[2] W. M. Wonham, *Linear Multivariable Control: A Geometric Approach*, 2nd ed. New York: Springer-Verlag, 1985.

[3] A. Saberi and P. Sannuti, “A special coordinate basis of multivariable linear systems-finite and infinite zero structure, squaring down and decoupling.,” *Int. J. Control*, vol. 45, pp. 1655–1704, 1987.

[4] B. M. Chen, *Robust and H_∞ Control*. Berlin, Germany: Springer-Verlag, 2000.

[5] M. A. Rotea, M. Corless, and S. M. Swei, “Necessary and sufficient conditions for quadratic controllability of a class of uncertain systems,” *Syst. Control Lett.*, vol. 26, pp. 195–201, 1995.

[6] J. M. Schumacher, “On the structure of strongly controllable systems,” *Int. J. Control*, vol. 38, pp. 525–545.

[7] P. P. Khargonekar, I. R. Petersen, and K. Zhou, “Robust stabilization of uncertain systems: Quadratic stabilizability and H^∞ control theory,” *IEEE Trans. Automat. Contr.*, vol. 35, pp. 356–361, Mar. 1990.

[8] C. C. Paige, “Properties of numerical algorithms related to computing controllability,” *IEEE Trans. Automat. Contr.*, vol. AC-26, pp. 130–138, Feb. 1981.

[9] D. Chu, X. Liu, and R. C. E. Tan, “On the numerical computation of a structural decomposition for linear systems,” Dept. Math., National Univ. Singapore, Singapore, Tech. Rep., 2001.

Polynomial-Time Verification of Diagnosability of Partially Observed Discrete-Event Systems

Tae-Sic Yoo and Stéphane Lafortune

***Abstract*—The problem of verifying the properties of diagnosability and I-diagnosability is considered. We present new polynomial-time algorithms for deciding diagnosability and I-diagnosability. These algorithms are based on the construction of a nondeterministic automaton called a verifier.**

***Index Terms*—Computational complexity, diagnosability verification, discrete-event systems, failure diagnosis.**

I. Introduction

The property of diagnosability in discrete-event systems is related to the ability to infer, from observed event sequences, about the occurrence of certain unobservable events (the “failure” events). A precise language-based characterization of the notion of diagnosability is given in [1]. For discrete-event systems modeled by regular languages, diagnosability can be verified by building the *diagnoser* corresponding to the finite-state automaton model of the system. Diagnosers are special types of observers that carry failure information by means of labels attached to states. Once the diagnoser has been built, diagnosability can be tested in polynomial time in the cardinality of the state space of the diagnoser. However, the state space of the diagnoser is in the worst case exponential in the cardinality of the state space of the system model. Recently, a test of diagnosability that requires polynomial time in the cardinality of the state space of the system was presented in [2]. The contribution of this note is to present a different method of testing diagnosability that also requires polynomial time in the cardinality of the state space of the system.[1] Our test does not rely on diagnosers. Rather, the new test is based on the construction of an automaton that we call a *verifier*. We show that verifiers can also be suitably modified for testing the property of I-diagnosability in polynomial time. Verifiers are reminiscent of the automata that are used for testing (in polynomial time) the properties of observability and normality [3], coobservability [4], and a generalized notion of coobservability introduced in [5]. Thus, the properties of diagnosability, I-diagnosability, observability, normality, and coobservability are all verifiable in polynomial time.

We assume basic knowledge of discrete-event systems and its common notations. The readers are directed to [6] for more complete introductory materials.

II. Preliminaries

We model the untimed discrete-event system as a deterministic finite-state automaton

$$G = \left(Q^G, \Sigma, \delta^G, q_0^G\right)$$

where Q^G is the finite state space, Σ is the set of events, and q_0^G is the initial state of the system. δ^G is the partial transition function and $\delta^G(q_1, \sigma) = q_2$ or $q_1 \xrightarrow{\sigma}_G q_2$ implies existence of a transition from state q_1 to state q_2 with event label σ. (The superscript or subscript G may be dropped if this is not likely to cause confusion.) The language generated by G is denoted by $\mathcal{L}(G)$ and is defined in the usual manner [6].

To reflect limitations on observation, we partition the set of events Σ as $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$ where Σ_o is the set of observable events and Σ_{uo} is the set of unobservable events.

In the context of failure diagnosis, let $\Sigma_f \subseteq \Sigma$ denote the set of failure events which should be diagnosed. We assume, without loss of generality, that $\Sigma_f \subseteq \Sigma_{uo}$, since an observable failure event can be diagnosed trivially. The objective is to identify the occurrence, if any, of the failure events, while tracking the observable traces generated by the system. In this regard, the set of failure events is partitioned into disjoint sets corresponding to different failure types

$$\Sigma_f = \Sigma_{f1} \dot{\cup} \cdots \dot{\cup} \Sigma_{fm}.$$

We denote this partition by Π_f. Hereafter, when we write that a failure of type F_i has occurred, we will mean that some event in the set Σ_{fi} has occurred. The formal definitions of diagnosability and I-diagnosability were first presented in [1] and are recalled below.

To define diagnosability, we need following notations. We will write $s \in \Psi(\Sigma_{fi})$ to denote that the last event of a trace $s \in L$ is a failure event of type F_i. That is

$$\Psi\left(\Sigma_{fi}\right) := \left\{s\sigma_f \in L : \sigma_f \in \Sigma_{fi}\right\}.$$

We denote by L/s the postlanguage of L after s, i.e.,

$$L/s := \left\{t \in \Sigma^* : st \in L\right\}.$$

With slight abuse of notation, we write $\Sigma_{fi} \in s$ to denote that $\bar{s} \cap \Psi(\Sigma_{fi}) \neq \emptyset$. The following assumptions on the language $\mathcal{L}(G)$ are made when diagnosability is considered:

A1) G has no cycles of unobservable events;

A2) $\mathcal{L}(G)$ is live.

We are now ready to state the definition of diagnosability introduced in [1].

Manuscript received March 29, 2001. Recommended by Associate Editor R. S. Sreenivas. This work was supported in part by the National Science Foundation under Grants ECS-0080406 and CCR-0082784, in part by the DDR&E MURI on Low Energy Electronics Design for Mobile Platforms, and managed by ARO under Grant ARO DAAH04-96-1-0377.

The authors are with the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109-2122 USA (e-mail: tyoo@eecs.umich.edu; stephane@eecs.umich.edu).

Publisher Item Identifier 10.1109/TAC.2002.802763.

[1] Our test was developed independently from that in [2].

Definition 1: A prefix-closed and live language L is said to be diagnosable with respect to Σ_o and Π_f on Σ_f if the following holds:

$$\begin{aligned}&(\forall i \in \Pi_f)(\exists N_i \in \mathbb{N})(\forall s \in \Psi(\Sigma_{fi}))(\forall t \in L/s)\\ &\quad [|t| \geq N_i \Rightarrow D]\end{aligned}$$

where the diagnosability condition D is

$$\forall w \in P_{\Sigma_o}^{-1} P_{\Sigma_o}(st) \cap \mathcal{L}(G) \Rightarrow \Sigma_{fi} \in w$$

where $P_{\Sigma_o} : \Sigma^* \rightarrow \Sigma_o^*$ is the usual projection mapping and $\mathbb{N}$ is the set of nonnegative integers.

We may drop the subscript Σ_o when it is considered to be obvious from the context. The definition of diagnosability requires condition D to hold for all traces of L containing a failure event. In [1], this notion is relaxed by considering only the traces in which the failure event is followed by certain indicator observable events associated with every failure type. This notion is called I-diagnosability. To define this notion, every failure event in Σ_f is mapped to one or more observable indicator events in $\Sigma_I \subseteq \Sigma_o$. Let $I_f : \Sigma_f \rightarrow 2^{\Sigma_I}$ denote the indicator map where

$$\sigma_{f1}, \sigma_{f2} \in \Sigma_{fi} \Rightarrow I_f(\sigma_{f1}) = I_f(\sigma_{f2}).$$

For notational convenience, let us define

$$I(\Sigma_{fi}) = I_f(\sigma_f) \text{ for any } \sigma_f \in \Sigma_{fi}.$$

Therefore, $I(\Sigma_{fi})$ denotes the set of observable indicator events associated with the failure type F_i. I-diagnosability can now be formally defined.

Definition 2: A prefix-closed and live language L is said to be I-diagnosable with respect to Σ_o and Π_f on Σ_f and indicator map I if the following holds:

$$\begin{aligned}&(\forall i \in \Pi_f)(\exists N_i \in \mathbb{N})(\forall s \in \Psi(\Sigma_{fi}))\\ &(\forall t_1 t_2 \in L/s : st_1 \in \Psi[I(\Sigma_{fi})])[|t_2| \geq N_i \Rightarrow D]\end{aligned}$$

where the diagnosability condition D is

$$\forall w \in P^{-1} P(st_1 t_2) \cap \mathcal{L}(G) \Rightarrow \Sigma_{fi} \in w.$$

III. Verification of Diagnosability in Polynomial-Time

Let $|Q^G| = n_1$, $|\Sigma| = n_2$ and $|\Pi_f| = n_3$. The diagnosability verification algorithm presented in [1] relies on the construction of the diagnoser, a step that requires exponential-time complexity with respect to n_1 and n_3 in the worst case. In this section, we develop an algorithm that can decide diagnosability and I-diagnosability in polynomial time with respect to n_1, n_2, and n_3.

A. Case of Diagnosability: The F_i-Verifier

First, we construct from G a *nondeterministic* automaton V_{F_i} for the failure events of type F_i. We call this automaton the F_i *-verifier*.

$$V_{F_i} = \mathrm{Trim}\left(Q^{V_{F_i}}, \Sigma, \delta^{V_{F_i}}, q_0^{V_{F_i}}\right)$$

where

$$\begin{aligned}Q^{V_{F_i}} &:= Q^G \times L_i \times Q^G \times L_i\\ q_0^{V_{F_i}} &:= \left(q_0^G, N, q_0^G, N\right)\end{aligned}$$

with the label set $L_i := \{N, F_i\}$ for the failure events of type F_i. Hereafter, only the accessible part of the state space $Q^{V_{F_i}}$ is considered when we refer the state space $Q^{V_{F_i}}$.

The (nondeterministic) transition rule $\delta^{V_{F_i}}$ is defined as follows.

For $\sigma \in \Sigma_{fi}$

$$\delta^{V_{F_i}}((q_1, l_1, q_2, l_2), \sigma) = \begin{cases}\left(\delta^G(q_1, \sigma), F_i, q_2, l_2\right)\\ \left(q_1, l_1, \delta^G(q_2, \sigma), F_i\right)\\ \left(\delta^G(q_1, \sigma), F_i, \delta^G(q_2, \sigma), F_i\right).\end{cases} \tag{1}$$

For $\sigma \in \Sigma_{uo} \setminus \Sigma_{fi}$

$$\delta^{V_{F_i}}((q_1, l_1, q_2, l_2), \sigma) = \begin{cases}\left(\delta^G(q_1, \sigma), l_1, q_2, l_2\right)\\ \left(q_1, l_1, \delta^G(q_2, \sigma), l_2\right)\\ \left(\delta^G(q_1, \sigma), l_1, \delta^G(q_2, \sigma), l_2\right).\end{cases} \tag{2}$$

For $\sigma \in \Sigma_o$

$$\delta^{V_{F_i}}((q_1, l_1, q_2, L_2), \sigma) = \left(\delta^G(q_1, \sigma), l_1, \delta^G(q_2, \sigma), l_2\right). \tag{3}$$

Intuitively, the aforementioned nondeterministic transition rule tracks two strings in $\mathcal{L}(G)$ that look identical under the projection P_{Σ_o} while updating the failure information as these two strings evolve. We define the following terminology for further arguments.

Definition 3: We say that $\{v_1, v_2, \ldots, v_n\} \subseteq Q^{V_{F_i}}$ form a path, denoted by $\langle v_1, v_2, \ldots, v_n\rangle_{V_{F_i}}$, if there are transitions such that $v_1 \xrightarrow{\sigma_1} v_2 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_{n-1}} v_n$. We say that a path, $\langle v_1, v_2, \ldots, v_n\rangle_{V_{F_i}}$, forms a cycle if $v_1 = v_n$ and at least one transition is contained along the path.

Definition 4: V_{F_i} is called F_i-confused if there is a cycle, $\langle v_1, v_2, \ldots, v_1\rangle_{V_{F_i}}$, such that for all $v_i := (q_1^{v_i}, l_1^{v_i}, q_2^{v_i}, l_2^{v_i})$, $l_1^{v_i} = F_i$ and $l_2^{v_i} = N$ or vice versa. We call this cycle an F_i-confused cycle. If there are no such cycles, we say that V_{F_i} is F_i-confusion free.

Let us denote the trivial partition of Σ_{fi} by $\hat{\Pi}_{fi}$. That is, Σ_{fi} itself is the partition of Σ_{fi}. With this, we have the following result.

Theorem 1: $\mathcal{L}(G)$ is diagnosable w.r.t. Σ_o and Π_f on Σ_f iff it is diagnosable w.r.t. Σ_o and $\hat{\Pi}_{fi}$ on Σ_{fi}, for all $i \in \Pi_f$.

Proof: From the definition of diagnosability, $\mathcal{L}(G)$ is not diagnosable w.r.t. Σ_o and Π_f on Σ_f iff there is $\sigma_{fi} \in \Sigma_{fi}$ that violates the diagnosability condition. Moreover, we have that there is $\sigma_i \in \Sigma_{fi}$ that violates the diagnosability condition iff it is not diagnosable w.r.t. Σ_o and $\hat{\Pi}_{fi}$ on Σ_{fi}. ■

In [1], the authors define the notion of F_i-indeterminate cycle in the diagnoser G_d. This concept provides a necessary and sufficient condition to decide the diagnosability of the given language $\mathcal{L}(G)$. The construction of the diagnoser G_d with the label space $L_1 \times \cdots \times L_m$ results in exponential-time complexity with respect to the number of failure types, $|\Pi_F|$, in the worst case. Instead of adopting the approach of [1] using $L_1 \times \cdots \times L_m$ as the label space, we construct the set of verifiers V_{F_i}, for all $i \in \Pi_f$. The following theorem shows that an F_i-confused cycle in the F_i verifier, V_{F_i}, can be utilized to verify diagnosability.

Theorem 2: $\mathcal{L}(G)$ is diagnosable w.r.t. Σ_o and Π_f on Σ_f iff V_{F_i} is F_i-confusion free for all $i \in \Pi_f$.

Proof: In view of Theorem 1, it is sufficient to show that, for each $i \in \Pi_f$, $\mathcal{L}(G)$ is diagnosable w.r.t. Σ_o and $\hat{\Pi}_{fi}$ on Σ_{fi} iff V_{F_i} is F_i-confusion free.

($\Rightarrow$) Assume that $\mathcal{L}(G)$ is diagnosable with respect to Σ_o and $\hat{\Pi}_{fi}$ on Σ_{fi}. For the sake of contradiction, suppose that V_{F_i} is F_i-confused. That is, there exists an F_i-confused cycle, $\langle v_1, v_2, \ldots, v_n\rangle_{V_{F_i}}$. Without loss of generality, let $v_1 := (q_1^{v_1}, F_i, q_2^{v_1}, N)$. Then, we have by the construction of V_{F_i} that there exist $s_0, s_0' \in \mathcal{L}(G)$ such that

$$\begin{aligned}&[P(s_0) = P(s_0')] \wedge \left[\delta^G\left(q_0^G, s_0\right) = q_1^{v_1}\right]\\ &\qquad \wedge \left[\delta^G\left(q_0^G, s_0'\right) = q_2^{v_1}\right]\\ &\qquad \wedge [\Sigma_{fi} \in s_0] \wedge \left[\Sigma_{fi} \notin s_0'\right].\end{aligned}$$

Let us denote the transitions over the cycle $\langle v_1, v_2, \ldots, v_n\rangle_{V_{F_i}}$ as follows:

$$v_1 \xrightarrow{\sigma_1} v_2 \xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_{n-1}} v_n.$$

Since $\langle v_1, v_2, \ldots, v_n\rangle_{V_{F_i}}$ forms an F_i-confused cycle, the following should hold:

$$\begin{aligned}(q_1^{v_1}, F_i, q_2^{v_1}, N) &\xrightarrow{\sigma_1} (q_1^{v_2}, F_i, q_2^{v_2}, N)\\ &\xrightarrow{\sigma_2} \cdots \xrightarrow{\sigma_{n-1}} (q_1^{v_n}, F_i, q_2^{v_n}, N)\end{aligned}$$

where $v_i := (q_1^{v_i}, F_i, q_2^{v_i}, N)$, for $i \in \{1, \ldots, n\}$. Let us define an indicator function $I : Q^G \times \Sigma \times Q^G \rightarrow \Sigma \cup \{\epsilon\}$ such that

$$I(q_1, \sigma, q_2) = \begin{cases} \sigma, & \text{if } \delta^G(q_1, \sigma) = q_2 \\ \epsilon, & \text{if } \delta^G(q_1, \sigma) \neq q_2. \end{cases}$$

Consider the two traces $w(k)$ and $w'(k)$ such that

$$\begin{aligned} w(k) &= s_0 \left\{\Pi_{i=1}^{n-1} I\left(q_1^{v_i}, \sigma_i, q_1^{v_{i+1}}\right)\right\}^k \\ w'(k) &= s'_0 \left\{\Pi_{i=1}^{n-1} I\left(q_2^{v_i}, \sigma_i, q_2^{v_{i+1}}\right)\right\}^k \end{aligned}$$

where $k \geq 0$. Then, from the construction of V_{F_i}, we have for all $k \geq 0$

$$\begin{aligned}\left[w(k), w'(k) \in \mathcal{L}(G)\right] &\wedge \left[P(w(k)) = P\left(w'(k)\right)\right] \\ &\wedge \left[\Sigma_{fi} \in w(k)\right] \wedge \left[\Sigma_{fi} \notin w'(k)\right].\end{aligned}$$

Since we have assumed that there is no unobservable cycle in $\mathcal{L}(G)$, we know that $P(\sigma_1 \cdots \sigma_{n-1}) \neq \epsilon$ from the construction of V_{F_i}. This implies that $|P\{\Pi_{i=1}^{n-1} I(q_1^{v_i}, \sigma_i, q_1^{v_{i+1}})\}| \geq 1$ and $|P\{\Pi_{i=1}^{n-1} I(q_2^{v_i}, \sigma_i, q_2^{v_{i+1}})\}| \geq 1$. Since $\Sigma_{fi} \in s_0$, we can find s such that

$$[s \in \bar{s}_0] \wedge [s \in \Psi(\Sigma_{fi})].$$

Let $t \in \mathcal{L}/s$ be such that $st = w(k)$. By choosing k arbitrarily large, we can get $|t| \geq N_1$ for any given $N_1 \geq 1$. However, we know for all $k \geq 0$

$$\left[w'(k) \in P^{-1}P(st) \cap \mathcal{L}(G)\right] \wedge \left[\Sigma_{fi} \notin w'(k)\right].$$

Therefore, the definition of diagnosability is violated.

($\Leftarrow$) Assume that V_{F_i} is F_i-confusion free. Now we suppose that $\mathcal{L}(G)$ is not diagnosable with respect to Σ_o and $\hat{\Pi}_{fi}$ on Σ_{fi} for the sake of contradiction. This implies that

$$\begin{aligned}&(\forall n \geq 1)\,(\exists s \in \Psi(\Sigma_{fi}))\,(\exists t \in \mathcal{L}(G)/s) \text{ s.t.} \\ &[|t| \geq n] \wedge \left[\left(\exists w' \in P^{-1}P(st) \cap \mathcal{L}(G)\right)\left[\Sigma_{fi} \notin w'\right]\right].\end{aligned}$$

Let us pick any $n \geq |Q^G|^2$. Since $w' \in P^{-1}P(st) \cap \mathcal{L}(G)$, we can pick a trace $s' \in \bar{w}'$ such that $s' \in P^{-1}P(s) \cap \mathcal{L}(G)$. Moreover, it is obvious that $\Sigma_{fi} \notin s'$ since $\Sigma_{fi} \notin w'$. Now, let us denote the states reached by s and s' as q_s and $q_{s'}$, respectively. That is

$$q_s := \delta^G\left(q_0^G, s\right) \qquad q_{s'} := \delta^G\left(q_0^G, s'\right).$$

Then, by the construction of V_{F_i}, $(q_s, F_i, q_{s'}, N) \in Q^{V_{F_i}}$ is an accessible state of V_{F_i}. Similarly, we define

$$q_{st} := \delta^G\left(q_0^G, st\right) \qquad q_{w'} := \delta^G\left(q_0^G, w'\right).$$

Then, $(q_{st}, F_i, q_{w'}, N) \in Q^{V_{F_i}}$ is an accessible state of V_{F_i}. Moreover, there exist transitions $\sigma_1\sigma_2 \ldots \sigma_{n'} := t' \in \Sigma^*$ such that $n' \geq n$ and

$$\begin{aligned}\left(q_{k_0}, F_i, q_{k'_0}, N\right) &\xrightarrow{\sigma_1}_{V_{F_i}} \left(q_{k_1}, F_i, q_{k'_1}, N\right) \\ &\xrightarrow{\sigma_2}_{V_{F_i}} \cdots \xrightarrow{\sigma_{n'}}_{V_{F_i}} \left(q_{k_{n'}}, F_i, q_{k'_{n'}}, N\right)\end{aligned}$$

where $(q_{k_0}, F_i, q_{k'_0}, N) := (q_s, F_i, q_{s'}, N)$ and $(q_{k_{n'}}, F_i, q_{k'_{n'}}, N) := (q_{st}, F_i, q_{w'}, N)$. Since $n' \geq n \geq |Q^G|^2$, there exist $1 \leq i < j \leq n'$ such that

$$\left(q_{k_i}, F_i, q_{k'_i}, N\right) = \left(q_{k_j}, F_i, q_{k'_j}, N\right).$$

Then, the set of states $\{(q_{k_l}, F_i, q_{k'_l}, N) : i \leq l \leq j\}$ forms an F_i-confused cycle. This contradicts the assumption. ■

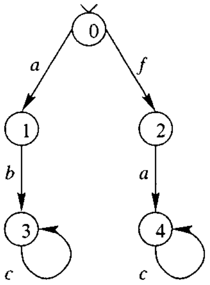

Fig. 1. System G.

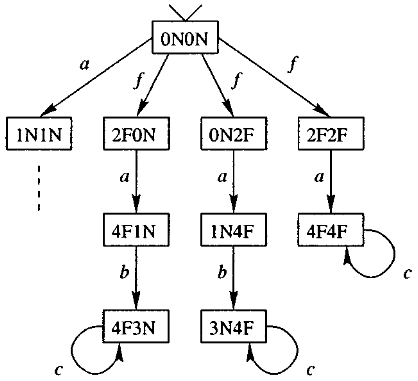

Fig. 2. F-verifier: V_F.

Example 1: The system to be diagnosed is shown in Fig. 1. We set $\Sigma_{f1} = \Sigma_f = \{f\}$, $\Sigma_o = \{a, c\}$. Let us look at the following traces:

$$w_n = fac^n \quad w'_n = abc^n.$$

Since $w'_n \in P^{-1}P(w_n) \cap \mathcal{L}(G)$ and $\Sigma_f \notin w'_n$ for all $n \geq 0$, we know that $\mathcal{L}(G)$ is not diagnosable w.r.t. Σ_o and Π_f on Σ_f. We show this result by constructing the F-verifier; the relevant part of V_F is shown in Fig. 2. From the initial state $(0, N, 0, N)$, two events, a and f, are feasible. Follow the transition f. Since $f \in \Sigma_{f1}$, there are three feasible transitions

$$\delta^{V_F}((0, N, 0, N), f) = \begin{cases} (2, F, 0, N) \\ (0, N, 2, F) \\ (2, F, 2, F). \end{cases}$$

These states are reached by the following pairs of traces:

$$\begin{aligned}(2, F, 0, N) &\leftarrow w = f, w' = \epsilon \\ (0, N, 2, F) &\leftarrow w = \epsilon, w' = f \\ (2, F, 2, F) &\leftarrow w = f, w' = f.\end{aligned}$$

Next, we do transition a from state $(2, F, 0, N)$. Since $a \in \Sigma_o$, one transition is possible

$$\delta^{V_F}((2, F, 0, N), a) = (4, F, 1, N)$$

and the corresponding traces are

$$(4, F, 1, N) \leftarrow w = fa, w' = a.$$

Next, we execute the transition b from state $(4, F, 1, N)$. Since $b \in \Sigma_{uo} \setminus \Sigma_{f1}$, three transitions could happen. However, only one transition is feasible

$$\delta^{V_F}((4, F, 1, N), b) = (4, F, 3, N).$$

The corresponding traces are

$$(4, F, 3, N) \leftarrow w = fa, \; w' = ab.$$

Finally, we consider the transition c from state $(4, F, 3, N)$. This observable transition is feasible and results in a self loop. The corresponding traces are

$$(4, F, 3, N) \leftarrow w_1 = fac, \; w_1' = abc.$$

We can see that an F-confused cycle, $< \quad (4, F, 3, N), (4, F, 3, N) >_{V_F}$, is reached by the pair of traces w_1 and w_1' whose continuations in $\mathcal{L}(G)$, denoted by w_n and w_n', demonstrate that the language $\mathcal{L}(G)$ is not diagnosable.

Suppose that we know that the system G is diagnosable. We may want to know how fast we can diagnose a failure "after" it happens. In [1], the authors obtain a bound of the length of the suffix following a failure event after which we can infer with certainty the occurrence of the failure. This bound is based on the diagnoser and involves counting the number of F_i-uncertain states. Naturally, it is an exponential bound in the worst case. We use the verifier to provide a bound that may be tighter. Let us suppose that s ends with a failure event of type F_i and consider the following set of strings:

$$C(s) := \left\{ s' \in \Sigma^* : s' \in P_{\Sigma_o}^{-1} P_{\Sigma_o}(s) \cap \mathcal{L}(G), \; \Sigma_{fi} \notin s' \right\}.$$

Take a string $t \in \Sigma^*$ such that $st \in \mathcal{L}(G)$ and $|t| = |Q^G|^2 = n_1^2$. We claim that $C(st) = \emptyset$. For the sake of contradiction, let us suppose that there exists $s't' \in C(st)$ such that $s' \in C(s)$. Denote $q_s := \delta(q_0^G, s)$, $q_{s'} := \delta(q_0^G, s')$, $q_{st} := \delta(q_0^G, st)$ and $q_{s't'} := \delta(q_0^G, s't')$. Then, by the construction of V_{F_i}, there will exist reachable states $(q_s, F_i, q_{s'}, N)$, $(q_{st}, F_i, q_{s't'}, N) \in Q^{V_{F_i}}$, and a string $r \in \Sigma^*$ such that $|r| \geq n_1^2$ and

$$(q_s, F_i, q_{s'}, N) \xrightarrow{r}_{V_{F_i}} (q_{st}, F_i, q_{s't'}, N).$$

It is easy to see that this implies that there is an F_i-confused cycle in V_{F_i}, which is a contradiction of the diagnosability of $\mathcal{L}(G)$. Consequently, we have the following result.

Proposition 1: Let $\mathcal{L}(G)$ be diagnosable with respect to Σ_o and Π_f on Σ_f. Then, any failure occurrence can be detected within $|Q^G|^2$ transitions after the failure occurs.

B. Computational Complexity

We consider the time complexity of the results of Section III-A. Recall that $|Q^G| = n_1$, $|\Sigma| = n_2$ and $|\Pi_f| = n_3$.

Proposition 2: Given $i \in \Pi_f$, V_{F_i} can be constructed in $O(n_1^2 n_2)$.

Proof: It is easy to see that for a reachable state $v \in Q^{V_{F_i}}$, the number of feasible transitions from v is $3n_2$ at most. Since the number of reachable states of V_{F_i} is $4n_1^2$ at most, the construction of V_{F_i} takes $12n_1^2 n_2$ time. Therefore, the overall complexity is $O(n_1^2 n_2)$ time. ■

Since we are only concerned with detecting the existence of an F_i-confused cycle in V_{F_i}, the event information over a path is not necessary. Therefore, we may consider the F_i-verifier as a directed graph rather than an automaton. That is, we consider a directed graph $G^i := (V^i, E^i)$ where

$$V^i := \left\{ (q_1, l_1, q_2, l_2) \in Q^{V_{F_i}} : l_1 \neq l_2 \right\}$$
$$E^i := \left\{ (u, v) : \exists \sigma \in \Sigma \text{ s.t. } \delta^{V_{F_i}}(u, \sigma) = v \right\}.$$

A directed graph is called *acyclic* if no path starts and ends at the same vertex. A more rigorous treatment of this notion can be found in [7]. Now, we can claim the following.

Proposition 3: V_{F_i} is F_i-confused free iff $G^i := (V^i, E^i)$ is acyclic.

Deciding if $G^i := (V^i, E^i)$ is acyclic takes $O(|V^i| + |E^i|)$ time [7]. With these, we can claim the following.

Proposition 4: Given V_{F_i}, the existence of an F_i-confused cycle can be decided in $O(n_1^2 n_2)$.

Proof: Since $|V^i| \leq 2n_1^2$ and $|E^i| \leq 2n_1^2 3n_2$, the claim follows consequently. ■

With Theorem 2 and Propositions 2 and 4, we can state the following theorem.

Theorem 3: The diagnosability of $\mathcal{L}(G)$ with respect to Σ_o and Π_f on Σ_f can be decided in $O(n_1^2 n_2 n_3)$.

C. Case of I-Diagnosability: The (F_i, i_i)-Verifier

In [1], the notion of I-diagnosability is also introduced. I-diagnosability requires the diagnosability condition D to hold not for all traces containing a failure event, but only for those in which the failure event is followed by certain indicator observable events associated with every failure type. With a slight modification of the construction of the F_i-verifier, we can obtain a result similar to Theorem 2. We modify the F_i-verifier as follows, resulting in the (F_i, I_i)*-verifier*.

$$V_{F_i I_i} := \text{Trim}\left(Q^{V_{F_i I_i}}, \Sigma, \delta^{V_{F_i I_i}}, q_0^{V_{F_i I_i}} \right)$$

where

$$Q^{V_{F_i I_i}} := Q^G \times L_i \times Q^G \times L_i$$
$$q_0^{V_{F_i I_i}} := \left(q_0^G, N, q_0^G, N \right)$$

with the label space $L_i := \{N, F_i, F_i I_i\}$ for the failure events of type F_i and the set of observable indicator events I_i. Let us define the label propagation function $LP_i : L_i \times \Sigma \rightarrow L_i$ as follows:

$$LP_i(l, \sigma) = \begin{cases} F_i I_i, & \text{if } l = F_i I_i \\ F_i, & \text{if } l \neq F_i I_i \text{ and } \sigma \in \Sigma_{fi} \\ F_i I_i, & \text{if } l = F_i \text{ and } \sigma \in \Sigma_{I_i} \\ l, & \text{o.w.} \end{cases}$$

The transition rule $\delta^{V_{F_i I_i}}$ is defined as follows.

For $\sigma \in \Sigma_{fi}$

$$\delta^{V_{F_i I_i}}\left((q_1, l_1, q_2, l_2), \sigma \right) = \begin{cases} \left(\delta^G(q_1, \sigma), LP_i(l_1, \sigma), q_2, l_2 \right) \\ \left(q_1, l_1, \delta^G(q_2, \sigma), LP_i(l_2, \sigma) \right) \\ \left(\delta^G(q_1, \sigma), LP_i(l_1, \sigma), \delta^G(q_2, \sigma), LP_i(l_2, \sigma) \right). \end{cases}$$

For $\sigma \in \Sigma_{uo} \setminus \Sigma_{fi}$

$$\delta^{V_{F_i I_i}}\left((q_1, l_1, q_2, l_2), \sigma \right) = \begin{cases} \left(\delta^G(q_1, \sigma), l_1, q_2, l_2 \right) \\ \left(q_1, l_1, \delta^G(q_2, \sigma), l_2 \right) \\ \left(\delta^G(q_1, \sigma), l_1, \delta^G(q_2, \sigma), l_2 \right). \end{cases}$$

For $\sigma \in \Sigma_o$

$$\delta^{V_{F_i I_i}}\left((q_1, l_1, q_2, L_2), \sigma \right) = \left(\delta^G(q_1, \sigma), LP_i(l_1, \sigma), \delta^G(q_2, \sigma), LP_i(l_2, \sigma) \right).$$

Intuitively, the previous nondeterministic transition rule tracks two strings in $\mathcal{L}(G)$ that look identical under the projection P_{Σ_o} while updating the failure information incorporating indicator events as these two strings evolve. We define the following terminology for further arguments.

Definition 5: $V_{F_iI_i}$ is called (F_i, I_i)-confused if there is a cycle $\langle v_1, v_2, \ldots, v_n \rangle_{V_{F_iI_i}}$ such that for all $v_i := (q_1^{v_i}, l_1^{v_i}, q_2^{v_i}, l_2^{v_i})$, $l_1^{v_i} = F_iI_i$, and $l_2^{v_i} = N$ or vice versa. We call this cycle an (F_i, I_i)-confused cycle. If there are no such cycles, we say that $V_{F_iI_i}$ is (F_i, I_i)-confusion-free.

We can prove the following set of analogous results regarding I-diagnosability with slight modifications of the corresponding results for diagnosability.

Theorem 4: $\mathcal{L}(G)$ is I-diagnosable w.r.t. Σ_o, Π_f on Σ_f and the indicator map I if and only if $V_{F_iI_i}$ is (F_i, I_i)-confusion free for all $i \in \Pi_f$.

Theorem 5: The I-diagnosability of $\mathcal{L}(G)$ with respect to Σ_o, Π_f on Σ_f and the indicator map I can be decided in $O(n_1^2 n_2 n_3)$.

IV. Conclusion

In this note, we presented polynomial-time algorithms for verifying diagnosability and I-diagnosability.

Acknowledgment

The authors would like to thank the reviewers for their comments and suggestions which helped to improve the presentation and readability of the note. They would also like to thank D. Teneketzis for useful discussions.

References

[1] M. Sampath, R. Sengupta, K. Sinnamohideen, S. Lafortune, and D. Teneketzis, "Diagnosability of discrete event systems," *IEEE Trans. Automat. Contr.*, vol. 40, pp. 1555–1575, Sept. 1995.

[2] S. Jiang, Z. Huang, V. Chandra, and R. Kumar, "A polynomial-time algorithm for diagnosability of discrete event systems," *IEEE Trans. Automat. Contr.*, vol. 46, pp. 1318–1321, Aug. 2001.

[3] J. N. Tsitsiklis, "On the control of discrete event dynamical systems," *Math. Control Sig. Syst.*, vol. 2, no. 2, pp. 95–107, 1989.

[4] K. Rudie and J. C. Willems, "The computational complexity of decentralized discrete-event control problems," *IEEE Trans. Automat. Contr.*, vol. 40, pp. 1313–1318, July 1995.

[5] T. Yoo and S. Lafortune, "A general architecture for decentralized supervisory control of discrete-event systems," *Discrete Event Dyn. Syst.: Theory Appl.*, vol. 12, no. 3, pp. 335–377, July 2002.

[6] C. G. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Norwell, MA: Kluwer, 1999.

[7] T. H. Cormen, C. E. Leiserson, and R. L. Rivest, *Introduction to Algorithms*. Cambridge, MA: MIT Press, 1990.

NP-Completeness of Sensor Selection Problems Arising in Partially Observed Discrete-Event Systems

Tae-Sic Yoo and Stéphane Lafortune

***Abstract*—We consider the three properties of diagnosability, normality, and observability of discrete-event systems. In each case, we consider the problem of finding an observable event set with minimum cardinality such that the property under consideration holds. We prove that these search problems are computationally hard by showing that the corresponding decision problems are NP-complete.**

***Index Terms*—Computational complexity, discrete-event systems, NP-completeness, sensor selection problems.**

I. Introduction

We consider the computational complexity of sensor set selection problems arising in monitoring and control of partially observed discrete-event systems. More specifically, we consider the properties of *diagnosability*, *observability*, and *normality* that have been characterized in the discrete-event systems literature; see, e.g., [1] and [2]. We are interested in finding observable event sets of minimum cardinality such that these properties hold.

The motivation of this problem is clear. Observations require sensors and sensors can be "costly." Therefore, any sensor that is redundant from the point of view of ensuring diagnosability (or observability, or normality) can be removed. (Of course, redundancy in sensors may still be desirable from the viewpoint of reliability. However, this issue is beyond the scope of this note). We note that there may be several incomparable observable event sets, each minimal with respect to set inclusion, such that a given property holds. Hence, we consider the problem of finding an observable event set *with minimum cardinality* such that a given property holds. The contribution of this note is to prove that these search problems are computationally hard for each of the three properties of interest by showing that their corresponding decision problems are NP-complete. Previous works that considered the problems of minimum-cardinality observable-event sets for the properties of observability and normality (see, e.g., [3]) proposed algorithms of exponential complexity. Our results show that this is to be expected since polynomial-time algorithms do not exist, in general (unless P = NP). One strategy for obtaining more efficient algorithms is to introduce further assumptions in the problem formulation. An example is the work in [4], where an efficient algorithm is presented for the sensor selection problem in the context of a probabilistic formulation of the problem and under specific probabilistic assumptions.

We assume basic knowledge of discrete-event systems and its common notations. The readers are directed to [1] for more complete introductory materials.

II. Preliminaries

We model the untimed discrete-event system as a deterministic finite-state automaton

$$G = \left(Q^G, \Sigma, \delta^G, q_0^G\right)$$

Manuscript received March 29, 2001. Recommended by Associate Editor R. S. Sreenivas. This work was supported in part by the National Science Foundation under Grant ECS-0080406 and Grant CCR-0082784, in part by the DDR&E MURI on Low Energy Electronics Design for Mobile Platforms, and managed by ARO under Grant ARO DAAH04-96-1-0377.

The authors are with the Department of Electrical Engineering and Computer Science, The University of Michigan, Ann Arbor, MI 48109-2122 USA (e-mail: tyoo@eecs.umich.edu; stephane@eecs.umich.edu).

Publisher Item Identifier 10.1109/TAC.2002.802762.