Automatica 48 (2012) 2047–2058

Contents lists available at SciVerse ScienceDirect

Automatica

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

On $\mathcal{K}$-diagnosability of Petri nets via integer linear programming☆

F. Basile [a], P. Chiacchio [a], G. De Tommasi [b,1]

[a] Dipartimento di Ingegneria Elettronica ed Ingegneria Informatica, Università degli Studi di Salerno, Salerno, Italy

[b] Dipartimento di Informatica e Sistemistica, Università degli Studi di Napoli Federico II, Napoli, Italy

ARTICLE INFO

Article history:
Received 29 December 2010
Received in revised form
11 January 2012
Accepted 12 April 2012
Available online 11 July 2012

Keywords:
Diagnosability
Discrete event systems
Petri nets
Integer linear programming

ABSTRACT

This paper deals with the problem of diagnosability of a fault after the firing of a finite number events (i.e., $\mathcal{K}$-diagnosability). This problem corresponds to diagnosability of a fault within a finite *delay* in the context of discrete event systems. The main contribution of this paper is a necessary and sufficient condition for $\mathcal{K}$-diagnosability of bounded nets. The proposed approach exploits the mathematical representation of Petri nets and the Integer Linear Programming optimization tool. In particular no specific assumptions are made on the structure of the net induced by the unobservable transitions, since the proposed approach permits to detect also the undiagnosability due to the presence of *unobservable cycles*.

1. Introduction

The fault diagnosis is crucial for the safety of both systems and operators in industry. Fault diagnosis has received a lot of attention in the discrete event systems (DES) community since the early 90s (Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1995). Diagnosability of DES deals with the possibility of detecting, within a finite delay, the occurrences of *unobservable* fault events using the record of observed events. Fault detection consists of on-line monitoring the system using the record of observed events to timely provide the set of faults that could have happened.

The formal definition of diagnosability has been given in the framework of finite state automata and regular languages (Sampath et al., 1995; Zad, Kwong, & Wonham, 2005). Necessary and sufficient conditions for diagnosability of DES modeled as automata have been given in Sampath et al. (1995). The diagnosability test is based on another automaton called *diagnoser* which gives, after each observed event, a set of faults that could have happened (Sampath et al., 1995), or a set of fault states that the system could have reached (Zad et al., 2005). The *diagnoser approach* has been used to extend the diagnosability concept to stochastic automata (Lunze & Schröder, 2001), and to the decentralized case (Debouk, Lafortune, & Teneketzis, 2000). The concept of diagnosability itself has been also extended in Paoli and Lafortune (2005).

The problem of diagnosability has been recently tackled within the Petri nets (PNs) framework. PNs have a twofold representation: graphical and mathematical. The mathematical representation of PNs allows use of standard tools, such as Integer Linear Programming, to solve DES diagnosis problems. The graphical nature helps to recognize if a model belongs to a certain net subclass. If this is the case, efficient algorithms that exploit the peculiarity of a given subclass can be devised. Furthermore, the local state representation often helps in reducing both computational complexity and memory requirements when solving the diagnosis problem. Indeed, the building of a diagnoser requires the exploration of the state space, whose number of nodes grows exponentially with respect to the net size.

Although a number of results are now available for fault detection when DESs are modeled as PNs, only few of them are available for diagnosability. Two approaches are mainly adopted when PNs are used:

(1) the first consists in computing a graph from a net system; diagnosability test and/or online fault detection are then performed by using this graph;
(2) the second provides algorithms which perform the diagnosability test and/or online fault detection working directly on the net model. In this case the mathematical representation of PNs is exploited.

As for approach (1), in Ushio, Onishi, and Okuda (1998) the concept of diagnosability is formulated for PN systems, and a diagnoser-based approach is used to check this property assuming that the

☆ The material in this paper was partially presented at the 10th International Workshop on Discrete Event Systems (WODES'10), August 30–September 1, 2010, Berlin, Germany. This paper was recommended for publication in revised form by Associate Editor Jan Komenda under the direction of Editor Ian R. Petersen.

E-mail addresses: fbasile@unisa.it (F. Basile), pchiacchio@unisa.it (P. Chiacchio), detommas@unina.it (G. De Tommasi).

[1] Tel.: +39 0817683853; fax: +39 0817683816.

0005-1098/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.automatica.2012.06.039

net marking is observable, all transitions are not observable, and the faults are associated to transitions. in this case the diagnoser turns to be equal to the reachability graph of the PN system with some additions. A sufficient condition for diagnosability of unbounded PNs is also presented. In Chung (2005) Chung presents a similar approach adding the assumption that some transitions are observable.

In Cabasino, Giua, and Seatzu (2009b) two graphs are presented, the *modified basis reachability graph* (MBRG) and the *basis reachability diagnoser* (BRD), assuming that the net marking is not observable. This approach is derived from the one proposed by the same authors in Cabasino, Giua, and Seatzu (2010) for fault detection, and it recalls the idea of reduced observer for fault detection proposed by Boel et al. in Boel and Jiroveanu (2004). Both the approaches proposed in Boel and Jiroveanu (2004) and Cabasino et al. (2010) require the PN model to be bounded. Although in most of the cases these two graphs are in general smaller than the reachability graph, the procedure proposed to build the MBRG can require a number of steps equal to the cardinality of the reachability set. Furthermore, the proposed diagnosability test requires to check the existence of cycles in the BRD, which, in the worst case, is a task with exponential complexity in time (Sampath, Sengupta, Lafortune, Sinnamohideen, & Teneketzis, 1996; Zad, Kwong, & Wonham, 2003).

Similarly, in Jiroveanu and Boel (2010) a automata called *ROF-automaton*, which may have state space that is significantly smaller than the reachability graph, is proposed to check diagnosability of bounded nets without unobservable cycles.

In their recent work (Cabasino, Giua, Lafortune, & Seatzu, 2009a), Cabasino et al. have also presented a necessary and sufficient condition for unbounded nets, which is based on the analysis of a net, called *verifier net*, that is built from the initial system. As in Cabasino et al. (2009b), the proposed approach for unbounded nets requires to search for the existence of cycles in the coverability graph of the verifier net, which is computationally demanding. Furthermore, the authors claim that when applicable the approach proposed in Cabasino et al. (2009b) may be preferable to the one in Cabasino et al. (2009a), because it also allows to solve the diagnosis problem within the same framework.

Different papers deal also with approach (2). In particular, using the assumption that the net marking and the transitions set are partially observable, and investigating the relation between diagnosability and the properties of the T-invariants of the net, a sufficient condition for diagnosability based on linear programming is proposed in Wen, Li, and Jeng (2005). In Trevino, Ruiz-Beltran, Rivera-Rangel, and Lopez-Mellado (2007) a sufficient condition has also been presented for safe and strongly connected PNs with an output function that associates an output vector to each net marking (interpreted PNs). Two sufficient conditions have been presented by the authors in Basile, Chiacchio, and De Tommasi (2008): the first is for undiagnosability of a fault transition t_f, while the second is for diagnosability of t_f. Such conditions use the concept of g-marking introduced for online fault detection in Basile, Chiacchio, and De Tommasi (2009a).

For the sake of completeness, different approaches to the fault diagnosis of DES modeled by PNs have been proposed in Lefebvre and Delherm (2007) and Wu and Hadjicostis (2005). In both cases it is assumed that the net marking is partially (Lefebvre & Delherm, 2007) or completely (Wu & Hadjicostis, 2005) observable, even if unobservable events (transitions) are admitted. However, they do not explicitly address the problem of diagnosability.

1.1. Contribution of the paper

This paper addresses the problem of $\mathcal{K}$-diagnosability of a fault in a DES modeled as a Petri net. This problem corresponds to the diagnosability of a fault within a finite *delay* (i.e., in $\mathcal{K}$ steps). The main result of this paper is a necessary and sufficient condition for $\mathcal{K}$-diagnosability of bounded nets. The proposed approach exploits the mathematical representation of Petri nets and the Integer Linear Programming (ILP) standard optimization tool, which has been recently used in Basile et al. (2009a), Basile, Chiacchio, and De Tommasi (2009b) and Dotoli, Fanti, and Mangini (2009) to successfully solve the fault detection problem.

The concept of $\mathcal{K}$-diagnosability has been originally formulated in Sampath et al. (1995) in the context of fault detection with automata. By definition, if a fault transition is diagnosable then there exists a minimum value $\bar{\mathcal{K}}$ such that it is also $\bar{\mathcal{K}}$-diagnosable. In the automata context, given an integer $\mathcal{K}$, $\mathcal{K}$-diagnosability can be checked by means a path search on the diagnoser (see Sampath et al., 1995, Corollary 1); furthermore the related concept of k-diagnoser has been recently adopted also to study the sensor minimization problem (Cassez, Tripakis, & Altisen, 2007). Although the concept of $\mathcal{K}$-diagnosability has been firstly extended to PNs by Cabasino et al. (2009a), the present paper is one of the few that deal with this subject within the PNs context without relying on a diagnoser-based approach.

The idea developed in this work is to characterize every sequence u, that enables a fault f from the initial marking, and every sequence v that continues the system evolution after the fault occurrence, in terms of two sets of firing count vectors satisfying a set of linear constraints. A second set of linear constraints is used to characterize, in terms of firing count vectors, the sequences of unobservable transitions which enable, and thus explain, the firing of the projection of u and v over the set of observable transitions. These two sets of constraints allow us to formulate the diagnosability of f as an integer linear programming problem.

As the conclusion of this section we would like to point out the main features of the proposed approach and some differences between this work and Cabasino et al. (2009a,b), which are the ones strictly related to the present work, and which give necessary and sufficient conditions for diagnosability of both bounded and unbounded nets. In particular, the proposed approach:

(1) uses a standard tool to check diagnosability, preventing the computation of a graph;
(2) does not require any specific assumption on the structure of the net induced by the unobservable transitions, while this net is supposed to be acyclic in Cabasino et al. (2009a,b); in literature such an assumption is usually exploited in order to being able to build the *diagnoser*, which is then used to check diagnosability. The proposed approach does not rely on a diagnoser, since it solves ILPs in order to detect the undiagnosability. In particular, the considered constraints include the state equation and the transition enabling conditions. Thanks to these constraints it is possible to avoid the spurious solutions obtained when only the state equation is used and when there are *unobservable cycles*;
(3) allows to check *practical* diagnosability, specifying a *quantitative* bound for the number of events in the continuation of u, i.e., it specifies an upper bound for the number of events that are needed to detect a fault. Given an integer $\mathcal{K}$, we provide a set of conditions that need to be satisfied if all the possible faults are diagnosable at most after $\mathcal{K}$ firings after their occurrence. This practical diagnosability permits to verify if the fault can be detected within a specified maximum time delay. If the maximum interleaving between two firings is given, and if it is required to detect the fault within a maximum delay, that implies the fault detection to be performed within a maximum number of firings, which is the design parameter $\mathcal{K}$. Hence the concept of $\mathcal{K}$-diagnosability is useful during the design phase, in order to check if the designed system fulfills the constraints in terms of maximum time needed to detect the faults;