Automatica 48 (2012) 2068–2078

Contents lists available at SciVerse ScienceDirect

Automatica

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

automatica

A Journal of IFAC The International Federation of Automatic Control

Robust diagnosis of discrete event systems against intermittent loss of observations[☆]

Lilian K. Carvalho, João C. Basilio[1], Marcos V. Moreira

Universidade Federal do Rio de Janeiro, COPPE—Programa de Engenharia Elétrica, 21949-900, Rio de Janeiro, RJ, Brazil

ARTICLE INFO

Article history:
Received 25 July 2011
Received in revised form
29 March 2012
Accepted 13 April 2012
Available online 7 July 2012

Keywords:
Discrete event systems
Fault diagnosis
Robust diagnosability
Automaton

ABSTRACT

In the usual approaches to fault diagnosis of discrete event systems it is assumed that not only all sensors work properly but also all information reported by sensors always reaches the diagnoser. Any bad sensor operation or communication failure between sensors and the diagnoser can be regarded as loss of observations of events initially assumed as observable. In such situations, it may be possible that either the diagnoser stands still or report some wrong information regarding the fault occurrence. In this paper we assume that intermittent loss of observations may occur and we propose an automaton model based on a new language operation (language dilation) that takes it into account. We refer to this problem as robust diagnosability against intermittent loss of observations (or simply robust diagnosability, where the context allows). We present a necessary and sufficient condition for robust diagnosability in terms of the language generated by the original automaton and propose two tests for robust language diagnosability, one that deploys diagnosers and another one that uses verifiers. We also extend the results to robust codiagnosability against intermittent loss of observations.

1. Introduction

In practice fault diagnosis of discrete event systems is usually performed by a deterministic automaton called diagnoser, which is designed based on a model of the physical system assuming that not only all sensors work properly but also all information reported by sensors always reaches the diagnoser correctly (Contant, Lafortune, & Teneketzis, 2006; Debouk, Lafortune, & Teneketzis, 2000; Kumar & Takai, 2009; Lin, 1994; Qiu & Kumar, 2006; Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1995; Thorsley & Teneketzis, 2005; Tripakis, 2002; Wang, Yoo, & Lafortune, 2007; Zad, Kwong, & Wonham, 2003). However, bad sensor operation can make sensors fail to report event occurrences. In addition bad electrical linkage and possible atmospheric interference in the communication channels may lead to loss of communication between sensors and the diagnoser. In both cases, the diagnoser fails to observe some of the event occurrences. When loss of observations of events occurs, the diagnoser may get stuck at some state – either due to lack of observed events or to the occurrence of events that are not in the active event set of its current state – or even issue an incorrect diagnostic decision (Carvalho, Basilio, & Moreira, 2010). This suggests that some change has to be made on diagnosers to make them robust to loss of observations.

The problem of robust diagnosis has been recently of great interest (Athanasopoulou, Lingxi, & Hadjicostis, 2010; Basilio & Lafortune, 2009; Carvalho et al., 2010; Lima, Basilio, Lafortune, & Moreira, 2010; Takai, 2010). The notion of robust codiagnosability was introduced by Basilio and Lafortune (2009) who formulated and solved the robust codiagnosability problem, *i.e.*, when entire partial diagnosers may fail and cease to operate. In a different context, Athanasopoulou et al. (2010) developed a probabilistic methodology for failure diagnosis in finite state machines based on a sequence of unreliable observations. Lima et al. (2010) have considered the problem of robust diagnosability in the presence of permanent sensor failures, and used the redundancy that may exist in the set of diagnosis bases (Basilio, Lima, Lafortune, & Moreira, 2012) to design a robust diagnoser that is able to cope with permanent sensor failures of sets of events associated with redundant event sets, and Carvalho et al. (2010), in a preliminary version of this paper, have considered the problem of intermittent sensor failures. In a different problem formulation, Takai (2010) has proposed a test based on verifiers to ascertain whether or not the language generated by a discrete event system modeled with

[☆] The research work of João Carlos Basilio has been supported by the Brazilian Research Council (CNPq), grants 307939/2007-3 and 306592/2010-0. The research works of Lilian Kawakami Carvalho and Marcos Vicente Moreira have been supported by Carlos Chagas Foundation (FAPERJ). The material in this paper was partially presented at the 10th International Workshop on Discrete Event Systems (WODES'10), September 5–7, 2010, Berlin, Germany. This paper was recommended for publication in revised form by Associate Editor Bart De Schutter under the direction of Editor Ian R. Petersen.

E-mail addresses: lilian.carvalho@poli.ufrj.br (L.K. Carvalho), basilio@pee.ufrj.br (J.C. Basilio), moreira@dee.ufrj.br (M.V. Moreira).

[1] Tel.: +55 21 2562 8021; fax: +55 21 2562 8627.

0005-1098/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2012.06.042

a class of automata is diagnosable. In the context of supervisory control of DES, sensor failures have been considered in Rohloff (2005), where permanent sensor failure is assumed, *i.e.*, if a sensor fails it never recovers again.

In this paper we address the problem of fault diagnosis of discrete event systems modeled as automata in the presence of intermittent loss of observations. In practice, loss of observations may be due to sensor malfunctioning or communication failure between sensors and the diagnoser which can be caused by bad electrical linkage, defective components, circuit heating, measurement noise, data communication failure, *etc.* Sensor failures not only change the dynamical evolution of the system but also invalidate the model originally developed for language diagnosability. Communication failures in the channel that links the supervisor and the plant sensors may lead the supervisor to take wrong decisions regarding the events to be enabled and so, the dynamic behavior of the controlled plant may be different from the nominal, *i.e.*, the one used to design the diagnoser. Therefore, we will assume throughout this paper that all sensors subject to failure and all communication failures between sensors and the diagnoser do not interfere in both the supervisory control system and in the continuous variable controller for the plant.

This paper is structured as follows. In Section 2 we present a background material on discrete event systems that is necessary in the sections that follows. In Section 3 we first present models for sensor and communication channel failures and their implications in the modeling of discrete event systems, and, in the sequel, we present an automaton model for discrete event systems subject to intermittent loss of observations. In Section 4 we present the definition of robust diagnosability against intermittent loss of observations. In Section 5, we initially present a necessary and sufficient condition for robust diagnosability expressed in terms of diagnosers, and introduce the so-called "robust diagnoser", *i.e.*, a diagnoser that is able to cope with intermittent loss of observations; in the sequel, we propose two different ways to build robust diagnosers: one starting from the automaton model of the plant and another one starting from the diagnoser originally developed for testing the language diagnosability of the system. To complete Section 5, we extend the results to robust codiagnosability against intermittent loss of observations. In Section 6 we consider the use of verifiers in the analysis of robust diagnosability and codiagnosability against intermittent loss of observations. Finally, in Section 7, we list the main contributions of the paper and outline some possible future works.

2. Preliminaries

2.1. Definitions and notation

Let $G = (X, \Sigma, f, \Gamma, x_0)$ denote a deterministic finite state automaton, where X is the finite set of states, Σ is the finite set of events, $f : X \times \Sigma \rightarrow X$ is the transition function, partially defined in its domain, $\Gamma : X \rightarrow 2^{\Sigma}$ is the active event set, and x_0 is the initial state. Assume that Σ is partitioned as $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$, where Σ_o and Σ_{uo} denote, respectively, the sets of observable and unobservable events. Let L denote the language generated by automaton G, *i.e.*, $\mathscr{L}(G) = L$, and $L/s = \{t \in \Sigma^* : st \in L\}$ the post-language of L after a trace $s \in L$, where Σ^* denotes the Kleene closure of Σ, and $L(G, x)$ the set of all traces that originate in state x of G. Let s denote a trace of L. Then, throughout the text, (i) s_f denotes the last event of s; (ii) $\bar{s}$ denotes the prefix-closure of s, *i.e.*, the set of all traces that are prefixes of s; (iii) $\|s\|$ denotes the length of s.

The language projection P_o is defined in the usual manner (Ramadge & Wonham, 1989), as $P_o : \Sigma^* \rightarrow \Sigma_o^*$ with the following properties: (i) $P_o(\epsilon) = \epsilon$; (ii) $P_o(\sigma) = \sigma$ if $\sigma \in \Sigma_o$; (iii) $P_o(\sigma) = \epsilon$, if $\sigma \in \Sigma_{uo}$; (iv) $P_o(s\sigma) = P_o(s)P_o(\sigma)$, for $s \in \Sigma^*$ and $\sigma \in \Sigma$, where ϵ denotes the empty trace. The inverse projection operator P_o^{-1} is defined as $P_o^{-1}(t) = \{s \in \Sigma^* : P_o(s) = t\}$. Both the projection and inverse projection operations can be extended to languages in a straightforward way by applying $P_o(s)$ and $P_o^{-1}(s)$ to all $s \in L$.

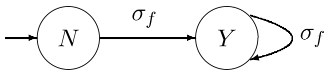


Fig. 1. Faulty label automaton A_ℓ.

Let $G_1 = (X_1, \Sigma_1, \Gamma_1, f_1, x_{0,1})$ and $G_2 = (X_2, \Sigma_2, \Gamma_2, f_2, x_{0,2})$. The synchronous or parallel composition of G_1 and G_2, denoted by $G_1 \| G_2$, is defined as $G_1 \| G_2 = Ac(X_1 \times X_2, \Sigma_1 \cup \Sigma_2, f_{1\|2}, (x_{0,1}, x_{0,2}))$, where $f_{1\|2}((x_1, x_2), \sigma) = (f_1(x_1, \sigma), f_2(x_2, \sigma))$, if $\sigma \in \Gamma_1(x_1) \cap \Gamma_2(x_2)$, $f_{1\|2}((x_1, x_2), \sigma) = (f_1(x_1, \sigma), x_2)$ if $\sigma \in \Gamma_1(x_1) \setminus \Sigma_2$, $f_{1\|2}((x_1, x_2), \sigma) = (x_1, f_2(x_2, \sigma))$, if $\sigma \in \Gamma_2(x_2) \setminus \Sigma_1$, and, undefined, otherwise. In the definition of $G_1 \| G_2$, $Ac(\cdot)$ denotes the accessible part of the automaton, *i.e.*, the operation that eliminates all states that are not reachable from the initial state and their related transitions. Finally, $Obs(G, \Sigma_o)$ denotes the observer automaton of G with respect to Σ_o, *i.e.*, assuming Σ_o as the set of observable events.[2]

2.2. Fault diagnosis of discrete event systems

Let $\Sigma_f \subseteq \Sigma_{uo}$ denote the set of fault events, and assume, for the sake of simplicity, that there is only one fault event, *i.e.*, $\Sigma_f = \{\sigma_f\}$. In addition, let $\Psi(\Sigma_f) = \{s \in L : s_f \in \Sigma_f\}$ denote the set of all finite traces of L that end with the fault event σ_f. With some abuse of notation, $\Sigma_f \in s$ denotes that $\bar{s} \cap \Psi(\Sigma_f) \neq \emptyset$. We make the following usual assumptions:

A1. L is live, *i.e.*, $\Gamma(x_i) \neq \emptyset$ for all $x_i \in X$;
A2. G has no cycle of unobservable events.

The language L is said to be diagnosable if the occurrence of σ_f can be detected within a finite number of transitions after its occurrence using only traces formed with events in Σ_o. Formally, language diagnosability is defined as follows (Sampath et al., 1995).

Definition 1. A prefix-closed and live language L is diagnosable with respect to projection P_o and $\Sigma_f = \{\sigma_f\}$ if the following holds true:

$$(\exists n \in \mathbb{N})(\forall s \in \Psi(\Sigma_f))(\forall t \in L/s)(\|t\| \geq n \Rightarrow D),$$

where the diagnosability condition D is

$$(\nexists \omega \in L)[(P_o(st) = P_o(\omega)) \wedge (\Sigma_f \notin \omega)]. \tag{1}$$

One way to verify language diagnosability of DES is by means of diagnosers (Sampath et al., 1995). Diagnosers are deterministic automata whose event set is formed with the observable events of G, and their states have labels Y and N attached to the states of G to indicate whether event σ_f has occurred or not. Formally, the diagnoser automaton G_d is defined as

$$G_d = (X_d, \Sigma_o, f_d, \Gamma_d, x_{0,d}) = Obs\,(G \| A_\ell, \Sigma_o), \tag{2}$$

where A_ℓ is the two state label automaton shown in Fig. 1.

A state $x_d \in X_d$ is called certain (or faulty), if $\ell = Y$ for all $(x, \ell) \in x_d$, and normal (or non-faulty) if $\ell = N$ for all $(x, \ell) \in x_d$. If there exist $(x, \ell), (y, \tilde{\ell}) \in x_d$, x not necessarily distinct from y such that $\ell = Y$ and $\tilde{\ell} = N$, then x_d is called an uncertain state of G_d. When the diagnoser is in a certain (normal) state, it is certain that

[2] For a detailed definition of observer, the reader is referred to Cassandras and Lafortune (2008, p. 102).

a fault has (resp. has not) occurred. However, if the diagnoser is in an uncertain state, it is not sure if the fault event has occurred or not. If there is a cycle[3] formed with uncertain states where the diagnoser can remain forever, then it will never be able to diagnose the fault occurrence; on the other hand if somehow it always leaves this cycle of uncertain states, then this cycle is not indeterminate. Therefore, it is important to distinguish between cycles of uncertain states that are indeterminate (in the sense that the diagnoser is not able to determine if the fault has occurred) and those cycles of uncertain states that are not indeterminate. This requires, besides the analysis of cycles formed with states of G_d, the search for cycles in G, as shown in the following definition.

Definition 2 (Sampath et al., 1995, *Indeterminate Cycles of* G_d**).** A set of uncertain states $\{x_{d_1}, x_{d_2}, \ldots, x_{d_p}\} \subset X_d$ forms an indeterminate cycle if the following conditions hold true:

(IC.1) $x_{d_1}, x_{d_2}, \ldots, x_{d_p}$ form a cycle in G_d;

(IC.2) $\exists (x_l^{k_l}, Y), (\tilde{x}_l^{r_l}, N) \in x_{d_l}$, $x_l^{k_l}$ not necessarily distinct from $\tilde{x}_l^{r_l}$, $l = 1, 2, \ldots, p$, $k_l = 1, 2, \ldots, m_l$, and $r_l = 1, 2, \ldots, \tilde{m}_l$ in such a way that the sequence of states $\{x_l^{k_l}\}$, $l = 1, 2, \ldots, p$, $k_l = 1, 2, \ldots, m_l$ and $\{\tilde{x}_l^{r_l}\}$, $l = 1, 2, \ldots, p$, $r_l = 1, 2, \ldots, \tilde{m}_l$ form cycles in G;

(IC.3) there exist $s = s_1 s_2 \cdots s_p \in \Sigma^*$ and $\tilde{s} = \tilde{s}_1 \tilde{s}_2 \cdots \tilde{s}_p \in \Sigma^*$ such that $P_o(s) = P_o(\tilde{s}) \neq \epsilon$, where $s_l = \sigma_{l,1}\sigma_{l,2} \cdots \sigma_{l,m_l-1}$, $f(x_l^j, \sigma_{l,j}) = x_l^{j+1}, j = 1, 2, \ldots, m_l - 1, f(x_l^{m_l}, \sigma_{l+1,0}) = x_{l+1}^1$, and $f(x_p^{m_p}, \sigma_{1,0}) = x_1^1$, and similarly for $\tilde{s}_l$.

Remark 1. For reasons that will become clear in the sequel, indeterminate cycles defined according to Definition 2 will be referred to as indeterminate observed cycle.

Using the definition of indeterminate observed cycles of G_d together with Definition 1, a necessary and sufficient condition for language diagnosability can be stated, as follows (Sampath et al., 1995).

Theorem 1. *Under Assumptions* A1 *and* A2*, language* L *generated by automaton* G *is diagnosable with respect to projection* P_o *and* $\Sigma_f = \{\sigma_f\}$ *if, and only if, its diagnoser* G_d *has no indeterminate observed cycles.* □

3. Modeling the observed behavior of an automaton in the presence of intermittent loss of observations

3.1. A motivating example

Fig. 2(a) and (b) show the state transition diagrams of an automaton G, for which $\Sigma = \{a, b, c, d, e, \sigma_f\}$, $\Sigma_o = \{a, b, c, d, e\}$ and $\Sigma_f = \{\sigma_f\}$, and the corresponding diagnoser G_d, respectively. It is immediate to see, according to Theorem 1, that, since G_d has no indeterminate cycles, the language generated by G is diagnosable with respect to P_o and Σ_f.

Assume, initially, that, for some $n \in \mathbb{N}$, the trace $s'_Y = c\sigma_f abd^n$ has been generated and suppose that the occurrence of event c has not been recorded somehow. Since event c has become unobservable, the first event occurrence to be recognized by G_d is a, which takes the diagnoser state to $\{5N\}$. When the next events of s'_Y occur, the diagnoser moves to state $\{6N\}$, where it stays as long as event d continues to occur, therefore displaying wrong information regarding the occurrence of σ_f. Assume, now, that, for some $n \in \mathbb{N}$, trace $s''_Y = c\sigma_f ce^n$ has been generated and assume also that event c is subject to intermittent loss of observations. If the first occurrence of event c is not recognized by the diagnoser, then G_d remains in its initial state. If, in the sequel, the communication between the system and the diagnoser is somehow restored before the second occurrence of event c, then when c occurs for the second time, the diagnoser moves to state $\{2N, 3Y\}$. Notice that since the next event of s''_Y to occur is e, which is not in the active event set of $\{2N, 3Y\}$, the diagnoser stands still in an uncertain state, and, once again, provides wrong information regarding the fault occurrence. This anomalous behavior suggests that the system model should be modified to take into account intermittent loss of observations due to sensor malfunction or communication failure between sensors and the diagnoser.

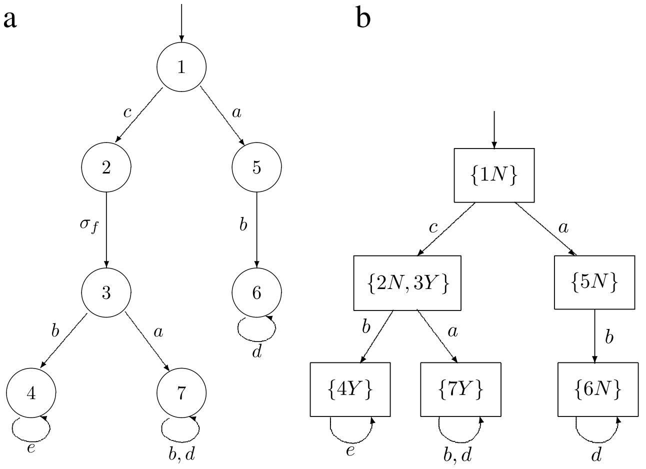


Fig. 2. Automaton G (a) and its corresponding diagnoser G_d (b).

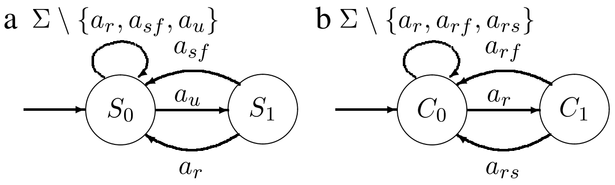

a $\Sigma \setminus \{a_r, a_{sf}, a_u\}$
a_{sf}
S_0
a_u
S_1
a_r
b $\Sigma \setminus \{a_r, a_{rf}, a_{rs}\}$
a_{rf}
C_0
a_r
C_1
a_{rs}

Fig. 3. Automata G_s and G_{cc} that model, respectively, intermittent sensor failure (a), and intermittent communication failure (b).

3.2. Modeling of sensor and communication channel intermittent failures

We now present automaton models for sensors and communication channels taking into account possible sensor malfunction and communication failure between the sensor and the diagnoser.

Fig. 3(a) shows automaton G_s that models sensor behavior under intermittent malfunction, where a_u denotes the system event whose occurrence must be recorded by the sensor, a_r denotes the event corresponding to the electrical signal generated by the sensor that records the occurrence of a_u, and a_{sf} is an event that models the failure of the sensor in recording a_u. We assume that a_u is an unobservable event, and it is clear that a_{sf} models an unobservable event. Fig. 3(b) shows automaton G_{cc} that models the dynamic behavior of communication channels taking into account possible communication failures, where a_{rs} is an observable event that models the successful transmission of the electrical signal generated by the sensor and a_{rf} is an unobservable event that models the unsuccessful transmission of event a_r to the diagnoser through the communication channel. The self-loops in states S_0 and C_0, in Fig. 3(a) and (b), respectively, were added to represent an

[3] A set of states $\{x_1, x_2, \ldots, x_n\} \subseteq X$ forms a cycle in an automaton G if there exists a trace $s = \sigma_1\sigma_2 \cdots \sigma_n \in L(G, x_1)$ such that $f(x_l, \sigma_l) = x_{l+1}$, $l = 1, \ldots, n-1$, and $f(x_n, \sigma_n) = x_1$.

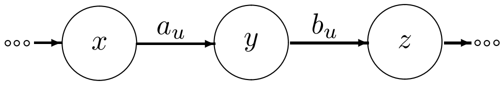


Fig. 4. Part of a system plant G.

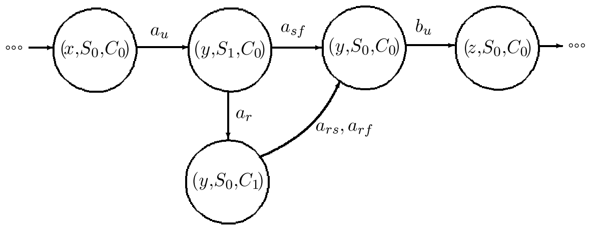


Fig. 5. Automaton $G_p = G\|G_s\|G_{cc}$.

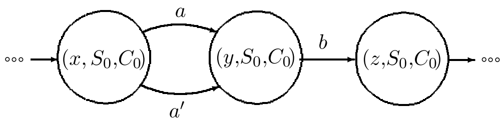


Fig. 6. A simplified automaton model.

immediate sensor response to the occurrence of event a_u and an immediate transmission to the diagnoser in the communication channel of event a_r. In both automata, Σ denotes the set of all events of the system, including the events of G_s and G_{cc}. The overall behavior of the system under intermittent loss of observations is obtained by performing the parallel composition $G_p = G\|G_s\|G_{cc}$.

Consider part of an automaton G represented in Fig. 4, where a_u is an unobservable event whose occurrence must be recorded by the sensor. The corresponding automaton $G_p = G\|G_s\|G_{cc}$ is shown in Fig. 5. Notice that trace $a_u a_r a_{rs}$ means that the occurrence of event a_u has been successfully reported to the diagnoser whereas the other two traces, $a_u a_{sf}$ and $a_u a_r a_{rf}$, model sensor and communication failures, respectively, since their last events are a_{sf} and a_{rf}; trace $a_u a_{sf}$ models the sensor failure in recording the occurrence of event a_u and trace $a_u a_r a_{rf}$ shows that event a_u was at first recorded by the sensor but due to some communication problem did not reach the diagnoser. As a consequence, we can replace the transitions that connect states (x, S_0, C_0) and (y, S_0, C_0) with two transitions, one labeled with an observable event a, that corresponds to the execution of the normal trace $a_u a_r a_{rs}$, and the other one labeled with unobservable event a', corresponding to traces $a_u a_r a_{rf}$ and $a_u a_{sf}$, as depicted in Fig. 6.

3.3. The language dilation operation

The diagnosability problems resulting from the loss of observations of event c in the motivating example of Section 3.1 can be explained with the help of the modeling of sensors and communication channels subject to intermittent failure as follows. Let us partition Σ_o as $\Sigma_o = \Sigma_{ilo}\dot{\cup}\Sigma_{nilo}$, where Σ_{ilo} is the subset of Σ_o whose events are associated with intermittent loss of observations and Σ_{nilo} is the set of events that are always observable. Assuming, initially, that $\Sigma_{ilo} = \emptyset$, then $L = \overline{L_G}$ where $L_G = \{ab\}\{d\}^* \cup \{c\sigma_f\}(\{c\}\{e\}^* \cup \{a\}\{b, d\}^*)$. On the other hand, when $\Sigma_{ilo} = \{c\}$, and defining $\Sigma'_{ilo} = \{c'\}$, where c' is an unobservable event that models the loss of observations of event c due to sensor malfunction or communication failure, the language that models the behavior of G subject to intermittent loss of observations of c is no longer L but $L_{dil} = \overline{L_{G,dil}}$, with $L_{G,dil} = \{ab\}\{d\}^* \cup \{c, c'\}\{\sigma_f\}(\{c, c'\}\{e\}^* \cup \{a\}\{b, d\}^*)$. The state transition diagram of an automaton that generates L_{dil} is shown in Fig. 7.

From the preceding discussion, it is clear that language diagnosability in the presence of intermittent loss of observations should not be stated in terms of the generated language L but in terms of language L_{dil}. As a consequence, it is necessary to obtain an automaton G_{dil} whose generated language not only accounts for the normal behavior of G, *i.e.*, when there is no loss of observations, but also for the influence of intermittent loss of observations on L. Such a language is obtained by dilating L, as follows.

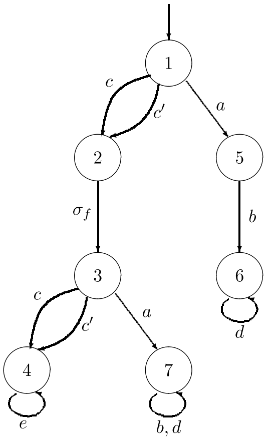


Fig. 7. Automaton G_{dil}.

Definition 3 (*Dilation*). Let $\Sigma = \Sigma_{ilo}\dot{\cup}\Sigma_{nilo}\dot{\cup}\Sigma_{uo}$ be a partition of Σ, where Σ_{ilo} is the set of observable events associated with intermittent loss of observations and Σ_{nilo} denotes the set of observable events not subject to intermittent loss of observations and let $\Sigma'_{ilo} = \{\sigma' : \sigma \in \Sigma_{ilo}\}$ and $\Sigma_{dil} = \Sigma \cup \Sigma'_{ilo}$. The dilation D is the mapping

$$\begin{aligned} D : \Sigma^* &\to 2^{(\Sigma_{dil})^*} \\ s &\mapsto D(s), \end{aligned} \tag{3}$$

where

$$\begin{aligned} D(\epsilon) &= \{\epsilon\}, \\ D(\sigma) &= \begin{cases} \{\sigma\}, & \text{if } \sigma \in \Sigma \setminus \Sigma_{ilo}, \\ \{\sigma, \sigma'\}, & \text{if } \sigma \in \Sigma_{ilo}, \end{cases} \\ D(s\sigma) &= D(s)D(\sigma), \quad s \in \Sigma^*, \sigma \in \Sigma. \end{aligned} \tag{4}$$

The dilation operation D can be extended from traces to languages by applying it to all sequences in the language, that is,

$$D(L) = \bigcup_{s \in L} D(s). \tag{5}$$

Example 1. In order to illustrate the dilation operation, let us assume that $\Sigma = \{a, b, c, d, e, \sigma_f\}$ and $\Sigma_{ilo} = \{c\}$ and consider language $L_G = \{ab\}\{d\}^* \cup \{c\sigma_f\}(\{c\}\{e\}^* \cup \{a\}\{b, d\}^*)$, whose prefix-closure is the language generated by automaton G of Fig. 2(a). Therefore $\Sigma_{dil} = \{a, b, c, c', d, e, \sigma_f\}$.

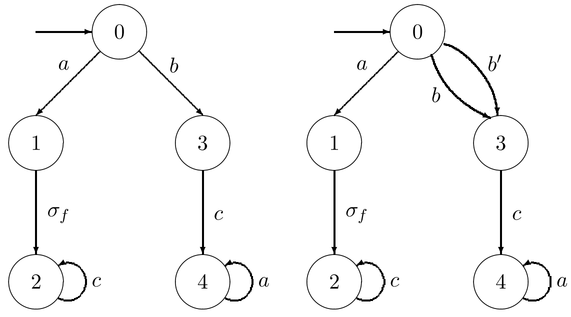
Let us, initially, illustrate the application of dilation to traces. For $s_1 = abd$ then $D(s_1) = \{abd\}$ since $a, b, d \notin \Sigma_{ilo}$. For trace $s_2 = c\sigma_f ce$ then, according to Definition 3, $D(s_2) = \{c, c'\}\{\sigma_f\}\{c, c'\}\{e\}$ $= \{c\sigma_f ce, c\sigma_f c'e, c'\sigma_f ce, c'\sigma_f c'e\}$.

Let us now apply the dilation to L_G. Then, it is not difficult to check that $D(L_G) = L_{G,dil}$, whose prefix-closure is the language generated by automaton G_{dil} of Fig. 7.

With the help of Definition 3, we can now formally define automaton G_{dil} that models the behavior of G when subject to intermittent loss of observations, as follows:

$$G_{dil} = (X, \Sigma_{dil}, f_{dil}, \Gamma_{dil}, x_0), \tag{6}$$

where $\Gamma_{dil}(x) = D[\Gamma(x)]$, and f_{dil} is defined as follows: $\forall \sigma_{dil} \in \Gamma_{dil}(x) : \sigma_{dil} \in D(\sigma), f_{dil}(x, \sigma_{dil}) = f(x, \sigma)$, where $\sigma \in \Gamma(x)$.



(a) Automaton G_1.

(b) Automaton $G_{1,dil}$.

Fig. 8. Automata G_1 and $G_{1,dil}$ of Example 2.

Remark 2. Notice that automaton G_{dil} is formed by adding to G transitions in parallel with the transitions associated with the events that are subject to intermittent loss of observations. The added transitions will be labeled with unobservable events and therefore the observable event set of G_{dil} remains Σ_o as in G. It is also important to remark that G_{dil} is a deterministic automaton with unobservable events as G.

The following result shows that G_{dil} models the behavior of G when subject to intermittent loss of observations by establishing a relationship between the languages generated by G and G_{dil}.

Theorem 2. *Let G_{dil} be a deterministic automaton obtained from G according to (6). Then, $L_{dil} = \mathscr{L}(G_{dil}) = D(L)$.*

Proof. The proof is by induction.

- The base case is for traces of length 0. Note, by definition, that $\epsilon \in L_{dil}$, and, since $\epsilon \in L$ and $D(\epsilon) = \{\epsilon\}$, then $\epsilon \in D(L)$.
- The induction hypothesis is that $\forall s_N : \|s_N\| \leq N, s_N \in L_{dil}, \Leftrightarrow s_N \in D(L) \Leftrightarrow \exists s'_N \in L, \|s'_N\| \leq N : s_N \in D(s'_N)$.
- Let $s_{N+1} = s_N \sigma_d$.

(1) Assume first that $s_{N+1} = s_N\sigma_d \in L_{dil}$. Therefore, $\sigma_d \in \Sigma_{dil}$ and so, $\sigma_d \in D(\sigma)$ for some $\sigma \in \Sigma$, which implies that either $\sigma_d = \sigma$ or $\sigma_d = \sigma'$. According to the induction hypothesis, there exists $s'_N \in L$ such that $s_N \in D(s'_N)$. As a consequence, there exist $s'_N\sigma \in L$ such that $s_N\sigma_d \in D(s'_N\sigma) \subseteq D(L)$, which ultimately implies that $s_{N+1} \in D(L)$.

(2) Assume now that $s_{N+1} = s_N\sigma_d \in D(L)$. From the induction hypothesis, there exists $s'_N \in L$ such that $s_N \in D(s'_N)$ and since $\sigma_d \in \Sigma_{dil}$ then there exists $\sigma \in \Sigma$ such that $\sigma_d \in D(\sigma)$. Therefore,

$$\begin{aligned} D(s'_N\sigma) &= D(s'_N)D(\sigma) \supset \{s_N\}D(\sigma) \\ &= \begin{cases} \{s_N\sigma\}, & \sigma \notin \Sigma_{ilo} \\ \{s_N\sigma, s_N\sigma'\}, & \sigma \in \Sigma_{ilo}, \end{cases} \end{aligned}$$

which implies, by the construction of G_{dil}, that $s_{N+1} = s_N\sigma_d \in L_{dil}$. □

4. Robust diagnosability of DES against intermittent loss of observations

The definition of language diagnosability by Sampath et al. (1995) is expressed in terms of the observed language generated by G. However, as we saw in the previous section, although the language generated by an automaton subject to intermittent loss of observations remains unchanged, the observed language dilates. This leads to the definition of language robust diagnosability, as follows.

Definition 4 (*Robust Diagnosability of DES Subject to Intermittent Loss of Observations*)**.** A prefix-closed and live language L, generated by an automaton G, is robustly diagnosable with respect to dilation D, projection $P_{dil,o} : \Sigma^*_{dil} \to \Sigma^*_o$ and $\Sigma_f = \{\sigma_f\}$ if the following holds true:

$$(\exists n \in \mathbb{N})(\forall s \in \Psi(\Sigma_f))(\forall t \in L/s)(\|t\| \geq n \Rightarrow R_D),$$

where the robust diagnosability condition R_D is

$$(\nexists \omega \in L)[(P_{dil,o}(D(st)) = P_{dil,o}(D(\omega))) \wedge (\Sigma_f \notin \omega)]. \tag{7}$$

Remark 3. Note that if $\Sigma_{ilo} = \emptyset$ then $L_{dil} = L$, $D(st) = \{st\}$ and $P_{dil,o}$ reduces to P_o. In this case, Definition 4 reduces to the usual definition of language diagnosability introduced by Sampath et al. (1995).

The following example illustrates the definition of robust diagnosability.

Example 2. Consider automata G_1 and G_2 whose state transition diagrams are depicted in Figs. 8(a) and 9(a), respectively, and assume, for both automata, that $\Sigma_o = \{a, b, c\}$, $\Sigma_{ilo} = \{b\}$ and $\Sigma_f = \{\sigma_f\}$. The objective here is to verify if the languages generated by G_1 and G_2 (L_1 and L_2, respectively) are robustly diagnosable with respect to D, P_o and $\Sigma_f = \{\sigma_f\}$.

Consider, initially, automaton G_1. From Fig. 8(a), we see that the faulty traces of L_1 are $s'_Y = a\sigma_f c^n$, $n \in \mathbb{N}$. Following the steps in the robust diagnosability condition R_D given in Eq. (7), we obtain:

$$D(s'_Y) = \{a\sigma_f c^n\} \Rightarrow P_{dil,o}\left[D(s'_Y)\right] = \{ac^n\}.$$

Let $L_{1,dil}$ denote the language generated by automaton $G_{1,dil}$, shown in Fig. 8(b). It is not difficult to see that, since

$$L_{1,dil} = \overline{\{a\sigma_f\}\{c\}^* \cup \{bc\}\{a\}^* \cup \{b'c\}\{a\}^*},$$

then

$$P^{-1}_{dil,o}\left\{P_{dil,o}\left[D(s'_Y)\right]\right\} \cap L_{1,dil} = \{a\sigma_f c^n\}.$$

Therefore, since $P^{-1}_{dil,o}\left\{P_{dil,o}\left[D(s_Y)\right]\right\} \cap L_{1,dil}$ has only the fault traces s'_Y, we may conclude that L_1 is robustly diagnosable with respect to D, P_o and $\Sigma_f = \{\sigma_f\}$.

Consider, now, automaton G_2 depicted in Fig. 9(a). In this case, the unique faulty traces of L_2 are $s''_Y = \sigma_f abc^n$, $n \in \mathbb{N}$. Following the robust diagnosability condition R_D, we have

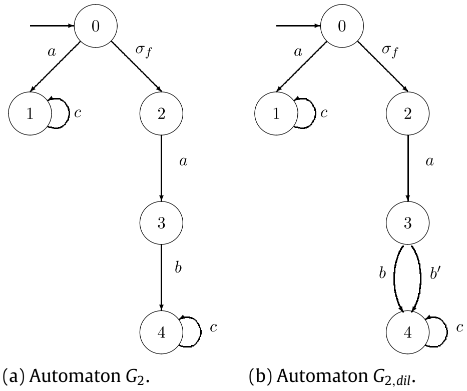
$$D(s''_Y) = \{\sigma_f abc^n, \sigma_f ab'c^n\} \Rightarrow P_{dil,o}\left[D(s''_Y)\right] = \{abc^n, ac^n\}.$$

From automaton $G_{2,dil}$, shown in Fig. 9(b), we obtain

$$L_{2_{dil}} = \overline{\{a\}\{c\}^* \cup \{\sigma_f ab\}\{c\}^* \cup \{\sigma_f ab'\}\{c\}^*}.$$

Therefore:

$$P^{-1}_{dil,o}\left\{P_{dil,o}\left[D(s''_Y)\right]\right\} \cap L_{2,dil} = \{\sigma_f abc^n, \sigma_f ab'c^n, ac^n\}.$$



(a) Automaton G_2. (b) Automaton $G_{2,dil}$.

Fig. 9. Automata G_2 and $G_{1,dil}$ of Example 2.

Since there is a normal trace in $P^{-1}_{dil,o}\left\{P_{dil,o}\left[D(s''_Y)\right]\right\}\cap L_{2,dil}$, we may conclude that L_2 is not robustly diagnosable with respect to D, P_o and $\Sigma_f=\{\sigma_f\}$. The lack of robust diagnosability of L_2 with respect to D, P_o and $\Sigma_f=\{\sigma_f\}$ can be explained as follows: it is not possible to assure if the normal traces ac^n occurred or the faulty traces $s''_Y=\sigma_f abc^n$ have occurred and, somehow, the observable event b has not been recorded by the diagnoser.

5. Verification of robust diagnosability using diagnosers

The robust diagnosability condition R_D, given in Eq. (7), replaces G, L and P_o with G_{dil}, $L_{dil}=D(L)$ and $P_{dil,o}$, respectively. Therefore, the reader could argue that in order to verify robust diagnosability with respect to D, $P_{dil,o}$ and Σ_f it is enough to apply Theorem 1 to G_{dil}. We show now that this is not as straightforward as it appears to be. This is so because Assumption A2 prevents G from having cycles of unobservable events. In order to illustrate this point, assume, for example, that σ is the unique observable event of a cycle of G that prevents G from having unobservable cycles. In addition, assume that event σ is subject to intermittent loss of observations. Therefore G_{dil} formed from G does not satisfy Assumption A2 since there will be a cycle in G_{dil} of unobservable events when the transition labeled with σ' is added in parallel to the one labeled with σ. Therefore, in this case Theorem 1 cannot be used to verify if L_{dil} is diagnosable with respect to $P_{dil,o}$. It is therefore necessary to remove Assumption A2 and, as a consequence, to derive a new necessary and sufficient condition for language diagnosability. In order to do so, consider, initially, the following definition.

Definition 5 (*Hidden Cycles and Indeterminate Hidden Cycles of G_d*). Let $x_d=\{x_1\ell_1, x_2\ell_2,\ldots,x_n\ell_n\}$ be a state of G_d. There exists a hidden cycle in x_d if for some $\{i_1,i_2,\ldots,i_k\}\subseteq\{1,2,\ldots,n\}$, the following conditions hold true:

(HC.1) $x_{i_1},x_{i_2},\ldots,x_{i_k}$ form a cycle in G;
(HC.2) $\{\sigma_{i_1},\sigma_{i_2},\ldots,\sigma_{i_k}\}\subseteq\Sigma_{uo}$, where $\sigma_{i_1},\sigma_{i_2},\ldots,\sigma_{i_k}$ are such that $f(x_{i_j},\sigma_{i_j})=x_{i_{j+1}}, j=1,2,\ldots,k-1$, and $f(x_{i_k},\sigma_{i_k})=x_{i_1}$.

If x_d is an uncertain state of G_d and besides conditions (HC.1) and (HC.2), the following condition is also satisfied,

(HC.3) $\ell_{i_j}=Y, j=1,2,\ldots,k$,

then x_d has an indeterminate hidden cycle.

The idea behind the definitions of hidden cycles and indeterminate hidden cycles is as follows. Notice that Assumptions (HC.1) and (HC.2) ensure that $x_{i_1},x_{i_2},\ldots,x_{i_k}$ form a cycle of states connected with unobservable events. Let us now consider a trace $s=s_o(\sigma_{i_1},\sigma_{i_2},\ldots,\sigma_{i_k})^n\in L\ (n\in\mathbb{N})$, and, without loss of generality, assume that the last event of s_o is observable. Let us suppose, initially, that $\sigma_f\notin s$ and that there is no faulty trace[4] s' such that $P_o(s)=P_o(s')$. In this case there will exist in G_d a state x_d^N such that $\{x_{i_1}N,x_{i_2}N,\ldots,x_{i_k}N\}\subseteq x_d^N$. Assume now that $\sigma_f\in s_o$ and $f_\ell(x_{0,\ell},s_o)=x_\ell^Y$, where f_ℓ is the transition function of $G_\ell=G\|A_\ell$ and $x_{0,\ell}$ and x_ℓ^Y are, respectively, the initial and a certain state of G_ℓ. In addition, assume that there is no normal traces s'' such that $P_o(s)=P_o(s'')$. Therefore, there will exist a certain state x_d^Y of G_d such that $(x_\ell^Y\cup\{x_{i_1}Y,x_{i_2}Y,\ldots,x_{i_k}Y\})\subseteq x_d^Y$. On the other hand, if there exists a normal trace s'' (bounded length or not) such that $f_\ell(x_{0,\ell},s_o)=x_\ell^N$, where x_ℓ^N is a normal state of G_ℓ, and $P_o(s)=P_o(s'')$, then there will exist an uncertain state x_d^{YN} in G_d such that $(x_\ell^Y\cup\{x_{i_1}Y,x_{i_2}Y,\ldots,x_{i_k}Y\}\cup x_\ell^N)\subseteq x_d^{YN}$. Consequently, in accordance with Definition 5, there exist hidden cycles in states x_d^N and x_d^Y of G_d and an indeterminate hidden cycle in x_d^{YN}. Notice that in the verification of language diagnosability, state x_d^Y (x_d^N) ensures that the fault has (resp. has not) occurred, and so, the existence of hidden cycles in normal or certain states of G_d does not affect the language diagnosability. On the other hand, the existence of indeterminate hidden cycles implies that the language is not diagnosable since there exist two traces, a faulty one, s, and a normal one, s'', such that $P_o(s)=P_o(s'')$. This is why hidden cycles formed with states of G that are labeled with Y in some uncertain state of G_d are termed indeterminate hidden cycles.

Hidden cycles are represented in the state transition diagrams of diagnosers by dashed self-loops: indeterminate hidden cycles are labeled as *ihc(.)* and hidden cycles are labeled simply as *hc(.)*, with the unobservable events that connect the states in the hidden cycles put inside the parentheses.

An immediate consequence of Definition 5 is that none of the assumptions made in Sampath et al. (1995) are required. This is so because of the following reasons.

(1) As we will show in the sequel, the language diagnosability condition can be expressed in terms of indeterminate hidden cycles, therefore allowing us to remove Assumption A2.
(2) With the definition of hidden and indeterminate hidden cycles, we can also remove Assumption A1 as follows: if for some state y of G, $\Gamma(y)=\emptyset$, then we replace G with a new automaton $G'=(X,\Sigma',f',\Gamma',x_0)$, where $\Sigma'=\Sigma\cup\{\sigma_u\}$, σ_u being an unobservable event, $f'(x,.)=f(x,.)$, for all $x\neq y$ and $f'(y,\sigma_u)=y$. Notice that the languages generated by G and G' have the same projection P_o, which does not change the diagnosability property of L. The consequence of this procedure is that a hidden cycle labeled with event σ_u will be formed in some state of G_d.

[4] A trace s is said to be faulty (normal) if $\sigma_f\in s$ (resp. $\sigma_f\notin s$).

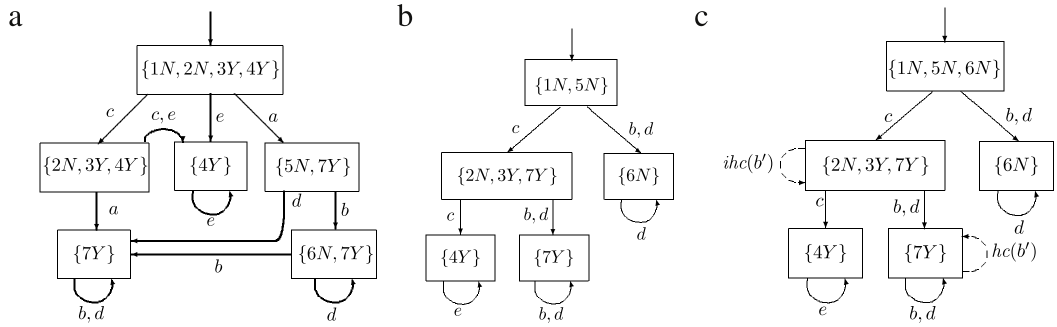


Fig. 10. Diagnosers for automaton G of Fig. 2 assuming $\Sigma_{ilo} = \{c\}$ (a), $\Sigma_{uo} = \{a, \sigma_f\}$ and $\Sigma_{ilo} = \{b\}$ (b), and $\Sigma_{uo} = \{a, \sigma_f\}$ and $\Sigma_{ilo} = \{b\}$ (c).

Therefore, from this point onwards, Assumptions A1 and A2 are no longer needed.

5.1. A robust diagnoser for DES subject to intermittent loss of observations

We will now present a necessary and sufficient condition for robust diagnosability of a DES subject to intermittent loss of observations. Since G_{dil} models the behavior of G in the presence of intermittent loss of observations, we will consider a diagnoser associated with G_{dil} instead of the usual diagnoser G_d for G.

Let us consider the following diagnoser automaton:

$$G_{dil,d} = Obs\,(G_{dil} \| A_\ell, \Sigma_o), \tag{8}$$

where A_ℓ is the label automaton shown in Fig. 1. We may state the following result.

Theorem 3. *The language L is robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_f if, and only if, the diagnoser $G_{dil,d}$ has no indeterminate (observed or hidden) cycles.*

Proof ($\Leftarrow$). Assume that L is not robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_f. Therefore, according to the robust diagnosability definition, for some trace $s \in \Psi(\Sigma_f)$ and for all $t \in L_{dil}/s$, $\|t\| \geq n$, n arbitrarily large, there exists a trace $\omega \in P^{-1}_{dil,o}(P_{dil,o}(D(st))) \cap L_{dil}$ such that $\Sigma_f \notin \omega$, where ω can have bounded or unbounded length.

Since $P_{dil,o}[D(\omega)] = P_{dil,o}[D(st)]$ and $G_{dil,d}$ is a deterministic automaton, then there exists an uncertain state $x_{dil,d} \in X_{dil,d}$ such that

$$x_{dil,d} = f_{dil,d}(x_{0_{dil,d}}, P_{dil,o}[D(st)]) = f_{dil,d}(x_{0_{dil,d}}, P_{dil,o}[D(\omega)]).$$

Let us consider, initially, ω of bounded length and assume that $|X_{dil,d}| = N_x$. If we make $n > N_x$, then there will exist a cycle of states whose events associated with the state transitions are either observable or unobservable. If the events are observable, $P_{dil,o}[D(\omega)] \neq P_{dil,o}[D(st)]$, which contradicts the initial assumption. On the other hand, if the events are unobservable, then there exists an indeterminate hidden cycle in $x_{dil,d} \in X_{dil,d}$.

Assume, now, that ω is unbounded and let, as in the previous case, $|X_{dil,d}| = N_x$. If $\|st\| > N_x$, then there will exist a cycle of states whose events associated with the transitions between the states of the cycle can either be observable or not. If at least one event is observable, then the cycle formed is indeterminate, otherwise there will be an indeterminate hidden cycle in the state reached by the trace whose projection has, as the last event, an observable event.

($\Rightarrow$) Let us consider, initially, the existence of indeterminate hidden cycles in $G_{dil,d}$. In order to do so, assume that there is an indeterminate hidden cycle in a state $x_{dil,d} = \{x_1\ell_1, x_2\ell_2, \ldots, x_n\ell_n\} \in X_{dil,d}$, where x_i is a state of G_{dil}. Therefore, according to Definition 5, there exists $\{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$ such that $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$ form a cycle in G_{dil}, and $\ell_{i_j} = Y, j = 1, 2, \ldots, k$. Then, it is not hard to see that there exists a trace $\omega_p = stu_p \in L_{dil}$ that satisfies the following conditions:

(1) $\Sigma_f \in s$ and $f_{dil,d}(x_{0_{dil,d}}, P_{dil,o}(s)) = x_{dil,d}$;
(2) $t \in (\Sigma'_{ilo} \cup \Sigma_{uo})^*$ such that $f_{dil,d}(x_{0_{dil,d}}, P_{dil,o}(st)) = x_{dil,d}$;
(3) $u_p \in (\Sigma'_{ilo} \cup \Sigma_{uo})^*$, $\|u_p\| = p$, with p arbitrarily large, is such that $f_{dil,d}(x_{0_{dil,d}}, P_{dil,o}(stu_p)) = x_{dil,d}$ and $f_{dil}(x_{i_1}\ell_{i_1}, u_j) = x_{i_j}\ell_{i_j}$, where $j = (p \bmod k) + 1$.

In addition, since $x_{dil,d}$ is an uncertain state, there exists $\omega \in L$ such that $\Sigma_f \notin \omega$ and $P_{dil,o}(\omega) = P_{dil,o}(\omega_p)$, which violates the diagnosability condition.

The proof that the diagnosability condition is also violated when $G_{dil,d}$ has indeterminate observed cycles follows the same steps as that presented in Sampath et al. (1995), with the difference that L is replaced with L_{dil}; it will be, therefore, omitted here. □

With the removal of Assumptions A1 and A2, Theorem 1 (Sampath et al., 1995) becomes a special case of Theorem 3, as follows.

Corollary 1. *The language L generated by automaton G is diagnosable with respect to projection P_o and $\Sigma_f = \{\sigma_f\}$ if, and only if, its diagnoser G_d has no indeterminate (observed or hidden) cycles.* □

The following example illustrates the results presented in Theorem 3.

Example 3. (a) Let us consider again automaton G of Fig. 2(a), and assume that event c is subject to intermittent loss of observations, *i.e.*, $\Sigma_{ilo} = \{c\}$. Automaton G_{dil} that models the behavior of G when subject to intermittent loss of observations is shown in Fig. 7, and the corresponding diagnoser $G_{dil,d}$ is depicted in Fig. 10(a). It is clear that $G_{dil,d}$ has an indeterminate cycle formed with state $\{6N, 7Y\}$, and, therefore, L is not robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_{ilo}. It is not difficult to see that, if trace $s_Y = c\sigma_f abd^n$, with n arbitrarily large, occurs and, in addition, the occurrence of event c is not recorded by the diagnoser, then $G_{dil,d}$ gets stuck in state $\{6N, 7Y\}$, being therefore uncertain about the fault occurrence. Notice that the non-occurrence of c is equivalent to the occurrence of the unobservable event c' in G_{dil} and thus $s'_Y = c'\sigma_f abd^n$ are ambiguous traces of L_{dil} since there exists a normal trace $s'_N = abd^n$ such that $P_{dil,o}(s'_Y) = P_{dil,o}(s'_N)$.

(b) Assume now that for the same automaton G of Fig. 2(a), a is an unobservable event and b is the event whose corresponding sensor is subject to intermittent loss of observations, *i.e.*, $\Sigma_{uo} = \{a, \sigma_f\}$ and $\Sigma_{ilo} = \{b\}$. The diagnoser G_d for G is shown in Fig. 10(b), from which it is clear that L is diagnosable with respect to P_o and Σ_f. The diagnoser $G_{dil,d}$ that takes into account intermittent loss of observations of event b is shown in Fig. 10(c). Notice that since $G_{dil,d}$ has an indeterminate hidden cycle in state $\{2N, 3Y, 7Y\}$, we may conclude that L is not robustly diagnosable with respect to D, $P_{dil,o}$

and Σ_{ilo}. As a consequence, if trace $s_Y = c\sigma_f ab^n$, n arbitrarily large, occurs, and the occurrence of event b is been recorded by the diagnoser, then $G_{dil,d}$ gets stuck in state $\{2N, 3Y, 7Y\}$. It is worth noting that since the permanent loss of observations of event b is equivalent that b' occurs indefinitely, then the occurrence of s_Y in G is equivalent to the occurrence of $s'_Y = c\sigma_f ab'^n$ in G_{dil}. Therefore s'_Y is an ambiguous trace since, for $s_N = c$, $P_{dil,o}(s'_Y) = P_{dil,o}(s_N) = c$. An important point regarding this example is that, if at anytime the observation of event b is performed again, then $G_{dil,d}$ will move to state $\{7Y\}$, indicating that the fault event σ_f has occurred; this is consistent with what is expected for the behavior of a diagnoser that is designed to cope with intermittent loss of observations.

It is important to remark that if the language generated by an automaton G is robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_f, then the diagnoser $G_{dil,d}$ not only provides an off-line test for robust diagnosability but can also be used at run-time to perform diagnosis of a DES subject to intermittent loss of observations. For this reason, $G_{dil,d}$ will be referred to as "robust diagnoser against intermittent loss of observations". This fact will be illustrated in the following example.

Example 4. Consider again automaton G of Fig. 2(a), and assume that $\Sigma_o = \{a, b, c, d, e\}$ and that event a is subject to intermittent loss of observations, *i.e.*, $\Sigma_{ilo} = \{a\}$. As it was concluded from the diagnoser G_d depicted in Fig. 2(b), L is diagnosable with respect to P_o and Σ_f. Fig. 11 shows diagnoser $G_{dil,d}$, which has no indeterminate (observed or hidden) cycles. Consequently, L is robustly diagnosable with respect to D, $P_{dil,o}$ and Σ_f.

Let us now consider the effect of intermittent loss of observations of event a in online fault detection. Assume that the faulty trace $s_Y = c\sigma_f ab^n$ (n arbitrarily large) has occurred. If we are using the non-robust diagnoser of Fig. 2(b), and if event a is not observed by G_d, the diagnoser gets stuck in state $\{2N, 3Y\}$ since $b \notin \Gamma_d(\{2N, 3Y\})$, being, therefore, permanently uncertain about the occurrence of the faulty event σ_f. When the robust diagnoser $G_{dil,d}$ of Fig. 11 is used, then, after the occurrence of event c, $G_{dil,d}$ moves to state $\{2N, 3Y, 7Y\}$. If either the sensor that records the occurrence of event a fails or its occurrence is not successfully reported to the diagnoser due to some failure in the communication channel, the next event to be recognized by $G_{dil,d}$ is b. When b occurs, the robust diagnoser updates its state to $\{7Y\}$, being, therefore, sure of the fault occurrence. On the other hand, if there is no loss of observations of event a, then a is the first event whose occurrence is recognized by $G_{dil,d}$ after the occurrence of c; thus $G_{dil,d}$ moves to $\{7Y\}$, and stays there permanently since b is the next event of trace s_Y to occur.

Notice that either occurring or not some intermittent loss of observations of event a, the robust diagnoser not only diagnoses the fault occurrence but also indicates the correct estimation of the state where the original automaton might be after the occurrence of each event of s_Y.

5.2. Construction of the robust diagnoser directly from diagnoser G_d

In the previous subsection, we built a diagnoser to test the robust diagnosability of L by first constructing an augmented automaton G_{dil} and, in the sequel, building a diagnoser for G_{dil}. Since robust diagnosability of L with respect to D, $P_{dil,o}$ and Σ_f requires that L be already diagnosable with respect to P_o and Σ_f, whose verification can be carried out with diagnosers, we may wonder if it is also possible to obtain an equivalent diagnoser directly from G_d by dilating the language generated by G_d, and then obtaining the observer for the augmented diagnoser. This approach is sketched in Fig. 12 (right branch) together with the approach presented in the previous subsection (left branch).

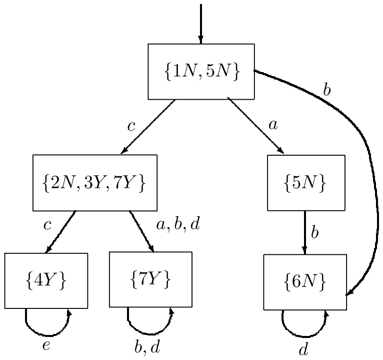


Fig. 11. The robust diagnoser against intermittent loss of observations of Example 4.

$$\begin{tikzcd}
 & G \arrow[dl] \arrow[dr] & \\
G_{dil} \arrow[dd] & & G_d \arrow[d] \\
 & & G_{d,dil} \arrow[d] \\
G_{dil,d} & & \hat{G}_{dil,d}=Obs(G_{d,dil},\Sigma_o)
\end{tikzcd}$$

Fig. 12. Two ways to obtain diagnosers to test for robust diagnosability.

It is not difficult to see that both automata, $G_{dil,d}$ and $\hat{G}_{dil,d}$, in Fig. 12 are deterministic, and thus, in order to prove that they are equivalent, it is enough to prove that they generate the same language. However, the states of diagnosers play an important role in diagnosability analysis, and thus, it is also necessary to establish some relationship between the states of $G_{dil,d}$ and $\hat{G}_{dil,d}$. Since $\mathscr{L}(G_{dil,d}) = P_{dil,o}[D(L)]$ and $\mathscr{L}(\hat{G}_{dil,d}) = P'_{oo}\{D[P_o(L)]\}$, where $P'_{oo} : \Sigma_o'^* \to \Sigma_o^*$, with $\Sigma'_o = \Sigma_o \cup \Sigma'_{ilo}$, we first need to prove that $P_{dil,o}[D(L)] = P'_{oo}\{D[P_o(L)]\}$.

Lemma 1.

A. *For any event* $\sigma \in \Sigma$, $P'_{oo}[D[P_o(\sigma)]] = P_{dil,o}[D(\sigma)]$.
B. *For any language L, defined in* Σ^*, $P'_{oo}[D[P_o(L)]] = P_{dil,o}[D(L)]$.

Proof. The proof for A follows directly from the definitions of dilation and projection, and will therefore be omitted.

The proof for B is by induction on the length of the traces in the two languages.

- The base case is for traces of length 0. For $s = \epsilon$, we have that, by definition, $P'_{oo}[D[P_o(\epsilon)]] = \epsilon$ and $P_{dil,o}[D(\epsilon)] = \epsilon$.
- The induction hypothesis is that for all traces $s_N \in L$, $\|s_N\| \leq N$, $P'_{oo}[D[P_o(s_N)]] = P_{dil,o}[D(s_N)]$.
- Consider, now, a trace $s_{N+1} = s_N\sigma \subset L$, where $\sigma \in \Sigma$. Then

$$\begin{aligned}
P'_{oo}[D[P_o(s_{N+1})]] &= P'_{oo}[D[P_o(s_N\sigma)]] \\
&= P'_{oo}[D[P_o(s_N)]]P'_{oo}[D[P_o(\sigma)]] \\
&= P_{dil,o}[D(s_N)]P_{dil,o}[D(\sigma)] \\
&= P_{dil,o}[D(s_N\sigma)] = P_{dil,o}[D(s_{N+1})]. \quad \square \qquad (9)
\end{aligned}$$

The next result shows that automata $G_{dil,d}$ and $\hat{G}_{dil,d}$ are not only language equivalent but also that their states are equal up to a straightforward renaming.

Theorem 4. *Automata $G_{dil,d}$ and $\hat{G}_{dil,d}$ are language equivalent,* i.e., *$\mathscr{L}(G_{dil,d}) = \mathscr{L}(\hat{G}_{dil,d})$ and their states are equal up to the following renaming:*

$$\hat{x}_{dil,d} = \{x_{d,1}, x_{d,2}, \dots, x_{d,q}\} \in \hat{X}_{dil,d} \Leftrightarrow x_{dil,d} = \bigcup_{i=1}^{q} x_{d,i} \in X_{dil,d}, \quad (10)$$

where $x_{d,i} \in X_d$, $x_{d,i} = \{x_{i1}\ell_{i1}, x_{i2}\ell_{i2}, \dots, x_{ip_i}\ell_{ip_i}\}$, $x_{ij} \in X$, $\ell_{ij} \in \{Y, N\}$, $i = 1, 2, \dots, q$, $j = 1, 2, \dots, p_i$, and $X_{dil,d}$ and $\hat{X}_{dil,d}$ denote, respectively, the state-space of $G_{dil,d}$ and $\hat{G}_{dil,d}$. In addition, any hidden cycle in a state $x_{dil,d}$ is also a hidden cycle in $\hat{x}_{dil,d}$ and vice versa.

Proof. Language equivalence of automata $G_{dil,d}$ and $\hat{G}_{dil,d}$ follows directly from Lemma 1.

Let us now prove relationship (10) between the states of $G_{dil,d}$ and $\hat{G}_{dil,d}$. In order to do so, assume that $\hat{x}_{dil,d} \in \hat{X}_{dil,d}$ is a state of $\hat{G}_{dil,d}$ reached by a trace $s' \in \mathscr{L}(\hat{G}_{dil,d})$. Then, for all $x_{d,i} \in \hat{x}_{dil,d}$, $i \in \{1, 2, \dots, q\}$, there exists a trace $s_{d,i} \in \mathscr{L}(G_d)$ such that $s' \in P'_{oo}[D(s_{d,i})]$ and $f_d(x_{0,d}, s_{d,i}) = x_{d,i}$. As a consequence, for all $x_{ij}\ell_{ij} \in x_{d,i}$, $j = 1, 2, \dots, p_i$, there exists a trace $s_{ij} \in L$ such that $P_o(s_{ij}) = s_{d,i}$, $f(x_0, s_{ij}) = x_{ij}$ and $\ell_{ij} = Y$, if $\Sigma_f \in s_{ij}$, or $\ell_{ij} = N$, if $\Sigma_f \notin s_{ij}$. Since $G_{dil,d}$ is a deterministic automaton and $P'_{oo}[D[P_o(s_{ij})]] = P_{dil,o}[D(s_{ij})]$, there exists $x_{dil,d} = f_{dil,d}(x_{0,dil,d}, s')$ such that $x_{ij}\ell_{ij} \in x_{dil,d}$. Hence, $x_{ij}\ell_{ij} \in x_{d,i} \in \hat{x}_{dil,d}$, which implies that $x_{dil,d} = \bigcup_{i=1}^{q} x_{d,i} \subseteq \hat{x}_{dil,d}$.

Consider, now, a state $x_{dil,d} \in X_{dil,d}$ such that $x_{dil,d} = f_{dil,d}(x_{0,dil,d}, s')$ for some $s' \in \mathscr{L}(G_{dil,d})$. Then, there exists $s_{ij} \in L$ such that $s' \in P_{dil,o}[D(s_{ij})]$ and $x_{ij} = f(x_0, s_{ij})$, with $x_{ij}\ell_{ij} \in x_{dil,d}$, where $\ell_{ij} = Y$, if $\Sigma_f \in s_{ij}$, or $\ell_{ij} = N$, if $\Sigma_f \notin s_{ij}$. Therefore, there exists $x_{d,i} = f_d(x_{0,d}, P_o(s_{ij}))$ such that $x_{ij}\ell_{ij} \in x_{d,i}$. In addition, since $P'_{oo}[D[P_o(s_{ij})]] = s'$ and $\hat{G}_{dil,d}$ is a deterministic automaton, then, according to Basilio and Lafortune (2009), there exists $\hat{x}_{dil,d} = \hat{f}_{dil,d}(\hat{x}_{0,dil,d}, s')$ such that $x_{d_i} \in \hat{x}_{dil,d}$ which implies that $\hat{x}_{dil,d} \subseteq \cup_{i=1}^{q} x_{d,i}$.

Let us now deal with the hidden cycles of $G_{dil,d}$ and $\hat{G}_{dil,d}$. First, assume that states $x_{i1}, x_{i2}, \dots, x_{ip}$, $p \leq p_i$ form a cycle in G and let $f(x_{ik}, \sigma_k) = x_{i,k+1}$, $k = 1, 2, \dots, p-1$ and $f(x_{ip}, \sigma_p) = x_{i1}$, where $\sigma_j \in \Sigma_{uo}$, $j \in \{1, 2, \dots, p\}$. It is clear that $x_{i1}, x_{i2}, \dots, x_{ip}$ is also a cycle of states of G_{dil} and thus $\exists x_{dil,d} \in X_{dil,d}$ such that $\{x_{i1}, x_{i2}, \dots, x_{ip}\} \subseteq x_{dil,d}$, which implies that $x_{i1}, x_{i2}, \dots, x_{ip}$ define a hidden cycle in $x_{dil,d}$. In addition, from the construction of G_d, it is not difficult to see that $\exists x_{d,i} \in X_d$ such that $x_{d,i} = \{x_{i1}\ell_{i1}, x_{i2}\ell_{i2}, \dots, x_{ip_i}\ell_{ip_i}\}$ has a hidden cycle. Since $\hat{G}_{dil,d}$ is obtained by merging states of G_d connected with events in Σ'_{ilo} then $\exists \hat{x}_{dil,d}$ such that $x_{d,i} \in \hat{x}_{dil,d}$, thus states $x_{i1}, x_{i2}, \dots, x_{ip}$ also define a hidden cycle in $\hat{x}_{dil,d}$.

Assume now that $x_{i1}, x_{i2}, \dots, x_{ip'}$, $p' \leq p_i$ and $x_{j1}, x_{j2}, \dots, x_{jp''}$, $i \neq j$, $p'' \leq p_j$ are states of G such that $f(x_{ik}, \sigma_k) = x_{i,k+1}$, $k = 1, 2, \dots, p'-1$ and $f(x_{jk}, \sigma_k) = x_{j,k+1}$, $k = 1, 2, \dots, p''-1$ where $\sigma_k \in \Sigma_{uo}$, $k \in \{1, 2, \dots, \max(p', p'')\}$. It is not difficult to see that $x_{i1}, x_{i2}, \dots, x_{ip'}$ and $x_{j1}, x_{j2}, \dots, x_{jp''}$ do not form cycles in G and, from the diagnoser construction, there exist $x_{d,i}, x_{d,j} \in X_d$ such that $\{x_{i1}, x_{i2}, \dots, x_{ip'}\} \in x_{d,i}$ and $\{x_{j1}, x_{j2}, \dots, x_{jp''}\} \in x_{d,j}$. Suppose there exist events $\sigma_{p'}, \sigma_{p''} \in \Sigma'_{ilo}$ such that $f(x_{ip'}, \sigma'_p) = x_{j1}$ and $f(x_{jp''}, \sigma_{p''}) = x_{i1}$. Therefore $x_{i1}, x_{i2}, \dots, x_{ip'}, x_{j1}, x_{j2}, \dots, x_{jp''}$ form a cycle in G_{dil}, which implies that there exists a state $x_{dil,d} \in X_{dil,d}$ such that $x_{d,ij} = \{x_{i1}\ell_{i1}, x_{i2}\ell_{i2}, \dots, x_{ip'}\ell_{ip'}, x_{j1}\ell_{j1}, x_{j2}\ell_{j2}, \dots, x_{jp''}\ell_{jp''}\} \subseteq x_{dil,d}$. As a consequence, $x_{i1}, x_{i2}, \dots, x_{ip'}, x_{j1}, x_{j2}, \dots, x_{jp''}$ defines a hidden cycle in $x_{dil,d}$. The assumption that $\sigma_{p'}, \sigma_{p''} \in \Sigma'_{ilo}$ implies that $x_{d,i}, x_{d,j}$ form a cycle in $G_{d,dil}$, and since $\hat{G}_{dil,d}$ is obtained by merging states of G_d connected with events in Σ'_{ilo}, then there exists $\hat{x}_{dil,d}$ such that $\{x_{d,i}, x_{d,j}\} \subseteq \hat{x}_{dil,d}$ which ultimately implies that $x_{i1}, x_{i2}, \dots, x_{ip'}, x_{j1}, x_{j2}, \dots, x_{jp''}$ also defines a hidden cycle in $\hat{x}_{dil,d}$. □

5.3. Extension to robust codiagnosability

A decentralized architecture for fault diagnosis has been proposed in Debouk et al. (2000), in which sensor readings are no longer centralized, but distributed over different sites, each site observing the system behavior based on its available sensing capabilities, or equivalently, on the set of observable events Σ_{o_i}, $i = 1, 2, \dots, n$—assuming there are n independent sites. Each site processes the information received (event occurrences), and, in the decentralized architecture proposed in Debouk et al. (2000), the local sites do not communicate with one another and no explicit coordination among sites is necessary. They can only communicate their diagnostics to a coordinator, which processes this information according to a prescribed rule and takes a decision on the fault occurrence. This is the situation corresponding to Protocol 3 in Debouk et al. (2000) and is often referred to in recent works (Qiu & Kumar, 2006; Wang et al., 2007) as *codiagnosability*. Codiagnosability refers to the situation where it is required that each fault be diagnosed by at least one local site, when all local sites operate autonomously by processing their local observations.

The definition of codiagnosability presented in Debouk et al. (2000) can be extended to robust codiagnosability of DES subject to intermittent loss of observations with the help of projections $P_{dil,o_i}: \Sigma^*_{dil} \to \Sigma^*_{o_i}$, $i = 1, \dots, n$, as follows.

Definition 6 (*Robust Codiagnosability Against Intermittent Loss of Observations*)**.** A prefix-closed and live language L is NOT robustly codiagnosable with respect to dilation D, projections P_{dil,o_i}, $i = 1, \dots, n$, and $\Sigma_f = \{\sigma_f\}$ if the following holds true

$$(\exists (s,t) \in \Psi(\Sigma_f) \times L/s)(\|t\| \geq n, \forall n \in \mathbb{N} \Rightarrow R_C),$$

where condition R_C is given as
$(\exists \omega_i \in L, i = 1, 2, \dots, n)(\Sigma_f \notin \omega_i)(\omega_k$ not necessarily distinct from ω_l, $k \neq l)[P_{o_i}(D(st)) = P_{o_i}(D(\omega_i)), i = 1, 2, \dots, n]$.

Comparing the definition of codiagnosability presented in Debouk et al. (2000) and Definition 6, we note that in Definition 6, st and ω_i are replaced with $D(st)$ and $D(\omega_i)$, respectively. Therefore, since $L_{dil} = D(L)$ we may say that robust codiagnosability with respect to dilation D, projections P_{dil,o_i}, $i = 1, \dots, n$, and $\Sigma_f = \{\sigma_f\}$ is equivalent to codiagnosability of G_{dil} with respect to projections P_{dil,o_i}, $i = 1, \dots, n$, and $\Sigma_f = \{\sigma_f\}$. We may state the following result.

Theorem 5. *A language L is robustly codiagnosable with respect to D, the set of projections P_{dil,o_i}, $i = 1, 2, \dots, n$ and $\Sigma_f = \{\sigma_f\}$ if, and only if,*

$$G_{dil,t} = (\|_{i=1}^{n} G_{dil,d_i}) \| G_{dil,d} \quad (11)$$

does not have any indeterminate (observed or hidden) cycles.

As in the construction of the diagnosers used to verify robust diagnosability with respect to loss of observations, the construction of the test automaton $G_{dil,t}$ can be carried in two ways as shown in Fig. 13. The path on the left is the one generated according to Eq. (11) whereas the path on the right uses the results of Theorem 4. The proof of the equivalence between $G_{dil,t}$ and $\hat{G}_{dil,t}$ is similar to that of Theorem 4 and will be therefore omitted.

5.4. Computational complexity analysis

The computational complexity to build $G_{dil,d}$ is $O(2^{|X_{dil}|} \times |\Sigma_{dil}|)$, where X_{dil} and Σ_{dil} denote, respectively, the state and event sets of G_{dil}. Since G_{dil} and G have the number of states (they actually have the same states) and $|\Sigma_{dil}| < 2|\Sigma|$, then the computational complexity to build $G_{dil,d}$ is, in the worst case, $O(2^{|X|} \times |\Sigma|)$.

According to Eq. (11), $G_{dil,\,t} = (\|_{i=1}^{n} G_{dil,d_i}) \| G_{dil,d}$, which implies that, in the worst case, the number of states of $G_{dil,\,t}$ is $|X_{dil,t}| = (2^{|X|})^{n+1} = 2^{(n+1)|X|}$, and so, the computational complexity to build $G_{dil,t}$ is $O(2^{n|X|} \times |\Sigma|)$ in the worst case.

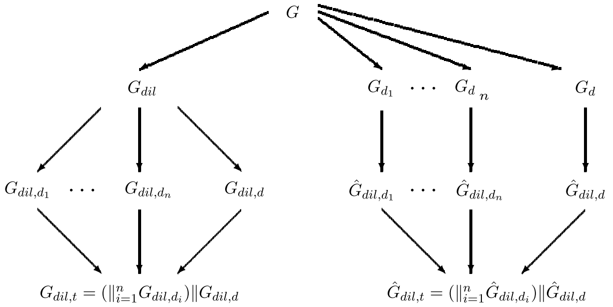

G
G_{dil}
G_{d_1} $\cdots$ G_{d_n}
G_d
G_{dil,d_1} $\cdots$ G_{dil,d_n}
$G_{dil,d}$
$\hat{G}_{dil,d_1}$ $\cdots$ $\hat{G}_{dil,d_n}$
$\hat{G}_{dil,d}$
$G_{dil,t} = (\|_{i=1}^{n} G_{dil,d_i}) \| G_{dil,d}$
$\hat{G}_{dil,t} = (\|_{i=1}^{n} \hat{G}_{dil,d_i}) \| \hat{G}_{dil,d}$

Fig. 13. Two ways to obtain test automata for verification of robust codiagnosability.

6. Verification of robust diagnosability using verifiers

Another way to verify language diagnosability is by using verifiers (Moreira, Jesus, & Basilio, 2010, 2011; Qiu & Kumar, 2006; Shengbing, Zhongdong, Chandra, & Kumar, 2001; Wang et al., 2007; Yoo & Lafortune, 2002). The main advantage of verifiers over diagnosers is that they require polynomial time in the state-space of the automaton. On the other hand, unlike diagnosers, verifiers are not suitable for online diagnosis. The verifier proposed in Moreira et al. (2011) has lower computational complexity than the methods proposed in Qiu and Kumar (2006), Shengbing et al. (2001), Wang et al. (2007), Yoo and Lafortune (2002), and, in addition, is deterministic. For these reasons it will be used here in the study of robust diagnosability in the presence of intermittent loss of observations.

The construction of the verifier automaton proposed by Moreira et al. (2011) (and also the above mentioned ones) does not require computation of observers (see Eq. (8)). Therefore, robust verifiers cannot, in general, be obtained directly from the verifier for G by a procedure similar to that presented in Section 5.2. For this reason, verification of robust diagnosability (and also codiagnosability) should be carried out according to Definition 4 by constructing the verified for G_{dil} (instead of G) and replacing the renaming function required in Step 3 of Algorithm 1 of Moreira et al. (2011) with the following one:

$$R_i(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \in \Sigma_{o_i} \cup \Sigma_f \\ \sigma_{R_i}, & \text{if } \sigma \in \Sigma_{uo_i} \setminus \Sigma_f, \end{cases} \qquad (12)$$

where $i = 1$ for robust diagnosability, and to ascertain the robust diagnosability (codiagnosability) of L with respect to D, $P_{dil,o}$ (resp. P_{dil,o_i} according to Theorem 1 of Moreira et al. (2011)).

As a consequence, the computational complexity to check robust diagnosability (codiagnosability) is the same as that to construct Moreira's verifier, *i.e.*, $O(|X|^2 \times |\Sigma|)$ and (resp. $O(n \times |X|^{n+1} \times |\Sigma|)$), therefore requiring polynomial time in the number of states and events of G.

7. Conclusions and future works

We have addressed in this paper the problem of fault diagnosis of discrete event systems modeled by automata subject to intermittent loss of observations. We have introduced a new language operation (dilation) which allowed us to derive an automaton model that accounts for both, normal behavior (with no intermittent loss of observations) and subject to intermittent loss of observations. We have also presented a definition of robust diagnosability against intermittent loss of observations and derived a necessary and sufficient condition. In order to derive such a necessary and sufficient condition, we removed Assumptions A1 and A2 of Sampath et al. (1995), which precludes the existence of cycles of states connected with unobservable events. As a consequence, the diagnosability condition presented in Sampath et al. (1995) has been changed, and become a particular case of the robust diagnosability condition derived here.

The verification of robust diagnosability against intermittent loss of observations only makes sense if the language is already diagnosable when there are no failures of the sensors and the corresponding communication channels. To take advantage of that, we presented two ways of computing the robust diagnoser: in the first way, we obtain a robust diagnoser from the plant model that takes into account intermittent loss of observations; in the second way, we modify the diagnoser automaton in the same way as we modify the plant in order to take into account intermittent loss of observations and, in the sequel, we obtain the observer of the resulting automaton with respect to the set of observable events. We proved that both ways lead to the same diagnoser, apart from some straightforward state renaming. It is important to remark that when robust diagnosability is assured, robust diagnosers can also be used in run-time to perform online fault diagnosis.

In dealing with sensor malfunction, we have assumed that possible defective sensors are neither part of the supervisory control system nor, in a lower level, part of the continuous variable controller for the plant. If, on the other hand, all sensors work properly but there is some failure in the communication channel that connects the sensor and the diagnoser, and, furthermore, this communication channel is not shared with the supervisor, then any intermittent loss of observations only affect the diagnoser. From the theoretical point of view, there is no difference in assuming either only communication failure or both sensor and communication failures, because it can be easily checked, by following the same reasoning as that of Section 3.2, that both assumptions lead to the same model. The real concern must be with the range of discrete event systems to which the theory introduced here can be applied, *i.e.*, those whose controlled behavior has not been affected by loss of observations. In this regard, an extension of the theory introduced here is in the design of sensor and communication failure tolerant control, generalizing the problem formulated by Rohloff (2005) to intermittent loss of observations. Notice that in the problem formulated by Rohloff (2005), it is assumed that sensors may fail even after the first occurrence of the event it records but once the failure occurs, the sensor never recovers, as opposed to our assumption of intermittent loss of observations which allows the sensor to recover.

Acknowledgments

We would like to thank the anonymous reviewers for their comments and suggestions which helped improve the presentation and readability of the paper.

References

Athanasopoulou, E., Lingxi, L., & Hadjicostis, C. (2010). Maximum likelihood failure diagnosis in finite state machines under unreliable observations. *IEEE Transactions on Automatic Control*, *55*(3), 579–593.

Basilio, J. C., & Lafortune, S. (2009). Robust codiagnosability of discrete event systems. In *Proc. of the American control conference* (pp. 2202–2209).

Basilio, J. C., Lima, S. T. S., Lafortune, S., & Moreira, M. V. (2012). Computation of minimal event bases that ensure diagnosability. *Discrete Event Dynamic Systems: Theory and Applications*, http://dx.doi.org/10.1007/s10626-012-0129-z.

Carvalho, L. K., Basilio, J. C., & Moreira, M. V. (2010). Robust diagnosability of discrete event systems subject to intermittent sensor failures. In *Proc. of the 10th international workshop on discrete event systems* (pp. 94–99).

Cassandras, C. G., & Lafortune, S. (2008). *Introduction to discrete event systems* (2nd ed.). New York: Springer.

Contant, O., Lafortune, S., & Teneketzis, D. (2006). Diagnosability of discrete event systems with modular structure. *Discrete Event Dynamic Systems: Theory and Applications*, *16*(1), 9–37.

Debouk, R., Lafortune, S., & Teneketzis, D. (2000). Coordinated decentralized protocols for failure diagnosis of discrete event systems. *Discrete Event Dynamic Systems: Theory and Applications*, *10*, 33–86.

Kumar, R., & Takai, S. (2009). Inference-based ambiguity management in decentralized decision-making: decentralized diagnosis of discrete-event systems. *IEEE Transactions on Automation Science and Engineering*, *6*(3), 479–491.

Lima, S. T. S., Basilio, J. C., Lafortune, S., & Moreira, M. V. (2010). Robust diagnosis of discrete-event systems subject to permanent sensor failures. In *Proc. of the 10th international workshop on discrete event systems* (pp. 100–107).

Lin, F. (1994). Diagnosability of discrete event systems and its applications. *Discrete Event Dynamic Systems: Theory and Applications*, *4*(2), 197–212.

Moreira, M. V., Jesus, T. C., & Basilio, J. C. (2010). Polynomial time verification of decentralized diagnosability of discrete event systems. In *Proc. of the American control conference* (pp. 3353–3358).

Moreira, M. V., Jesus, T. C., & Basilio, J. C. (2011). Polynomial time verification of decentralized diagnosability of discrete event systems. *IEEE Transactions on Automatic Control*, *56*(7), 1679–1684.

Qiu, W., & Kumar, R. (2006). Decentralized failure diagnosis of discrete event systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, *36*(2), 384–395.

Ramadge, P. J., & Wonham, W. M. (1989). The control of discrete-event systems. *Proceedings of the IEEE*, *77*, 81–98.

Rohloff, K. R. (2005). Sensor failure tolerant supervisory control. In *44th IEEE conference on decision and control and European control conference* (pp. 3493–3498).

Sampath, M., Sengupta, R., Lafortune, S., Sinnamohideen, K., & Teneketzis, D. (1995). Diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *40*, 1555–1575.

Shengbing, J., Zhongdong, H., Chandra, V., & Kumar, R. (2001). A polynomial algorithm for testing diagnosability of discrete-event systems. *IEEE Transactions on Automatic Control*, *46*(8), 1318–1321.

Takai, S. (2010). Robust failure diagnosis of partially observed discrete event systems. In *Proc. of 10th international workshop on discrete event systems* (pp. 215–220).

Thorsley, D., & Teneketzis, D. (2005). Diagnosability of stochastic discrete-event systems. *IEEE Transactions on Automatic Control*, *50*, 476–492.

Tripakis, S. (2002). Fault diagnosis for timed automata. In W. Damm, & E.-R. Olderog (Eds.), *Lecture notes in computer sciences*: *Vol. 2469*. *Formal techniques in real time and fault tolerant systems* (pp. 205–221). Springer-Verlag.

Wang, Y., Yoo, T. S., & Lafortune, S. (2007). Diagnosis of discrete event systems using decentralized architectures. *Discrete Event Dynamic Systems: Theory and Applications*, *17*(2), 233–263.

Yoo, T. S., & Lafortune, S. (2002). Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Transactions on Automatic Control*, *47*(9), 1491–1495.

Zad, S. H., Kwong, R. H., & Wonham, W. M. (2003). Fault diagnosis in discrete-event systems: framework and model reduction. *IEEE Transactions on Automatic Control*, *48*(7), 1199–1212.

Lilian K. Carvalho was born on March, 11, 1979 in São Paulo, Brazil. She received the Electronic Engineer degree, the M.Sc. degree and the D. Sc. degree in Control from the Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, in 2003, 2005 and 2011, respectively. Since 2011, she has been an Associate Professor at the Department of Electrical Engineering at the Federal University of Rio de Janeiro. Her main interests are fault diagnosis of discrete-event systems, supervisory control applied to mobile robotics, and the development of control laboratory techniques.

João C. Basilio was born on March 15, 1962 in Juiz de Fora, Brazil. He received the Electrical Engineering degree in 1986 from the Federal University of Juiz de Fora, Juiz de Fora, Brazil, the M.Sc. degree in Control from the Military Institute of Engineering, Rio de Janeiro, Brazil, in 1989, and the Ph.D. degree in Control from Oxford University, Oxford, UK, in 1995. He began his career in 1990 as an Assistant Lecturer at the Department of Electrical Engineering of the Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, and, since 2007, has been a Senior Associate Professor in Control at the same department. He served as the Academic Chair for the graduation course in Control and Automation from January, 2005, to December, 2006, and as the Chair for the Electrical Engineering Post-graduation Program from January, 2008, to February, 2009. From September, 2007, to December, 2008, he spent a sabbatical leave at the University of Michigan, Ann Arbor. He is currently interested in discrete-event systems and in the development of control and automation laboratories and new teaching techniques. Dr. Basilio is the recipient of the Correia Lima Medal.

Marcos V. Moreira was born on May, 11, 1976 in Rio de Janeiro, Brazil. He received the Electrical Engineer degree, the M.Sc. degree and the D. Sc. degree in Control from the Federal University of Rio de Janeiro, Rio de Janeiro, Brazil, in 2000, 2002 and 2006, respectively. Since 2007, he has been an Associate Professor at the Department of Electrical Engineering at the Federal University of Rio de Janeiro. His main interests are multivariable control, robust control, discrete-event systems and the development of control laboratory techniques.