2017 IEEE 56th Annual Conference on Decision and Control (CDC)
December 12-15, 2017, Melbourne, Australia

# Infinite-step opacity of nondeterministic finite transition systems: A bisimulation relation approach

Kuize Zhang and Majid Zamani

***Abstract*— It is known that the problem of verifying the infinite-step opacity of nondeterministic finite transition systems (NFTSs) is PSPACE-hard. In this paper, we investigate whether it is possible to use classical bisimulation relation to come up with abstract NFTSs and verify the infinite-step opacity of original NFTSs over their abstractions. First, we show that generally bisimulation relation does not preserve infinite-step opacity. Second, by adding some additional conditions to bisimulation relation, we prove that a stronger version of bisimulation relation, called here *opacity-preserving* bisimulation relation, preserves infinite-step opacity. Therefore, if one can find an abstract NFTS for a large NFTS under an opacity-preserving bisimulation relation, then the infinite-step opacity of the original NFTS can be verified by investigating that over the abstract NFTS. Finally, we show that under some mild assumptions, the quotient relation between an NFTS and its quotient system becomes opacity-preserving bisimulation relation which provides a scheme for constructing opacity-preserving abstractions of large-scale NFTSs. We show the effectiveness of the results using several examples throughout the paper.**

## I. Introduction

The notion of opacity is introduced in the analysis of cryptographic protocols [6], and describes the ability that a system has to forbid leaking secret information.

In the framework of discrete event systems (DESs), the opacity problem has been widely investigated. In different practical situations, opacity of DESs can be formulated as whether a system can prevent an intruder from observing whether the initial state (resp., the current state, each state within $K$ steps prior to the current state for some natural number $K$, each state prior to the current state) of the system is secret, i.e., the so-called initial-state [10] (resp. current-state [7], $K$-step [8], and infinite-step [9]) opacity. It is known that the existing algorithms for verifying these types of opacity have exponential time computational complexity (cf. the above references and [14]), and it is unlikely that there exist polynomial time algorithms for verifying them. Particularly, the problems of determining the initial-state opacity, the $K$-step opacity, and the infinite-step opacity of DESs are **PSPACE**-complete [10], **NP**-hard [8], and **PSPACE**-hard [9], respectively. More related results are referred to [2], [4], [11], [13], [15].

This work was supported in part by Knut och Alice Wallenbergs Foundation, Swedish Foundation for Strategic Research, Swedish Research Council, and the German Research Foundation (DFG) through the grant ZA 873/1-1.

K. Zhang is with ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, 10044 Stockholm, Sweden (zkz0017@163.com). M. Zamani is with the Department of Electrical and Computer Engineering, Technical University of Munich, D-80290 Munich, Germany (zamani@tum.de).

Among the above types of opacity, infinite-step opacity has the strongest ability to stop leaking secret information. In this paper, we focus on this type of opacity.

Nondeterministic finite transition systems (NFTSs) consist of finitely many states, inputs, and outputs, and play a fundamental role in the verification and control of hybrid systems [3], [5], [12], [16], and model checking [1]. In this paper, we formulate and study the infinite-step opacity problem of NFTSs. Note that by regarding an (input, output)-pair at the same time step as an event, an NFTS can be seen roughly as a DES. So the techniques used in [9], [14] can be used to check the infinite-step opacity of NFTSs as well, and it is obtained that the problem of verifying the infinite-step opacity of NFTSs is also **PSPACE**-hard [9].

In this paper, we investigate the application of bisimulation relation in verifying the infinite-step opacity of NFTSs. Intuitively, for two NFTSs $\Sigma_1$ and $\Sigma_2$, $\Sigma_2$ simulates $\Sigma_1$ if each output sequence generated by $\Sigma_1$ can also be generated by $\Sigma_2$; $\Sigma_2$ bisimulates $\Sigma_1$ if $\Sigma_2$ simulates $\Sigma_1$ and $\Sigma_1$ simulates $\Sigma_2$ (cf. [5], [12]). Usually, bisimulation relation can be used to abstract a large-scale system to a smaller one, and if the smaller system bisimulates the larger one, then in some sense the smaller system can take place of the larger one in some of the analysis and synthesis (cf. [12], [16]). In this paper, we first define a new notion of opacity-preserving bisimulation relation, then we use the proposed notion to give some necessary and sufficient conditions for the infinite-step opacity of NFTSs. Hence, if one can find an appropriate opacity-preserving bisimulation relation between the original NFTS $\Sigma_1$ and a small-scale NFTS $\Sigma_2$ such that the size of $\Sigma_2$ is remarkably smaller than that of $\Sigma_1$, then the infinite-step opacity of $\Sigma_1$ can be checked by verifying the infinite-step opacity of $\Sigma_2$ which is faster. In addition, we prove that under some mild assumptions, the bisimulation relation between an NFTS and its quotient system becomes opacity-preserving bisimulation relation, which provides a constructive scheme for computing opacity-preserving abstractions of large-scale NFTSs.

The remainder of this paper is organized as follows. In Section II, the basic concepts of NFTSs and bisimulation relation are introduced. In Section III, we show the main results of the paper. Section IV concludes the paper.

## II. Preliminaries

We use the following notations throughout the paper:

- $\emptyset$: the empty set;
- $\mathbb{N}$: the set of non-negative integers;
- $[a, b] := \{a, a+1, \ldots, b\}$, where $a, b \in \mathbb{N},\ a \leq b$.

978-1-5090-2873-3/17/$31.00 ©2017 IEEE

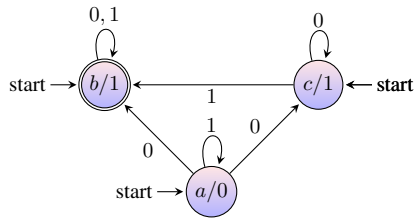


Fig. 1. State transition diagram of the NFTS in Example 2.1.

Note that although we focus on NFTSs, all results of this paper remain valid for transition systems with *infinitely* many states, inputs, and outputs (e.g. control systems).

NFTSs are defined as in [5], [12] with some modifications to accommodate for secret states.

*Definition 1:* An NFTS $\Sigma$ is a septuple $(X, X_0, S, U, \rightarrow, Y, h)$ consisting of

- a finite set $X$ of states;
- a subset $X_0 \subseteq X$ of initial states;
- a subset $S \subseteq X$ of secret states;
- a finite set $U$ of inputs;
- a transition relation $\rightarrow \subseteq X \times U \times X$;
- a set $Y$ of outputs;
- an output map $h : X \rightarrow Y$.

In this paper, we consider total NFTSs, i.e., for all $x$ in $X$ and $u$ in $U$, there exists at least one state $x'$ in $X$ such that $(x, u, x') \in \rightarrow$. In this case, the transition relation $\rightarrow \subseteq X \times U \times X$ can be equivalently represented as a mapping from $X \times U$ to $2^X \setminus \emptyset$. Elements of $\rightarrow$ are called transitions. Let $X^*$ be the set of strings of finite length over $X$ including the string $\epsilon$ of length 0. For each $\alpha \in X^*$, $|\alpha|$ denotes the length of $\alpha$. For each $\alpha \in X^*$, for all integers $0 \leq i \leq j \leq |\alpha| - 1$, we use $\alpha[i, j]$ to denote $\alpha(i)\alpha(i+1)\ldots\alpha(j)$ for short. Sets $U^*$ and $Y^*$ are defined analogously. A string $\alpha \in X^*$ is called a run of the system over input sequence $\beta \in U^*$ if $|\alpha| - 1 = |\beta|$, $\alpha(0) \in X_0$, and for all $i \in [0, |\alpha| - 2]$, $(\alpha(i), \beta(i), \alpha(i+1)) \in \rightarrow$. Transitions determined by $\alpha$ and $\beta$ can be denoted as $\alpha(0) \xrightarrow{\beta(0)} \alpha(1) \xrightarrow{\beta(1)} \cdots \xrightarrow{\beta(|\beta|-1)} \alpha(|\alpha| - 1)$.

An NFTS can be represented as its state transition diagram, i.e., a directed graph whose vertices correspond to the states and their associated outputs of the NFTS and whose edges correspond to state transitions. Each edge is labeled with the inputs associated with the transition, a state directly connected from "start" means an initial state, a double circle denotes a secret state. We give an example to depict these concepts.

*Example 2.1:* Consider NFTS $(X, X_0, S, U, \rightarrow, Y, h)$, where $X = \{a, b, c\}$, $X_0 = X$, $S = \{b\}$, $U = Y = \{0, 1\}$, $\rightarrow = \{(a, 1, a), (a, 0, b), (a, 0, c), (b, 0, b), (b, 1, b), (c, 0, c), (c, 1, b)\}$, $h(a) = 0$, $h(b) = h(c) = 1$ (see Fig. 1).

Here, we recall the conventional notions of (bi)simulation relations [12].

*Definition 2 (simulation):* Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U_i, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called a simulation relation from $\Sigma_1$ to $\Sigma_2$ if

1) for every $x_{1,0} \in X_{1,0}$, there exists $x_{2,0} \in X_{2,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$, if there is a transition $x_1 \xrightarrow{u_1}_1 x_1'$ in $\Sigma_1$ then there exists a transition $x_2 \xrightarrow{u_2}_2 x_2'$ in $\Sigma_2$ satisfying $(x_1', x_2') \in \sim$.

Under a simulation relation $\sim \subseteq X_1 \times X_2$ from $\Sigma_1$ to $\Sigma_2$, we say $\Sigma_2$ simulates $\Sigma_1$, and denote $\Sigma_1 \preceq_S \Sigma_2$.

*Definition 3 (bisimulation):* Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U_i, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called a bisimulation relation between $\Sigma_1$ and $\Sigma_2$ if

1) a) for every $x_{1,0} \in X_{1,0}$, there exists $x_{2,0} \in X_{2,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   b) for every $x_{2,0} \in X_{2,0}$, there exists $x_{1,0} \in X_{1,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) a) for every $(x_1, x_2) \in \sim$, if there exists a transition $x_1 \xrightarrow{u_1}_1 x_1'$ in $\Sigma_1$ then there exists a transition $x_2 \xrightarrow{u_2}_2 x_2'$ in $\Sigma_2$ satisfying $(x_1', x_2') \in \sim$;
   b) for every $(x_1, x_2) \in \sim$, if there exists a transition $x_2 \xrightarrow{u_2}_2 x_2'$ in $\Sigma_2$ then there exists a transition $x_1 \xrightarrow{u_1}_1 x_1'$ in $\Sigma_1$ satisfying $(x_1', x_2') \in \sim$.

Under a bisimulation relation $\sim \subseteq X_1 \times X_2$ between $\Sigma_1$ and $\Sigma_2$, we say $\Sigma_2$ bisimulates $\Sigma_1$ (or vice versa), and denote $\Sigma_1 \cong_S \Sigma_2$.

From Definitions 2 and 3, one can readily see that if $\Sigma_2$ simulates $\Sigma_1$ then each output sequence generated by $\Sigma_1$ can be generated by $\Sigma_2$ as well; and if $\Sigma_2$ bisimulates $\Sigma_1$ then the set of output sequences generated by $\Sigma_1$ coincides with the ones generated by $\Sigma_2$.

Here, we recall notions of quotient relation and quotient systems [12] with some modifications which will be used later to show one of the main results of the paper.

*Definition 4:* Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NFTS and $\sim \subseteq X \times X$ an equivalence relation on $X$ satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. The quotient system of $\Sigma$ by $\sim$, denoted by $\Sigma_\sim$, is defined as the system $\Sigma_\sim = (X_\sim, X_{\sim,0}, S_\sim, U, \rightarrow_\sim, Y, h_\sim)$ satisfying

1) $X_\sim = X/\sim = \{[x] | x \in X\}$;
2) $X_{\sim,0} = \{[x] | x \in X, [x] \cap X_0 \neq \emptyset\}$;
3) $S_\sim = \{[x] | x \in X, [x] \cap S \neq \emptyset\}$;
4) for all $[x], [x'] \in X_\sim$ and $u \in U$, there exists transition $[x] \xrightarrow{u}_\sim [x']$ in $\Sigma_\sim$ if there exists transition $\bar{x} \xrightarrow{u} \bar{x}'$ in $\Sigma$ for some $\bar{x} \in [x]$ and $\bar{x}' \in [x']$;
5) $h_\sim([x]) = h(\bar{x})$ for every $\bar{x} \in [x]$;

where for every $x \in X$, $[x]$ denotes the equivalence class generated by $x$, i.e., $[x] := \{y \in X | (y, x) \in \sim\}$.

It can be seen that for all $x, x' \in X$, 1) either $[x] = [x']$ or $[x] \cap [x'] = \emptyset$; 2) $x \in [x']$ if and only if $[x] = [x']$. Then the set of all distinct equivalence classes corresponding to $\sim$ partitions set $X$. Note that in [12], there is no item for $S_\sim$, since the system $\Sigma$ considered in [12] does not have secret states. From Definition 4, one can readily verify that the quotient system $\Sigma_\sim$ has no more states than $\Sigma$ does.

Consider an NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ and its quotient system $\Sigma_\sim = (X_\sim, X_{\sim,0}, S_\sim, U, \rightarrow_\sim, Y, h_\sim)$ defined by an equivalence relation $\sim \subseteq X \times X$ satisfying

$h(x) = h(x')$ for all $(x, x') \in \sim$. By defining a quotient relation

$$\sim_{\mathrm{Q}} := \{(x, [x]) | x \in X\} \subseteq X \times X_{\sim}, \tag{1}$$

the following result holds [12].

*Proposition 2.2:* Consider an NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ and its quotient system $\Sigma_{\sim} = (X_{\sim}, X_{\sim,0}, S_{\sim}, U, \rightarrow_{\sim}, Y, h_{\sim})$ defined by an equivalence relation $\sim \subseteq X \times X$ satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. Under quotient relation $\sim_{\mathrm{Q}}$ defined in (1), $\Sigma_{\sim}$ simulates $\Sigma$. Moreover, $\Sigma_{\sim}$ bisimulates $\Sigma$ under $\sim_{\mathrm{Q}}$ if and only if $\Sigma$ bisimulates $\Sigma$ under $\sim$.

Later on, we provide similar results as in Proposition 2.2 but using so-called opacity-preserving bisimulation relation.

## III. Main Results

### A. Opacity-preserving bisimulation relation

In this subsection, we provide one of the main results of the paper. We first define the notion of infinite-step opacity of NFTSs.

*Definition 5:* Let $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ be an NFTS. $\Sigma$ is said to be infinite-step opaque if for all $x_0 \in X_0$, all $\alpha \in U^*$, all runs $x_0 x_1 \dots x_{|\alpha|} \in X^*$ over $\alpha$, all $i \in [0, |\alpha|]$, if $x_i \in S$ then there exists $x'_0, \dots, x'_{|\alpha|} \in X$ such that $x'_0 \in X_0$, $x'_i \in X \setminus S$, $x'_0 \dots x'_{|\alpha|}$ is also a run over $\alpha$, and $h(x_j) = h(x'_j)$ for all $j \in [0, |\alpha|]$.

Intuitively, if a system $\Sigma$ is infinite-step opaque, then the intruder cannot make sure whether any state prior to the current state is secret or not.

One of the main goals of this paper is to provide a bisimulation-based method for verifying the infinite-step opacity of NFTSs. Particularly, for two NFTSs $\Sigma_1$ and $\Sigma_2$, we are interested in providing a new stronger notion of bisimulation relation such that $\Sigma_2$ bisimulating $\Sigma_1$ implies that $\Sigma_1$ being infinite-step opaque is equivalent to $\Sigma_2$ being infinite-step opaque. Hence the central problem we should consider first is whether the classical bisimulation relation preserves infinite-step opacity. We next show that generally classical bisimulation relation does not preserve infinite-step opacity.

*Proposition 3.1:* Bisimulation relation in Definition 3 does not preserve infinite-step opacity.

*Proof:* We provide a counterexample to prove the statement. Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$, shown in Fig. 2, where $X_1 = \{1, 2\} = X_{1,0}$, $S_1 = \{1\} = U$, $Y = \{1, 2\}$; $X_2 = \{1', 2', 3', 4'\} = X_{2,0}$, $S_2 = \{1'\}$.

By Definition 5, system $\Sigma_1$ is not infinite-step opaque, because for secret state 1, there exists no other state producing the same output as 1. Again by Definition 5, system $\Sigma_2$ is infinite-step opaque, because for input sequence $\alpha := 1 \dots 1 \in U_2^*$, for every run $x_1 := \dots 1' \dots$ over $\alpha$, there is a unique run $x_2 := \dots 3' \dots$ over $\alpha$ such that they produce the same output sequence, where $1' \in S_2$ and $3' \in X_2 \setminus S_2$ are at the same time step.

On the other hand, it can be readily verified that under relation $\sim = \{(1, 1'), (2, 2'), (1, 3'), (2, 4')\}$, $\Sigma_2$ bisimulates $\Sigma_1$. Hence bisimulation relation does not preserve infinite-step opacity.

■

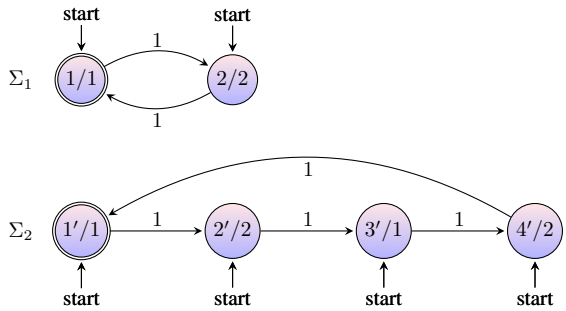


Fig. 2. State transition diagrams of two NFTSs in the proof of Proposition 3.1.

Since generally bisimulation relation does not preserve infinite-step opacity, we strengthen this notion to make it infinite-step opacity-preserving.

*Definition 6 (opacity-preserving bisimulation):* Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. A relation $\sim \subseteq X_1 \times X_2$ is called an opacity-preserving bisimulation relation between $\Sigma_1$ and $\Sigma_2$ if

1) a) for all $x_{1,0} \in S_1 \cap X_{1,0}$, there exists $x_{2,0} \in S_2 \cap X_{2,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   b) for all $x_{1,0} \in X_{1,0} \setminus S_1$, there exists $x_{2,0} \in X_{2,0} \setminus S_2$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   c) for all $x_{2,0} \in S_2 \cap X_{2,0}$, there exists $x_{1,0} \in S_1 \cap X_{1,0}$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
   d) for all $x_{2,0} \in X_{2,0} \setminus S_2$, there exists $x_{1,0} \in X_{1,0} \setminus S_1$ such that $(x_{1,0}, x_{2,0}) \in \sim$;
2) for every $(x_1, x_2) \in \sim$, $h_1(x_1) = h_2(x_2)$;
3) for every $(x_1, x_2) \in \sim$,
   a) for every transition $x_1 \xrightarrow{u}_1 x'_1 \in S_1$, there exists transition $x_2 \xrightarrow{u}_2 x'_2 \in S_2$ such that $(x'_1, x'_2) \in \sim$;
   b) for every transition $x_1 \xrightarrow{u}_1 x'_1 \in X_1 \setminus S_1$, there exists transition $x_2 \xrightarrow{u}_2 x'_2 \in X_2 \setminus S_2$ such that $(x'_1, x'_2) \in \sim$;
   c) for every transition $x_2 \xrightarrow{u}_2 x'_2 \in S_2$, there exists transition $x_1 \xrightarrow{u}_1 x'_1 \in S_1$ such that $(x'_1, x'_2) \in \sim$;
   d) for every transition $x_2 \xrightarrow{u}_2 x'_2 \in X_2 \setminus S_2$, there exists transition $x_1 \xrightarrow{u}_1 x'_1 \in X_1 \setminus S_1$ such that $(x'_1, x'_2) \in \sim$.

Intuitively, 1) ensures that each initial secret (non-secret) state in $\Sigma_1$ has a corresponding initial secret (non-secret) state in $\Sigma_2$ such that they are in the relation, and vice versa; 3) guarantees that each transition to a secret (non-secret) state in $\Sigma_1$ has a corresponding transition to a secret (non-secret) state in $\Sigma_2$, and vice versa. 1) and 3) make bisimulation relation preserve infinite-step opacity, which is shown in the following theorem.

*Theorem 3.2:* Consider two NFTSs $\Sigma_i = (X_i, X_{i,0}, S_i, U, \rightarrow_i, Y, h_i)$, $i = 1, 2$. If there exists an opacity-preserving bisimulation relation $\sim \subseteq X_1 \times X_2$ between $\Sigma_1$ and $\Sigma_2$, then $\Sigma_1$ is infinite-step opaque if and only if $\Sigma_2$ is infinite-step opaque.

*Proof:* Assume there exists an opacity-preserving bisimulation relation $\sim \subseteq X_1 \times X_2$ between $\Sigma_1$ and $\Sigma_2$ and

system $\Sigma_1$ is infinite-step opaque. Now we show that $\Sigma_2$ is also infinite-step opaque.

For system $\Sigma_2$, we arbitrarily choose input sequence $\alpha \in U^*$, states $x_{2,0} \in X_{2,0}$ and $x_{2,1}, \ldots, x_{2,|\alpha|} \in X_2$ such that

$$x_{2,0} \xrightarrow{\alpha(0)}_2 x_{2,1} \xrightarrow{\alpha(1)}_2 \cdots \xrightarrow{\alpha(|\alpha|-1)}_2 x_{2,|\alpha|},$$

and $x_{2,i} \in S_2$ for some $i \in [0, |\alpha|]$.

Since $\Sigma_1$ simulates $\Sigma_2$, by 1c), 1d), 2), 3c), and 3d), there exist $x_{1,0} \in X_{1,0}$, $x_{1,j} \in X_1$, $j \in [1, |\alpha|]$ such that $x_{1,i} \in S_1$, $h_1(x_{1,k}) = h_2(x_{2,k})$, $k \in [0, |\alpha|]$, and

$$x_{1,0} \xrightarrow{\alpha(0)}_1 x_{1,1} \xrightarrow{\alpha(1)}_1 \cdots \xrightarrow{\alpha(|\alpha|-1)}_1 x_{1,|\alpha|}.$$

Since $\Sigma_1$ is infinite-step opaque, there exist $x'_{1,0} \in X_{1,0}$, $x'_{1,j} \in X_1$, $j \in [1, |\alpha|]$ such that $x'_{1,i} \in X_1 \setminus S_1$, $h_1(x_{1,k}) = h_1(x'_{1,k})$, $k \in [0, |\alpha|]$, and

$$x'_{1,0} \xrightarrow{\alpha(0)}_1 x'_{1,1} \xrightarrow{\alpha(1)}_1 \cdots \xrightarrow{\alpha(|\alpha|-1)}_1 x'_{1,|\alpha|}.$$

Since $\Sigma_2$ simulates $\Sigma_1$, by 1a), 1b), 2), 3a), and 3b), there exist $x'_{2,0} \in X_{2,0}$ and $x'_{2,1}, \ldots, x'_{2,|\alpha|} \in X_2$ such that $x'_{2,i} \in X_2 \setminus S_2$, $h_1(x'_{1,j}) = h_2(x'_{2,j})$, $j \in [0, |\alpha|]$, and

$$x'_{2,0} \xrightarrow{\alpha(0)}_2 x'_{2,1} \xrightarrow{\alpha(1)}_2 \cdots \xrightarrow{\alpha(|\alpha|-1)}_2 x'_{2,|\alpha|}.$$

Hence $h_2(x_{2,j}) = h_2(x'_{2,j})$, $j \in [0, |\alpha|]$, and $\Sigma_2$ is infinite-step opaque.

Symmetrically, assume that there exists an opacity-preserving bisimulation relation $\sim \subseteq X_1 \times X_2$ between $\Sigma_1$ and $\Sigma_2$ and system $\Sigma_2$ is infinite-step opaque, we can show that $\Sigma_1$ is also infinite-step opaque. ■

*Remark 1:* Note that although we add in total 8 additional conditions in Definition 6 to make bisimulation relation infinite-step opacity-preserving, these conditions are somehow necessary. That is, without some of them, bisimulation relation may not preserve infinite-step opacity any more. Taking the two NFTSs shown in Fig. 2 for example, bisimulation relation $\sim = \{(1,1'), (2,2'), (1,3'), (2,4')\}$ satisfies 1a), 1b), 1c), 2), 3b), and 3c), but does not satisfy 1d), 3a), or 3d).

*Remark 2:* Remark that the argument for simulation relation preserving infinite-step opacity (one-sided relation) becomes invalid without any one of the conditions in Definition 6. In fact, opacity-preserving simulation relation coincides with opacity-preserving bisimulation relation.

### B. Opacity-preserving quotient relation

From the results in the previous subsection, one can verify the infinite-step opacity of the original system $\Sigma_1$ by verifying it over its abstraction $\Sigma_2$ provided that there exists an opacity-preserving bisimulation relation between $\Sigma_1$ and $\Sigma_2$. In this subsection, we show that the quotient relation defined in (1) between an NFTS and its quotient system is an opacity-preserving bisimulation relation under certain mild assumptions. Hence, one can leverage the existing bisimulation algorithms in the literature [12] with some modifications to construct opacity-preserving abstractions (if existing).

*Theorem 3.3:* Let $\Sigma = (X, X_0, S, U, \to, Y, h)$ be an NFTS and $\sim \subseteq X \times X$ an equivalence relation on $X$ satisfying $h(x) = h(x')$ for all $(x, x') \in \sim$. Assume that for all $x \in S$ and $x' \in X$, if $(x, x') \in \sim$ then $x' \in S$. Then $\sim_Q$ is an opacity-preserving bisimulation relation between $\Sigma$ and $\Sigma_\sim$ if and only if $\sim$ is an opacity-preserving bisimulation relation between $\Sigma$ and itself.

*Proof:* By assumption we have for all $x \in S$ and $x' \in X$, if $(x, x') \in \sim$ then $x' \in S$. This is equivalent to that for all $x \in X$, either $[x] \subseteq S$ or $[x] \cap S = \emptyset$, i.e., $S_\sim = \{[x] | x \in S\}$.

(if:) Assume that $\sim$ is an opacity-preserving bisimulation relation between $\Sigma$ and itself. Next we show that $\sim_Q$ is also an opacity-preserving bisimulation relation between $\Sigma$ and $\Sigma_\sim$ according to Definition 6.

For all $x \in X_0 \cap S$, we have $[x] \in X_{\sim,0} \cap S_\sim$, and $(x, [x]) \in \sim_Q$, i.e., 1a) in Definition 6 holds.

For all $x \in X_0 \setminus S$, we have $[x] \in X_{\sim,0} \setminus S_\sim$, and $(x, [x]) \in \sim_Q$, i.e., 1b) in Definition 6 holds.

For all $[x] \in X_{\sim,0} \cap S_\sim$, we have $[x] \cap X_0 \neq \emptyset$, and $[x] \subseteq S$, then there exists $\bar{x} \in [x]$ such that $\bar{x} \in X_0 \cap S$, and $(\bar{x}, [x]) \in \sim_Q$, i.e., 1c) in Definition 6 holds.

For all $[x] \in X_{\sim,0} \setminus S_\sim$, we have $[x] \cap X_0 \neq \emptyset$, and $[x] \cap S = \emptyset$, then there exists $\bar{x} \in [x]$ such that $\bar{x} \in X_0 \setminus S$, and $(\bar{x}, [x]) \in \sim_Q$, i.e., 1d) in Definition 6 holds.

Now consider an arbitrary pair $(\bar{x}, [x]) \in \sim_Q$, i.e., $\bar{x} \in [x]$. Since $(\bar{x}, x) \in \sim$ and $\sim$ is an opacity-preserving bisimulation relation between $\Sigma$ and itself, one gets $h(\bar{x}) = h(x)$ and using Definition 4, one obtains $h(\bar{x}) = h_\sim([x])$, i.e., 2) in Definition 6 holds.

Now consider an arbitrary pair $(\bar{x}, [x]) \in \sim_Q$, i.e., $\bar{x} \in [x]$.

For every transition $\bar{x} \xrightarrow{u} \bar{x}' \in S$, where $u \in U$, we have $[x] \xrightarrow{u}_\sim [\bar{x}'] \in S_\sim$, and $(\bar{x}', [\bar{x}']) \in \sim_Q$, i.e., 3a) in Definition 6 holds.

For every transition $\bar{x} \xrightarrow{u} \bar{x}' \in X \setminus S$, where $u \in U$, we have $[x] \xrightarrow{u}_\sim [\bar{x}'] \in X_\sim \setminus S_\sim$, and $(\bar{x}', [\bar{x}']) \in \sim_Q$, i.e., 3b) in Definition 6 holds.

For every transition $[x] \xrightarrow{u}_\sim [x'] \in S_\sim$, where $u \in U$, there exists transition $\hat{x} \xrightarrow{u} \hat{x}' \in S$ such that $\hat{x} \in [x]$, and $\hat{x}' \in [x']$. Since $(\bar{x}, \hat{x}) \in \sim$, and $\sim$ is opacity-preserving, there exists transition $\bar{x} \xrightarrow{u} \bar{x}' \in S$ such that $(\hat{x}', \bar{x}') \in \sim$, hence $(\bar{x}', [x']) \in \sim_Q$, i.e., 3c) in Definition 6 holds.

For every transition $[x] \xrightarrow{u}_\sim [x'] \in X_\sim \setminus S_\sim$, where $u \in U$, there exists transition $\hat{x} \xrightarrow{u} \hat{x}' \in X \setminus S$ such that $\hat{x} \in [x]$, and $\hat{x}' \in [x']$. Since $(\bar{x}, \hat{x}) \in \sim$, and $\sim$ is opacity-preserving, there exists transition $\bar{x} \xrightarrow{u} \bar{x}' \in X \setminus S$ such that $(\hat{x}', \bar{x}') \in \sim$, hence $(\bar{x}', [x']) \in \sim_Q$, i.e., 3d) in Definition 6 holds. Hence $\sim_Q$ is opacity-preserving.

(only if:) Assume that $\sim_Q$ is an opacity-preserving bisimulation relation between $\Sigma$ and $\Sigma_\sim$. Now we show that $\sim$ is also an opacity-preserving bisimulation relation between $\Sigma$ and itself according to Definition 6. Since $\sim$ is an equivalence relation, we have $(x, x) \in \sim$ for all $x \in X$.

For all $x \in X_0 \cap S$, we have $(x, x) \in \sim$, i.e., 1a) in Definition 6 holds. Similarly, 1b), 1c), and 1d) in Definition 6 hold.

By the definition of $\sim$, we have $h(x_1) = h(x_2)$ for all $(x_1, x_2) \in \sim$. Hence 2) in Definition 6 holds.

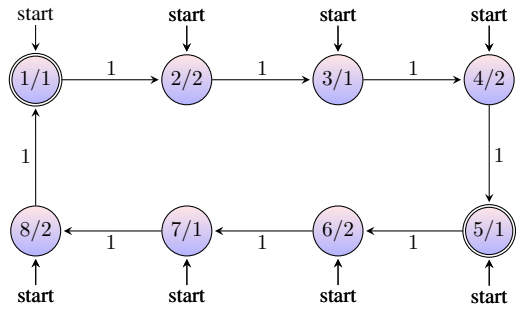


Fig. 3. State transition diagram of the NFTS in Example 3.4.

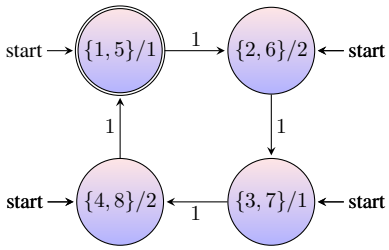


Fig. 4. State transition diagram of the quotient system of the NFTS in Example 3.4 shown in Fig. 3.

Now consider an arbitrary pair $(x_1, x_2) \in \sim$.

For every transition $x_1 \xrightarrow{u} x_1' \in S$, where $u \in U$, we have $[x_1] \xrightarrow{u}_{\sim} [x_1'] \in S_{\sim}$. Since $\sim_{\mathsf{Q}}$ is opacity-preserving, and $(x_2, [x_1]) \in \sim_{\mathsf{Q}}$, there exists transition $x_2 \xrightarrow{u} x_2' \in S \cap [x_1'] = [x_1']$, then $(x_1', x_2') \in \sim$, i.e., 3a) in Definition 6 holds.

For every transition $x_1 \xrightarrow{u} x_1' \in X \setminus S$, where $u \in U$, we have $[x_1] \xrightarrow{u}_{\sim} [x_1'] \in X_{\sim} \setminus S_{\sim}$. Since $\sim_{\mathsf{Q}}$ is opacity-preserving, and $(x_2, [x_1]) \in \sim_{\mathsf{Q}}$, there exists transition $x_2 \xrightarrow{u} x_2' \in (X \setminus S) \cap [x_1'] = [x_1']$, then $(x_1', x_2') \in \sim$, i.e., 3b) in Definition 6 holds.

Symmetrically, 3c) and 3d) in Definition 6 hold. Hence, $\sim$ is an opacity-preserving bisimulation relation between $\Sigma$ and itself. ■

*Remark 3:* Note that the assumption in Theorem 3.3 is necessary for showing the equivalence between $\sim$ being opacity-preserving and $\sim_{\mathsf{Q}}$ being opacity-preserving.

*Example 3.4:* Consider NFTS $\Sigma = (X, X_0, S, U, \rightarrow, Y, h)$ shown in Fig. 3, where $X = \{1,2,3,4,5,6,7,8\} = X_0$, $S = \{1,5\}$, $U = \{1\}$, $Y = \{1,2\}$. It can be readily seen that the equivalence relation $\sim = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(7,7),(8,8),(1,5),(5,1),(2,6),(6,2),(3,7),(7,3),(4,8),(8,4)\} \subseteq X \times X$ is an opacity-preserving bisimulation relation between $\Sigma$ and itself. Under this relation, the quotient system of $\Sigma$ is $\Sigma_{\sim} = (X_{\sim}, X_{\sim,0}, S_{\sim}, U, \rightarrow_{\sim}, Y, h_{\sim})$, where $X_{\sim} = X/\sim = X_{\sim,0}$, $X/\sim = \{\{1,5\},\{2,6\},\{3,7\},\{4,8\}\}$, $S_{\sim} = \{\{1,5\}\}$, which is shown in Fig. 4. It can be easily seen that $\Sigma_{\sim}$ is infinite-step opaque. Therefore, the original NFTS $\Sigma$ is also infinite-step opaque due to the results in Theorem 3.3.

## IV. Conclusion

In this paper, we proposed a bisimulation-based method to verify the infinite-step opacity of nondeterministic finite transition systems (NFTSs). We provided a stronger version of bisimulation relation, called opacity-preserving bisimulation relation, that preserves infinite-step opacity. Therefore, one can try to find an abstraction of a large-scale NFTS based on the relation and then verify the infinite-step opacity of the original NFTS by verifying it over its abstraction. We also used a stronger version of quotient relation between an NFTS and its quotient system to provide a scheme for constructing opacity-preserving abstractions whose constructions will be investigated more in the future.

## References


[1] C. Baier and J. P. Katoen. *Principles of Model Checking*. The MIT Press, 2008.

[2] R. Jacob, J.-J. Lesage, and J.-M. Faure. Overview of discrete event systems opacity: Models, validation, and quantification. *Annual Reviews in Control*, 41:135–146, 2016.

[3] M. Kloetzer and C. Belta. A fully automated framework for control of linear systems from temporal logic specifications. *IEEE Transactions on Automatic Control*, 53(1):287–297, Feb 2008.

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

[5] H. Lin and P. J. Antsaklis. Hybrid dynamical systems: An introduction to control and verification. *Foundations and Trends® in Systems and Control*, 1(1):1–172, 2014.

[6] L. Mazaré. Using unification for opacity properties. *Verimag Technical Report*, 2004.

[7] A. Saboori and C. N. Hadjicostis. Notions of security and opacity in discrete event systems. In *2007 46th IEEE Conference on Decision and Control*, pages 5056–5061, Dec 2007.

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

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

[10] A. Saboori and C. N. Hadjicostis. Verification of initial-state opacity in security applications of discrete event systems. *Information Sciences*, 246:115–132, 2013.

[11] K. Schmidt. Abstraction-based verification of codiagnosability for discrete event systems. *Automatica*, 46(9):1489–1494, 2010.

[12] P. Tabuada. *Verification and Control of Hybrid Systems: A Symbolic Approach*. Springer Publishing Company, Incorporated, 1st edition, 2009.

[13] Y. Wu and S. Lafortune. Comparative analysis of related notions of opacity in centralized and coordinated architectures. *Discrete Event Dynamic Systems*, 23(3):307–339, Sep 2013.

[14] X. Yin and S. Lafortune. A new approach for the verification of infinite-step and $K$-step opacity using two-way observers. *Automatica*, 80:162–171, 2017.

[15] M. Yokotani, T. Kondo, and S. Takai. Abstraction-based verification and synthesis for prognosis of discrete event systems. *Asian Journal of Control*, 18(4):1279–1288, 2016. asjc.1210.

[16] M. Zamani, A. Abate, and A. Girard. Symbolic models for stochastic switched systems: A discretization and a discretization-free approach. *Automatica*, 55:183–196, 2015.