IEICE TRANS. INF. & SYST., VOL.E97–D, NO.5 MAY 2014

PAPER Special Section on Formal Approach

Bisimilarity Control of Nondeterministic Discrete Event Systems under Event and State Observations

Katsuyuki KIMURA[†a)], *Nonmember and* **Shigemasa TAKAI**[†b)], *Member*

SUMMARY In this paper, we study a supervisory control problem for plants and specifications modeled by nondeterministic automata. This problem requires to synthesize a nondeterministic supervisor such that the supervised plant is bisimilar to a given specification. We assume that a supervisor can observe not only the event occurrence but also the current state of the plant, and introduce a notion of completeness of a supervisor which guarantees that all nondeterministic transitions caused by events enabled by the supervisor are defined in the supervised plant. We define a notion of partial bisimulation between a given specification and the plant, and prove that it serves as a necessary and sufficient condition for the existence of a bisimilarity enforcing complete supervisor.

key words: *discrete event system, supervisory control, nondeterministic system, bisimilarity control*

1. Introduction

The supervisory control theory for controlling discrete event systems (DESs) with logical specifications was introduced in [1]. In the conventional supervisory control problem, both a plant and a specification are represented by deterministic automata, and equivalence between the generated or marked language of the supervised plant and the specification language is required.

Due to the model abstraction or the unmodeled dynamics, nondeterminism of transitions can arise in the plant and specification models [2], [3]. Various supervisory control problems for nondeterministic systems were studied in [2]–[10]. In particular, a general case that both the plant and the specification are nondeterministic, and a supervisor is allowed to be nondeterministic was considered in [2], [9]. When both the plant and the specification are nondeterministic, a notion of equivalence stronger than language equivalence is required between the supervised plant and the specification. Bisimulation equivalence introduced in [11] is such a notion of equivalence widely-used for verification and control of dynamical systems.

A problem of synthesizing a nondeterministic supervisor enforcing bisimulation equivalence between the supervised plant and the specification was studied in [2], [9]. In [2], a supervisor observes each event occurrence of the plant, and the supervised plant is modeled by the synchronous composition of the plant and the supervisor. A small model theorem was provided to show that a supervisor enforcing bisimulation equivalence between the supervised plant and the specification exists if and only if such a supervisor whose state space is the power set of the Cartesian product of the plant and the specification state spaces exists. The complexity of verifying the existence of a supervisor using the small model theorem is doubly exponential in the sizes of the plant and the specification. The small model theorem was generalized to the setting of partial event observation in [12]. To reduce the computational complexity for verifying the existence of a supervisor, a special case that a supervisor is deterministic was considered in [10]. It was shown that, in this special case, the complexity for verifying the existence of a bisimilarity enforcing deterministic supervisor is linear in the size of the plant and singly exponential in the size of the specification. In [9], a nondeterministic automaton model of the supervised plant was defined with respect to a certain relation between the plant and the specification state spaces. A notion of simulation-based controllability was introduced as a necessary and sufficient condition for the existence of a bisimilarity enforcing supervisor (under full event observation). However, it is possible that certain nondeterministic transitions become deterministic and that certain transitions by uncontrollable events have to be disabled to achieve bisimilarity between the supervised plant and the simulation-based controllable specification as shown in this paper. Disabling transitions by uncontrollable events is unsuitable for the framework of supervisory control.

State feedback control of DESs with state based specifications has been widely studied in the literature including [13]–[18] under the assumption that the current state of the system is fully observable. For example, the state set of a machine can be modeled as {ON, OFF}, {BUSY, IDLE, DOWN}, and so on [19]. The state set of a computer running a program can be modeled as {WAITING FOR INPUT, RUNNING, DOWN} [19]. Such a state of a machine/computer can be generally identified by monitoring. In addition, an inventory consisting of discrete entities such as products and people has the state space $\{0, 1, 2, \ldots, \}$ [19]. The number of such entities can be counted in general.

In this paper, we assume that a supervisor can observe not only the event occurrence but also the current state of the plant, and in a similar way to [9], define a nondeterministic automaton model of the supervised plant based on a certain relation between the state spaces of the plant and the supervisor. The purpose of this paper is to show that if

Manuscript received July 4, 2013.
Manuscript revised October 25, 2013.

[†]The authors are with the Division of Electrical, Electronic and Information Engineering, Osaka University, Suita-shi, 565–0871 Japan.
a) E-mail: kimura@is.eei.eng.osaka-u.ac.jp
b) E-mail: takai@eei.eng.osaka-u.ac.jp

DOI: 10.1587/transinf.E97.D.1140

the current state of the plant is observable in addition to the event occurrence, then the existence of a bisimilarity enforcing supervisor can be polynomially verified. We introduce a notion of completeness of a supervisor, which requires that all nondeterministic transitions caused by events enabled by the supervisor are defined in the supervised plant. This notion of completeness in the nondeterministic setting can be regarded as an extension of completeness in the deterministic setting of [1]. In contrast to [9], the notion of completeness guarantees that nondeterministic transitions never become deterministic and that transitions caused by uncontrollable events are never disabled. Furthermore, we define a notion of partial bisimulation between a given specification and the plant in the nondeterministic setting. This notion of partial bisimulation can be regarded as an extension of that defined in the deterministic setting in [20]. Then, we prove that partial bisimulation is a necessary and sufficient condition for the existence of a complete supervisor such that the supervised plant is bisimilar to a given specification. Moreover, when the state sets of the plant and the specification are finite, we show how to search for a partial bisimulation relation between the specification and the plant in order to verify the condition for the existence of a complete supervisor efficiently. Compared to [2], we impose an additional assumption that a supervisor can observe the current state of the plant. However, the complexity of verifying the condition for the existence of a complete supervisor is polynomial in the sizes of the plant and the specification.

The results of this paper were first reported in [21] but without proofs. This paper contains their complete proofs and a new example.

2. Preliminaries

A nondeterministic automaton G is defined as a 5-tuple $G = (X, \Sigma, \alpha, X_0, X_m)$, where X is the set of states, Σ is the finite set of events, $\alpha : X \times \Sigma \to 2^X$ is the state transition function, $X_0 \subseteq X$ is the set of initial states, and $X_m \subseteq X$ is the set of marked states. Here, 2^X is the power set of X. For simplicity, we do not consider ε-transitions.

Let Σ^* be the set of all finite strings of elements in Σ, including the empty string ε. The state transition function α can be generalized to $\alpha : X \times \Sigma^* \to 2^X$ as follows:

- $\forall x \in X : \alpha(x, \epsilon) = \{x\}$.
- $\forall x \in X, \forall s \in \Sigma^*, \forall \sigma \in \Sigma :$

$$\alpha(x, s\sigma) = \bigcup_{x' \in \alpha(x,s)} \alpha(x', \sigma).$$

In addition, for any $X' \subseteq X$ and any $s \in \Sigma^*$, we let $\alpha(X', s) = \bigcup_{x' \in X'} \alpha(x', s)$. The generated and marked languages of G are defined as $L(G) = \{s \in \Sigma^* \mid \alpha(X_0, s) \neq \emptyset\}$ and $L_m(G) = \{s \in \Sigma^* \mid \alpha(X_0, s) \cap X_m \neq \emptyset\}$, respectively.

We introduce a simulation relation and a bisimulation relation for nondeterministic automata.

Definition 1: Let $G_1 = (X_1, \Sigma, \alpha_1, X_{01}, X_{m1})$ and $G_2 = (X_2, \Sigma, \alpha_2, X_{02}, X_{m2})$ be two nondeterministic automata. If the following three conditions are satisfied by a relation $\Phi \subseteq X_1 \times X_2$, Φ is said to be a simulation relation from G_1 to G_2.

- $\forall x_{01} \in X_{01}, \exists x_{02} \in X_{02} : (x_{01}, x_{02}) \in \Phi$.
- $\forall (x_1, x_2) \in \Phi, \forall \sigma \in \Sigma, \forall x'_1 \in \alpha_1(x_1, \sigma), \exists x'_2 \in \alpha_2(x_2, \sigma) : (x'_1, x'_2) \in \Phi$.
- $\forall (x_1, x_2) \in \Phi : x_1 \in X_{m1} \Rightarrow x_2 \in X_{m2}$.

If Φ is a simulation relation from G_1 to G_2, we denote $G_1 \sqsubseteq_\Phi G_2$.

For any relation $\Phi \subseteq X_1 \times X_2$, its inverse relation $\Phi^{-1} \subseteq X_2 \times X_1$ is defined as $\Phi^{-1} = \{(x_2, x_1) \in X_2 \times X_1 \mid (x_1, x_2) \in \Phi\}$.

Definition 2: Let $G_1 = (X_1, \Sigma, \alpha_1, X_{01}, X_{m1})$ and $G_2 = (X_2, \Sigma, \alpha_2, X_{02}, X_{m2})$ be two nondeterministic automata. If a relation $\Phi \subseteq X_1 \times X_2$ is a simulation relation from G_1 to G_2, and its inverse relation $\Phi^{-1} \subseteq X_2 \times X_1$ is a simulation relation from G_2 to G_1, then Φ is said to be a bisimulation relation between G_1 and G_2.

If Φ is a bisimulation relation between G_1 and G_2, we denote $G_1 \simeq_\Phi G_2$.

If there exists a simulation relation from G_1 to G_2, G_1 is said to be simulated by G_2, and we denote $G_1 \sqsubseteq G_2$. In addition, if there exists a bisimulation relation between G_1 and G_2, G_1 is said to be bisimilar to G_2, and we denote $G_1 \simeq G_2$.

3. Supervisory Control under Event and State Observations

In this section, we define a relation-based supervised plant model, and formulate a bisimilarity enforcing supervisory control problem under event and state observations. We assume that the plant and the specification are modeled by nondeterministic automata $G = (X, \Sigma, \alpha, X_0, X_m)$ and $R = (Q, \Sigma, \delta, Q_0, Q_m)$, respectively. The set Σ of events is partitioned into the controllable event set Σ_c and the uncontrollable event set Σ_{uc}, where $\Sigma = \Sigma_c \cup \Sigma_{uc}$ and $\Sigma_c \cap \Sigma_{uc} = \emptyset$ [1]. Also, we assume that a supervisor can observe each event occurrence and the current state of the plant.

Formally, a supervisor $\mathscr{S}$ is defined as a pair

$$\mathscr{S} = (S, f)$$

of a nondeterministic automaton $S = (Y, \Sigma, \beta, Y_0, Y_m)$ and a feedback map $f : Y \to \Gamma$, where $\Gamma = \{\gamma \in 2^\Sigma \mid \Sigma_{uc} \subseteq \gamma\}$. Here, Γ is the set of control patterns, and $\Sigma_{uc} \subseteq \gamma$ implies that all uncontrollable events are enabled under a control pattern γ. That is, $f(y)$ is the set of events enabled by the supervisor $\mathscr{S}$ at the state $y \in Y$ of S.

For a supervisor $\mathscr{S} = (S, f)$, we define a set $\mathcal{R}_{Y \times X}$ of relations $\Psi \subseteq Y \times X$ such that any initial state $y_0 \in Y_0$ of the supervisor (respectively, $x_0 \in X_0$ of the plant) is related to an initial state $x_0 \in X_0$ of the plant (respectively, $y_0 \in Y_0$ of the supervisor) by Ψ (respectively, Ψ^{-1}) as follows:

$$\mathcal{R}_{Y \times X} = \{\Psi \subseteq Y \times X \mid [\forall y_0 \in Y_0, \exists x_0 \in X_0 :$$

$$(y_0, x_0) \in \Psi] \wedge [\forall x_0 \in X_0, \exists y_0 \in Y_0 : (x_0, y_0) \in \Psi^{-1}]\}.$$

The plant $\mathscr{S}^{\Psi}/G$ supervised by a supervisor $\mathscr{S} = (S, f)$ with respect to a relation $\Psi \in \mathcal{R}_{Y\times X}$ is defined as a nondeterministic automaton

$$\mathscr{S}^{\Psi}/G = (Y \times X, \Sigma, \xi, Y_0 \times X_0 \cap \Psi, Y_m \times X_m),$$

where the state transition function $\xi : (Y \times X) \times \Sigma \to 2^{Y\times X}$ is defined as

$$\begin{aligned}&\forall (y, x), (y', x') \in Y \times X, \forall \sigma \in \Sigma :\\ &\quad (y', x') \in \xi((y, x), \sigma) \Leftrightarrow \sigma \in f(y) \wedge (y', x') \in \Psi\\ &\quad \wedge y' \in \beta(y, \sigma) \wedge x' \in \alpha(x, \sigma).\end{aligned}$$

Let us assume that the current state of $\mathscr{S}^{\Psi}/G$ is (y, x). By the occurrence of an event $\sigma \in f(y)$ enabled by the supervisor, $\mathscr{S}^{\Psi}/G$ makes a transition to a state (y', x') in Ψ nondeterministically, where y' and x' are reachable from y and x by σ, respectively. For $\mathscr{S}^{\Psi}/G$, the set $Z(\mathscr{S}^{\Psi}/G)$ of states reachable from initial states is defined as

$$\begin{aligned}Z(\mathscr{S}^{\Psi}/G) = \{&(y, x) \in Y \times X \mid \exists s \in L(\mathscr{S}^{\Psi}/G) :\\ &(y, x) \in \xi(Y_0 \times X_0 \cap \Psi, s)\}.\end{aligned}$$

By the definition of the state transition function ξ, we have

$$Z(\mathscr{S}^{\Psi}/G) \subseteq \Psi. \tag{1}$$

In the plant $\mathscr{S}^{\Psi}/G$ supervised by a supervisor $\mathscr{S} = (S, f)$, the control mechanism is explained as follows. Let $(y, x) \in Z(\mathscr{S}^{\Psi}/G)$ be the current state of $\mathscr{S}^{\Psi}/G$. We assume that an event $\sigma \in f(y)$ enabled by the supervisor $\mathscr{S}$ occurs in G and the transition from x to $x' \in \alpha(x, \sigma)$ is caused. The supervisor $\mathscr{S}$ observes not only the occurrence of σ but also the destination state x'. Then, the transition from y to $y' \in \beta(y, \sigma)$ such that $(y', x') \in \Psi$ is nondeterministically made in S. That is, the next state of S is chosen such that the relation Ψ is satisfied. Note that the set $\beta(y, \sigma)$ of nondeterministic transitions is restricted to

$$\beta_{\Psi}(y, \sigma, x') := \{y' \in \beta(y, \sigma) \mid (y', x') \in \Psi\}$$

based on x' and Ψ in $\mathscr{S}^{\Psi}/G$. Then, events in $f(y')$ are enabled by $\mathscr{S}$ at the state $y' \in Y$. We introduce a notion of completeness of a supervisor in our control framework in order to guarantee that there exists $y' \in \beta(y, \sigma)$ such that $(y', x') \in \Psi$ and $(y', x') \in \xi((y, x), \sigma)$.

Definition 3: A supervisor $\mathscr{S} = (S, f)$ is said to be complete with respect to a relation $\Psi \in \mathcal{R}_{Y\times X}$ if

$$\begin{aligned}&\forall (y, x) \in Z(\mathscr{S}^{\Psi}/G), \forall \sigma \in \Sigma :\\ &\quad \sigma \in f(y) \Rightarrow \forall x' \in \alpha(x, \sigma), \exists y' \in \beta(y, \sigma) :\\ &\qquad (y', x') \in \xi((y, x), \sigma).\end{aligned}$$

Remark 1: The notion of completeness of a supervisor introduced in Definition 3 can be regarded as an extension of completeness in the deterministic setting of [1] to our nondeterministic setting.

Remark 2: In order to implement a supervisor $\mathscr{S}$, a mechanism for choosing the next state of the nondeterministic automaton S is needed. One possible way is to choose the next state based on transition probabilities. We introduce a function $p : Y \times \Sigma \times Y \to [0, 1]$ which satisfies the following two conditions for any $y \in Y$ and any $\sigma \in \Sigma$:

- $\forall y' \in Y : y' \in \beta(y, \sigma) \Leftrightarrow p(y, \sigma, y') \neq 0$.
- $\beta(y, \sigma) \neq \emptyset \Rightarrow \sum_{y' \in \beta(y,\sigma)} p(y, \sigma, y') = 1$.

Let $(y, x) \in Z(\mathscr{S}^{\Psi}/G)$ be the current state of $\mathscr{S}^{\Psi}/G$. We assume that an enabled event $\sigma \in f(y)$ occurs in G and the transition from x to $x' \in \alpha(x, \sigma)$ is caused. Then, the supervisor has to choose the next state of S from $\beta_{\Psi}(y, \sigma, x')$. The probability of the transition from y to each $y' \in \beta_{\Psi}(y, \sigma, x')$ is computed as

$$p_{\Psi}(y, \sigma, x', y') = \frac{p(y, \sigma, y')}{\sum_{y'' \in \beta_{\Psi}(y,\sigma,x')} p(y, \sigma, y'')},$$

and y' is chosen as the next state based on the probability $p_{\Psi}(y, \sigma, x', y')$. If the probability of each transition caused by an event σ is equally assigned, that is, $p(y, \sigma, y') = p(y, \sigma, y'')$ for any $y', y'' \in \beta_{\Psi}(y, \sigma, x') \neq \emptyset$, $p_{\Psi}(y, \sigma, x', y')$ is simply given as

$$p_{\Psi}(y, \sigma, x', y') = \frac{1}{|\beta_{\Psi}(y, \sigma, x')|}.$$

In this paper, we consider a problem of synthesizing a complete supervisor $\mathscr{S} = (S, f)$ such that $\mathscr{S}^{\Psi}/G$ is bisimilar to a given specification R with respect to some relation $\Psi \in \mathcal{R}_{Y\times X}$.

In [9], a nondeterministic automaton of the supervised plant was defined with respect to a relation $\Psi \subseteq Q \times X$ in a similar way. Theorem 1 of [9] shows that, when all events are observable, a necessary and sufficient condition for the existence of a bisimilarity enforcing supervisor is simulation-based controllability of R, that is, $R \sqsubseteq G$ and

$$\begin{aligned}&\forall s \in \Sigma^*, \forall q \in \delta(q_0, s), \forall \sigma \in \Sigma_{uc} :\\ &\quad s\sigma \in L(G) \Rightarrow \delta(q, \sigma) \neq \emptyset.\end{aligned}$$

However, in the supervised plant of [9], it is implicitly assumed that each nondeterministic transition labeled by the same event is controlled independently. Hence, as shown in the following example, it is possible that certain nondeterministic transitions become deterministic and that certain transitions by uncontrollable events are disabled to achieve bisimilarity between the supervised plant and the simulation-based controllable specification.

Example 1: We consider the automaton G of the plant and the automaton R of the specification shown in Fig. 1 and Fig. 2, respectively, where the initial state is identified by $\rightarrow$ to a circle and a marked state is identified by a double circle. We assume that $\Sigma_{uc} = \{a\}$ and $\Sigma_c = \{b, c\}$. We can verify that R is simulation-based controllable.

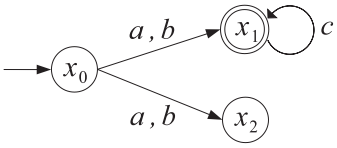

Fig. 1 Plant G.

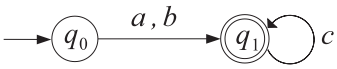

Fig. 2 Specification R of G.

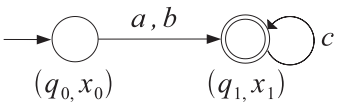

Fig. 3 Supervised plant.

We consider the unique simulation relation

$$\Psi = \{(q_0, x_0), (q_1, x_1)\} \subseteq Q \times X$$

from R to G. By Theorem 1 of [9], there exists a supervisor such that the supervised plant is bisimilar to the specification, and the automaton of the supervised plant with respect to Ψ is shown in Fig. 3. Thus, the supervisor initially enables both the uncontrollable event a and the controllable event b. Here, the state transitions from x_0 to x_2 by both a and b are disabled since $(q_1, x_2) \notin \Psi$. Thus, nondeterministic transitions labeled by a or b become deterministic by supervisory control in this example. Further, disabling transitions by uncontrollable events is unsuitable for the framework of supervisory control.

By contrast, in this paper, we require that a supervisor is complete in the sense of Definition 3. Therefore, transitions by events enabled by a supervisor, including uncontrollable events, are never disabled. Note that a relation Ψ is used to determine the next state of a complete supervisor in this paper, while, in [9], Ψ is also used to restrict the behavior of the plant as in Example 1. This is the difference between the relation-based control mechanism of this paper and that of [9].

4. Existence Condition of Supervisor

In this section, we present a necessary and sufficient condition for the existence of a complete supervisor such that the supervised plant is bisimilar to a given specification.

First, we introduce a partial simulation relation and a partial bisimulation relation for nondeterministic automata G and R which represent the plant and the specification, respectively.

Definition 4: Let $G = (X, \Sigma, \alpha, X_0, X_m)$ and $R = (Q, \Sigma, \delta, Q_0, Q_m)$ be two nondeterministic automata. If the following two conditions are satisfied by a relation $\Phi \subseteq X \times Q$, Φ is said to be a partial simulation relation from G to R.

- $\forall x_0 \in X_0, \exists q_0 \in Q_0 : (x_0, q_0) \in \Phi$.
- $\forall (x, q) \in \Phi, \forall \sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$, $\forall x' \in \alpha(x, \sigma), \exists q' \in \delta(q, \sigma) : (x', q') \in \Phi$.

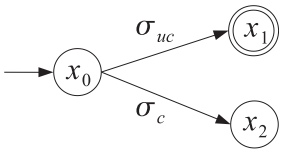

Fig. 4 Automaton G.

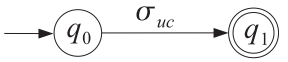

Fig. 5 Automaton R.

The notation $G \sqsubseteq^p_\Phi R$ means that Φ is a partial simulation relation from G to R.

Remark 3: Let $\Phi \subseteq X \times Q$ be a relation. We consider any $(x, q) \in \Phi$. The second condition of Definition 1 of the simulation relation requires that, for any $\sigma \in \Sigma$,

$$\forall x' \in \alpha(x, \sigma), \exists q' \in \delta(q, \sigma) : (x', q') \in \Phi. \tag{2}$$

By contrast, the second condition of Definition 4 of the partial simulation relation requires that (2) holds for any $\sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$. In addition, the third condition of Definition 1 on marked states is not required in Definition 4. Therefore, the notion of partial simulation is weaker than that of simulation. Note that $\Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$ is the set of events which should be enabled by a bisimilarity enforcing supervisor. The second condition of the partial simulation relation requires that all transitions caused by such events in G are simulated in R.

The following example shows the difference between the partial simulation relation and the simulation relation.

Example 2: We consider the automaton G of the plant and the automaton R of the specification shown in Fig. 4 and Fig. 5, respectively, where $\Sigma = \{\sigma_{uc}, \sigma_c\}$, $\Sigma_{uc} = \{\sigma_{uc}\}$, and $\Sigma_c = \{\sigma_c\}$.

We consider a relation $\Phi = \{(x_0, q_0), (x_1, q_1)\}$. In the automaton G, there exists a transition caused by the event σ_c from the state x_0 to the state x_2. However, in the automaton R, there exists no transition caused by the event σ_c from the state q_0. So, the relation Φ does not satisfy the second condition of Definition 1. Thus, Φ is not a simulation relation from G to R.

Recall that, by contrast, the partial simulation relation of Definition 4 requires that (2) holds for $\sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$. In this example, since $\sigma_c \in \Sigma_c$ and $\delta(q_0, \sigma_c) = \emptyset$, the existence of $q \in \delta(q_0, \sigma_c)$ such that $(x_2, q) \in \Phi$ is not required for $x_2 \in \alpha(x_0, \sigma_c)$. Thus, the relation Φ satisfies the two conditions of Definition 4, that is, $G \sqsubseteq^p_\Phi R$.

We next define a partial bisimulation relation.

Definition 5: Let $G = (X, \Sigma, \alpha, X_0, X_m)$ and $R = (Q, \Sigma, \delta, Q_0, Q_m)$ be two nondeterministic automata. If the following two conditions are satisfied by a relation $\Phi \subseteq Q \times X$, Φ is said to be a partial bisimulation relation between R and G.

- $R \sqsubseteq_\Phi G$.
- $G \sqsubseteq^p_{\Phi^{-1}} R$.

If there exists a partial bisimulation relation between R and G, R is said to be partially bisimilar to G.

Remark 4: A notion of partial bisimulation was defined for deterministic plants and specifications modeled by Moore automata in [20]. This notion requires that all transitions in the specification are simulated in the plant, and all uncontrollable transitions in the plant are simulated in the specification. When both G and R are deterministic, the second condition of Definition 4 can be weakened as

$$\forall (x, q) \in \Phi, \forall \sigma \in \Sigma_{uc}, \forall x' \in \alpha(x, \sigma), \\ \exists q' \in \delta(q, \sigma) : (x', q') \in \Phi.$$

In this sense, partial bisimulation introduced in this paper (for nondeterministic plants and specifications) coincides with that defined in [20] in the deterministic setting.

By using the notion of partial bisimulation defined in Definition 5, we present a necessary and sufficient condition for the existence of a complete supervisor that enforces bisimilarity between the supervised plant and the specification.

Theorem 1: Let $G = (X, \Sigma, \alpha, X_0, X_m)$ and $R = (Q, \Sigma, \delta, Q_0, Q_m)$ be two nondeterministic automata. Then, there exists a complete supervisor $\mathscr{S} = (S, f)$ such that $\mathscr{S}^\Psi/G \simeq R$ with respect to some relation $\Psi \in \mathcal{R}_{Y \times X}$ if and only if R is partially bisimilar to G.

(Proof) We first prove the sufficiency part. We assume that R is partially bisimilar to G. Then, there exists a partial bisimulation relation $\Phi \subseteq Q \times X$ between R and G. Let

$$S = R = (Q, \Sigma, \delta, Q_0, Q_m), \\ \Phi' = \{((q, x), q) \in (Q \times X) \times Q \mid (q, x) \in \Phi\}.$$

In addition, we consider $f : Q \to \Gamma$ such that

$$f(q) = \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\} \tag{3}$$

for each $q \in Q$.

Since $R \sqsubseteq_\Phi G$, for any $q_0 \in Q_0$, there exists $x_0 \in X_0$ such that $(q_0, x_0) \in \Phi$. In addition, since $G \sqsubseteq^p_{\Phi^{-1}} R$, for any $x_0 \in X_0$, there exists $q_0 \in Q_0$ such that $(x_0, q_0) \in \Phi^{-1}$. Thus, we have $\Phi \in \mathcal{R}_{Q \times X}$. Since $\mathscr{S} = (R, f)$, we can define $\mathscr{S}^\Phi/G$ with respect to Φ.

We prove that $\mathscr{S}^\Phi/G \simeq_{\Phi'} R$ in order to show $\mathscr{S}^\Phi/G \simeq R$.

First, we prove that $\mathscr{S}^\Phi/G \sqsubseteq_{\Phi'} R$.

- For any $(q_0, x_0) \in Q_0 \times X_0 \cap \Phi$, we have $q_0 \in Q_0$ and $((q_0, x_0), q_0) \in \Phi'$.
- For any $((q, x), q) \in \Phi'$, we consider any $\sigma \in \Sigma$ and any $(q', x') \in \xi((q, x), \sigma)$. By the definition of ξ, we have $q' \in \delta(q, \sigma)$ and $(q', x') \in \Phi$. Then, we have $((q', x'), q') \in \Phi'$.
- For any $((q, x), q) \in \Phi'$, we have $q \in Q_m$ when $(q, x) \in Q_m \times X_m$.

Thus, it follows that $\mathscr{S}^\Phi/G \sqsubseteq_{\Phi'} R$.

Next, we prove that $R \sqsubseteq_{\Phi'^{-1}} \mathscr{S}^\Phi/G$.

- By $R \sqsubseteq_\Phi G$, for any $q_0 \in Q_0$, there exists $x_0 \in X_0$ such that $(q_0, x_0) \in \Phi$. Thus, we have $(q_0, x_0) \in Q_0 \times X_0 \cap \Phi$ and $(q_0, (q_0, x_0)) \in \Phi'^{-1}$.
- For any $(q, (q, x)) \in \Phi'^{-1}$ and $\sigma \in \Sigma$, we consider any $q' \in \delta(q, \sigma)$. Since $(q, (q, x)) \in \Phi'^{-1}$, we have $(q, x) \in \Phi$. By $R \sqsubseteq_\Phi G$, there exists $x' \in \alpha(x, \sigma)$ such that $(q', x') \in \Phi$. Furthermore, since $q' \in \delta(q, \sigma) \neq \emptyset$, we have $\sigma \in f(q)$. By the definition of ξ, we have $(q', x') \in \xi((q, x), \sigma)$. Since $(q', x') \in \Phi$, we obtain $(q', (q', x')) \in \Phi'^{-1}$.
- We consider any $(q, (q, x)) \in \Phi'^{-1}$. Since $R \sqsubseteq_\Phi G$ and $(q, x) \in \Phi$, if $q \in Q_m$ then $x \in X_m$. Thus, we have $(q, x) \in Q_m \times X_m$ if $q \in Q_m$.

Thus, it follows that $R \sqsubseteq_{\Phi'^{-1}} \mathscr{S}^\Phi/G$. By Definition 2, we obtain $\mathscr{S}^\Phi/G \simeq_{\Phi'} R$.

It remains to prove that $\mathscr{S}$ is complete with respect to Φ.

For any $(q, x) \in Z(\mathscr{S}^\Phi/G)$ and any $\sigma \in \Sigma$, we assume that $\sigma \in f(q)$. By (1), we have $(q, x) \in \Phi$, that is, $(x, q) \in \Phi^{-1}$. We consider any $x' \in \alpha(x, \sigma)$. By (3), we have $\sigma \in f(q) = \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$. Since $G \sqsubseteq^p_{\Phi^{-1}} R$, for $(x, q) \in \Phi^{-1}$ and $x' \in \alpha(x, \sigma)$, there exists $q' \in \delta(q, \sigma)$ such that $(x', q') \in \Phi^{-1}$, that is, $(q', x') \in \Phi$. So, by the definition of ξ, we have $(q', x') \in \xi((q, x), \sigma)$. Thus, $\mathscr{S}$ is complete with respect to Φ.

Next, we prove the necessity part. We assume that there exists a complete supervisor $\mathscr{S} = (S, f)$ such that $\mathscr{S}^\Psi/G \simeq R$ with respect to some relation $\Psi \in \mathcal{R}_{Y \times X}$. Then, there exists a bisimulation relation Φ' between $\mathscr{S}^\Psi/G$ and R. We define a relation $\Phi \subseteq Q \times X$ as

$$\Phi = \{(q, x) \in Q \times X \mid \exists y \in Y : ((y, x), q) \in \Phi' \\ \wedge (y, x) \in Z(\mathscr{S}^\Psi/G)\},$$

and show that this relation Φ is a partial bisimulation relation between R and G.

First, we show that $R \sqsubseteq_\Phi G$.

- We consider any $q_0 \in Q_0$. By $\mathscr{S}^\Psi/G \simeq_{\Phi'} R$, there exists $(y_0, x_0) \in Y_0 \times X_0 \cap \Psi$ such that $((y_0, x_0), q_0) \in \Phi'$. In addition, we have $(y_0, x_0) \in Z(\mathscr{S}^\Psi/G)$. Thus, by the definition of Φ, we have $(q_0, x_0) \in \Phi$.
- We consider any $(q, x) \in \Phi$, any $\sigma \in \Sigma$, and any $q' \in \delta(q, \sigma)$. Since $(q, x) \in \Phi$, there exists $y \in Y$ such that $((y, x), q) \in \Phi'$ and $(y, x) \in Z(\mathscr{S}^\Psi/G)$. By $\mathscr{S}^\Psi/G \simeq_{\Phi'} R$, there exists $(y', x') \in \xi((y, x), \sigma) \subseteq Z(\mathscr{S}^\Psi/G)$ such that $((y', x'), q') \in \Phi'$. By the definition of ξ, we have

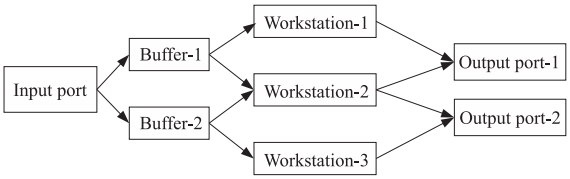

Fig. 6 Manufacturing system.

$x' \in \alpha(x, \sigma)$. Furthermore, by the definition of Φ, we have $(q', x') \in \Phi$.

- We consider any $(q, x) \in \Phi$. There exists $y \in Y$ such that $(q, (y, x)) \in \Phi'^{-1}$. By $\mathscr{S}^{\Psi}/G \simeq_{\Phi'} R$, if $q \in Q_m$, then $(y, x) \in Y_m \times X_m$, which implies that $x \in X_m$.

Thus, it follows that $R \sqsubseteq_{\Phi} G$.

Next, we show that $G \sqsubseteq^{p}_{\Phi^{-1}} R$.

- We consider any $x_0 \in X_0$. Since $\Psi \in \mathcal{R}_{Y \times X}$, there exists $y_0 \in Y_0$ such that $(y_0, x_0) \in \Psi$. It follows that $(y_0, x_0) \in Y_0 \times X_0 \cap \Psi \subseteq Z(\mathscr{S}^{\Psi}/G)$. Furthermore, since $\mathscr{S}^{\Psi}/G \simeq_{\Phi'} R$, there exists $q_0 \in Q_0$ such that $((y_0, x_0), q_0) \in \Phi'$. Thus, by the definition of Φ, we have $(x_0, q_0) \in \Phi^{-1}$.
- We consider any $(x, q) \in \Phi^{-1}$ and any $\sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$. By $(q, x) \in \Phi$, there exists $y \in Y$ such that $((y, x), q) \in \Phi'$ and $(y, x) \in Z(\mathscr{S}^{\Psi}/G)$.
  There are two cases that $\sigma \in \Sigma_{uc}$ and $\sigma \in \Sigma_c$. We consider the case that $\sigma \in \Sigma_{uc}$. By the definition of f, we have $\sigma \in f(y)$. We also consider the case that $\sigma \in \Sigma_c$. Then, we have $\delta(q, \sigma) \neq \emptyset$. We consider any $q'' \in \delta(q, \sigma)$. By $\mathscr{S}^{\Psi}/G \simeq_{\Phi'} R$, there exists $(y'', x'') \in \xi((y, x), \sigma)$ such that $((y'', x''), q'') \in \Phi'$. By the definition of ξ, we have $\sigma \in f(y)$.
  Since the supervisor $\mathscr{S}$ is complete with respect to Ψ, for any $x' \in \alpha(x, \sigma)$, there exists $y' \in \beta(y, \sigma)$ such that $(y', x') \in \xi((y, x), \sigma)$, which implies together with $(y, x) \in Z(\mathscr{S}^{\Psi}/G)$ that $(y', x') \in Z(\mathscr{S}^{\Psi}/G)$. In addition, by $\mathscr{S}^{\Psi}/G \simeq_{\Phi'} R$, there exists $q' \in \delta(q, \sigma)$ such that $((y', x'), q') \in \Phi'$. Thus, by the definition of Φ, we have $(x', q') \in \Phi^{-1}$.

Thus, it follows that $G \sqsubseteq^{p}_{\Phi^{-1}} R$.

By Definition 5, the relation Φ is a partial bisimulation relation between R and G, which implies that R is partially bisimilar to G. □

By the proof of the sufficiency part, if the specification automaton R is partially bisimilar to the plant automaton G, then a bisimilarity enforcing supervisor is synthesized as a pair of R and $f : Q \to \Gamma$ given by (3).

Example 3: We consider a manufacturing system shown in Fig. 6. This system consists of one input port, two buffers, three workstations, and two output ports. Initially, a workpiece is taken from the input port and nondeterministically transferred to the buffer-1 or buffer-2. A workpiece in the buffer-1 (respectively, buffer-2) is processed on the workstation-1 or workstation-2 (respectively, workstation-2 or workstation-3). After processing, a workpiece processed on the workstation-1 (respectively, workstation-3) is transferred to the output port-1 (respectively, output port-2). In addition, a workpiece processed on the workstation-2 is transferred to the output port-1 or output port-2. The control specification requires that a workpiece transferred to the buffer-1 (respectively, buffer-2) is transferred to the output port-1 (respectively, output port-2) after processing.

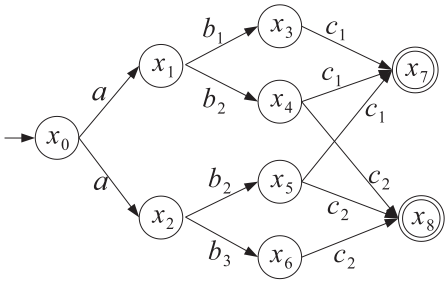

Fig. 7 Plant G.

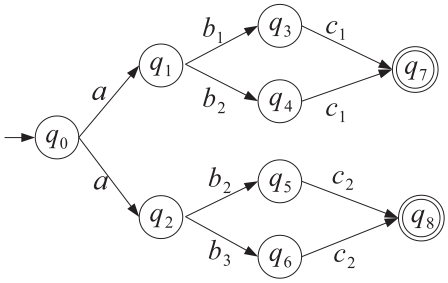

Fig. 8 Specification R of G.

For this manufacturing system, the automaton G of the plant and the automaton R of the specification are shown in Fig. 7 and Fig. 8, respectively. The event set is $\Sigma = \{a, b_1, b_2, b_3, c_1, c_2\}$, and the event labels represent the following actions.

- a: a workpiece is nondeterministically transferred to the buffer-1 or buffer-2.
- b_i: a workpiece is processed on the workstation-i ($i = 1, 2, 3$).
- c_j: a workpiece is transferred to the output port-j ($j = 1, 2$).

We can verify that $L(G) = L(R)$ and $L_m(G) = L_m(R)$, that is, G is language equivalent to R. However, it is possible that a workpiece transferred to the buffer-1 (respectively, buffer-2) is transferred to the output port-2 (respectively, output port-1) in G, which violates the specification. By contrast, G is not bisimilar to R, and bisimilarity enforcing control is required to achieve the specification.

Let $\Sigma_{uc} = \{a\}$ and $\Sigma_c = \{b_1, b_2, b_3, c_1, c_2\}$. We consider a relation

$$\Phi = \{(q_0, x_0), (q_1, x_1), (q_2, x_2), (q_3, x_3), (q_4, x_4), (q_5, x_5), (q_6, x_6), (q_7, x_7), (q_8, x_8)\}.$$

We can verify that Φ is a partial bisimulation relation between R and G.

Let $S = R$. The feedback map $f : Q \to \Gamma$ defined by

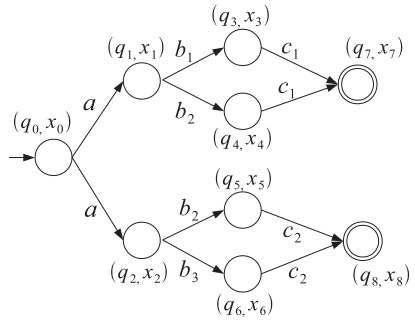

Fig. 9 Supervised plant $\mathscr{S}^{\Phi}/G$.

(3) is given as

$$f(q) = \begin{cases} \Sigma_{uc}, & \text{if } q \in \{q_0, q_7, q_8\}, \\ \Sigma_{uc} \cup \{b_1, b_2\}, & \text{if } q = q_1, \\ \Sigma_{uc} \cup \{b_2, b_3\}, & \text{if } q = q_2, \\ \Sigma_{uc} \cup \{c_1\}, & \text{if } q \in \{q_3, q_4\}, \\ \Sigma_{uc} \cup \{c_2\}, & \text{if } q \in \{q_5, q_6\}. \end{cases}$$

The automaton $\mathscr{S}^{\Phi}/G$ of the supervised plant is shown in Fig. 9. Then, $\mathscr{S}$ is complete with respect to Φ. Furthermore, $\mathscr{S}^{\Phi}/G \simeq_{\Phi'} R$ is satisfied, where

$$\begin{aligned} \Phi' = \{&((q_0, x_0), q_0), ((q_1, x_1), q_1)), ((q_2, x_2), q_2), \\ &((q_3, x_3), q_3), ((q_4, x_4), q_4), ((q_5, x_5), q_5), \\ &((q_6, x_6), q_6), ((q_7, x_7), q_7), ((q_8, x_8), q_8)\}. \end{aligned}$$

Thus, there exists a complete supervisor $\mathscr{S} = (S, f)$ such that $\mathscr{S}^{\Phi}/G \simeq R$ with respect to the relation $\Phi \in \mathcal{R}_{Q\times X}$.

5. Verification of Supervisor Existence

In this section, we consider how to search for a partial bisimulation relation between the specification automaton R and the plant automaton G in order to verify the condition of Theorem 1 for the existence of a complete supervisor efficiently.

We assume that the state sets Q and X of R and G, respectively, are finite. We define a function $F : 2^{Q\times X} \to 2^{Q\times X}$ as follows. Let $W \subseteq Q \times X$ be any relation. For any $(q, x) \in Q \times X$, $(q, x) \in F(W)$ if and only if the following four conditions are satisfied.

- $(q, x) \in W$.
- $\forall \sigma \in \Sigma, \forall q' \in \delta(q, \sigma), \exists x' \in \alpha(x, \sigma) : (q', x') \in W$.
- $q \in Q_m \Rightarrow x \in X_m$.
- $\forall \sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}, \forall x' \in \alpha(x, \sigma), \exists q' \in \delta(q, \sigma) : (x', q') \in W^{-1}$.

By the definition of F, F is monotone, that is,

$$\forall W, W' \subseteq Q \times X : W \subseteq W' \Rightarrow F(W) \subseteq F(W').$$

Since $Q \times X$ is finite,

$$W^* = \bigcap_{i\geq 0} F^i(Q \times X) \tag{4}$$

is obtained after at most $|Q| \times |X|$ iterations, and W^* is the unique maximal fixed-point of F. In each iteration, for $(q, x) \in F^i(Q \times X)$, we need to consider transitions from q and x, respectively, for each $\sigma \in \Sigma$. Since $|F^i(Q \times X)|$, $|\delta(q, \sigma)|$, and $|\alpha(x, \sigma)|$ are at most $|Q| \times |X|$, $|Q|$, and $|X|$, respectively, the complexity for performing each transition is $O(|Q|^2 \times |X|^2 \times |\Sigma|)$. Therefore, the complexity for computing W^* is $O(|Q|^3 \times |X|^3 \times |\Sigma|)$.

The following lemma characterizes partial bisimulation relations using the function F.

Lemma 1: Let $G = (X, \Sigma, \alpha, X_0, X_m)$ and $R = (Q, \Sigma, \delta, Q_0, Q_m)$ be two nondeterministic automata. Consider the function $F : 2^{Q\times X} \to 2^{Q\times X}$ defined above. For any $W \subseteq Q \times X$, W is a partial bisimulation relation between R and G if and only if $W = F(W)$ and $W \in \mathcal{R}_{Q\times X}$.

(Proof) We first prove the sufficiency part. We consider any relation $W \subseteq Q \times X$ such that $W = F(W)$ and $W \in \mathcal{R}_{Q\times X}$. Then, we show that this relation W is a partial bisimulation relation between R and G.

First, we show that $R \sqsubseteq_W G$.

- We consider any $q_0 \in Q_0$. By $W \in \mathcal{R}_{Q\times X}$, there exists $x_0 \in X_0$ such that $(q_0, x_0) \in W$.
- We consider any $(q, x) \in W$, any $\sigma \in \Sigma$, and any $q' \in \delta(q, \sigma)$. Since $(q, x) \in F(W)$, there exists $x' \in \alpha(x, \sigma)$ such that $(q', x') \in W$.
- We consider any $(q, x) \in W$. Since $(q, x) \in F(W)$, if $q \in Q_m$, then $x \in X_m$.

Thus, it follows that $R \sqsubseteq_W G$.

Next, we show that $G \sqsubseteq^p_{W^{-1}} R$.

- We consider any $x_0 \in X_0$. By $W \in \mathcal{R}_{Q\times X}$, there exists $q_0 \in Q_0$ such that $(x_0, q_0) \in W^{-1}$.
- We consider any $(x, q) \in W^{-1}$, any $\sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$, and any $x' \in \alpha(x, \sigma)$. Since $(q, x) \in F(W)$, there exists $q' \in \delta(q, \sigma)$ such that $(x', q') \in W^{-1}$.

Thus, it follows that $G \sqsubseteq^p_{W^{-1}} R$.

We next prove the necessity part. We assume that $W \subseteq Q \times X$ is a partial bisimulation relation between R and G.

First, we show that $W \in \mathcal{R}_{Q\times X}$. Since $R \sqsubseteq_W G$, for any $q_0 \in Q_0$, there exists $x_0 \in X_0$ such that $(q_0, x_0) \in W$. In addition, since $G \sqsubseteq^p_{W^{-1}} R$, for any $x_0 \in X_0$, there exists $q_0 \in Q_0$ such that $(x_0, q_0) \in W^{-1}$. Thus, we have $W \in \mathcal{R}_{Q\times X}$.

Next, we show that $W = F(W)$. By the definition of F, $F(W) \subseteq W$ trivially holds. We consider any $(q, x) \in W$. Since $R \sqsubseteq_W G$, for any $\sigma \in \Sigma$ and $q' \in \delta(q, \sigma)$, there exists $x' \in \alpha(x, \sigma)$ such that $(q', x') \in W$. In addition, if $q \in Q_m$ then $x \in X_m$. Since $G \sqsubseteq^p_{W^{-1}} R$, for any $\sigma \in \Sigma_{uc} \cup \{\sigma \in \Sigma_c \mid \delta(q, \sigma) \neq \emptyset\}$ and any $x' \in \alpha(x, \sigma)$, there exists $q' \in \delta(q, \sigma)$ such that $(x', q') \in W^{-1}$. Therefore, $(q, x) \in F(W)$, which shows that $W \subseteq F(W)$. □

By using Lemma 1, the following theorem is obtained.

Theorem 2: Let $G = (X, \Sigma, \alpha, X_0, X_m)$ and $R = (Q, \Sigma, \delta, Q_0, Q_m)$ be two nondeterministic automata. Then, R is partially bisimilar to G if and only if W^* defined by (4)

satisfies $W^* \in \mathcal{R}_{Q\times X}$.

(Proof) We first prove the sufficiency part. We assume that W^* defined by (4) satisfies $W^* \in \mathcal{R}_{Q\times X}$. Since W^* is the unique maximal fixed-point of F, we have $W^* = F(W^*)$. By Lemma 1, W^* is a partial bisimulation relation between R and G, which implies that R is partially bisimilar to G.

We next prove the necessity part. We assume that R is partially bisimilar to G. Then, there exists a partial bisimulation relation $W \subseteq Q \times X$ between R and G. By Lemma 1, we have $W = F(W)$ and $W \in \mathcal{R}_{Q\times X}$. Since W^* is the unique maximal fixed-point of F, we have $W \subseteq W^*$. Therefore, W^* satisfies $W^* \in \mathcal{R}_{Q\times X}$. □

Remark 5: In [2], bisimilarity enforcing supervisory control of nondeterministic systems was studied in a different setting, where a supervisor observes only event occurrences and the supervised plant is modeled by the synchronous composition of the plant and the supervisor. Theorem 2 of [2] presents a necessary and sufficient condition for the existence of a bisimilarity enforcing supervisor. The complexity of verifying this condition is $O(2^{2^{|Q|\times|X|}})$. By contrast, we impose the additional assumption that a supervisor can observe the current state of the plant. However, the complexity of verifying the condition of Theorem 2 is $O(|Q|^3\times|X|^3\times|\Sigma|)$ since the complexity of computing W^* is $O(|Q|^3\times|X|^3\times|\Sigma|)$. Thus, our framework has a computational advantage for verifying the existence condition of a supervisor.

Example 4: We consider the automaton G of the plant and the automaton R of the specification shown in Fig. 7 and Fig. 8, respectively. By using Theorem 2, we verify whether R is partially bisimilar to G. We perform the iteration of F over $Q \times X$. Since

$$\begin{aligned}
F^0(Q\times X) &= Q\times X,\\
F^1(Q\times X) &= \{(q_0,x_0),(q_1,x_1),(q_2,x_2),(q_3,x_3),\\
&\quad (q_3,x_4),(q_3,x_5),(q_4,x_3),(q_4,x_4),\\
&\quad (q_4,x_5),(q_5,x_4),(q_5,x_5),(q_5,x_6),\\
&\quad (q_6,x_4),(q_6,x_5),(q_6,x_6),(q_7,x_7),\\
&\quad (q_7,x_8),(q_8,x_7),(q_8,x_8)\},\\
F^2(Q\times X) &= \{(q_0,x_0),(q_1,x_1),(q_2,x_2),(q_3,x_3),\\
&\quad (q_3,x_4),(q_3,x_5),(q_4,x_3),(q_4,x_4),\\
&\quad (q_4,x_5),(q_5,x_4),(q_5,x_5),(q_5,x_6),\\
&\quad (q_6,x_4),(q_6,x_5),(q_6,x_6),(q_7,x_7),\\
&\quad (q_7,x_8),(q_8,x_7),(q_8,x_8)\},
\end{aligned}$$

we obtain the unique maximal fixed-point W^* of F after two iterations, that is,

$$\begin{aligned}
W^* &= F^1(Q\times X)\\
&= \{(q_0,x_0),(q_1,x_1),(q_2,x_2),(q_3,x_3),(q_3,x_4),\\
&\quad (q_3,x_5),(q_4,x_3),(q_4,x_4),(q_4,x_5),(q_5,x_4),\\
&\quad (q_5,x_5),(q_5,x_6),(q_6,x_4),(q_6,x_5),(q_6,x_6),\\
&\quad (q_7,x_7),(q_7,x_8),(q_8,x_7),(q_8,x_8)\}.
\end{aligned}$$

Since $W^* \in \mathcal{R}_{Q\times X}$, we can conclude that R is partially bisimilar to G.

6. Conclusion

In this paper, we have considered a supervisory control problem for nondeterministic DESs, which requires bisimulation equivalence between the supervised plant and a given nondeterministic specification. We have introduced a notion of partial bisimulation for nondeterministic plants and specifications, and proved that it serves as a necessary and sufficient condition for the existence of a complete supervisor such that the supervised plant is bisimilar to a given specification. Furthermore, when the state sets of the plant and the specification are finite, we have presented a method for verifying the existence of a complete supervisor whose complexity is polynomial in the sizes of the plant and the specification.

When the existence condition of a bisimilarity enforcing complete supervisor fails, we need to find a stronger specification that is partially bisimilar to the plant. It is desirable that such a specification is least restrictive. This issue is currently under investigation.

Acknowledgements

The authors would like to thank Prof. Toshimitsu Ushio for his helpful comments. This work was supported in part by Grant-in-Aid for Scientific Research (No. 24560547).

References

[1] P.J. Ramadge and W.M. Wonham, "Supervisory control of a class of discrete event processes," SIAM J. Control Optim., vol.25, no.1, pp.206–230, 1987.
[2] C. Zhou, R. Kumar, and S. Jiang, "Control of nondeterministic discrete-event systems for bisimulation equivalence," IEEE Trans. Autom. Control, vol.51, no.5, pp.754–765, 2006.
[3] R. Su, J.H. van Schuppen, and J.E. Rooda, "Model abstraction of nondeterministic finite-state automata in supervisor synthesis," IEEE Trans. Autom. Control, vol.55, no.11, pp.2527–2541, 2010.
[4] M.A. Shayman and R. Kumar, "Supervisory control of nondeterministic systems with driven events via prioritized synchronization and trajectory models," SIAM J. Control Optim., vol.33, no.2, pp.469–497, 1995.
[5] R. Kumar and M.A. Shayman, "Nonblocking supervisory control of nondeterministic systems via prioritized synchronization," IEEE Trans. Autom. Control, vol.41, no.8, pp.1160–1175, 1996.
[6] A. Overkamp, "Supervisory control using failure semantics and partial specifications," IEEE Trans. Autom. Control, vol.42, no.4, pp.498–510, 1997.
[7] M. Heymann and F. Lin, "Discrete-event control of nondeterministic systems," IEEE Trans. Autom. Control, vol.43, no.1, pp.3–17, 1998.
[8] S. Jiang and R. Kumar, "Supervisory control of nondeterministic discrete-event systems with driven events via masked prioritized synchronization," IEEE Trans. Autom. Control, vol.47, no.9, pp.1438–1449, 2002.
[9] F. Liu, H. Lin, and Z. Dziong, "Bisimilarity control of partially observed nondeterministic discrete event systems and a test algorithm," Automatica, vol.47, no.4, pp.782–788, 2011.
[10] C. Zhou and R. Kumar, "Bisimilarity enforcement for discrete event

systems using deterministic control," IEEE Trans. Autom. Control, vol.56, no.12, pp.2986–2991, 2011.
[11] R. Milner, A. Calculus of Communicating Systems, Springer-Verlag, 1980.
[12] C. Zhou and R. Kumar, "A small model theorem for bisimilarity control under partial observation," IEEE Trans. Autom. Sci. Eng., vol.4, no.1, pp.93–97, 2007.
[13] P.J. Ramadge and W.M. Wonham, "Modular feedback logic for discrete event systems," SIAM J. Control Optim., vol.25, no.5, pp.1202–1218, 1987.
[14] T. Ushio, "Feedback logic for discrete event systems with arbitrary control patterns," Int. J. Control, vol.52, no.1, pp.159–174, 1990.
[15] T. Ushio, Y. Li, and W.M. Wonham, "Concurrency and state feedback in discrete-event systems," IEEE Trans. Autom. Control, vol.37, no.8, pp.1180–1184, 1992.
[16] R. Kumar, V. Garg, and S.I. Marcus, "Predicates and predicate transformers for supervisory control of discrete event dynamical systems," IEEE Trans. Autom. Control, vol.38, no.2, pp.232–247, 1993.
[17] Y. Li and W.M. Wonham, "Control of vector discrete-event systems *I*-The base model," IEEE Trans. Autom. Control, vol.38, no.8, pp.1214–1227, 1993.
[18] Y. Li and W.M. Wonham, "Concurrent vector discrete-event systems," IEEE Trans. Autom. Control, vol.40, no.4, pp.628–638, 1995.
[19] C.G. Cassandras and S. Lafortune, Introduction to Discrete Event Systems, Second Ed., Springer, 2008.
[20] J.J.M.M. Rutten, "Coalgebra, concurrency, and control," Technical Report SEN-R9921, CWI, 1999.
[21] K. Kimura, M. Nomura, and S. Takai, "Bisimilarity enforcing supervisory control of nondeterministic systems under event and state observations," Preprints 11th Int. Workshop on Discrete Event Syst., pp.169–174, 2012.

Katsuyuki Kimura received the B.E. and M.E. degrees in 2012 and 2014, respectively, from Osaka University. His research interests include supervisory control.

Shigemasa Takai received the B.E. and M.E. degrees from Kobe University in 1989 and 1991, respectively, and the Ph.D. degree from Osaka University in 1995. From 1992 to 1998, he was a Research Associate at Osaka University. He joined Wakayama University as a Lecturer in 1998, and became an Associate Professor in 1999. From 2004 to 2009, he was an Associate Professor at Kyoto Institute of Technology. Since 2009, he has been a Professor at Osaka University. His research interests include supervisory control and fault diagnosis of discrete event systems. He is a member of SICE, ISCIE, and IEEE.