Diagnosis using labeled Petri nets with silent or undistinguishable fault events

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu*†

Abstract

A commonplace assumption in the fault diagnosis of discrete event systems is that of modeling faulty events with unobservable transitions, i.e., transitions whose occurrence does not produce any observable label. The diagnostic system must thus infer the occurrence of a fault from the observed behavior corresponding to the firing of non-faulty transitions. The presence of non-faulty unobservable transitions is a source of additional complexity in the diagnostic procedure.

In this paper we assume that fault events can also be modeled by observable transitions, i.e., transitions whose occurrence produces an observable label. This does not mean, however, that the occurrence of such a transition can be unambiguously detected: in fact, the same label may be shared with other fault transitions (e.g., belonging to different fault classes) or with other non-faulty transitions. We generalize to this new setting our previous results on the diagnosis of discrete event systems using Petri nets based on the notions of minimal explanations and basis markings. The presented procedure does not require the enumeration of the complete reachability set, but only of the subset of basis markings, thus reducing the computational complexity of solving a diagnosis problem.

Published as:
M.P. Cabasino, A. Giua, C. Seatzu, "Fault diagnosis using labeled Petri nets where faults may either be silent or undistinguishable events," *EEE Transactions on Systems, Man, and Cybernetics–Part A: Systems*, Vol. 43, No. 2, pp. 345-355, Mar 2013. The original publication is available at www.ieeexplore.ieee.org.

*M.P. Cabasino, A. Giua and C. Seatzu are with the Department of Electrical and Electronic Engineering, University of Cagliari, Piazza D'Armi, 09123 Cagliari, Italy. E-mail:{cabasino,giua,seatzu}@diee.unica.it.

†This work has been partially supported by the European Community's Seventh Framework Programme under project DISC (Grant Agreement n. INFSO-ICT-224498).

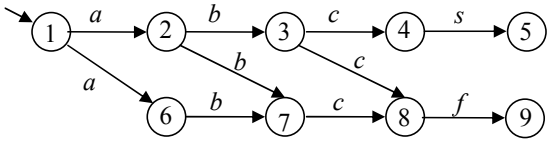

Figure 1: A sketch of an immobilizer key system.

1 Introduction

In this paper we focus on the problem of deriving an efficient approach for the fault diagnosis of discrete event systems (DES). Solving a problem of diagnosis means that to each observed string of events is associated a diagnosis state, such as "normal" or "faulty" or "uncertain". This problem has attracted the attention of several researchers and engineers in the last decades. A survey of some of the most important contributions in the Petri nets framework [1, 27, 15, 10, 14, 8, 23, 22, 5, 3, 9, 24, 25, 11, 16, 21, 17] is reported in the next section. In almost all such works, faults are considered as unobservable transitions. However, in some real applications they can also be modeled as observable transitions. As an example let us consider the immobilizer key system, namely the electronic device fitted to an automobile which prevents the engine from running unless the correct key (or other token) has been inserted. Its behavior can be synthesized by the scheme in Fig. 1. The event labeled a represents the insertion of the key, the event labeled b represents the activation of the micro-circuit inside the key and event labeled c determines the validity of the coded key. The sensors associated with these events may produce a label also if something went wrong. In fact, a may also be observed if the key does not perfectly fit into the key slot, b may also be observed if the micro-circuit is not working well and c could also be observed if the signal with the validity of the key has not been sent. States from 1 to 5 represent the nominal behavior, states from 6 to 9 represent that at least one fault has occurred. Finally event s represents that the code is valid and that the Engine Control Unit activates the fuel-injection sequence, while f means that at least one fault has occurred.

The main feature of our procedure [5, 3] is the concept of *basis marking* that allows one to represent the reachability space in a more compact manner, only enumerating a subset of its markings. In our previous paper [5] we presented an approach for on-line diagnosis of Petri nets (PNs) where fault transitions are only modeled by silent transitions, but there also exist other silent transitions that model regular behavior. In [3] we dealt with labeled PNs and this enabled us to also take into account a new source of nondeterminism originating from the fact that different observable transitions modeling regular behavior may share the same label. Both approaches apply to all net systems whose unobservable subnet is acyclic.

In this paper, that is a journal version of [4], we generalize the previous problem statement assuming that fault transitions are not necessarily silent, but they can also be observable transitions that share the same label with transitions belonging to different fault classes and/or with transitions modeling a regular behavior. As for the previous approaches we require that the unobservable subnet of the considered net system is acyclic.

The considered generalization requires to significantly rewrite our previous formulation [3]. In particular, we need to introduce new vectors, called γ-vectors, that keep into account all possible sequences of observable transitions that may have actually fired given the observation, as well as the iterative procedure to compute them. Moreover, we need to redefine the diagnosis states in [3], each one corresponding to a different degree of alarm, and rewrite the procedure for their computation. Furthermore, we show that if the net system is bounded, the most burdensome part of the procedure can be moved off-line defining a particular graph, that we call *Basis Reachability Graph*. Note that the Basis Reachability Graph has also been introduced in [3]. In particular, the number of nodes coincides in the two cases (here and in [3]) with the number of possible basis markings, while arcs are defined in a different way. Indeed, now we also need to keep into account additional information on possible occurrences of observable fault transitions. Finally, the procedure to perform on-line diagnosis using the Basis Reachability Graph should be rewritten accordingly. Note that, since the number of nodes of the Basis Reachability Graph is the same in the two cases, all conclusions drawn in [3] relatively to the advantages in terms of computational complexity originating from using basis markings, also apply in this more general setting.

2 Literature review

The diagnosis problem of discrete event systems has been extensively investigated in the last decades and several original theoretical approaches have been proposed in the literature, both in the automata [7, 28, 12, 26] and in the PN framework [1, 27, 15, 10, 14, 8, 23, 22, 5, 3, 9, 24, 25, 11, 16, 21, 17]. In this section we briefly survey the most significant and recent contributions in the PN area. Note that most of such contributions are based on very different assumptions on the PN model (e.g., untimed or timed model), on different assumptions on the admissible observations (e.g., transitions and/or marking of certain places), on the structure of the diagnoser (e.g., centralized or decentralized), and so on. As a result of this it is very difficult, and often not significant, to make a detailed comparison among them, both in terms of computational complexity and fault detection capability. In particular, to the best of our knowledge, the possibility of modeling faults as observable undistinguishable events, that is the main feature of the approach presented in this paper, has been considered by very few authors [9, 24].

There are three main differences between our contribution and the work of Garcia et al. [9] and its generalization to hybrid Petri nets by Rodriguez et al. [24]. Firstly, in [9] P-Timed Colored Petri nets are considered and timing information are also used to perform diagnosis, while we consider logical (i.e., untimed) models. Secondly, while [9] uses colored nets to obtain a more compact model of the diagnosed system, we use the basis markings technique to reduce the state space the diagnoser needs to explore. Finally, while in [9] both intermittent and permanent faults are considered, in our approach only permanent faults are taken into account. Note however, that intermittent faults could be introduced in our procedure extending it as follows. If the recovery event is observable a simple reset rule on the diagnosis state should be introduced. On

the contrary, if the recovery event is not observable a detection procedure on such an event, based on the same features of the fault detection procedure here presented, should be applied.

Other DES diagnosis approaches assume that faults are modeled either by unobservable transitions or by unobservable places, while observable but undistinguishable transitions always model regular behavior. The most significant works are mentioned in the following.

One of the first contributions is due to Benveniste *et al.* [1] who use a net unfolding approach for designing an on-line asynchronous diagnoser.

Wu and Hadjicostis [27] use redundancy into a given PN to enable fault detection and identification using algebraic decoding techniques. In this paper the authors consider two types of faults: place faults that corrupt the net marking, and transition faults that cause a not correct update of the marking after event occurrence. Although this approach is general, the net marking has to be periodically observable even if unobservable events occur. Analogously, Lefebvre and Delherm [15] investigate on the determination of the set of places that must be observed for the exact and immediate estimation of faults occurrence.

Genc and Lafortune [10] propose a diagnoser on the basis of a modular approach that performs the diagnosis of faults in each module. A communication system connects the different modules and updates the diagnosis information.

Jiroveanu and Boel [14] propose an algorithm for the model based design of a distributed protocol for fault detection and diagnosis for large systems. The overall process is modeled as time PN models that interact with each other via guarded transitions that become enabled only when certain conditions are satisfied.

Dotoli *et al.* [8] address the on-line fault detection of discrete event systems modeled by PNs. The paper recalls a previously proposed diagnoser that works on-line and employs an algorithm based on the definition and solution of some integer linear programming problems to decide whether the system behavior is normal or exhibits some possible faults.

In [23] Ramirez-Treviño *et al.* employ Interpreted Petri nets (IPNs) to model the system behavior that includes both events and states partially observable. Based on the IPN model derived from an on-line methodology, a scheme utilizing a solution of a programming problem is proposed to solve the problem of diagnosis. Moreover, the authors provide sufficient structural conditions for diagnosability of permanent faults based on the condition that any T-semiflow must contain all risky transitions. Then they extend the approach allowing a finite distance between risky transitions and any other transition. In [22] Ramirez-Treviño *et al.* use the relative distance concept introduced in [23] to present a new characterization providing sufficient conditions for diagnosability of partially observable IPNs. Polynomial time procedures for determining this area are presented enlarging the class of IPNs that can be characterized.

Ru and Hadjicostis [25] perform fault diagnosis assuming that certain transitions, including fault transitions, are silent and the content of certain places can be measured. What is interesting and original in this work is that a degree of confidence regarding the occurrence of the different

types of faults is calculated.

Ghazel *et al.* [11] present a procedure to refine the state estimation on the basis of timing information. This allows to obtain reliable predictions of possible future event scenarios and in particular on possible failure occurrences. This is obviously important in many real applications, such as transportation.

Lefebvre and Leclercq [16] propose an approach based on PNs that are used to design reference and faulty models. The main contribution concerns the design and identification of PN reference models according to a systematic statistical analysis of alarm sequences that are collected when the system is working. A "black box" approach is proposed, and no information concerning the internal structure of the system is required to design the reference model.

Mahulea *et al.* [17] investigate the effect of fluidization on fault diagnosis focusing on untimed continuous PNs. The authors define a diagnoser and prove that, given an observation, the resulting diagnosis state can be computed solving linear programming problems rather than integer programming problems as in the discrete case. The main advantages of fluidization is that it enables to deal with much more general PN structures and that the compact representation of the set of consistent markings using convex polytopes can be seen in some cases as an improvement in terms of computational complexity.

Finally, Qu *et al.* [21] propose an approach for the optimal design of fault-tolerant Petri net controllers. Given a system controller that is modeled by a PN, they present an approach for obtaining a fault-tolerant redundant Petri net controller that is able to retain the functionality and properties of the original controller and enable the fault detection and identification. They develop an algorithm that is able to design this fault-tolerant redundant controller in an optimal sense. The optimality is in terms of minimizing the sum of arc weights in the input and output incident matrices of the fault-tolerant controller.

3 Background on labeled Petri nets

In this section we recall the formalism used in the paper. For more details on PNs we refer to [19].

A *Place/Transition net* (P/T net) is a structure $N = (P, T, Pre, Post)$, where P is a set of m places; T is a set of n transitions; $Pre : P \times T \to \mathbb{N}$ and $Post : P \times T \to \mathbb{N}$ are the *pre*– and *post*– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M : P \to \mathbb{N}$ that assigns to each place of a P/T net a nonnegative integer number of tokens, represented by black dots. We denote $M(p)$ the marking of place p. A P/T *system* or *net system* $\langle N, M_0 \rangle$ is a net N with an initial marking M_0. A transition t is enabled at M iff $M \geq Pre(\cdot, t)$ and may fire yielding the marking $M' = M + C(\cdot, t)$. We write $M\ [\sigma\rangle$ to denote that the sequence of transitions $\sigma = t_{j_1} \cdots t_{j_k}$ is enabled at M, and we write $M\ [\sigma\rangle\ M'$ to denote that the firing of σ yields M'. We also write $t \in \sigma$ to denote that a transition t is

contained in σ. The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M_0) = \{\sigma \in T^* \mid M_0[\sigma\rangle\}$.

Given a sequence $\sigma \in T^*$, we call $\pi : T^* \to \mathbb{N}^n$ the function that associates with σ a vector $y \in \mathbb{N}^n$, named the *firing vector* of σ. In particular, $y = \pi(\sigma)$ is such that $y(t) = k$ if the transition t is contained k times in σ.

A marking M is *reachable* in $\langle N, M_0\rangle$ iff there exists a firing sequence σ such that $M_0\ [\sigma\rangle\ M$. The set of all markings reachable from M_0 defines the *reachability set* of $\langle N, M_0\rangle$ and is denoted $R(N, M_0)$. Finally, we denote $PR(N, M_0)$ the *potentially reachable set*, i.e., the set of all markings $M \in \mathbb{N}^m$ for which there exists a vector $y \in \mathbb{N}^n$ that satisfies the *state equation* $M = M_0 + C \cdot y$, i.e., $PR(N, M_0) = \{M \in \mathbb{N}^m \mid \exists\, y \in \mathbb{N}^n : M = M_0 + C \cdot y\}$. It holds that $R(N, M_0) \subseteq PR(N, M_0)$.

A PN having no directed circuits is called *acyclic*.

Theorem 1 [6] Let N be an acyclic PN.

(i) If the vector $y \in \mathbb{N}^n$ satisfies the equation $M_0 + C \cdot y \geq 0$ there exists a firing sequence σ firable from M_0 and such that the firing vector associated with σ is equal to y.

(ii) A marking M is reachable from M_0 iff there exists a nonnegative integer solution y satisfying the state equation $M = M_0 + C \cdot y$, i.e., $R(N, M_0) = PR(N, M_0)$.

A net system $\langle N, M_0\rangle$ is *bounded* if there exists a positive constant k such that, for $M \in R(N, M_0)$, $M(p) \leq k$.

A *labeling function* $\mathcal{L} : T \to E \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet E or the empty string ε.

4 Problem Setting

In this paper we solve the diagnosis problem for labeled PNs where faults can be modeled either by unobservable transitions or by observable undistinguishable events, i.e., the same label may be assigned to fault transitions and to transitions modeling regular observable behavior.

We denote T_o the set of transitions labeled with a symbol in E. Transitions in T_o are called *observable* because when they fire their label can be observed. We assume that the same label $l \in E$ can be associated with more than one transition. In particular, two transitions $t_1, t_2 \in T_o$ are called *undistinguishable* if they share the same label, i.e., $\mathcal{L}(t_1) = \mathcal{L}(t_2)$. The set of transitions sharing the same label l is denoted T_l. The set of observable transitions is partitioned into two subsets, namely

$$T_o = T_{o,f} \cup T_{o,reg}$$

where

- $T_{o,f}$ includes fault transitions that are observable,

- $T_{o,reg}$ includes all transitions relative to observable and regular events.

In general transitions in $T_{o,f}$ are undistinguishable with respect to transitions in $T_{o,reg}$ because they share the same label and it may occur that they are simultaneously enabled.

We denote T_u the set of transitions whose label is ε, i.e., $T_u = \{t \in T \mid \mathcal{L}(t) = \varepsilon\}$. Transitions in T_u are called *unobservable* or *silent*. The set of unobservable transitions is partitioned into two subsets, namely

$$T_u = T_{u,f} \cup T_{u,reg}$$

where

- $T_{u,f}$ includes fault transitions,
- $T_{u,reg}$ includes all transitions relative to unobservable but regular events.

The set of fault transitions

$$T_f = T_{u,f} \cup T_{o,f}$$

is further partitioned into r different subsets T_f^i, where $i = 1, \ldots, r$, that model the different fault classes.

In the following we denote C_u (C_o, $C_{o,f}$) the restriction of the incidence matrix to T_u (T_o, $T_{o,f}$) and denote n_u, n_o and $n_{o,f}$, respectively, the cardinality of the sets T_u, T_o and $T_{o,f}$. Moreover, given a sequence $\sigma \in T^*$, $P_u(\sigma)$, resp., $P_o(\sigma)$, $P_{o,f}(\sigma)$, denotes the projection of σ over T_u, resp., T_o, $T_{o,f}$.

5 Preliminary definitions and results

Let $w = P_o(\sigma)$ be the observed word of events associated with a sequence σ. Note that the length of a sequence σ (denoted $|\sigma|$) is always greater than or equal to the length of the corresponding word w (denoted $|w|$). In fact, if σ contains k' transitions in T_u then $|\sigma| = k' + |w|$.

Definition 2 [3] Let $\langle N, M_0 \rangle$ be a labeled net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in E^*$ be an observed word. We define

$$\mathcal{S}(w) = \{\sigma \in L(N, M_0) \mid P_o(\sigma) = w\}$$

the set of firing sequences *consistent* with $w \in E^*$, and

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \mid \exists\, \sigma \in \mathcal{S}(w) \ \wedge M_0[\sigma\rangle M\}$$

the set of markings *consistent* with $w \in E^*$. ■

In plain words, given an observation w, $\mathcal{S}(w)$ is the set of sequences that may have fired, while $\mathcal{C}(w)$ is the set of markings in which the system may actually be.

To solve a diagnosis problem, it is essential to be able to compute the set of sequences and markings consistent with a given observation w. In this section we recall some definitions and results that are necessary to characterize these sets without resorting to explicit enumeration.

5.1 Minimal explanations and minimal e-vectors

Definition 3 [5] Given a marking M and an observable transition $t \in T_o$, we define

$$\Sigma(M,t) = \{\sigma \in T_u^* \mid M[\sigma\rangle M',\ M' \geq Pre(\cdot,t)\}$$

the set of *explanations* of t at M, and

$$Y(M,t) = \pi(\Sigma(M,t))$$

the *e-vectors* (or *explanation vectors*), i.e., firing vectors associated with the explanations. ■

Thus $\Sigma(M,t)$ is the set of unobservable sequences whose firing at M enables t. Among the above sequences we want to select those whose firing vector is minimal. The firing vectors of these sequences are called *minimal e-vectors*.

Definition 4 [5] Given a marking M and a transition $t \in T_o$, we define

$$\Sigma_{\min}(M,t) = \{\sigma \in \Sigma(M,t) \mid \nexists\, \sigma' \in \Sigma(M,t) : \pi(\sigma') \lneq \pi(\sigma)\}$$

the set of *minimal explanations* of t at M, and we define

$$Y_{\min}(M,t) = \pi(\Sigma_{\min}(M,t))$$

the corresponding set of *minimal e-vectors*. ■

In [6] it was shown that, if the unobservable subnet is acyclic and backward conflict-free, then $|Y_{\min}(M,t)| = 1$.

Different approaches can be used to compute $Y_{\min}(M,t)$, e.g., [2, 13, 3]. In particular, in [3] we proposed an approach that simply requires algebraic manipulations and is inspired by the procedure proposed by Martinez and Silva [18] for the computation of minimal P-invariants.

In the case of labeled PNs what we observe are symbols in E. Thus, it is useful to compute the following sets.

Definition 5 [3] Given a marking M and an observation $l \in E$, we define the set of *minimal explanations of l at M* as

$$\hat{\Sigma}_{\min}(M,l) = \cup_{t \in T_l} \cup_{\sigma \in \Sigma_{\min}(M,t)} (t,\sigma),$$

i.e., the set of pairs (transition labeled l, corresponding minimal explanation), and we define the set of *minimal e-vectors of l at M* as

$$\hat{Y}_{\min}(M,l) = \cup_{t \in T_l} \cup_{e \in Y_{\min}(M,t)} (t,e),$$

i.e., the set of pairs (transition labeled l, corresponding minimal e-vector). ■

Thus, $\hat{\Sigma}_{\min}(M,l)$ is the set of pairs whose first element is the transition labeled l and whose second element is the corresponding minimal explanation $\sigma \in \Sigma_{\min}(M,t)$, namely the corresponding sequence of unobservable transitions whose firing at M enables l and whose firing vector is minimal. Moreover, $\hat{Y}_{\min}(M,l)$ is the set of pairs whose first element is the transition labeled l and whose second element is the firing vector $e \in Y_{\min}(M,t)$ corresponding to the second element in $\hat{\Sigma}_{\min}(M,l)$.

Obviously, $\hat{\Sigma}_{\min}(M,l)$ and $\hat{Y}_{\min}(M,l)$ are a generalization of the sets of minimal explanations and minimal e-vectors introduced for unlabeled PNs with unobservable transitions. Moreover, in the above sets $\hat{\Sigma}_{\min}(M,l)$ and $\hat{Y}_{\min}(M,l)$ different sequences σ and different e-vectors e, respectively, could be associated in general with the same $t \in T_l$.

5.2 Basis markings and j-vectors

Given a sequence of observed events $w \in E^*$, a basis marking M_b is a marking reached from M_0 with the firing of the observed word w and all unobservable transitions whose firing is strictly necessary to enable w. Such a sequence of unobservable transitions is called *justification.* Note that, in general several sequences $\sigma_o \in T_o^*$ may correspond to the same w, i.e., there are several sequences of observable transitions such that $\mathcal{L}(\sigma_o) = w$ that may have actually fired. Moreover, in general, to any of such sequences σ_o a different sequence of unobservable transitions interleaved with it is necessary to make it firable at the initial marking.

Definition 6 Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in E^*$ be a given observation. We define

$$\begin{aligned}\hat{\mathcal{J}}(w) \quad &= \{\ (\sigma_o, \sigma_u),\ \sigma_o \in T_o^*,\ \mathcal{L}(\sigma_o) = w,\ \sigma_u \in T_u^*\ \mid \\ &\quad [\exists \sigma \in \mathcal{S}(w)\ :\ \sigma_o = P_o(\sigma),\ \sigma_u = P_u(\sigma)] \wedge \\ &\quad [\nexists \sigma' \in \mathcal{S}(w) :\ \sigma_o = P_o(\sigma'),\ \sigma'_u = P_u(\sigma') \wedge \\ &\qquad\qquad \pi(\sigma'_u) \lneq \pi(\sigma_u)]\}\end{aligned}$$

the set of pairs (sequence $\sigma_o \in T_o^*$ with $\mathcal{L}(\sigma_o) = w$; corresponding *justification* of w). Moreover, we define

$$\begin{aligned}\hat{Y}_{\min}(M_0, w) = \{(\sigma_o, y),\ &\sigma_o \in T_o^*, \mathcal{L}(\sigma_o) = w, y \in \mathbb{N}^{n_u}\ \mid \\ &\exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w) : \pi(\sigma_u) = y\}\end{aligned}$$

the set of pairs (sequence $\sigma_o \in T_o^*$ with $\mathcal{L}(\sigma_o) = w$; corresponding *j-vector*). ■

In simple words, $\hat{\mathcal{J}}(w)$ is the set of pairs whose first element is the sequence $\sigma_o \in T_o^*$ labeled w and whose second element is the corresponding sequence of unobservable transitions interleaved with σ_o whose firing enables σ_o and whose firing vector is minimal. The firing vectors of these sequences are called *j-vectors.*

Definition 7 [3] Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let w be a given observation and $(\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)$ be

a generic pair (sequence of observable transitions labeled w; corresponding justification). The marking

$$M_b = M_0 + C_u \cdot y + C_o \cdot y', \qquad y = \pi(\sigma_u), \;\; y' = \pi(\sigma_o),$$

i.e., the marking reached firing σ_o interleaved with the justification σ_u, is called *basis marking* and y is called its *j-vector* (or *justification-vector*). ■

Obviously, because in general more than one justification exists for a word w (the set $\hat{\mathcal{J}}(w)$ is generally not a singleton), the basis marking may be not unique as well.

Proposition 8 [3] Given a net system $\langle N, M_0 \rangle$ with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Assume that the unobservable subnet is acyclic. Let $w = w'l$ be a given observation. It holds:

$$\begin{aligned} \hat{Y}_{\min}(M_0, w'l) = \{(\sigma_o, y) \;\; | \;\; & \sigma_o = \sigma_o' t \wedge y = y' + e \;\; : \\ & (\sigma_o', y') \in \hat{Y}_{\min}(M_0, w'), \\ & (t, e) \in \hat{Y}_{\min}(M_b', l) \text{ and } \mathcal{L}(t) = l\}, \end{aligned}$$

where $M_b' = M_0 + C_u \cdot y' + C_o \cdot \pi(\sigma_o')$.

6 New definitions and characterization of the set of consistent markings

In this section we first introduce some new definitions that are fundamental in the computation of the diagnosis states. Then, we provide a linear algebraic characterization of the set of consistent markings.

Definition 9 Let $\langle N, M_0 \rangle$ be a net system with labeling function $\mathcal{L} : T \to E \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in E^*$ be an observed word. We define

$$\begin{aligned} \bar{\mathcal{M}}(w) = \{(M, y, \gamma) \mid \; & (\exists \sigma \in \mathcal{S}(w) \;\; : \;\; M_0[\sigma\rangle M) \wedge \\ & (\exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w) \;\; : \;\; \sigma_o = P_o(\sigma), \\ & \quad \sigma_u = P_u(\sigma), \;\; y = \pi(\sigma_u)) \wedge \\ & \sigma_{o,f} = P_{o,f}(\sigma), \;\; \gamma = \pi(\sigma_{o,f})\} \end{aligned}$$

where $\gamma = \pi(\sigma_{o,f})$ is called γ-*vector* of sequence $\sigma_{o,f}$. ■

In simple words the set $\bar{\mathcal{M}}(w)$ is the set of triples (basis marking, relative j-vector, relative γ-vector) that are *consistent* with $w \in E^*$. It keeps track of all the information really significant when performing diagnosis in the considered framework, namely: the basis markings that can be reached after the firing of w, the firing vectors relative to sequences of unobservable transitions that may have fired to reach them, and the sequences of fault observable transitions that may have actually fired.

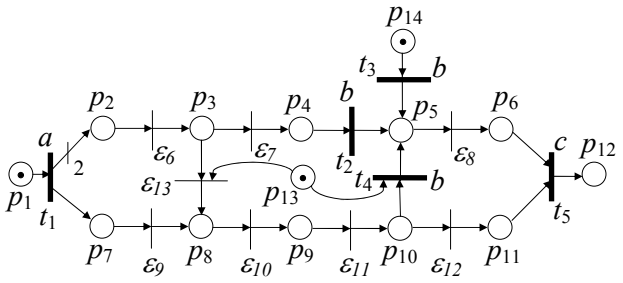

Figure 2: The PN system considered in Sections 6 to 8.

Example 10 Let us consider the Petri net system in Fig. 2. This net is similar to the one used in [5]. It represents a production line processing damaged parts, namely metallic slabs where two plates instead of one, have been placed in a wrong decentralized position. When a damaged part is ready to be processed (tokens in p_1) slabs and plates are separated (transition t_1) and the two plates are sent in the upper line (modeled by places p_2, p_3, p_4, p_5, p_6), while the slab is sent in the lower line (modeled by places p_7, p_8, p_9, p_{10}, p_{11}). In the two lines parts are processed, namely smoothed, cleaned up, painted and polished (this corresponds to the firing of transitions t_2 and ε_6 to ε_{12}). In particular, in the upper line a signal is produced every time a part is painted (part entering in p_5). Finally one metallic plate is inserted in the slab in the correct position (transition t_5). The second plate is used again for other slabs, but this part of the process is not modeled here. We assume that two different fault behaviors (fault classes) may occur: (1) either a plate of a different type (e.g., different material, or different size) enters the upper line or a slab is moved to the upper line ($T_f^2 = \{t_3, t_4\}$); (2) a plate is moved to the lower line ($T_f^1 = \{\varepsilon_{13}\}$).

We assume that $T_o = \{t_1, t_2, t_3, t_4, t_5\}$, $T_{o,reg} = \{t_1, t_2, t_5\}$, $T_{o,f} = \{t_3, t_4\}$ and $T_u = \{\varepsilon_6, \varepsilon_7, \varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}, \varepsilon_{13}\}$, $T_{u,reg} = \{\varepsilon_6, \varepsilon_7, \varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}\}$, $T_{u,f} = \{\varepsilon_{13}\}$, where for a better understanding unobservable transitions have been denoted ε_i rather than t_i. The labeling function is defined as follows: $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_2) = \mathcal{L}(t_3) = \mathcal{L}(t_4) = b$ and $\mathcal{L}(t_5) = c$.

Let us assume $w = a$. In this case $\hat{\mathcal{J}}(w) = \{(t_1, \varepsilon)\}$, $\hat{Y}_{min}(M_0, w) = \{(t_1, \vec{0})\}$, $\sigma_{o,f,1} = P_{o,f}(t_1) = \varepsilon$, $\gamma_1 = \pi(\sigma_{o,f,1}) = [0\ 0]^T$. The set of basis markings is a singleton and is equal to $M_b^1 = [0\ 2\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$, thus $\bar{\mathcal{M}}(a) = \{(M_b^1, \vec{0}, [0\ 0]^T)\}$.

Now let $w = ab$. In this case $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon_6\varepsilon_7), (t_1t_3, \varepsilon), (t_1t_4, \varepsilon_9\varepsilon_{10}\varepsilon_{11}\}$, $\hat{Y}_{min}(M_0, w) = \{(t_1t_2, e_1), (t_1t_3, \vec{0}), (t_1t_4, e_2)\}$, where $e_1 = [1\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T$ and $e_2 = [0\ 0\ 0\ 1\ 1\ 1\ 0\ 0]^T$, $\sigma_{o,f,1} = P_{o,f}(t_1t_2) = \varepsilon$, $\sigma_{o,f,2} = P_{o,f}(t_1t_3) = t_3, \sigma_{o,f,3} = P_{o,f}(t_1t_4) = t_4$, $\gamma_1 = \pi(\sigma_{o,f,1}) = [0\ 0]^T$, $\gamma_2 = \pi(\sigma_{o,f,2}) = [1\ 0]^T$, $\gamma_3 = \pi(\sigma_{o,f,3}) = [0\ 1]^T$. The basis markings are respectively $M_b^2 = [0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$, $M_b^3 = [0\ 2\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$, $M_b^4 = [0\ 2\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T$. Thus $\bar{\mathcal{M}}(ab) = \{(M_b^2, e_1, [0\ 0]^T), (M_b^3, \vec{0}, [1\ 0]^T), (M_b^4, e_2, [0\ 1]^T)\}$. ■

In the rest of the paper we assume that the following assumption holds:

(A) The unobservable subnet is acyclic.

Under assumption (A) the set $\bar{\mathcal{M}}(w)$ can be recursively constructed using the following algorithm.

Algorithm 11 [Computation of the set $\bar{\mathcal{M}}(w)$]

1. Let $w = \varepsilon$.
2. Let $\bar{\mathcal{M}}(w) = \{(M_0, \vec{0}, \vec{0})\}$.
3. Wait until a new label l is observed.
4. Let $w' = w$ and $w = w'l$.
5. Let $\bar{\mathcal{M}}(w) = \emptyset$.
6. For all M' such that $(M', y', \gamma') \in \bar{\mathcal{M}}(w')$, do
  6.1. for all $t \in T_l$, do
    6.1.1. for all $e \in Y_{\min}(M', t)$, do
    6.1.1.1. let $M = M' + C_u \cdot e + C(\cdot, t)$,
    6.1.1.2. for all y' such that $(M', y', \gamma') \in \bar{\mathcal{M}}(w')$, do
      6.1.2.1. let $y = y' + e$,
      6.1.2.2. if $t \in T_{o,f}$, let $\gamma = \gamma + \vec{t}$,
      6.1.2.3. let $\bar{\mathcal{M}}(w) = \bar{\mathcal{M}}(w) \cup \{(M, y, \gamma)\}$.
7. Goto Step 3.

■

In simple words, the above algorithm can be explained as follows. We assume that a certain word w (that is equal to the empty string at the initial step) has been observed. Then, a new observable t fires and we observe its label $l = \mathcal{L}(t)$. We consider all basis markings at the observation w' before the firing of t, and we select among them those that may have allowed the firing of at least one transition $t \in T_l$, also taking into account that this may have required the firing of appropriate sequences of unobservable transitions. In particular, we focus on the minimal explanations, and thus on the corresponding minimal e-vectors (Step 6.1.1). Finally, we update the set $\bar{\mathcal{M}}(w)$ including all triples of new basis markings, j-vectors and γ-vectors, taking into account that for each basis marking at w' it may correspond more than one j-vector and more than one γ-vector.

Definition 12 Let $\langle N, M_0 \rangle$ be a net system where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Assume that the unobservable subnet is acyclic. Let $w \in T_o^*$ be an observed word. We denote

$$\mathcal{M}_{basis}(w) = \{M \in \mathbb{N}^m \mid \exists y \in \mathbb{N}^{n_u},\ \exists \gamma \in \mathbb{N}^{n_{o,f}},\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)\}$$

the set of basis markings at w. Moreover, we denote

$$\mathcal{M}_{basis} = \bigcup_{w \in T_o^*} \mathcal{M}_{basis}(w)$$

the set of all basis markings for any observation w. ■

Note that if the net system is bounded then the set $\mathcal{M}_{basis}$ is *finite* being the set of basis markings a subset of the reachability set.

Finally, the set of consistent markings in terms of basis markings can be characterized as follows.

Theorem 13 [3] Let us consider a net system $\langle N, M_0 \rangle$ whose unobservable subnet is acyclic. For any $w \in E^*$ it holds that

$$\mathcal{C}(w) = \{M \in \mathbb{N}^m \quad | \quad M = M_b + C_u \cdot y \ : y \geq \vec{0}, \\ M_b \in \mathcal{M}_{basis}(w)\}.$$

7 Diagnosis using Petri nets

In this section we solve the diagnosis problem, i.e., the problem of identifying the occurrence of a fault given an observation, in the setting introduced in Section 4. The following definition introduces the notion of *diagnoser*.

Definition 14 A *diagnoser* is a function $\Delta : E^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \to \{0, 1, 2, 3\}$ that associates with each observation $w \in E^*$ and with each fault class T_f^i, $i = 1, \ldots, r$, a *diagnosis state*.

- $\Delta(w, T_f^i) = 0$ if for all $\sigma \in \mathcal{S}(w)$ and for all $t_f \in T_f^i$ it holds $t_f \notin \sigma$.

In such a case the ith fault cannot have occurred, because none of the firing sequences consistent with the observation contains fault transitions of class i.

- $\Delta(w, T_f^i) = 1$ if:

(i) there exist $\sigma \in \mathcal{S}(w)$ and $t_f \in T_f^i$ such that $t_f \in \sigma$ but

(ii) for all $(\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)$ and for all $t_f \in T_f^i$ it holds that $t_f \notin \sigma_u$ and $t_f \notin \sigma_o$.

In such a case a fault transition of class i may have occurred but it is neither contained in any justification of w, nor it is contained in a sequence of observed transitions labeled w.

- $\Delta(w, T_f^i) = 2$ if there exist $(\sigma_o, \sigma_u), (\sigma'_o, \sigma'_u) \in \hat{\mathcal{J}}(w)$ such that

(i) there exists $t_f \in T_f^i$ such that: either $t_f \in \sigma_u$ or $t_f \in \sigma_o$ (or both);

(ii) for all $t_f \in T_f^i$, $t_f \notin \sigma'_u$ and $t_f \notin \sigma'_o$.

In such a case a fault transition of class i is either contained in one justification of w or in a sequence of observable transitions labeled w (or both), but there also exists at least one other sequence of transitions that is consistent with the observation w, that does not contain fault transitions and whose justifications do not contain fault transitions as well.

- $\Delta(w, T_f^i) = 3$ if for all $\sigma \in \mathcal{S}(w)$ there exists $t_f \in T_f^i$ such that $t_f \in \sigma$.

In such a case the ith fault must have occurred, because all firable sequences consistent with the observation contain at least one fault in T_f^i. ■

The following example clarifies the notion of *diagnoser*.

Example 15 Let us consider the PN in Fig. 2 previously introduced in Example 10, where $T_f^1 = T_{o,f} = \{t_3, t_4\}$ and $T_f^2 = T_{u,f} = \{\varepsilon_{13}\}$.

Let us first assume that no event is observed, i.e., $w = \varepsilon$. Then $\Delta(w, T_f^1) = \Delta(w, T_f^2) = 0$, being $\hat{\mathcal{J}}(w) = \{(\varepsilon, \varepsilon)\}$ and $\mathcal{S}(w) = \{\varepsilon\}$. This means that no fault may have occurred.

Let us now observe $w = a$. Then $\Delta(w, T_f^1) = 0$ and $\Delta(w, T_f^2) = 1$, being $\hat{\mathcal{J}}(w) = \{(t_1, \varepsilon)\}$ and $t_1\varepsilon_6\varepsilon_{13} \in \mathcal{S}(w)$. This means that the fault transition ε_{13} belonging to the second fault class may have occurred (but it is not contained in any justification), while no fault of the first fault class may have occurred.

Finally, let $w = ab$. Then $\Delta(w, T_f^1) = 2$ and $\Delta(w, T_f^2) = 1$, being $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon_6\varepsilon_7), (t_1t_3, \varepsilon), (t_1t_4, \varepsilon_9\varepsilon_{10}\varepsilon_{11}\}$ and $t_1\varepsilon_6\varepsilon_{13}t_3 \in \mathcal{S}(w)$. In fact, for the first fault class a fault transition is contained in a sequence of observable transitions labeled w but there also exist one other sequence of transitions that is consistent with the observation w, that does not contain fault transitions (since the first fault class contains no unobservable fault transitions there is no need to check also the justifications); while for the second fault class the fault transition ε_{13} may have occurred but it is not contained in any justification. ■

The following proposition presents how the diagnosis states can be characterized analyzing basis markings and justifications.

Proposition 16 Consider an observed word $w \in E^*$.

• $\Delta(w, T_f^i) \in \{0, 1\}$ iff for all $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it holds that: for all $t_f \in T_f^i \cap T_{u,f}$, $y(t_f) = 0$, and for all $t_f \in T_f^i \cap T_{o,f}$, $\gamma(t_f) = 0$.

• $\Delta(w, T_f^i) = 2$ iff there exist $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $(M', y', \gamma') \in \bar{\mathcal{M}}(w)$ such that:
(i) either there exists $t_f \in T_f^i \cap T_{u,f}$ such that $y(t_f) > 0$ or there exists $t_f \in T_f^i \cap T_{o,f}$ such that $\gamma(t_f) > 0$ (or both),
(ii) for all $t_f \in T_f^i \cap T_{u,f}$ it is $y'(t_f) = 0$, and for all $t_f \in T_f^i \cap T_{o,f}$ it is $\gamma'(t_f) = 0$.

• $\Delta(w, T_f^i) = 3$ iff for all $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ either there exists $t_f \in T_f^i \cap T_{u,f}$ such that $y(t_f) > 0$ or there exists $t_f \in T_f^i \cap T_{o,f}$ such that $\gamma(t_f) > 0$ (or both).

Proof By Definition 14, $\Delta(w, T_f^i) = 0$ iff no fault transition $t_f \in T_f^i$ is contained in any firing sequence that is consistent with w, while $\Delta(w, T_f^i) = 1$ iff no fault $t_f \in T_f^i$ is contained in any justification of w and no observed label in w may correspond to a transition in $T_f^i \cap T_{o,f}$, but there exists at least one sequence that is consistent with w that contains a transition $t_f \in T_f^i \cup T_{u,f}$. Therefore, a necessary and sufficient condition to have $\Delta(w, T_f^i) \in \{0, 1\}$ is that for all j-vectors y at w and all $t_f \in T_f^i$ it is $y(t_f) = 0$ and $\gamma(t_f) = 0$, thus proving the first item.

Analogously, $\Delta(w, T_f^i) = 2$ either if a transition $t_f \in T_f^i$ is contained in at least one (but not in all) justification of w, or at least one (but not all) sequence of observable transitions that may have actually fired contains a transition in $T_f^i \cap T_{o,f}$, or both cases occur. Thus, to have $\Delta(w, T_f^i) = 2$ it is necessary and sufficient that either there exists at least one j-vector y or at least one γ-vector γ (or both) that contain at least one transition $t_f \in T_f^i$, and one j-vector y' and the corresponding γ-vector γ' that do not contain transitions $t_f \in T_f^i$, thus proving the second item.

Finally, given an observed word w and a fault class T_f^i we have $\Delta(w, T_f^i) = 3$ if all firable sequences consistent with w contain at least one fault transition $t_f \in T_f^i$. Thus, to have $\Delta(w, T_f^i) = 3$ it is necessary and sufficient that either all the justifications contain at least one transition $t_f \in T_f^i$, or all the γ-vectors relative to justifications containing no transition in T_f^i, contain themselves a transition in T_f^i (or both conditions hold). This proves the third item. □

In plain words, the diagnosis state $\Delta(w, T_f^i)$ is either 0 or 1 iff for all triples (M, y, γ) consistent with w both y and γ have null entries associated with fault transitions in the ith class. The diagnosis state $\Delta(w, T_f^i)$ is equal to 2 iff either a justification or a γ-vector (or both) contain a non null entry relative to a transition in the ith fault class, but there also exists at least a triple (M', y', γ') consistent with w such that both y' and γ' do not contain fault transitions in the ith class. Finally, $\Delta(w, T_f^i)$ is equal to 3 iff for all triples (M, y, γ) consistent with w either y or γ (or both) are non null for at least one entry relative to a fault transition in the ith class.

The following proposition shows how to distinguish between diagnosis states 0 and 1.

Proposition 17 For a PN whose unobservable subnet is *acyclic*, let $w \in E^*$ be an observed word such that for all $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it holds $y(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{u,f}$ and $\gamma(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{o,f}$. Let us consider the constraint set

$$\mathcal{T}(M, T_f^i) \quad = \quad \begin{cases} M + C_u \cdot z \geq \vec{0}, \\ \displaystyle\sum_{t_f \in T_f^i} z(t_f) > 0, \\ z \in \mathbb{N}^{n_u}. \end{cases} \tag{1}$$

- $\Delta(w, T_f^i) = 0$ if $\forall \ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ the constraint set (1) is not feasible.
- $\Delta(w, T_f^i) = 1$ if $\exists \ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ such that the constraint set (1) is feasible.

Proof Let $w \in E^*$ be an observed word such that $\forall (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it is $y(t_f) = 0 \, \forall \, t_f \in T_f^i \cap T_{u,f}$ and $\gamma(t_f) = 0 \ \forall \ t_f \in T_f^i \cap T_{o,f}$. By Definition 14 it immediately follows that:

- $\Delta(w, T_f^i) = 0$ if $\forall (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $\forall t_f \in T_f^i$ there does not exist a sequence $\sigma \in T_u^*$ such that $M[\sigma\rangle$ and $t_f \in \sigma$;
- $\Delta(w, T_f^i) = 1$ if $\exists$ at least one $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and a sequence $\sigma \in T_u^*$ such that for at least one $t_f \in T_f^i$, $M[\sigma\rangle$ and $t_f \in \sigma$.

Now, if a PN is *acyclic* the state equation gives necessary and sufficient conditions for marking reachability [19]. Therefore, being the unobservable subnet acyclic, the set $\mathcal{T}(M, T_f^i)$ characterizes the reachability set of the unobservable net at marking M via firing sequences that contain at least one faulty transition. Thus, due to this fact and the above two items, we can conclude that there exists a sequence containing a transition $t_f \in T_f^i$ firable at M on the unobservable subnet if and only if $\mathcal{T}(M, T_f^i)$ is feasible. □

In plain words, the diagnosis state $\Delta(w, T_f^i)$ is equal to 0 if for all triples (M, y, γ) consistent with w, the constraint set (1) is unfeasible, namely starting from any M there does not exist a firable sequence of unobservable transitions containing a fault transition in the ith class. If this is not the case $\Delta(w, T_f^i)$ is equal to 1.

On the basis of the above two results, if the unobservable subnet is acyclic, diagnosis may be carried out by simply looking at the set $\bar{\mathcal{M}}(w)$ for any observed word w and, should the diagnosis state be either 0 or 1, by additionally evaluating the feasibility of the corresponding integer constraint set (1).

Example 18 Let us consider again the PN in Fig. 2 where $T_f^1 = T_{o,f} = \{t_3, t_4\}$ and $T_f^2 = T_{u,f} = \{\varepsilon_{13}\}$.

Let $w = a$. In this case $\bar{\mathcal{M}}(w) = \{(M_b^1, \vec{0}, [0\ 0]^T)\}$, where M_b^1 is reported in Example 10, and $\mathcal{T}(M_b^1, T_f^i)$ is not feasible for $T_f^i = T_f^1$ while it is feasible for $T_f^i = T_f^2$. Thus it is $\Delta(w, T_f^1) = 0$ and $\Delta(w, T_f^2) = 1$.

Let $w = ab$. It is $\Delta(w, T_f^1) = 2$ and $\Delta(w, T_f^2) = 1$ being $\bar{\mathcal{M}}(w) = \{(M_b^2, e_1, [0\ 0]^T), (M_b^3, \vec{0}, [1\ 0]^T), (M_b^4, e_2, [0\ 1]^T)\}$, where M_b^2, M_b^3, M_b^4, e_1 and e_2 are reported in Example 10, and $\mathcal{T}(M_b^i, T_f^2)$ is feasible for $i \in \{3, 4\}$. ■

8 Basis Reachability Graph

In this section we show that, as in the case where fault events may only correspond to silent events [5, 3], if the considered net system is bounded, the most burdensome part of the procedure can be moved off-line defining a graph called *Basis Reachability Graph* (BRG).

Definition 19 The BRG is a deterministic graph that has as many nodes as the number of possible basis markings.

To each node is associated a different basis marking M and a row vector with as many entries as the number of fault classes. The i-th entry of this vector may only take binary values: 1 if $\mathcal{T}(M, T_f^i)$ is feasible, 0 otherwise.

Arcs are labeled with observable events in E, e-vectors and vectors $z \in \{0, 1\}^{n_{o,f}}$ where z are binary vectors with as many entries as the number $n_{o,f}$ of transitions in $T_{o,f}$: if the current label l is relative to a transition $t \in T_{o,f}$, then the only non zero entry of z is $z(t)$, otherwise if $t \in T_{o,reg}$, z is a zeros' vector. More precisely, an arc exists from a node containing the basis marking M to a node containing the basis marking M' if and only if there exists a transition t for which an explanation exists at M and the firing of t and one of its minimal explanations leads to M'. The arc going from M to M' is labeled $(\mathcal{L}(t), e, z)$, where $e \in Y_{\min}(M, t)$ and $M' = M + C_u \cdot e + C(\cdot, t)$. ■

Note that the number of nodes of the BRG is always finite being the set of basis markings a subset of the set of reachable markings, that is finite being the net bounded. Moreover, the row

vector of binary values associated with the nodes of the BRG allows us to distinguish between the diagnosis state 1 or 0.

The main steps for the computation of the BRG in the case of labeled PNs are summarized in the following algorithm.

Algorithm 20 [Computation of the BRG]

1. Label the initial node (M_0, x_0) where $\forall i = 1, \ldots, r$,

$$x_0(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}(M_0, T_f^i) \text{ is feasible,} \\ 0 & \text{otherwise.} \end{cases}$$

Assign no tag to it.

2. While nodes with no tag exist

select a node with no tag and do

2.1. let M be the marking in the node (M, x),

2.2. for all $l \in E$

2.2.1. for all $t : \mathcal{L}(t) = l \wedge Y_{\min}(M, t) \neq \emptyset$, do

- for all $e \in Y_{\min}(M, t)$, do
  - let $M' = M + C_u \cdot e + C(\cdot, t)$,
  - if $\nexists$ a node (M, x) with $M = M'$, do
    - add a new node to the graph containing (M', x') where $\forall i = 1, \ldots, r$,

$$x'(T_f^i) = \begin{cases} 1 & \text{if } \mathcal{T}(M', T_f^i) \text{ is feasible,} \\ 0 & \text{otherwise.} \end{cases}$$

and arc (l, e, z) from (M, x) to (M', x')

where $\forall i = 1, \ldots, r$, $z_i = \begin{cases} 1 & \text{if } t \in T_{o,f} \\ 0 & \text{otherwise} \end{cases}$

  - else
    - add arc (l, e, z) from (M, x) to (M', x') if it does not exist yet

where $\forall i = 1, \ldots, r$, $z_i = \begin{cases} 1 & \text{if } t \in T_{o,f} \\ 0 & \text{otherwise} \end{cases}$

2.3. tag the node "old".

3. Remove all tags. ■

The algorithm constructs the BRG starting from the initial node to which it corresponds the initial marking and a binary vector defining which classes of fault may occur at M_0. Now, we consider all the labels $l \in E$ such that there exists a transition t with $\mathcal{L}(t) = l$ for which a minimal explanation at M_0 exists. For any of these transitions we compute the marking resulting from firing t at $M_0 + C_u \cdot e$, for any $e \in Y_{\min}(M_0, t)$. If a pair (marking, binary vector) not contained in the previous nodes is obtained, a new node is added to the graph. The arc going from the initial node to the new node is labeled (l, e, z) where z keeps track of the label l that may be associated with a fault transition. The procedure is iterated until all basis markings have been considered. Note that, our approach always requires to enumerate a state space that is a subset (usually

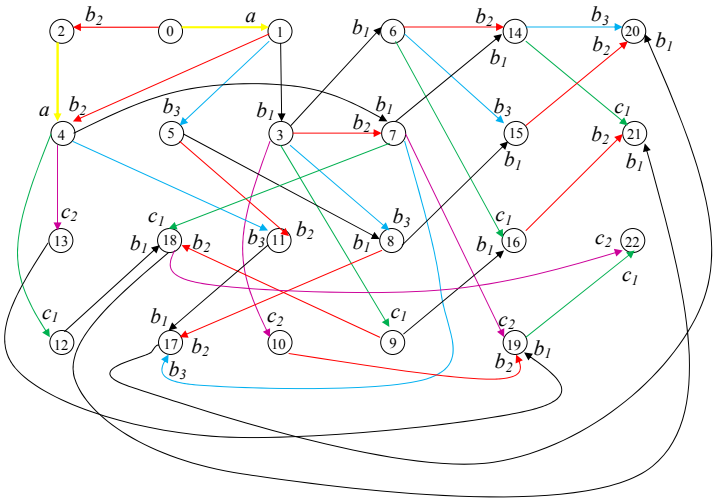

Figure 3: The BRG of the PN in Fig. 2.

a strict subset) of the reachability space. However, as in general for diagnosis approaches, the combinatory explosion cannot be avoided.

Example 21 Let us consider again the PN system in Fig. 2 where $T_o = \{t_1, t_2, t_3, t_4, t_5\}$, $T_{o,reg} = \{t_1, t_2, t_5\}$, $T_{o,f} = \{t_3, t_4\}$, $T_u = \{\varepsilon_6, \varepsilon_7, \varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}, \varepsilon_{13}\}$, $T_{u,reg} = \{\varepsilon_6, \varepsilon_7, \varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}\}$, $T_{u,f} = \{\varepsilon_{13}\}$ and $T_f^1 = T_{o,f} = \{t_3, t_4\}$ and $T_f^2 = T_{u,f} = \{\varepsilon_{13}\}$. The labeling function is defined as follows: $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_2) = \mathcal{L}(t_3) = \mathcal{L}(t_4) = b$ and $\mathcal{L}(t_5) = c$.

The BRG is shown in Fig. 3 where the nodes and arcs are described in Tables 1 and 2. For simplicity of notation, to the ith node it corresponds the ith basis marking. Each node contains a different basis marking and a two entries vector, because there are two fault classes. The first entry is always equal to 0 because $\mathcal{T}(M_b^i, T_f^1)$ is not feasible for all M_b^i since the first fault class does not contain unobservable faulty transitions. As an example, [0 0] is associated with M_b^0 because $\mathcal{T}(M_b^0, T_f^2)$ is not feasible, while [0 1] is associated with M_b^1 because $\mathcal{T}(M_b^1, T_f^2)$ is feasible. Node 1 has three different output arcs labeled b. Arc b_1 goes from node 1 to node 3, b_2 goes from 1 to 4 and b_3 goes from 1 to 5. This means that basis markings M_b^3, M_b^4, M_b^5 are reached firing a transition labeled b at M_b^1: M_b^3 is reached firing $t_2 \in T_{o,reg}$ while M_b^4 and M_b^5 are respectively reached firing t_3 and $t_4 \in T_{o,f}$, thus $z_{b_1} = [0\ 0]^T$, $z_{b_2} = [1\ 0]^T$ and $z_{b_3} = [0\ 1]^T$. ■

The following algorithm summarizes the main steps of the on-line diagnosis carried out by looking at the BRG.

Algorithm 22 [Diagnosis using the BRG]

1. Let $w = \varepsilon$.
2. Let $\bar{\mathcal{M}}(w) = \{(M_0, \vec{0}, \vec{0})\}$.
3. Wait until a new observable transition fires.
Let l be the observed event.

Node	Basis Marking	x
0	$[1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$	$[0\ 0]$
1	$[0\ 2\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$	$[0\ 1]$
2	$[1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$	$[0\ 0]$
3	$[0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$	$[0\ 1]$
4	$[0\ 2\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$	$[0\ 1]$
5	$[0\ 2\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T$	$[0\ 0]$
6	$[0\ 0\ 0\ 0\ 2\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]^T$	$[0\ 0]$
7	$[0\ 1\ 0\ 0\ 2\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$	$[0\ 1]$
8	$[0\ 1\ 0\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T$	$[0\ 0]$
9	$[0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1]^T$	$[0\ 1]$
10	$[0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1]^T$	$[0\ 0]$
11	$[0\ 2\ 0\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$	$[0\ 0]$
12	$[0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0]^T$	$[0\ 1]$
13	$[0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0]^T$	$[0\ 0]$
14	$[0\ 0\ 0\ 0\ 3\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0]^T$	$[0\ 0]$
15	$[0\ 0\ 0\ 0\ 3\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]^T$	$[0\ 0]$
16	$[0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1]^T$	$[0\ 0]$
17	$[0\ 1\ 0\ 0\ 3\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$	$[0\ 0]$
18	$[0\ 1\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0]^T$	$[0\ 1]$
19	$[0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ ]^T$	$[0\ 0]$
20	$[0\ 0\ 0\ 0\ 4\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$	$[0\ 0]$
21	$[0\ 0\ 0\ 0\ 2\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0]^T$	$[0\ 0]$
22	$[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 2\ 0\ 0]^T$	$[0\ 0]$

Table 1: The nodes of the BRG in Fig. 3.

Arc Name	Trans. label	e-vector	z
a	a	$[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$	$[0\ 0]^T$
b_1	b	$[1\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T$	$[0\ 0]^T$
b_2	b	$[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]^T$	$[1\ 0]^T$
b_3	b	$[0\ 0\ 0\ 1\ 1\ 1\ 0\ 0]^T$	$[0\ 1]^T$
c_1	c	$[0\ 0\ 1\ 1\ 1\ 1\ 1\ 0]^T$	$[0\ 0]^T$
c_2	c	$[1\ 0\ 1\ 0\ 1\ 1\ 1\ 1]^T$	$[0\ 0]^T$

Table 2: The arcs of the BRG in Fig. 3.

4. Let $w' = w$ and $w = w'l$.
5. Let $\bar{\mathcal{M}}(w) = \emptyset$, **[Computation of $\bar{\mathcal{M}}(w)$]**
6. For all nodes containing $M' : (M', y', \gamma') \in \bar{\mathcal{M}}(w')$, do
6.1. for all arcs exiting from the node with M', do
6.1.1. let M be the marking of the output node,
e be the minimal e-vector on the edge, and
z be the third vector on the edge (see Def. 19)
from M' to M,
6.1.2. for all y' such that $(M', y', \gamma') \in \bar{\mathcal{M}}(w')$, do
6.1.2.1. let $y = y' + e$,
6.1.2.2. let $\gamma = \gamma' + z$,
6.1.2.3. let $\bar{\mathcal{M}}(w) = \bar{\mathcal{M}}(w) \cup \{(M, y, \gamma)\}$,
7. for all $i = 1, \ldots, r$, do
[Computation of the diagnosis states]
7.1. if $\forall\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and
$\forall t_f \in T_f^i$ it is $y(t_f) = 0$ and $\gamma(t_f) = 0$, do
7.1.1. if $\forall\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ it holds $x(i) = 0$,
where x is the binary vector in node M, do
7.1.1.1. let $\Delta(w, T_f^i) = 0$,
7.1.2. else
7.1.2.1. let $\Delta(w, T_f^i) = 1$,
7.2. if $\exists\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $(M', y', \gamma') \in \bar{\mathcal{M}}(w)$
s.t.:
(i) $\exists t_f \in T_f^i$ such that $y(t_f) > 0$ or $\gamma(t_f) > 0$,
or both,
(ii) $\forall t_f \in T_f^i$, $y'(t_f) = 0$ and $\gamma'(t_f) = 0$, do
7.2.1. let $\Delta(w, T_f^i) = 2$,
7.3. if $\forall\ (M, y, \gamma) \in \bar{\mathcal{M}}(w)\ \exists t_f \in T_f^i : y(t_f) > 0$
or $\gamma(t_f) > 0$ (or both), do
7.3.1. let $\Delta(w, T_f^i) = 3$.
8. Goto Step 3. ■

Steps 1 to 6 of Algorithm 22 enable us to compute the set $\bar{\mathcal{M}}(w)$.

Step 7 of Algorithm 22 computes the diagnosis state. Let us consider the generic ith fault class. If $\forall (M, y, \gamma) \in \bar{\mathcal{M}}(w)$ and $\forall t_f \in T_f^i$ it holds $y(t_f) = 0$ and $\gamma(t_f) = 0$, we have to check the ith entry of all the binary row vectors associated with the basis markings M, such that $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$. If the ith entry is equal to 0, we set $\Delta(w, T_f^i) = 0$, otherwise we set $\Delta(w, T_f^i) = 1$. On the other hand, if there exists at least one triple $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$ with either $y(t_f) > 0$ or $\gamma(t_f) > 0$ (or both) for any $t_f \in T_f^i$, and there exists at least one triple $(M', y', \gamma') \in \bar{\mathcal{M}}(w)$ with $y(t_f) = 0$ and $\gamma(t_f) = 0$ for all $t_f \in T_f^i$, then $\Delta(w, T_f^i) = 2$. Finally, if for all triples $(M, y, \gamma) \in \bar{\mathcal{M}}(w)$, either $y(t_f) > 0$ or $\gamma(t_f) > 0$ (or both) for any $t_f \in T_f^i$, then $\Delta(w, T_f^i) = 3$.

The following example shows how to perform diagnosis on-line simply looking at the BRG.

Example 23 Let us consider again the PN system in Fig. 2. Its BRG has 23 nodes and is reported in Fig. 3.

Let $w = \varepsilon$. By looking at the BRG we establish that $\Delta(\varepsilon, T_f^i) = 0$ for $i = \{1, 2\}$ being the vector x associated with M_0 equal to [0 0].

Now, let us consider $w = b$. In such a case $\bar{\mathcal{M}}(w) = \{(M_b^2, \vec{0}, [1\ 0]^T)\}$, where M_b^2 is the basis marking contained in node 2 of Table 1 and $x(2) = 0$ for M_b^2. Thus $\Delta(b, T_f^1) = 3$ and $\Delta(b, T_f^2) = 0$.

Finally, for $w = ab$ it holds $\Delta(ab, T_f^1) = 2$ and $\Delta(ab, T_f^2) = 1$. In fact $\bar{\mathcal{M}}(w) = \{(M_b^3, [1\ 1\ 0\ 0\ 0\ 0\ 0\ 0]^T, [0\ 0]^T), (M_b^4, \vec{0}, [1\ 0]^T), (M_b^5, [0\ 0\ 1\ 1\ 1\ 0\ 0\ 0]^T, [0\ 1]^T)\}$ and $x(2) = 1$ for both M_b^3 and M_b^4, where M_b^3, M_b^4 and M_b^5 are respectively contained in nodes $3, 4$ and 5. ■

Remark 24 The main contribution of this paper consists in generalizing the problem statement and consequently, the approach in [3] assuming that undistinguishable observable transitions may also model faults. In terms of computational complexity, its advantage with respect to other approaches in the literature, is exactly the same we already discussed in [3], that consists in the fact that we do not need an exhaustive enumeration of the set of markings consistent with a given observation, but we only need to enumerate the set of basis markings, that is a subset, of it.

Example 23 clearly shows this. Indeed, it can be verified using the software in [20] that the number of nodes of the reachability graph is equal to 510, while the number of basis markings is equal to 23. A detailed discussion in this respect has been recently proposed in [3] and we do not report it here to avoid repeating material already published. In particular, in [3] we considered a parametric example, where increasing values of the parameters correspond to larger reachability sets and larger sets of basis markings. However, the number of basis markings never exceeds the value of $17,500$ for the considered sets of parameters, while the cardinality of the reachability set may reach orders of $1,400,000$. Such a discussion also applies to the case at hand since the number of nodes of the BRG in [3] and in this paper are the same. The difference is in the information associated with arcs. ■

9 Conclusions and future work

This paper presents a diagnosis approach for labeled PNs based on the notion of basis markings that enables us to avoid an exhaustive enumeration of the reachability set. The proposed approach applies to all bounded and unbounded PN systems whose unobservable subnet is acyclic. Moreover, if we consider bounded net systems the most burdensome part of the procedure may be moved off-line computing the Basis Reachability Graph.

The main difference with respect to our previous works in this framework is that now fault transitions do not necessarily correspond to silent events, but may also be observable undistinguishable events, i.e., they share the same label with transitions belonging to different fault classes and/or

with transitions modeling regular behavior.

Our future work will be that of studying distributed diagnosis and diagnosability analysis procedures in the considered framework, i.e., assuming that faults may also be modeled as observable but undistinguishable transitions.

References

[1] A. Benveniste, E. Fabre, S. Haar, and C. Jard. Diagnosis of asynchronous discrete event systems, A net unfolding approach. *IEEE Trans. on Automatic Control*, 48(5):714–727, 2003.

[2] R.K. Boel and G. Jiroveanu. Distributed contextual diagnosis for very large systems. In *Proc. 7th IFAC Work. on Discrete Event Systems*, Reims, France, 2004.

[3] M. P. Cabasino, A. Giua, M. Pocci, and C. Seatzu. Discrete event diagnosis using labeled Petri nets. An application to manufacturing systems. *Control Engineering Practice*, 19(9):989–1001, 2011.

[4] M. P. Cabasino, A. Giua, and C. Seatzu. Diagnosis using labeled Petri nets: faults may either be silent or undistinguishable events. In *Proc. IEEE Conference on Automation Science and Engineering*, Toronto, Canada, 2010.

[5] M. P. Cabasino, A. Giua, and C. Seatzu. Fault detection for discrete event systems using Petri nets with unobservable transitions. *Automatica*, 46(9):1531–1539, 2010.

[6] D. Corona, A. Giua, and C. Seatzu. Marking estimation of Petri nets with silent transitions. *IEEE Trans. on Automatic Control*, 52(9):1695–1699, 2007.

[7] R. Debouk, S. Lafortune, and D. Teneketzis. Coordinated decentralized protocols for failure diagnosis of discrete-event systems. *Discrete Events Dynamical Systems*, 10(1):33–86, 2000.

[8] M. Dotoli, M.P. Fanti, A.M. Mangini, and W. Ukovich. On-line fault detection in discrete event systems by Petri nets and integer linear programming. *Automatica*, 45(11):2665–2672, 2009.

[9] E. Garcia, L. Rodriguez, F. Morant, A. Correcher, E. Quiles, and R. Blasco. Fault diagnosis with Coloured Petri Nets using Latent Nestling Method. In *Proc. IEEE International Symposium on Industrial Electronics, Cambridge, UK*, 2008.

[10] S. Genc and S. Lafortune. Distributed diagnosis of place-bordered Petri nets. *IEEE Trans. on Automation Science and Engineering*, 4(2):206–219, 2007.

[11] Mohamed Ghazel, Armand Toguyéni, and Pascal Yim. State Observer for DES Under Partial Observation with Time Petri Nets. *Discrete Event Dynamic Systems*, 19(2):137–165, 2009.

[12] S. Jiang and R. Kumar. Failure diagnosis of discrete-event systems with linear-time temporal logic specifications. *IEEE Trans. on Automatic Control*, 49(6):934–945, 2004.

[13] G. Jiroveanu and R.K. Boel. Contextual analysis of Petri nets for distributed applications. In *Proc. 16th Int. Symp. on Mathematical Theory of Networks and Systems*, Leuven, Belgium, 2004.

[14] G. Jiroveanu and R.K. Boel. A distributed approach for fault detection and diagnosis based on time Petri nets. *Mathematics and Computers in Simulation*, 70(5):287–313, 2006.

[15] D. Lefebvre and C. Delherm. Diagnosis of DES with Petri net models. *IEEE Trans. on Automation Science and Engineering*, 4(1):114–118, 2007.

[16] D. Lefebvre and E. Leclercq. Stochastic Petri Net Identification for the Fault Detection and Isolation of Discrete Event Systems. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 41(2):213 –225, 2011.

[17] C. Mahulea, C. Seatzu, M. P. Cabasino, and M. Silva. Fault Diagnosis of Discrete-Event Systems Using Continuous Petri Nets. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, (99):1 –15, 2012. (in press).

[18] J. Martinez and M. Silva. A simple and fast algorithm to obtain all invariants of a generalized Petri net. In *Informatik-Fachberichte 52: Application and Theory of Petri Nets*, pages 301–310. Springer-Verlag, 1982.

[19] T. Murata. Petri nets: properties, analysis and applications. *Proc. of the IEEE*, 77(4):541–580, 1989.

[20] Marco Pocci. This matlab tool is available at the website: *http://www.diee.unica.it/giua/TESI/09_Marco.Pocci/PN_DIAG.zip*.

[21] Y. Qu, L. Li, Y. Chen, and Y. Dai. An Optimal Design Approach for Fault-Tolerant Petri Net Controllers Using Arc Weights Minimization. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, (99):1 –8, 2012. (in press).

[22] A. Ramirez-Trevino, E. Ruiz-Beltran, J. Aramburo-Lizarraga, and E. Lopez-Mellado. Structural Diagnosability of DES and Design of Reduced Petri Net Diagnosers. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 42(2):416 –429, 2012.

[23] A. Ramirez-Treviño, E. Ruiz-Beltràn, I. Rivera-Rangel, and E. Lopez-Mellado. Online fault diagnosis of discrete event systems. A Petri net-based approach. *IEEE Trans. on Automation Science and Engineering*, 4(1):31–39, 2007.

[24] L. Rodriguez, E. Garcia, F. Morant, A. Correcher, and E. Quiles. Hybrid Latent Nesting Method: A fault diagnosis case study in the wind turbine subsets. In *Proc. IEEE/ASME International Conference on Advanced Intelligent Mechatronics, Budapest, Hungary*, 2011.

[25] Yu Ru and Christoforos N. Hadjicostis. Fault Diagnosis in Discrete Event Systems Modeled by Partially Observed Petri Nets. *Discrete Event Dynamic Systems*, 19(4):551–575, 2009.

[26] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *IEEE Trans. on Automatic Control*, 40(9):1555–1575, 1995.

[27] Y. Wu and C.N. Hadjicostis. Algebraic approaches for fault identification in discrete-event systems. *IEEE Trans. Robotics and Automation*, 50(12):2048–2053, 2005.

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