Diagnosability of discrete event systems using labeled Petri nets

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu*†

March 17, 2014

Abstract

In this paper we focus on labeled Petri nets with silent transitions that may either correspond to fault events or to regular unobservable events. We address the problem of deriving a procedure to determine if a given net system is diagnosable, i.e., the occurrence of a fault event may be detected for sure after a finite observation. The proposed procedure is based on our previous results on the diagnosis of discrete event systems modeled with labeled Petri nets, whose key notions are those of *basis markings* and *minimal explanations*, and is inspired by the diagnosability approach for finite state automata proposed by Sampath *et al.* in 1995. In particular, we first give necessary and sufficient conditions for diagnosability. Then, we present a method to test diagnosability that is based on the analysis of two graphs that depend on the structure of the net, including the faults model, and the initial marking.

Note to Practitioners Fault diagnosis is a very important problem in several domains of applications, such as manufacturing, telecommunication, electronics, and so on, since after the occurrence of a fault the system usually deviates from its nominal behavior and appropriate actions of recovery should be performed. As a consequence this problem has been extensively studied in the past years both in the case of time-driven and discrete-event systems, and several approaches have been proposed. A problem strictly related to fault diagnosis is diagnosability. Solving a problem of diagnosability is equivalent to determine if a system is diagnosable with respect to a given fault, i.e., to determine if, once the fault has occurred, the system can detect its occurrence after a finite observation of the system evolution. Obviously, diagnosability is an essential property that must hold if a diagnosis approach is to be applied in real life applications. This paper is devoted to diagnosability analysis and a procedure based on labeled Petri nets is proposed.

Published as:
M.P. Cabasino, A. Giua, C. Seatzu, "Diagnosability of discrete event systems using labeled Petri

*M.P. Cabasino, gratefully acknowledges Sardinia Regional Government for the financial support of her Post Doc fellowship (P.O.R. Sardegna F.S.E. Operational Programme of the Autonomous Region of Sardinia, European Social Fund 2007-2013 - Axis IV Human Resources, Objective l.3, Line of Activity l.3.1.).

†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. Alessandro Giua is also with Aix-Marseille University, LSIS, France.

nets", *IEEE Trans. on Automation Science and Engineering*, Vol. 11, No. 1, pp. 144-153, Jan 2014. The original publication is available at www.ieeexplore.ieee.org.

1 Introduction

Failure detection and isolation in industrial systems is a subject that has received a lot of attention in the past few decades. In the discrete event systems (DES) framework two different problems can be addressed: *diagnosis* and *diagnosability*. Solving a diagnosis problem means associate with each observed string of events a diagnosis state, such as "normal" or "faulty" or "uncertain". It is performed on-line based on the observed sequence. The problem of diagnosability consists in determining a priori if a system is diagnosable, i.e., if it is possible to reconstruct the occurrence of fault events observing words of finite length, and it has been largely investigated in the literature. The first results have been presented within the framework of automata [15, 19, 12, 14]. More recently a series of interesting contributions have been proposed using Petri nets (PNs) [21, 11, 22, 23, 16, 13, 4, 6, 2].

In our previous papers [10, 8] we presented an approach for the diagnosis of PNs. Based on such results, in this paper we provide a necessary and sufficient condition for *diagnosability* of *bounded* PNs, namely PNs whose set of reachable markings is finite. The proposed method, firstly introduced in the conference paper [9], is based on the construction of two labeled and oriented graphs denoted respectively *Modified Basis Reachability Graph* (MBRG) and *Basis Reachability Diagnoser* (BRD), where the MBRG is a slight variation of the *Basis Reachability Graph* (BRG) introduced in [8] for the diagnosis of bounded labeled PNs. Basically, the analysis consists in determining if certain cycles exist in the BRD, and in the case of a positive answer, in verifying if certain other conditions are satisfied in the MBRG, thus establishing if such cycles are *indeterminate* or not. The results relative to diagnosability are inspired by the diagnosability approach for finite state automata proposed by Sampath *et al.* [19], [20]. However, while in the automata approach it is necessary to exhaustively enumerate the state space, our approach requires the enumeration of a subset of the reachability set. The effectiveness of the proposed procedure has been illustrated in [7], where we showed that especially in the presence of highly concurrent systems the number of basis markings is always much smaller with respect to the number of reachable markings (that increase exponentially with the size of the net).

Note that similar results have been derived independently and in parallel by Jiroveanu and Boel in [3, 4]. A similar notion of minimal explanations to provide a compact representation of the state space has been used in [3]. Under slightly different assumptions on the unobservable subnet, they presented an automaton called *ROF* that is the counterpart of our MBRG [4]. A more detailed comparison is presented in Section 8. The main contribution of our paper with respect to [4] consists in providing necessary and sufficient conditions for diagnosability based on the BRD.

2 Background on labeled Petri nets

In this section we recall the formalism used in the paper. For more details on PNs we refer to [17].

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 if $M \geq Pre(\cdot, t)$ 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 (or Parikh 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 $R(N, M_0)$.

A PN having no directed circuits is called *acyclic*. For this subclass, it can be shown that the state equation gives necessary and sufficient conditions for reachability [17].

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* $\mathcal{L} : T \to L \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet L or the empty string ε. We call *labeled Petri net system* the triple $\langle N, M_0, \mathcal{L} \rangle$.

We denote as 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*. We denote as T_o the set of transitions labeled with a symbol in L. Transitions in T_o are called *observable* because when they fire their label can be observed.

In the following we denote C_u (C_o) the restriction of the incidence matrix to T_u (T_o) and denote as n_u and n_o, respectively, the cardinality of the above sets. Moreover, given a sequence $\sigma \in T^*$, $P_u(\sigma)$ ($P_o(\sigma)$) denotes the projection of σ over T_u (T_o). Given a language $K \subseteq T^*$, we denote K/σ the post-language of K after σ, i.e., $K/\sigma = \{\sigma' \in T^* \mid \sigma\sigma' \in K\}$.

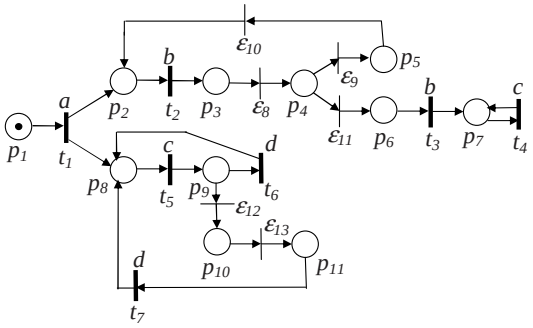

Figure 1: The PN system considered in Example 2.2.

We denote as w the word of events associated with the sequence σ, i.e., $w = \mathcal{L}(\sigma)$.

Definition 2.1 *Let $\langle N, M_0, \mathcal{L}\rangle$ be a labeled net system, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define*

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

the set of firing sequences consistent *with $w \in L^*$.* ■

Example 2.2 *Let us consider the labeled PN system in Fig. 1. Let us assume $T_o = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7\}$ and $T_u = \{\varepsilon_8, \varepsilon_9, \varepsilon_{10}, \varepsilon_{11}, \varepsilon_{12}, \varepsilon_{13}\}$, where for a better understanding unobservable transitions have been denoted ε_i rather than t_i. The labeling function is defined as follows: $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_2) = \mathcal{L}(t_3) = b$, $\mathcal{L}(t_4) = \mathcal{L}(t_5) = c$, $\mathcal{L}(t_6) = \mathcal{L}(t_7) = d$.*

Let $w = ab$ be the observed word. The set of firing sequences that are consistent with w is $\mathcal{S}(w) = \{t_1t_2, t_1t_2\varepsilon_8, t_1t_2\varepsilon_8\varepsilon_9, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}, t_1t_2\varepsilon_8\varepsilon_{11}\}$. ■

Definition 2.3 *Given a net $N = (P, T, Pre, Post)$, and a subset $T' \subseteq T$ of its transitions, we define the $T'-$*induced subnet *of N as the new net $N' = (P, T', Pre', Post')$ where $Pre', Post'$ are the restrictions of $Pre, Post$ to T'. The net N' can be thought as obtained from N removing all transitions in $T \setminus T'$.* ■

3 Preliminary results

In this paper we consider labeled PN systems where the structure of N is known as well as the initial marking M_0. The set of transitions is partitioned as $T = T_o \cup T_u$, where T_o is the set of observable transitions, and T_u is the set of unobservable transitions. Furthermore, the set of unobservable transitions is partitioned into two subsets, namely $T_u = T_f \cup T_{reg}$ where T_f includes all fault transitions, while T_{reg} includes all transitions relative to unobservable but regular events. Finally, the set T_f is further partitioned into r different subsets T_f^i, where $i = 1, \ldots, r$, that model the different fault classes. The labeling function $\mathcal{L} : T_o \to L$ may associate the same label to different transitions. In particular, two transitions $t_1, t_2 \in T_o$ are called *indistinguishable* if they share the same label, i.e., $\mathcal{L}(t_1) = \mathcal{L}(t_2) = l \in L$.

We make the following assumption.

(A1) The T_u-induced subnet is *acyclic*.

This assumption is analogous to the classical hypothesis in the theory of automata where no cycle of unobservable events can appear.

Definition 3.1 *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.* ■

Definition 3.2 *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. ■

Definition 3.3 *Let $\langle N, M_0, \mathcal{L}\rangle$ be a labeled net system, where $N = (P,T,Pre,Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ 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*).* ■

Definition 3.4 *Let $\langle N, M_0, \mathcal{L}\rangle$ be a labeled net system, 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 minimal 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 minimal justification σ_u, is called basis marking *and y is called its* j-vector *(or* justification-vector*).* ■

Example 3.5 *Let us consider the labeled PN system in Fig. 1 previously introduced in Example 2.2. Let us assume* $w = ab$. *It is* $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon)\}$, $\hat{Y}_{min}(M_0, w) = \{(t_1t_2, \mathbf{0})\}$ *and the basis marking is* $M_b = [0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$. ■

Definition 3.6 *[8] A* diagnoser *is a function* $\Delta : L^* \times \{T_f^1, T_f^2, \ldots, T_f^r\} \to \{0, 1, 2, 3\}$ *that associates with each observation* $w \in L^*$ *and 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* $t_f \notin \sigma$.
- $\Delta(w, T_f^i) = 1$ *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* $t_f \notin \sigma_u$.
- $\Delta(w, T_f^i) = 2$ *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* $t_f \in \sigma_u$;
  (ii) for all $t_f \in T_f^i$, $t_f \notin \sigma'_u$.
- $\Delta(w, T_f^i) = 3$ *if for all* $\sigma \in \mathcal{S}(w)$ *there exists* $t_f \in T_f^i$ *such that* $t_f \in \sigma$.

■

Example 3.7 *Let us consider the PN system in Fig. 1 previously introduced in Example 2.2. Let* $T_f = \{\varepsilon_{11}, \varepsilon_{12}\}$. *Assume that the two fault transitions belong to different fault classes, i.e.,* $T_f^1 = \{\varepsilon_{11}\}$ *and* $T_f^2 = \{\varepsilon_{12}\}$.

Let us observe $w = ab$. *In this case* $\Delta(w, T_f^1) = 1$ *and* $\Delta(w, T_f^2) = 0$, *being* $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon)\}$ *and* $\mathcal{S}(w) = \{t_1t_2, t_1t_2\varepsilon_8, t_1t_2\varepsilon_8\varepsilon_9, t_1t_2\varepsilon_8\varepsilon_9\varepsilon_{10}, t_1t_2\varepsilon_8\varepsilon_{11}\}$. ■

In [8] it has been explained how the diagnosis states can be computed. In particular, we proved that to distinguish between states 0 and 1 we need to establish if the constraint set

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

is feasible.

4 Diagnosability of bounded Petri nets: problem statement

Let us now introduce the definition of diagnosability of PNs inspired by the definition of diagnosability for (regular) languages [19]. Let $\Psi(T')$ be the set of all firing sequences in $L(N, M_0)$ that end with a transition $t' \in T'$, i.e., $\Psi(T') = \{\sigma t' \in L(N, M_0) : t' \in T'\}$.

Definition 4.1 *A labeled PN system $\langle N, M_0, \mathcal{L}\rangle$ having no deadlock after the occurrence of any transition $t_f \in T_f^i$, for $i \in \{1, \ldots, r\}$, is* diagnosable wrt the fault class T_f^i *if*

$$\begin{aligned} &\forall \sigma' \in \Psi(T_f^i), \quad \exists K \in \mathbb{N}, \quad \forall \sigma'' \in L(N, M_0)/\sigma', \\ &|\sigma''| \geq K \;\Rightarrow\; \forall \sigma \in \mathcal{L}^{-1}(\mathcal{L}(\sigma'\sigma'')),\; \exists t_f \in T_f^i \;:\; t_f \in \sigma. \end{aligned} \tag{2}$$

A labeled PN system $\langle N, M_0, \mathcal{L}\rangle$ is said to be diagnosable *if it is diagnosable wrt all fault classes.* ■

In words, given a firing sequence σ' that ends in a fault transition, let σ'' be any sufficiently long continuation of it, i.e., $|\sigma''| \geq K$, where K depends on σ'. A labeled PN system $\langle N, M_0, \mathcal{L}\rangle$ having no deadlock after the occurrence of any transition $t_f \in T_f^i$, for $i \in \{1, \ldots, r\}$, is *diagnosable wrt the fault class* T_f^i if any firing sequence σ belonging to the language and having the same observable projection of $\sigma'\sigma''$ contains a fault transition in T_f^i. This implies that along any continuation σ'' of σ' the occurrence of a fault transition in T_f^i can be detected in a finite number of transitions firings (at most K).

In the rest of the paper we investigate the problem of providing necessary and sufficient conditions for diagnosability. In particular, we suppose that the considered labeled PN satisfies also the following two assumptions.

(A2) The net system $\langle N, M_0\rangle$ is *bounded.*

(A3) The net system $\langle N, M_0\rangle$ *does not deadlock after the firing of any fault transition.*

5 Modified Basis Reachability Graph

We first introduce the definition of *extended basis markings*, then we define the *Modified Basis Reachability Graph* (MBRG), and finally we show how it can be constructed.

Definition 5.1 *An* extended basis marking *is a basis marking computed assuming that all fault transitions are observable.*

■

Definition 5.2 *The MBRG is a deterministic graph whose nodes are labeled with a pair (M, x): $M \in \mathbb{N}^m$ is an extended basis marking, and x is a row vector in $\{0,1\}^r$ where $x(i) = 1$ if $\mathcal{T}(M, T_f^i)$ in (1) is feasible wrt the ith class, $x(i) = 0$ otherwise.*

Since we are considering the extended basis markings, the minimal explanations are restricted to transitions in T_{reg}. In the following we denote as $Y_{\min}^{mod}(M, t)$ the set of minimal e-vectors restricted to T_{reg}, and C_{reg} the restriction of the incidence matrix to T_{reg}.

Arcs may be labeled in two different ways depending on the associated event.

In the case of events corresponding to the firing of transitions in T_o, labels are strings $(l(t), e)$, where $l \in L$ is the observed label, t is the transition labeled l whose firing at the input node is enabled by a sequence of regular transitions with firing vector $e \in Y^{mod}_{\min}(M, t)$, and that leads to the marking in the output node.

In the case of events corresponding to the firing of fault transitions labels are pairs (t_f, e), where $t_f \in T_f$ is the fault transition whose firing at the input node is enabled by a sequence with firing vector $e \in Y^{mod}_{\min}(M, t)$, and that leads to the marking in the output node. ■

Algorithm 5.3 [Computation of the MBRG]

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

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

Assign no tag to it.

2. While nodes with no tag exist

2.1. select a node with no tag,

2.2. let (M, x) be the selected node,

2.3. for all $l \in L$

2.3.1. for all $t : \mathcal{L}(t) = l \wedge Y^{mod}_{\min}(M, t) \neq \emptyset$, do

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

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

  - add arc $(l(t), e)$ from node (M, x) to node (M', x')

2.4. for all $i = 1, \ldots, r$

2.4.1. for all $t_f \in T^i_f : Y^{mod}_{\min}(M, t_f) \neq \emptyset$, do

- for all $e \in Y^{mod}_{\min}(M, t_f)$, do
  - let $M' = M + C_{reg} \cdot e + C(\cdot, t_f)$,
  - if $\nexists$ already a node with M', do
    - add a new node to the graph containing the pair (M', x') where $\forall i = 1, \ldots, r$,

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

  - add arc (t_f, e) from node (M, x) to node (M', x')

2.5. tag the node (M, x) "old".

3. Remove all tags.

■

The algorithm constructs the MBRG starting from the initial node to which it corresponds the initial marking and a binary vector defining which classes of faults may occur at M_0. Now, we consider all labels $l \in L$ (Step 2.3) and all fault classes $i = 1, \ldots, r$ (Step 2.4) such that there exists a transition t with $\mathcal{L}(t) = l$ or a fault transition $t_f \in T_f^i$ for which a minimal explanation at M_0 exists. For any of such transitions, that can be either $t \in T_o$ or $t_f \in T_f^i$, we compute the marking M' resulting from its firing at $M_0 + C_{reg} \cdot e$ ($e \in Y_{\min}^{mod}(M_0, t)$ or $e \in Y_{\min}^{mod}(M_0, t_f)$, respectively). If a new pair (marking, binary vector) is obtained, a new node is added to the graph, labeled with the resulting marking M' and the corresponding vector x'. The arc going from the initial node to the new node is either labeled $(l(t), e)$ or (t_f, e), depending on the considered event. The procedure is iterated until all nodes have been examined.

The following proposition provides a characterization of the language generated by the finite state automaton defining the MBRG.

Proposition 5.4 *Let us consider a bounded labeled Petri net system $\langle N, M_0, \mathcal{L} \rangle$ with $N = (P, T, Pre, Post)$, $T = T_o \cup T_u$ and $T_u = T_{reg} \cup T_f$.*

For each path from the initial node of the MBRG, we build a sequence $\sigma \in (T_o \cup T_f)^*$ such that: for each arc connecting two nodes in the path we take either t if the arc is labeled by the string $(l(t), e)$ or t_f if the arc is labeled by the pair (t_f, e).

The set of sequences $\sigma \in (T_o \cup T_f)^*$ built in this way coincides with the projection of $L(N, M_0)$ over the set of transitions $T_o \cup T_f$.

Follows from the fact that the MBRG is constructed assuming that the minimal explanations are defined on the set of transitions T_{reg} and the arcs contain the information on which transition has fired at the extended basis marking that labels the considered node. □

Proposition 5.5 *If a labeled net system $\langle N, M_0, \mathcal{L} \rangle$ is bounded then the set of extended basis markings $\mathcal{M}_{MBRG}$ associated with the nodes of the MBRG satisfies the following inclusion relationship:*

$$\mathcal{M}_{MBRG} \subseteq R(N, M_0). \tag{3}$$

It follows from the fact that the set $R(N, M_0)$ includes all markings in $\mathcal{M}_{MBRG}$, i.e., all extended basis markings, plus all those markings that can be reached from markings in $\mathcal{M}_{MBRG}$ firing transitions in T_{reg}. □

Example 5.6 *In Fig. 2 is shown the MBRG corresponding to the PN system in Fig. 1 previously introduced in Example 2.2. Let $T_f^1 = \{\varepsilon_{11}\}$ and $T_f^2 = \{\varepsilon_{12}\}$. The notation used in Fig. 2 is detailed in Tables 1 and 2.*

Each node is labeled with an extended basis marking and a vector with two entries (because there are two fault classes). As an example, vector [0 0] is associated with M_0 because $\mathcal{T}(M_0, T_f^i)$ is not feasible for $i = \{1, 2\}$. On the contrary, vector [1 0] is associated with M_3 because $\mathcal{T}(M_3, T_f^i)$ is feasible only for $i = 1$. In fact, fault transition ε_{11} is enabled at M_3.

M_0	[	1	0	0	0	0	0	0	0	0	0	$]^T$
M_1	[	0	1	0	0	0	0	0	1	0	0	$]^T$
M_2	[	0	1	0	0	0	0	0	0	1	0	0	$]^T$
M_3	[	0	0	1	0	0	0	0	1	0	0	0	$]^T$
M_4	[	0	0	1	0	0	0	0	0	1	0	0	$]^T$
M_5	[	0	0	0	0	0	0	1	1	0	0	0	$]^T$
M_6	[	0	0	0	0	0	0	1	0	1	0	0	$]^T$
M_7	[	0	1	0	0	0	0	0	0	0	1	0	$]^T$
M_8	[	0	0	0	0	0	1	0	1	0	0	0	$]^T$
M_9	[	0	0	0	0	0	1	0	0	1	0	0	$]^T$
M_{10}	[	0	0	1	0	0	0	0	0	0	1	0	$]^T$
M_{11}	[	0	0	0	0	0	1	0	0	0	1	0	$]^T$
M_{12}	[	0	0	0	0	0	0	1	0	0	1	0	$]^T$

Table 1: The extended basis markings of the MBRG in Fig. 2.

	[	ε_8	ε_9	ε_{10}	ε_{13} $]^T$
e_1	[	1	1	1	0 $]^T$
e_2	[	1	0	0	0 $]^T$
e_3	[	0	0	0	1 $]^T$

Table 2: The modified minimal e-vectors of the MBRG in Fig. 2.

Arcs are labeled either by the string (label (relative transition), corresponding modified minimal e-vector) (see e.g. $(c(t_5), \mathbf{0})$ from M_3 to M_4), or by the pair (fault transition, corresponding modified minimal e-vector) (see e.g. (ε_{11}, e_2) from M_3 to M_8).

Finally, let us observe that as shown in Proposition 5.5 the set of extended basis markings is a super set of the set of basis markings. In this example, markings from M_0 to M_6 are basis markings, while markings from M_7 to M_{12} are extended basis markings, in fact they are reached firing a fault transition. Note however, that the number of extended markings in the MBRG is equal to the number of reachable markings only in the worst case, but in general is smaller, as in this example. ■

6 Basis Reachability Diagnoser

Definition 6.1 *The BRD is a deterministic graph where each node is labeled with:*

- *one or more triples (M, x, h), where:*

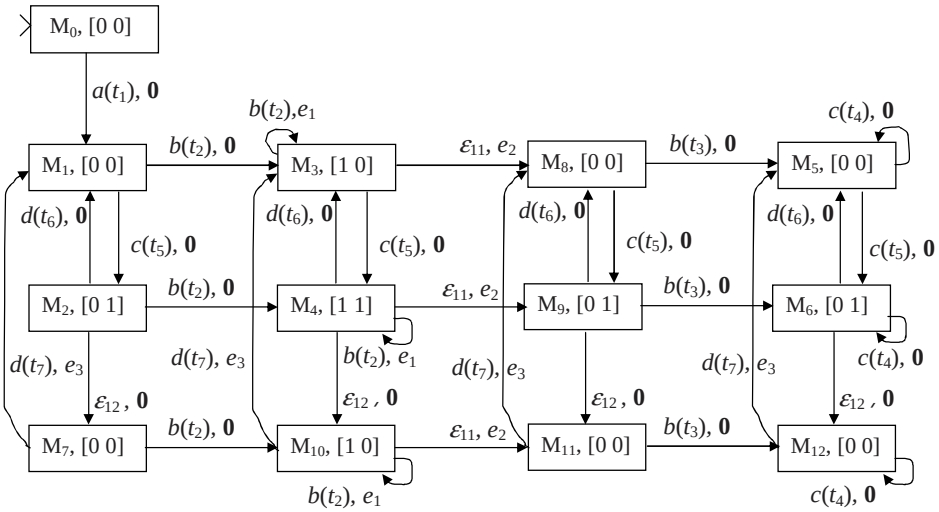

Figure 2: The MBRG of the Petri net system in Fig. 1.

- *M is a basis marking;*
- *$x \in \{0,1\}^r$ is a row vector whose ith entry is equal to 1 if $\mathcal{T}(M, T_f^i)$ is feasible, and is equal to 0 otherwise;*
- *$h \in \{N,F\}^r$ is a row vector whose ith entry is equal to N if reaching M from M_0 no fault in T_f^i has occurred, and is equal to F otherwise;*

• *r tags Δ_i, $i = 1, \ldots, r$, that represent the diagnosis state of the node wrt the r fault classes.*

Finally, arcs are labeled with a symbol in L. ■

The BRD can be easily computed starting from the MBRG. In particular, the values of M and x are obtained from the MBRG by only looking at the nodes containing basis markings.

The values of h can be deduced by looking at the path(s) from M_0 to the corresponding value of M (denoted as $M_0 \rightsquigarrow M$). If there exists a path $M_0 \rightsquigarrow M$ containing fault transitions in the ith class, then to the pair M, x it is associated a value of $h(i) = F$. If there exists a path $M_0 \rightsquigarrow M$ containing no fault transition in the ith class, then to the pair M, x it is associated a value of $h(i) = N$. Note that, since in general there may exist more than one path going from M_0 to M, one containing a fault in T_f^i and another not, then the pair M, x may appear twice in the same node, once associated with $h(i) = F$ and once associated with $h(i) = N$.

The diagnosis state for the ith fault class is trivially obtained by just looking at the ith entry of the two vectors h and x of all triples in the node.

The following algorithm summarizes the main steps for the construction of the BRD. Note that to simplify the notation, we assume that each class only includes one fault transition, thus $|T_f| = r$. The extension to the more general case is trivial and is not reported here for the sake of brevity.

Algorithm 6.2 [Computation of the BRD]

1. Label the initial node $d_0 = (M_0, x_0, h_0)$, $h_0 = N^r$.
For $i = 1, \ldots, r$, if $x_0(i) = 0$ then $\Delta_i = 0$,
else $\Delta_i = 1$. Assign no tag to it.

2. While nodes with no tag exist

2.1. select a node d with no tag and do

2.2. for all $l \in L$

2.2.1. for all $M \in d$: $Y_{\min}(M, t) \neq \emptyset$ for some transition t : $\mathcal{L}(t) = l$

- for all triples with marking M in d
  - let $\tilde{d} = \emptyset$
  - for all output arcs of (M, x) in the MBRG labeled l, do
    - let (M', x') be the output node in the MBRG,
    - let

$$\begin{cases} h'(i) = N & \text{if } h(i) = N \\ h'(i) = F & \text{if } h(i) = F \end{cases}$$

  - let $\tilde{d} = \tilde{d} \cup \{(M', x', h')\}$
  - for all output paths of (M, x) in the MBRG labeled $\sigma_f l$ such that $\pi(\sigma_f) \in Y_{\min}(M, t)$ and $\mathcal{L}(t) = l$,
    - let (M', x') be the final node in the MBRG,
    - let

$$\begin{cases} h'(i) = N & \text{if } h(i) = N \wedge t_{f_i} \notin M \rightsquigarrow M' \\ h'(i) = F & \text{if } h(i) = F \\ h'(i) = F & \text{if } h(i) = N \wedge t_{f_i} \in M \rightsquigarrow M' \end{cases}$$

  - let $\tilde{d} = \tilde{d} \cup \{(M', x', h')\}$
  - if $\forall\ M' \in \tilde{d}$ it is $h'(i) = N$ and $x'(i) = 0$, then
    - let $\Delta_i = 0$
  - else if $\forall M' \in \tilde{d}$ it is $h'(i) = N$ and $x'(i) = 1$, then
    - let $\Delta_i = 1$
  - else if $\exists (M', x', h') \in \tilde{d} : h'(i) = N$ and $\exists (M'', x'', h'') \in \tilde{d}$: $h''(i) = F$, then
    - let $\Delta_i = 2$
  - else if $\forall\ M' \in \tilde{d}$ it is $h'(i) = F$, then
    - let $\Delta_i = 3$

2.2.2 if $\nexists$ a node $\bar{d} = \tilde{d}$ in the graph then

- add a new node $\tilde{d}$ to the graph

2.2.3 add arc l from d to $\tilde{d}$

2.3. tag d *old*.
2.4 Goto Step 2.1.
3. Remove all tags.

■

The algorithm constructs the BRD starting from the initial node to which it corresponds a triple (M_0, x_0, h_0), where M_0 and x_0 are the components of the initial node of the MBRG and $h_0 = N^r$. Its diagnosis state Δ_i is set to zero if no fault transition in T_f^i may have occurred from the initial marking, namely if the ith entry of x_0 (associated with the only, for assumption, fault transition $t_{f_i} \in T_f^i$) is null, otherwise Δ_i is set to one.

Starting from the initial node and looking at the MBRG we focus on the set of basis markings that are reachable firing transitions with label l at M_0, either immediately or after the firing of one or more fault transitions.

The new node will be composed by all triples (M', x', h') such that the pair (M', x') is reached in the MBRG either firing a transition labeled l at M_0, or firing a minimal explanation containing one or more fault transitions and then the considered label l; h' is computed considering h_0 and all paths $M_0 \rightsquigarrow M'$ in the MBRG.

Finally, for each node the diagnosis state Δ_i depends on the ith entry of the two vectors x and h of all the markings appearing in the node.

The procedure is iterated until all nodes have been explored.

The following proposition characterizes the language associated with the BRD.

Proposition 6.3 *Let us consider a bounded labeled net system $\langle N, M_0, \mathcal{L}\rangle$. The language of the finite state automaton defining its BRD is equal to $\mathcal{L}(L(N, M_0))$.*

Follows from the rules of construction of the BRD. In fact, the first element of the initial node d_0 is the initial marking M_0. For such a node all labels $l \in L$ are considered (see Step 2.2) and for any label $l \in L$ all transitions labeled l are examined (see Step 2.2.1) in order to compute the set of markings that can be reached from d_0 firing all transitions labeled l that can be enabled at M_0 after, eventually, the firing of some unobservable transition. This set of markings reached when label l is observed formed a new node d. The same procedure is repeated for each new node d computing for all labels $l \in L$ and all transitions labeled l the set of markings that can be reached from node d firing all transitions labeled l that can be enabled at some marking in the node d after, eventually, the firing of some unobservable transition. □

Example 6.4 *In Fig. 3 is reported the BRD of the PN system in Fig. 1. The initial node is labeled* (M_0, [0 0], [N N]) *and its diagnosis states are* $\Delta_1 = \Delta_2 = 0$ *being* $x_0 =$ [0 0]. *From this node an output arc labeled a exists that leads to node* (M_1, [0 0], [N N]), *where* $M_1 = [0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$. *Also for this node diagnosis states are* $\Delta_1 = \Delta_2 = 0$.

Now, let us consider $w = abb$. *In this case we reach a node labeled by the two triples* (M_3, [1 0],

$[N\ N]$) *and* (M_5, $[0\ 0]$, $[F\ N]$), *where* $M_3 = [0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0]^T$ *and* $M_5 = [0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0]^T$. *In fact, two different sequences of observable transitions,* $t_1t_2t_2$ *or* $t_1t_2t_3$, *may have fired. Diagnosis states are equal to* $\Delta_1 = 2$, *being* $h_3(1) = N$ *and* $h_5(1) = F$, *and* $\Delta_2 = 0$, *since* $h_3(2) = h_5(2) = N$ *and* $x_3(2) = x_5(2) = 0$ *(where* $x_j(i)$ *and* $h_j(i)$ *indicate the entries of vectors* x *and* h, *respectively, associated with marking* M_j *wrt to the fault class* i*).*

Finally, let us consider $w = abbcc$. *In this case we reach a node labeled by the two triples* (M_5, $[0\ 0]$, $[F\ N]$) *and* (M_6, $[0\ 1]$, $[F\ N]$), *where* $M_6 = [0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0]^T$. *Diagnosis states are* $\Delta_1 = 3$, *being* $h_5(1) = h_6(1) = F$, *and* $\Delta_2 = 1$, *since* $h_5(2) = h_6(2) = N$ *and* $x_6(2) = 1$.

Note that all BRD's nodes only contain basis markings. ■

7 Necessary and sufficient conditions for diagnosability

In this section we provide necessary and sufficient conditions for diagnosability based on the notions of uncertain and indeterminate cycles. These conditions can be verified using the BRD in conjunction with the MBRG. In particular, first we check if the BRD contains an uncertain cycle, namely a potentially indeterminate cycle; then using the MBRG, we verify if that cycle is indeterminate or not.

Definition 7.1 *Let* γ *be a cycle in the BRD labeled* $\rho \in L^*$. *The cycle* γ *is* uncertain *wrt a fault class* T_f^i *if it only includes states with* $\Delta_i = 1$ *and/or* $\Delta_i = 2$. ■

Definition 7.2 *Let* γ *be an uncertain cycle in the BRD labeled* $\rho \in L^*$. *Let* ζ *be a path in the BRD from the initial node to any node of the cycle labeled* $p \in L^*$. *The cycle* γ *is* indeterminate *wrt a fault class* T_f^i *if there exist two sequences of infinite length* $\sigma_1, \sigma_2 \in L(N, M_0)$ *that can be written as*

$$\sigma_1 = \sigma_1'(\sigma_1'')^*, \qquad \sigma_2 = \sigma_2'(\sigma_2'')^*$$

such that

(i) $\mathcal{L}(\sigma_1'') = \mathcal{L}(\sigma_2'') = \rho$;

(ii) $\mathcal{L}(\sigma_1') = \mathcal{L}(\sigma_2') = p$;

(iii) Either σ_1' *or* σ_1'' *(or both) contain a fault in* T_f^i, *while neither* σ_2' *nor* σ_2'' *contain a fault in* T_f^i. ■

Proposition 7.3 *Let* γ *be an uncertain cycle in the BRD labeled* $\rho \in L^*$. *Let* ζ *be a path in the BRD from the initial node to any node of the cycle labeled* $p \in L^*$. *The cycle* γ *is* indeterminate *wrt a fault class* T_f^i *if in the MBRG there exist two cycles* γ_1 *and* γ_2 *satisfying the following three conditions:*

(i) both cycles are labeled ρ;

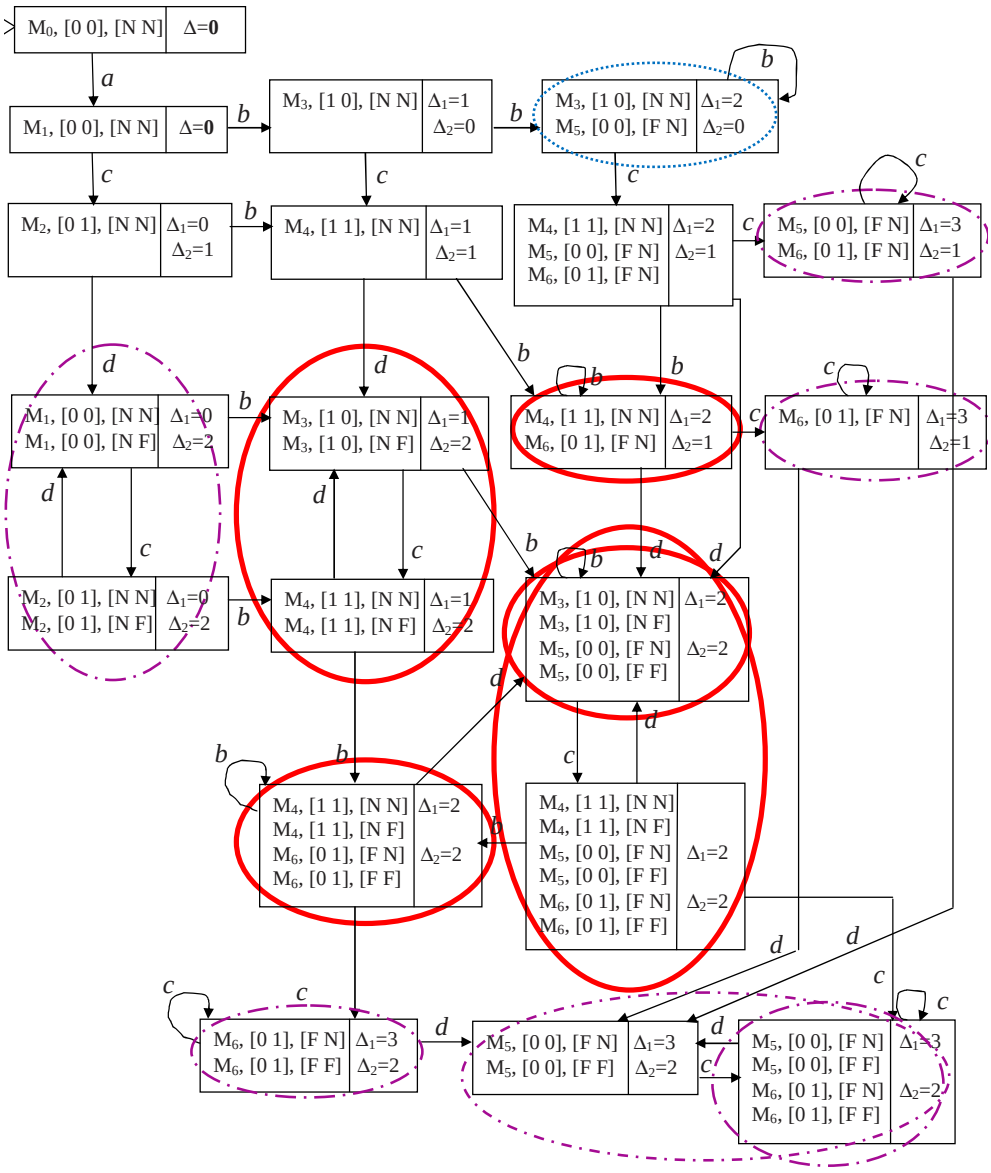

Figure 3: The BRD of the PN system in Fig. 1 with thick red ellipses denoting uncertain cycles for both fault classes, thin dotted blue ellipses and thin dashed purple ellipses respectively, denoting uncertain cycles for the first and the second fault class, respectively.

(ii) *there exist two paths ζ_1 and ζ_2 respectively labeled p_1 and p_2, that from the initial node in the MBRG enable respectively cycles γ_1 and γ_2. These cycles are respectively labeled ρ_1 and ρ_2;*

(iii) *Neither ρ_2 nor p_2 contain a fault in T_f^i, while either ρ_1 or p_1 (or both) contain a fault in T_f^i.* ■

Follows from Proposition 5.4 who claims that the set of sequences $\sigma \in (T_o \cup T_f)^*$ that are enabled at the initial node of the MBRG coincides with the projection of $L(N, M_0)$ over the set of transitions $T_o \cup T_f$. □

Example 7.4 *Let us consider the BRD in Fig. 3 that corresponds to the PN system in Fig. 1, where thin dotted blue ellipses, thin dashed purple ellipses and thick red ellipses denote, respectively, the uncertain cycles for the first, the second and both fault classes.*

Let us consider the uncertain cycle for the first fault class

$$\begin{aligned}\gamma = \quad & [(M_3, [1\ 0], [N\ N]), (M_5, [0\ 0], [F\ N])] \underrightarrow{b} \\ & [(M_3, [1\ 0], [N\ N]), (M_5, [0\ 0], [F\ N])],\end{aligned}$$

labeled b. This cycle only contains one node and there exists only one path from the initial node to a node, namely

$$\begin{aligned}\zeta = \quad & (M_0, [0\ 0], [N\ N]) \underrightarrow{a} (M_1, [0\ 0], [N\ N]) \underrightarrow{b} \\ & (M_3, [1\ 0], [N\ N]) \underrightarrow{b},\end{aligned}$$

labeled abb. Looking at the MBRG in Fig. 2, it is easy to see that conditions of Definition 7.2 are not satisfied. In fact, there does not exist a path labeled $p_1 = abb$ that contains the fault and that enables a cycle γ_1 such that $\mathcal{L}(\gamma_1) = b$. Therefore this cycle is not indeterminate.

Now, let us consider the uncertain cycle for both fault classes

$$\begin{aligned}\gamma = \quad & [(M_3, [1\ 0], [N\ N]), (M_3, [1\ 0], [N\ F])] \underrightarrow{c} \\ & [(M_4, [1\ 1], [N\ N]), (M_4, [1\ 1], [N\ F])] \underrightarrow{d} \\ & [(M_3, [1\ 0], [N\ N]), (M_3, [1\ 0], [N\ F])]\end{aligned}$$

denoted with a thick red ellipse in Fig. 3 and whose label is $\rho = cd$. Let

$$\begin{aligned}\zeta = \quad & (M_0, [0\ 0], [N\ N]) \underrightarrow{a} (M_1, [0\ 0], [N\ N]) \underrightarrow{b} \\ & (M_3, [1\ 0], [N\ N]) \underrightarrow{c} (M_4, [1\ 1], [N\ N]) \underrightarrow{d}\end{aligned}$$

be the path from the initial node to the first node of γ. Its label is $p = abcd$. It is easy to verify that the three conditions of Definition 7.2 are satisfied for both fault classes, therefore the cycle γ is indeterminate for T_f^1 and T_f^2.

In fact, for the first fault class in the MBRG there exist two cycles

$$\gamma_1 = (M_8, [0\ 0]) \underrightarrow{c(t_5)} (M_9, [0\ 1]) \underrightarrow{d(t_6)} (M_8, [0\ 0])$$

and

$$\gamma_2 = (M_3, [1\ 0])\underrightarrow{c(t_5)}(M_4, [1\ 1])\underrightarrow{d(t_6)}(M_3, [1\ 0])$$

labeled cd and there also exist two paths

$$\begin{aligned}\zeta_1 = \quad & (M_0, [0\ 0])\underrightarrow{a(t_1)}(M_1, [0\ 0])\underrightarrow{b(t_2)}(M_3, [1\ 0])\underrightarrow{\varepsilon_{11}} \\ & (M_8, [0\ 0])\underrightarrow{c(t_5)}(M_9, [0\ 1])\underrightarrow{d(t_6)}\end{aligned}$$

and

$$\begin{aligned}\zeta_2 = \quad & (M_0, [0\ 0])\underrightarrow{a(t_1)}(M_1, [0\ 0])\underrightarrow{b(t_2)}(M_3, [1\ 0])\underrightarrow{c(t_5)} \\ & (M_4, [1\ 1])\underrightarrow{d(t_6)}\end{aligned}$$

labeled abcd and that from the initial node enable γ_1 and γ_2. Finally, both ζ_2 and γ_2 do not contain fault transition ε_{11}, while ζ_1 contains ε_{11}.

Finally, for the second fault class in the MBRG there exist two cycles

$$\gamma_1 = (M_3, [1\ 0])\underrightarrow{c(t_5)}(M_4, [1\ 1])\underrightarrow{\varepsilon_{12}}(M_{10}, [1\ 0])\underrightarrow{d(t_7)}(M_3, [1\ 0])$$

and

$$\gamma_2 = (M_3, [1\ 0])\underrightarrow{c(t_5)}(M_4, [1\ 1])\underrightarrow{d(t_6)}(M_3, [1\ 0])$$

both labeled $\rho = cd$ and there also exist two paths

$$\begin{aligned}\zeta_1 = \zeta_2 = \quad & (M_0, [0\ 0])\underrightarrow{a(t_1)}(M_1, [0\ 0])\underrightarrow{b(t_2)}(M_3, [1\ 0])\underrightarrow{c(t_5)} \\ & (M_4, [1\ 1])\underrightarrow{d(t_6)}\end{aligned}$$

both labeled $p = abcd$, that from the initial node enable γ_1 and γ_2. Finally, both ζ_2 and γ_2 do not contain fault transition ε_{12}, while γ_1 contains ε_{12}. ■

Theorem 7.5 *A labeled net system $\langle N, M_0, \mathcal{L}\rangle$ satisfying assumptions (A1) to (A3) is* diagnosable *wrt the fault class T_f^i iff its BRD has no cycle that is indeterminate wrt T_f^i.*

We prove the if and only if statements separately.

(Only if) Assume by contradiction that an indeterminate cycle labeled ρ exists in the BRD. Moreover, we assume that in the MBRG there exist two cycles γ_1 and γ_2 labeled respectively ρ_1 and ρ_2 satisfying conditions (i) to (iii) in Proposition 7.3. This obviously implies that there exist two sequences relative to $p_1\rho_1$ and $p_2\rho_2$ having the same observable projection, one containing a fault in the ith class and the other one not, that are of arbitrary length, because ρ_1 and ρ_2 can be repeated an arbitrary large number of times. Thus, by Definition 4.1 the system is not diagnosable wrt to the ith class.

(If) Assume that the BRD has no cycle that is indeterminate wrt T_f^i. By Definition 4.1 the sequences that may potentially lead to a violation of the diagnosability property because they have the same observable projection and are of arbitrary length, are those corresponding to cycles with one of the following features: (1) they include at least one node with $\Delta_i = 0$; (2) they only

include nodes with $\Delta_i = 3$; (3) they include nodes with $\Delta_i = 1$ and/or $\Delta_i = 2$ but they are not indeterminate.

Case (1) means that after a finite number of observed events (at most equal to the number of events of the cycle in the BRD) it is possible to be sure that no fault has occurred, thus the third condition of Definition 4.1 does not hold.

Case (2) means that a fault has certainly occurred, thus the second condition of Definition 4.1 does not hold.

Case (3) means that there do not exist two sequences σ_1 and σ_2 having the same observable projection where σ_2 is of arbitrary length, namely there do not exist two sequences satisfying the conditions in Definition 4.1. □

Corollary 7.6 *A labeled net system $\langle N, M_0, \mathcal{L}\rangle$ satisfying assumptions (A1) to (A3) is* diagnosable *iff its BRD has no cycle that is indeterminate wrt all fault classes.* ■

Example 7.7 *Let us consider the Petri net system in Fig. 1 whose BRD is given in Fig. 3. From the analysis on the indeterminate cycles reported in Example 7.4 we can conclude that the system is not diagnosable wrt both fault classes.* ■

Note that, as soon as one finds an indeterminate cycle for a fault class one can conclude that the system is not diagnosable wrt that fault class. On the contrary, to establish if a system is diagnosable wrt to a fault class it is necessary to examine all uncertain cycles for that fault class and show that none is indeterminate. A MATLAB tool for the diagnosability analysis of PNs can be found in [1]. Numerical simulations showing that, especially in the presence of highly concurrent systems, the number of basis markings is always much smaller with respect to the number of reachable markings (that increase exponentially with the size of the net) is presented in [7].

We conclude this section with a brief discussion on the complexity of the proposed approach. The size of the state space of the MBRG (and consequently of the BRD) increases exponentially with the system complexity (net structure, and number of tokens in the initial marking). Moreover, to compute diagnosability we need to examine all uncertain cycles in the BRD and the paths that lead from the initial node to each uncertain cycle. After an analysis of the complexity of the existing methods (see [18] for more details), we determined that the exhaustive enumeration of all paths in the BRD and consequent identification of the cycles is the most efficient method and its complexity is $\mathcal{O}(L^{|BRD|})$, where L is the alphabet of the PN system.

8 Comparison with the approach in [4]

Our paper presents some analogies with the paper by Jiroveanu and Boel (J&B) [4]. In this section we discuss differences and analogies between the two approaches that have been developed independently and in parallel.

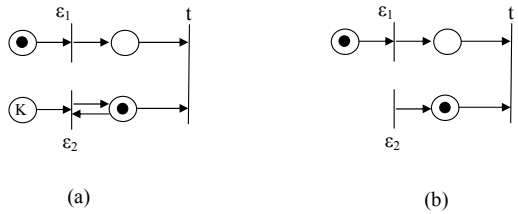

Figure 4: Two Petri net systems that show the differences between our definition of minimal explanations and the one proposed by Jiroveanu and Boel.

The diagnosability approach in [4] is also based on the notion of minimal explanation introduced in [3]. This notion is different from the one used in this paper. In fact, while our concept of minimality is based on the minimality of the firing vector, according to J&B an explanation is minimal if no transition belonging to the sequence of unobservable transitions, and preceding the observable transition, can fire after the firing of the transition itself. In the case of nets with no unobservable cycles the two definitions of minimal explanations lead to the same sequences, while in the presence of unobservable cycles this does not happen as illustrated in the following example.

Let us consider the Petri net system in Figure 4.(a). Assume the observed word is $w = t$. In our case ε_1 is the only minimal explanation, while in their case there are $K+1$ minimal explanations of the type $\varepsilon_1\varepsilon_2^i t$, for $i \in \{0, 1, \ldots, K\}$ (note that their minimal explanation also contains the observed transition). As an example $\varepsilon_1\varepsilon_2 t$ is a minimal explanation according to J&B because the sequence $\varepsilon_1 t\varepsilon_2$ can never fire (the firing of t disables ε_2).

Another difference is due to the fact that our definition of minimal explanation also applies to unbounded nets, while this is not true in the case of J&B as shown in the following example. Let us consider the Petri net system in Figure 4.(b). Assume the observed word is $w = t$. In our case ε_1 is still the minimal explanation, while this case cannot be handled by J&B since their number of minimal explanations is infinite.

The algorithms for the computation of the minimal explanations according to the two definitions are also different. The algorithm proposed by J&B in [5] is based on a backward search within the unobservable subnet. The advantage of this approach is that all sequences computed are minimal explanations, but only the subset that is compatible with the initial marking should be kept. On the contrary, the algorithm we proposed in [8] provides the firing vectors associated with the minimal explanations using algebraic manipulation of matrices. It presents the advantage that all the firing vectors computed are compatible with the initial marking, but it requires a final check to remove some explanations that are not minimal. We do not believe that one method is always preferable to the other one. In fact, our conjecture is that this depends on the structure of the unobservable subnet (in particular on the number of concurrent transitions) and on the initial marking. However, such a comparison is still an open issue.

Note that, although both us in [10, 8] and J&B in [5] use the notion of minimal explanation for the diagnosis approach, the two diagnosis procedures are totally different. Indeed, while our

procedure is based on the notion of basis marking that allows one to move the most burdensome part of the computations offline, thanks to the construction of the so called Basis Reachability Graph, the approach of J&B does not use the concept of basis marking and is an on-the-fly approach.

Concerning the differences between ROF and MBRG, we preliminary observe that, while the MBRG was introduced under the assumption of acyclicity of the unobservable subnet (structural property), the ROF was presented under the assumption that no cycle of unobservable transitions may fire (behavioral property). Thus J&B can also deal with nets whose structure contains cycles of unobservable transitions (see e.g. Figure 1 in [4]). We can state that under common assumptions on the acyclicity of the unobservable subnet the two graphs share the same structure (same nodes and edges). However the MBRG contains some additional information that have been appropriately introduced to be used in conjunction with the BRD for the analysis of the diagnosability. On the contrary ROF is defined to be used as an input for automata based diagnosability approaches, e.g. the verifier net approach [24].

Finally, we observe that beyond the differences between the two diagnostic approaches the main contribution between our approach and the one proposed in [4] consists in providing necessary and sufficient conditions for diagnosability based on the BRD.

9 Conclusions

The main contribution of this paper is to use the notion of basis markings, that overcomes the problem of the exhaustive enumeration of the state space, to solve the problem of diagnosability of bounded PNs. First we have given a necessary and sufficient condition for diagnosability. Then, we have provided a method to test the diagnosability that is based on the analysis of a diagnoser that we call *Basis Reachability Diagnoser*, in conjunction with another graph (that is used for the construction of the diagnoser) called *Modified Basis Reachability Graph*.

References

[1] http://www.diee.unica.it/giua/tesi/09_marco.pocci/pn_diag.zip. 2009.

[2] F. Basile, P. Chiacchio, and G. De Tommasi. On K-diagnosability of Petri nets via Integer linear programming. *Automatica*, 48(9):2047–2058, 2012.

[3] R.K. Boel and G. Jiroveanu. Distributed contextual diagnosis for very large systems. In *Proc. IFAC WODES'04: 7th Work. on Discrete Event Systems*, pages 343–348, September 2004.

[4] R.K. Boel and G. Jiroveanu. The Diagnosability of Petri Net Models Using Minimal Explanations. *IEEE Trans. on Automatic Control*, 55(7):1663–1668, 2010.

[5] R.K. Boel, G. Jiroveanu, and B. Bordbar. On-line monitoring of large Petri net models under partial observation. *Discrete Events Dynamical Systems*, 18:323Ű354, 2008.

[6] M.P. Cabasino, A. Giua, S. Lafortune, and C. Seatzu. A New Approach for Diagnosability Analysis of Petri Nets Using Verifier Nets. *IEEE Trans. on Automatic Control*, 57(12):3104–3117, December 2012.

[7] M.P. Cabasino, A. Giua, L. Marcias, and C. Seatzu. A comparison among tools for the diagnosability of discrete event systems. In *Proc. 8th IEEE Conf. on Automation Science and Engineering*, Seoul, Korea, August 2012.

[8] 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.

[9] M.P. Cabasino, A. Giua, and C. Seatzu. Diagnosability of bounded Petri nets. In *Proc. 48th IEEE Conf. on Decision and Control*, Shangai, China, December 2009.

[10] 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.

[11] S.L. Chung. Diagnosing PN-based models with partial observable transitions. *International Journal of Computer Integrated Manufacturing*, 12 (2):158–169, 2005.

[12] 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.

[13] S. Haar. Qualitative diagnosability of labeled Petri nets revisited. In *Proc. 48th IEEE Conf. on Decision and Control*, Shanghai, China, December 2009.

[14] 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.

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

[16] A. Madalinski, F. Nouioua, and P. Dague. Diagnosability verification with Petri net unfoldings. *International Journal of Knowledge-Based and Intelligent Engineering Systems*, 14(2):49–55, 2010.

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

[18] M. Pocci. A Toolbox for place/transition net diagnosability. Master's thesis, Dep. Electric and Electronic Engineering, University of Cagliari, Cagliari, Italy, 2009. (In Italian).

[19] 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.

[20] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Failure diagnosis using discrete-event models. *IEEE Trans. on Control Systems Technology*, 4(2):105–124, 1996.

[21] T. Ushio, L. Onishi, and K. Okuda. Fault detection based on Petri net models with faulty behaviors. In *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, San Diego, CA, USA, October 1998.

[22] Y. Wen and M. Jeng. Diagnosability analysis based on T-invariants of Petri nets. In *Proc. IEEE Networking, Sensing and Control*, Tucson, Arizona, March 2005.

[23] Y. Wen, C. Li, and M. Jeng. A polynomial algorithm for checking diagnosability of Petri nets. In *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, Hawaii, USA, October 2005.

[24] T.-S. Yoo and S. Lafortune. Polynomial-time verification of diagnosability of partially observed discrete-event systems. *IEEE Trans. on Automatic Control*, 47(9):1491–1495, 2002.