Automatica 97 (2018) 115–120

Contents lists available at ScienceDirect

Automatica

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

Brief paper

Exact fault recovery for asynchronous sequential machines with output bursts[☆]

Jung-Min Yang

School of Electronics Engineering, Kyungpook National University, 80 Daehakro, Bukgu, Daegu, 41566, Republic of Korea

ARTICLE INFO

Article history:
Received 17 June 2017
Received in revised form 4 December 2017
Accepted 25 June 2018
Available online 18 August 2018

Keywords:
Asynchronous sequential machines (ASMs)
Corrective control
Fault tolerant control
Output bursts

ABSTRACT

This paper presents an enhanced fault tolerant control strategy for a class of input/output asynchronous sequential machines (ASMs) in which output feedback takes the form of bursts. We design a corrective controller that counteracts any unauthorized state transition occurring to the ASM. As the controlled machine is steered on a feedback path, uncertainty about the goal state is reduced by the information that output bursts provide. Hence the use of output bursts in the correction procedure allows the controller to conduct more refined fault recovery than the case of accessing unit output characters as feedback. We present the existence condition and design procedure for a controller that achieves exact fault recovery, and provide an illustrative example to demonstrate the procedure of controller synthesis.

1. Introduction

As an event-driven feedback scheme, corrective control is used to compensate for asynchronous sequential machines (ASMs). Even though an ASM has undesirable transient characteristics, its stable-state behavior can be adjusted by virtue of asynchrony so as to show the desirable behavior. The performance of corrective control is prominent especially in diagnosing and tolerating various faults occurring to ASMs. Theoretical development of this topic is found in, e.g., Geng and Hammer (2005), Murphy, Geng, and Hammer (2003), Xu and Hong (2013), Yang (2010), and experimental verification in Yang and Kwak (2015).

We study fault tolerant control of input/output ASMs. As addressed by Geng and Hammer (2005), a critical subject of input/output control of ASMs is how to deal with uncertainty about the state, as access to the state is infeasible in input/output control. In Geng and Hammer (2005) and Peng and Hammer (2012), output feedback takes the form of bursts, or a quick succession of output characters, and state observers are designed to derive the current state. On the other hand, in the author's previous work (Yang, 2015) a simple controller is presented that uses neither bursts nor state observers, albeit needing stricter existence conditions for controllers.

Our objective is to propose an enhanced fault tolerant control scheme for input/output ASMs. While the proposed configuration employs bursts as output feedback, it does not require state observers unlike the prior work. In this sense, the present approach is similar to Yang (2015). However, the present study has the following novel contributions. First, when unit characters are available as output feedback, some harsh condition is needed to determine the end of stable transitions (Yang, 2015). On the other hand, since the burst gives more information on the current stable transition, the controller is more likely to determine its end, which is crucial to preserving fundamental mode operations. Next, in this study the controller achieves *exact fault recovery*, namely, the ASM can be controlled to return to the original state at which it stayed at the moment of fault occurrence. We can reduce the state uncertainty using bursts so that the closed-loop system converges to the original state.

We first present fault detectability to diagnose the end of unauthorized transitions. Main consideration is given to addressing *exact feedback paths* that are needed to define a trajectory along which the ASM can return to the original state at which the fault occurs. Uncertainty about the current state as well as the original state will be refined throughout exact feedback paths. Using an exact feedback path, we present the existence condition and design procedure for a corrective controller realizing fault recovery and validate them in an illustrative example.

2. Modeling

Fig. 1 shows the corrective control system for an input/output ASM $\Sigma = (A, Z, X, X_0, f, h)$, where A, Z, X are the input, output, and

☆ This research was supported in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. NRF-2015R1D1A1A01056764), and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2018R1A5A1025137). The material in this paper was not presented at any conference. This paper was recommended for publication in revised form by Associate Editor Christoforos Hadjicostis under the direction of Editor Christos G. Cassandras.

E-mail address: jmyang@ee.knu.ac.kr.

https://doi.org/10.1016/j.automatica.2018.08.001
0005-1098/

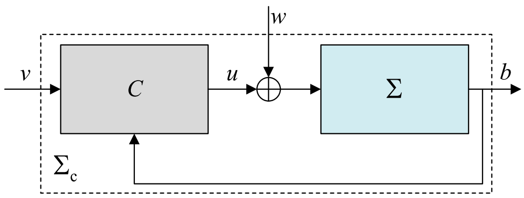

Fig. 1. Corrective control system with output burst.

state sets, respectively, $X_0 \subset X$ are the initial states, $f : X \times A \to X$ is the state transition function partially defined on $X \times A$, and $h : X \to Z$ is the output function. A is divided into $A = A_n \dot{\cup} A_d$ where A_n and A_d are the sets of normal and adversarial inputs, respectively. C is the corrective controller and Σ_c is the closed-loop system composed of C and Σ. Due to asynchrony, Σ responds only to direct input changes with very rapid transient transitions. When Σ transfers from a stable state x to the next stable state x' with an input u, it traverses intermediate transient states instantaneously. Hence a chain of transitions from a stable state to the next one can be regarded as a single transition, termed a *stable transition*. The latter property is characterized by the stable recursion function $s : X \times A \to X$ defined as $s(x, u) := x'$ where x' is the next stable state of (x, u). The domains of s are extended to $X \times A^+$ in a natural way, where A^+ is set of all non-empty strings of characters of A.

A sequence of output characters is generated in a stable transition. Since repeating characters are indiscernible in dynamics of ASMs, the output feedback takes the form of a *burst* $b \in Z^+$ (Geng & Hammer, 2005) in which any segment of repeating characters is compressed to a single one. Denote by $\beta(\mathbf{z})$ the burst of an output sequence $\mathbf{z} \in Z^+$. For $\mathbf{z} = z_1 \cdots z_{|\mathbf{z}|-1} z_{|\mathbf{z}|}$, let $\beta_{-1}(\mathbf{z}) := \beta(z_1 \cdots z_{|\mathbf{z}|-1})$. For notational convenience, let $\beta(x, u)$ denote the burst generated in the stable transition $s(x, u) = x'$.

Definition 1 (*Murphy et al., 2003*)**.** For Σ with $X := \{x_1, \ldots, x_n\}$, the matrix of stable transitions $R(\Sigma)$ is an $n \times n$ matrix whose (i, j) entry is defined as

$$R_{i,j}(\Sigma) := \{t \in A_n^+ | s(x_i, t) = x_j,\ 1 \leqslant |t| \leqslant n - 1\}.$$

$R_{i,j}(\Sigma)$ contains all input strings with which Σ transfers from x_i to x_j via a chain of stable transitions.

When an adversarial input $w \in A_d$ happens, it overrides the current input $u \in A_n$, causing Σ to undergo an unauthorized transition. Unless recovered immediately, Σ would have incorrect next behavior. For $x \in X$, let

$$W(x) := \{w \in A_d | s(x, w)!, s(x, w) \neq x\}$$

be the set of adversarial inputs that can occur to Σ when it stays at x ('$s(x, w)!$' means that $s(x, w)$ is defined). Also, for $X_1 \subset X$, let $W(X_1) := \cup_{x \in X_1} W(x)$.

Referring to Fig. 1, C receives the external input $v \in A_n$ and the output feedback $b \in Z^+$ to generate the control input $u \in A_n$. C is modeled as an input/output ASM

$$C = (A_n \times Z^+, A_n, \Xi, \xi_0, \phi, \eta)$$

where Ξ is the state set, $\xi_0 \in \Xi$ is the initial state, $\phi : \Xi \times A_n \times Z^+ \to \Xi$ is the recursion function, and $\eta : \Xi \to A_n$ is the output function. The control objective is to achieve immediate fault recovery against any unauthorized transitions caused by w. In the prior work (Peng & Hammer, 2012; Yang, 2015), fault recovery is evaluated in terms of the input/output behavior, namely, it is regarded as achieved if Σ_c is controlled to reach any state generating the original output. This specification is attributed to the constraint that C does not have access to the state of Σ.

In this paper, we present a novel scheme that accomplishes exact fault recovery by taking Σ towards the original state at which the fault occurs. This is made possible by updating state uncertainties based on the obtained bursts. Compared with a unit character, a burst contains more information on the trajectory traversed by Σ. For $s(x, u) = x'$, $\beta(x, u)$ has all discernible output values of intermediate transient states, while the unit output feedback only displays the last value $h(x')$. A downside of using bursts is that computational complexity increases since the controller must be endowed with a buffer or memory to record the burst. The buffer size is also proportional to the cardinality of the state set.

3. State uncertainty

To deal with inaccessibility of the state, we define *state uncertainty* $\chi \subset X$ that contains all possible states where Σ may stay. If $f(x, u)!$ for every $x \in \chi$, (χ, u) is called a valid pair. χ is updated in the course of normal and unauthorized transitions. Assume first that Σ with χ takes a normal stable transition in response to a valid u, generating burst b. Let

$$T_n(\chi, u, b) := \{x' \in X | \exists x \in \chi,\ s(x, u) = x', \beta(x, u) = b\}$$

be a mapping that provides the updated uncertainty with respect to χ, u, and b in normal transitions. Once b is received, we trace b back to the states from which Σ may originate. For $x' \in T_n(\chi, u, b)$, let

$$Q_n(x', u, b) := \{x \in \chi | s(x, u) = x', \beta(x, u) = b\}$$

be the set of such states. $Q_n(x', u, b) \subset \chi$ is a refinement of χ with respect to x', u, and b, that is, if the current state is x', Σ must have stayed at a state of $Q_n(x', u, b)$ when u enters Σ. For $\chi' \subseteq T_n(\chi, u, b)$, define $Q_n(\chi', u, b) := \cup_{x' \in \chi'} Q_n(x', u, b)$.

Next, consider an unauthorized transition by w, which is perceived by observing that the output feedback changes while the control input remains fixed. Suppose Σ staying at a (unknown) state $x \in \chi$ undergoes an unauthorized transition such that the burst changes to b. Let

$$T_d(\chi, b) := \{x' \in X | \exists x \in \chi, \exists w \in W(x),\ s(x, w) = x', \beta(x, w) = b\}$$

be the uncertainty updated from χ after an unauthorized transition with b. Similarly, let

$$Q_d(x', b) := \{x \in \chi | \exists w \in W(x), s(x, w) = x', \beta(x, w) = b\}$$

be the refined uncertainty of χ with respect to $x' \in T_d(\chi, b)$ after the unauthorized transition. Also, for $\chi' \subseteq T_d(\chi, b)$, define $Q_d(\chi', b) := \cup_{x' \in \chi'} Q_d(x', b)$.

To prohibit unpredictable outcomes caused by the absence of a synchronizing clock, Σ_c must comply with the principle of fundamental mode operations (Kohavi & Jha, 2010). To this end, C must always identify the end of a stable transition; otherwise, Σ could have unintended transitions as the control input may change while Σ is in transient transitions. The latter condition is called *strong detectability* for normal transitions (Peng & Hammer, 2012) and *strong fault detectability* for unauthorized transitions (Yang, 2015).

One can determine the end of a normal stable transition $s(x, u)$ if and only if the end of the output sequence is signified by a difference in the burst, which is written as $\beta_{-1}(x, u) \neq \beta(x, u)$ (Geng & Hammer, 2005). Under the existence of uncertainty χ, we cannot predict which burst will be generated. Thus the foregoing condition should be valid for all the possible bursts. Let

$$B_n(\chi, u) := \{\beta(x, u) | x \in \chi\}$$
$$B_d(\chi) := \{\beta(x, w) | x \in \chi, w \in W(x)\}$$

be the sets of all bursts that can be generated in the stable transition from χ with u and in the unauthorized transition from χ, respectively.