Nonlinear Analysis: Hybrid Systems 42 (2021) 101084

Contents lists available at ScienceDirect

Nonlinear Analysis: Hybrid Systems

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

Verification of approximate opacity for switched systems: A compositional approach☆

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

[a] Technical University of Munich, 80333 Munich, Germany
[b] University of Colorado Boulder, CO 80309, USA
[c] LMU Munich, 80538 Munich, Germany

ARTICLE INFO

Article history:
Received 30 June 2020
Received in revised form 1 April 2021
Accepted 28 June 2021
Available online 5 July 2021

Keywords:
Switched systems
Opacity
Compositionality
Large-scale systems

ABSTRACT

The security in information-flow has become a major concern for cyber–physical systems (CPSs). In this work, we focus on the analysis of an information-flow security property, called *opacity*. Opacity characterizes the plausible deniability of a system's secret in the presence of a malicious outside intruder. We propose a methodology of checking a notion of opacity, called approximate opacity, for networks of discrete-time switched systems. Our framework relies on compositional constructions of finite abstractions for networks of switched systems and their approximate opacity-preserving simulation functions. Those functions characterize how close concrete networks and their finite abstractions are in terms of the satisfaction of approximate opacity. We show that such simulation functions can be obtained compositionally by assuming some small-gain type conditions and composing local simulation functions constructed for each switched subsystem separately. Additionally, assuming certain stability property of switched systems, we also provide a technique on constructing their finite abstractions together with the corresponding local simulation functions. Finally, we illustrate the effectiveness of our results through an example.

© 2021 Elsevier Ltd. All rights reserved.

1. Introduction

Cyber–physical systems (CPSs) are complex systems resulting from intricate interaction between embedded cyber devices and physical plants. While the increased interaction between cyber and physical components increases systems' functionalities, it also exposes CPSs to more vulnerabilities and security challenges. Recently, the world has witnessed numerous cyber-attacks which have led to great losses in people's livelihoods [1,2]. Therefore, ensuring the security of CPSs has become significantly more important.

In this work, we focus on an information-flow security property, called *opacity*, which characterizes whether or not the secret information of a system can be revealed to a malicious intruder outside the system. Opacity was first introduced in [3] to analyze cryptographic protocols. Later, opacity was widely studied in the domain of Discrete Event Systems (DESs), see [4,5] and the references therein. In this context, existing works on the analysis of various notions of opacity mostly apply to systems modeled by finite state automata, which are more suitable for the cyber-layers of CPSs. However, for the physical components, system dynamics are in general hybrid with uncountable number of states.

☆ This work was supported in part by the H2020 ERC Starting Grant AutoCPS (grant agreement No. 804639), China Scholarship Council, the German Research Foundation (DFG) under Grant ZA 873/7-1, and the National Science Foundation (NSF), USA under Grant ECCS-2015403.

* Corresponding author.
E-mail address: sy.liu@tum.de (S. Liu).

https://doi.org/10.1016/j.nahs.2021.101084
1751-570X/© 2021 Elsevier Ltd. All rights reserved.

1.1. Related works

There have been some recent attempts to extend the notion of opacity to continuous-space dynamical systems [6–11]. In [6,7], a framework for opacity was introduced for the class of discrete-time linear systems, where the notion of opacity was formulated as an output reachability property rather than an information-flow one. The results in [8] presented a new opacity enforcement mechanism for CPSs modeled as linear time-invariant systems, where the security metric is considered as the interference attenuation capacity of the system. The results in [9] presented a formulation of opacity-preserving (bi)simulation relations between transition systems, which allows one to verify opacity of an infinite-state transition system by leveraging its associated finite quotient one. However, the notion of opacity proposed in this work assumes that the outputs of systems are symbols and are exactly distinguishable from each other, thus, is only suitable for systems with purely logical output sets. In a more recent paper [10], a new notion of *approximate opacity* was proposed to accommodate imperfect measurement precision of intruders. Based on this, the authors proposed a notion of approximate opacity-preserving simulation relation to capture the closeness between continuous-space systems and their finite abstractions (a.k.a symbolic models) in terms of preservation of approximate opacity. The recent results in [11] investigated 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 (a.k.a. finite Markov decision processes).

Although the results in [9–11] look promising, the computational complexity of the construction of finite abstractions in those works grows exponentially with respect to the dimension of the state set, and, hence, those existing approaches will become computationally intractable when dealing with large-scale systems.

Motivated by those abstraction-based techniques in [9–11] and their limitations, this work proposes an approach to analyze approximate opacity for networks of switched systems by constructing their opacity-preserving finite abstractions compositionally. There have been some recent results [12–18]proposing compositional techniques for constructing finite abstractions for networks of systems. The results in [12] first explored small-gain conditions for the compositional construction of *complete* finite abstractions for a network of discrete-time control systems. Later, the compositional framework was extended in [16] to continuous-time systems based on a notion of disturbance bisimulation relation. The results in [15] proposed a max-type small-gain type compositional condition which results in a finite abstraction with smaller approximation error. There are also other results in the literature [13,14] which provide compositional construction of *sound* abstractions without imposing strong compositionality conditions. However, the aforementioned compositional schemes above are proposed for the sake of controller synthesis for temporal logic properties, and none of them are applicable to deal with security properties including opacity. Recently, a compositional framework is presented in [19] motivated by the computational complexity encountered in the analysis of a related property, called *critical observability*, for large-scale networks of finite state machines. A bisimulation equivalence is defined taking into account criticalities. More recently, the results in [20] present a compositional framework for the construction of opacity-preserving finite abstractions for interconnected *control* systems without any discrete dynamic. Here we enlarge the class of systems for the first time to hybrid ones with switching signals. If switched subsystems accept common incremental Lyapunov functions, our proposed results here recover the ones presented in the previous work. Compositional construction of finite abstractions for networks of switched systems is proposed in [17,18] using different compositionality schemes based on dissipativity theory and small-gain type conditions, respectively. Our result here differs from the ones in [17,18] in two main aspects. First note that we are interested in the *verification* of opacity based on a new notion of *opacity-preserving simulation functions*, while the works in [17,18] rely on the standard notion of *alternating simulation functions* (ASFs) to handle the problem of controller *synthesis* against temporal logic properties. Although requiring stronger conditions than ASFs, our new notion of opacity-preserving simulation functions is shown to preserve approximate opacity across related systems. Hence, it can be used for the abstraction-based verification of approximate opacity for switched systems. Secondly, we provide here a *top-down* compositional construction framework along with a detailed design guideline (cf. Algorithm 1), whereas the results in [17,18] present a *bottom-up* compositional approach. In particular, our methodology shows that given any desired precision for the overall opacity-preserving finite abstraction, under a sufficient small-gain type condition, one can always orderly design local quantization parameters to achieve the overall abstraction precisions. Note that such a systematic compositional scheme cannot be achieved by the results in [17,18].

1.2. Contributions

In this paper, we provide for the first time a compositional approach to analyze approximate opacity of a network of switched systems using their finite abstractions. We consider two types of approximate opacity, i.e., approximate initial-state opacity and approximate current-state opacity. A new notion of approximate initial-state (resp. current-state) opacity-preserving simulation function (InitSOPSF, resp. CurSOPSF) is introduced as a system relation to characterize the closeness between two networks in terms of preservation of approximate initial-state (resp. current-state) opacity. We show that such an InitSOPSF (resp. CurSOPSF) can be established by composing certain local InitSOPSFs (resp. CurSOPSFs) which relate each switched subsystem to its local finite abstraction. Moreover, under some assumptions ensuring incremental input-to-state stability of discrete-time switched systems, an approach is provided to construct

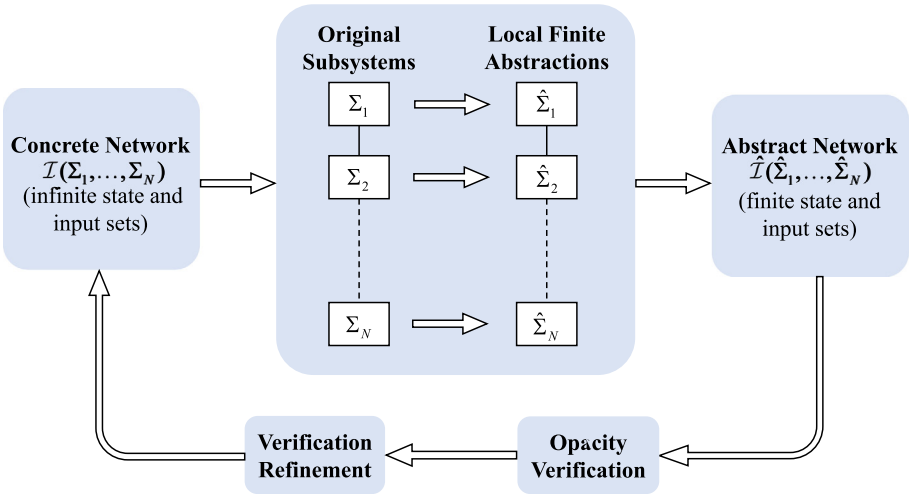

Fig. 1. Compositional framework for opacity verification of networks of switched systems.

local finite abstractions along with the corresponding local InitSOPSFs (resp. CurSOPSFs) for all of the subsystems. Then, we derive some small-gain type conditions, under which one can construct a finite abstraction of the concrete network of switched systems by interconnecting local finite abstractions of subsystems. Finally, one can verify opacity based on the constructed finite abstraction, and then refine the results back to the concrete network based on their opacity-preserving system relation. The proposed compositional abstraction-based opacity verification pipeline is depicted in Fig. 1.

1.3. Organization

The rest of this paper is organized as follows. In Section 2, we first introduce necessary notations and preliminaries of the paper. Then, new notions of approximate opacity-preserving simulation functions (InitSOPSFs and CurSOPSFs) are proposed in Section 3. In Section 4, we provide a compositional framework for the construction of InitSOPSFs and CurSOPSFs for a network of discrete-time switched systems. In Section 5, we present how to construct local finite abstractions for a class of incrementally input-to-state stable subsystems, and then propose a small-gain type condition required for the main compositionality result. Next, an illustrative example is provided in Section 6 that showcases how one can leverage our compositionality results for the verification of opacity for a network of switched systems. Finally, we conclude the paper in Section 7.

A preliminary investigation of our results appeared in [21]. Our results here improve and extend those in [21] in the following directions. First, we provide here the proofs of all statements which were omitted in [21]. We also add more detailed descriptions and discussions of the results announced in [21], with all definitions reformulated in a more uniform manner. Second, we present here compositional approaches to tackle both initial-state and current-state opacity, while [21] only considers initial-state opacity. Finally, an algorithm is provided here to serve as a systematic guideline for the compositional construction of abstractions with any desired approximation precision, which is not presented in [21].

2. Notation and preliminaries

2.1. 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 obvious way, e.g. $\mathbb{R}_{>0}$ denotes the positive real numbers. We denote the closed, open, and half-open intervals in $\mathbb{R}$ by $[a, b]$, (a, b), $[a, b)$, and $(a, b]$, respectively. For $a, b \in \mathbb{N}$ and $a \leq b$, we use $[a; b]$, $(a; b)$, $[a; b)$, and $(a; b]$ to denote the corresponding intervals in $\mathbb{N}$. Given any $a \in \mathbb{R}$, $|a|$ denotes the absolute value of a. Given $N \in \mathbb{N}_{\geq 1}$ vectors $\nu_i \in \mathbb{R}^{n_i}$, $n_i \in \mathbb{N}_{\geq 1}$, and $i \in [1; N]$, we use $\nu = [\nu_1; \ldots; \nu_N]$ to denote the vector in $\mathbb{R}^n$ with $n = \sum_i n_i$ consisting of the concatenation of vectors ν_i. Moreover, $\|\nu\|$ denotes the infinity norm of ν. The individual elements in a matrix $A \in \mathbb{R}^{m\times n}$, are denoted by $\{A\}_{i,j}$, where $i \in [1; m]$ and $j \in [1; n]$. We denote by $\text{card}(\cdot)$ the cardinality of a given set and by $\emptyset$ the empty set. 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 $X_i \subseteq \mathbb{R}^{n_i}$, $\forall i \in [1; N]$, are of the form of finite union of boxes, and any positive (component-wise) 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 $\phi = [\eta; \ldots; \eta]$, where

$0 < \eta \leq span(S)$, we simply use notation $[S]_\eta$ rather than $[S]_\phi$. With a slight abuse of notation, we write $[S]_0 := S$. Note that $[S]_\eta \neq \emptyset$ for any $0 \leq \eta \leq span(S)$. We use notations $\mathcal{K}$ and $\mathcal{K}_\infty$ to denote different classes of comparison functions, as follows: $\mathcal{K} = \{\alpha : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0} |\ \alpha \text{ is continuous, strictly increasing, and } \alpha(0) = 0\}$; $\mathcal{K}_\infty = \{\alpha \in \mathcal{K} |\ \lim_{r\to\infty} \alpha(r) = \infty\}$. For $\alpha, \gamma \in \mathcal{K}_\infty$ we write $\alpha \leq \gamma$ if $\alpha(r) \leq \gamma(r)$, and, with abuse of the notation, $\alpha = c$ if $\alpha(r) = cr$ for all $c, r \geq 0$. Finally, we denote by $\mathcal{I}_d$ the identity function over $\mathbb{R}_{\geq 0}$, that is $\mathcal{I}_d(r) = r, \forall r \in \mathbb{R}_{\geq 0}$. Given sets X and Y with $X \subset Y$, the complement of X with respect to Y is defined as $Y \backslash X = \{x : x \in Y, x \notin X\}$.

2.2. Discrete-time switched systems

We consider discrete-time switched systems of the following form.

Definition 1. A discrete-time switched system (dt-SS) Σ is defined by the tuple $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, \mathbb{W}, F, \mathbb{Y}, h)$, where

- $\mathbb{X} \subseteq \mathbb{R}^n$ is the state set;
- $\mathbb{X}_0 \subseteq \mathbb{X}$ is the initial state set;
- $\mathbb{X}_s \subseteq \mathbb{X}$ is the secret state set;
- $P = \{1, \ldots, m\}$ is the finite set of modes;
- $\mathbb{W} \subseteq \mathbb{R}^m$ is the internal input set;
- $F = \{f_1, \ldots, f_m\}$ is a collection of set-valued maps $f_p : \mathbb{X} \times \mathbb{W} \rightrightarrows \mathbb{X}$ for all $p \in P$;
- $\mathbb{Y} \subseteq \mathbb{R}^q$ is the output set;
- $h : \mathbb{X} \to \mathbb{Y}$ is the output map.

The dt-SS Σ is described by difference inclusions of the form

$$\Sigma : \begin{cases} \mathbf{x}(k+1) & \in f_{\mathrm{p}(k)}(\mathbf{x}(k), \omega(k)), \\ \mathbf{y}(k) & = h(\mathbf{x}(k)), \end{cases} \tag{1}$$

where $\mathbf{x} : \mathbb{N} \to \mathbb{X}$, $\mathbf{y} : \mathbb{N} \to \mathbb{Y}$, $\mathrm{p} : \mathbb{N} \to P$, and $\omega : \mathbb{N} \to \mathbb{W}$ are the state, output, switching, and internal input signal, respectively.

Let $\varphi_k, k \in \mathbb{N}_{\geq 1}$, denote the time when the kth switching instant occurs. We assume that signal p satisfies a dwell-time condition [22] (i.e. there exists $k_d \in \mathbb{N}_{\geq 1}$, called the dwell-time, such that for all consecutive switching time instants φ_k, φ_{k+1}, $\varphi_{k+1} - \varphi_k \geq k_d$). If for all $x \in \mathbb{X}, p \in P, w \in \mathbb{W}$, $\mathrm{card}(f_p(x, w)) \leq 1$, we say the system Σ is deterministic, and non-deterministic otherwise. System Σ is called finite if $\mathbb{X}, \mathbb{W}$ are finite sets and infinite otherwise. We assume that for every initial condition and any sequence of switching signals, the corresponding state signal is defined for all $k \geq 0$.

2.3. Transition systems

In this subsection, we employ the notion of transition systems, originally introduced in [23], to provide an alternative description of switched systems that can be later directly related to their finite abstractions in a common framework.

Definition 2. Given a dt-SS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, \mathbb{W}, F, \mathbb{Y}, h)$, we define the associated transition system $T(\Sigma) = (X, X_0, X_s, U, W, \mathcal{F}, Y, \mathcal{H})$, where:

- $X = \mathbb{X} \times P \times \{0, \ldots, k_d - 1\}$ is the state set;
- $X_0 = \mathbb{X}_0 \times P \times \{0\}$ is the initial state set;
- $X_s = \mathbb{X}_s \times P \times \{0, \ldots, k_d - 1\}$ is the secret state set;
- $U = P$ is the external input set;
- $W = \mathbb{W}$ is the internal input set;
- $\mathcal{F}$ is the transition function given by $(x^+, p^+, l^+) \in \mathcal{F}((x, p, l), u, w)$ if and only if $x^+ \in f_p(x, w)$, $u = p$ and one of the following scenarios hold:
  - $l < k_d - 1$, $p^+ = p$ and $l^+ = l + 1$: switching is not allowed because the time elapsed since the latest switch is strictly smaller than the dwell time;
  - $l = k_d - 1$, $p^+ = p$ and $l^+ = k_d - 1$: switching is allowed but no switch occurs;
  - $l = k_d - 1$, $p^+ \neq p$ and $l^+ = 0$: switching is allowed and a switch occurs;
- $Y = \mathbb{Y}$ is the output set;
- $\mathcal{H} : X \to Y$ is the output map defined as $\mathcal{H}(x, p, l) = h(x)$.

Note that in the above definition, two additional variables p and l are added to the state tuple of the system Σ. The variable l serves as a counter to record the sojourn time of the switching signal, which allows or prevents the system from switching depending on whether the dwell-time condition is satisfied; the variable p acts as a memory to record the current mode of the system.

The following proposition is borrowed from [17] showing that the output runs of a dt-SS Σ and its associated transition system $T(\Sigma)$ are equivalent so that one can use Σ and $T(\Sigma)$ interchangeably.

Proposition 3. *Consider a transition system $T(\Sigma)$ in Definition 2 associated to Σ as in Definition 1. Any output trajectory of Σ can be uniquely equated to an output trajectory of $T(\Sigma)$ and vice versa.*

Next, let us introduce a formal definition of networks of dt-SS (or equivalently, networks of transition systems).

2.4. Networks of systems

Consider $N \in \mathbb{N}_{\geq 1}$ dt-SS $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, P_i, \mathbb{W}_i, F_i, \mathbb{Y}_i, h_i)$, $i \in [1; N]$, with partitioned internal inputs and outputs as

$$w_i = [w_{i1}; \ldots; w_{i(i-1)}; w_{i(i+1)}; \ldots; w_{iN}], \quad \mathbb{W}_i = \prod_{j=1, j\neq i}^{N} \mathbb{W}_{ij}, \tag{2}$$

$$h_i(x_i) = [h_{i1}(x_i); \ldots; h_{iN}(x_i)], \quad \mathbb{Y}_i = \prod_{j=1}^{N} \mathbb{Y}_{ij}, \tag{3}$$

with $w_{ij} \in \mathbb{W}_{ij}$, and $y_{ij} = h_{ij}(x_i) \in \mathbb{Y}_{ij}$. The outputs y_{ii} are considered as external ones, whereas y_{ij} with $i \neq j$ are interpreted as internal ones which are used to construct interconnections between systems. In particular, we assume that $w_{ij} = y_{ji}$, if there is connection from system Σ_j to Σ_i, otherwise, we set $h_{ji} \equiv 0$. In the sequel, we denote by $\mathcal{N}_i = \{j \in [1; N], j \neq i | h_{ji} \neq 0\}$ the collection of neighboring systems $\Sigma_j, j \in \mathcal{N}_i$, that provide internal inputs to system Σ_i.

Now, we introduce the notions of networks (in both concrete and abstract domains) based on the notion of interconnected systems in [24]. For a concrete network constructed as the interconnection of $N \in \mathbb{N}_{\geq 1}$ concrete subsystems, Definition 1 reduces to the tuple $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, F, \mathbb{Y}, h)$ without internal inputs and outputs as in the following definition.

Definition 4. Consider $N \in \mathbb{N}_{\geq 1}$ dt-SS $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, P_i, \mathbb{W}_i, F_i, \mathbb{Y}_i, h_i)$, $i \in [1; N]$ with the input–output structure given by (2) and (3). The network, representing the interconnection of $N \in \mathbb{N}_{\geq 1}$ dt-SS Σ_i, is a tuple $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, F, \mathbb{Y}, h)$, denoted by $\mathcal{I}(\Sigma_1, \ldots, \Sigma_N)$, where $\mathbb{X} = \prod_{i=1}^{N} \mathbb{X}_i$, $\mathbb{X}_0 = \prod_{i=1}^{N} \mathbb{X}_{0_i}$, $\mathbb{X}_s = \prod_{i=1}^{N} \mathbb{X}_{s_i}$, $P = \prod_{i=1}^{N} P_i$, $F = \prod_{i=1}^{N} F_i$, $\mathbb{Y} = \prod_{i=1}^{N} \mathbb{Y}_{ii}$, $h(x) := [h_{11}(x_1); \ldots; h_{NN}(x_N)]$ with $x = [x_1; \ldots; x_N]$, subject to the constraint:

$$y_{ji} = w_{ij}, \mathbb{Y}_{ji} \subseteq \mathbb{W}_{ij}, \forall i \in [1; N], j \in \mathcal{N}_i. \tag{4}$$

Similarly, given transition systems $T(\Sigma_i)$, one can also define a network of transition systems $\mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_N))$. For the rest of the paper, we mainly deal with the transition systems as they allow us to model dt-SS Σ and their finite abstractions in a common framework.

For an interconnection of $N \in \mathbb{N}_{\geq 1}$ finite dt-SS $\hat{\Sigma}_i$, with input–output structure configuration as in (2) and (3), we introduce the following definition of networks of finite dt-SS.

Definition 5. Consider $N \in \mathbb{N}_{\geq 1}$ finite dt-SS $\hat{\Sigma}_i = (\hat{\mathbb{X}}_i, \hat{\mathbb{X}}_{0_i}, \hat{\mathbb{X}}_{s_i}, \hat{P}_i, \hat{\mathbb{W}}_i, \hat{F}_i, \hat{\mathbb{Y}}_i, \hat{h}_i)$, $i \in [1; N]$ with the input–output structure given by (2) and (3). The network, representing the interconnection of $N \in \mathbb{N}_{\geq 1}$ finite dt-SS $\hat{\Sigma}_i$, is a tuple $\hat{\Sigma} = (\hat{\mathbb{X}}, \hat{\mathbb{X}}_0, \hat{\mathbb{X}}_s, \hat{P}, \hat{F}, \hat{\mathbb{Y}}, \hat{h})$, denoted by $\hat{\mathcal{I}}(\hat{\Sigma}_1, \ldots, \hat{\Sigma}_N)$, where $\hat{\mathbb{X}} = \prod_{i=1}^{N} \hat{\mathbb{X}}_i$, $\hat{\mathbb{X}}_0 = \prod_{i=1}^{N} \hat{\mathbb{X}}_{0_i}$, $\hat{\mathbb{X}}_s = \prod_{i=1}^{N} \hat{\mathbb{X}}_{s_i}$, $\hat{P} = \prod_{i=1}^{N} \hat{P}_i$, $\hat{F} = \prod_{i=1}^{N} \hat{F}_i$, $\hat{\mathbb{Y}} = \prod_{i=1}^{N} \hat{\mathbb{Y}}_{ii}$, $\hat{h}(x) := \left[\hat{h}_{11}(\hat{x}_1); \ldots; \hat{h}_{NN}(\hat{x}_N)\right]$ with $\hat{x} = \left[\hat{x}_1; \ldots; \hat{x}_N\right]$, subject to the constraint:

$$\forall \hat{y}_{ji} \in \hat{\mathbb{Y}}_{ji}, \exists \hat{w}_{ij} \in \hat{\mathbb{W}}_{ij}, \text{ s.t. } \|\hat{y}_{ji} - \hat{w}_{ij}\| \leq \phi_{ij}, i \in [1; N], j \in \mathcal{N}_i, \tag{5}$$

where ϕ_{ij} is an internal input quantization parameter designed for constructing local finite abstractions (cf. Definition 20).

Similarly, given finite transition systems $T(\hat{\Sigma}_i)$, one can also define a network of transition systems as $\hat{\mathcal{I}}(T(\hat{\Sigma}_1), \ldots, T(\hat{\Sigma}_N))$.

An example of a concrete network and an abstract network is illustrated in Fig. 2, where each consists of three switched subsystems.

Remark 6. Note that in the above definitions, the interconnection constraint in (4) for the concrete network is different from that for the abstract network in (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 (5) for having a well-posed interconnection. The values of ϕ_{ij} will be designed later in Definition 20 when constructing local finite abstractions of the subsystems.

Before introducing the notion of approximate initial-state opacity for networks of transition systems, we introduce some notations that will be used to characterize opacity property. Consider network $T(\Sigma)$. We use z^k to denote a state of $T(\Sigma)$ reached at time $k \in \mathbb{N}$ from initial state z^0 under an input sequence $\bar{u}$ with length k, and denote by $\{z^0, z^1, \ldots, z^n\}$ a finite state run of $T(\Sigma)$ with length $n \in \mathbb{N}$.

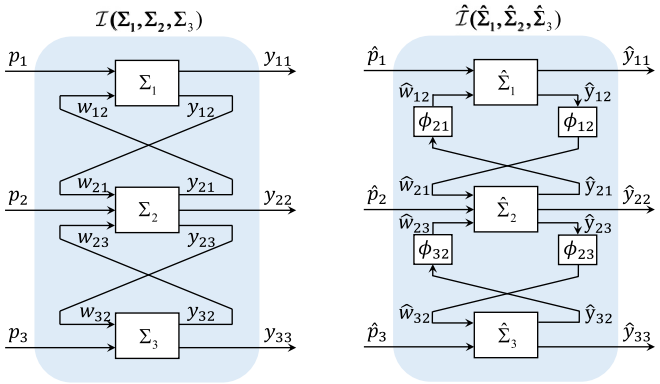

Fig. 2. [Left]: Concrete network composed of three switched subsystems Σ_1, Σ_2, and Σ_3 with $h_{13} = h_{31} = 0$, where $y_{ji} = w_{ij}$, $\forall i, j \in [1; 3]$; [Right]: Abstract network composed of three finite subsystems $\hat{\Sigma}_1$, $\hat{\Sigma}_2$, and $\hat{\Sigma}_3$ with $\hat{h}_{13} = \hat{h}_{31} = 0$, and the internal inputs $\hat{w}_{ij}$ for system $\hat{\Sigma}_i$ are taken from the discretized internal outputs of system $\hat{\Sigma}_j$ under the constraint $\|\hat{y}_{ji} - \hat{w}_{ij}\| \leq \phi_{ij}$, $\forall i, j \in [1; 3]$, where ϕ_{ij} are internal input quantization parameters.

2.5. Approximate opacity

Here, let us review a notion of approximate initial-state (resp. current-state) opacity [10]. In this context, the system's behaviors are assumed to be observed by an outside intruder which aims at inferring secret information of the system. The adopted concept of secrets are formulated as state-based.

Definition 7. Consider network $T(\Sigma) = (X, X_0, X_s, U, \mathcal{F}, Y, \mathcal{H})$ and a constant $\delta \geq 0$. Network $T(\Sigma)$ is said to be

- *δ-approximate initial-state opaque* if for any $z^0 \in X_0 \cap X_s$ and any finite state run $\{z^0, z^1, \ldots, z^n\}$, there exist $\bar{z}^0 \in X_0 \setminus X_s$ and a finite state run $\{\bar{z}^0, \bar{z}^1, \ldots, \bar{z}^n\}$ such that $\max_{k\in[0;n]} \|\mathcal{H}(z^k) - \mathcal{H}(\bar{z}^k)\| \leq \delta$.
- *δ-approximate current-state opaque* if for any $z^0 \in X_0$ and finite state run $\{z^0, z^1, \ldots, z^n\}$ such that $z^n \in X_s$, there exists $\bar{z}^0 \in X_0$ and a finite state run $\{\bar{z}^0, \bar{z}^1, \ldots, \bar{z}^n\}$ such that $\bar{z}^n \in X \setminus X_s$ and $\max_{k\in[0;n]} \|\mathcal{H}(z^k) - \mathcal{H}(\bar{z}^k)\| \leq \delta$.

Intuitively, the notion of δ-approximate initial-state opacity requires that, whenever observing any output run, an intruder with measurement precision δ is never certain that the system is initiated from a secret state. In other words, the systems' secret information can never be revealed in the presence of an intruder that does not have an enough measurement precision. Similarly, δ-approximate current-state opacity says that the intruder with measurement precision δ never knows for sure that the system is currently at a secret state no matter which output run is generated.

In the next corollary, we show that if a system equipped with secret set X_s is δ-approximate opaque, then the system is also δ-approximate opaque with a smaller secret set contained in X_s.

Corollary 8. *Consider networks $T(\Sigma_1) = (X, X_0, X_s, U, \mathcal{F}, Y, \mathcal{H})$ and $T(\Sigma_2) = (X, X_0, X_s', U, \mathcal{F}, Y, \mathcal{H})$ with $X_s' \subseteq X_s$. If $T(\Sigma_1)$ is δ-approximate initial-state (resp. current-state) opaque, then $T(\Sigma_2)$ is also δ-approximate initial-state (resp. current-state) opaque.*

Proof. We start by showing the preservation of approximate initial-state opacity across systems $T(\Sigma_1)$ and $T(\Sigma_2)$. Consider any $z^0 \in X_0 \cap X_s'$ and any finite state run $\{z^0, z^1, \ldots, z^n\}$ in $T(\Sigma_2)$. Given that $X_s' \subseteq X_s$, we get $z^0 \in X_0 \cap X_s$. Since $T(\Sigma_1)$ is δ-approximate initial-state opaque, from Definition 7, there exist $\bar{z}^0 \in X_0 \setminus X_s$ and a finite state run $\{\bar{z}^0, \bar{z}^1, \ldots, \bar{z}^n\}$ such that $\max_{k\in[0;n]} \|\mathcal{H}(z^k) - \mathcal{H}(\bar{z}^k)\| \leq \delta$. Moreover, given that $\{X_0 \setminus X_s\} \subseteq \{X_0 \setminus X_s'\}$, we get $\bar{z}^0 \in X_0 \setminus X_s'$. Therefore, by Definition 7, $T(\Sigma_2)$ is also δ-approximate initial-state opaque. Similarly, we show the preservation of approximate current-state opacity across systems $T(\Sigma_1)$ and $T(\Sigma_2)$. Consider any $z^0 \in X_0$ and any finite state run $\{z^0, z^1, \ldots, z^n\}$ such that $z^n \in X_s'$ in $T(\Sigma_2)$. Since $T(\Sigma_1)$ is δ-approximate current-state opaque, from Definition 7, there exist $\bar{z}^0 \in X_0$ and a finite state run $\{\bar{z}^0, \bar{z}^1, \ldots, \bar{z}^n\}$ such that $\bar{z}^n \in X \setminus X_s$ and $\max_{k\in[0;n]} \|\mathcal{H}(z^k) - \mathcal{H}(\bar{z}^k)\| \leq \delta$. Moreover, given that $\{X \setminus X_s\} \subseteq \{X \setminus X_s'\}$, we get $\bar{z}^n \in X \setminus X_s'$. Therefore, by Definition 7, $T(\Sigma_2)$ is also δ-approximate current-state opaque. □

Remark 9. Note that it is assumed in Definitions 4 and 5 that the secret set of the network is the Cartesian product of the secret sets of the subsystems. However, if the secret set of the original network is in a more general from (e.g. polytopes), one can use minimum bounding box algorithms [25] to compute the smallest hyper-rectangle containing the secret set of the original network. If we consider this hyper-rectangle as the new secret set and follow the same procedure to verify opacity of the system, then by Corollary 8, the results (if successful) can be carried over to the original network.

Remark 10. The notions of approximate initial-state and current-state opacity are, in general, hard to check for a concrete network since there is no systematic way in the literature to check opacity for systems with infinite state set so far. On the other hand, existing tool DESUMA[1] and algorithms [26,27], [9, Sec. IV] in DESs literature can be leveraged to check *exact* opacity for networks with finite state sets. For the verification of approximate opacity of the constructed finite abstractions, one can readily resort to [10, Sec. IV] for an effective verification approach that was developed for the notion of *approximate opacity* for finite systems. The above-mentioned algorithms helps us to verify opacity for networks consisting of finite abstractions and then carry back the verification result to concrete ones, given a formal simulation relation between those networks. To this purpose, an opacity-preserving simulation relation will be introduced in the next section which formally relate a network of transition systems and its finite abstraction.

3. Opacity-preserving simulation functions

In this section, we introduce notions of approximate opacity-preserving simulation functions to quantitatively relate two networks of transition systems in terms of preserving approximate initial-state and current-state opacity. Such a function can be constructed compositionally as shown in Section 4.

First, we introduce a notion of approximate initial-state opacity-preserving simulation functions in the following definition.

Definition 11. Consider networks $T(\Sigma) = (X, X_0, X_s, U, \mathcal{F}, Y, \mathcal{H})$ and $T(\hat{\Sigma}) = (\hat{X}, \hat{X}_0, \hat{X}_s, \hat{U}, \hat{\mathcal{F}}, \hat{Y}, \hat{\mathcal{H}})$ with $\hat{Y} \subseteq Y$. For $\varepsilon \in \mathbb{R}_{\geq 0}$, a function $\mathcal{S} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ is called an ε-approximate initial-state opacity-preserving simulation function (ε-InitSOPSF) from $T(\Sigma)$ to $T(\hat{\Sigma})$ if there exists a function $\alpha \in \mathcal{K}_\infty$ such that

1 (a) $\forall z^0 \in X_0 \cap X_s$, $\exists \hat{z}^0 \in \hat{X}_0 \cap \hat{X}_s$, s.t. $\mathcal{S}(z^0, \hat{z}^0) \leq \varepsilon$;
(b) $\forall \hat{z}^0 \in \hat{X}_0 \setminus \hat{X}_s$, $\exists z^0 \in X_0 \setminus X_s$, s.t. $\mathcal{S}(z^0, \hat{z}^0) \leq \varepsilon$;
2 $\forall z \in X, \forall \hat{z} \in \hat{X}$, $\alpha(\|\mathcal{H}(z) - \hat{\mathcal{H}}(\hat{z})\|) \leq \mathcal{S}(z, \hat{z})$;
3 $\forall z \in X, \forall \hat{z} \in \hat{X}$ s.t. $\mathcal{S}(z, \hat{z}) \leq \varepsilon$, one has:

(a) $\forall u \in U, \forall z^+ \in \mathcal{F}(z, u)$, $\exists \hat{u} \in \hat{U}, \exists \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$, s.t. $\mathcal{S}(z^+, \hat{z}^+) \leq \varepsilon$;
(b) $\forall \hat{u} \in \hat{U}, \forall \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$, $\exists u \in U, \exists z^+ \in \mathcal{F}(z, u)$, s.t. $\mathcal{S}(z^+, \hat{z}^+) \leq \varepsilon$.

Similarly, we introduce a notion of approximate current-state opacity-preserving simulation functions defined as follows.

Definition 12. Consider networks $T(\Sigma) = (X, X_0, X_s, U, \mathcal{F}, Y, \mathcal{H})$ and $T(\hat{\Sigma}) = (\hat{X}, \hat{X}_0, \hat{X}_s, \hat{U}, \hat{\mathcal{F}}, \hat{Y}, \hat{\mathcal{H}})$ with $\hat{Y} \subseteq Y$. For $\varepsilon \in \mathbb{R}_{\geq 0}$, a function $\mathcal{S} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ is called an ε-approximate current-state opacity-preserving simulation function (ε-CurSOPSF) from $T(\Sigma)$ to $T(\hat{\Sigma})$ if there exists a function $\alpha \in \mathcal{K}_\infty$ such that

1 $\forall z^0 \in X_0$, $\exists \hat{z}^0 \in \hat{X}_0$, s.t. $\mathcal{S}(z^0, \hat{z}^0) \leq \varepsilon$;
2 $\forall z \in X, \forall \hat{z} \in \hat{X}$, $\alpha(\|\mathcal{H}(z) - \hat{\mathcal{H}}(\hat{z})\|) \leq \mathcal{S}(z, \hat{z})$;
3 $\forall z \in X, \forall \hat{z} \in \hat{X}$ s.t. $\mathcal{S}(z, \hat{z}) \leq \varepsilon$, one has:

(a) $\forall u \in U, \forall z^+ \in \mathcal{F}(z, u)$, $\exists \hat{u} \in \hat{U}, \exists \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$, s.t. $\mathcal{S}(z^+, \hat{z}^+) \leq \varepsilon$;
(b) $\forall u \in U, \forall z^+ \in \mathcal{F}(z, u)$ s.t. $z^+ \in X_s$, $\exists \hat{u} \in \hat{U}, \exists \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$ with $\hat{z}^+ \in \hat{X}_s$, s.t. $\mathcal{S}(z^+, \hat{z}^+) \leq \varepsilon$;
(c) $\forall \hat{u} \in \hat{U}, \forall \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$ $\exists u \in U, \exists z^+ \in \mathcal{F}(z, u)$, s.t. $\mathcal{S}(z^+, \hat{z}^+) \leq \varepsilon$;
(d) $\forall \hat{u} \in \hat{U}, \forall \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$ s.t. $\hat{z}^+ \in \hat{X} \setminus \hat{X}_s$, $\exists u \in U, \exists z^+ \in \mathcal{F}(z, u)$ with $z^+ \in X \setminus X_s$, s.t. $\mathcal{S}(z^+, \hat{z}^+) \leq \varepsilon$.

We say that $T(\hat{\Sigma})$ is an abstraction of $T(\Sigma)$ if there exists an ε-InitSOPSF, or ε-CurSOPSF, from $T(\Sigma)$ to $T(\hat{\Sigma})$. In addition, if $T(\hat{\Sigma})$ is finite ($\hat{X}$ is a finite set), system $T(\hat{\Sigma})$ is called a finite abstraction (symbolic model) of the network $T(\Sigma)$, and is denoted by $T(\Sigma) \preceq^{\varepsilon} T(\hat{\Sigma})$.

Although Definitions 11 and 12 are general in the sense that networks $T(\Sigma)$ and $T(\hat{\Sigma})$ can be either infinite or finite, network $T(\hat{\Sigma})$ practically consists of $N \in \mathbb{N}_{\geq 1}$ finite abstractions. Hence, checking approximate initial-state, or current-state, opacity for the concrete network $T(\Sigma)$ can be done by resorting to that of its finite abstraction $T(\hat{\Sigma})$ and then carry the results back to the concrete network. Since $T(\hat{\Sigma})$ is a finite system, one can verify opacity of $T(\hat{\Sigma})$ algorithmically. We refer interested readers to an existing verification approach proposed in [10, Sec.IV], which is tailored to the notion of *approximate opacity* for finite systems.

The next proposition shows that the existence of an ε-InitSOPSF (resp. ε-CurSOPSF) as we proposed in Definition 11 (resp. Definition 12) for networks of transition systems implies the existence of an approximate initial-state (resp. current-state) opacity-preserving simulation relations which was originally proposed in [10, Definition V.1] (resp. [10, Definition V.6]).

[1] Available at URL http://www.eecs.umich.edu/umdes/toolboxes.html.

Proposition 13. *Consider networks $T(\Sigma) = (X, X_0, X_s, U, \mathcal{F}, Y, \mathcal{H})$ and $T(\hat{\Sigma}) = (\hat{X}, \hat{X}_0, \hat{X}_s, \hat{U}, \hat{\mathcal{F}}, \hat{Y}, \hat{\mathcal{H}})$ where $\hat{Y} \subseteq Y$. Assume $\mathcal{S}$ is an ε-InitSOPSF (resp. ε-CurSOPSF) from $T(\Sigma)$ to $T(\hat{\Sigma})$ as in Definition 11 (resp. Definition 12). Then, relation $R \subseteq X \times \hat{X}$ defined by*

$$R = \left\{(z, \hat{z}) \in X \times \hat{X} | \mathcal{S}(z, \hat{z}) \leq \varepsilon\right\}, \tag{6}$$

is an $\hat{\varepsilon}$-InitSOP (resp. $\hat{\varepsilon}$-CurSOP) simulation relation from $T(\Sigma)$ to $T(\hat{\Sigma})$ with

$$\hat{\varepsilon} = \alpha^{-1}(\varepsilon). \tag{7}$$

Proof. First, we show that the proposed definition of ε-InitSOPSF implies the notion of $\hat{\varepsilon}$-InitSOP simulation relation as in [10, Definition V.1]. Condition 1 of the $\hat{\varepsilon}$-InitSOP simulation relation follows immediately from condition 1 in Definition 11, i.e. $S(z^0, \hat{z}^0) \leq \varepsilon$. Next, we show that $\forall (z, \hat{z}) \in R$: $\|\mathcal{H}(z) - \hat{\mathcal{H}}(\hat{z})\| \leq \hat{\varepsilon}$. From the definition of R and condition 2 in Definition 11, it is readily seen that $\|\mathcal{H}(z) - \hat{\mathcal{H}}(\hat{z})\| \leq \alpha^{-1}(\varepsilon) = \hat{\varepsilon}$. Finally, we show condition 3 for R. Consider any pair of $(z, \hat{z}) \in X \times \hat{X}$ in relation R and by the definition of R, one has $S(z, \hat{z}) \leq \varepsilon$. Additionally, from 3(a) in Definition 11, one also has $\forall u \in U$, $\forall z^+ \in \mathcal{F}(z, u)$, $\exists \hat{u} \in \hat{U}$, $\exists \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$ s.t. $S(z^+, \hat{z}^+) \leq \varepsilon$. Hence, it follows that $(z^+, \hat{z}^+) \in R$ which satisfies condition 3(a) of R. Condition 3(b) can be proved in the same way and is omitted here. Note that by following a similar reasoning as above, one can show that the definition of ε-CurSOPSF implies the notion of $\hat{\varepsilon}$-CurSOP simulation relation. □

Instead of directly working with the opacity-preserving simulation relations [10, Definitions V.1 and V.6], in the sequel, we will mainly focus on the proposed notions of ε-InitSOPSFs and ε-CurSOPSFs as in Definitions 11 and 12 which allow us to establish our compositionality result in an easier way.

The following corollary borrowed from [10] shows the usefulness of an approximate opacity-preserving simulation function in terms of preserving approximate opacity across related networks.

Corollary 14. *Consider networks $T(\Sigma) = (X, X_0, X_s, U, \mathcal{F}, Y, \mathcal{H})$ and $T(\hat{\Sigma}) = (\hat{X}, \hat{X}_0, \hat{X}_s, \hat{U}, \hat{\mathcal{F}}, \hat{Y}, \hat{\mathcal{H}})$ where $\hat{Y} \subseteq Y$. Assume there exists an approximate opacity-preserving simulation function from $T(\Sigma)$ to $T(\hat{\Sigma})$ as in Definitions 11 and 12 associated with $\varepsilon \in \mathbb{R}_{\geq 0}$ and $\alpha \in \mathcal{K}_\infty$. Let $\hat{\varepsilon}, \delta \in \mathbb{R}_{\geq 0}$ where $\hat{\varepsilon} = \alpha^{-1}(\varepsilon)$ and $\hat{\varepsilon} \leq \frac{\delta}{2}$. Then the following implication holds*

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

$\Rightarrow T(\Sigma)$ is δ-approximate opaque.

Note that the above implication across two related systems holds for both notions of approximate initial-state and current-state opacity in Definition 7. Corollary 14 provides us a sufficient condition for verifying approximate opacity of a complex network using abstraction-based techniques. Particularly, when confronted with a large network of switched systems, one can construct a finite abstraction $T(\hat{\Sigma})$ of the concrete network $T(\Sigma)$, conduct the opacity verification over the simpler network $T(\hat{\Sigma})$ and carry back the results to the concrete one.

4. Compositional construction of approximate opacity-preserving simulation function

As shown in the previous section, the proposed ε-InitSOPSF (resp. ε-CurSOPSF) can be used for checking approximate initial-state (resp. current-state) opacity of concrete networks by leveraging their finite abstractions. However, for a network consisting of a large number of switched subsystems, constructing the corresponding simulation function and the abstract network monolithically is not feasible in general due to curse of dimensionality. Hence, in this section, we introduce a compositional framework based on which one can break down the intricate task in parts that are more manageable to accomplish. In particular, we first relate local finite abstractions of the subsystems via local InitSOPSFs or CurSOPSFs. Then, one can obtain the abstract network by interconnecting the local finite abstractions of the subsystems. Additionally, the corresponding ε-InitSOPSF (resp. ε-CurSOPSF) to capture the closeness between the concrete and the abstract networks can be established by composing the local InitSOPSFs (resp. CurSOPSFs) as well.

Let us first introduce new notions of local InitSOPSFs and CurSOPSFs for switched subsystems with internal inputs in the following subsection.

4.1. Local approximate opacity-preserving simulation function

Suppose that we are given N dt-SS $\Sigma_i = (\mathbb{X}_i, \mathbb{X}_{0_i}, \mathbb{X}_{s_i}, P_i, \mathbb{W}_i, F_i, \mathbb{Y}_i, h_i)$, $i \in [1; N]$, or equivalently, $T(\Sigma_i) = (X_i, X_{0_i}, X_{s_i}, U_i, W_i, \mathcal{F}_i, Y_i, \mathcal{H}_i)$. Moreover, we assume that each system $T(\Sigma_i)$ and its abstraction $T(\hat{\Sigma}_i)$ admit a local approximate opacity-preserving simulation function as defined next.

Definition 15. Consider transition systems $T(\Sigma_i) = (X_i, X_{0_i}, X_{s_i}, U_i, W_i, \mathcal{F}_i, Y_i, \mathcal{H}_i)$ and $T(\hat{\Sigma}_i) = (\hat{X}_i, \hat{X}_{0_i}, \hat{X}_{s_i}, \hat{U}_i, \hat{W}_i, \hat{\mathcal{F}}_i, \hat{Y}_i, \hat{\mathcal{H}}_i)$, for all $i \in [1; N]$, where $\hat{W}_i \subseteq W_i$ and $\hat{Y}_i \subseteq Y_i$. For $\varepsilon_i \in \mathbb{R}_{\geq 0}$, a function $\mathcal{S}_i : X_i \times \hat{X}_i \to \mathbb{R}_{\geq 0}$ is called a local ε_i-InitSOPSF from $T(\Sigma_i)$ to $T(\hat{\Sigma}_i)$ 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) $\forall z_i^0 \in X_{0_i} \cap X_{s_i}$, $\exists \hat{z}_i^0 \in \hat{X}_{0_i} \cap \hat{X}_{s_i}$, s.t. $\mathcal{S}_i(z_i^0, \hat{z}_i^0) \leq \varepsilon_i$;
(b) $\forall \hat{z}_i^0 \in \hat{X}_{0_i} \setminus \hat{X}_{s_i}$, $\exists z_i^0 \in X_{0_i} \setminus X_{s_i}$, s.t. $\mathcal{S}_i(z_i^0, \hat{z}_i^0) \leq \varepsilon_i$;
2 $\forall z_i \in X_i, \forall \hat{z}_i \in \hat{X}_i$, $\alpha_i(\|\mathcal{H}_i(z_i) - \hat{\mathcal{H}}_i(\hat{z}_i)\|) \leq \mathcal{S}_i(z_i, \hat{z}_i)$;
3 $\forall z_i \in X_i, \forall \hat{z}_i \in \hat{X}_i$ s.t. $\mathcal{S}_i(z_i, \hat{z}_i) \leq \varepsilon_i$, $\forall w_i \in W_i$, $\forall \hat{w}_i \in \hat{W}_i$ s.t. $\|w_i - \hat{w}_i\| \leq \vartheta_i$, one has:

(a) $\forall u_i \in U_i, \forall z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$, $\exists \hat{u}_i \in \hat{U}_i$, $\exists \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$ s.t. $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$;
(b) $\forall \hat{u}_i \in \hat{U}_i, \forall \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$, $\exists u_i \in U_i$, $\exists z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$ s.t. $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$.

Note that the local ε_i-InitSOPSFs are mainly proposed for constructing a ε-InitSOPSF for the networks and they are not directly used for deducing approximate initial-state opacity-preserving simulation relation. Similarly, we introduce a notion of local ε_i-CurSOPSFs for subsystems that can be used to establish ε-CurSOPSF for networks of switched systems.

Definition 16. Consider transition systems $T(\Sigma_i) = (X_i, X_{0_i}, X_{s_i}, U_i, W_i, \mathcal{F}_i, Y_i, \mathcal{H}_i)$ and $T(\hat{\Sigma}_i) = (\hat{X}_i, \hat{X}_{0_i}, \hat{X}_{s_i}, \hat{U}_i, \hat{W}_i, \hat{\mathcal{F}}_i, \hat{Y}_i, \hat{\mathcal{H}}_i)$, for all $i \in [1; N]$, where $\hat{W}_i \subseteq W_i$ and $\hat{Y}_i \subseteq Y_i$. For $\varepsilon_i \in \mathbb{R}_{\geq 0}$, a function $\mathcal{S}_i : X_i \times \hat{X}_i \to \mathbb{R}_{\geq 0}$ is called a local ε_i-CurSOPSF from $T(\Sigma_i)$ to $T(\hat{\Sigma}_i)$ if there exist a constant $\vartheta_i \in \mathbb{R}_{\geq 0}$, and a function $\alpha_i \in \mathcal{K}_\infty$ such that

1 $\forall z_i^0 \in X_{0_i}$, $\exists \hat{z}_i^0 \in \hat{X}_{0_i}$, s.t. $\mathcal{S}_i(z_i^0, \hat{z}_i^0) \leq \varepsilon_i$;
2 $\forall z_i \in X_i, \forall \hat{z}_i \in \hat{X}_i$, $\alpha_i(\|\mathcal{H}_i(z_i) - \hat{\mathcal{H}}_i(\hat{z}_i)\|) \leq \mathcal{S}_i(z_i, \hat{z}_i)$;
3 $\forall z_i \in X_i, \forall \hat{z}_i \in \hat{X}_i$ s.t. $\mathcal{S}_i(z_i, \hat{z}_i) \leq \varepsilon_i$, $\forall w_i \in W_i$, $\forall \hat{w}_i \in \hat{W}_i$ s.t. $\|w_i - \hat{w}_i\| \leq \vartheta_i$, one has:

(a) $\forall u_i \in U_i, \forall z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$, $\exists \hat{u}_i \in \hat{U}_i$, $\exists \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$ s.t. $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$;
(b) $\forall u_i \in U_i, \forall z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$ s.t. $z_i^+ \in X_{s_i}$, $\exists \hat{u}_i \in \hat{U}_i$, $\exists \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$ with $\hat{z}_i^+ \in \hat{X}_{s_i}$ s.t. $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$;
(c) $\forall \hat{u}_i \in \hat{U}_i, \forall \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$, $\exists u_i \in U_i$, $\exists z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$ s.t. $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$;
(d) $\forall \hat{u}_i \in \hat{U}_i, \forall \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$ s.t. $\hat{z}_i^+ \in \hat{X}_i \setminus \hat{X}_{s_i}$, $\exists u_i \in U_i$, $\exists z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$ with $z_i^+ \in X_i \setminus X_{s_i}$ s.t. $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$.

We say that $T(\hat{\Sigma}_i)$ is an abstraction of $T(\Sigma_i)$ if there exists a local ε_i-InitSOPSF, or ε_i-CurSOPSF, from $T(\Sigma_i)$ to $T(\hat{\Sigma}_i)$. In addition, if $T(\hat{\Sigma}_i)$ is finite ($\hat{X}_i$ and $\hat{W}_i$ are finite sets), system $T(\hat{\Sigma}_i)$ is called a finite abstraction (symbolic model) of $T(\Sigma_i)$, and is denoted by $T(\Sigma_i) \preceq_L^{\varepsilon_i} T(\hat{\Sigma}_i)$.

Next, we show how to compose the above defined local simulation functions so that it can be used to quantify the distance between two networks.

4.2. Compositional construction of opacity-preserving simulation function

In this subsection, we provide one of the main results of the paper. The following theorem provides a compositional approach for the construction of an opacity-preserving simulation function from $T(\Sigma)$ to $T(\hat{\Sigma})$ via the proposed local ε_i-InitSOPSF (resp. ε_i-CurSOPSF) from $T(\Sigma_i)$ to $T(\hat{\Sigma}_i)$.

Theorem 17. *Consider network $T(\Sigma) = \mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_N))$. Assume that each $T(\Sigma_i)$ admits an abstraction $T(\hat{\Sigma}_i)$ together with a local ε_i-InitSOPSF (resp. ε_i-CurSOPSF) $\mathcal{S}_i$, associated with function α_i and constant ϑ_i as in Definition 15 (resp. Definition 16). Let $\varepsilon = \max_i \varepsilon_i$. If $\forall i \in [1; N]$, $\forall j \in \mathcal{N}_i$,*

$$\alpha_j^{-1}(\varepsilon_j) + \phi_{ij} \leq \vartheta_i, \tag{8}$$

where ϕ_{ij} is an internal input quantization parameter for constructing the local finite abstractions $T(\hat{\Sigma}_i)$, then, function $\mathcal{S} : X \times \hat{X} \to \mathbb{R}_{\geq 0}$ defined as

$$\mathcal{S}(z, \hat{z}) := \max_i \{\frac{\varepsilon}{\varepsilon_i} \mathcal{S}_i(z_i, \hat{z}_i)\}, \tag{9}$$

is an ε-InitSOPSF (resp. ε-CurSOPSF) from $T(\Sigma) = \mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_N))$ to $T(\hat{\Sigma}) = \hat{\mathcal{I}}(T(\hat{\Sigma}_1), \ldots, T(\hat{\Sigma}_N))$.

Proof. First, we show that condition 1(a) in Definition 11 holds. Consider any $z^0 \in X_0 \cap X_S$. For any system $T(\Sigma_i)$ and the corresponding ε_i-InitSOPSF $\mathcal{S}_i$, from the definition of $\mathcal{S}_i$, we have $\forall z_i^0 \in X_{0_i} \cap X_{s_i}$, $\exists \hat{z}_i^0 \in \hat{X}_{0_i} \cap \hat{X}_{s_i}$ s.t. $\mathcal{S}_i(z_i^0, \hat{z}_i^0) \leq \varepsilon_i$. Then, from the definition of $\mathcal{S}$ in (9) we get $\mathcal{S}(z^0, \hat{z}^0) \leq \varepsilon$, where $\hat{z}^0 \in \hat{X}_0 \cap \hat{X}_s$. Thus, condition 1(a) in Definition 11 holds. Condition 1(b) can be proved in the same way, thus is omitted. Now, we show that condition 2 in Definition 11 holds for some $\mathcal{K}_\infty$ function α. Consider any $z = [z_1; \ldots; z_N] \in X$ and $\hat{z} = \left[\hat{z}_1; \ldots; \hat{z}_N\right] \in \hat{X}$. Then, using condition 2 in Definition 15, one gets

$$\begin{aligned}
&\|\mathcal{H}(z) - \hat{\mathcal{H}}(\hat{z})\| = \max_i \{\|\mathcal{H}_{ii}(z_i) - \hat{\mathcal{H}}_{ii}(\hat{z}_i)\|\} \\
&\leq \max_i \{\|\mathcal{H}_i(z_i) - \hat{\mathcal{H}}_i(\hat{z}_i)\|\} \leq \max_i \{\alpha_i^{-1} \circ \mathcal{S}_i(z_i, \hat{z}_i)\} \leq \hat{\alpha} \circ \max_i \{\frac{\varepsilon}{\varepsilon_i} \mathcal{S}_i(z_i, \hat{z}_i)\},
\end{aligned}$$

where $\hat{\alpha} = \max_i\{\alpha_i^{-1}\}$. By defining $\alpha = \hat{\alpha}^{-1}$, one obtains

$$\alpha(\|\mathcal{H}(z) - \hat{\mathcal{H}}(\hat{z})\|) \leq \mathcal{S}(z, \hat{z}),$$

which satisfies condition 2 in Definition 11. Now, we show that condition 3 holds. Let us consider any $z \in X$ and $\hat{z} \in \hat{X}$ such that $\mathcal{S}(z, \hat{z}) \leq \varepsilon$. It can be seen that from the structure of $\mathcal{S}$ in (9), we get $\mathcal{S}_i(z_i, \hat{z}_i) \leq \varepsilon_i$, $\forall i \in [1; N]$. For each pair of systems $T(\Sigma_i)$ and $T(\hat{\Sigma}_i)$, the internal inputs satisfy the chain of inequality

$$\begin{aligned}
&\|w_i - \hat{w}_i\| = \max_{j\in\mathcal{N}_i}\{\|w_{ij} - \hat{w}_{ij}\|\} = \max_{j\in\mathcal{N}_i}\{\|y_{ji} - \hat{y}_{ji} + \hat{y}_{ji} - \hat{w}_{ij}\|\}\\
&\leq \max_{j\in\mathcal{N}_i}\{\|y_{ji} - \hat{y}_{ji}\| + \phi_{ij}\} \leq \max_{j\in\mathcal{N}_i}\{\|\mathcal{H}_j(z_j) - \hat{\mathcal{H}}_j(\hat{z}_j)\| + \phi_{ij}\}\\
&\leq \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1} \circ \mathcal{S}_j(z_j, \hat{z}_j) + \phi_{ij}\} \leq \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j) + \phi_{ij}\}.
\end{aligned}$$

Using (8), one has $\|w_i - \hat{w}_i\| \leq \vartheta_i$. Therefore, by condition 3(a) in Definition 15, for each pair of systems $T(\Sigma_i)$ and $T(\hat{\Sigma}_i)$, one has $\forall u_i \in U_i$, $\forall z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$, there exists $\hat{u}_i \in \hat{U}_i$ and $\hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$ such that $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$. As a result, we get $\forall u = [u_1; \ldots; u_N] \in U$, $\forall z^+ \in \mathcal{F}(z, u)$, there exists $\hat{u} = \left[\hat{u}_1; \ldots; \hat{u}_N\right] \in \hat{U}$ and $\hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$ such that $\mathcal{S}(z^+, \hat{z}^+) = \max_i\{\frac{\varepsilon}{\varepsilon_i}\mathcal{S}_i(z_i^+, \hat{z}_i^+)\} \leq \varepsilon$. Therefore, condition 3(a) in Definition 11 is satisfied with $\varepsilon = \max_i \varepsilon_i$. In addition, by condition 3(b) in Definition 15, for each pair of systems $T(\Sigma_i)$ and $T(\hat{\Sigma}_i)$, one has $\forall \hat{u}_i \in \hat{U}_i$, $\forall \hat{z}_i^+ \in \hat{\mathcal{F}}_i(\hat{z}_i, \hat{u}_i, \hat{w}_i)$, there exists $u_i \in U_i$ and $z_i^+ \in \mathcal{F}_i(z_i, u_i, w_i)$ such that $\mathcal{S}_i(z_i^+, \hat{z}_i^+) \leq \varepsilon_i$. As a result, we get $\forall \hat{u} = \left[\hat{u}_1; \ldots; \hat{u}_N\right] \in \hat{U}$, $\forall \hat{z}^+ \in \hat{\mathcal{F}}(\hat{z}, \hat{u})$, there exists $u = [u_1; \ldots; u_N] \in U$ and $z^+ \in \mathcal{F}(z, u)$ such that $\mathcal{S}(z^+, \hat{z}^+) = \max_i\{\frac{\varepsilon}{\varepsilon_i}\mathcal{S}_i(z_i^+, \hat{z}_i^+)\} \leq \varepsilon$. It follows that condition 3(b) in Definition 11 is satisfied as well. Therefore, we conclude that $\mathcal{S}$ is an ε-InitSOPSF from $T(\Sigma) = \mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_N))$ to $T(\hat{\Sigma}) = \hat{\mathcal{I}}(T(\hat{\Sigma}_1), \ldots, T(\hat{\Sigma}_N))$. Note that by following similar lines of reasoning as above, one can prove that $\mathcal{S}$ is also an ε-CurSOPSF from $T(\Sigma) = \mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_N))$ to $T(\hat{\Sigma}) = \hat{\mathcal{I}}(T(\hat{\Sigma}_1), \ldots, T(\hat{\Sigma}_N))$. □

Till here, we have seen that one can construct an abstraction of a network of switched systems by interconnecting local abstractions of the subsystems. The overall InitSOPSF (resp. CurSOPSF) between two networks is established by composing local InitSOPSFs (resp. local CurSOPSFs) as well. This abstract network satisfies Definition 11 or Definition 12, which allows us to check approximate opacity property over the simpler abstract network and carry the results back to the concrete network using the results provided in Corollary 14.

Next, we are going to impose certain conditions on the dynamics of the subsystems, such that one can construct proper abstractions for all of the subsystems together with the corresponding local InitSOPSFs or CurSOPSFs.

5. Construction of finite abstractions

In this section, we are going to explore how to construct finite abstractions together with local InitSOPSFs or CurSOPSFs for subsystems. The dt-SS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, \mathbb{W}, F, \mathbb{Y}, h)$ are assumed to be infinite and deterministic. Moreover, we assume the output map h satisfies the following general Lipschitz assumption: there exists an $\ell \in \mathcal{K}_\infty$ such that: $\|h(x) - h(y)\| \leq \ell(\|x - y\|)$ for all $x, y \in \mathbb{X}$. Here, we also use Σ_p to denote a dt-SS Σ in (1) with constant switching signal $\mathfrak{p}(k) = p$, $\forall k \in \mathbb{N}$.

5.1. Construction of local finite abstractions

Note that throughout this subsection, we are mainly talking about switched subsystems rather than the overall network. However, for the sake of better readability, we omit index i of subsystems throughout the text in this subsection, e.g., we write $T(\Sigma)$ instead of $T(\Sigma_i)$.

Here, we establish a local ε-InitSOPSF or ε-CurSOPSF between $T(\Sigma)$ and its finite abstraction by assuming that, for all $p \in P$, Σ_p is incrementally input-to-state stable (δ-ISS) [28] as defined next.

Definition 18. System Σ_p is δ-ISS if there exist so-called δ-ISS Lyapunov functions $V_p : \mathbb{X} \times \mathbb{X} \to \mathbb{R}_{\geq 0}$, $\underline{\alpha}_p, \overline{\alpha}_p, \rho_p \in \mathcal{K}_\infty$, and constant $0 < \kappa_p < 1$, such that for all $x, \hat{x} \in \mathbb{X}$, and for all $w, \hat{w} \in \mathbb{W}$

$$\underline{\alpha}_p(\| x - \hat{x} \|) \leq V_p(x, \hat{x}) \leq \overline{\alpha}_p(\|x - \hat{x}\|), \tag{10}$$

$$V_p(f_p(x, w), f_p(\hat{x}, \hat{w})) \leq \kappa_p V_p(x, \hat{x}) + \rho_p(\|w - \hat{w}\|). \tag{11}$$

Remark 19. We say that V_p, $\forall p \in P$, are multiple δ-ISS Lyapunov functions for subsystem Σ if it satisfies (10) and (11). Moreover, if $V_p = V_{p^+}$, $\forall p, p^+ \in P$, we omit the index p in (10), (11), and say that V is a common δ-ISS Lyapunov function for system Σ. We refer interested readers to [22] for more details on common and multiple Lyapunov functions for switched systems.

Next, we provide an approach, inspired by [29], to construct a local finite abstraction $T(\hat{\Sigma})$ of transition system $T(\Sigma)$ associated to the switched subsystem Σ in which each mode Σ_p is δ-ISS.

Definition 20. Consider a transition system $T(\Sigma) = (X, X_0, X_s, U, W, \mathcal{F}, Y, \mathcal{H})$, associated to the switched subsystem $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, \mathbb{W}, F, \mathbb{Y}, h)$, where $\mathbb{X}, \mathbb{W}$ are assumed to be finite unions of boxes. Let Σ_p be δ-ISS as in Definition 18. Then one can construct a finite abstraction $T(\hat{\Sigma}) = (\hat{X}, \hat{X}_0, \hat{X}_s, \hat{U}, \hat{W}, \hat{\mathcal{F}}, \hat{Y}, \hat{\mathcal{H}})$ where:

- $\hat{X} = \hat{\mathbb{X}} \times P \times \{0, \ldots, k_d - 1\}$, where $\hat{\mathbb{X}} = [\mathbb{X}]_\eta$ and $0 < \eta \leq \min\{span(\mathbb{X}_s), span(\mathbb{X} \setminus \mathbb{X}_s)\}$ is the state set quantization parameter;
- $\hat{X}_0 = \hat{\mathbb{X}}_0 \times P \times \{0\}$, where $\hat{\mathbb{X}}_0 = [\mathbb{X}_0]_\eta$;
- $\hat{X}_s = \hat{\mathbb{X}}_s \times P \times \{0, \ldots, k_d - 1\}$, where $\hat{\mathbb{X}}_s = [\mathbb{X}_s^\theta]_\eta$, and $\mathbb{X}_s^\theta = \{x \in \mathbb{X} \mid \exists \bar{x} \in \mathbb{X}_s, \|x - \bar{x}\| \leq \theta\}$ denotes the θ-expansion of set $\mathbb{X}_s$ where $\theta > 0$ is a design parameter;
- $\hat{U} = U = P$;
- $(\hat{x}^+, p^+, l^+) \in \hat{\mathcal{F}}((\hat{x}, p, l), \hat{u}, \hat{w})$ if and only if $\|f_p(\hat{x}, \hat{w}) - \hat{x}^+\| \leq \eta$, $\hat{u} = p$ and one of the following scenarios hold:
  - $l < k_d - 1$, $p^+ = p$ and $l^+ = l + 1$;
  - $l = k_d - 1$, $p^+ = p$ and $l^+ = k_d - 1$;
  - $l = k_d - 1$, $p^+ \neq p$ and $l^+ = 0$;
- $\hat{Y} = \{\mathcal{H}(\hat{x}, p, l) | (\hat{x}, p, l) \in \hat{X}\}$;
- $\hat{\mathcal{H}} : \hat{X} \to \hat{Y}$, defined as $\hat{\mathcal{H}}(\hat{x}, p, l) = \mathcal{H}(\hat{x}, p, l) = h(\hat{x})$;
- $\hat{W} = [\mathbb{W}]_\phi$, where ϕ, satisfying $0 < \|\phi\| \leq span(\mathbb{W})$, is the internal input set quantization parameter.

Note that in the case when the concrete switched subsystem Σ admits a common δ-ISS Lyapunov function as in Remark 19, Definition 20 boils down to the following.

Definition 21. Consider a transition system $T(\Sigma) = (X, X_0, X_s, U, W, \mathcal{F}, Y, \mathcal{H})$, associated to the switched subsystem $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, \mathbb{W}, F, \mathbb{Y}, h)$, where $\mathbb{X}, \mathbb{W}$ are assumed to be finite unions of boxes. Suppose Σ admits a common δ-ISS Lyapunov function as in Remark 19. Then one can construct a finite abstraction $T(\hat{\Sigma}) = (\hat{X}, \hat{X}_0, \hat{X}_s, \hat{U}, \hat{W}, \hat{\mathcal{F}}, \hat{Y}, \hat{\mathcal{H}})$ where:

- $\hat{X} = [\mathbb{X}]_\eta$, where $0 < \eta \leq \min\{span(\mathbb{X}_s), span(\mathbb{X} \setminus \mathbb{X}_s)\}$ is the state set quantization parameter;
- $\hat{X}_0 = [\mathbb{X}_0]_\eta$;
- $\hat{X}_s = [\mathbb{X}_s^\theta]_\eta$, 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 set $\mathbb{X}_s$ where $\theta > 0$ is a design parameter;
- $\hat{U} = P$;
- $\hat{x}^+ \in \hat{\mathcal{F}}(\hat{x}, \hat{u}, \hat{w})$ if and only if $\|f_{\hat{u}}(\hat{x}, \hat{w}) - \hat{x}^+\| \leq \eta$;
- $\hat{Y} = \{h(\hat{x}) | \hat{x} \in \hat{X}\}$;
- $\hat{\mathcal{H}} : \hat{X} \to \hat{Y}$, defined as $\hat{\mathcal{H}}(\hat{x}) = h(\hat{x})$;
- $\hat{W} = [\mathbb{W}]_\phi$, where ϕ, satisfying $0 < \|\phi\| \leq span(\mathbb{W})$, is the internal input set quantization parameter.

In order to construct a local ε-InitSOPSF or ε-CurSOPSF from $T(\Sigma)$ to $T(\hat{\Sigma})$, we raise the following assumptions on functions V_p appeared in Definition 18, which are used to prove some of the main results later.

Assumption 22. There exists $\mu \geq 1$ such that

$$\forall x, y \in \mathbb{X}, \quad \forall p, q \in P, \quad V_p(x, y) \leq \mu V_q(x, y). \tag{12}$$

Assumption 22 is an incremental version of a similar assumption in [30] that is used to prove input-to-state stability of switched systems under constrained switching signals.

Assumption 23. For all $p \in P$, there exists a $\mathcal{K}_\infty$ function γ_p such that

$$\forall x, y, z \in \mathbb{X}, \quad V_p(x, y) \leq V_p(x, z) + \gamma_p(\|y - z\|). \tag{13}$$

Assumption 23 is non-restrictive as shown in [31] provided that one is interested to work on a compact subset of $\mathbb{X}$.

Now, we establish the relation between $T(\Sigma)$ and $T(\hat{\Sigma})$, introduced above, via the notion of local ε-InitSOPSF as in Definition 15.

Theorem 24. *Consider a dt-SS $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, \mathbb{W}, F, \mathbb{Y}, h)$ with its equivalent transition system $T(\Sigma) = (X, X_0, X_s, U, W, \mathcal{F}, Y, \mathcal{H})$. Suppose Σ_p is δ-ISS as in Definition 18, with a function V_p equipped with functions $\underline{\alpha}_p, \overline{\alpha}_p, \rho_p$ and constant κ_p, and Assumptions 22 and 23 hold. Let $\epsilon > 1$. For any design parameters $\varepsilon, \vartheta \in \mathbb{R}_{>0}$, let $T(\hat{\Sigma})$ be a finite abstraction of $T(\Sigma)$ constructed as in Definition 20 with any quantization parameter $\eta \in \mathbb{R}_{>0}$ satisfying*

$$\eta \leq \min\{\hat{\gamma}^{-1}((1 - \kappa)\varepsilon - \rho(\vartheta)), \overline{\alpha}^{-1}(\varepsilon)\}, \tag{14}$$

where $\kappa = \max_{p\in P}\left\{\kappa_p^{\frac{\epsilon-1}{\epsilon}}\right\}$, $\rho = \max_{p\in P}\left\{\kappa_p^{-\frac{k_d}{\epsilon}}\rho_p\right\}$, $\hat{\gamma} = \max_{p\in P}\left\{\kappa_p^{-\frac{k_d}{\epsilon}}\gamma_p\right\}$, $\overline{\alpha} = \max_{p\in P}\left\{\kappa_p^{-\frac{l}{\epsilon}}\overline{\alpha}_p\right\}$. *If,* $\forall p \in P$, $k_d \geq \epsilon\frac{\ln(\mu)}{\ln(\frac{1}{\kappa_p})} + 1$, *then function* $\mathcal{V}$ *defined as*

$$\mathcal{V}((x,p,l),(\hat{x},p,l)) := V_p(x,\hat{x})\kappa_p^{\frac{-l}{\epsilon}}, \tag{15}$$

is a local ε*-InitSOPSF from* $T(\Sigma)$ *to* $T(\hat{\Sigma})$ *and from* $T(\hat{\Sigma})$ *to* $T(\Sigma)$.

Proof. We start by proving condition 1 in Definition 15. Consider any initial and secret state $(x^0,p^0,0) \in X_0 \cap X_s$ in $T(\Sigma)$. From Definition 20, for every $(x^0,p^0,0) \in X_0 \cap X_s$, there always exists $(\hat{x}^0,p^0,0) \in \hat{X}_0 \cap \hat{X}_s$ such that $\|x^0 - \hat{x}^0\| \leq \eta$. Hence, using (10), there exists $(\hat{x}^0,p^0,0) \in \hat{X}_0 \cap \hat{X}_s$ with $\mathcal{V}((x^0,p^0,0),(\hat{x}^0,p^0,0)) \leq \frac{\overline{\alpha}_p(\|x^0-\hat{x}^0\|)}{\kappa_p^{\frac{l}{\epsilon}}} \leq \frac{\overline{\alpha}_p(\eta)}{\kappa_p^{\frac{l}{\epsilon}}}$, and condition 1(a) is satisfied with $\overline{\alpha} = \max_{p\in P}\left\{\kappa_p^{-\frac{l}{\epsilon}}\overline{\alpha}_p\right\}$ and $\overline{\alpha}(\eta) \leq \varepsilon$ by (14). For every $(\hat{x}^0,p^0,0) \in \hat{X}_0 \setminus \hat{X}_s$, by choosing $x^0 = \hat{x}^0$ with $(x^0,p^0,0)$ also being inside $X_0 \setminus X_s$, we get $\mathcal{V}((x^0,p^0,0),(\hat{x}^0,p^0,0)) = 0 \leq \varepsilon$. Hence, condition 1(b) in Definition 15 holds as well.

Next, we show condition 2 in Definition 15 holds. Given the Lipschitz assumption on h and since, $\forall p \in P$, Σ_p is δ-ISS, from (10), $\forall(x,p,l) \in X$ and $\forall(\hat{x},p,l) \in \hat{X}$, we have

$$\begin{aligned}
&\|\mathcal{H}(x,p,l) - \hat{\mathcal{H}}(\hat{x},p,l)\| = \|h(x) - \hat{h}(\hat{x})\| \leq \ell(\|x-\hat{x}\|)\\
&\leq \ell \circ \underline{\alpha}_p^{-1}(V_p(x,\hat{x})) = \ell \circ \underline{\alpha}_p^{-1}\left(\kappa_p^{\frac{l}{\epsilon}}\mathcal{V}((x,p,l),(\hat{x},p,l))\right)\\
&\leq \ell \circ \underline{\alpha}_p^{-1}\left(\mathcal{V}((x,p,l),(\hat{x},p,l))\right) \leq \hat{\alpha}\left(\mathcal{V}((x,p,l),(\hat{x},p,l))\right),
\end{aligned}$$

where $\hat{\alpha} = \max_{p\in P}\{\ell \circ \underline{\alpha}_p^{-1}\}$. By defining $\alpha = \hat{\alpha}^{-1}$, one obtains

$$\alpha(\|\mathcal{H}(x,p,l) - \hat{\mathcal{H}}(\hat{x},p,l)\|) \leq \mathcal{V}((x,p,l),(\hat{x},p,l)),$$

satisfying condition 2. Now we show condition 3 in Definition 15. From (13), $\forall x \in \mathbb{X}$, $\forall \hat{x} \in \hat{\mathbb{X}}$, $\forall w \in W$, $\forall \hat{w} \in \hat{W}$, we have

$$V_p(f_p(x,w),\hat{x}^+) \leq V_p(f_p(x,w),f_p(\hat{x},\hat{w})) + \gamma_p(\|\hat{x}^+ - f_p(\hat{x},\hat{w})\|),$$

for any $\hat{x}^+$ such that $(\hat{x}^+,p^+,l^+) \in \hat{\mathcal{F}}((\hat{x},p,l),\hat{u},\hat{w})$. Now, from Definition 20, the above inequality reduces to

$$V_p(f_p(x,w),\hat{x}^+) \leq V_p(f_p(x,w),f_p(\hat{x},\hat{w})) + \gamma_p(\eta).$$

Note that by (11), one gets

$$V_p(f_p(x,w),f_p(\hat{x},\hat{w})) \leq \kappa_p V_p(x,\hat{x}) + \rho_p(\|w-\hat{w}\|).$$

Hence, $\forall x \in \mathbb{X}$, $\forall \hat{x} \in \hat{\mathbb{X}}$, $\forall w \in W$, $\forall \hat{w} \in \hat{W}$, one obtains

$$V_p(f_p(x,w),\hat{x}^+) \leq \kappa_p V_p(x,\hat{x}) + \rho_p(\|w-\hat{w}\|) + \gamma_p(\eta), \tag{16}$$

for any $\hat{x}^+$ such that $(\hat{x}^+,p^+,l^+) \in \hat{\mathcal{F}}((\hat{x},p,l),\hat{u},\hat{w})$. Now, in order to show function $\mathcal{V}$ defined in (15) satisfies condition 3 in Definition 15, we consider the different scenarios in Definition 20:

- $l < k_d - 1$, $p^+ = p$ and $l^+ = l+1$, using (16) and $k_d > l+1$, we have

$$\begin{aligned}
&\mathcal{V}((x^+,p^+,l^+),(\hat{x}^+,p^+,l^+)) = \frac{V_{p^+}(x^+,\hat{x}^+)}{\kappa_p^{\frac{l^+}{\epsilon}}} = \frac{V_p(f_p(x,w),\hat{x}^+)}{\kappa_p^{\frac{l+1}{\epsilon}}}\\
&\leq \frac{\kappa_p V_p(x,\hat{x}) + \rho_p(\|w-\hat{w}\|) + \gamma_p(\eta)}{\kappa_p^{\frac{l+1}{\epsilon}}} = \frac{\kappa_p}{\kappa_p^{\frac{1}{\epsilon}}}\frac{V_p(x,\hat{x})}{\kappa_p^{\frac{l}{\epsilon}}} + \frac{\rho_p(\|w-\hat{w}\|) + \gamma_p(\eta)}{\kappa_p^{\frac{l+1}{\epsilon}}}\\
&\leq \kappa_p^{\frac{\epsilon-1}{\epsilon}}\mathcal{V}((x,p,l),(\hat{x},p,l)) + \frac{\rho_p(\|w-\hat{w}\|) + \gamma_p(\eta)}{\kappa_p^{\frac{k_d}{\epsilon}}}.
\end{aligned}$$

- $l = k_d - 1$, $p^+ = p$ and $l^+ = k_d - 1$, using (16) and $\frac{\epsilon-1}{\epsilon} < 1$, one gets

$$\begin{aligned}
&\mathcal{V}((x^+,p^+,l^+),(\hat{x}^+,p^+,l^+)) = \frac{V_{p^+}(x^+,\hat{x}^+)}{\kappa_p^{\frac{l^+}{\epsilon}}} = \frac{V_p(f_p(x,w),\hat{x}^+)}{\kappa_p^{\frac{l}{\epsilon}}}\\
&\leq \frac{\kappa_p V_p(x,\hat{x}) + \rho_p(\|w-\hat{w}\|) + \gamma_p(\eta)}{\kappa_p^{\frac{l}{\epsilon}}} = \kappa_p\frac{V_p(x,\hat{x})}{\kappa_p^{\frac{l}{\epsilon}}} + \frac{\rho_p(\|w-\hat{w}\|) + \gamma_p(\eta)}{\kappa_p^{\frac{l}{\epsilon}}}
\end{aligned}$$

$$\leq \kappa_p^{\frac{\epsilon-1}{\epsilon}} \mathcal{V}((x,p,l),(\hat{x},p,l)) + \frac{\rho_p(\|w-\hat{w}\|)+\gamma_p(\eta)}{\kappa_p^{\frac{k_d}{\epsilon}}}.$$

- $l = k_d - 1$, $p^+ \neq p$ and $l^+ = 0$, using (16), $\mu\kappa_p^{\frac{k_d-1}{\epsilon}} \leq 1$, and $\frac{\epsilon-1}{\epsilon} < 1$, one has

$$\mathcal{V}((x^+,p^+,l^+),(\hat{x}^+,p^+,l^+)) = \frac{V_{p^+}(x^+,\hat{x}^+)}{\kappa_{p^+}^{\frac{l^+}{\epsilon}}} \leq \mu V_p(f_p(x,w),\hat{x}^+)$$

$$\leq \frac{\mu\kappa_p^{\frac{k_d-1}{\epsilon}}\left(\kappa_p V_p(x,\hat{x}) + \rho_p(\|w-\hat{w}\|)+\gamma_p(\eta)\right)}{\kappa_p^{\frac{k_d-1}{\epsilon}}}$$

$$= \kappa_p \frac{V_p(x,\hat{x})}{\kappa_p^{\frac{l}{\epsilon}}} + \frac{\rho_p(\|w-\hat{w}\|)+\gamma_p(\eta)}{\kappa_p^{\frac{l}{\epsilon}}}$$

$$\leq \kappa_p^{\frac{\epsilon-1}{\epsilon}} \mathcal{V}((x,p,l),(\hat{x},p,l)) + \frac{\rho_p(\|w-\hat{w}\|)+\gamma_p(\eta)}{\kappa_p^{\frac{k_d}{\epsilon}}}.$$

Note that $\forall p \in P$, $\mu\kappa_p^{\frac{k_d-1}{\epsilon}} \leq 1$, since $\forall p \in P$, $k_d \geq \epsilon\frac{\ln(\mu)}{\ln(\frac{1}{\kappa_p})} + 1$. Hence, $\forall (x,p,l) \in X$, $\forall (\hat{x},p,l) \in \hat{X}$, $\forall w \in W$, $\forall \hat{w} \in \hat{W}$, one gets

$$\mathcal{V}((x^+,p^+,l^+),(\hat{x}^+,p^+,l^+)) \leq \kappa\mathcal{V}((x,p,l),(\hat{x},p,l)) + \rho(\|w-\hat{w}\|) + \hat{\gamma}(\eta). \tag{17}$$

Now, we show the condition 3(a) in Definition 15 holds. Let us consider any pair of states $(x,p,l) \in X$, $(\hat{x},p,l) \in \hat{X}$, satisfying $\mathcal{V}((x,p,l),(\hat{x},p,l)) \leq \varepsilon$, and any $w \in W$, $\hat{w} \in \hat{W}$ such that $\|w-\hat{w}\| \leq \vartheta$. Combining (17) with (14) for any $(x^+,p^+,l^+) \in \mathcal{F}((x,p,l),u,w)$ and any $(\hat{x}^+,p^+,l^+) \in \hat{\mathcal{F}}((\hat{x},p,l),\hat{u},\hat{w})$ with $\hat{u} = u$, one obtains:

$$\mathcal{V}((x^+,p^+,l^+),(\hat{x}^+,p^+,l^+)) \leq \kappa\varepsilon + \rho(\vartheta) + \hat{\gamma}(\hat{\gamma}^{-1}((1-\kappa)\varepsilon - \rho(\vartheta))) = \varepsilon, \tag{18}$$

which shows that condition 3(a) is satisfied. Similarly, for any $(\hat{x}^+,p^+,l^+) \in \hat{\mathcal{F}}((\hat{x},p,l),\hat{u},\hat{w})$, condition 3(b) is also satisfied using the same reasoning with $(x^+,p^+,l^+) \in \mathcal{F}((x,p,l),\hat{u},w)$. Therefore, we conclude that $\mathcal{V}$ is a local ε-InitSOPSF from $T(\Sigma)$ to $T(\hat{\Sigma})$. Similarly, one can show that $\mathcal{V}$ is a also a local ε-InitSOPSF from $T(\hat{\Sigma})$ to $T(\Sigma)$. □

Note that a similar framework for constructing symbolic models of switched systems was first proposed in [29], where the results take a monolithic view of the concrete switched systems without considering the distinction between internal and external inputs and outputs. However, their distinction plays an important role in our proposed compositional scheme which allows us to build symbolic models for switched subsystems individually and then construct a symbolic model for the overall network by interconnecting those local ones.

Next, we provide a similar result as in Theorem 24, but tailored to approximate current-state opacity.

Theorem 25. *Consider a dt-SS $\Sigma = (\mathbb{X},\mathbb{X}_0,\mathbb{X}_s,P,\mathbb{W},F,\mathbb{Y},h)$ with its equivalent transition system $T(\Sigma) = (X,X_0,X_s,U,W,\mathcal{F},Y,\mathcal{H})$. Suppose Σ_p is δ-ISS as in Definition 18, with a function V_p equipped with functions $\underline{\alpha}_p,\overline{\alpha}_p,\rho_p$ and constant κ_p, and Assumptions 22 and 23 hold. Let $\epsilon > 1$. For any design parameters $\varepsilon,\vartheta \in \mathbb{R}_{\geq 0}$, let $T(\hat{\Sigma})$ be a finite abstraction of $T(\Sigma)$ constructed as in Definition 20 with any quantization parameters $\eta \in \mathbb{R}_{>0}$ and $\theta \in \mathbb{R}_{>0}$ satisfying*

$$\eta \leq \min\{\hat{\gamma}^{-1}((1-\kappa)\varepsilon - \rho(\vartheta)), \overline{\alpha}^{-1}(\varepsilon)\}; \tag{19}$$

$$\underline{\alpha}^{-1}(\varepsilon) \leq \theta, \tag{20}$$

where $\kappa = \max_{p\in P}\left\{\kappa_p^{\frac{\epsilon-1}{\epsilon}}\right\}$, $\rho = \max_{p\in P}\left\{\kappa_p^{-\frac{k_d}{\epsilon}}\rho_p\right\}$, $\hat{\gamma} = \max_{p\in P}\left\{\kappa_p^{-\frac{k_d}{\epsilon}}\gamma_p\right\}$, $\overline{\alpha} = \max_{p\in P}\left\{\kappa_p^{-\frac{l}{\epsilon}}\overline{\alpha}_p\right\}$, $\underline{\alpha} = \min_{p\in P}\left\{\kappa_p^{-\frac{l}{\epsilon}}\underline{\alpha}_p\right\}$. If, $\forall p \in P$, $k_d \geq \epsilon\frac{\ln(\mu)}{\ln(\frac{1}{\kappa_p})} + 1$, then function $\mathcal{V}$ defined as

$$\mathcal{V}((x,p,l),(\hat{x},p,l)) := V_p(x,\hat{x})\kappa_p^{\frac{-l}{\epsilon}}, \tag{21}$$

is a local ε-CurSOPSF from $T(\Sigma)$ to $T(\hat{\Sigma})$.

Proof. We start by proving condition 1 in Definition 16. Consider any initial state $(x^0,p^0,0) \in X_0$ in $T(\Sigma)$. Note that from Definition 20, we have $\hat{X}_0 = \hat{\mathbb{X}}_0 \times P \times \{0\}$, where $\hat{\mathbb{X}}_0 = [\mathbb{X}_0]_\eta$. Therefore, for every $(x^0,p^0,0) \in X_0$, there always exists $(\hat{x}^0,p^0,0) \in \hat{X}_0$ such that $\|x^0-\hat{x}^0\| \leq \eta$. Hence, one gets $\mathcal{V}((x^0,p^0,0),(\hat{x}^0,p^0,0)) \leq \frac{\overline{\alpha}_p(\|x^0-\hat{x}^0\|)}{\kappa_p^{\frac{l}{\epsilon}}} \leq \frac{\overline{\alpha}_p(\eta)}{\kappa_p^{\frac{l}{\epsilon}}}$ by (10), and condition 1 is satisfied with $\overline{\alpha} = \max_{p\in P}\left\{\kappa_p^{-\frac{l}{\epsilon}}\overline{\alpha}_p\right\}$ and $\overline{\alpha}(\eta) \leq \varepsilon$ by (19). The proof for conditions 2, 3(a), and 3(c) in Definition 16 is similar to that of Theorem 24, and is omitted here.

For condition 3(b), let us consider any $u \in U$ s.t. $(x^+, p^+, l^+) \in X_s$. By choosing $\hat{u} = u$ and following same reasoning as in Theorem 24, we obtain $\mathcal{V}((x^+, p^+, l^+), (\hat{x}^+, p^+, l^+)) \leq \varepsilon$. Additionally, by combining (10) and (21), one gets

$$\|x^+ - \hat{x}^+\| \overset{(10)}{\leq} \underline{\alpha}_p^{-1}(V_p(x^+, \hat{x}^+)) \overset{(21)}{=} \underline{\alpha}_p^{-1}\kappa_p^{\frac{l}{\epsilon}}(\mathcal{V}((x^+, p^+, l^+), (\hat{x}^+, p^+, l^+))) \leq \underline{\alpha}^{-1}(\varepsilon),$$

where $\underline{\alpha} = \min_{p\in P}\left\{\kappa_p^{-\frac{l}{\epsilon}}\underline{\alpha}_p\right\}$. Moreover, by (20), one gets $\|x^+ - \hat{x}^+\| \leq \underline{\alpha}^{-1}(\varepsilon) \leq \theta$. Note that by the structure of the abstraction as in Definition 20, we have $\hat{X}_s = \hat{\mathbb{X}}_s \times P \times \{0, \ldots, k_d - 1\}$ where $\hat{\mathbb{X}}_s = [\mathbb{X}_s^\theta]_\eta$ and $\mathbb{X}_s^\theta = \{x \in \mathbb{X} \mid \exists \bar{x} \in \mathbb{X}_s, \|x - \bar{x}\| \leq \theta\}$. This implies that $(\hat{x}^+, p^+, l^+) \in \hat{X}_s$, and thus, condition 3(b) is satisfied as well. Condition 3(d) of Definition 16 can be proved in a similar way and is omitted here. Therefore, we conclude that $\mathcal{V}$ is a local ε-CurSOPSF from $T(\Sigma)$ to $T(\hat{\Sigma})$. □

Remark 26. If Σ admits a common δ-ISS Lyapunov function satisfying Assumption 23, then functions $\mathcal{V}$ defined in Theorems 24 and 25 reduce to $\mathcal{V}((x, p, l), (\hat{x}, p, l)) := V(x, \hat{x})$.

Given the results of Theorems 17 and 24 (resp. 25), one can see that conditions (8) and (14) (resp. (19)) may not hold at the same time. In the following subsection, we will discuss about the inherent property that the network should have such that one can design suitable quantization parameters to satisfy conditions (8) and (14) (resp. (19)) simultaneously.

5.2. Compositionality result

We raise the following assumption which provides a small-gain type condition, inspired by [32, Theorem 5.2], so that one can verify whether the competing conditions (8) and (14) (resp. (19)) can be satisfied simultaneously.

Assumption 27. Consider network $\mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_N))$ induced by $N \in \mathbb{N}_{\geq 1}$ transition systems $T(\Sigma_i)$. Assume that each $T(\Sigma_i)$ and its finite abstraction $T(\hat{\Sigma}_i)$ admit a local ε_i-InitSOPSF (resp. ε_i-CurSOPSF) $\mathcal{V}_i$ defined in (15) (resp. (21)), associated with functions and constants κ_i, α_i, and ρ_i that appeared in Theorem 24 (resp. Theorem 25). Define

$$\gamma_{ij} := \begin{cases} (1-\kappa_i)^{-1}\rho_i \circ \alpha_j^{-1} & \text{if } j \in \mathcal{N}_i, \\ 0 & \text{otherwise}, \end{cases} \tag{22}$$

for all $i, j \in [1; N]$, and assume that functions γ_{ij} defined in (22) satisfy

$$\gamma_{i_1 i_2} \circ \gamma_{i_2 i_3} \circ \cdots \circ \gamma_{i_{r-1} i_r} \circ \gamma_{i_r i_1} < \mathcal{I}_d, \tag{23}$$

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

Now, we show that, under the above small-gain assumption, one can always compositionally design local quantization parameters to satisfy conditions (8) and (14) (resp. (19)) simultaneously.

Theorem 28. *Suppose that Assumption 27 holds. Then, there always exist local quantization parameters η_i and ϕ_{ij}, $\forall i, j \in [1; N]$, as designed in Algorithm 1, such that (8) and (14) (resp. (19)) can be satisfied simultaneously.*

Proof. First, let us note that the small-gain condition (23) implies that $\exists \sigma_i \in \mathcal{K}_\infty$ satisfying $\forall i \in [1; N]$,

$$\max_{j\in\mathcal{N}_i}\{\gamma_{ij} \circ \sigma_j\} < \sigma_i, \tag{24}$$

see [32, Theorem 5.2]. Then, from (22), we have $\forall i \in [1; N]$,

$$\begin{aligned} &\max_{j\in\mathcal{N}_i}\{\gamma_{ij} \circ \sigma_j\} < \sigma_i \Longrightarrow \max_{j\in\mathcal{N}_i}\{(1-\kappa_i)^{-1}\rho_i \circ \alpha_j^{-1} \circ \sigma_j\} < \sigma_i \\ &\Longrightarrow \rho_i \circ \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1} \circ \sigma_j\} < (1-\kappa_i)\sigma_i. \end{aligned} \tag{25}$$

Next, suppose that we are given a sequence of functions $\sigma_i \in \mathcal{K}_\infty$, $\forall i \in [1; N]$, satisfying (24). Assume we are given any desired precision ε as in Definition 11. Let us set $\varepsilon_i = \sigma_i(r)$, $\forall i \in [1; N]$, where $r \in \mathbb{R}_{>0}$ is chosen such that $\max_i\{\sigma_i(r)\} = \varepsilon$. Then, we choose internal input quantization parameters ϕ_{ij}, $\forall i, j \in [1; N]$, such that

$$\max_{j\in\mathcal{N}_i}\{\phi_{ij}\} < \rho_i^{-1}((1-\kappa_i)\varepsilon_i) - \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j)\}. \tag{26}$$

Now, by setting $\vartheta_i = \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j) + \phi_{ij}\}$, and combining (25) and (26), one has $\forall i \in [1; N]$

$$\rho_i(\vartheta_i) = \rho_i(\max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j) + \phi_{ij}\}) \leq \rho_i(\max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j) + \max_{j\in\mathcal{N}_i}\{\phi_{ij}\}\}) < (1-\kappa_i)\varepsilon_i. \tag{27}$$

Thus, by (27), given any pair of parameters $(\varepsilon_i, \vartheta_i)$, one can always find suitable local parameters η_i to satisfy (14) (resp. (19)). Additionally, the selection of $\vartheta_i = \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j) + \phi_{ij}\}$ ensures that (8) is satisfied as well, which concludes the proof. □

Algorithm 1: Compositional design of local quantization parameters $\eta_i \in \mathbb{R}_{>0}$ and $\phi_{ij} \in \mathbb{R}_{>0}$, $\forall i \in [1; N]$.

Input: The desired precision $\varepsilon \in \mathbb{R}_{>0}$; the simulation functions $\mathcal{V}_i$ equipped with functions κ_i, α_i, ρ_i, $\hat{\gamma}_i$, and $\overline{\alpha}_i$, $\forall i \in [1; N]$; functions σ_i, $\forall i \in [1; N]$, satisfying (24).

1 Choose $r \in \mathbb{R}_{>0}$ s.t. $\max_{i\in[1;N]} \{\sigma_i(r)\} = \varepsilon$;

2 Set $\varepsilon_i = \sigma_i(r)$, $\forall i \in [1; N]$;

3 Design $\phi_{ij} \in \mathbb{R}_{>0}$ s.t. $\max_{j\in\mathcal{N}_i}\{\phi_{ij}\} < \rho_i^{-1}((1-\kappa_i)\varepsilon_i) - \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j)\}$, $\forall i, j \in [1; N]$;

4 Set $\vartheta_i = \max_{j\in\mathcal{N}_i}\{\alpha_j^{-1}(\varepsilon_j) + \phi_{ij}\}$, $\forall i \in [1; N]$;

5 Design $\eta_i \in \mathbb{R}_{>0}$ s.t. $\eta_i \leq \min\{\hat{\gamma}_i^{-1}((1-\kappa_i)\varepsilon_i - \rho_i(\vartheta_i)), \overline{\alpha}_i^{-1}(\varepsilon_i)\}$;

Output: Quantization parameters $\eta_i \in \mathbb{R}_{>0}$ and $\phi_{ij} \in \mathbb{R}_{>0}$, $\forall i \in [1; N]$.

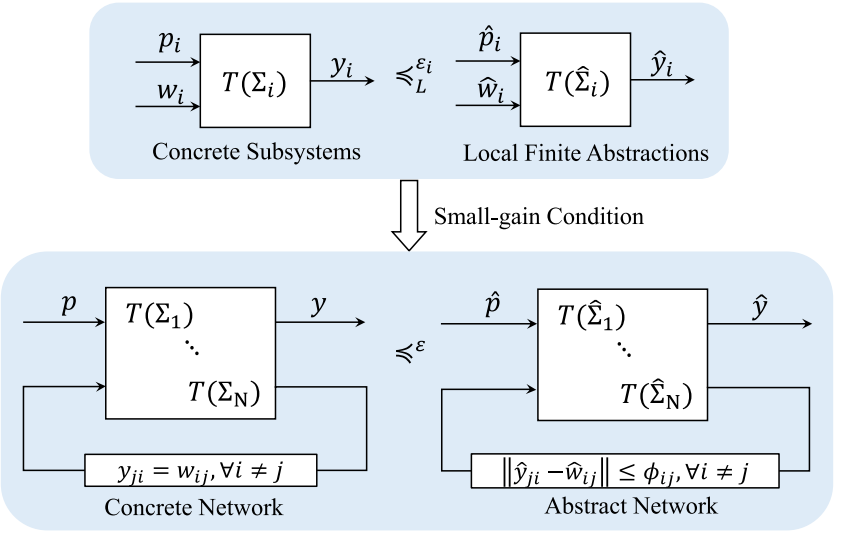

Fig. 3. Compositionality result.

Remark 29. The compositionality result in Theorem 28 imposes a small-gain type condition on the concrete network of switched subsystems for the existence of proper compositional finite abstraction, as depicted in Fig. 3. In particular, under such small-gain type conditions, one can always find suitable local quantization parameters to construct local finite abstractions. The interconnection of the local finite abstractions can be used to serve as a finite abstraction for the concrete network satisfying the simulation relation $T(\Sigma) \preceq^{\varepsilon} T(\hat{\Sigma})$. Intuitively, the small-gain type condition facilitates the compositional construction of finite abstractions by certifying a small (weak) interaction of the subsystems which prevents an amplification of the signals across the possible interconnections.

Remark 30. Let us provide a general guideline on the computation of $\mathcal{K}_\infty$ functions σ_i, $i \in [1; N]$, that are used in Theorem 28: (*i*) in a general case when the network is consisting of $N \geq 1$ subsystems, functions σ_i, $i \in [1; N]$, can be constructed numerically by leveraging the algorithm introduced in [33] and the technique presented in [32, Proposition 8.8], see [34, Chapter 4]; (*ii*) for the case of having two and three subsystems in the network, there have been some construction techniques proposed in [35] and [32, Section 9], respectively; (*iii*) when the gain functions appeared in (22) satisfy $\gamma_{ij} < \mathcal{I}_d$, $\forall i, j \in [1; N]$, then one can always choose σ_i, $i \in [1; N]$ to be identity functions.

6. Illustrative example

Here, we provide an illustrative example to show how one can leverage the proposed compositional approach to check approximate initial-state opacity of a network of switched systems based on its finite abstraction.

Consider a network of discrete-time switched systems $\Sigma = (\mathbb{X}, \mathbb{X}_0, \mathbb{X}_s, P, F, \mathbb{Y}, h)$ as in Definition 4, consisting of n subsystems Σ_i each described by:

$$\Sigma_i : \begin{cases} \mathbf{x}_i(k+1) &= a_{i\mathbf{p}_i(k)}\mathbf{x}_i(k) + d_i\omega_i(k) + b_{i\mathbf{p}_i(k)}, \\ \mathbf{y}_i(k) &= c_i\mathbf{x}_i(k), \end{cases} \tag{28}$$

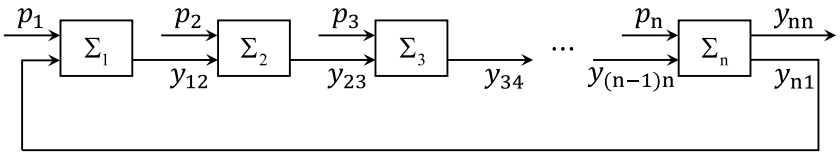

Fig. 4. The interconnection topology of the network of discrete-time switched subsystems Σ_i.

where $\mathrm{p}_i(k) \in P_i = \{1, 2\}$, $\forall k \in \mathbb{N}$, denotes the modes of each subsystem Σ_i. The other parameters are as the following: $a_{i1} = 0.05$, $a_{i2} = 0.1$, $b_{i1} = 0.1$, $b_{i2} = 0.15$, $d_i = 0.05$, $c_i = [c_{i1}; \ldots; c_{in}]$ with $c_{i(i+1)} = 1$, $c_{ij} = 0$, $\forall i \in [1; n-1]$, $\forall j \neq i+1$, $c_{n1} = c_{nn} = 1$, $c_{nj} = 0$, $\forall j \in [2; n-1]$. The internal inputs are subject to the constraints $\omega_1(k) = c_{n1}\mathbf{x}_n(k)$ and $\omega_i(k) = c_{(i-1)i}\mathbf{x}_{(i-1)}(k)$, $\forall i \in [2; n]$. For each switched subsystem, the state set is $\mathbb{X}_i = \mathbb{X}_{0_i} = (0, 0.6)$, $\forall i \in [1; n]$, 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 $\mathbb{Y}_{i(i+1)} = (0, 0.6)$, $\mathbb{Y}_{ii} = \mathbb{Y}_{ij} = \{0\}$, $\forall i \in [1; n-1]$, $\forall j \neq i+1$, $\mathbb{Y}_{nn} = \mathbb{Y}_{n1} = (0, 0.6)$, $\mathbb{Y}_{nj} = \{0\}$, $\forall j \in [2; n-1]$, and internal input set is $\mathbb{W}_1 = \mathbb{Y}_{ni}$, $\mathbb{W}_i = \mathbb{Y}_{(i-1)i}$, $\forall i \in [2; n]$. Intuitively, the output of the network is the external output of the last subsystem Σ_n. The interconnection topology of the network is depicted in Fig. 4.

The main goal of this example is to check approximate initial-state opacity of the concrete network using its finite abstraction. Now, let us construct a finite abstraction of Σ compositionally with accuracy $\hat{\varepsilon} = 0.25$ as defined in (7), which preserves approximate initial-state opacity. We implement our compositional approach to achieve this goal.

Consider functions $V_{ip_i} = |x_i - \hat{x}_i|$, $\forall i \in [1; n]$. It can be readily verified that (10) and (11) are satisfied with $\underline{\alpha}_{ip_i} = \overline{\alpha}_{ip_i} = \mathcal{I}_d$, $\rho_{ip_i} = 0.05$, $\forall p_i \in P_i$, $\kappa_{i1} = a_{i1} = 0.05$, $\kappa_{i2} = a_{i2} = 0.1$. Condition (13) is satisfied with $\gamma_{ip_i} = \mathcal{I}_d$, $\forall p_i \in P_i$. Moreover, since $V_{ip_i} = V_{ip_i^+}$, $\forall p_i, p_i^+ \in P_i$, $V_i(x_i, \hat{x}_i) = |x_i - \hat{x}_i|$ is a common δ-ISS Lyapunov function for subsystem Σ_i. Next, given functions $\kappa_i = 0.1$, $\rho_i = 0.06\mathcal{I}_d$, $\alpha_i = \mathcal{I}_d$, $\hat{\gamma}_i = 1.05\mathcal{I}_d$, $\overline{\alpha}_i = \mathcal{I}_d$ as appeared in Theorem 24, we have $\gamma_{ij} < \mathcal{I}_d$ by (22), $\forall i, j \in [1; n]$. Hence, the small-gain condition (23) is satisfied. Then, by applying Theorem 28 and choosing functions $\sigma_i = \mathcal{I}_d$, $\forall i \in [1; n]$, such that (24) holds, we obtain proper pairs of local parameters $(\varepsilon_i, \vartheta_i) = (0.25, 0.25)$ for all of the transition systems. Accordingly, we provide a suitable choice of local quantization parameters as $\eta_i = 0.2$, $\forall i \in [1; n]$, such that inequality (14) for each transition system $T(\Sigma_i)$ is satisfied. Then, we construct local finite abstractions $T(\hat{\Sigma}_i) = (\hat{X}_i, \hat{X}_{0_i}, \hat{X}_{s_i}, \hat{U}_i, \hat{W}_i, \hat{\mathcal{F}}_i, \hat{Y}_i, \hat{\mathcal{H}}_i)$ as in Definition 21, where:

$$\hat{X}_i = \hat{X}_{0_i} = \{0.2, 0.4\}, \forall i \in [1; n],$$

$$\hat{X}_{s_i} = \begin{cases} \{0.2\}, & \text{if } i = 1 \\ \{0.4\}, & \text{if } i = 2 \\ \{0.2, 0.4\}, & \text{otherwise} \end{cases}$$

$$\hat{Y}_i = \begin{cases} \prod_{j=1}^{i}\{0\} \times \{0.2, 0.4\} \times \prod_{j=i+2}^{n}\{0\}, & \text{if } i \in [1; n-1] \\ \{0.2, 0.4\} \times \prod_{j=2}^{n-1}\{0\} \times \{0.2, 0.4\}, & \text{otherwise} \end{cases}$$

$$\hat{W}_i = \{0.2, 0.4\}, \forall i \in [1; n].$$

Using the result in Theorem 24, one can verify that $V_i(x_i, \hat{x}_i) = |x_i - \hat{x}_i|$ is a local ε_i-InitSOPSF from each $T(\Sigma_i)$ to its finite abstraction $T(\hat{\Sigma}_i)$. Furthermore, by the compositionality result in Theorem 17, we obtain that $V = \max_i\{V_i(x_i, \hat{x}_i)\} = \max_i\{|x_i - \hat{x}_i|\}$ is an ε-InitSOPSF from $T(\Sigma) = \mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_n))$ to $T(\hat{\Sigma}) = \hat{\mathcal{I}}(T(\hat{\Sigma}_1), \ldots, T(\hat{\Sigma}_n))$ with $\varepsilon = \max_i \varepsilon_i = 0.25$.

Now, let us verify approximate initial-state opacity for $T(\Sigma)$ using the network of finite abstractions $T(\hat{\Sigma})$. To do this, we first show an example of a network consisting of 3 transition systems, as shown in Figs. 5 and 6. The three automata in Fig. 5 represent the finite abstractions of the local transition systems, and the one in Fig. 6 is the network of finite abstractions. 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. The states marked in red represent the secret states. The symbols on the edges show the switching signals $\mathrm{p}(k) \in \{1, 2\}^3$ and internal inputs coming from other local transition systems. For simplicity of demonstration, we use symbols to represent the state and output vectors, where the states of local transition systems are denoted by $q_1 = [0.4]$, $q_2 = [0.2]$, the states of network of transition systems are denoted by

$$z_1 = [q_1; q_2; q_2], z_2 = [q_2; q_2; q_2], z_3 = [q_2; q_1; q_2], z_4 = [q_1; q_1; q_2],$$
$$z_5 = [q_1; q_2; q_1], z_6 = [q_1; q_1; q_1], z_7 = [q_2; q_2; q_1], z_8 = [q_2; q_1; q_1],$$

and the outputs of the corresponding states are represented as $y = 0.2$ and $Y = 0.4$ with the symbols like $00y = [0; 0; 0.2]$, $00Y = [0; 0; 0.4]$ representing concatenated output vectors. One can easily see that $\hat{\mathcal{I}}(T(\hat{\Sigma}_1), T(\hat{\Sigma}_2), T(\hat{\Sigma}_3))$ is 0-approximate initial-state opaque, since for any run starting from any secret state, i.e. z_3 and z_8, there exists a run from a non-secret state, i.e. z_1 and z_6, such that the output trajectories are exactly the same. Essentially, one can verify that the abstract network holds this property regardless of the number of systems (i.e. n), due to the homogeneity of systems Σ_i and the symmetry of the circular network topology. Thus, one can conclude that $T(\hat{\Sigma}) =$

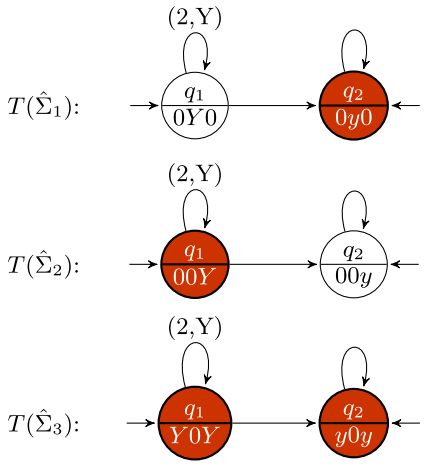

Fig. 5. Local finite abstractions of transition systems.

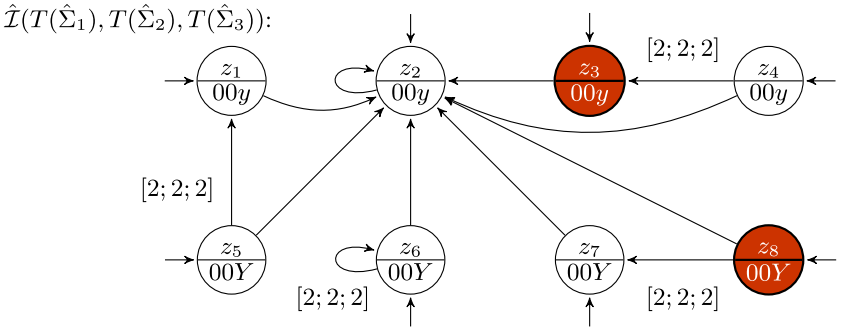

Fig. 6. Finite abstraction of a network of 3 transition systems.

$\hat{\mathcal{I}}(T(\hat{\Sigma}_1), \ldots, T(\hat{\Sigma}_n))$ is 0-approximate initial-state opaque. Therefore, by Corollary 14, we obtain that the original network $T(\Sigma) = \mathcal{I}(T(\Sigma_1), \ldots, T(\Sigma_n))$ is 0.5-approximate initial-state opaque.

7. Conclusion and discussion

In this paper, we provided a compositional framework for the construction of opacity-preserving finite abstractions for networks of discrete-time switched systems. First, an approximate opacity-preserving simulation function is defined to characterize the simulation relation between two networks, which facilitates the abstraction-based opacity verification process. Then we presented a compositional approach to construct finite abstractions locally for concrete subsystems under incremental input-to-state stability property. The interconnection of local finite abstractions forms an abstract network that mimics the behaviors of the concrete network while preserving approximate initial-state (resp. current-state) opacity via the proposed simulation functions. Furthermore, we derived a small-gain type condition, under which one can guarantee the existence of proper quantization parameters for the construction of finite abstractions. Note that we presented compositionality results on the construction of finite abstractions for notions of approximate initial-state and current-state opacity. One can readily follow the same lines of reasoning to establish similar results for the notion of approximate infinite-step opacity [10,36]. We preferred to not include those results for the sake of brevity. For future work, it would be interesting to investigate opacity property for large-scale switched systems with unstable modes, and also for other classes of hybrid systems, e.g., impulsive systems.

CRediT authorship contribution statement

Siyuan Liu: Conceptualization, Methodology, Visualization, Validation, Writing - original draft, Writing review & editing. **Abdalla Swikir:** Conceptualization, Methodology, Validation, Writing - original draft. **Majid Zamani:** Supervision, Conceptualization, Methodology, Validation, Writing - original draft, Writing - review & editing, Funding acquisition, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, et al., Challenges for securing cyber physical systems, in: Workshop on Future Directions in Cyber-Physical Systems Security, 5, 2009.
[2] Y. Ashibani, Q.H. Mahmoud, Cyber physical systems security: Analysis, challenges and solutions, Comput. Secur. 68 (2017) 81–97, http://dx.doi.org/10.1016/j.cose.2017.04.005.
[3] L. Mazaré, Using unification for opacity properties, in: Proceedings of Workshop on Issues in the Theory of Security, 2004, pp. 165–176.
[4] S. Lafortune, F. Lin, C.N. Hadjicostis, On the history of diagnosability and opacity in discrete event systems, Annu. Rev. Control 45 (2018) 257–266, http://dx.doi.org/10.1016/j.arcontrol.2018.04.002.
[5] C.N. Hadjicostis, Estimation and Inference in Discrete Event Systems, Springer. http://dx.doi.org/10.1007/978-3-030-30821-6.
[6] B. Ramasubramanian, W.R. Cleaveland, S. Marcus, Notions of centralized and decentralized opacity in linear systems, IEEE Trans. Automat. Control 65 (4) (2019) 1442–1455, http://dx.doi.org/10.1109/TAC.2019.2920837.
[7] B. Ramasubramanian, R. Cleaveland, S.I. Marcus, Opacity for switched linear systems: Notions and characterization, in: Proceedings of the 56th Conference on Decision and Control, IEEE, 2017, pp. 5310–5315, http://dx.doi.org/10.1109/CDC.2017.8264445.
[8] L. An, G.-H. Yang, Opacity enforcement for confidential robust control in linear cyber-physical systems, IEEE Trans. Automat. Control 65 (3) (2019) 1234–1241, http://dx.doi.org/10.1109/TAC.2019.2925498.
[9] K. Zhang, X. Yin, M. Zamani, Opacity of nondeterministic transition systems: A (bi) simulation relation approach, IEEE Trans. Automat. Control 64 (12) (2019) 5116–5123, http://dx.doi.org/10.1109/TAC.2019.2908726.
[10] X. Yin, M. Zamani, S. Liu, On approximate opacity of cyber-physical systems, IEEE Trans. Automat. Control 66 (4) (2021) 1630–1645, http://dx.doi.org/10.1109/TAC.2020.2998733.
[11] S. Liu, X. Yin, M. Zamani, On a notion of approximate opacity for discrete-time stochastic control systems, in: American Control Conference, IEEE, 2020, pp. 5413–5418, http://dx.doi.org/10.23919/ACC45564.2020.9147235.
[12] G. Pola, P. Pepe, M.D.D. Benedetto, Symbolic models for networks of control systems, IEEE Trans. Automat. Control 61 (11) (2016) 3663–3668, http://dx.doi.org/10.1109/TAC.2016.2528046.
[13] P.J. Meyer, A. Girard, E. Witrant, Compositional abstraction and safety synthesis using overlapping symbolic models, IEEE Trans. Automat. Control 63 (6) (2017) 1835–1841, http://dx.doi.org/10.1109/TAC.2017.2753039.
[14] E.S. Kim, M. Arcak, M. Zamani, Constructing control system abstractions from modular components, in: Proceedings of the 21st International Conference on Hybrid Systems: Computation and Control (Part of CPS Week), 2018, pp. 137–146, http://dx.doi.org/10.1145/3178126.3178144.
[15] A. Swikir, M. Zamani, Compositional synthesis of finite abstractions for networks of systems: A small-gain approach, Automatica 107 (11) (2019) 551–561, http://dx.doi.org/10.1016/j.automatica.2019.06.021.
[16] K. Mallik, A. Schmuck, S. Soudjani, R. Majumdar, Compositional synthesis of finite-state abstractions, IEEE Trans. Automat. Control 64 (6) (2019) 2629–2636, http://dx.doi.org/10.1109/TAC.2018.2869740.
[17] A. Swikir, M. Zamani, Compositional synthesis of symbolic models for networks of switched systems, IEEE Control Syst. Lett. 3 (4) (2019) 1056–1061, http://dx.doi.org/10.1109/LCSYS.2019.2920766.
[18] A. Swikir, M. Zamani, Compositional abstractions of interconnected discrete-time switched systems, in: 18th European Control Conference, 2019, pp. 1251–1256, http://dx.doi.org/10.23919/ECC.2019.8796176.
[19] G. Pola, E. De Santis, M.D. Di Benedetto, D. Pezzuti, Design of decentralized critical observers for networks of finite state machines: A formal method approach, Automatica 86 (2017) 174–182, http://dx.doi.org/10.1016/j.automatica.2017.08.025.
[20] S. Liu, M. Zamani, Compositional synthesis of opacity-preserving finite abstractions for interconnected systems, 2020, ArXiv Preprint ArXiv:2004.00131.
[21] S. Liu, A. Swikir, M. Zamani, Compositional verification of initial-state opacity for switched systems, in: 59th IEEE Conference on Decision and Control, 2020, pp. 2146–2151, http://dx.doi.org/10.1109/CDC42340.2020.9304322.
[22] D. Liberzon, Switching in Systems and Control, Birkhäuser Basel, 2003, http://dx.doi.org/10.1007/978-1-4612-0017-8.
[23] P. Tabuada, Verification and Control of Hybrid Systems: A Symbolic Approach, Springer Science & Business Media, 2009, http://dx.doi.org/10.1007/978-1-4419-0224-5.
[24] Y. Tazaki, J.-i. Imura, Bisimilar finite abstractions of interconnected systems, in: International Workshop on Hybrid Systems: Computation and Control, Springer, 2008, pp. 514–527, http://dx.doi.org/10.1007/978-3-540-78929-1_37.
[25] G. Barequet, S. Har-Peled, Efficiently approximating the minimum-volume bounding box of a point set in three dimensions, J. Algorithms 38 (1) (2001) 91–109, http://dx.doi.org/10.1006/jagm.2000.1127.
[26] X. Yin, S. Lafortune, A new approach for the verification of infinite-step and K-step opacity using two-way observers, Automatica 80 (2017) 162–171, http://dx.doi.org/10.1016/j.automatica.2017.02.037.
[27] A. Saboori, C.N. Hadjicostis, Verification of initial-state opacity in security applications of discrete event systems, Inform. Sci. 246 (2013) 115–132, http://dx.doi.org/10.1016/j.ins.2013.05.033.
[28] D. Angeli, A Lyapunov approach to incremental stability properties, IEEE Trans. Automat. Control 47 (3) (2002) 410–421, http://dx.doi.org/10.1109/9.989067.
[29] A. Girard, G. Pola, P. Tabuada, Approximately bisimilar symbolic models for incrementally stable switched systems, IEEE Trans. Automat. Control 55 (1) (2009) 116–126, http://dx.doi.org/10.1109/TAC.2009.2034922.
[30] L. Vu, D. Chatterjee, D. Liberzon, Input-to-state stability of switched systems and switching adaptive control, Automatica 43 (4) (2007) 639–646, http://dx.doi.org/10.1016/j.automatica.2006.10.007.
[31] M. Zamani, P. Mohajerin Esfahani, R. Majumdar, A. Abate, J. Lygeros, Symbolic control of stochastic systems via approximately bisimilar finite abstractions, IEEE Trans. Automat. Control 59 (12) (2014) 3135–3150, http://dx.doi.org/10.1109/TAC.2014.2351652.
[32] S. Dashkovskiy, B. Rüffer, F. Wirth, Small gain theorems for large scale systems and construction of ISS Lyapunov functions, SIAM J. Control Optim. 48 (6) (2010) 4089–4118, http://dx.doi.org/10.1137/090746483.
[33] B.C. Eaves, Homotopies for computation of fixed points, Math. Program. 3 (1) (1972) 1–22, http://dx.doi.org/10.1007/BF01584975.
[34] B.S. Ruffer, Monotone dynamical systems, graphs, and stability of largescale interconnected systems, in: Fachbereich 3, Mathematik Und Informatik (Ph.D. thesis), UniversitÄt Bremen, Germany, 2007.
[35] Z.-P. Jiang, I.M. Mareels, Y. Wang, A Lyapunov formulation of the nonlinear small-gain theorem for interconnected ISS systems, Automatica 32 (1) (1996) 1211–1215, http://dx.doi.org/10.1016/0005-1098(96)00051-9.
[36] A. Saboori, C.N. Hadjicostis, Verification of infinite-step opacity and complexity considerations, IEEE Trans. Automat. Control 57 (5) (2012) 1265–1269, http://dx.doi.org/10.1109/tac.2011.2173774.