Diagnosability of bounded Petri nets

Maria Paola Cabasino, Alessandro Giua, Carla Seatzu

Abstract

In this paper we present an approach to solve the problem of diagnosability of bounded Petri net systems. 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. The first graph is called *basis reachability diagnoser*, the second one is called *modified basis reachability graph*.

Published as:

M.P. Cabasino, A. Giua, C. Seatzu, ”Diagnosability of bounded Petri nets,” CDC09: 48th IEEE Conf. on Decision and Control (Shanghai, China), Dec. 2009.

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

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, {cabasino,giua,seatzu}@diee.unica.it

I. INTRODUCTION

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.

This problem has been extensively studied within the framework of automata, and diagnosability was first formally defined by Sampath *et al.* in [1], [2]. On the contrary, very few results have been proposed within the framework of Petri nets (PNs). Ushio *et al.* [3] presented a sufficient condition for diagnosability of unbounded PNs based on indeterminate cycles defined as in [1], [2]. Chung in [4], in contrast with Ushio's paper, assumes that part of the transitions of the PN is observable and shows as the additional information from observed transitions in general adds diagnosability to the analyzed system. In [5] Wen and Jeng propose an approach to test diagnosability by checking the structure property of T-invariant of the nets. In [6] Wen *et al.* present an algorithm, based on a linear programming problem, of polynomial complexity in the number of nodes for computing a sufficient condition of diagnosability of discrete event systems modeled by PNs. Finally, in [7] we present an approach for diagnosability of labeled *unbounded* PNs. The ideas behind the two approaches are completely different. In particular, in [7] we give necessary and sufficient conditions for diagnosability and present a test to analyze diagnosability based on the coverability graph of a particular net, called *verifier net*, built from the PN model of the system to be diagnosed. In this paper we solve the problem of diagnosability of *bounded* PNs using an approach based on the notion of basis markings. The main advantage of this approach is that it does not require the exhaustive enumeration of the state space. Moreover the approach in this paper also allows us to perform diagnosis, namely to evaluate the diagnosis state of the system after each observation, both in the case of bounded and unbounded PNs (see [8]).

This paper is based on our results in [8]–[10]. In these papers we presented an approach for diagnosis of PNs where fault transitions are assumed to be unobservable, but there also exist other transitions that are unobservable as well and that model regular behavior. In particular, while in [9], [10] we only consider free-labeled PNs, thus all transitions that are observable are also distinguishable, in [8] we extend such an approach to arbitrary labeled PNs, and the observable events are the labels associated to transitions. In both cases the proposed diagnosis approach is based on the notions of *minimal explanations* and *basis markings*, and allow us to represent the reachability space in a compact manner. Moreover, in the case of bounded systems,

we showed how the most burdensome part of the procedure can be moved off-line, constructing a particular graph called *basis reachability graph* (BRG).

In this paper we focus on bounded PN systems: we provide a necessary and sufficient condition for diagnosability and give a systematic method to analyze the diagnosability of a given PN system. Such a method requires 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 BRG. 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 proposed results are inspired by the diagnosability approach for finite state automata proposed by Sampath *et al.* [1], [2]. 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.

II. Background on labeled Petri nets

In this section we recall the formalism used in the paper. For more details on PNs we refer to [11].

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; $Pre: P \times T \rightarrow \mathbb{N}$ and $Post: P \times T \rightarrow \mathbb{N}$ are the pre– and $post$– incidence functions that specify the arcs; $C = Post - Pre$ is the incidence matrix.

A *marking* is a vector $M: P \rightarrow \mathbb{N}$ 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'.

The set of all sequences that are enabled at the initial marking M_0 is denoted $L(N, M_0)$, i.e., $L(N, M0) = \{\sigma \in T^* \mid M[\sigma\rangle\}$.

Given a sequence $\sigma \in T^*$, we call $\pi: T^* \rightarrow \mathbb{N}^n$ the function that associates to 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*. For this subclass the following result holds.

***Theorem** 2.1 ([12]):* 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 to σ is equal to y.

(ii) A marking M is reachable from M_0 iff there exists a non negative 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* $\mathcal{L} : T \to L \cup \{\varepsilon\}$ assigns to each transition $t \in T$ either a symbol from a given alphabet L or the empty string ε.

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*.

In this paper we assume that the same label $l \in L$ can be associated to more than one transition. Two transitions $t_1, t_2 \in T_o$ are called *undistinguishable* if they share the same label, i.e., $\mathcal{L}(t_1) = \mathcal{L}(t_2) = l \in L$. The set of transitions sharing the same label l are denoted as T_l. Transitions in T_o are called *observable*.

In the following we denote as 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).

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

***Definition** 2.2:* Let $\langle N, M_0\rangle$ be a labeled PN system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, 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 $w \in L^*$. ■

In plain words, given an observation w, $\mathcal{S}(w)$ is the set of sequences that may have fired.

***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 restriction of $Pre, Post$ to T'. The net N' can be thought as obtained from N removing all transitions in $T \setminus T'$. We also write $N' \prec_{T'} N$. ■

III. Problem Statement

Assume that 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. When an observable transition fires we observe its label, thus our observations consist in sequences of symbols in the alphabet L.

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 (modeling anomalous or fault behavior), while T_{reg} includes all transitions relative to unobservable but regular events. 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.

***Definition** 3.1:* A live PN system $\langle N, M_0 \rangle$ is said *diagnosable with respect to* (wrt) *a fault class* T_f^i if there do not exist two sequences σ_1 and σ_2 in T^* satisfying the following conditions:

- $\mathcal{L}(\sigma_1) = \mathcal{L}(\sigma_2)$,
- $\forall t_f \in T_f^i$, $t_f \notin \sigma_1$,
- $\exists$ at least one $t_f \in T_f^i$ such that $t_f \in \sigma_2$,
- σ_2 can be made arbitrarily long after a fault $t_f \in T_f^i$.

■

***Definition** 3.2:* A PN system $\langle N, M_0 \rangle$ is said *diagnosable* if it is diagnosable wrt all fault classes. ■

Note that the diagnosability of a system does not imply that we are able to distinguish among transitions in the same class. It simply implies that if one or more transitions in a given fault class have fired, then after a finite number of observations we are able to establish that at least one transition of that class has fired.

In this paper we investigate the problem of providing necessary and sufficient conditions for diagnosability. In particular, we consider labeled PN systems under the following assumptions.

A1) The net system $\langle N, M_0 \rangle$ is *bounded* and *does not deadlock after the firing of any fault transition*.

A2) The T_u-induced subnet is *acyclic*.

A3) The labeling function $\mathcal{L} : T_o \to L$ may associate the same label to different transitions.

A4) The structure of N is known as well as the initial marking M_0.

IV. Basic definitions and results

In this section we recall some basic definitions and results we first introduced in [8], [9].

***Definition** 4.1 ([9]):* Given a marking M and a transition $t \in T_o$, we define

$$\Sigma_{\min}(M,t) = \{\sigma \in T_u^* \;\; | \;\; M[\sigma\rangle M',\; M' \geq Pre(\cdot,t),\; \nexists\, \sigma' \;\; | \;\; M[\sigma'\rangle M'',\; M'' \geq Pre(\cdot,t) \;\; : \;\; \pi(\sigma') \lneqq \pi(\sigma)\}$$

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 the case of labeled PNs what we observe is a label l. Thus, it is useful to define the following sets.

***Definition** 4.2 ([8]):* Given a marking M and an observation $l \in L$, 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). ■

Obviously, in the above sets $\hat{\Sigma}_{\min}(M,l)$ and $\hat{Y}_{\min}(M,l)$ different sequences σ and different e-vectors e, respectively, are associated in general to the same transition $t \in T_l$.

Given a word $w \in L^*$ we call *justification of w* the corresponding sequence of unobservable transitions interleaved with σ_o whose firing enables σ_o and whose firing vector is minimal.

***Definition** 4.3 ([8]):* Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be a given observation. We define

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

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

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

the set of couples (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 couples sequence $\sigma_o \in T_o^*$ labeled w – justification and the firing vectors of these sequences are called *j-vectors*.

***Definition** 4.4 ([8]):* Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, 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 couple (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*). ■

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.

***Definition** 4.5 ([8]):* Let $\langle N, M_0\rangle$ be a net system with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w \in L^*$ be an observed word. We define

$$\begin{aligned}\mathcal{M}(w) = \{(M, y) \mid\ \ &(\exists \sigma \in \mathcal{S}(w)\ :\ M_0[\sigma\rangle M) \wedge \\ &(\exists (\sigma_o, \sigma_u) \in \hat{\mathcal{J}}(w)\ :\ \sigma_o = P_o(\sigma), \\ &\qquad \sigma_u = P_u(\sigma),\ y = \pi(\sigma_u))\}\end{aligned}$$

the set of couples (basis marking – relative j-vector) that are *consistent* with $w \in L^*$. ■

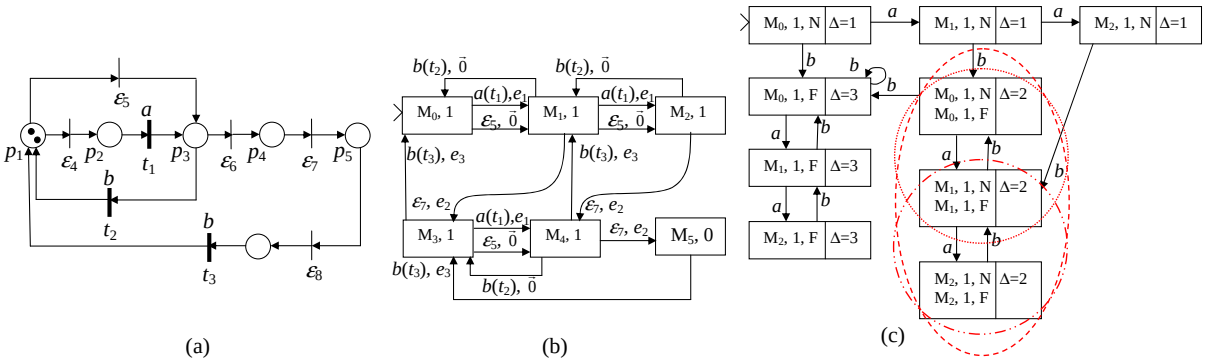

Fig. 1. A PN (a), its MBRG (b) and its BRD (c).

Note that the set $\mathcal{M}(w)$ does not keep into account the sequences of observable transitions that may have actually fired. It only keeps track of the basis markings that can be reached and of the sequences of unobservable transitions that have fired to reach them. Indeed, this is the information really significant when performing diagnosis. The notion of $\mathcal{M}(w)$ is fundamental to provide a recursive way to compute the set of minimal explanation.

***Proposition** 4.6 ([8]):* Given a net system $\langle N, M_0\rangle$ with labeling function $\mathcal{L} : T \to L \cup \{\varepsilon\}$, where $N = (P, T, Pre, Post)$ and $T = T_o \cup T_u$. Let $w = w'l$ be a given observation.

The set $\hat{Y}_{\min}(M_0, w'l)$ is defined as:

$$\begin{aligned}\hat{Y}_{\min}(M_0, w'l) = \quad & \{(\sigma_o, y) \mid \sigma_o = \sigma'_0 t \wedge y = y' + e \ : \\ & (\sigma'_o, y') \in \hat{Y}_{\min}(M_0, w'), \\ & (t, e) \in \hat{Y}_{\min}(M'_b, l) \text{ and } \mathcal{L}(t) = l\},\end{aligned}$$

where $M'_b = M_0 + C_u \cdot y' + C_o \cdot \pi(\sigma'_o)$.

***Example** 4.7:* Let us consider the PN in Fig. 1.(a), where the set of observable transitions is $T_o = \{t_1, t_2, t_3\}$ and the set of unobservable transitions is $T_u = \{\varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7, \varepsilon_8\}$. The labeling function is $\mathcal{L}(t_1) = a$ and $\mathcal{L}(t_2) = \mathcal{L}(t_3) = b$.

Let us assume $w = ab$. The set of justifications is $\hat{\mathcal{J}}(w) = \{(t_1t_2, \varepsilon_4), (t_1t_3, \varepsilon_4\varepsilon_6\varepsilon_7\varepsilon_8)\}$ and the set of j-vectors is $\hat{Y}_{min}(M_0, w) = \{(t_1t_2, [1\ 0\ 0\ 0\ 0]^T), (t_1t_3, [1\ 0\ 1\ 1\ 1]^T)\}$. The above j-vectors lead to the same basis marking $M_0 = [2\ 0\ 0\ 0\ 0\ 0]^T$. Thus $\mathcal{M}(w) = \{(M_0, [1\ 0\ 0\ 0\ 0]^T), (M_0, [1\ 0\ 1\ 1\ 1]^T)\}$.

■

V. DIAGNOSIS USING PETRI NETS

***Definition** 5.1 ([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 to each observation w and to 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 in T_f^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 $t_f \notin \sigma_u$.

In such a case a fault transition of the ith class may have occurred but is not contained in any justification of 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 $t_f \in \sigma_u$;

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

In such a case a fault transition in the ith class is contained in one (but not in all) justification of w.

- $\Delta(w, T_f^i) = 3$ 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 transition in the ith class. ■

***Proposition** 5.2 ([9]):* Consider an observed word $w \in L^*$.

- $\Delta(w, T_f^i) \in \{0, 1\}$ iff for all $(M, y) \in \mathcal{M}(w)$ and for all $t_f \in T_f^i$ it holds $y(t_f) = 0$.
- $\Delta(w, T_f^i) = 2$ iff there exist $(M, y) \in \mathcal{M}(w)$ and $(M', y') \in \mathcal{M}(w)$ such that:
  (i) there exists $t_f \in T_f^i$ such that $y(t_f) > 0$,
  (ii) for all $t_f \in T_f^i$, $y'(t_f) = 0$.
- $\Delta(w, T_f^i) = 3$ iff for all $(M, y) \in \mathcal{M}(w)$ there exists $t_f \in T_f^i$ such that $y(t_f) > 0$.

***Proposition** 5.3 ([9]):* For a PN whose unobservable subnet is acyclic, let $w \in L^*$ be an observed word such that for all $(M, y) \in \mathcal{M}(w)$ it holds $y(t_f) = 0 \ \forall \ t_f \in T_f^i$.

Let us consider the constraint set

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

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

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

***Example** 5.4:* Let us consider again the PN in Fig. 1.(a), where $T_f = \{\varepsilon_5, \varepsilon_7\}$.

Let $w = ab$. It is $\mathcal{M}(w) = \{(M_0, [1\ 0\ 0\ 0\ 0]^T), (M_0, [1\ 0\ 1\ 1\ 1]^T)\}$, where $M_0 = [2\ 0\ 0\ 0\ 0\ 0]^T$ is the initial marking and has been computed in Example 4.7. In such a case it is $\Delta(w, T_f) = 2$. In fact, $y_1 = [1\ 0\ 0\ 0\ 0]^T$ does not contain a fault transition $t_f \in T_f$, while $y_2 = [1\ 0\ 1\ 1\ 1]^T$ contains ε_7. ■

In [9] we have shown that in the case of bounded PNs a useful tool to perform diagnosis is the *Basis Reachability Graph* (BRG). In particular, it enables us to move off-line the most burdensome part of the procedure. In [8] we showed how the BRG can still be defined in the case of arbitrary labeled PNs.

VI. Modified Basis Reachability Graph

The BRG needs to be modified if we want to use it as an auxiliary tool to establish if the system is diagnosable. To this aim we define a new graph, that we call *Modified Basis Reachability Graph* (MBRG).

The MBRG is a deterministic graph whose nodes contain two elements (M, x): $M \in \mathbb{N}^m$ is a marking defined as below, and x is a row vector in $\{0, 1\}^r$, where $x(i) = 1$ if $\mathcal{T}(M)$ in (1) is feasible wrt the ith class, $x(i) = 0$ otherwise.

Markings M in the nodes are defined as basis markings computed assuming that all fault transitions are observable. This means that minimal explanations are restricted to transitions in T_{reg}.

In the following we denote as $Y^{mod}_{\min}(M,t)$ 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, the label contains three informations summarized as $(l(t), e)$, 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 the label only contains two informations summarized as (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** 6.1:* **[Computation of the MBRG]**

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

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

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 couple (M', x') where $\forall i = 1, \ldots, r$,

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

  - add arc $(l(t), e)$ from

node (M, x) to node (M', x')

2.4. for all $i = 1, \ldots, r \ : \ x(T_f^i) = 1$

2.4.1. for all $t_f \in T_f^i : Y_{\min}^{mod}(M, t_f) \neq \emptyset$, do

- for all $e \in Y_{\min}^{mod}(M, t_f)$, 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 couple (M', x') where $\forall i = 1, \ldots, r$,

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

  - 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 $M_0 + C_u \cdot e$ ($e \in Y_{\min}^{mod}(M_0, t)$ or $e \in Y_{\min}^{mod}(M_0, t_f)$, respectively). If a new couple (marking, binary vector) is obtained, a new node is added to the graph, containing 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.

Note that if the net is bounded the procedure terminates in a finite number of steps because the number of nodes is upper limited by the cardinality of the set $R(N, M_0)$.

***Example** 6.2:* In Fig. 1.(b) is shown the MBRG corresponding to the PN in Fig. 1.(a) (introduced in Examples 4.7 and 5.4). Here $M_1 = [1\ 0\ 1\ 0\ 0\ 0]^T$, $M_2 = [0\ 0\ 2\ 0\ 0\ 0]^T$, $M_3 = [1\ 0\ 0\ 0\ 1\ 0]^T$, $M_4 = [0\ 0\ 1\ 0\ 1\ 0]^T$, $M_5 = [0\ 0\ 0\ 0\ 2\ 0]^T$, $e_1 = [1\ 0\ 0]^T$, $e_2 = [0\ 1\ 0]^T$ and

$e_3 = [0\ 0\ 1]^T$.

Each node contains a different marking and a scalar (because there is only one fault class). As an example, the scalar 1 is associated to M_0 because $\mathcal{T}(M_0)$ is feasible.

Arcs are labeled either by (label (relative transition), corresponding modified minimal e-vector) (see e.g. $(a(t_1), e_1)$ from the initial node), or by (unobservable transition, corresponding modified minimal e-vector) (see e.g. (ε_7, e_2) from M_1).

Finally, let us observe that not all the markings in the nodes are basis markings. Precisely, M_0, M_1, and M_2 are basis markings, while M_3, M_4, M_5 are markings reached from basis markings firing the fault transitions ε_5 and ε_7. This shows that memory requirements necessary to solve the problem of diagnosability are greater than those required to perform diagnosis. Note however, that the number of markings in the MBRG is equal to the number of consistent markings only in the worst case, but in general is smaller, as in this example. ■

VII. Basis Reachability Diagnoser

In this section we define a diagnoser called *Basis Reachability Diagnoser* (BRD). It is a deterministic graph that, used in addition with the MBRG, allows us to state necessary and sufficient conditions for diagnosability.

***Definition** 7.1:* The BRD is a deterministic graph where each node contains the following items:

- one or more triples (M, x, h), where:
  - M is a basis marking;
  - $x \in \{0,1\}^{|T_f|}$ is a row vector whose ith entry is equal to 1 if $\mathcal{T}(M)$ is feasible wrt the ith class, and is equal to 0 otherwise;
  - $h \in \{N, F\}^{|T_f|}$ 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 readable 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 couple 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 couple 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 couple M, x may appear twice in the same node, both with $h(i) = F$ and with $h(i) = N$.

The diagnosis state for each fault class is trivially obtained by definition just looking at the last two entries 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 $|T_f| = r$.

***Algorithm** 7.2:* **[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 entry of x_0 associated to 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 couple (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.

***Example** 7.3:* In Fig. 1.(c) is reported the BRD of the PN in Fig. 1.(a), where $T_f = \{\varepsilon_5, \varepsilon_7\}$.

The initial node contains the triple $(M_0, 1, N)$ and its diagnosis state is $\Delta = 1$ being $x_0 = 1$. From this node a and b are both enabled and they lead respectively to node $(M_1, 1, N)$ and to node $(M_0, 1, F)$. The diagnosis state of these two nodes is $\Delta = 1$ and $\Delta = 3$, respectively. In fact $(M_1, 1, N)$ is reached firing no fault transition ($h = N$) but it is $x = 1$, while the second node has only one triple having $h = F$.

Finally, the node reached from $(M_1, 1, N)$ firing b has diagnosis state $\Delta = 2$. In fact, it is composed by two triples, one with $h = N$ and the other one with $h = F$. ■

VIII. 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 have to check if the BRD contains an uncertain cycle, namely a potential indeterminate cycle, and then using the MBRG to verify if that cycle is indeterminate or not.

***Definition** 8.1:* Let γ be a cycle in the BRD with observable projection $\rho \in L^*$ and let $p \in L^*$ be a path from the initial node to any node of the cycle. The cycle γ is *uncertain* wrt a fault class T_f^i if it only includes states with $\Delta_i = 2$, or $\Delta_i = 1$, or $\Delta_i = 1$ and $\Delta_i = 2$. ■

***Definition** 8.2:* Let γ be an uncertain cycle in the BRD with observable projection $\rho \in L^*$ and let $p \in L^*$ be a path from the initial node to any node of the cycle. 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) their observable projection is equal to ρ;

(ii) there exist two paths p_1 and p_2 with observable projection p, that from the initial node in the MBRG enable γ_1 and γ_2;

(iii) both γ_2 and p_2 do not contain a fault in T_f^i, while either γ_1 or p_1 or both contain a fault in T_f^i. ■

***Example** 8.3:* Let us consider the BRD in Fig. 1.(c) corresponding to the PN in Fig. 1.(a). The dotted ellipses represent the uncertain cycles for the unique fault class.

Let us consider in the BRD the uncertain cycle $\gamma = [(M_0, 1, N), (M_0, 1, F)] \underrightarrow{a} [(M_1, 1, N), (M_1, 1, F)] \underrightarrow{b} [(M_0, 1, N), (M_0, 1, F)]$ for which $\rho = ab$ and $p = [(M_0, 1, N)] \underrightarrow{a} [(M_1, 1, N)] \underrightarrow{b}$. Looking at the MBRG in Fig. 1.(b) we can see that this cycle is indeterminate since conditions of Definition 8.2 are satisfied. In fact, in the MBRG there exist two cycles $\gamma_1 = (M_0, 1)\underrightarrow{a(t_1)}(M_1, 1)\underrightarrow{\varepsilon_7}(M_3, 1)\underrightarrow{b(t_3)}(M_0, 1)$ and $\gamma_2 = (M_0, 1)\underrightarrow{a(t_1)}\ (M_1, 1)\underrightarrow{b(t_2)}(M_0, 1)$ having the same observable projection ρ and there exist two paths $p_1 = p_2 = (M_0, 1)\underrightarrow{a(t_1)}\ (M_1, 1)\underrightarrow{b(t_2)}(M_0, 1)$ having the same observable projection of p and that from the initial node enable γ_1 and γ_2. Finally both p_2 and γ_2 do not contain fault transitions, while γ_1 contains ε_4. ■

***Theorem** 8.4:* A net system $\langle N, M_0 \rangle$ satisfying assumptions (A1) to (A4) is *diagnosable* wrt the fault class T_f^i iff its BRD has no cycle that is indeterminate wrt T_f^i.

Proof: We prove the if and only if statements separately.

(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 satisfying conditions (i) to (iii) in Definition 8.2. This obviously implies that there exist two sequences relative to $p_1\gamma_1$ and $p_2\gamma_2$ having the same observable projection, one containing a fault in the ith class and the other one not, that can be made arbitrary long, because γ_1 and γ_2 can be repeated an arbitrary large number of times. Thus, by Definition 3.1 the system is not diagnosable wrt to the ith class.

(Only if) Assume that the BRD has no cycle that is indeterminate wrt T_f^i. By Definition 3.1 the other sequences that may potentially lead to a violation of the diagnosability property because they have the same observable projection and can be made arbitrary long, 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 item of Definition 3.1 may never happen.

Case (2) means that a fault has occurred for sure, thus the second item of Definition 3.1 may never hold.

Case (3) means that there do not exist two sequences σ_1 and σ_2 having the same observable projection where σ_2 can be made arbitrary long, namely there do not exist two sequences satisfying the conditions in Definition 3.1. □

Corollary *8.5:* A net system $\langle N, M_0 \rangle$ satisfying assumptions (A1) to (A4) is *diagnosable* iff its BRD has no cycle that is indeterminate wrt all fault classes. ■

Example *8.6:* Let us consider the PN system in Figure 1.(a) whose BRD is given in Figure 1.(c). From the analysis of the indeterminate cycles reported in Example 8.3 we can conclude that the system is not diagnosable. ■

IX. Conclusions

In this paper we presented an approach to solve the problem of diagnosability of bounded PNs based on the concept of *basis marking*, that allows us to represent the reachability space in a compact manner. We first give a necessary and sufficient condition for diagnosability. Then, we provide 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] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. Automatic Control*, vol. 40 (9), pp. 1555–1575, 1995.

[2] ——, "Failure diagnosis using discrete-event models," *IEEE Trans. Contr. Syst. Tech*, vol. 4 (2), pp. 105–124, 1996.

[3] T. Ushio, L. Onishi, and K. Okuda, "Fault detection based on Petri net models with faulty behaviors," in *Proc. SMC'98: IEEE Int. Conf. on Systems, Man, and Cybernetics (San Diego, CA, USA)*, Oct. 1998, pp. 113–118.

[4] S. Chung, "Diagnosing pn-based models with partial observable transitions," *International Journal of Computer Integrated Manufacturing*, vol. 12 (2), pp. 158–169, 2005.

[5] Y. Wen and M. Jeng, "Diagnosability analysis based on t-invariants of Petri nets," in *Networking, Sensing and Control, 2005. Proceedings*, Mar. 2005, pp. 371– 376.

[6] Y. Wen, C. Li, and M. Jeng, "A polynomial algorithm for checking diagnosability of Petri nets," in *Proc. SMC'05: IEEE Int. Conf. on Systems, Man, and Cybernetics*, Oct. 2005, pp. 2542– 2547.

[7] M. Cabasino, A. Giua, S. Lafortune, and C. Seatzu, "Diagnosability analysis of unbounded Petri nets," in *Proc. 48th IEEE Conf. on Decision and Control*, Dec. 2009.

[8] M. Cabasino, A. Giua, and C. Seatzu, "Diagnosis of discrete event systems using labeled Petri nets," in *Proc. 2nd IFAC Workshop on Dependable Control of Discrete Systems (Bari, Italy)*, Jun. 2009.

[9] ——, "Fault detection for discrete event systems using Petri nets with unobservable transitions," *Automatica*, (Preliminary accepted).

[10] A. Giua and C. Seatzu, "Fault detection for discrete event systems using Petri nets with unobservable transitions," in *Proc. 44th IEEE Conf. on Decision and Control*, Dec. 2005, pp. 6323–6328.

[11] T. Murata, "Petri nets: properties, analysis and applications," *Proceedings of the IEEE*, vol. 77, no. 4, 1989.

[12] D. Corona, A. Giua, and C. Seatzu, "Marking estimation of Petri nets with silent transitions," in *Proc. IEEE 43rd Int. Conf. on Decision and Control (Atlantis, The Bahamas)*, Dec. 2004.