K-diagnosability analysis of bounded and unbounded Petri nets using linear optimization

Amira Chouchane, Mohamed Ghazel, Abderraouf Boussif

https://doi.org/10.1016/j.automatica.2022.110689
Availbale online at: https://www.sciencedirect.com/science/article/pii/S0005109822005532

K-Diagnosability Analysis of Bounded and Unbounded Petri Nets using Linear Optimization ⋆

Amira Chouchane [a], Mohamed Ghazel [a], Abderraouf Boussif [b]

[a] *Univ. Gustave Eiffel, COSYS-ESTAS, F-59650 Villeneuve d'Ascq, France*

[b] *Institut de Recherche Technologique Railenium, F-59300, Famars, France*

Abstract

We propose an algebraic approach to investigate K-diagnosability of partially observed labeled Petri nets which can be either bounded or unbounded. Namely, a necessary and sufficient condition for K-diagnosability is established based on the resolution of an Integer Linear Programming (ILP) problem. When the system is K-diagnosable, our approach also yields the minimal value $K_{min} \leq K$ that ensures K_{min}-diagnosability. The value of K_{min} is calculated directly, using the same ILP formulation, *i.e.*, without testing $1, ..., (K_{min} - 1)$-diagnosability. A second K-diagnosability approach, which is derived from the first one, is also developed on a compacted horizon providing a sufficient condition for K-diagnosability. This second technique allows for reducing the system dimensionality yielding a higher computational efficiency and allowing the characterization of the length of the sequences that lead to the fault occurrence, which is necessary to perform the K-diagnosability test of the first approach.

Key words: K/K_{min}-diagnosability; Petri nets; Discrete-event systems; Integer linear programming.

1 Introduction and related works

Diagnosability analysis is one of the fundamental verification problems in Discrete Event Systems (DES) [9]. The first formulation of the diagnosability feature in DES was introduced in the seminal work of Sampath et al. [23] while considering a Finite State Automaton (FSA) framework. The authors of [23] define diagnosability as the ability to diagnose (detect and identify) any fault (or fault class) occurrence within a finite delay (*i.e.*, a bounded number of events) after its occurrence. The early works that addressed DES diagnosability issues mostly considered FSA models [10,23]. Then, diagnosability analysis was extended to the Petri Net (PN) formalism [1, 2, 5, 7, 8, 14, 19, 28, 29], taking advantage of its mathematical and graphical representations. On the one hand, the idea behind the works that investigate the graphical representation of PN state set consists in extending the FSA based techniques (i.e., diagnoser-based and verifier-based techniques) by considering the behavior of the PN captured by its reachability graph (in the case of bounded systems) or coverability graph (in the case of unbounded systems). Such approaches are referred to as *graph-based* [5, 7, 8, 14, 19]. On the other hand, some further works are based on the mathematical representation of PN in order to reformulate the diagnosability problem as a linear optimization problem, which can be then tackled by means of existing optimization techniques, particularly, Integer Linear Programming (ILP). Such approaches are referred to as *algebraic techniques* [1–3, 28, 29]. To get a general overview of the literature attending to DES diagnosability, the reader can refer to the reviews in [4, 12, 13, 32].

Beside the classic diagnosability, a *quantified* variant of this feature (called K-diagnosability), was discussed and formulated in [1, 7, 10, 14, 16, 17, 19, 21, 26, 31]. Generally, K-diagnosability refers to the ability to diagnose any fault with certainty, provided that at least K events have occurred following the fault occurrence. In fact, K-diagnosability can be of particular interest in practice, since, in some applications, the delay required for detecting and identifying fault occurrences may have considerable impact in terms of safety and/or performance.

In this paper, we are interested in the test of K-diagnosability of DES modeled by a partially observed Labeled Petri Net (LPN). Faults are modeled by means

⋆ This work is part of the ELSAT2020 program co-funded by the European Union with the European Regional Development Fund, the French state and the Hauts-de-France.

Email addresses: amira.chouchane@univ-eiffel.fr (Amira Chouchane), mohamed.ghazel@univ-eiffel.fr (Mohamed Ghazel), abderraouf.boussif@railenium.eu (Abderraouf Boussif).

of unobservable transitions. We also assume that different observable transitions can share the same label. Moreover, the fault transitions are divided into various fault classes. Hence, K-diagnosability can be investigated w.r.t these various classes.

In the context of PNs, K-diagnosability was investigated in [7, 14] in *graph-based* setting and in [1, 2] in an *algebraic* setting. In [7], the authors provided necessary and sufficient conditions for the classic diagnosability and K-diagnosability. They also proposed a technique to compute the bound K based on the analysis of the reachability/coverability graph of a structure, called modified verifier (which is a synchronous composition of the PN model with itself). In this work, the value K refers to the number of observable transitions/events after the fault occurrence. In [14], the authors provided necessary and sufficient conditions for K-diagnosability and K_{min}-diagnosability (the minimum value of K ensuring K-diagnosability) and proposed an on-the-fly and incremental technique for computing the diagnoser automaton and checking the diagnosability properties, in parallel.

In [1], the authors discussed K-diagnosability and proposed necessary and sufficient conditions to check K-diagnosability for labeled bounded PNs, based on ILP problems. The established ILP formulation depends on a parameter, denoted by $\mathcal{J}$, which is necessary for stating the condition for K-diagnosability. A lower bound of $\mathcal{J}$, denoted by $\mathcal{J}_{min}$, was characterized, which permits to fully describe the set of markings reachable from the initial marking, which enable the considered fault transition for the first time. An overestimation of $\mathcal{J}_{min}$ is equal to the number of reachable markings. In [1], the established necessary and sufficient condition for K-diagnosability requires that $\mathcal{J} \geq \mathcal{J}_{min}$, which may lead to a large and computationally complex ILP problem.

In the present paper, we build on the work of Basile et al. [1], and we discuss three main contributions: First, a new algebraic formulation of the K-diagnosability problem for both bounded and unbounded LPN is proposed. Such a formulation provides a necessary and sufficient condition for K-diagnosability, and allows for investigating this feature by means of linear optimization techniques. Moreover, our formulation makes it possible to consider each fault class as a whole, instead of a single fault transition. Furthermore, if the fault class is K-diagnosable, the minimum value $K_{min} \leq K$ ensuring K_{min}-diagnosability is determined all at once. Our ILP formulation involves a parameter J, and we show that it suffices to take a value of J that is at least equal to a value J_K that depends on K. The value of J_K corresponds to the maximum length of some *particular* fault-free sequences that enable the considered fault class. The above results are firstly derived under the assumption that the unobservable subnet is *acyclic*. The case of LPN with unobservable cycles is then discussed and a sufficient condition for K-diagnosability is provided. In this first contribution, the value of parameter J is assumed to be known (as in [1] for parameter $\mathcal{J}$). Secondly, a variant of the above technique is then developed. The technique compacts the fault-free sequences that precede the first occurrence of the fault (from the considered fault class). This second contribution does not involve parameter J, and establishes a sufficient condition for K-diagnosability, based on a new ILP formulation of the problem. The advantages of this technique are twofold. On the one hand, it dispenses with parameter J, which can be difficult to determine, enabling to reduce the number of variables of the ILP problem formulated to test K-diagnosability. If the established sufficient condition for K-diagnosability is fulfilled, a value K_c that is potentially lower than K, and which ensures (K_c)-diagnosability, is given, where $K_{min} \leq K_c \leq K$. On the other hand, the compression of the interval preceding the fault occurrence allows the characterization of parameter J, which is necessary to implement the first approach.

The paper is organized as follows. In section 2, we introduce some relevant preliminary notions and algebraic concepts pertaining to LPN. Useful definitions related to K-diagnosability are also given. In section 3, we expose the principle of our ILP based approach to investigate K-diagnosability. A characterization of the length of some prefix sequences that precede the fault occurrence, which are relevant for K-diagnosability is also discussed. Such a characterization is fundamental to establishing the algebraic model used for K-diagnosability test. In section 4, a necessary and sufficient condition to check K-diagnosability of a fault class is established. K_{min}-diagnosability is also discussed. In section 5, using a compacted horizon, a sufficient condition for K-diagnosability is established. A characterization of parameter J which is necessary to implement the first approach is also accomplished. In section 6, computational complexity analysis and comparative results are presented. A railway benchmark is used to illustrate the effectiveness of the proposed techniques. Section 7 concludes the paper and provides a number of perspectives for the present work.

2 Preliminaries

2.1 Background on LPN

A Petri net (Place/Transition net) is a 4-tuple $\mathcal{N} = (P, T, W^-, W^+)$, where P and T are non-empty finite sets of places and transitions, respectively. $W^- : P \times T \to \mathbb{N}$ and $W^+ : P \times T \to \mathbb{N}$ are the ***pre***- and ***post***-*incidence* matrices, respectively. $W = W^+ - W^-$ is the incidence matrix of $\mathcal{N}$. For a given transition $t \in T$, an *input* (*output*) place of t is a place $p \in P$ such that $W^-(p,t) > 0$ ($W^+(p,t) > 0$). A marking is a vector $M \in \mathbb{N}^{|P|}$ that assigns a non-negative integer (a number of tokens) to

each place. We denote by $M(p)$ the marking of place p. A marked PN $(\mathcal{N}, M_0)$ is a PN $\mathcal{N}$ with a known initial marking M_0. For short, a marked PN will be called PN in what follows.

A transition $t \in T$ is *enabled* by marking M, denoted by $M\ [\ t\ \succ$, *iff* $M(p) \geq W^-(p,t), \forall p \in P$. An enabled transition may fire, yielding marking $M' = M + W(\cdot, t)$. Hence, marking M' is said to be *reachable* from marking M by firing transition t, also denoted by $M\ [\ t \succ M'$. A sequence of transitions $\sigma = t_1 t_2 \dots t_k$ is firable at marking M_0, denoted by $M_0\ [\ \sigma \succ$, if $\exists\ M_1, M_2, \dots, M_{k-1}$ s.t. $M_0\ [\ t_1 \succ M_1\ [\ t_2 \succ \cdots\ M_{k-1}\ [\ t_k \succ$. We denote by $L(\mathcal{N}, M_0)$ the set of sequences resulting in all the reachable markings of $\mathcal{N}$ from M_0.

Suppose that T is ordered as $T = \{t_1, \dots, t_{|T|}\}$, function $\pi_T : T^* \to \mathbb{N}^{|T|}$ assigns to each sequence $\sigma \in T^*$ its *count vector* $\pi_T(\sigma)$, where the i^{th} element of vector $\pi_T(\sigma)$ represents the number of firings of transition t_i in σ. For a given marking M that is reachable from marking M_0 through a transition sequence σ (i.e., $M_0[\sigma > M$), the *state equation* $M = M_0 + W \cdot x$ holds with $x = \pi_T(\sigma)$. However, if the state equation above is satisfied for some positive integer vector $x \in \mathbb{N}^{|T|}$, this does not necessarily imply that there exists a corresponding sequence $\sigma \in T^*$ of count vector x, such that $M_0[\sigma \succ$.

In the context of partially observed PN, the set of transitions is partitioned as $T = T_o \uplus T_u$, where T_o is the set of observable transitions, and T_u is the set of unobservable ones. Given a sequence $\sigma \in T^*$, $P_o(\sigma)$ (resp. $P_u(\sigma)$) corresponds to the projection of σ over T_o^* (resp. T_u^*). We define the restriction of the function π_T on the set of observable transitions (respectively unobservable transitions) as $\pi_{T_o} : T_o^* \to \mathbb{N}^{|T_o|}$ (respectively $\pi_{T_u} : T_u^* \to \mathbb{N}^{|T_u|}$). For the set of observable transitions T_o, we define the observable subnet of PN $\mathcal{N}$ by $\mathcal{N}_o = (P, T_o, W_o^-, W_o^+)$, with $W_o^- = W_{|T_o}^-$, and $W_o^+ = W_{|T_o}^+$. Similarly, the unobservable subnet is defined by $\mathcal{N}_u = (P, T_u, W_u^-, W_u^+)$, with $W_u^- = W_{|T_u}^-$, and $W_u^+ = W_{|T_u}^+$. Additionally, we write $T_f \in \sigma$ to denote that $\exists t \in T_f$ such that $t \in \sigma$.

An LPN is a structure $\mathcal{N}_\mathcal{L} = ((\mathcal{N}, M_0), E, \mathcal{L})$, where $(\mathcal{N}, M_0)$ is a marked PN, E is a finite set of events (i.e., labels) and $\mathcal{L} : T \to E \cup \{\varepsilon\}$ is the *labeling function*, which assigns to each transition $t \in T$ either a label from E if $t \in T_o$, or ε if $t \in T_u$. It is worth noting that two observable transitions may share the same label. The labeling function $\mathcal{L}$ can also be extended to transition sequences, $\mathcal{L} : T^* \to \{E \bigcup \{\varepsilon\}\}^*$. It is also possible to define the projection of $\sigma \in T^*$ in the set of observable labels E^* as $P_l(\sigma) = \mathcal{L}(P_o(\sigma))$. For $w \in E^*$, the inverse projection operator is defined as $P_l^{-1}(w) = \{\sigma \in T^* \mid P_l(\sigma) = w\}$. The vector $\pi_E(w)$ is called the count vector of word w, where $\pi_E : E^* \to \mathbb{N}^{|E|}$ is the function that assigns to any word $w \in E^*$, the vector $y = \pi_E(w) \in \mathbb{N}^{|E|}$ of elements representing the number of occurrences of each label of set E in w.

Definition 1. *(Explanations and explanation vectors [8]). Given a marking M and an observable transition $t \in T_o$, we define $\Sigma(M,t) = \{\sigma_u \in T_u^* \mid M[\sigma_u t \succ\}$ as the set of explanations of t at M, and $E(M,t) = \pi(\Sigma(M,t))$ as the set of explanation vectors, i.e., firing vectors associated with the explanations in $\Sigma(M,t)$.*

In the context of fault diagnosis, the set of unobservable transitions is partitioned into two disjoint subsets $T_u = T_f \uplus T_{reg}$, where T_f corresponds to the set of fault transitions while T_{reg} corresponds to the regular (*i.e.*, non-faulty) unobservable transitions. Furthermore, the set of fault transitions T_f can also be partitioned into r disjoint subsets ($T_f = \uplus_{i=1}^{r} F_i$) that represent the different fault classes. Without loss of generality and for the sake of clarity, one single fault class, denoted as T_f, will be considered. A sequence $\sigma \in T^*$ is said to be faulty if σ contains at least one fault transition of T_f (*i.e.*, $\exists t_f \in T_f$ such that $t_f \in \sigma$). In the remainder of the paper, we say that *fault class T_f occurred* to mean that there exists a fault transition $t_f \in T_f$ which has fired.

We denote by $\psi(T_f)$ the set of sequences that enable fault class T_f *for the first time*. Formally:

$$\psi(T_f) = \{\sigma \in T^* \mid (\ T_f \notin \sigma) \wedge (\exists\, t_f \in T_f : M_0[\sigma t_f \succ)\}.$$

2.2 Algebraic modeling of LPN

In this section, a number of algebraic derivations of LPN concepts are provided. Such formulations allow us to outline our contributions subsequently.

2.2.1 Modeling of firing sequences

Let us consider a feasible firing sequence σ from the initial marking M_0. If we consider an estimation *horizon* $h \in \mathbb{N}^*$ with $h \geq |\sigma|$, then we can derive a sequence $\widetilde{\sigma}$ as $\widetilde{\sigma} = t^{<1>}t^{<2>}...t^{<h>}$ where $t^{<i>} \in T \cup \{\zeta\}$ for all $i \in [\![1, h]\!]$, and ζ stands for the empty step sequence. That is, we interleave the transitions in σ with empty step sequences so as to fill all the indexes of the estimation horizon, *i.e.,* from 1 to h. Therefore, there exists a list of markings $M^{<1>}, M^{<2>}, \dots, M^{<h+1>}$ such that $M^{<1>}[t^{<1>} \succ M^{<2>}[t^{<2>} \succ M^{<3>} \dots M^{<h>}[t^{<h>} \succ M^{<h+1>}$ where $M^{<1>} = M_0$.

In the sequel, we denote $\pi_T(t^{<i>})$ as by $x^{<i>}$, $i \in [\![1...h]\!]$. Based on the fundamental equations of markings and the firing conditions of transitions $t^{<1>}, t^{<2>}, ..., t^{<h>}$ respectively, we get the following relationships specifying

the evolution of count vectors:

$$\begin{aligned} & W^- \cdot x^{<1>} \leq M_0 \\ & -W. \sum_{i=1}^{j-1} x^{<i>} + W^- \cdot x^{<j>} \leq M_0 \quad ; \forall j \in [\![2, h]\!] \end{aligned} \tag{1}$$

Let us define augmented vector $X \geq \mathbf{0}$ as follows:

$$X = \left((x^{<1>})^\top \ (x^{<2>})^\top \ \dots \ (x^{<h>})^\top \right)^\top \tag{2}$$

In view of equations (1), we get the system:

$$\Gamma.X \leq \Theta \tag{3}$$

where $\Gamma = \begin{pmatrix} W^- & \mathbf{0} & \dots & \dots & \mathbf{0} \\ -W & W^- & & & \vdots \\ \vdots & & & & \mathbf{0} \\ -W & -W & \dots & -W & W^- \end{pmatrix}$ and $\Theta = \begin{pmatrix} M_0 \\ M_0 \\ \vdots \\ M_0 \end{pmatrix}$.

The dimensions of matrix Γ and vector Θ are $h.|P| \times h.|T|$ and $h.|P| \times 1$, respectively.

2.2.2 Modeling of explanation vectors

Let us consider a feasible firing sequence σ from M_0, and let $\sigma_o = P_o(\sigma)$ be the observable projection of σ. Similarly to section 2.2.1, we can derive a sequence $\widetilde{\sigma_o}$ from σ_o as $\widetilde{\sigma_o} = t_o^{<1>} t_o^{<2>} ... t_o^{<h>}$, where $t_o^{<i>} \in T_o \cup \{\zeta\}$ for all $i \in [\![1, h]\!]$ with $h \geq |\sigma_o|$ being the estimation horizon. We denote by $x_o^{<i>} = \pi_{T_o}(t_o^{<i>})$ the count vector corresponding to $t_o^{<i>}$. Let $\sigma_u^{<1>}, \sigma_u^{<2>}, \cdots, \sigma_u^{<h>}$ be a set of unobservable explanations that are coherent with transitions $t_o^{<1>}, t_o^{<2>}, \cdots, t_o^{<h>}$, respectively. That is, $\sigma_u^{<1>} t_o^{<1>} \sigma_u^{<2>} t_o^{<2>} ... \sigma_u^{<h>} t_o^{<h>}$ is a feasible firing sequence from M_0. Then, there exists a suite of markings $M'^{<1>}, \cdots, M'^{<h>}$ such that $M_0 = M'^{<1>}[\sigma_u^{<1>} t_o^{<1>} \succ M'^{<2>} \cdots M'^{<h>}[\sigma_u^{<h>} t_o^{<h>} \succ M'^{<h+1>}$.

We denote by $x_u^{<i>} = \pi_{T_u}(\sigma_u^{<i>})$ and $x_o^{<i>} = \pi_{T_o}(t_o^{<i>})$ where $i \in [\![1...h]\!]$ to represent the rearrangement of the LPN transitions with respects to T_u and T_o, respectively. Based on the fundamental equations of markings and the firing conditions of sequences $\sigma_u^{<1>}, t_o^{<1>}, \sigma_u^{<2>}, t_o^{<2>}, ..., \sigma_u^{<h>}$ and $t_o^{<h>}$, we get the following relationships specifying the evolution of count vectors:

$$\begin{aligned} & -W_u.x_u^{<1>} + W_o^-.x_o^{<1>} \leq M_0 \\ & -W_u \cdot \sum_{i=1}^{j} x_u^{<i>} - W_o. \sum_{i=1}^{j-1} x_o^{<i>} + W_o^-.x_o^{<j>} \leq M_0 \quad ; \forall j \in [\![2, h]\!] \end{aligned} \tag{4}$$

Let us consider the augmented vector X in (2) where $x^{<i>}, i \in [\![1, h]\!]$ is defined as follows:

$$x^{<i>} = [(x_o^{<i>})^\top \ (x_u^{<i>})^\top]^\top \tag{5}$$

In view of equations (4) and by ordering the transitions in T as $T = \{t_{o_1}, \cdots, t_{o_{|T_o|}}, t_{u_1}, \cdots, t_{u_{|T_u|}}\}$ so that we can write W as $W = (W_o | W_u)$, the following system can be formulated:

$$\Gamma'.X \leq \Theta \ \text{ where} \tag{6}$$

$$\Gamma' = \begin{pmatrix} \boxed{W_o^- \ -W_u} & \mathbf{0} & \cdots & \mathbf{0} \\ -W & \boxed{W_o^- \ -W_u} & & \vdots \\ \vdots & & \ddots & \mathbf{0} \\ -W & \cdots & -W & \boxed{W_o^- \ -W_u} \end{pmatrix}.$$

The dimensions of matrix Γ' is $h.|P| \times h.|T|$. Note that vector Θ is as defined in (3).

Note that, when the estimate of count vector ${x_u}^{<i>}$ corresponds to a sequence that can be executed by the LPN (from $M'^{<i>}$), we can say that this count vector is an explanation vector of $t_o^{<i>}$ from $M'^{<i>}$ (cf. Definition 1), *i.e.*, $x_u^{<i>} \in E(M'^{<i>}, t_o^{<i>})$.

2.2.3 Modeling indistinguishable observable transitions

Let us now establish the relationship between ${x_o}^{<i>}$ and $y^{<i>}, i \in [\![1, h]\!]$ where $y^{<i>}$ is the count vector of the observed label associated with the i^{th} iteration. To this end, let us consider that $T_o = \{t_1 \cdots t_{|T_o|}\}$ and $E = \{\ell_1 \cdots \ell_{|E|}\}$. Then, we can define the labeling matrix $\wp \in \{0, 1\}^{|E| \times |T_o|}$ whose general term $\wp_{qr}$ with $q \in [1...|T_o|]$ and $r \in [1...|E|]$ and which is defined by:

$$\begin{cases} \wp_{qr} = 1 \ if \ \mathcal{L}(t_r) = \ell_q \\ \wp_{qr} = 0 \ otherwise \end{cases} \tag{7}$$

Hence, we get the following relation relating ${x_o}^{<i>}$ to $y^{<i>}$:

$$y^{<i>} = \wp \cdot {x_o}^{<i>} \ ; \forall i \in [\![1, h]\!] \tag{8}$$

Finally, we can deduce the following relationship between the count vector of observed labels $Y = ((y^{<1>})^\top ... (y^{<h>})^\top)^\top$ and the count vector X defined in (2) and (5):

$$\boldsymbol{D}.X = Y \tag{9}$$

where $\boldsymbol{D} = \begin{pmatrix} \boxed{\wp\ \mathbf{0}} & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \ddots & & \vdots \\ \vdots & & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & \boxed{\wp\ \mathbf{0}} \end{pmatrix}$.

The boxes in D represent the concatenation of matrix $\wp$ of dimention $|E| \times |T_o|$ with a zero matrix of dimension $|E| \times |T_u|$. $\boldsymbol{D}$ is a block-diagonal-matrix of dimension $h.|E| \times h.|T|$.

2.3 K-diagnosability of LPN

The classic definition of diagnosability (as initially introduced by Sampath et al. [23]) can be formulated in the context of LPN for a fault class T_f as follows:

Definition 2. (diagnosability of a fault class [7]) *An LPN system, having no deadlock after the occurrence of any faulty transition t_f in fault class T_f, is diagnosable with respect to T_f if the following holds:*

$$(\forall \sigma_{bf} \in \psi(T_f))(\exists \kappa \in \mathbb{N}^*)(\forall \sigma_{af} | M_0[\sigma_{bf} t_f \sigma_{af} \succ ; t_f \in T_f) : |\sigma_{af}| \geq \kappa \Rightarrow \text{Diag}$$

where the diagnosability condition Diag *is:* $\sigma \in P_l^{-1}[P_l(\sigma_{bf}\sigma_{af})] \Rightarrow T_f \in \sigma$.

The above definition can be explained as follows: Let σ_{bf} [1] be a non-faulty sequence (with respect to fault class T_f) generated by the LPN, which reaches a marking that enables a fault transition from class T_f. Condition *Diag* requires that there exists a finite delay upon which one can detect the occurrence of a fault from T_f with certainty. Note that the bound κ in definition 2 may depend on the particular sequence σ_{bf}.

Let us now define the notion of diagnosability in K steps, also called K-diagnosability.

Definition 3. (K-diagnosability of a fault class) *An LPN system, having no deaddlock after the occurrence of any faulty transition t_f in fault class T_f, is diagnosable with respect to T_f if the following holds:*

$$(\forall \sigma_{bf} \in \psi(T_f))(\forall \sigma_{af} | M_0[\sigma_{bf} t_f \sigma_{af} \succ ; t_f \in T_f) : |\sigma_{af}| \geq K \Rightarrow \text{Diag}$$

The above definition means that the firing of any fault transition $t_f \in T_f$ can be detected with certainty provided that at least K transitions have been fired since the firing of t_f.

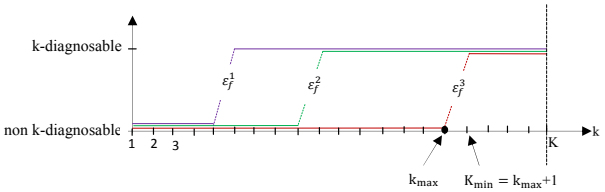

Fig. 1. Principle of K-diagnosability of fault class $T_f = \{t_f^1, t_f^2, t_f^3\}$

The following definition of K-diagnosability which is equivalent to Definition 3 can also be introduced. This reformulation will be used in the sequel to develop our technique for K-diagnosability analysis.

Proposition 1. *An LPN is K-diagnosable with respect to a fault class T_f iff there do not exist two firing sequences $\sigma, \sigma' \in T^*$ such that:*

- $\sigma = \sigma_{bf} t_f \sigma_{af}$, *with* $t_f \in T_f$
- $\sigma_{bf} \in \psi(T_f)$
- $|\sigma_{af}| \geq K$
- $T_f \notin \sigma'$
- $P_l(\sigma) = P_l(\sigma')$

Proof. the above result is a reformulation of the K-diagnosability feature as stated in Definition 3. □

According to Proposition 1, a fault class T_f is said to be K-diagnosable *iff* for any feasible faulty sequence σ having at least K transitions following the first fault class occurrence, there does not exist any fault-free sequence σ' that generates the same observation as σ. Therefore, checking K-diagnosability of a fault class T_f amounts to checking that no such couple (σ, σ') of transition sequences exists for the LPN.

3 Approach principle

Given an LPN and a fault class T_f, the K-diagnosability problem can be reformulated as follows:
"Is there $K_{min} \leq K$ such that T_f is K_{min}-diagnosable and T_f is not $(K_{min} - 1)$-diagnosable? If so, T_f is K-diagnosable."
Therefore, checking K-diagnosability of T_f consists in determining whether or not there exists a specific *minimum* value $K_{min} \leq K$ that ensures the K_{min}-diagnosability of T_f (see Figure 1).

3.1 Reformulation of the K and K_{min}-diagnosability problems

It is straightforward that for non K-diagnosable models, there is no $K_{min} \leq K$ ensuring K_{min}-diagnosability. How-

[1] In the sequel, σ_{bf} (resp. σ_{af}) stands for the prefix (resp. suffix) preceding (resp. following) the first transition of the considered fault class.

ever, in the case of K-diagnosable fault class, there exists some $K_{min} \in [\![1;K]\!]$, that ensures K_{min}-diagnosability. Two cases should be distinguished:
– If $K_{min} = 1$ then there does not exist any value $\kappa \in [\![1;K]\!]$ such that T_f is not κ-diagnosable.
– If $K_{min} \in [\![2;K]\!]$ then $\forall \kappa \in [\![1;K_{min}-1]\!]$, T_f is not κ-diagnosable, and $\forall \kappa \in [\![K_{min};K]\!]$, T_f is κ-diagnosable.

We suppose that T_f is K_{min}-diagnosable where $1 \leq K_{min} \leq K$. To determine the value of K_{min}, we identify the maximum value of $\kappa \leq K$, denoted as κ_{max} such that the following set is not empty:

$$C(\kappa) = \{\ (\sigma,\sigma') \in L^2(\mathcal{N},M_0) \mid \sigma = \sigma_{bf}\, t_f\, \sigma_{af}\,, \\ \sigma_{bf} \in \psi(T_f), t_f \in T_f, |\sigma_{af}| = \kappa; T_f \notin \sigma'; \\ P_l(\sigma) = P_l(\sigma')\ \}$$

In fact, $C(\kappa)$ represents the set of couples of indistinguishable sequences (σ,σ') where σ is a feasible faulty sequence with exactly κ transitions (with $\kappa \leq K$) following the first fault class occurrence, while σ' is a fault-free sequence. Therefore, K_{min} can be deduced (from the value of κ_{max}) as follows:

- If $\nexists \kappa \in [\![1;K]\!]$ such that $\exists(\sigma,\sigma') \in C(\kappa)$ (i.e. κ_{max} does not exist), then $K_{min} = 1$.
- If $\exists \kappa_{max} \in [\![1;K[\![$ such that $\forall \kappa \in [\![1;\kappa_{max}]\!]$, $C(\kappa) \neq \emptyset$ and $\forall \kappa \in]\!]\kappa_{max};K]\!]$, $C(\kappa) = \emptyset$ then $K_{min} = \kappa_{max} + 1$.
- If $\forall \kappa \in [\![1;K]\!]$, $C(\kappa) \neq \emptyset$, then $\kappa_{max} = K$ which implies T_f is not K-diagnosable.

In the following section, we will show that we can verify the existence of such $K_{min} \in [\![1,K]\!]$ and, if so, determine its value, by solving one single linear optimization problem. However, before that, we need to characterize the set of sequences $\psi(T_f)$ that enable fault class T_f for the first time.

In the remainder of the paper, we consider the following assumption:
H0. The considered LPN does not reach a deadlock after firing any fault transition.

3.2 Preliminary results

In order to reduce the computational complexity and the memory requirements needed to solve the K-diagnosability problem, we have every interest to restrict, as much as possible, the scope of the firing sequences to be considered. Unlike in [1], to perform the K-diagnosability test we do not consider all the sequences in $\psi(T_f)$ (sequences that lead to the first occurrence of some fault in T_f). Indeed, we need to investigate only a subset of faulty sequences that have some fault-free indistinguishable sequence.

Firstly, for a given value $\kappa \in [\![1;K]\!]$, we define the following subset $\psi_D(T_f,\kappa) \subseteq \psi(T_f)$ which holds the sequences σ_{bf} that lead to a first firing of some transition in T_f, and which fulfill the following: *(i)* σ_{bf} is the prefix of some feasible faulty sequence $\sigma = \sigma_{bf}\epsilon_f\sigma_{af}$, and *(ii)* σ is associated with some indistinguishable fault-free sequence σ' such that $(\sigma,\sigma') \in C(\kappa)$. Thus, $\psi_D(T_f,\kappa)$ can be formally defined as follows:

$$\psi_D(T_f,\kappa) = \{\sigma_{bf} \in \psi(T_f) \mid \exists(\sigma,\ \sigma') \in C(\kappa) \\ with\ \sigma = \sigma_{bf}\, t_f\, \sigma_{af},\ t_f \in T_f\}$$

Finding one pair $(\sigma,\sigma') \in C(\kappa)$ is sufficient to infer that the net is not κ-diagnosable. Hence, we can seek for a particular couple $(\sigma,\sigma') \in C(\kappa)$ such that σ corresponds to a shortest faulty sequence. In fact, for some fixed $\kappa \in [\![1;K]\!]$, a shortest fault sequence $\sigma = \sigma_{bf}\, t_f\, \sigma_{af}$ is also associated with a shortest sequence σ_{bf}. Therefore, for a given $\kappa \in [\![1;K]\!]$ we can further reduce the scope of our investigation by considering only the set of shortest sequences in $\psi_D(T_f,\kappa)$, which is defined as follows:

$$\psi_D^{min}(T_f,\kappa) = \{\sigma_{bf} \in \psi_D(T_f,\kappa) \mid \nexists \sigma'_{bf} \in \psi_D(T_f,\kappa) \\ \text{s.t } |\sigma_{bf}| > |\sigma'_{bf}|\}$$

Hence, to check K-diagnosability based on the verification of the existence of K_{min} between 1 and K, it is necessary to verify the existence of such couple $(\sigma,\sigma') \in C(\kappa)$ for each $\kappa \in [\![1;K]\!]$. Consequently, it suffices to characterize the following subset of $\psi(T_f)$, denoted as $\psi_D^K(T_f)$:

$$\psi_D^K(T_f) = \bigcup_{1\leq\kappa\leq K} \psi_D^{min}(T_f,\kappa) = \bigcup_{1\leq\kappa\leq K_{min}-1} \psi_D^{min}(T_f,\kappa)$$

The problem formulation we propose for analyzing K-diagnosability allows us to characterize the set $\psi_D^K(T_f)$ without resorting to explicit enumeration of the feasible sequences of this set. In fact, it suffices to determine the maximum length of the sequences in set $\psi_D^K(T_f)$, as will be shown in Section 4. Consequently, the following result can be stated:

Proposition 2. *For an LPN without any deadlock following the firing of any transition of fault class T_f, checking K-diagnosability of T_f can be determined only for a subset of $\psi(T_f)$ that includes sequences of maximum length denoted J_K defined as follows:*

$$J_K = \max_{1\leq\kappa\leq K} \min_{\sigma_{bf}\in\psi_D(T_f,\kappa)} |\sigma_{bf}| \qquad (10)$$

Proof.
T_f is K-diagnosable *iff* there exists a minimum value $K_{min} \in [\![1,K]\!]$ that ensures K_{min}-diagnosability of T_f. Therefore, $\forall \kappa \in [\![1;K_{min}-1]\!]$, T_f is not κ-diagnosable

and $\forall \kappa \in [\![K_{min}; K]\!]$, T_f is κ-diagnosable. For a fixed $\kappa \in [\![1; K]\!]$, (T_f is not κ-diagnosable) *iff* $(\exists(\sigma_1, \sigma_1') \in C(\kappa)$ such that $\sigma_1 = \sigma_{bf}^1 t_f \sigma_{af}^1$ and $\sigma_{bf}^1 \in \psi_D^{min}(T_f, \kappa))$. The length of σ_{bf}^1 is $J_\kappa = \min_{\sigma_{bf} \in \psi_D(T_f,\kappa)} |\sigma_{bf}|$. Since $K_{min} \leq K$ is not known a priori, we have to consider all $\sigma_{bf} \in \psi_D^{min}(T_f, \kappa)$ for all $\kappa \in [\![1; K]\!]$ to find a couple $(\sigma_1, \sigma_1') \in C(\kappa)$ if there exists. Therefore, a sufficient maximal length of σ_{bf} for K-diagnosability analysis is $J_K = \max_{1 \leq \kappa \leq K} J_\kappa$. □

In other terms, J_K represents the maximum length among the set of sequences in $\psi_D^K(T_f)$. Or, phrased differently, J_K stands for the maximal length of the shortest sequences leading to the firing of some faulty transition in T_f, that admit a continuation of length 1 to K, such that there exists a corresponding indistinguishable fault-free sequence.

Remark 1. *It is straightforward that the theoretic value of J_K is finite even for unbounded nets. Indeed, J_K is the solution of a max−min optimization problem, and corresponds to the maximum value among a finite number of integers. In fact, although Proposition 1 does not provide an operative way to determine a value for J_K, this result is crucial in our approach for K-diagnosability analysis, that will be discussed in section 4. Indeed, the finiteness of J_K allows the applicability of our technique to both bounded and unbounded LPN.*

In general, the computation of J_K (or an overestimate $J \geq J_K$) is not trivial. Of course, this value depends on the net structure and can be very large. It is worth noting that an overestimation of J can lead to a too much complex ILP problem to be solved, being given that the resolution of an ILP problem is exponential in the worst case w.r.t. the number of variables. On the other hand, an under-estimation of J can yield an erroneous verdict regarding K-diagnosability. In the remainder of the paper, K-diagnosability analysis will be performed while considering the two cases of known and unknown value of $J \geq J_K$.

4 Analysis of K/K_{min}-diagnosability

The main result discussed in this section is a necessary and sufficient condition for K-diagnosability of a fault class T_f under the hypothesis of acyclicity of unobservable subnet (denoted later by assumption ***H1***). An appropriate value of $J \geq J_K$ is supposed to be known. In case T_f is K-diagnosable, the value of K_{min} is also given. The developed technique is based on the resolution of an ILP problem that will be formulated in what follows.

Assume that fault class T_f is K_{min}-diagnosable with $K_{min} > 1$, then there exists at least one firable sequence $\sigma = t^{<1>} \dots t^{<J>} t^{<J+1>} \dots t^{<J+K_{min}>}$ from M_0 such that:

- $t^{<i>} \in (T \setminus T_f) \cup \{\zeta\}$ for $1 \leq i \leq J$;
- $t^{<J+1>} = t_f \in T_f$;
- $t^{<J+2>}, \dots, t^{<J+K_{min}>} \in T$; and
- there exists at least one sequence $\sigma' \in (T \setminus T_f)^*$ enabled from M_0, such that $P_l(\sigma) = P_l(\sigma')$.

4.1 Modeling the faulty sequence

Since $K_{min} \leq K$ is not known a priori, for the computation of the count vector associated with faulty sequence $\sigma = t^{<1>} t^{<2>} \dots t^{<J>} \dots t^{<J+K_{min}>}$, we expand the firing sequence σ over horizon $J + K + 1$ by taking $t^{<J+K_{min}+1>}, \dots, t^{<J+K+1>}$ as empty step sequences. Therefore, we can write $\sigma = t^{<1>} t^{<2>} \cdots t^{<J+K+1>}$, where $t^{<i>}, i \in [\![1, J + K + 1]\!]$ can correspond to an observable transition, an unobservable transition or even the empty step sequence ζ.

We denote by $x_o^{<i>} = \pi_{T_o}(t^{<i>})$ and $x_u^{<i>} = \pi_{T_u}(t^{<i>})$ to represent the rearrangement of the LPN transitions with respect to T_o and T_u respectively, yielding $x^{<i>} = [(x_o^{<i>})^\top \quad (x_u^{<i>})^\top]^\top$. The firing count vector of faulty sequence σ is defined as follows:

$$X = \left((x^{<1>})^\top \; (x^{<2>})^\top \; \dots \; (x^{<J+K+1>})^\top \right)^\top \tag{11}$$

Vector X satisfies (3) with $h = J + K + 1$.

At every iteration $< j >$ from $< 1 >$ to $< J + K + 1 >$, at most one transition is fired. Therefore, $0 \leq c.x^{<j>} \leq 1 \;\; ; \forall j \in [\![1, J + K + 1]\!]$ where c is a row vector of $1'$s of dimension $|T|$. This can be expressed as follows:

$$\mathbf{0} \;\; \leq v_1.X \leq \overrightarrow{1} \tag{12}$$

where $v_1 = \begin{pmatrix} c & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & \ddots & & \vdots \\ \vdots & & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & \mathbf{0} & c \end{pmatrix}$

From iteration $< 1 >$ to iteration $< J >$, no fault transition of fault class T_f occurs. Therefore, the firing number of fault transitions from iteration $< 1 >$ to iteration $< J >$ is equal to zero. The first occurrence of a fault transition from T_f appears at the $(J + 1)^{th}$ iteration. Therefore, $\sum_{j=1}^{<J>} c_f.x^{<j>} = 0$ and $c_f.x^{<J+1>} = 1$ where c_f is a row vector of dimension $|T|$, of which all the elements are null, except the elements that are associated with fault

transitions in T_f, which are equal to 1. Hence, we get:

$$\begin{cases} f_1.X = 0 \\ f_2.X = 1 \end{cases} \quad (13)$$

where $f_1 = \left(c_f \;\; c_f \;\; \cdots \;\; c_f \;\middle|\; \mathbf{0}_{1\times|T|.(K+1)} \right)$, and $f_2 = \left(\mathbf{0}_{1\times|T|.J} \middle| c_f \middle| \mathbf{0}_{1\times|T|.K} \right)$.

Regarding iterations $< J+2 >$ to $< J+K+1 >$, iteration $< J+K_{min}+1 >$ is the point from which the sum of the count vector elements irrevocably switches from 1 to 0, *i.e.*, remains equal to 0 till the final iteration $< J+K+1 >$, which implies $c.x^{<j>} - c.x^{<j+1>} \geq 0 \;\; ; \forall j \in [\![J+2; J+K]\!]$. The underlying idea of the previous relationship is to ensure that exactly one transition is actually fired at each iteration from the $< J+2 >^{th}$ to $< J+K_{min} >^{th}$ iteration, (*i.e.*, no void iteration), and that σ does not hold further transitions. Hence, we can count the maximum number of firable transitions following the fault occurrence while assuming that there is at least one corresponding fault-free sequence that generates the same observation. The previous relation can be written using the following matrix/vector form:

$$v_2.X \leq \mathbf{0} \quad (14)$$

with $v_2 = \left(\mathbf{0}_{(K-1)\times|T|.(J+1)} \middle| \begin{matrix} -c & c & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & -c & c \end{matrix} \right)$

The faulty sequence σ holds at least one transition and at most K transitions following the first occurrence of the fault class. Therefore, $1 \leq \sum_{i=J+2}^{J+K+1} c.x^{<i>} \leq K$ which can be expressed as a dot product, as follows:

$$1 \leq \lambda^\top.X \leq K \quad (15)$$

with $\lambda = \left(\mathbf{0}_{1\times|T|.(J+1)} \;\middle|\; c \;\; c \;\; \cdots \;\; c \right)^\top$.

According to relations (3) for $h = J+K+1$, (12), (13) and (14), the count vector $X \in \mathbb{N}^{(J+K+1).|T|}$ of faulty sequence σ fulfills the following polyhedron:

$$A_f^{J,K}.X \leq b_f^{J,K} \quad (16)$$

where $A_f^{J,K} = \begin{pmatrix} \Gamma \\ f1 \\ -f1 \\ f2 \\ -f2 \\ v_1 \\ -v_1 \\ v_2 \\ \lambda^\top \\ -\lambda^\top \end{pmatrix}$ and $b_f^{J,K} = \begin{pmatrix} \Theta \\ 0 \\ 0 \\ 1 \\ -1 \\ \overrightarrow{1} \\ \mathbf{0} \\ \mathbf{0} \\ K \\ -1 \end{pmatrix}$

Theorem 3. *[22] Consider a marked PN $(\mathcal{N}, M_0)$ with reachability space $\mathcal{R}(\mathcal{N}, M_0)$ and let $\mathcal{R}^h(\mathcal{N}, M_0)$ denote the set of markings $M \in \mathcal{R}(\mathcal{N}, M_0)$ that are reachable from M_0 through some firable transition sequence σ with $|\sigma| \leq h$, $h \in \mathbb{N}$. Also, let $L^h(\mathcal{N}, M_0)$ denote the set of solution vectors $M \in \mathbb{N}^{|P|}$ of the following system of linear inequalities, in variables M and e_i, $i \in \{1, \ldots, h\}$:*

$$\begin{cases} M = M_0 + W.\sum_{i=1}^{<h>} e_i \\ M_0 + W.\sum_{j=1}^{<i-1>} e_j \geq W^-.e_i \;\; \forall i \in \{1, \ldots, h\} \\ \left(1 \;\; \cdots \;\; 1 \right).e_i \leq 1 \;\; \forall i \in \{1, \ldots, h\} \\ e_i \in \{0,1\}^{|T|} \;\; \forall i \in \{1, \ldots, h\} \end{cases} \quad (17)$$

Then, $\mathcal{R}^h(\mathcal{N}, M_0) = L^h(\mathcal{N}, M_0)$.

Based on Theorem 3, let us introduce the following lemma.

Lemma 4. *Under **H0**, system (16) is satisfied iff there exists a feasible faulty sequence σ with at most K transition firings after the first occurrence of fault class T_f.*

Proof. System (16) is the state equation that describes a faulty sequence σ (with $|\sigma| \leq J+K+1$) by considering at most one transition firing at each iteration (vector X satisfies (3) with $h = J+K+1$). Therefore, according to Theorem 3, (16) is satisfied *iff* there exists a corresponding feasible faulty sequence σ with at most K transition firings after the first occurrence of T_f.

4.2 Modeling the fault-free sequence

Now that faulty sequence σ has been formally characterized, let us assume that there exists a corresponding non-faulty (w.r.t. T_f) indistinguishable sequence σ', *i.e.*, σ' generates the same observation as faulty sequence σ ($P_l(\sigma) = P_l(\sigma') = w$). Since σ contains at most $J+K+1$ transitions ($|\sigma| \leq J+K+1$), then $w = P_l(\sigma') = P_l(\sigma)$ satisfies $|w| \leq J+K+1$. Hence, we can

write w as $w = l^{<1>}l^{<2>}...l^{<J+K+1>}$, where $l^{<i>}$ is the label produced at iteration $< i >$. Here, $l^{<i>}$ can be either a label from E or the the empty step label expressing the non-occurrence of an observable event at the $< i >^{th}$ iteration. Let $\sigma_o^{'} = P_o(\sigma')$ be the observable projection of σ'. We can then write $\sigma_o^{'}$ as $\sigma_o^{'} = t_o^{'<1>}t_o^{'<2>}...t_o^{'<J+K+1>}$ where $t_o^{'<i>} \in \mathcal{L}^{-1}(l^{<i>})$. We denote by $x_o^{'<i>} = \pi_{T_o}(t_o^{'<i>})$ to represent the count vector corresponding to $t_o^{'<i>}$. Let $\sigma_u^{'<1>}, \sigma_u^{'<2>}, ..., \sigma_u^{'<J+K+1>}$ be the unobservable sequences (explanations) that are coherent with transitions $t_o^{'<1>}, t_o^{'<2>}, ..., t_o^{'<J+K+1>}$, respectively. An ordering of the set of transitions T with regards to T_o and T_u yields $x^{'<i>} = ((x_o^{'<i>})^\top \ (x_u^{'<i>})^\top)^\top$. The firing count vector of the fault-free sequence $\sigma^{'} = \sigma_u^{'<1>}t_o^{'<1>}\sigma_u^{'<2>}t_o^{'<2>}...\sigma_u^{'<J+K+1>}t_o^{'<J+K+1>}$ can then be expressed as follows:

$$X' = \left((x'^{<1>})^\top \ (x'^{<2>})^\top \ \dots \ (x'^{<J+K+1>})^\top \right)^\top \quad (18)$$

Vector X' satisfies relation (6) as well, with $h = J+K+1$, for $\sigma^{'}$ to be feasible.

Sequence $\sigma^{'}$ must not include any fault transition. This can be expressed by the relation $\sum_{i=1}^{J+K+1} c_f.x'^{<i>} = 0$, which can be written in vector dot product form as:

$$f_3.X' = 0 \quad (19)$$

where $f_3 = \left(c_f \ c_f \ \cdots \ c_f \right)$.

According to (6) for $h = J + K + 1$ and (19), the count vector of the fault-free sequence $\sigma^{'}$ fulfills the following polyhedron:

$$A_n^{J,K}.X' \leq b_n^{J,K} \quad (20)$$

where $A_n^{J,K} = \begin{pmatrix} \Gamma' \\ f_3 \\ -f_3 \end{pmatrix}$ and $b_n^{J,K} = \begin{pmatrix} \Theta \\ 0 \\ 0 \end{pmatrix}$

The two sequences σ and σ' have the same observable projection, this can be formulated as:

$$\boldsymbol{D}.X = \boldsymbol{D}.X' \quad (21)$$

where D is as defined in relation (9) and $h = J + K + 1$.

Assuming that vector X in (21) satisfies (16), the integer solutions of system (20) satisfying (21) form a set of vectors that includes the count vectors of sequences σ' which fulfill condition $C_{\sigma,\sigma'}(\kappa)$ with $\kappa \in [\![1; K]\!]$.

Theorem 5. *[15] In an acyclic PN, marking M is reachable from M_0 iff there exists a non negative integer solution x satisfying $M = M_0 + W.x$.*

The theorem ensures that, in an acyclic PN, every positive solution of state equation $M = M_0 + W.x$ corresponds to a count vector of an actual feasible firing sequence. However, in the presence of cycles in the net, the above result does not apply. That is, the solution x does not necessarily correspond to feasible firing sequences. Based on Theorem 5, the following result can be inferred.

Lemma 6. *Under hypotheses **H0** and **H1**, equation (20) is satisfied if and only if there exists a feasible fault-free sequence σ'.*

Proof. We recall here that we suppose that the LPN does not include any cyclic unobservable subnet. Therefore, by propagating the result of Theorem 5 at every iteration successively from $< 1 >$ to $< J + K + 1 >$, every sequence of vectors $x_u^{'<1>}, \dots, x_u^{'<J+K+1>}$ associated with a solution X' of (20) coincides with a sequence of valid explanation vectors of respectively $t_o^{'<1>}, \dots, t_o^{'<J+K+1>}$ having, respectively, as count vectors $x_o^{'<1>}, \dots, x_o^{'<J+K+1>}$ in (20). □

4.3 Main results

As already mentioned, our technique for K-diagnosability analysis under assumptions ***H0*** and ***H1*** is based on the verification of the existence of the minimum value K_{min} of κ in $[\![1; K]\!]$ ensuring κ-diagnosability. Therefore, based on linear optimization techniques, we aim to determine the maximum value κ_{max} of κ such that there exits a couple of feasible firing sequences (σ, σ') belonging to $C(\kappa)$ where $1 \leq \kappa \leq K$. Firstly, let us introduce the following proposition.

Proposition 7. *The existence of a couple $(\sigma, \sigma') \in C(\kappa)$ under assumptions **H0** and **H1** is equivalent to the existence of a couple of vectors $(X, X') \in \mathbb{N}^{(J+K+1).|T|} \times \mathbb{N}^{(J+K+1).|T|}$ satisfying the following polyhedron:*

$$A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K} \quad (22)$$

where $A^{J,K} = \begin{pmatrix} A_f^{J,K} & \mathbf{0} \\ \mathbf{0} & A_n^{J,K} \\ \boldsymbol{D} & -\boldsymbol{D} \\ -\boldsymbol{D} & \boldsymbol{D} \end{pmatrix}$ and $b^{J,K} = \begin{pmatrix} b_f^{J,K} \\ b_n^{J,K} \\ \boldsymbol{0} \\ \boldsymbol{0} \end{pmatrix}$

The dimensions of matrix $A^{J,K}$ and vector $b^{J,K}$ are $(2|T|(J+K+1)) \times ((J+K+1).(2|P|+2|T|+|E|+2)+K+7)$ and $(2|T|(J + K + 1)) \times 1$, respectively.

Proof. This is a direct result of Lemma 4 (by referring to system (16)), and Lemma 6 (by referring to systems (20)), while considering relation (21). □

Therefore, κ_{max} is the cost function of the following optimization problem when system (22) is feasible:

$$\begin{cases} \max\limits_{\mathbb{N}}(\lambda^\top.X) \\ \text{such that (22)} \\ X, X' \in \mathbb{N}^{(J+K+1).|T|} \end{cases} \tag{23}$$

Remark. In the sequel, we simply write max() and min() to denote $\max\limits_{\mathbb{N}}()$ and $\min\limits_{\mathbb{N}}()$, respectively.

We can now establish the following result, which gives a necessary and sufficient condition for K-diagnosability based on the ILP problem (23):

Theorem 8. *Consider an LPN under hypotheses **H0** and **H1**, and fault class T_f. Given $K \in \mathbb{N}^*$, T_f is K-diagnosable **iff** either of the two following conditions is satisfied:*
-i- (23) has no solution, or
-ii- (23) has a solution and $\max(\lambda^\top.X) < K$

Proof. -i- ((23) has no solution) *iff* ((22) admits no solution) *iff* (according to proposition 7, $\nexists(\sigma,\sigma') \in C(\kappa) \forall \kappa \in [\![1;K]\!]$) *iff* ($T_f$ is 1-diagnosable).
-ii-((23) has a solution and $\max(\lambda^\top.X) < K$) *iff* (for $\kappa = \lambda^\top.X = \max(\lambda^\top.X) < K$, (22) admits a solution and for $\kappa = \lambda^\top.X = \max(\lambda^\top.X)+1 \leq K$, (22) has no solution) *iff* (according to proposition 7, for $\kappa = \max(\lambda^\top.X) < K$, $\exists(\sigma,\sigma') \in C(\kappa)$ and for $\kappa = \max(\lambda^\top.X) + 1 \leq K$, $\nexists(\sigma,\sigma') \in C(\kappa)$ *iff* (T_f is K_{min}-diagnosable with $K_{min} = \max(\lambda^\top.X) + 1$) *iff* ($T_f$ is K-diagnosable.) □

Based on the proof of Theorem 8, we can derive the following corollary giving the value of $K_{min} \leq K$ if the K-diagnosability is fulfilled.

Corollary 1. *Consider an LPN under hypotheses **H0** and **H1**. If fault class T_f is K-diagnosable then T_f is K_{min}-diagnosable where K_{min} is defined as follows:*
– $K_{min} = 1$ if (23) is not feasible.
– $K_{min} = \max(\lambda^\top.X) + 1$ if (23) is feasible and $\max(\lambda^\top.X) < K$.

Let us now relax assumption ***H1*** of acyclicity. We shall show that a sufficient condition for K-diagnosability can be established, as stated in the following theorem.

Theorem 9. *Consider an LPN under hypothesis **H0**. For a given $K \in \mathbb{N}^*$, T_f is K-diagnosable **if** at least one of the two following conditions is satisfied:*
-i- (23) has no solution, or
-ii- (23) admits a solution and $\max(\lambda^\top.X) < K$.

Proof.

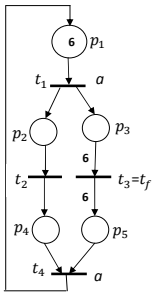

Fig. 2. A bounded LPN

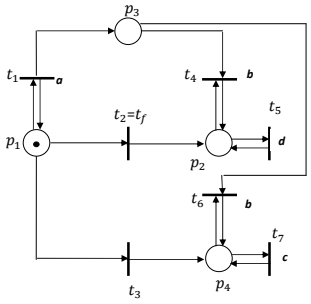

Fig. 3. An unbounded LPN

i– If (23) has no solution, then there does not exist any couple of vectors (X, X') satisfying (22). Thus, there does not exist any couple $(\sigma,\sigma') \in C(\kappa)$ for all $\kappa \in [\![1;K]\!]$, and consequently T_f is 1-diagnosable.
ii– If (23) admits a solution and $\max(\lambda^\top.X) < K$, then for $\kappa = \max(\lambda^\top.X) + 1 \leq K$, there does not exist any couple of vectors (X, X') satisfying (22). Hence, for $\kappa = \max(\lambda^\top.X) + 1 \leq K$, there does not exist any couple $(\sigma,\sigma') \in C(\kappa)$. Therefore, T_f is K_{cyc}-diagnosable with $K_{cyc} = \max(\lambda^\top.X) + 1 \leq K$ and consequently, T_f is K-diagnosable. □

According to the proof of Theorem 9, when the sufficient condition of K-diagnosability is fulfilled, although the minimum value K_{min} ensuring K_{min}-diagnosability cannot be determined, we can provide a value K_{cyc} potentially lower than K, such that T_f is K_{cyc}-diagnosable and $K_{min} \leq K_{cyc} \leq K$. In fact, the case $K_{min} \neq K_{cyc}$ is possible since some solutions X' of (22) can be spurious solutions, *i.e.,* do not correspond to any (fault-free) sequence. This is due to the relaxation of (***H1***) which implies that the result of Theorem 5 does not apply anymore.

Corollary 2. *Consider an LPN under hypothis **H0**. If fault class T_f is K-diagnosable then T_f is K_{cyc}-diagnosable where K_{cyc} is defined as follows:*
– $K_{cyc} = K_{min} = 1$ if (23) is not feasible.
– $K_{cyc} = \max(\lambda^\top.X) + 1 \in [\![K_{min}\ ,\ K]\!]$ if (23) is feasible and $\max(\lambda^\top.X) < K$ *in (23).*

Example 1. *Let us consider the LPN of Fig. 2, where $T_u = \{t_2, t_3\}$, $T_f = \{t_3\}$, $T_o = \{t_1, t_4\}$, $\mathcal{L}(t_1) = \mathcal{L}(t_4) = a$ and $M_0 = [6\ 0\ 0\ 0\ 0]^\top$. We assume J to be given, $J = 6$ and we aim to investigate the K-diagnosability of the net with $K = 5$. Thus, the horizon is $h = J + K + 1 = 12$. The results of the K-diagnosability analysis are presented in Table 1.*

The unobservable subnet of the LPN is acyclic and we get $\kappa_{max} = \max(\lambda^\top.X) = 5$. Thus, T_f is not 5-diagnosable. Indeed, the results of Table 1 can be interpreted as follows: the maximum value of κ such that T_f is not κ-diagnosable is $\kappa_{max} = 5$. Namely, this is due to the existence of two feasible firing sequences $\sigma_1 = t_1t_1t_1t_1t_1t_1t_3t_2t_2t_2t_2t_2$ (faulty) and $\sigma'_1 = t_1t_1t_1t_1t_1t_1$ (normal) such that $(\sigma_1, \sigma'_1) \in C(5)$.

j	1	2	3	4	5	6	7	8	9	10	11	12
$x_u^{<j>}$	0 0	0 0	0 0	0 0	0 0	0 0	0 1	1 0	1 0	1 0	1 0	1 0
$x_o^{<j>}$	1 0	1 0	1 0	1 0	1 0	1 0	0 0	0 0	0 0	0 0	0 0	0 0
σ	t_1	t_1	t_1	t_1	t_1	t_1	t_3	t_2	t_2	t_2	t_2	t_2
$x'^{<j>}_u$	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
$x'^{<j>}_o$	1 0	1 0	1 0	1 0	1 0	1 0	0 0	0 0	0 0	0 0	0 0	0 0
σ'	t_1	t_1	t_1	t_1	t_1	t_1	ζ	ζ	ζ	ζ	ζ	ζ

Table 1 Results of diagnosability test for $K = 5$.

Let us now investigate K-diagnosability with $K = 10$. Thus, the horizon is $h = J + K + 1 = 17$. The results of the K-diagnosability analysis are presented in Table 2.

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
$x_u^{<j>}$	0 0	0 0	0 0	0 0	0 0	0 0	0 1	1 0	1 0	1 0	1 0	1 0	1 0	0 0	0 0	0 0	0 0
$x_o^{<j>}$	1 0	1 0	1 0	1 0	1 0	1 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
σ	t_1	t_1	t_1	t_1	t_1	t_1	t_3	t_2	t_2	t_2	t_2	t_2	t_2	ζ	ζ	ζ	ζ
$x'^{<j>}_u$	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
$x'^{<j>}_o$	1 0	1 0	1 0	1 0	1 0	1 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
σ'	t_1	t_1	t_1	t_1	t_1	t_1	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ

Table 2 Results of diagnosability test for $K = 10$.

Here, we get $\kappa_{max} = \max(\lambda^\top.X) = 6$. Thus, T_f is K_{min}-diagnosable with $K_{min} = 7$. Indeed, the results of Table 2 can be interpreted as follows: the maximum value of κ such that T_f is not κ-diagnosable is $\kappa_{max} = 6$. Namely, this is due to the existence of two feasible firing sequences $\sigma_1 = t_1t_1t_1t_1t_1t_1t_3t_2t_2t_2t_2t_2$ (faulty) and $\sigma'_1 = t_1t_1t_1t_1t_1t_1$ (normal) such that $(\sigma_1, \sigma'_1) \in C(6)$.

5 K-diagnosability test on a compacted horizon

The determination of an appropriate value for J can be burdensome. Moreover, this value can be high, which impacts the computational effectiveness of the approach discussed in section 4 (which will be called ***Approach 1*** in the sequel). In this section, we will develop a variant of *Approach 1*, where parameter J is no more involved for the checking of K-diagnosability, hence significantly reducing the size of the ILP problem to be solved. In fact, the vectors from iteration $< 1 >$ to $< J >$ will be compressed without needing to know the value of J. Assumption ***H1*** will also be relaxed. A sufficient condition for K-diagnosability is then provided based on a new ILP formulation of the problem. In the sequel, this variant of *Approach 1* based on horizon compression will be referred to ***Approach 2***. In the last part of this section, we will show how the ILP formulation we develop in *Approach 2* can be advantageously used to characterize the value of J, which is necessary in *Approach 1*.

5.1 Modeling the faulty sequence

The compression of count vector X, corresponding to the faulty sequence σ (defined as (11)), on the interval $[\![1, J]\!]$ gives the following new vector $X_c \in \mathbb{N}^{(K+2).|T|}$:

$$X_c = \left((x^{<1\rightarrow J>})^\top \ (x^{<J+1>})^\top \ \dots \ (x^{<J+K+1>})^\top \right)^\top$$

where the compressed part $x^{<1\rightarrow J>}$ is as follows:

$$x^{<1\rightarrow J>} = \sum_{i=1}^{J} x^{<i>} = \begin{pmatrix} x_o^{<1\rightarrow J>} \\ x_u^{<1\rightarrow J>} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{J} x_o^{<i>} \\ \sum_{i=1}^{J} x_u^{<i>} \end{pmatrix}$$

while $x^{<J+1>}, \dots, x^{<J+K+1>}$ remain unchanged compared to X. To establish the model of the faulty sequence σ under horizon compression, we consider the following relations:

– Applying the positivity constraint to marking $M^{<J+1>}$ and the firing condition in (1) for all $j \in [\![J+1; J+K+1]\!]$ replacing $\sum_{i=1}^{J} x^{<i>}$ by $x^{<1\rightarrow J>}$, give $\Gamma_c.X_c \leq \Theta_c$ with:

$$\Gamma_c = \begin{pmatrix} -W & \mathbf{0} & \dots & \dots & \mathbf{0} \\ -W & W^- & & & \vdots \\ \vdots & & & & \mathbf{0} \\ -W & -W & \dots & -W & W^- \end{pmatrix} \text{ and } \Theta_c = \begin{pmatrix} M_0 \\ M_0 \\ \vdots \\ M_0 \end{pmatrix}$$

The dimensions of matrix Γ_c and vector Θ_c are $(2 + K).|P| \times (2 + K).|T|$ and $(2 + K).|P| \times 1$, respectively.

– The vector X_c also fulfills relations (12), (13), (14) and (15) which can be rewritten on a compacted horizon while replacing $\sum_{i=1}^{J} x^{<i>}$ by $x^{<1\rightarrow J>}$ and X by X_c. Therefore, while setting J to 1, v_1, f_1, f_2, v_2 and λ are replaced with v_{1c}, f_{1c}, f_{2c}, v_{2c} and λ_c, respectively.

Hence, we obtain the following polyhedron:

$$A_f^K.X_c \leq b_f^K \tag{24}$$

$$\text{with } A_f^K = \begin{pmatrix} \Gamma_c \\ f_{1c} \\ -f_{1c} \\ f_{2c} \\ -f_{2c} \\ v_{1c} \\ -v_{1c} \\ v_{2c} \\ \lambda_c^\top \\ -\lambda_c^\top \end{pmatrix} \text{ and } b_f^K = \begin{pmatrix} \Theta_c \\ 0 \\ 0 \\ 1 \\ -1 \\ \overrightarrow{1} \\ \mathbf{0} \\ \mathbf{0} \\ K \\ -1 \end{pmatrix}$$

5.2 Modeling the fault-free sequence

The compression of the count vector X' of the fault-free sequence defined as (18) on the interval $[1...J]$ gives the following new vector $X'_c \in \mathbb{N}^{(K+2).|T|}$:

$$X'_c = \left((x'^{<1\rightarrow J>})^\top \ (x'^{<J+1>})^\top \ \dots \ (x'^{<J+K+1>})^\top \right)^\top$$

where the compressed vector $x'^{<1\rightarrow J>}$ is defined as:

$$x'^{<1\rightarrow J>} = \sum_{i=1}^{J} x'^{<i>} = \begin{pmatrix} x'^{<1\rightarrow J>}_o \\ x'^{<1\rightarrow J>}_u \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{J} x'^{<i>}_o \\ \sum_{i=1}^{J} x'^{<i>}_u \end{pmatrix} \quad (25)$$

while $x'^{<J+1>}, \dots, x'^{<J+K+1>}$ remain unchanged. The model of fault-free sequence σ' under horizon compression satisfies the following constraints:
– Positivity constraint of marking $M'^{<J+1>} = M_0 + W.x'^{<1\rightarrow J>}$ and the firing conditions defined in (4) for $j \in [\![J+1; J+K+1]\!]$, give $\Gamma'_c.X'_c \leq \Theta_c$ with:

$$\Gamma'_c = \begin{pmatrix} -W & \mathbf{0} & \cdots & \mathbf{0} \\ -W & \boxed{W_o^- \ -W_u} & & \vdots \\ \vdots & & \ddots & \mathbf{0} \\ -W & \cdots & \cdots -W & \boxed{W_o^- \ -W_u} \end{pmatrix}$$

The dimensions of matrix Γ'_c is $(2+K).|P| \times (2+K).|T|$.
– Sequence σ' does not include any fault transition of class T_f, then we get $f_{3c}.X'_c = 0$ with $f_{3c} = \begin{pmatrix} c_f & c_f & \cdots & c_f \end{pmatrix}$.
Finally, we obtain the following polyhedron:

$$A_n^K.X'_c \leq b_n^K \quad (26)$$

where $A_n^K = \begin{pmatrix} \Gamma'_c \\ f_{3c} \\ -f_{3c} \end{pmatrix}$ and $b_n^K = \begin{pmatrix} \Theta_c \\ 0 \\ 0 \end{pmatrix}$

Faulty sequence σ and fault-free sequence σ' have the same observable projection, this can be expressed as:

$$D_c.X_c = D_c.X'_c \quad (27)$$

where D_c is the adaptation of the vector D defined in (9) to the horizon $h = K+2$. The dimension of $\boldsymbol{D}_c$ is then $(K+2).|E| \times (K+2).|T|$.

5.3 K_c-diagnosability condition

According to (24), (26) and (27), if there exists a couple of sequences $(\sigma, \sigma') \in C(\kappa)$ where $1 \leq \kappa \leq K$ under hypothesis ***H0***, then there exists a couple of corresponding count vectors $(X, X') \in \mathbb{N}^{(2+K).|T|} \times \mathbb{N}^{(2+K).|T|}$ that fulfills the following polyhedron:

$$A^K.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leq b^K \quad (28)$$

where $A^K = \begin{pmatrix} A_f^K & \mathbf{0} \\ \mathbf{0} & A_n^K \\ \boldsymbol{D}_c & -\boldsymbol{D}_c \\ -\boldsymbol{D}_c & \boldsymbol{D}_c \end{pmatrix}$ and $b^K = \begin{pmatrix} b_f^K \\ b_n^K \\ \mathbf{0} \\ \mathbf{0} \end{pmatrix}$

The dimensions of matrix A^K and vector b^K are $(2|T|(K+2)) \times ((K+2).(2|P| + 2|T| + |E| + 3) + 5)$ and $(2|T|(K+2)) \times 1$, respectively.

Let us consider the following optimization problem:

$$\begin{cases} \max(\lambda_c^\top.X_c) \text{ such that } (28) \\ X_c, X'_c \in \mathbb{N}^{(2+K).|T|} \end{cases} \quad (29)$$

We can now introduce the following result:

Theorem 10. *Consider an LPN under hypothesis **H0** and fault class T_f. Given $K \in \mathbb{N}^*$, T_f is K-diagnosable **if** either of the following two conditions is fulfilled:*
-i- (29) has no solution, or
-ii- (29) has a solution and $\max(\lambda_c^\top.X_c) < K$.

Proof. *i-* If (29) has no solution, then (23) has no solution either. Thus, according to Theorem 9 and Corollary 2, T_f is K-diagnosable and in particular 1-diagnosable. *ii-* If (29) has a solution and $\max(\lambda_c^\top.X_c) < K$, then for $\kappa = \max(\lambda_c^\top.X_c) + 1 \leq K$, there does not exist a couple of vectors (X_c, X'_c) satisfying (28). Thus, for $\kappa = \max(\lambda_c^\top.X_c) + 1 \leq K$, there does not exist a couple $(\sigma, \sigma') \in C(\kappa)$ and then T_f is K_c-diagnosable with $K_c = \max(\lambda_c^\top.X_c) + 1 \leq K$. Consequently, T_f is K-diagnosable.

Corollary 3. *If the sufficient condition for K-diagnosability in Theorem 10 is satisfied, then not only we can conclude that T_f is K-diagnosable but also that it is K_c-diagnosable where:*
a) $K_c = 1$ if (29) has no solution.
b) $K_c = \max_{\mathbb{N}}(\lambda_c^\top.X_c) + 1$ if (29) has a solution.
In addition, we can infer that $K_{min} \leq K_{cyc} \leq K_c \leq K$.

Remark 2. *Under hypothesis **H1**, the possible difference between K_c and K_{min} (i.e., the case when $K_c < K_{min}$) is due to the spurious solutions of state equation (28) as a consequence of the horizon compression.*

Example 2. *Again, let us consider the LPN of Fig. 2 and let $K = 10$. If we aim to test the K-diagnosability of t_f by compacting the interval $[\![1, J]\!]$, we obtain a compacted horizon $\tilde{h} = K + 2 = 12$. The resolution of the ILP problem (29) gives $\kappa'_{max} = \max(\lambda_c^\top.X_c) = 6 < K$. Therefore, we can conclude that t_f is 7-diagnosable and, hence, 10-diagnosable.*

j	$1 \to 6$	7	8	9	10	11	12	13	14	15	16	17
$x_u^{<j>}$	0	0	1	1	1	1	1	1	0	0	0	0
	0	1	0	0	0	0	0	0	0	0	0	0
$x_o^{<j>}$	6	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0
σ	$6 \times t_1$	t_3	t_2	t_2	t_2	t_2	t_2	t_2	ζ	ζ	ζ	ζ
$x'^{<j>}_u$	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0
$x'^{<j>}_o$	6	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0
σ'	$6 \times t_1$	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ	ζ

Table 3 10-diagnosability test based on a compacted horizon

5.4 Characterization of J

As highlighted in [1], the determination of a bound for the length of the relevant sequences leading to a fault (J that is necessary in *Approach 1* discussed in section 4 in our case , or $\mathcal{J}$ in [1]) is not an easy task, and no method is available yet to determine such a value. Although we do not provide a systematic method to compute a value of bound J, the contribution we discuss in this section aims to provide some characterization of this bound. Namely, we show that using the compressed system (28), we can determine a lower bound J^- of J. In fact, in the case when (28) has no solution, we get $K_c = K_{min} = 1$ in (29) and therefore determining a value for J to check K-diagnosability is useless. Therefore, we restrict the following analysis to the case when (28) admits a solution. In this case, let us denote by $\kappa'_{max} = \max(\lambda_c^\top.X_c)$ the computed cost function of system (29). The assumption ***H1*** of acyclicity is also considered in this subsection.

For some given $\kappa \in [\![1; K]\!]$, let us consider the two following sets:

$$S_1(\kappa) = \{\, \pi(\sigma_{bf}) \in \mathbb{N}^{|T|} \mid \sigma_{bf} \in \psi_D(T_f, \kappa) \,\}$$

$$S_2(\kappa) = \{\, x^{<1\to J>} \in \mathbb{N}^{|T|} \mid (28) \wedge (\lambda_c^\top.X_c = \kappa), \text{ with } X_c = (x^{<1\to J>\top} x^{<J+1>\top} \dots x^{<J+K+1>\top})^\top \}$$

Set $S_1(\kappa)$ corresponds to the count vectors of the sequences in $\psi_D(T_f, \kappa)$ (as introduced in section 3.2), while set $S_2(\kappa)$ holds the vectors $x^{<1\to J>}$ which are components of some vector X_c, which satisfies the following conditions: i)There exists X'_c such that(X_c, X'_c) satisfies (28) ii) $\lambda_c^\top.X_c = \kappa$. It is clear that $S_1(\kappa) \subseteq S_2(\kappa)$. Therefore, $\min_{S1(\kappa)} \|\pi(\sigma_{bf})\|_1 \geq \min_{S2(\kappa)} \|x^{<1\to J>}\|_1$ with $\kappa \in [\![1; K]\!]$ and then $J_K = \max_{1\leq\kappa\leq K} \min_{S1(\kappa)} \|\pi(\sigma_{bf})\|_1 \geq \max_{1\leq\kappa\leq K} \min_{S2(\kappa)} \|x^{<1\to J>}\|_1$. On the other hand, we have $\max_{1\leq\kappa\leq K} \min_{S2(\kappa)} \|x^{<1\to J>}\|_1 = \max_{1\leq\kappa\leq\kappa'_{max}} \min_{S2(\kappa)} \|x^{<1\to J>}\|_1$. Consequently, we get a lower bound of J_K, defined as follows:

$$\begin{cases} J_{low} = \max\limits_{1\leq\kappa\leq\kappa'_{max}} \min\limits_{\kappa} \|x^{<1\to J>}\|_1 \text{ such that (28)} \\ \text{and } \lambda_c^\top.X_c = \kappa \end{cases} \tag{30}$$

Furthermore, given the lower bound J_{low} of J_K, we can determine a lower bound κ^-_{max} for κ_{max} as follows:

$$\begin{cases} \kappa^-_{max} = \max(\gamma^\top.X) \text{ such that (22)} \\ J = J_{low} \end{cases} \tag{31}$$

We denote J^- the minimal value of J allowing the generation of κ^-_{max} such that $J^- \leq J_{low}$ Therefore, J^- is determined once κ^-_{max} in (31) is computed, as follows:

$$\begin{cases} J^- = \min(\| \sum\limits_{i=1}^{J} x^{<i>} \|_1) \text{ such that (22)} \\ J = J_{low} \\ \gamma^\top.X = \kappa^-_{max} \end{cases} \tag{32}$$

Now that lower bounds for κ_{max} and J_K, namely κ^-_{max} and J^-, respectively, have been determined analytically, we shall show how we can improve these bounds, empirically. Figure 4 represents a possible evolution of cost

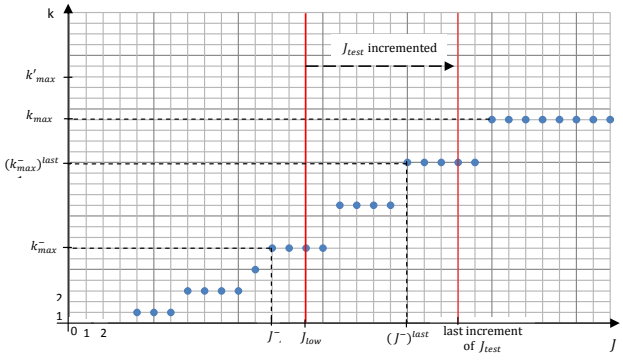

Fig. 4. Evolution of cost function $\max(\gamma^\top.X)$ of ILP problem (23) as a function of J under assumption ***H1***, when the fault class is not 1-diagnosable

function $\max(\gamma^\top.X)$ in ILP problem (23) as a function of J having integer values from 0 onwards in case (22) admits some solution (*i.e., T_f* is not 1-diagnosable). Let us denote by J_{test} the variable used to increment the value of J to improve (increase) the lower bounds of J_K and κ_{max}. Then, starting from $J_{test} = J_{low}$, we can increment the value of J_{test} iteratively, and we solve successively the two ILP problems (31) and (32) while replacing J_{low} by J_{test} in these systems. Based on the

fix-point theorem [24], one can be sure that the cost function of (31) will reach the value (κ_{max}) if J keeps increasing ($\kappa_{max} = K_{min} - 1$ if T_f is K-diagnosable with $K \geq 2$ and $\kappa_{max} = K$ if T_f is not K-diagnosable). It is however not possible to determine analytically when (κ_{max}) shall be reached (since κ_{max} is unknown). Therefore, in practice, unless the solution of (31) reaches κ'_{max} (such a case is considered in Remark 3), we can take as a lower bound of κ_{max} the value $(\kappa^{-}_{max})^{last}$ which is the cost function of (31) while replacing J_{low} by the last (highest) taken value of J_{test}. In addition, we can take as a lower bound of J, the cost function $(J^{-})^{last}$ of (32) while replacing J_{low} by the last (highest) taken value of J_{test}.

Remark 3. *In case the solution of (31) reaches κ'_{max}, we are sure that:*
–If $1 < \kappa'_{max} < K$, then K_{min} is determined, $K_{min} = K_c$;
–If $\kappa'_{max} = K$, then T_f is not K-diagnosable.
– J^{-} converges to the value of J_K, which is an optimal value of parameter J that is necessary in Approach 1. Such solution corresponds to the cost function of (32) while replacing J_{low} by the last (highest) taken value of J_{test}, and κ^{-}_{max} by κ'_{max}.

Example 3. *Let us consider the LPN of Figure 3 (used in both [1] and [7]), where $T_u = \{t_2, t_3\}$, $T_f = \{t_2\}$, $T_o = \{t_1, t_4, t_5, t_6, t_7\}$ with $\mathcal{L}(t_1) = a$, $\mathcal{L}(t_4) = \mathcal{L}(t_6) = b$, $\mathcal{L}(t_7) = c$, $\mathcal{L}(t_5) = d$, and $M_0 = [1\ 0\ 0\ 0]^{\top}$. We aim to verify the K-diagnosability with $K = 30$, on a compacted horizon $\tilde{h} = K + 2 = 32$. The cost function of system (29) gives $\kappa'_{max} = \max_{\mathbb{N}}(\lambda_c^{\top}.X_c) = 30 = K$. In this case, we cannot conclude on the K-diagnosability of t_f using a compact horizon. The resolution of the ILP problem (30) gives $J_{low} = 30$ which is a lower bound of J. The resolution of the ILP problem (31) on the horizon $(J_{low} + K + 1 = 61)$ gives $\kappa^{-}_{max} = 30 = \kappa'_{max}$. Then, according to Remark 3, t_f is not 30-diagnosable and $J = J_K = 30$.*

6 Discussion

6.1 Computational remarks and comparisons

The ILP formulation of the K-diagnosability test of *Approach 1* (see Section 4) involves $2|T|(J+K+1)$ unknowns and $(J + K + 1).(2|P| + 2|T| + |E| + 2) + K + 7$ constraints (cf. (22)). We recall here that the resolution of an ILP problem is NP-hard and can be done in an exponential time in the worst case w.r.t the system size. As we have mentioned earlier in the paper, the determination of the value of J is not an easy task, and such a value can be very large, which directly affects the complexity of the procedure. In fact, The number of variables and constraints of the above ILP formulation are as a function of J. To tackle this issue, we developed a second technique to investigate K-diagnosability while compacting the interval preceding the first fault class occurrence, therefore reducing the ILP system dimension and making the resolution procedure independent of J. This second ILP formulation involves $2|T|(K + 2)$ unknowns and $(K + 2).(2|P| + 2|T| + |E| + 3) + 5$ constraints (cf. (28)).

In the following, we present a comparison between our approach (*Approach 1*) for K/K_{min}-diagnosability analysis and a number of efficient relevant methods from the related literature. We firstly consider *graph-based* techniques, then *algebraic* approaches. In fact, it is worth noting that substantial improvements in terms of complexity have been brought by diagnosability techniques, that consider an FSA setting. In recent years, polynomial time algorithms w.r.t the number of states of the FSA model have been proposed in [17, 25]. In [27], Viana et al. proposed an even more efficient (polynomial) algorithm for (co)diagnosability analysis and then K_{min}-(co)diagnosability computation using a *verifier* model. The aforementioned approaches can be adapted to investigate K/K_{min}-diagnosability issues in bounded PNs. Nevertheless, this would require building the reachability graph of the net, and then to build some dedicated models for performing K/K_{min}-diagnosability analysis (verifier, etc.). We should also mention that some approaches have already been developed to tackle K/K_{min}-diagnosability issues in bounded PNs using *graph-based* settings. For instance, in [20], a subset of the reachability graph, namely the Basis Reachability Graph (BRG), is computed to perform (co)diagnosability analysis of a bounded LPN, and then to determine K_{min}-(co)diagnosability. A main issue is related to the combinatorial explosion when building the reachability graph (or the BRG) this computation raises. This motivates the use of algebraic techniques to deal with K/K_{min}-diagnosability issues in PNs. In fact, these techniques exploit the mathematical representation of PNs, and do not require computing the state space of the net. We can also mention that, based on ILP formulations, some techniques can be brought into play to improve the efficiency of the K-diagnosability analysis, such as, for instance, by achieving some relaxation of the ILP.

For unbounded PNs, an interesting approach is proposed in [7] to check K/K_{min}-diagnosability by investigating the coverability graph of a *verifier net*. A procedure to compute the value of K (and K_{min} when possible) was proposed based on a modified verifier net. The procedure determines the desired value of K directly from the marking of a new place that is added to the net structure. In [19], the authors investigate the K-(co)diagnosability of bounded/unbounded LPNs on the basis of a verifier established from the reachability/coverability graph of the net, and then the K_{min}-(co)diagnosability analysis is performed. The main drawback of the aforementioned approaches lies in the need of computing the coverability graph (for unbounded PNs), for which the computational complexity is not even in primitive recursive space (i.e., it requires more than exponential space) [18, 30].

From the above discussion, the approach in [1] remains one of the most efficient approaches for checking K-diagnosability, and it is also the closest one to our work. Thus, here-below, we provide a detailed comparison with our approach. Besides, in [3,6], we have carried out some comparative experimental studies that showed the advantages of algebraic approaches to investigate PN diagnosability issues, comparatively to graph-based ones, in terms of memory and time consumption.

In [1], the defined ILP problem involves the parameter $\mathcal{J}$. A lower bound of $\mathcal{J}$, denoted as $\mathcal{J}_{min}$, was defined that permits to fully describe the set of markings reachable from the initial marking and which enable for the first time the considered fault transition. The value of $\mathcal{J}_{min}$ is determined only for live and bounded nets. In addition, an upper bound of $\mathcal{J}_{min}$ is defined as a function of the initial marking and the minimal T-invariants of the LPN, and can be then very large, which directly impacts the complexity of the computation. In [1], the K-diagnosability test of a given fault transition t_f is then carried out by solving an ILP problem of $2(|TR|+|TR_u|)(J+K)$ unknowns and $3(J+K)|P|+3|P|+1$ constraints, thus at a comparable order of complexity as the first technique discussed in the present paper. However, in the case where the LPN is K-diagnosable, the technique in [1] does not provide the minimum value K_{min} ensuring K_{min}-diagnosability. To compute such a value, several executions of the K-diagnosability test are required, using for instance incrementation of K from 1 onwards. In contrast, the algebraic formulation developed in the present paper allows for performing the K-diagnosability test of a given fault class, considered as a whole, and if this fault class is K-diagnosable, the minimum value $K_{min} \leq K$ that ensures diagnosability is also determined directly, all at once. It is worth noticing here that the sufficient maximal length of J that we consider for K-diagnosability analysis in *Approach 1* (the value J_K) is potentially much lower than the value J defined in [1]. Indeed, while parameter $\mathcal{J}$ in [1] corresponds to an upper bound of the length of all the prefixes that enable a fault transition for the first time, we only consider a subset of these aforementioned prefixes in our analysis. Namely, we restrict the analysis to the subset of prefixes that have some continuation (of length 1 to K) upon the fault occurrence, in such a way that at least one corresponding indistinguishable fault-free sequence exists.

More importantly, we have shown that the length J_K of the longest sequence of this subset is finite even for unbounded PN. As a consequence, the established results are not limited to the case of bounded PNs. Besides, replacing the value of J in [1] by J_K allows for extending the results of [1] to the case of unbounded nets.

6.2 Experimental results

In this section, we report the experimental results of the K-diagnosability techniques developed in this paper. The railway benchmark proposed in [11] is used. It is about a railway level crossing system with n railway tracks (n variable). To assess the three approaches experimentally, and perform a comparison with that of [1], a Matlab® code was developed, which calls the FICO™ Xpress optimization solver (Note that the technique of [1] is also encoded as a Matlab® program calling FICO™ Xpress). The experiments were carried out on a dual core Intel(R) Xeon(R) CPU with a clock of 3.30 Ghz each, and 32 GB of RAM. We fix K to 125 and test the K/K_{min}-diagnosability of fault transition t_6 while incrementing the number of tracks n from 1 to 18, so as to increase the size of the model. To compare *Approach 1* with the approach in [1], we perform the tests using the same values of parameters J and $\mathcal{J}$. The obtained results are presented in Table 4. The benefits of the two developed approaches can be clearly noticed from the computation times. It should also be noted that the values of K_{min} determined in [3] for the cases n = 11 and n = 12 are not valid. This is indeed due to the underestimation of the value of $\mathcal{J}$ (fixed to 12) considered in the experiments performed in [3].

n	J	Approach of Basile et al. [1]			*Approach 1*		*Approach 2*	
		K-diag?	$T(s)$ [2]	K_{min}-diag	**K-diag?**	$T(s)$	**K-diag?** / K_c	$T(s)$
1	3	YES	62	7	YES / 7	4	YES / 7	6
2	6	YES	31	13	YES / 13	16	YES / 13	13
3	9	YES	59	19	YES / 19	105	YES / 19	24
4	12	YES	70	25	YES / 25	55	YES / 25	31
5	15	YES	100	31	YES / 31	57	YES / 31	25
6	18	YES	108	37	YES / 37	107	YES / 37	117
7	21	YES	145	43	YES / 43	1399	YES / 43	63
8	24	YES	211	49	YES / 49	145	YES / 49	1332
9	27	YES	334	55	YES / 55	195	YES / 55	105
10	30	YES	224	61	YES / 61	195	YES / 61	174
11	33	YES	325	67	YES / 67	277	YES / 67	199
12	36	YES	352	73	YES / 73	439	YES / 73	165
13	39	YES	109	79	o.m		YES / 79	851
14	42	YES	157	85	o.t		YES / 85	368
15	45	o.m		10931	(> 2 hours)		YES / 91	399
16	48	(out of memory)					YES / 97	356
17	51						YES / 103	406

Table 4 Obtained results for the 3 approaches

7 Conclusion

In this paper, we proposed a number of algebraic approaches for K-diagnosability analysis in DES, modeled as partially observable LPN, that can be unbounded. The first approach is based on ILP optimization techniques, and provides a necessary and sufficient condition for K-diagnosability of a fault class, under the hy-

pothesis of acyclicity of the unobservable subnet. If the investigated fault class is K-diagnosable, the minimum value $K_{min} \leq K$ ensuring K_{min}-diagnosability is also computed, simultaneously. Moreover, the parameter J defined in our approach to characterize the subset of faulty sequences that are relevant for investigating K-diagnosability allows for extending the approach of [1] to the case of unbounded LPNs. The relaxation of the acyclicity hypothesis on the unobservable subnet is also discussed. Namely, we show that based on the developed formulation, a sufficient condition for K-diagnosability can be established in this case. A second approach using a compacted horizon is then developed, reducing the system dimension and, above all, dispensing with the parameter J that characterizes the number of possible events preceding the first fault occurrence. Such a parameter being not easy to determine. In the second approach, we relax the acyclicity hypothesis regarding the unobservable subnet. A sufficient condition for K-diagnosability is established and can be checked as an integer optimization problem. If the condition is fulfilled, a value K_c that is potentially lower than K ($K_c \in [\![K_{min}; K]\!]$) ensuring ($K_c$-)diagnosability is also determined. A characterization of the parameter J used in *Approach 1* is performed based on horizon compression.

In future work, the characterization of parameter J will be pursued. Moreover, an extension of our techniques to the case of intermittent faults will be investigated.

References

[1] Francesco Basile, Pasquale Chiacchio, and Gianmaria De Tommasi. On K-diagnosability of Petri nets via integer linear programming. *Automatica*, 48(9):2047–2058, 2012.

[2] Francesco Basile, Gianmaria De Tommasi, and Claudio Sterle. Sensors selection for K-diagnosability of Petri nets via integer linear programming. In *23rd Mediterranean Conference on Control and Automation*, pages 168–175. IEEE, 2015.

[3] Francesco Basile, Gianmaria De Tommasi, Claudio Sterle, Abderraouf Boussif, and Mohamed Ghazel. Efficient diagnosability assessment via ilp optimization: a railway benchmark. In *23rd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, volume 1, pages 441–448. IEEE, 2018.

[4] Abderraouf Boussif, Mohamed Ghazel, and João Carlos Basilio. Intermittent fault diagnosability of discrete event systems: an overview of automaton-based approaches. *Discrete Event Dynamic Systems*, 31:1–44, 2020.

[5] Abderraouf Boussif, Mohamed Ghazel, and Kais Klai. A semi-symbolic diagnoser for fault diagnosis of bounded labeled Petri nets. *Asian Journal of Control*, 23:648–660, 2020.

[6] Abderraouf Boussif, Baisi Liu, and Mohamed Ghazel. An experimental comparison of three diagnosis techniques for discrete event systems. *In 28th International Workshop on Principles of Diagnosis (DX'17)*, 2017.

[7] Maria Paola Cabasino, Alessandro Giua, Stéphane Lafortune, and Carla Seatzu. A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Transactions on Automatic Control*, 57(12):3104–3117, 2012.

[8] Maria Paola Cabasino, Alessandro Giua, and Carla Seatzu. Diagnosability of bounded Petri nets. In *Proceedings of the 48th IEEE Conference on Decision and Control (CDC)*, pages 1254–1260. IEEE, 2009.

[9] Christos G. Cassandras and Steéphane Lafortune. *Introduction to discrete event systems*. Springer Science & Business Media, 2009.

[10] Eric Dallal and Stéphane Lafortune. On most permissive observers in dynamic sensor activation problems. *IEEE Transactions on Automatic Control*, 59(4):966–981, 2013.

[11] Mohamed Ghazel and Baisi Liu. A customizable railway benchmark to deal with fault diagnosis issues in DES. In *13th International Workshop on Discrete Event Systems (WODES)*, pages 177–182. IEEE, 2016.

[12] Christoforos N. Hadjicostis. *Estimation and Inference in Discrete Event Systems: A Model-Based Approach with Finite Automata*. Springer International Publishing, 2020.

[13] Stéphane Lafortune, Feng Lin, and Christoforos N. Hadjicostis. On the history of diagnosability and opacity in discrete event systems. *Annual Reviews in Control*, 45:257–266, 2018.

[14] Baisi Liu, Mohamed Ghazel, and Armand Toguyeni. On-the-fly and incremental technique for fault diagnosis of discrete event systems modeled by labeled Petri nets. *Asian Journal of Control*, 19(5):1659–1671, 2017.

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

[16] J Pan and Shahin Hashtrudi-Zad. Diagnosability test for timed discrete-event systems. In *2006 18th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'06)*, pages 63–72. IEEE, 2006.

[17] Wenbin Qiu and Ratnesh Kumar. Decentralized failure diagnosis of discrete event systems. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 36(2):384–395, 2006.

[18] Charles Rackoff. The covering and boundedness problems for vector addition systems. *Theoretical Computer Science*, 6(2):223–231, 1978.

[19] Ning Ran, Jinyuan Hao, Zijian Dong, Zhou He, Zhiheng Liu, Yuan Ruan, and Shouguang Wang. K-codiagnosability verification of labeled petri nets. *IEEE Access*, 7:185055–185062, 2019.

[20] Ning Ran, Hongye Su, Alessandro Giua, and Carla Seatzu. Codiagnosability analysis of bounded petri nets. *IEEE Transactions on Automatic Control*, 63(4):1192–1199, 2017.

[21] Ning Ran, Hongye Su, and Shouguang Wang. An improved approach to test diagnosability of bounded Petri nets. *IEEE/CAA Journal of Automatica Sinica*, 4(2):297–303, 2017.

[22] Spyros Reveliotis. A necessary and sufficient condition for the liveness and reversibility of process-resource nets with acyclic, quasi-live, serializable, and reversible process subnets. *IEEE transactions on automation science and engineering*, 3(4):462–468, 2006.

[23] Meera Sampath, Raja Sengupta, Stéphane Lafortune, Kasim Sinnamohideen, and Demosthenis Teneketzis. Diagnosability of discrete-event systems. *IEEE Transactions on automatic control*, 40(9):1555–1575, 1995.

[24] Alfred Tarski. A lattice-theoretical fixpoint theorem and its applications. *Pacific journal of Mathematics*, 5(2):285–309, 1955.

[25] Jean HA Tomola, Felipe G Cabral, Lilian K Carvalho, and Marcos V Moreira. Robust disjunctive-codiagnosability of discrete-event systems against permanent loss of observations. *IEEE Transactions on Automatic Control*, 62(11):5808–5815, 2016.

[26] Gustavo S Viana and João C Basilio. Codiagnosability of discrete event systems revisited: A new necessary and sufficient condition and its applications. *Automatica*, 101:354–364, 2019.

[27] Gustavo S Viana, Marcos V Moreira, and Joao C Basilio. Codiagnosability analysis of discrete-event systems modeled by weighted automata. *IEEE Transactions on Automatic Control*, 64(10):4361–4368, 2019.

[28] YuanLin Wen and Muder Jeng. Diagnosability analysis based on T-invariants of Petri nets. In *Proceedings of IEEE Networking, Sensing and Control*, pages 371–376. IEEE, 2005.

[29] YuanLin Wen, ChunHsi Li, and Muder Jeng. A polynomial algorithm for checking diagnosability of Petri nets. In *IEEE International Conference on Systems, Man and Cybernetics*, volume 3, pages 2542–2547. IEEE, 2005.

[30] Xiang Yin and Stéphane Lafortune. On the decidability and complexity of diagnosability for labeled petri nets. *IEEE Transactions on Automatic Control*, 62(11):5931–5938, 2017.

[31] Tae-Sic Yoo and H Garcia. Computation of fault detection delay in discrete-event systems. In *Proceedings of the 14th International Workshop on Principles of Diagnosis, DX'03*, pages 207–212, 2003.

[32] Janan Zaytoon and Stéphane Lafortune. Overview of fault diagnosis methods for discrete event systems. *Annual Reviews in Control*, 37(2):308–320, 2013.

Amira Chouchane is currently a post-doc researcher at University Gustave Eiffel (COSYS/ESTAS laboratory), France. She received the Electrical and Automatic Control Engineering degree in 2010 and the M.Sc. degree in Automatic and Intelligent Techniques in 2011 from the National Engineering School of Gabès, Tunisia. She obtained the Ph.D. degree in Control, Production and Robotics from the University of Angers, France, jointly with the Ph.D. degree in Electrical Engineering from the National Engineering School of Sfax, Tunisia, in 2018. Her research deals with modeling, control and diagnosis of discrete event systems.

Mohamed Ghazel is a Research Director with the University Gustave Eiffel - COSYS/ESTAS team. He received the Master and Ph.D. degrees in Automatic Control and Industrial Computer Sciences from the École Centrale de Lille in 2002 and 2005, respectively; and the HDR (Habilitation à Diriger des Recherches) from University Lille Nord de France in 2014. His research mainly focuses on the engineering, safety and interoperability of transportation systems using discrete event models and formal methods. Dr. Ghazel is a member of the IFAC TC 7.4 on Transportation Systems and TC 9.2 on Social Impact of Automation, and has been involved in several national and European research projects. He acts as an expert for the European Commission in the framework of innovation programs.

Abderraouf Boussif is a Researcher with the French Railway Technological Research Institute (IRT Railenium). He received the B.-Eng. degree in System Control Engineering from the École Nationale Polytechnique, Algiers, Algeria, in 2012, the Master degree in Complex Systems Engineering from the École Normale Supérieure de Cachan, Paris, in 2013, and the Ph.D. degree in Safety System Engineering from the University of Lille, France, in 2016. His research interests are mainly in railway safety assurance, formal methods, model-based safety analysis, and fault diagnosis of safety-critical systems.