leq \mu < span(\mathbb{U})$ is the external input set quantization, ϕ is the internal input set quantization parameter, where $0 \leq \|\phi\| \leq span(\mathbb{W})$, and $\theta \in \mathbb{R}_{\geq 0}$ is a design parameter. A local finite abstraction can be represented as the tuple $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{\mathbb{U}}, \hat{\mathbb{W}}, \hat{f}, \hat{\mathbb{Y}}, \hat{h})$, where $\hat{\mathbb{X}} = \hat{\mathbb{X}}_0 = [\mathbb{X}]_\eta$, $\hat{\mathbb{X}}_s = [\mathbb{X}_s^\theta]_\eta$, $\hat{\mathbb{U}} = [\mathbb{U}]_\mu$, $\hat{\mathbb{W}} = [\mathbb{W}]_\phi$, $\hat{\mathbb{Y}} = \{h(\hat{x}) | \hat{x} \in \hat{\mathbb{X}}\}$, $\hat{h}(\hat{x}) = h(\hat{x})$, $\forall \hat{x} \in \hat{\mathbb{X}}$, and $\hat{x}_d \in \hat{f}(\hat{x}, \hat{u}, \hat{w})$ if and only if $\|\hat{x}_d - f(\hat{x}, \hat{u}, \hat{w})\| \leq \eta$, where $\mathbb{X}_s^\theta = \{x \in \mathbb{X} \mid \exists \bar{x} \in \mathbb{X}_s, \|x - \bar{x}\| \leq \theta\}$ denotes the θ-expansion of $\mathbb{X}_s$.

Next, we show that if the abstraction $\hat{\Sigma}$ of a δ-ISS Σ is constructed with the tuple of parameters satisfying some conditions, then function $\mathcal{G}$ in Definition 5.1 is a local InitSOPSF (resp. CurSOPSF or InfSOPSF) from Σ to $\hat{\Sigma}$.

Theorem 5.2. *Consider a δ-ISS dt-CS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, \mathbb{W}, f, \mathbb{Y}, h)$ as in Definition 5.1 with function $\mathcal{G}$ satisfying (5.1)–(5.3) with $\mathcal{K}_\infty$ functions $\underline{\alpha}, \overline{\alpha}, \kappa, \rho_{int}, \rho_{ext}, \hat{\gamma}$. For any design parameters $\varpi, \vartheta \in \mathbb{R}_{\geq 0}$, let $\hat{\Sigma}$ be a finite abstraction of Σ with a tuple $q = (\eta, 0, \mu, \phi)$ of parameters satisfying*

$$\eta \leq \min\{\hat{\gamma}^{-1}[\kappa(\varpi) - \rho_{int}(\vartheta) - \rho_{ext}(\mu)], \overline{\alpha}^{-1}(\varpi)\}. \tag{5.4}$$

Then, $\mathcal{G}$ is a local ϖ-InitSOPSF from Σ to $\hat{\Sigma}$ and from $\hat{\Sigma}$ to Σ.

The proof of this theorem is omitted here due to lack of space and can be found in the preprint (Liu & Zamani, 2020). Next, we provide a similar result as in Theorem 5.2, but tailored to current-state and infinite-step opacity.

Theorem 5.3. *Consider a δ-ISS dt-CS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, \mathbb{U}, \mathbb{W}, f, \mathbb{Y}, h)$ as in Definition 5.1 with function $\mathcal{G}$ satisfying (5.1)–(5.3) with $\mathcal{K}_\infty$ functions $\underline{\alpha}, \overline{\alpha}, \kappa, \rho_{int}, \rho_{ext}, \hat{\gamma}$. For any design parameters $\varpi, \vartheta \in \mathbb{R}_{\geq 0}$, let $\hat{\Sigma}$ be a finite abstraction of Σ with a tuple $q = (\eta, \theta, \mu, \phi)$ of parameters satisfying*

$$\eta \leq \min\{\hat{\gamma}^{-1}[\kappa(\varpi) - \rho_{int}(\vartheta) - \rho_{ext}(\mu)], \overline{\alpha}^{-1}(\varpi)\}; \tag{5.5}$$

$$\underline{\alpha}^{-1}(\varpi) \leq \theta. \tag{5.6}$$

Then, $\mathcal{G}$ is a local ϖ-CurSOPSF (resp. InfSOPSF) from Σ to $\hat{\Sigma}$.

Remark 5.4. Note that the proposed local simulation functions provide one-sided relations since condition 1 in Definition 4.1 (or 4.2) is not symmetric. On the other hand, the two-sided (symmetric) decay condition 3 in Definition 4.1 (or 4.2) is similar to the *approximate bisimulation relation* proposed in Girard and Pappas (2007). We refer interested readers to Zhang et al. (2019, Examples 3.5 and 3.6), where the two-sided conditions are shown to be necessary to ensure the preservation of opacity. Therefore, in order to find suitable local opacity-preserving simulation functions, the δ-ISS assumption is still required for the subsystems. Notice that under the δ-ISS assumption, we showed that concrete system and its abstraction simulates each other in terms of preserving initial-state opacity (cf. Theorem 5.2). However, in the case of CurSOPSF and InfSOPSF, having δ-ISS property only ensures that the abstract system simulates the concrete one and not the other direction (cf. Theorem 5.3).

One can observe that in order to satisfy conditions (4.1) and (5.4) (resp. (5.5)) simultaneously, the interconnected system must hold some property. In the next subsection, we will discuss about the inherent property that the interconnected system should hold such that one can design suitable quantization parameters to satisfy these competing conditions at the same time.

5.2. Compositionality result

In this subsection, we exploit the interconnection topology of the overall network and employ the knowledge from graph theory as an essential tool in our main result. Here, we first introduce some terminologies that will be used later based on the notion of strongly connected components (SCCs) (Baier & Katoen, 2008), which are used to represent sub-networks of an interconnected system.

Consider an interconnected dt-CS $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ δ-ISS subsystems Σ_i. We denote by $G = (I, E)$ the directed graph associated with Σ, where $I = [1; N]$ is the set of vertices with each vertex $i \in I$ labeled with subsystem Σ_i, and $E \subseteq I \times I$ is the set of ordered pairs (i, j), $\forall i, j \in I$, with $y_{ji} \neq 0$. The SCCs of G are denoted by $\bar{G}_k = (I_k, E_k)$, $k \in [1; \bar{N}]$, where $\bar{N}$ is the number of SCCs in G. For any $\bar{G}_k$, we set $I_k = \{k_1, \ldots, k_{\bar{N}_k}\}$ and $\bar{N}_k = \text{card}(I_k)$. We denote by $\mathcal{N}_I(i) = \{j \in I | \exists (i, j) \in E\}$ and $\mathcal{M}_I(i) = \{j \in I | \exists (j, i) \in E\}$ the set of vertices in I which are

Algorithm 1: Compositional design of local parameters $\varpi_i \in \mathbb{R}_{>0}$ and $\vartheta_i \in \mathbb{R}_{>0}$, $\forall i \in [1; N]$

Input: The desired precision $\varpi \in \mathbb{R}_{>0}$; the directed graph G composed of SCCs $\bar{G}_k$ and functions σ_{k_i} $\forall i \in I_k$ satisfying (5.9) for $\bar{G}_k$, $\forall k \in [1; \bar{N}]$; the functions $\mathcal{G}_i$ equipped with functions κ_i, α_i, and ρ_{inti}, $\forall i \in [1; N]$.

Output: $\varpi_i \in \mathbb{R}_{>0}$ and $\vartheta_i \in \mathbb{R}_{>0}$, $\forall i \in [1; N]$.

1 Set $\varpi_i := \infty$, $\vartheta_i := \infty$, $\forall i \in [1; N]$, $\forall k \in [1; \bar{N}]$, $G^* = G$

2 **while** $G^* \neq \varnothing$ **do**

3 **foreach** $\bar{G}_k \in \text{BSCC}(G^*)$ **do**

4 **if** $G^* = G$ **then**

5 **if** $\bar{N}_k > 1$ **then** choose $r \in \mathbb{R}_{>0}$ s.t. $\max_{i\in I_k}\{\sigma_i(r)\} = \varpi$; set $\varpi_i = \sigma_i(r)$, choose ϕ_{ij} s.t. $\max_{j\in\mathcal{N}_{I_k}(i)}\{\phi_{ij}\} < \rho_{inti}^{-1} \circ \kappa_i(\varpi_i) - \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j)\}$, $\forall i, j \in I_k$, set $\vartheta_i = \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j) + \phi_{ij}\}$, $\forall i \in I_k$, and choose $\phi_{ij} < \vartheta_i$, $\forall i \in I_k$, $\forall j \in \mathcal{N}_{I\setminus I_k}(i)$;

6 **else** set $\varpi_i = \varpi$, choose $\vartheta_i \in \mathbb{R}_{>0}$ s.t. $\vartheta_i < \rho_{inti}^{-1} \circ \kappa_i(\varpi_i)$, $i \in I_k$; choose $\phi_{ij} < \vartheta_i$, $\forall i \in I_k$, $\forall j \in \mathcal{N}_{I\setminus I_k}(i)$;

7 **else**

8 **if** $\bar{N}_k > 1$ **then** choose $r \in \mathbb{R}_{>0}$ s.t. $\sigma_i(r) \leq \alpha_i(\min_{j\in\mathcal{M}_{I\setminus I_k}(i)}\{\vartheta_j - \phi_{ji}\})$, $\forall i \in I_k$ with $\mathcal{M}_{I\setminus I_k}(i) \neq \varnothing$; set $\varpi_i = \sigma_i(r)$, choose ϕ_{ij} s.t. $\max_{j\in\mathcal{N}_{I_k}(i)}\{\phi_{ij}\} < \rho_{inti}^{-1} \circ \kappa_i(\varpi_i) - \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j)\}$, $\forall i, j \in I_k$, set $\vartheta_i = \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j) + \phi_{ij}\}$, $\forall i \in I_k$, and choose $\phi_{ij} < \vartheta_i$, $\forall i \in I_k$, $\forall j \in \mathcal{N}_{I\setminus I_k}(i)$;

9 **else** set $\varpi_i \leq \alpha_i(\min_{j\in\mathcal{M}_{I\setminus I_k}(i)}\{\vartheta_j - \phi_{ji}\})$, choose $\vartheta_i \in \mathbb{R}_{>0}$ s.t. $\vartheta_i < \rho_{inti}^{-1} \circ \kappa_i(\varpi_i)$, $i \in I_k$; choose $\phi_{ij} < \vartheta_i$, $\forall i \in I_k$, $\forall j \in \mathcal{N}_{I\setminus I_k}(i)$;

10 $G^* = G^* \setminus \text{BSCC}(G^*)$;

direct predecessors of i and direct successors of i, respectively. We denote by BSCC(G) the collection of bottom SCCs of G from which no vertex in G outside $\bar{G}_k$ is reachable.

Now, we raise the following small-gain type assumption which is essential for the main compositionality result.

Assumption 5.5. Consider an interconnected dt-CS $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$ induced by $N \in \mathbb{N}_{\geq 1}$ δ-ISS subsystems Σ_i which is associated with a directed graph G. Assume that each Σ_i and its abstraction $\hat{\Sigma}_i$ admit a local ϖ_i-InitSOPSF (resp. CurSOPSF or InfSOPSF) $\mathcal{G}_i$, together with functions κ_i, α_i, and ρ_{inti} as appeared in Definition 4.1 (resp. Definition 4.2 or Definition 4.3) and Definition 5.1. For every SCC $\bar{G}_k$ in G, we define

$$\gamma_{ij} = \begin{cases} \kappa_i^{-1} \circ \rho_{inti} \circ \alpha_j^{-1} & \text{if } j \in \mathcal{N}_{I_k}(i), \\ 0 & \text{otherwise}, \end{cases} \tag{5.7}$$

where $\mathcal{N}_{I_k}(i) = \{j \in I_k | \exists (i, j) \in E\}$, $\forall i, j \in I_k$. We assume that for every $\bar{G}_k$, $k \in [1; \bar{N}]$, the following holds

$$\gamma_{i_1 i_2} \circ \gamma_{i_2 i_3} \circ \cdots \circ \gamma_{i_{r-1} i_r} \circ \gamma_{i_r i_1} < \mathcal{I}_d, \tag{5.8}$$

$\forall (i_1, \ldots, i_r) \in \{k_1, \ldots, k_{\bar{N}_k}\}^r$, where $r \in \{1, \ldots, \bar{N}_k\}$.

Now, we provide the next main result showing that under the above assumption, one can always compositionally design local quantization parameters such that conditions (4.1) and (5.4) (resp. (5.5)) are fulfilled simultaneously.

Theorem 5.6. *Suppose that Assumption 5.5 holds. Then, for any desired precision $\varpi \in \mathbb{R}_{>0}$ as in Definition 3.1 (resp. Definition 3.2 or 3.3), there always exist quantization parameters η_i, μ_i, ϕ_i, $\forall i \in [1; N]$, such that (4.1) and (5.4) (resp. (5.5)) are satisfied simultaneously, where the local parameters $\vartheta_i \in \mathbb{R}_{>0}$ and $\varpi_i \in \mathbb{R}_{>0}$, $\forall i \in [1; N]$, are obtained from Algorithm 1.*

Proof. First, let us note that the small-gain type condition (5.8) implies that for each $\bar{G}_k$, there exists $\sigma_i \in \mathcal{K}_\infty$ satisfying, $\forall i \in I_k$,

$$\max_{j\in\mathcal{N}_{I_k}(i)}\{\gamma_{ij} \circ \sigma_j\} < \sigma_i; \tag{5.9}$$

see Dashkovskiy, Rüffer, and Wirth (2010, Theorem 5.2). Now, given a desired precision ϖ, we apply Algorithm 1 to design the pair of parameters (ϖ_i, ϑ_i) for all of the subsystems. In order to show that the algorithm guarantees the simultaneous satisfaction of conditions (4.1) and (5.4) (resp. (5.5)), let us consider different scenarios of the SCCs. First, we consider the SCCs which are composed of only 1 subsystem, i.e. $\bar{N}_k = 1$. From lines 6 and 9, one observes that the selections of ϖ_i and ϑ_i for each subsystem immediately ensure that $\kappa_i(\varpi_i) - \rho_{inti}(\vartheta_i) > 0$, which implies that there always exist quantization parameters η_i, μ_i to satisfy (5.4) (resp. (5.5)). Next, let us consider the SCCs with more than 1 subsystems, i.e. $\bar{N}_k > 1$. Suppose that for each $\bar{G}_k$, we are given functions $\sigma_i \in \mathcal{K}_\infty$, $\forall i \in I_k$ satisfying (5.9). From (5.7) and (5.9), we have

$$\begin{aligned} &\max_{j\in\mathcal{N}_{I_k}(i)}\{\gamma_{ij} \circ \sigma_j\} < \sigma_i \Longrightarrow \max_{j\in\mathcal{N}_{I_k}(i)}\{\kappa_i^{-1} \circ \rho_{inti} \circ \alpha_j^{-1} \circ \sigma_j\} < \sigma_i \\ &\Longrightarrow \rho_{inti} \circ \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1} \circ \sigma_j\} < \kappa_i \circ \sigma_i, \end{aligned} \tag{5.10}$$

which holds for each $i \in I_k$. Now, let us set $\varpi_i = \sigma_i(r)$, $\forall i \in I_k$, where r is chosen under the criteria in lines 5 and 8, and choose the internal input quantization parameters ϕ_{ij} such that $\forall i, j \in I_k$

$$\max_{j\in\mathcal{N}_{I_k}(i)}\{\phi_{ij}\} < \rho_{inti}^{-1} \circ \kappa_i(\varpi_i) - \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j)\}. \tag{5.11}$$

By setting $\vartheta_i = \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j) + \phi_{ij}\}$ and combining (5.11) with (5.10), one has, $\rho_{inti}(\vartheta_i) = \rho_{inti}(\max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j) + \phi_{ij}\}) \leq \rho_{inti}(\max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j)\} + \max_{j\in\mathcal{N}_{I_k}(i)}\{\phi_{ij}\}) < \kappa_i(\varpi_i)$, which again implies that one can always find suitable local parameters η_i, μ_i to satisfy (5.4) (resp. (5.5)). Additionally, the selection of $\vartheta_i = \max_{j\in\mathcal{N}_{I_k}(i)}\{\alpha_j^{-1}(\varpi_j) + \phi_{ij}\}$ as in lines 5 and 8, together with the design procedure for ϖ_i and ϕ_{ij} ensure that (4.1) is satisfied as well, which concludes the proof. □

Notice that the design procedure in Algorithm 1 follows the hierarchy of the acyclic directed graph which is composed of SCCs as vertices. Since the interconnected system considered in this paper is composed of finite number of SCCs, Algorithm 1 terminates in finite iterations.

Remark 5.7. Note that small-gain type conditions have been leveraged in Mallik et al. (2018), Pola et al. (2016), Swikir and Zamani (2019) and Tazaki and Imura (2008) to facilitate the compositional construction of finite abstractions. The results in Mallik et al. (2018), Pola et al. (2016) and Tazaki and Imura (2008) rely on classic sum-type small-gain conditions which require almost linear growth on gains of subsystems. In contrast, our compositionality result here are based on max-type small-gain

conditions formulated in a general nonlinear form, which can potentially lead to much smaller approximation errors of finite abstractions; see Swikir and Zamani (2019, Remark 3.6) for some discussions on this point. It should be noted that if the small-gain type condition (5.8) is satisfied by every SCC in the network, then this condition holds for the overall network as well. However, by involving the notion of SCCs in the parameter design procedure, we are allowed to check the small-gain condition and design local parameters inside each SCC only, instead of the entire network. Moreover, by exploiting the interconnection topology, the proposed result presents a *top-down* compositional design framework. That is, as long as Assumption 5.5 holds, given any desired precision $\varpi \in \mathbb{R}_{>0}$, Algorithm 1 always provides us with suitable local quantization parameters to achieve the overall abstraction accuracy. Note that such a systematic compositional scheme cannot be achieved by the results in Swikir and Zamani (2019).

6. An illustrative example

Consider a concrete interconnected discrete-time linear system Σ as in Definition 2.2, consisting of $n \in \mathbb{N}_{\geq 1}$ subsystems Σ_i, each described by:

$$\Sigma_i : \begin{cases} \mathbf{x}_i(k+1) &= a_i\mathbf{x}_i(k) + \nu_i(k) + d_i\omega_i(k), \\ \mathbf{y}_i(k) &= c_i\mathbf{x}_i(k), \end{cases}$$

where $a_i = 0.1$, $d_i = 0.05$, $c_i = [c_{i1}; \ldots; c_{in}]$ with $c_{i(i+1)} = 1$, $c_{ij} = 0, \forall i \in [1; n-1], \forall j \neq i+1$, $c_{nn} = 1$, $c_{nj} = 0, \forall j \in [1; n-1]$, $\nu_i(k) = 0.145$, $\omega_1(k) = 0$, and $\omega_i(k) = \mathbf{y}_{(i-1)i}(k)$, $\forall i \in [2; n]$. For each subsystem, the state set is $\mathbb{X}_i = \mathbb{X}_{0_i} =]0\ 0.6[$, the input set is $\mathbb{U}_i = \{0.145\}$, the secret set is $\mathbb{X}_{s_1} =]0\ 0.2]$, $\mathbb{X}_{s_2} = [0.4\ 0.6[$, $\mathbb{X}_{s_i} =]0\ 0.6[$, $\forall i \in [3; n]$, the output set is $\mathbb{Y}_i = \prod_{j=1}^{n} \mathbb{Y}_{ij}$ where $\mathbb{Y}_{i(i+1)} =]0\ 0.6[$, $\mathbb{Y}_{ij} = 0, \forall i \in [1; n-1], \forall j \neq i+1$, $\mathbb{Y}_{nn} =]0\ 0.6[$, $\mathbb{Y}_{nj} = 0$, $\forall j \in [1; n-1]$, and the internal input set is $\mathbb{W}_i = \prod_{j=1, j\neq i}^{n} \mathbb{Y}_{ji}$. Intuitively, the output of the overall system is the external output of the last subsystem Σ_n. The main goal of this example is to verify approximate initial-state opacity of the concrete network using its finite abstraction. Now, let us construct compositionally a finite abstraction of Σ that preserves initial-state opacity, with desired accuracy $\varepsilon = 0.25$ in Proposition 3.4. We apply our main results of previous sections to achieve this goal. Consider functions $V_i = |x_i - x_i'|$, $\forall i \in [1; n]$. It can be readily verified that V_i are δ-ISS Lyapunov functions for subsystems Σ_i satisfying (5.1) and (5.2) in Definition 5.1, with $\kappa_i(s) = (1-a_i)s = 0.9s$, $\rho_{exti}(s) = \hat{\gamma}_i(s) = \underline{\alpha}_i(s) = \overline{\alpha}_i(s) = s$, and $\rho_{inti}(s) = 0.05s$. It can be seen that the system is made up of n identical subsystems in a cascade interconnection, thus, the resulting directed graph $G = (I, E)$ is specified by $I = [1; n]$, $E = \{(1, 2), (2, 3), (3, 4), \ldots, (n-1, n)\}$. Note that each subsystem is a strongly connected component of G and the small-gain condition (5.8) is satisfied readily. Then, by applying Algorithm 1 and choosing functions $\sigma_i = \mathcal{I}_d$, $\forall i \in [1; n]$, we obtain proper pairs of local parameters $(\varpi_i, \vartheta_i) = (0.25, 0.25)$ for all of the subsystems. Then, a suitable tuple $q_i = (\eta_i, \mu_i, \theta_i, \phi_i) = (0.2, 0, 0, 0)$ of quantization parameters is chosen such that inequality (5.4) for each subsystem Σ_i is satisfied. Next, we construct local abstractions $\hat{\Sigma}_i = (\hat{\mathbb{X}}_i, \hat{\mathbb{X}}_{0_i}, \hat{\mathbb{X}}_{s_i}, \hat{\mathbb{U}}_i, \hat{\mathbb{W}}_i, \hat{f}_i, \hat{\mathbb{Y}}_i, \hat{h}_i)$ for subsystems as in Section 5.1, where $\hat{\mathbb{X}}_i = \hat{\mathbb{X}}_{0_i} = \{0.2, 0.4\}$, $\hat{\mathbb{X}}_{s_1} = \{0.2\}$, $\hat{\mathbb{X}}_{s_2} = \{0.4\}$, $\hat{\mathbb{X}}_{s_i} = \{0.2, 0.4\}$, $\forall i \in [3; n]$, $\hat{\mathbb{Y}}_i = \prod_{j=1}^{i}\{0\} \times \{0.2, 0.4\} \times \prod_{j=i+2}^{n}\{0\}$, $\forall i \in [1; n-1]$, $\hat{\mathbb{Y}}_n = \prod_{j=1}^{n-1}\{0\} \times \{0.2, 0.4\}$, $\hat{W}_i = \{0.2, 0.4\}$, $\forall i \in [1; n]$. Using the result in Theorem 5.2, one can verify that $V_i = |x_i - x_i'|$ is a local ϖ_i-InitSOPSF from each Σ_i to its abstraction $\hat{\Sigma}_i$. Furthermore, by the compositionality result in Theorem 4.4, we obtain that $\hat{V} = \max_i\{V_i(x_i, \hat{x}_i)\} = \max_i\{|x_i - x_i'|\}$ is an ϖ-InitSOPSF from $\Sigma = \mathcal{I}(\Sigma_1, \ldots, \Sigma_n)$ to $\hat{\Sigma} = \hat{\mathcal{I}}(\hat{\Sigma}_1, \ldots, \hat{\Sigma}_n)$ satisfying the conditions in Definition 3.1 with $\varpi = \max_i \varpi_i = 0.25$.

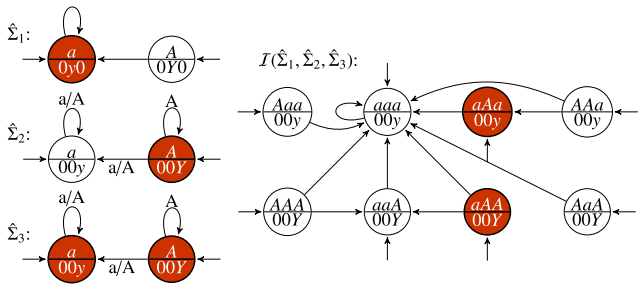

Fig. 1. Compositional abstraction of an interconnected discrete-time linear system consisting of 3 subsystems. Each circle is labeled by the state (top half) and the corresponding output (bottom half). Initial states are distinguished by being the target of a sourceless arrow. Secret states are marked in red. The symbols on the edges show the internal inputs coming from other subsystems. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Now, let us verify approximate initial-state opacity for Σ using the interconnected abstraction $\hat{\Sigma}$. An example of a network consisting of 3 subsystems is shown in Fig. 1. The three smaller automata in the left represent the symbolic subsystems and the one in the right represents the interconnected abstraction for the whole network. For simplicity of demonstration, we use symbols to represent the state and output vectors, where the states and outputs of local transition systems are denoted by $a = [0.2]$, $A = [0.4]$, $y = 0.2$ and $Y = 0.4$, respectively. The symbols such as $aaa = [0.2; 0.2; 0.2]$ and $00y = [0; 0; 0.2]$ represent the concatenated state and output vectors for the interconnected abstraction, respectively. As seen in Fig. 1, for any run starting from any secret state, i.e., *aAa* and *aAA*, there exists a run from a non-secret state, i.e., *Aaa* and *AAA*, such that the output trajectories are exactly the same. Due to lack of space, we do not plot the automata for the case of $n = 4$, but we verified that the network is still 0-approximate initial-state opaque. We expect that the network holds this property regardless of the number of subsystems due to the homogeneity of subsystems and the structure of the network topology. Thus, one can conclude that $\hat{\mathcal{I}}(\hat{\Sigma}_1, \ldots, \hat{\Sigma}_n)$ is 0-approximate initial-state opaque. Therefore, by Proposition 3.4, we obtain that the concrete network $\mathcal{I}(\Sigma_1, \ldots, \Sigma_n)$ is 0.5-approximate initial-state opaque.

7. Conclusion

In this paper, we proposed a methodology to compositionally construct opacity-preserving finite abstractions of interconnected discrete-time control systems. New notions of so-called opacity-preserving simulation functions are introduced to characterize the relations between two systems in terms of preservation of opacity. By leveraging these simulation functions, we first constructed local abstractions of the subsystems. Then, a finite abstraction of the network can be obtained by interconnecting the local finite abstractions while retaining the opacity property. Finally, we presented an illustrative example to show the effectiveness of our main results in verifying opacity of interconnected systems. Note that in this paper, the local finite abstractions are constructed based on δ-ISS assumptions on subsystems. Due to the strong decay conditions appeared in the notions of opacity-preserving simulation functions, although conservative, this assumption is indeed required to ensure the existence of opacity-preserving finite abstractions for general nonlinear systems (cf. Remark 5.4). For future works, in the spirit of Tabuada (2004), one potential direction to relax the stability assumption is to utilize *flatness* properties of nonlinear systems for the construction of opacity-preserving finite abstractions.

References

Angeli, D. (2002). A Lyapunov approach to incremental stability properties. *IEEE Transactions on Automatic Control*, *47*(3), 410–421.

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers and Security*, *68*, 81–97.

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

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

Girard, A., & Pappas, G. J. (2007). Approximation metrics for discrete and continuous systems. *IEEE Transactions on Automatic Control*, *52*(5), 782–798.

Jacob, R., Lesage, J., & Faure, J. (2016). Overview of discrete event systems opacity: Models, validation, and quantification. *Annual Reviews in Control*, *41*, 135–146.

Kim, E. S., Arcak, M., & Zamani, M. (2018). Constructing control system abstractions from modular components. In *21st international conference on hybrid systems: Computation and control* (pp. 137–146).

Lafortune, S., Lin, F., & Hadjicostis, C. N. (2018). On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control*, *45*, 257–266.

Lin, F. (2011). Opacity of discrete event systems and its applications. *Automatica*, *47*(3), 496–503.

Liu, S., Yin, X., & Zamani, M. (2020). On a notion of approximate opacity for discrete-time stochastic control systems. In *American control conference* (pp. 5413–5418).

Liu, S., & Zamani, M. (2020). Compositional synthesis of opacity-preserving finite abstractions for interconnected systems. arXiv:2004.00131.

Mallik, K., Schmuck, A., Soudjani, S., & Majumdar, R. (2018). Compositional synthesis of finite-state abstractions. *IEEE Transactions on Automatic Control*, *64*(6), 2629–2636.

Mazaré, L. (2004). Using unification for opacity properties. In *4th workshop on issues in the theory of security, Vol. 7* (pp. 165–176).

Pola, G., Pepe, P., & Di Benedetto, M. (2016). Symbolic models for networks of control systems. *IEEE Transactions on Automatic Control*, *61*(11), 3663–3668.

Ramasubramanian, B., Cleaveland, W. R., & Marcus, S. (2020). Notions of centralized and decentralized opacity in linear systems. *IEEE Transactions on Automatic Control*, *65*(4), 1442–1455.

Saboori, A., & Hadjicostis, C. N. (2007). Notions of security and opacity in discrete event systems. In *46th IEEE conf. on decision and control* (pp. 5056–5061).

Saboori, A., & Hadjicostis, C. N. (2011). Verification of K-step opacity and analysis of its complexity. *IEEE Transactions on Automation Science and Engineering*, *8*(3), 549–559.

Saboori, A., & Hadjicostis, C. N. (2012). Verification of infinite-step opacity and complexity considerations. *IEEE Transactions on Automatic Control*, *57*(5), 1265–1269.

Saboori, A., & Hadjicostis, C. N. (2013a). Current-state opacity formulations in probabilistic finite automata. *IEEE Transactions on Automatic Control*, *59*(1), 120–133.

Saboori, A., & Hadjicostis, C. N. (2013b). Verification of initial-state opacity in security applications of discrete event systems. *Information Sciences*, *246*, 115–132.

Swikir, A., & Zamani, M. (2019). Compositional synthesis of finite abstractions for networks of systems: A small-gain approach. *Automatica*, *107*, 551–561.

Tabuada, P. (2004). Flatness and finite bisimulations in discrete time. In *16th intl symp. on mathematical theory of networks and systems*.

Tazaki, Y., & Imura, J. I. (2008). Bisimilar finite abstractions of interconnected systems. In *11th international conference on hybrid systems: Computation and control* (pp. 514–527).

Tong, Y., Li, Z., Seatzu, C., & Giua, A. (2017). Decidability of opacity verification problems in labeled Petri net systems. *Automatica*, *80*, 48–53.

Wu, B., & Lin, H. (2018). Privacy verification and enforcement via belief abstraction. *IEEE Control Systems Letters*, *2*(4), 815–820.

Yin, X., Zamani, M., & Liu, S. (2021). On approximate opacity of cyber-physical systems. *IEEE Transactions on Automatic Control*, *66*(4), 1630–1645.

Zhang, K., Yin, X., & Zamani, M. (2019). Opacity of nondeterministic transition systems: A (bi) simulation relation approach. *IEEE Transactions on Automatic Control*, *64*(12), 5116–5123.

Siyuan Liu is currently a Ph.D. candidate in the Department of Electrical and Computer Engineering, Technical University of Munich, Munich, Germany. She received the B. Eng degree in Automation Science and the M.Eng. degree in Control Engineering both from Beihang University, Beijing, China, in 2014 and 2017, respectively.

Her current research interests include formal methods, security properties of cyber–physical systems, and compositional methods for verification and control of large-scale systems.

Majid Zamani is an Assistant Professor in the Computer Science Department at the University of Colorado Boulder, USA. He is also a guest professor in the Computer Science Department at the Ludwig Maximilian University of Munich. He received a B.Sc. degree in Electrical Engineering in 2005 from Isfahan University of Technology, Iran, an M.Sc. degree in Electrical Engineering in 2007 from Sharif University of Technology, Iran, an MA degree in Mathematics and a Ph.D. degree in Electrical Engineering both in 2012 from University of California, Los Angeles, USA. Between September 2012 and December 2013 he was a postdoctoral researcher at the Delft Center for Systems and Control, Delft University of Technology, Netherlands. From May 2014 to January 2019 he was an Assistant Professor in the Department of Electrical and Computer Engineering at the Technical University of Munich, Germany. From December 2013 to April 2014 he was an Assistant Professor in the Design Engineering Department, Delft University of Technology, Netherlands. He received an ERC starting grant award from the European Research Council in 2018.

His research interests include verification and control of hybrid systems, embedded control software synthesis, networked control systems, and incremental properties of nonlinear control systems.