World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:12, No:1, 2018

Conditions for Fault Recovery of Interconnected Asynchronous Sequential Machines with State Feedback

Jung–Min Yang

Abstract**—In this paper, fault recovery for parallel interconnected asynchronous sequential machines is studied. An adversarial input can infiltrate into one of two submachines comprising parallel composition of the considered asynchronous sequential machine, causing an unauthorized state transition. The control objective is to elucidate the condition for the existence of a corrective controller that makes the closed-loop system immune against any occurrence of adversarial inputs. In particular, an efficient existence condition is presented that does not need the complete modeling of the interconnected asynchronous sequential machine.**

Keywords**—Asynchronous sequential machines, parallel composition, corrective control, fault tolerance.**

I. Introduction

AS a unique automatic control theory exclusively targeting asynchronous sequential machines, corrective control has been studied actively for the past decade [1]–[4]. The core of corrective control lies in the property that corrective controllers are also implemented as asynchronous sequential machines so that the interaction between controllers and controlled machines is executed very fast under asynchrony. Hence, even if the controlled machine does not possess desirable transitions, it can be controlled to show the desirable input/state or input/output behavior as long as stable reachability that can be used to make an appropriate feedback trajectory exists in the dynamics of the machine.

In the early studies, corrective control is mainly applied to solving the model matching problem of single asynchronous sequential machines with various deficiencies such as critical races [5], infinite cycles [6], nondeterminism in their transitions [7], etc. Recently, the subject of corrective control is extended to tackling the problem of model matching and fault tolerance for composite asynchronous sequential machines. In [8], a corrective controller is designed to match the closed-loop system of a composite asynchronous sequential machine with cascade connection to that of a reference model. In [9], fault diagnosis of asynchronous sequential machines with parallel composition is studied. On the other hand, [10] and [11] address the model matching problem of switched asynchronous sequential machines in the framework of corrective control.

In this paper, we address the problem of fault tolerant control for a composite asynchronous sequential machine. The considered machine consists of parallel composition of two single input/state asynchronous sequential machines in which two submachines receive the same control input and undergo their own state transitions. The overall composite asynchronous sequential machine can be regarded as having two-dimensional state space. The control objective is to elucidate the existence condition for a corrective control that diagnoses any occurrence of state transition faults and steers the controlled composite machine towards the original state immediately. We assume that the controller has access to full state feedback of two single asynchronous sequential machines. Main consideration will be given to addressing the existence condition for a controller. The design procedure for a controller is similar to that in the prior work (e.g., [7], [8]).

Note that a study of fault diagnosis on parallel interconnected asynchronous sequential machines is already addressed in the author's prior work [9]. The present report is an extension of [9] in which fault recoverability against unauthorized state transitions is analyzed in the framework of corrective control. Specifically, we focus our concern on presenting the existence condition of a controller while avoiding computational burden of identifying the entire dynamics of the composite machine. It is known that parallel composition of two independent finite-state machines causes the problem of state explosion [12]. But our scheme is efficient in that it does not require exact transition characteristics of the composite machine. The derivation of the existence condition (and design procedure) for a corrective controller needs only the information on state transitions of each constituent single machine.

II. Notation and Basics

The modeling formalism for composite asynchronous sequential machines is first addressed in the author's previous work [9]. A parallel interconnected asynchronous sequential machine $\Sigma = \Sigma_1 || \Sigma_2$ is composed of parallel composition of two input/state asynchronous sequential machines Σ_1 and Σ_2 that are represented as

$$\Sigma_1 = (A, X, x_0, f_1)$$
$$\Sigma_2 = (A, Y, y_0, f_2)$$

This research was supported in part by the Human Resource Training Program for Regional Innovation and Creativity through the Ministry of Education and National Research Foundation of Korea (No. 2015H1C1A1035914) and in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2015R1D1A1A01056764).

J.–M. Yang is with the School of Electronics Engineering, Kyungpook National University, 80 Daehak-ro, Buk-gu, Daegu 41566, Republic of Korea (e-mail: jmyang@ee.knu.ac.kr).

where X and Y are the state set of Σ_1 and Σ_2, respectively, $x_0 \in X$ and $y_0 \in Y$ are the initial states, and $f_1 : X \times A \to X$ and $f_2 : Y \times A \to Y$ are the state transition functions partially defined on $X \times A$ and $Y \times A$. Let $n := |X|$ and $m := |Y|$ be the cardinality of X and Y, respectively. The input set A is separated into the set of normal inputs A_n and that of adversarial inputs A_d. Thus we have $A = A_n \dot{\cup} A_d$.

In a single asynchronous sequential machine Σ_1, every valid state–input pair $(x, v') \in X \times A$ is either a stable or transient pair. If $f_1(x, v') = x$, (x, v') is a stable pair at which Σ_1 stays indefinitely unless the input does not change. When the input v' changes to another value $v \in A$ for which $f_1(x, v) \neq x$, (x, v) is a transient pair and Σ begins a chain of transient transitions, e.g.,

$$f_1(x, v) = x_1, \; f_1(x_1, v) = x_2, \dots$$

during which Σ passes through transient states $x_1, x_2, \dots$ instantaneously and v remains unchanged. This chain of transients may or may not end. If it does not end, it makes an infinite cycle. In this study we assume that neither Σ_1 nor Σ_2 has infinite cycles. Then Σ_1 will reach the *next stable state* x' where $x' = f(x, v)$. Often we omit underlying transient transitions $x_1, x_2, \dots$ due to their instantaneousness in the asynchronous mechanism and instead describe the transitions only in terms of the initial and next stable states—called a *stable transition*. To this end, we define the *stable recursion function* s as [5]

$$\begin{aligned} s_1 &: X \times A \to X \\ s_1(x, v) &:= x' \end{aligned}$$

where x' is the next stable state of a valid state–input combination (x, v). We can expand the domain of s_1 to $X \times A_n^+$ whenever necessary (A_n^+ is the set of all nonempty strings of characters in A_n), i.e.,

$$\begin{aligned} s_1(x, v_1 v_2 \cdots v_k) &:= s_1(s_1(x, v_1), v_2 \cdots v_k), \\ & v_1 v_2 \cdots v_k \in A_n^+. \end{aligned}$$

The definition of the stable recursion function is equally applied to Σ_2.

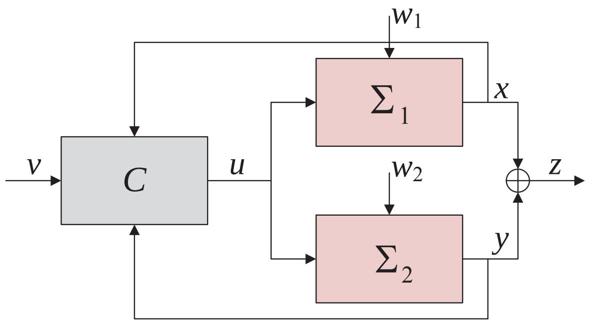

Fig. 1 Control configuration of a parallel interconnected asynchronous sequential machine $\Sigma = \Sigma_1 || \Sigma_2$

Fig. 1 shows the feedback control configuration of a parallel interconnected asynchronous sequential machine $\Sigma = \Sigma_1 || \Sigma_2$. C is the corrective controller, also having the form of an input/ouptut asynchronous sequential machine, $v \in A_n$ is the externa input, $u \in A_n$ is the control input provided by C, x and y are the state of Σ_1 and Σ_2, z is the output of Σ, and $w_1, w_2 \in A_d$ are the adversarial inputs infiltrating into Σ_1 and Σ_2, respectively. We denote by Σ_c the closed-loop system consisting of C and Σ. When w_1 or w_2 enters a single asynchronous sequential machine, it override the present control input $u \in A_n$, causing the corresponding asynchronous sequential machine to experience an unauthorized state transition. For instance, if Σ_2 has been staying at a stable state y when w_2 occurs for which $s_2(y, w_1) = y'$, Σ_2 undergoes the unauthorized transition from y to y'. The next operation of Σ would be incorrect unless Σ_2 is counteracted from this fault immediately.

In view of Fig. 1, we can describe Σ by an input/output asynchronous sequential machine of the form

$$\begin{aligned} \Sigma &= \Sigma_1 || \Sigma_2 \\ &= (A_n, Z, X \times Y, (x_0, y_0), f, h) \end{aligned}$$

where A_n and Z are the input and output set, respectively, $X \times Y$ are the state set with the initial state (x_0, y_0), $f : X \times Y \times A \to X \times Y$ is the state transition equation, and $h : X \times Y \to Z$ is the output function (assuming that Σ is a Moor machine).

To prevent unpredictable outcomes caused by the absence of a synchronizing clock, the closed-loop system Σ_c is supposed to preserve the principle of fundamental mode operations [13] whereby an input, state, or output variable must change its value when both C and Σ are in stable states, and no two or more variables can be changed at the same time. Under the principle of fundamental mode operations, we must assume that if the input $u \in A$ changes, one of Σ_1 and Σ_2 takes a stable transition in the first, and the second asynchronous sequential machine doest not start its stable transition until the end of the first transition. Which asynchronous sequential machine among Σ_1 and Σ_2 takes the first transition is nondeterministic in general. However, without regard to the relative order, the next stable states reached by Σ_1 and Σ_2 are always deterministic. In this respect, the stable recursion function of Σ $s : X \times Y \times A \to X \times Y$ is defined as

$$s(x, y, u) := \begin{cases} (s_1(x, u), s_2(y, u)) & s_1(x, u)! \text{ and } s_2(y, u)! \\ (s_1(x, u), y) & s_1(x, u)! \text{ and } s_2(y, u)\text{¡} \\ (x, s_2(y, u)) & s_1(x, u)\text{¡} \text{ and } s_2(y, u)! \\ \text{undefined} & \text{otherwise} \end{cases} \tag{1}$$

where '$s_1(x, u)!$' and '$s_1(x, u)$¡' indicate that $s_1(x, u)$ is defined and undefined, respectively. $h(x, y)$ is the output function whose value $h(x, y) = z \in Z$ is determined by the present state pair $(x, y) \in X \times Y$. Note that in the previous work [9], we assumed that the output of Σ is given as the form of *burst* [1], a quick succession of output characters. In the present study, on the other hand, we do not use the burst output. Even the use of output feedback itself is entirely excluded from the study; only state feedback will be transmitted to the controller as illustrated in Fig. 1.

Referring to Fig. 1, C can be represented as an input/output stable-state asynchronous sequential machine of the form

$$C = (A_n \times X \times Y, A_n, \Xi, \xi_0, \phi, \eta)$$

where $A_n \times X \times Y$ is the input set (v, x, and y), A_n is the output set serving as the control input u, Ξ is the state set, $\xi_0 \in \Xi$ is the initial state, $\phi : \Xi \times X \times Y \times A_n \to \Xi$ is the stable recursion function, and $\eta : \Xi \to Z$ is the output function. The objective is to design C such that the closed-loop system Σ_c maintains the normal input/state behavior against any occurrence of w_1 or w_2. Whenever an adversarial input occurs to Σ, C will diagnose it and provide a sequence of control inputs so that Σ is steered towards the original state at which the fault occurred.

III. Condition for Fault Recovery

Since both states x and y are available as feedback in the proposed architecture, fault diagnosis on occurrences of w_1 and w_2 is straightforward as already addressed in [9]. Take an occurrence of w_1 for example. Assume that Σ has been staying at a stable state $(\bar{x}, \bar{y}) \in X \times Y$ when w_1 occurs, enforcing Σ_1 to reach $s_1(\bar{x}, w_1) = x'$. C can diagnose the occurrence of w_1 by observing that the state feedback of Σ_1 changes to x' while the external input remains fixed. Since only one variable can change at a time under the principle of fundamental mode operations [13], w_2 never happens at the moment w_1 happens. Thus the next state Σ reaches by w_1 is $(x', \bar{y})$. An occurrence of w_2 is similarly analyzed. In short, when full state feedback is available to C, we can diagnose any fault event merely by observing a change of state feedback. A detailed result of fault diagnosis is found in [9].

In corrective control for a single asynchronous sequential machine $\Sigma_1 = (A, X, x_0, f_1)$, stable reachability between two states measured in $n-1$ ($n = |X|$) or less steps is sufficient to describe the entire reachability of the machine [5]. On the other hand, when two single asynchronous sequential machines Σ_1 and Σ_2 are combined into parallel composition, one must take into consideration more steps because although the current input makes a valid transition with Σ_1, it may not with Σ_2 and vice versa (refer to (1)). To consider more steps of stable reachability, we introduce a generalized stable recursion function $\hat{s}_1 : X \times A \to X$ and $\hat{s}_2 : Y \times A \to Y$ of Σ_1 and Σ_2, respectively, defined as a total function:

$$\hat{s}_1(x, u) := \begin{cases} s_1(x, u) & s_1(x, u)! \\ x & s_1(x, u)¡ \end{cases}$$

$$\hat{s}_2(y, u) := \begin{cases} s_2(y, u) & s_2(y, u)! \\ y & s_2(y, u)¡ \end{cases}$$

All the undefined state–input pairs are considered as stable combinations in $\hat{s}_1$ and $\hat{s}_2$. We assert that this setting is not restrictive because an asynchronous sequential machine would not respond to any incoming input that is not defined at the current state, thus maintaining the same state. In association with $\hat{s}_1$ and $\hat{s}_2$, s in (1) is written as

$$s(x, y, u) = (\hat{s}_1(x, u), \hat{s}_2(y, u)).$$

The domain of s is extended to $X \times A_n^+$ in the same way as s_1 and s_2. Further, we extend it to $P(X) \times A$, where $P(X)$ is the power set of X, as

$$s(X', u) := \{s(x, u) | x \in X'\} \text{ for } X' \subset X.$$

Similarly, we extend the domain and range of the output function to $h : P(X) \to P(Z)$ as $h(X') := \{h(x) | x \in X'\}$.

Definition 1: Let $X := \{x_1, \ldots, x_n\}$ for $\Sigma_1 = (A, X, x_0, f_1)$ with $|X| = n$, and let $Y := \{y_1, \ldots, y_m\}$ for $\Sigma_2 = (A, Y, y_0, f_2)$ with $|Y| = m$. $\hat{R}(\Sigma_1)$ and $\hat{R}(\Sigma_2)$, the extended matrix of stable transitions of Σ_1 and Σ_2, are $n \times n$ and $m \times m$ matrices whose (p, q) entries are defined as

$$\hat{R}_{p,q}(\Sigma_1) := \{t \in A_n^+ | \hat{s}_1(x_p, t) = x_q, |t| \leqslant n + m - 2\}$$
$$p, q \in \{1, \ldots, n\}$$
$$\hat{R}_{p,q}(\Sigma_2) := \{t \in A_n^+ | \hat{s}_2(y_p, t) = y_q, |t| \leqslant n + m - 2\}$$
$$p, q \in \{1, \ldots, m\}$$

$\hat{R}(\Sigma_1)$ and $\hat{R}(\Sigma_2)$ contain not only essential input sequences representing stable reachability of Σ_1 and Σ_2, but also redundant ones that can make valid transitions with other asynchronous sequential machines. $|t| \leqslant n + m - 2$ implies that $\hat{R}(\Sigma_1)$ and $\hat{R}(\Sigma_2)$ have all the sequences of external input characters that can induce valid transitions with respect to both Σ_1 (with the maximal length $n-1$) and Σ_2 (with the maximal length $m-1$).

We now present the existence condition for a corrective controller C that tolerates unauthorized state transitions caused by w_1 and w_2. The recovery procedure by C similar to the prior work [8]. Assume that Σ_1 and Σ_2 have been staying at stable states $\bar{x}$ and $\bar{y}$ when w_1 occurs to Σ_1, causing the unauthorized state transition $s_1(\bar{x}, w_1) := x'$. As addressed before, C is able to diagnose this fault occurrence by observing the change of the state feedback from $(\bar{x}, \bar{y})$ to $(x', \bar{y})$. The control goal is to design C so as to drive the closed-loop system Σ_c from $(x', \bar{y})$ to the original state $(\bar{x}, \bar{y})$ before further change of the external input.

In the former methodology of controlling single asynchronous sequential machines [1], [5], [7], the existence condition for a corrective controller is equivalent to the existence of a sequence of external inputs that steers Σ from $(x', \bar{y})$ to $(\bar{x}, \bar{y})$. The latter can be examined by deriving the complete state transition characteristics of Σ and by deriving matrix of stable transitions $R(\Sigma)$ according to [5]. But this method gives much computationally burden, as the dimension of $R(\Sigma)$ is $nm \times nm$.

Here we present an alternative method that does not need the complete modeling of the composite machine Σ. This is made possible by utilizing the extended matrix of stable transitions of Σ_1 and Σ_2 introduced in Definition 1. In controlling Σ from $(x', \bar{y})$ to $(\bar{x}, \bar{y})$, Σ_1 and Σ_2 must be steered such that Σ_1 be driven from x' to $\bar{x}$ and Σ_2 transfer from $\bar{y}$ to $\bar{y}$, i.e., Σ_2 must circulate around $\bar{y}$. Let $t \in A_n^+$ be a control input sequence that achieves the fault tolerant control procedure from $(x', \bar{y})$ to $(\bar{x}, \bar{y})$. For notational convenience, assume that $\bar{x} := x_p$, $x' := x_q$, and $\bar{y} := y_r$. In view of Definition 1, an appropriate condition for t is described as

$$t \in \hat{R}_{q,p}(\Sigma_1) \cap \hat{R}_{r,r}(\Sigma_2).$$

Note that the above condition can be verified by referring to the dynamics of submachines Σ_1 and Σ_2. The existence condition for a corrective controller for tolerating occurrences of w_2 at Σ_2 is similarly derived as follows. Assume that Σ

undergoes an unauthorized state transition from $(\bar{x}, \bar{y})$ to $(\bar{x}, y')$ where there exists $w_2 \in A_d$ such that $s_2(\bar{y}, w_2) = y'$. Assume further that $\bar{x} := x_p$, $\bar{y} := y_r$, and $y' := y_s$. Then, a fault tolerant corrective controller C tolerating this unauthorized transition can be designed if a control input sequence $t' \in A_n^+$ exists such that

$$t' \in \hat{R}_{p,p}(\Sigma_1) \cap \hat{R}_{s,r}(\Sigma_2).$$

Let us summarize this result in the following theorem.

Theorem 1: Assume that the parallel interconnected asynchronous sequential machine $\Sigma = \Sigma_1 || \Sigma_2$ has been staying at a stable state (x_p, y_r), when an unauthorized state transition occurs so that Σ transfers to (x_q, y_r) or (x_p, y_s). Then, a corrective controller C of Fig. 1 exists for which Σ_c returns to the original input/state behavior at which the fault occurred if and only if there exists $t \in A_n^+$ or $t' \in A_n^+$ such that

(a) $t \in \hat{R}_{q,p}(\Sigma_1) \cap \hat{R}_{r,r}(\Sigma_2)$; and
(b) $t' \in \hat{R}_{p,p}(\Sigma_1) \cap \hat{R}_{s,r}(\Sigma_2)$,

where $\hat{R}(\Sigma_1)$ and $\hat{R}(\Sigma_2)$ are the extended matrices of stable transitions of Σ_1 and Σ_2 defined in Definition 1.

IV. Example

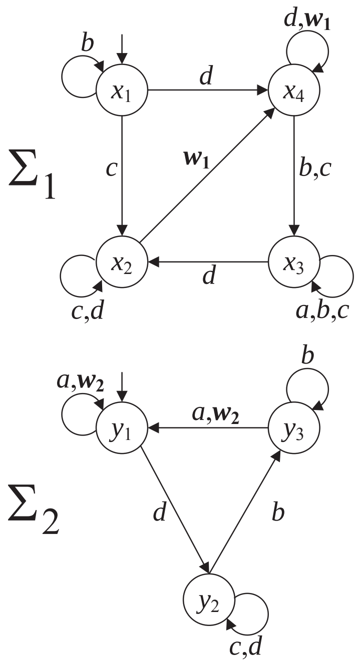

Fig. 2 $\Sigma = \Sigma_1 || \Sigma_2$

Consider a parallel interconnected asynchronous machine $\Sigma = \Sigma_1 || \Sigma_2$ shown in Fig. 2 where $X = \{x_1, x_2, x_3, x_4\}$ with $x_0 = x_1$, $Y = \{y_1, y_2, y_3\}$ with $y_0 = y_1$, $A_n = \{a, b, c, d\}$, and $A_d = \{w_1, w_2\}$. We set $f_i = s_i$, $\forall i = 1, 2$ for the sake of simplicity.

First, assume that Σ has been staying at the stable combination $((x_2, y_2), c)$, when the adversarial input w_1 occurs to Σ_1, causing the unauthorized transition $s_1(x_2, c) = x_4$. This event is diagnosed by observing that the state feedback changes from (x_2, y_2) to (x_4, y_2) while the external input c remains fixed. To investigate the existence of a fault tolerant controller, we apply the result of Theorem 1. Computing $\hat{R}(\Sigma_1)$ and $\hat{R}(\Sigma_2)$ (omitted) and applying Theorem 1(a) lead to the existence of a control input sequence $t = bad$ such that $t \in \hat{R}_{4,2}(\Sigma_1) \cap \hat{R}_{2,2}(\Sigma_2)$. Hence, by Theorem 1, a corrective controller C can be designed that achieves fault recovery against w_1.

In a similar fashion, we examine the existence of a fault tolerant controller for an unauthorized transition by w_2. Referring to Fig. 2, w_2 may happen when Σ_2 stays at the stable combination (y_3, b) with which Σ_1 may stay at (x_1, b) or (x_3, b). Thus possible original stable combinations of Σ are $((x_1, y_3), b)$ and $((x_3, y_3), b)$. But no feasible control input sequences exist that satisfy condition (b) of Theorem 1 for any initial state. Hence fault recovery against w_2 is impossible.

V. Summary

We have investigated fault recovery for a class of composite asynchronous sequential machines with parallel composition. We have examined whether an unauthorized state transition can be tolerated in the closed-loop system of composite asynchronous sequential machines endowed with full state feedback. Specifically, the condition for fault recovery is addressed using an extended matrix of stable transitions, while avoiding computational burden of deriving the entire dynamics of the composite machine. The proposed method has been demonstrated using a simple illustrative example.

References

[1] X. Geng and J. Hammer, "Input/output control of asynchronous sequential machines," *IEEE Trans. Autom. Control*, vol. 50, no. 12, pp. 1956–1970, 2005.
[2] J. Peng and J. Hammer, "Input/output control of asynchronous sequential machines with races," *Int. J. Control*, vol. 83, no. 1, pp. 125–144, 2010.
[3] J. Hammer, "Automatic defensive control of asynchronous sequential machines," *Int. J. Control*, vol. 89, no. 1, pp. 193–209, 2015.
[4] B. Wang, J. E. Feng, and M. Meng, "Matrix approach to model matching of composite asynchronous sequential machines," *IET Control Theory Appl.*, vol. 11, no. 13, pp. 2122–2130, 2017.
[5] T. E. Murphy, X. Geng, and J. Hammer, "On the control of asynchronous machines with races," *IEEE Trans. Autom. Control*, vol. 48, no. 6, pp. 1073–1081, 2003.
[6] N. Venkatraman and J. Hammer, "On the control of asynchronous sequential machines with infinite cycles," *Int. J. Control*, vol. 79, no. 7, pp. 764–785, 2006.
[7] J. Peng and J. Hammer, "Bursts and output feedback control of non-deterministic asynchronous sequential machines," *Eur. J. Control*, vol. 18, no. 3, pp. 286–300, 2012.
[8] J.–M. Yang, "Corrective control of composite asynchronous sequential machines under partial observation," *IEEE Trans. Autom. Control*, vol. 61, no. 2, pp. 473–478, 2016.
[9] J.–M. Yang, "On fault diagnosis of asynchronous sequential machines with parallel composition," *WASET Int. J. Comput., Electr., Automat., Control, Info. Eng.*, vol. 11, no. 9, pp. 947–950, 2017.
[10] J.–M. Yang, "Modeling and control of switched asynchronous sequential machines," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2714–2719, 2016.
[11] J.–M. Yang, "Conditions for model matching of switched asynchronous sequential machines with output feedback," *WASET Int. J. Electr. Comput. Energ. Electron. Commun. Eng.*, vol. 11, no. 1, pp. 55–59, 2017.
[12] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*, 2nd ed., New York, NY: Springer-Verlag, 2008.
[13] Z. Kohavi and N. K. Jha, *Switching and Finite Automata Theory*, 3rd ed., Cambridge, UK: Cambridge University Press, 2010.