Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 50-1 (2017) 9272–9277

Detectability of Nondeterministic Finite Transition Systems [★]

Kuize Zhang and Majid Zamani

Department of Electrical and Computer Engineering
Technical University of Munich, D-80290 Munich, Germany
(e-mail: {kuize.zhang,zamani}@tum.de)

Abstract: Nondeterministic finite transition systems (NFTSs) have been widely used in the past decade to (approximately) abstract physical systems described by ordinary differential equations. One can leverage the NFTSs and algorithmic machinery for automated synthesis of finite systems to automatically synthesize controllers for the original physical systems against complex logical specifications. The current state detection/estimation of NFTSs is of fundamental importance, as the current state is often used inside the synthesized controllers to compute the current input value for the concrete physical systems. In this paper, the problem of detectability is formulated as whether one can determine the current and all subsequent states of the NFTSs considered by using any sufficiently long input sequence and the corresponding output sequence. We design a polynomial time algorithm to verify the detectability, and based on the algorithm, we design a detector, i.e., a partial function that maps the set of (input, output) sequences of a specific length to the set of states, to determine the current and all subsequent states of detectable NFTSs.

Keywords: Nondeterministic finite transition system, Detectability, Detector

1. INTRODUCTION

In the past few years, *symbolic controller synthesis* has witnessed significant attention Girard and Pappas (2007); Kloetzer and Belta (2008); Reissig (2011); Tabuada (2009); Zamani et al. (2015, 2014, 2012). In this methodology, the requirements for the system are described using a temporal logic (such as linear temporal logic) or using automata Baier and Katoen (2008). Then, one constructs a finite and often nondeterministic abstraction (a.k.a. transition system) of the continuous dynamical system with the property that a controller designed on the abstraction can be refined into a controller on the original system. Finally, using automata-theoretic algorithms from computer science, one computes a discrete controller that ensures that the specifications are met, which is then refined.

Most of the existing techniques on the symbolic controller synthesis require the full (quantized) state information in order to refine the synthesized discrete controllers for the concrete control systems in the closed loop fashion. Unfortunately, this is not the case in many safety-critical applications in which one only has partial state information. Therefore, in order to refine symbolic controllers with only partial state information, one requires to detect/estimate the full (quantized) state information of the plant by leveraging its finite nondeterministic transition system. To this end, one needs to first introduce appropriate notions of detectability and detector for finite nondeterministic transition system which is the main topic of this work.

For linear control systems, many basic control properties, e.g., controllability, observability, disturbance decoupling, etc., have been fully characterized Kalman et al. (1969); Wonham (1985). However, for nonlinear control systems, it is still not known whether the problems of checking controllability, observability, etc., are decidable or not. Since it is difficult to solve those basic control problems for nonlinear control systems, discrete approximation methods have been adopted recently to solve these problems for some classes of nonlinear control systems Girard and Pappas (2007). Although checking controllability and observability for nonlinear control systems may not be decidable, they are mostly decidable for their finite abstractions Broy et al. (2005); Moore (1956). Note that the study on the controllability and observability of finite transition systems goes back to 1956, where "controllability" and "observability" are called "strong connectedness" and "gedanken-experiment", respectively, in Moore (1956).

In the context of symbolic control, the current state and all subsequent states of the nondeterministic symbolic model are of fundamental importance, because these states will be used inside symbolic controllers to compute appropriate control values for the original nonlinear control system to achieve some complex logical specifications. For deterministic finite transition systems, detecting the current state is equivalent to detecting the current and all subsequent states, since once the current state has been obtained, given an input sequence, all subsequent states can be determined. However, this is not the case for nondeterministic finite transition systems. For deterministic finite transition systems, Fornasini and Valcher (2013); Xu and Hong (2013) characterize a strong version of detectability (called "reconstructability" in Fornasini and Valcher (2013), and "current-state observability" in Xu and Hong (2013)) and give quadratic polynomial time algorithms for verifying the detectability in the number of states and inputs. They also propose schemes to design detectors (i.e., a partial function that maps the set of (input, output) sequences of a specific length to the set of states, called "observer" in Fornasini and Valcher (2013), and

[★] This work was supported in part by the German Research Foundation (DFG) through the grant ZA 873/1-1.

10.1016/j.ifacol.2017.08.909

"current-state observer" in Xu and Hong (2013)) to recover the current and all subsequent states. Sandberg (2005); Zhang et al. (2016) characterize a weak version of detectability (called "reconstructibility" in Zhang et al. (2016), and "existence of homing sequences" in Sandberg (2005)). Sandberg (2005) designs a cubic polynomial time algorithm for verifying the weak version of detectability in the number of states and inputs, and Zhang et al. (2016) design a quadratic polynomial time algorithm for verifying the notion. However, no detector is constructed in Sandberg (2005); Zhang et al. (2016).

For nondeterministic finite transition systems, Kushik et al. (2014) study the weak version of detectability in the sense of only determining the current state. To the best of our knowledge, there has been no result on the strong version of detectability of nondeterministic finite transition systems. Due to the importance of the current and all subsequent states, in order to construct a detector, we characterize the strong version of detectability for nondeterministic finite transition systems. In the field of discrete event systems, the strong version of detectability has been studied, and a polynomial time algorithm for verifying the notion in the number of states and events (events are the same as inputs of transition systems from a mathematical point of view) is given in Shu and Lin (2011). Note that nondeterministic finite automata are chosen as the model of discrete event systems in Shu and Lin (2011). In this model, events are spontaneous and can be regarded as the only observations (i.e., outputs). Hence the model of finite automata is intrinsically different from the model of finite transition systems. Despite of this, we can borrow the idea in Shu and Lin (2011) to obtain our main results. On the other hand, if we regard an (input, output)-pair at the same time of a nondeterministic finite transition system as an event, then the detectability studied in this paper is the same as the strong detectability studied in Shu and Lin (2011).

The contribution of this paper is two-fold. First, we give a polynomial time algorithm for verifying the strong version of detectability of nondeterministic finite transition systems. Second, based on the algorithm, we design a detector for detectable nondeterministic finite transition systems. We illustrate the effectiveness of the results via some small examples.

The remainder of this paper is organized as follows. In Section 2, the basic concepts of nondeterministic finite transition systems is introduced. In Section 3, the concept of detectability, an algorithm for verifying the detectability, and a detector for detectable nondeterministic finite transition systems are proposed. Section 4 concludes the paper.

2. NONDETERMINISTIC FINITE TRANSITION SYSTEMS

The following notations are used throughout the paper:

- $\emptyset$: the empty set;
- 2^A: the power set of set A;
- $\mathbb{N}$: the set of non-negative integers;
- $|A|$: the cardinality of set A;
- $[a,b] := \{a, a+1, \dots, b\}, a, b \in \mathbb{N},\ a \le b$.

Nondeterministic finite transition systems (NFTSs) are defined as follows Lin and Antsaklis (2014); Tabuada (2009).

Definition 1. An NFTS S is a sextuple $(X, X_0, U, \to, Y, h)$ consisting of

- a finite set X of states,
- a subset $X_0 \subset X$ of initial states,
- a finite set U of inputs,
- a transition relation $\to \subset X \times U \times X$,
- a set Y of outputs, and
- an output mapping $h : X \to Y$.

In this paper, we consider only total NFTSs, i.e., for all x in X and u in U, there exists at least one x' in X such that $(x, u, x') \in \to$. Actually, for non-total NFTSs, one can make it total by adding a sink state to the NFTS with a self loop labeled with all inputs such that for every state x and input u such that there exists no transition from x under u in the original NFTS, there exists a new transition from x to the sink state under u. For total NFTSs, the transition relation $\to \subset X \times U \times X$ can be equivalently represented as a mapping from $X \times U$ to $2^X \setminus \emptyset$. That is, for all $x, x' \in X$ and $u \in U$, $(x, u, x') \in \to$ if and only if $x' \in \to (x, u)$. In what follows, we will use these two forms alternatively for convenience. An NFTS $(X, X_0, U, \to, Y, h)$ is called deterministic if for all $x \in X$ and $u \in U$, $|\to (x, u)| \le 1$. For every transition $(x, u, x') \in \to$, we also denote (x, u, x') as $x \overset{u}{\to} x'$. For all $x \in X$ and $u \in U$, a state $x' \in X$ satisfying that $(x, u, x') \in \to$ is called a u-successor of x. The set of u-successors of x is denoted by $\mathrm{post}_u(x) := \{x' \in X | (x, u, x') \in \to\}$. Note that for all $x \in X$ and $u \in U$, $|\mathrm{post}_u(x)| \ge 1$.

Let X^* be the set of strings of finite length over X including the string ϵ of length 0, X^ω the set of strings of infinite length also over X. For each $\alpha \in X^* \cup X^\omega$, $|\alpha|$ denotes the length of α, and $|\alpha| = \infty$ if $\alpha \in X^\omega$. For each $\alpha \in X^*$ ($\alpha \in X^\omega$), for all integers $0 \le i \le j \le |\alpha| - 1$ ($0 \le i \le j$), we use $\alpha[i, j]$ to denote $\alpha(i)\alpha(i+1)\dots\alpha(j)$ for short. U^*,U^ω, Y^*,Y^ω are described analogously. For all $x \in X$ and $\alpha \in U^*$ such that $|\alpha| \ge 1$, $x' \in X$ is called an α-successor of x, if there exist $x_0, \dots, x_{|\alpha|} \in X$ such that $x_0 = x$, $x_{|\alpha|} = x'$, and $(x_i, \alpha(i), x_{i+1}) \in \to$ for all integers $0 \le i \le |\alpha| - 1$. The set of α-successors of $x \in X$ (resp. a subset $X' \subset X$) is denoted by $\mathrm{post}_\alpha(x)$ (resp. $\mathrm{post}_\alpha(X') := \cup_{x \in X'} \mathrm{post}_\alpha(x)$). For all $x \in X$, $\alpha \in U^*$ and $\beta \in Y^*$ such that $|\alpha| + 1 = |\beta| \ge 2$, $x' \in X$ is called an (α, β)-successor of x, if there exist $x_0, \dots, x_{|\alpha|} \in X$ such that $x_0 = x$, $x_{|\alpha|} = x'$, $h(x_{|\alpha|}) = \beta(|\alpha|)$, $h(x_i) = \beta(i)$, and $(x_i, \alpha(i), x_{i+1}) \in \to$ for all integers $0 \le i \le |\alpha| - 1$. The set of (α, β)-successors of $x \in X$ (resp. a subset $X' \subset X$) is denoted by $\mathrm{post}_\alpha^\beta(x)$ (resp. $\mathrm{post}_\alpha^\beta(X') := \cup_{x \in X'} \mathrm{post}_\alpha^\beta(x)$). Particularly, we denote $\mathrm{post}_\epsilon^y(X_0) := \{x \in X_0 | h(x) = y\}$ for each $y \in Y$.

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. We give an example to depict these concepts.

Example 2. Consider NFTS $(X, X_0, U, \to, Y, h)$, where $X = \{a, b, c\}$, $X_0 = X$, $U = Y = \{0, 1\}$, $\to = \{(a, 1, a), (a, 0, b), (a, 0, c), (b, 0, b), (b, 1, b), (c, 0, c), (c, 1, b)\}$, $h(a) = 0$, $h(b) = h(c) = 1$ (see Fig. 1).

It can be readily verified that $\mathrm{post}_0(a) = \{b, c\}$, $\mathrm{post}_0^{00}(a) = \emptyset$, $\mathrm{post}_{00}(a) = \{b, c\} = \mathrm{post}_{00}^{011}(a)$.

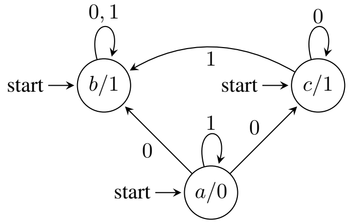

Fig. 1. State transition diagram of the NFTS in Example 2.

3. MAIN RESULTS

In this section, we show the main results of this paper, that is, the notion of detectability of NFTSs, a polynomial time algorithm for verifying the detectability, and a detector for detectable NFTSs.

3.1 Notion of detectability

Definition 3. An NFTS $(X, X_0, U, \to, Y, h)$ is called detectable, if one can determine the current and all subsequent states after a finite steps of observations, formally, there exists a positive integer T_t such that for all input sequences $\alpha \in U^*$ of length $\geq T_t$, and all output sequences $\beta \in Y^*$ of length $|\alpha|+1$, the set $\mathrm{post}_{\alpha}^{\beta}(X_0)$ of (α,β)-successors of the set X_0 of initial states has cardinality ≤ 1.

From Definition 3 one can see that the notion of detectability describes whether the trajectories of the NFTS will enter a fixed set of states, and never leave the set again, but no matter how the NFTS enters the set. So the limit behavior of the NFTS is the key point. From this viewpoint, we characterize the detectability by investigating the limit behavior of the NFTS.

3.2 Verifying detectability

Next we design an algorithm that takes an NFTS as its input, and returns a nondeterministic finite automaton (NFA) that reflects the limit behavior of the NFTS. Let us first recall the notion of an NFA from Sipser (1996). An NFA is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$, where Q is a finite set of states, Σ is a finite set (called alphabet), $\delta \subset Q \times \Sigma \times Q$ is the transition relation, $q_0 \in Q$ is the initial state, and $F \subset Q$ is the set of final states. The transition relation δ is extended to $\delta^* \subset Q \times \Sigma^* \times Q$ in the usual way: for all $q, q' \in Q$, $(q, \epsilon, q') \in \delta^*$ if and only if $q = q'$; for all $q, q' \in Q$ and $\sigma_0 \dots \sigma_{n-1} \in \Sigma^* \setminus \{\epsilon\}$, $(q, \sigma_0 \dots \sigma_{n-1}, q') \in \delta^*$ if and only if there exist $q_1, \dots, q_{n-1} \in Q$ such that $(q, \sigma_0, q_1), (q_1, \sigma_1, q_2), \dots, (q_{n-1}, \sigma_{n-1}, q') \in \delta$. Hereinafter we use δ to denote δ^*, as no confusion will occur. A state $q \in Q$ is said to be reachable from a state $q' \in Q$, if there exists $\sigma \in \Sigma^*$ such that $(q', \sigma, q) \in \delta$. A state $x \in Q$ is called reachable from a subset Q' of Q, if x is reachable from some state of Q'. A sequence of states $q_0, \dots, q_n \in Q$ is called a path, if there exist $\sigma_0, \dots, \sigma_{n-1} \in \Sigma$ such that $(q_0, \sigma_0, q_1), \dots, (q_{n-1}, \sigma_{n-1}, q_n) \in \delta$. A path $q_0, \dots, q_n \in Q$ is called a cycle, if $q_0 = q_n$. Note that $\delta \subset Q \times \Sigma^* \times Q$ is equivalently represented as a function $\delta : Q \times \Sigma^* \to 2^Q$: for all $q, q' \in Q$ and $\sigma \in \Sigma^*$, $(q, \sigma, q') \in \delta$ if and only if $q' \in \delta(q, \sigma)$. In what follows, we will also use these two forms alternatively for convenience. For more details, we refer the reader to Sipser (1996). With these basic concepts, we present the following algorithm.

Algorithm 1. Receive an NFTS $(X, X_0, U, \to, Y, h)$, and initiate an NFA $(Q, \Sigma, \delta, q_0, F)$, where $Q = \{\diamond\}$, $\Sigma = \delta = F = \emptyset$, $q_0 = \diamond$. $Q_1 := \emptyset$, $Q_2 := \emptyset$. Let symbol ϕ not be in Y.

```
(1) For each $y \in Y$, denote $X_y := \{x \in X_0 | h(x) = y\}$,
    (a) if $|X_y| = 1$, then $Q_1 := Q_1 \cup \{X_y\}$, $\Sigma := \Sigma \cup \{(\phi, y)\}$, $\delta := \delta \cup \{(\diamond, (\phi, y), X_y)\}$,
    (b) else if $|X_y| > 1$, then $Q_1 := Q_1 \cup \{Z \subset X_y | |Z| = 2\}$, $\Sigma := \Sigma \cup \{(\phi, y)\}$, for each $Z \subset X_y$ satisfying that $|Z| = 2$, $\delta := \delta \cup \{(\diamond, (\phi, y), Z)\}$.
    $Q := Q \cup Q_1$, $Q_2 := Q_2 \cup Q_1$, $Q_1 := \emptyset$.
(2) If $Q_2 = \emptyset$, stop, otherwise for each $q_2 \in Q_2$, denote $y_0 := h(x)$, where $x \in q_2$, for each $u \in U$ and each $y \in Y$,
    (a) if $|\mathrm{post}_u^{y_0 y}(q_2)| = 1$, then $\Sigma := \Sigma \cup \{(u, y)\}$, $\delta := \delta \cup \{(q_2, (u, y), \mathrm{post}_u^{y_0 y}(q_2))\}$, if $\mathrm{post}_u^{y_0 y}(q_2) \notin Q$ then $Q_1 := Q_1 \cup \{\mathrm{post}_u^{y_0 y}(q_2)\}$,
    (b) else if $|\mathrm{post}_u^{y_0 y}(q_2)| > 1$, then $\Sigma := \Sigma \cup \{(u, y)\}$, for each $Z \subset \mathrm{post}_u^{y_0 y}(q_2)$ satisfying $|Z| = 2$, $\delta := \delta \cup \{(q_2, (u, y), Z\}$, if $Z \notin Q$ then $Q_1 := Q_1 \cup \{Z\}$.
    $Q := Q \cup Q_1$, $Q_2 := \emptyset$, $Q_2 := Q_1$, $Q_1 := \emptyset$.
(3) Go to Step (2). (Since $X, U, Y$ are finite, the algorithm will terminate.)
```

Putting the NFTS in Example 2 (shown in Fig. 1) into Algorithm 1, we illustrate how Algorithm 1 returns an NFA step by step in Fig. 2.

If we regard the NFA that Algorithm 1 returns as a dynamical system in which each state is initial, and regard each state of the NFA as a point of the dynamical system, then limit points can be defined as below by borrowing the concept of limit points of cellular automata Kari (2016).

Definition 4. Consider an NFA that Algorithm 1 returns as a nondeterministic dynamical system. Regarding each state of the NFA as initial, and regarding each state as a point of the system, then limit points are defined as points that can be visited at each time step. The limit set consists of limit points.

It can be seen that limit points are exactly the points reachable from some cycle. According to this concept, after we put an NFTS $(X, X_0, U, \to, Y, h)$ into Algorithm 1, each state of the obtained NFA has a successor, hence reaches a state of the limit set, and the NFA has a nonempty limit set, since the NFTS is total.

Definition 5. The smallest natural number T_t such that each pair of input sequence of length T_t and output sequence of length $T_t + 1$ changes the initial state of the NFA to a state of the limit set is called the transient period.

That is,

$$\begin{aligned} T_t = \min\{ & t \in \mathbb{N} | \forall u_1, \dots, u_t \in U, \forall y_0, \dots, y_t \in Y, \\ & \text{if } \delta(\diamond, (\phi, y_0)(u_1, y_1) \dots (u_t, y_t)) \text{ is not empty,} \\ & \text{then all elements of } \delta(\diamond, (\phi, y_0)(u_1, y_1) \dots (u_t, y_t)) \\ & \text{are limit points of the NFA.}\}. \end{aligned} \tag{1}$$

Taking the NFA shown in the bottom of Fig. 2 for example, its limit set is $\{\{a\}, \{b\}, \{b, c\}\}$, and its transient period T_t equals 0. From this figure, if we choose input sequence 0^ω, where 0^ω means an infinite sequence consisting of 0's, and if the corresponding output sequence is 1^ω, then at each time step, the state can be either b or c, i.e., the NFTS in Example 2 is not

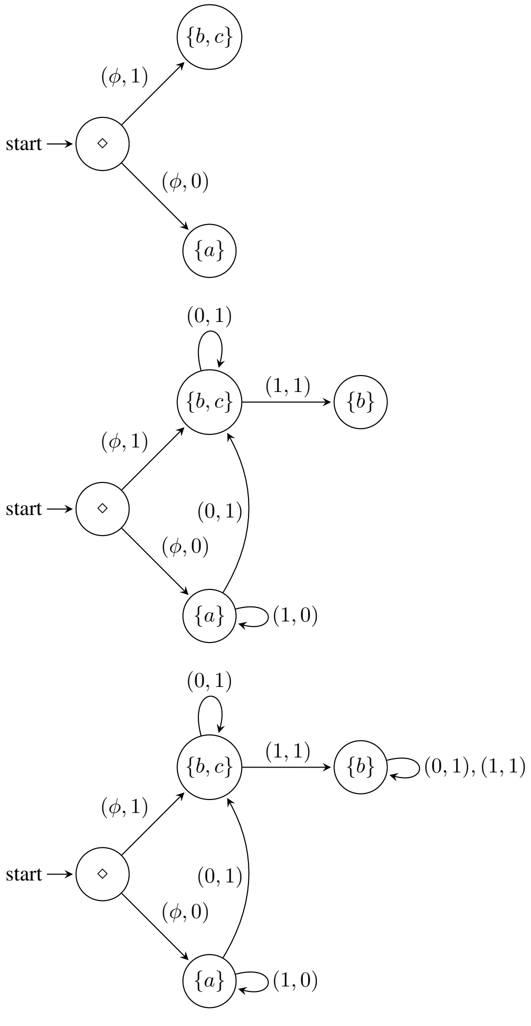

Fig. 2. Process of Algorithm 1 receiving the NFTS in Example 2 and returning an NFA.

detectable. The following theorem that can be used to verify the detectability of NFTSs follows from this intuitive idea.

Theorem 6. An NFTS $(X, X_0, U, \to, Y, h)$ is detectable if and only if in the NFA that Algorithm 1 returns after taking the NFTS as input, each state reachable from some cycle is a singleton, i.e., a subset of X with cardinality 1.

Proof. Note that the number of states of the NFA $\mathcal{A} = (Q, \Sigma, \delta, \diamond, \emptyset)$ that Algorithm 1 returns is no greater than $N := |X|(|X|-1)/2 + |X| + 1$.

Assume that the NFTS is not detectable. Then there exists an input sequence $\alpha \in U^*$ of length greater than N and an output sequence $\beta \in Y^*$ of length $|\alpha|+1$ such that $\mathrm{post}_{\alpha}^{\beta}(X_0)$ has cardinality > 1, and for each integer $0 \le i < |\alpha|$, $\mathrm{post}_{\alpha[0,i]}^{\beta[0,i+1]}(X_0)$ is not empty. Choose $q_{|\alpha|} \subset \mathrm{post}_{\alpha}^{\beta}(X_0)$ satisfying that $|q_{|\alpha|}| = 2$. For all $j = 2, \dots, |\alpha|$, choose nonempty $q_{|\alpha|-j+1} \subset \mathrm{post}_{\alpha[0,|\alpha|-j]}^{\beta[0,|\alpha|-j+1]}(X_0)$ satisfying that $|q_{|\alpha|-j+1}| = 2$ if $|\mathrm{post}_{\alpha[0,|\alpha|-j]}^{\beta[0,|\alpha|-j+1]}(X_0)| \ge 2$, and for each $x \in q_{|\alpha|-j+2}$, $(x', \alpha(|\alpha|-j+1), x) \in \to$ for some $x' \in q_{|\alpha|-j+1}$. Choose $q_0 \subset X_0$ satisfying that $|q_0| = 2$ if $|X_0| \ge 2$, and for each $x \in q_1$, $(x', \alpha(0), x) \in \to$ for some $x' \in q_0$.

Then $q_0, \dots, q_{|\alpha|}$ are states of the NFA $\mathcal{A}$, q_i is reachable from q_{i-1} for all integers $0 < i \le |\alpha|$, and there exist $0 \le j < k \le |\alpha|$ such that $q_j = q_k$ by the pigeon-hole principle. Hence $q_{|\alpha|}$ is reachable from the cycle $q_j, \dots, q_k$, i.e., $q_{|\alpha|}$ is a limit point of $\mathcal{A}$ with cardinality > 1. Hence the "if" part holds.

Assume that the NFTS is detectable. We are given an arbitrary state q of the NFA $\mathcal{A}$ and assume that q is reachable from a cycle. Then there exist states $q_1, \dots, q_p \in Q$ such that q_1 is reachable from $\diamond$, q_{i+1} is reachable from q_i for all integers $1 \le i < p$, q is reachable from q_p, and $q_j = q_k$ for some integers $1 \le j < k \le p$. By the automaton $\mathcal{A}$, there exist $u_1, \dots, u_p \in U$ and $y_0, \dots, y_p \in Y$ such that $(\diamond, (\phi, y_0), q_1), (q_1, (u_1, y_1), q_2), \dots, (q_p, (u_p, y_p), q) \in \delta$. Since the NFTS is detectable, for sufficiently large integer n, the set $\mathrm{post}_{\mathbb{U}_n}^{\mathbb{Y}_n}(X_0)$ has cardinality ≤ 1, where $\mathbb{U}_n = u_1 \dots u_{j-1}(u_j \dots u_{k-1})^n u_k \dots u_p$, $\mathbb{Y}_n = y_0 y_1 \dots y_{j-1} (y_j \dots y_{k-1})^n y_k \dots y_p$, and $(\cdot)^n$ means the concatenation of n copies of $\cdot$. We also have $\emptyset \ne q \subset \mathrm{post}_{\mathbb{U}_n}^{\mathbb{Y}_n}(X_0)$, then $|q| = 1$, which completes the proof.

Next we give an example to illustrate Theorem 6.

Example 7. Consider the NFTS $(X, X_0, U, \to, Y, h)$, where $X = \{a,b,c,d,e,f,g\}$, $X_0 = \{a,b,c\}$, $U = \{u_1, u_2\}$, $Y = \{a,b\}$, $\to = \{(a,u_1,d), (a,u_2,d), (b,u_2,d), (b,u_1,e), (b,u_2,e), (c,u_2,e), (c,u_1,f), (c,u_1,g), (d,u_1,d), (d,u_2,d), (e,u_1,d), (e,u_2,d), (f,u_1,e), (f,u_2,e), (g,u_1,f), (g,u_2,f)\} \subset X \times U \times X$, $h(a) = h(b) = h(c) = a$, $h(d) = h(e) = h(f) = h(g) = b$, as illustrated in Fig. 3.

Put this NFTS into Algorithm 1, we obtain the NFA $(Q, \Sigma, \delta, \diamond, \emptyset)$ (shown in Fig. 4), where $Q = \{\diamond, \{a,b\}, \{b,c\}, \{a,c\}, \{d,e\}, \{e,f\}, \{e,g\}, \{f,g\}, \{d,f\}, \{d,g\}, \{d\}\}$, $\Sigma = \{(\phi,a), (u_1,b), (u_2,b)\}$, $\delta = \{(\diamond, (\phi,a), \{a,b\}), (\diamond, (\phi,a), \{b,c\}), (\diamond, (\phi,a), \{a,c\}), (\{a,b\}, (u_1,b), \{d,e\}), (\{a,b\}, (u_2,b), \{d,e\}), (\{b,c\}, (u_2,b), \{d,e\}), (\{b,c\}, (u_1,b), \{e,f\}), (\{b,c\}, (u_1,b), \{e,g\}), (\{b,c\}, (u_1,b), \{f,g\}), (\{a,c\}, (u_1,b), \{f,g\}), (\{a,c\}, (u_1,b), \{d,f\}), (\{a,c\}, (u_1,b), \{d,g\}), (\{a,c\}, (u_2,b), \{d,e\}), (\{d,e\}, (u_1,b), \{d\}), (\{d,e\}, (u_2,b), \{d\}), (\{d\}, (u_1,b), \{d\}), (\{d\}, (u_2,b), \{d\}), (\{e,f\}, (u_1,b), \{d,e\}), (\{e,f\}, (u_2,b), \{d,e\}), (\{e,g\}, (u_1,b), \{d,f\}), (\{e,g\}, (u_2,b), \{d,f\}), (\{f,g\}, (u_1,b), \{e,f\}), (\{f,g\}, (u_2,b), \{e,f\}), (\{d,f\}, (u_1,b), \{d,e\}), (\{d,f\}, (u_2,b), \{d,e\}), (\{d,g\}, (u_1,b), \{d,f\}), (\{d,g\}, (u_2,b), \{d,f\})\}$. The limit set of the NFA is $\{\{d\}\}$, where $\{d\}$ is a singleton, hence the NFTS is detectable. The transient period of the NFA equals 4 (see one of the longest paths from the initial state $\diamond$ to the limit set of the NFA (the path represented by thick arrows) in Fig. 4).

3.3 Complexity analysis

Let us analyze the computational complexity of using Theorem 6 to verify the detectability of NFTSs. The NFA that Algorithm 1 returns has at most $|X|(|X|-1)/2 + |X| + 1$ states, from each state there exist at most $|X|(|X|-1)/2 + |X|$ transitions since the elements of successors of each state of the NFA under a given (input, output)-pair produce the same output, so the construction of the NFA costs at most $|X|(|X|-1)/2 + |X| + 1 + (|X|(|X|-1)/2 + |X| + 1)(|X|(|X|-1)/2 + |X|)$. In order to find the limit set, one can use the classical depth-first search algorithm Jungnickel (2013), i.e, visit an arbitrary path from the initial state step by step, until the first time a state

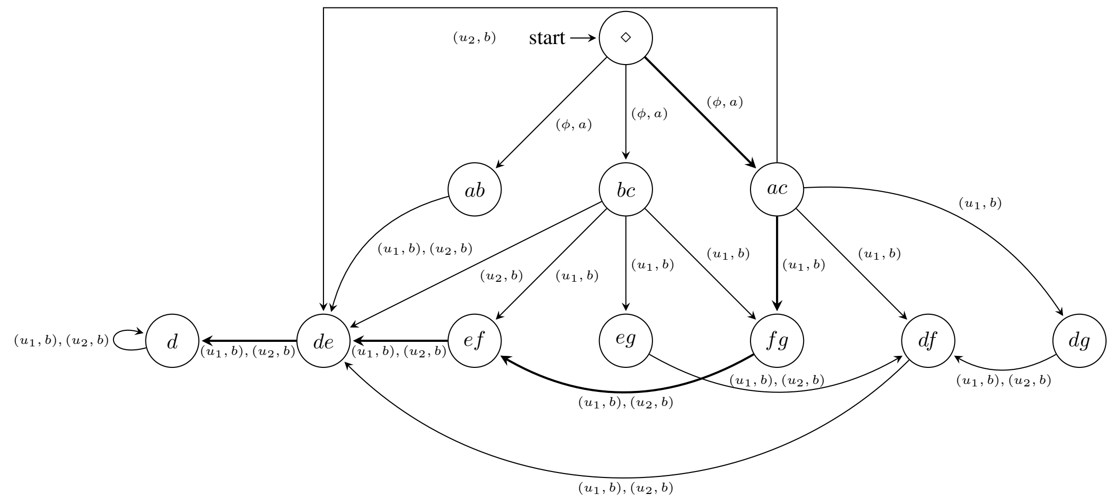

Fig. 4. NFA returned by Algorithm 1 after receiving the NFTS in Example 7 (shown in Fig. 3) as its input.

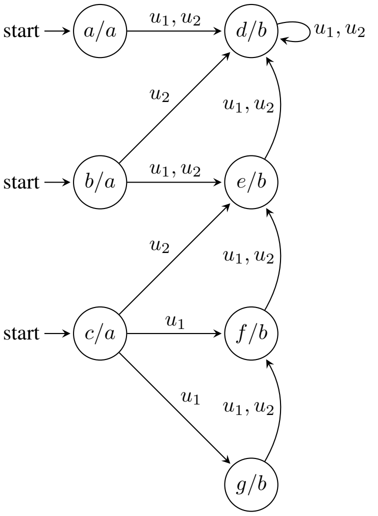

Fig. 3. State transition diagram of the NFTS in Example 7.

has been visited twice, then all states reachable from the state belong to the limit set. After that, one can repeat this procedure until every state has been visited. The process of finding the limit set is proportional to the size of the NFA. Hence the overall computational complexity of using Theorem 6 to verify the detectability of NFTSs is $O(|X|^4)$.

3.4 Detector

We use Algorithm 1 and Theorem 6 to construct a detector for a detectable NFTS. Given a detectable NFTS $(X, X_0, U, \to, Y, h)$ and feeding it into Algorithm 1, one obtains an NFA $(Q, \Sigma, \delta, \diamond, \emptyset)$. Denoted by T_t, the transient period of the NFA, the following proposition holds.

Proposition 8. Given a detectable NFTS $(X, X_0, U, \to, Y, h)$, let T_t be the transient period of the NFA $\mathcal{A} = (Q, \Sigma, \delta, \diamond, \emptyset)$ that Algorithm 1 returns after receiving the NFTS. Then for all input sequences $\alpha \in U^*$ of length $\geq T_t$ and output sequences $\beta \in Y^*$ of length $|\alpha| + 1$, $\mathrm{post}_\alpha^\beta(X_0)$ has cardinality ≤ 1.

Proof. Since the NFTS is detectable, all limit points of $\mathcal{A}$ are singletons by Theorem 6. In order to prove this proposition, we only need to prove that for all input sequences $\alpha \in U^*$ of length T_t and output sequences $\beta \in Y^*$ of length $|\alpha| + 1$, $\delta(\diamond, (\phi, \beta(0))(\alpha(0), \beta(1)) \dots (\alpha(T_t - 1), \beta(T_t)))$ has cardinality ≤ 1. (Note that the union of elements of $\delta(\diamond, (\phi, \beta(0))$ $(\alpha(0), \beta(1)) \dots (\alpha(T_t - 1), \beta(T_t)))$ equals $\mathrm{post}_\alpha^\beta(X_0)$.) Suppose on the contrary that there exist $u_1, \dots, u_{T_t} \in U$, $y_0, \dots, y_{T_t} \in Y$, $q_0, \dots, q_{T_t}, q'_0, \dots, q'_{T_t} \subset X$ such that $0 < |q_i| \leq 2$ and $0 < |q'_i| \leq 2$ for all integers $0 \leq i \leq T_t$, $|q_{T_t}| = |q'_{T_t}| = 1$, $q_{T_t} \neq q'_{T_t}$, $(\diamond, (\phi, y_0), q_0), (\diamond, (\phi, y_0), q'_0) \in \delta$, $(q_j, (u_{j+1}, y_{j+1}), q_{j+1}), (q'_j, (u_{j+1}, y_{j+1}), q'_{j+1}) \in \delta$ for all integers $0 \leq j \leq T_t - 1$. For each integer $0 \leq i \leq T_t$, choose $x_i \in q_i$, $x'_i \in q'_i$ such that $(x_0, u_1, x_1) \in \to$, $(x'_0, u_1, x'_1) \in \to$, $\dots$, $(x_{T_t-1}, u_{T_t}, x_{T_t}) \in \to$, $(x'_{T_t-1}, u_{T_t}, x'_{T_t}) \in \to$. Denote $q''_i := \{x_i, x'_i\}$, $i = 0, \dots, T_t$. Then $|q''_{T_t}| = 2$. If $|q''_0| = 1$, and there exists $x \in X \setminus q''_0$ satisfying $h(x) = h(x_0)$, then add at most one such x into q''_0, i.e., $q''_0 := q''_0 \cup \{x\}$, and in this case $|q''_0| = 2$. Then we modify $q''_1, \dots, q''_{T_t-1}$ successively as follows. For all integers $j = 1, \dots, T_t - 1$, if $|q''_j| = 1$, and there exists $x \in X \setminus q''_j$ satisfying that $h(x) = h(x_j)$, and $(x', u_j, x) \in \to$ for some $x' \in q''_{j-1}$, then we add at most one such x into q''_j, i.e., $q''_j := q''_j \cup \{x\}$, and in this case $|q''_j| = 2$. As a result, $q''_0, \dots, q''_{T_t}$ are states of $\mathcal{A}$, and $(\diamond, (\phi, y_0), q''_0) \in \delta$, $(q''_j, (u_{j+1}, y_{j+1}), q''_{j+1}) \in \delta$ for all integers $0 \leq j \leq T_t - 1$. By the definition of transient period, q''_{T_t} is a limit point of $\mathcal{A}$. But q''_{T_t} has cardinality 2, which contradicts that all limit points of $\mathcal{A}$ are singletons. Hence Proposition 8 holds.

Note that for a detectable NFTS, by Proposition 8 one gets

$$T_t \geq T'_t := \min\{t \in \mathbb{N} | \text{for all } \alpha \in U^* \text{ and } \beta \in Y^* \text{ satisfying } |\alpha| \geq t \text{ and } |\beta| = |\alpha| + 1, |\mathrm{post}_\alpha^\beta(X_0)| \leq 1\}.$$

Remark that the strict inequality (e.g. $>$) may hold in the above inequality. For example, take the NFTS $(X, X_0, U, \to, Y, h)$, where $X = \{a, b\} = Y$, $X_0 = \{a\}$, $U = \{0\}$, $\to = \{(a, 0, b), (b, 0, b)\}$, $h(a) = a$, and $h(b) = b$. It can be readily seen that this NFTS is detectable, and satisfies that $T_t = 1 > T'_t = 0$.

In order to design a detector, one should observe an NFTS from any time, so any time should be regarded as the initial time. In order to guarantee this, we assume that $X_0 = X$ hereinafter. Under this assumption, according to Proposition 8, a detector is defined as a partial function $\mathrm{det} : U^{T_t} \times Y^{T_t+1} \to X$: for all

$(\alpha, \beta) \in U^{T_t} \times Y^{T_t+1}$,

$$\det(\alpha,\beta) = \begin{cases} \begin{array}{l}\text{the unique element of}\\ \operatorname{post}_{\alpha}^{\beta}(X_0)\end{array} & \text{if } |\operatorname{post}_{\alpha}^{\beta}(X_0)| = 1, \\ \text{undefined} & \text{otherwise.} \end{cases} \tag{2}$$

4. CONCLUSION

In this paper, we gave a polynomial time algorithm for verifying a strong version of detectability of nondeterministic finite transition systems, and also designed a detector for detectable nondeterministic finite transition systems. The problems of how to define and verify weaker versions of detectability, and how to design detectors in the sense of those versions of detectability are left for further study.

REFERENCES

Baier, C. and Katoen, J.P. (2008). *Principles of Model Checking*. The MIT Press.

Broy, M., Jonsson, B., Katoen, J.P., Martin, L., and Pretschner, A. (2005). *Model-Based Testing of Reactive Systems: Advanced Lectures (Lecture Notes in Computer Science)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA.

Fornasini, E. and Valcher, M.E. (2013). Observability, reconstructibility and state observers of boolean control networks. *IEEE Transactions on Automatic Control*, 58(6), 1390–1401.

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

Jungnickel, D. (2013). *Graphs, Networks and Algorithms*. Springer Publishing Company, Incorporated, fourth edition.

Kalman, R.E., Falb, P.L., and Arbib, M.A. (1969). *Topics in mathematical system theory*. International series in pure and applied mathematics. McGraw-Hill.

Kari, J. (2016). *Cellular Automata*. `http://users.utu.fi/jkari/ca2016/`.

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

Kushik, N.G., Kulyamin, V.V., and Evtushenko, N.V. (2014). On the complexity of existence of homing sequences for nondeterministic finite state machines. *Programming and Computer Software*, 40(6), 333–336.

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

Moore, E.F. (1956). Gedanken-experiments on sequential machines. *Automata Studies, Annals of Math. Studies*, 34, 129–153.

Reissig, G. (2011). Computing abstractions of nonlinear systems. *IEEE Transactions on Automatic Control*, 56(11), 2583–2598.

Sandberg, S. (2005). *1 Homing and Synchronizing Sequences*, 5–33. Springer Berlin Heidelberg, Berlin, Heidelberg.

Shu, S. and Lin, F. (2011). Generalized detectability for discrete event systems. *Systems & Control Letters*, 60(5), 310–317.

Sipser, M. (1996). *Introduction to the Theory of Computation*. International Thomson Publishing, 1st edition.

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

Wonham, W.M. (1985). *Linear Multivariable Control: a Geometric Approach 3rd Ed.* Springer-Verlag New York.

Xu, X. and Hong, Y. (2013). Observability analysis and observer design for finite automata via matrix approach. *IET Control Theory Applications*, 7(12), 1609–1615.

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

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

Zamani, M., Pola, G., Mazo, M., and Tabuada, P. (2012). Symbolic models for nonlinear control systems without stability assumptions. *IEEE Transactions on Automatic Control*, 57(7), 1804–1809.

Zhang, K., Zhang, L., and Su, R. (2016). A weighted pair graph representation for reconstructibility of boolean control networks. *SIAM Journal on Control and Optimization*, 54(6), 3040–3060.