An Efficient Algorithm for K -Diagnosability Analysis of Bounded and Unbounded Petri Nets

A Chouchane, M Ghazel

An Efficient Algorithm for K-Diagnosability Analysis of Bounded and Unbounded Petri Nets ⋆

A. Chouchane *, **M. Ghazel** *

* *COSYS-ESTAS, Univ. Gustave Eiffel, Lille Campus, F-59650, Villeneuve d'Ascq, France (e-mail: chouchanea41@gmail.com, mohamed.ghazel@univ-eiffel.fr).*

Abstract: In this paper, we propose a polynomial algorithm for conducting K-diagnosability analysis on both bounded and unbounded labeled Petri nets. More specifically, we formulate a sufficient condition for K-diagnosability by addressing the relaxation (in $\mathbb{R}$) of an Integer Linear Programming (ILP) problem defined on a compacted horizon. In addition, if the model is K-diagnosable, the technique provides a value K_{relax}, potentially lower than K, that ensures (K_{relax}-)diagnosability. To assess the performance and efficiency of the developed method, a Petri net model of a railway benchmark is investigated.

Keywords: K-diagnosability, bounded and unbounded labeled Petri nets, discrete event systems, linear optimization technique.

1. INTRODUCTION AND RELATED WORKS

In this paper, our focus is on investigating the K-diagnosability of Discrete Event Systems (DES) modeled by a partially observed Labeled Petri Net (LPN). K-diagnosability refers to the ability to diagnose any fault with certainty, provided that at least K events have occurred following the fault occurrence ($K \in \mathbb{N}$). 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 a recent work Chouchane et al. (2023), we have investigated the K/K_{min}-diagnosability problems in bounded and unbounded LPNs, while assuming the unobservable subnet to be acyclic. The main contribution lies in the development of a necessary and sufficient condition for K-diagnosability, which can be checked by means of ILP optimization techniques. Besides, if the investigated fault class is K-diagnosable, the minimum value $K_{min} \leqslant K$ ensuring K_{min}-diagnosability is also provided by the same analysis, without requiring further investigation. Furthermore, the parameter J introduced in this methodology (distinct from the one defined in Basile et al. (2012)), which serves to characterize the set of faulty sequences that are relevant to the examination of K-diagnosability, enabled an expansion of the approach proposed in Basile et al. (2012) to address the case of unbounded nets.

The present work is, in fact, an extension of the approach established in Chouchane et al. (2023). In fact, using algebraic techniques offers crucial advantages in terms of efficiency compared to *graph-based* approaches (Liu et al. (2017); Cabasino et al. (2012)), since algebraic techniques (Basile et al. (2012, 2015); Zhu et al. (2021)) do not require building the state space of the net. Yet, addressing ILP problems can entail significant computational costs. Specifically, these problems are NP-hard, and their solving complexity grows exponentially with the number of variables, in the worst case (Boccia et al. (2020); Lancia and Serafini (2021)). Our goal here is to improve the computational complexity of the approach in Chouchane et al. (2023), while dispensing from the determination of parameter J. Namely, we propose a new algorithm for K-diagnosability analysis, in a compacted horizon, based on the relaxation of an ILP problem (in $\mathbb{R}$). Using a compacted horizon not only reduces the system's dimensionality but also eliminates the need for parameter J, which could be difficult to determine in an optimal way. The technique we discuss in the present paper provides a sufficient condition for K-diagnosability. Moreover, when the established (sufficient) condition is fulfilled, a value K_{relax} is given such that the fault class is K_{relax}-diagnosable where $K_{min} \leqslant K_{relax} \leqslant K$.

The structure of the paper is outlined as follows. In Section 2, we introduce some essential preliminary concepts and highlight key findings from Chouchane et al. (2023), focusing on K-diagnosability using ILP problems. Section 3 explores the relaxation of the ILP problem in $\mathbb{R}$ and establishes a sufficient condition for K-diagnosability. Section 4 illustrates the developed technique on the basis of a railway Petri Net model, while demonstrating the effectiveness of our technique. Finally, in Section 5, we conclude the paper and present potential directions for future research.

2. PRELIMINARIES

2.1 Notations

A Petri net, denoted as $\mathcal{N} = (P, T, W^-, W^+)$, is defined by sets P and T, representing non-empty finite sets of places

⋆ This paper was not presented at any IFAC meeting.

and transitions, respectively. The pre-incidence matrix is denoted as W^- and the post-incidence matrix as W^+. The incidence matrix W is calculated as $W = W^+ - W^-$.
The marking of a place p is denoted as $M(p)$. A marked Petri net is represented as $(\mathcal{N}, M_0)$, where M_0 is the known initial marking. The notation $M\ [\ t\ \succ$ signifies a transition t *enabled* by marking M if $M(p) \geqslant W^-(p,t)$ for all places $p \in P$. The term $M\ [\ t\ \succ M'$ indicates that marking M' is reachable from marking M by firing transition t ($M' = M + W(\cdot, t)$). The reachability set of $(\mathcal{N}, M_0)$ is denoted as $R(\mathcal{N}, M_0)$. The language of the net is represented by $L(\mathcal{N}, M_0) = \{\sigma \in T^* | \exists M \in R(\mathcal{N}, M_0) : M_0\ [\sigma \succ M\}$.
The notation $\pi_T(\sigma)$ refers to the *count vector* associated with sequence $\sigma \in T^*$ where the i^{th} element of vector $\pi_T(\sigma)$ represents the number of firings of transition t_i in σ. The set T_o represents observable transitions, while T_u denotes unobservable ones. $P_o(\sigma)$ and $P_u(\sigma)$ correspond to the projection of σ on T_o^*, and T_u^*, respectively. The function $\pi_{T_o} : T_o^* \rightarrow \mathbb{N}^{|T_o|}$ restricts the application of function π_T to observable sequences and, similarly, $\pi_{T_u} : T_u^* \rightarrow \mathbb{N}^{|T_u|}$ restricts it to the set of unobservable sequences. The observable subnet of Petri Net $\mathcal{N}$ is denoted as $\mathcal{N}_o = (P, T_o, W_o^-, W_o^+)$, with $W_o^- = W_{|T_o}^-$, and $W_o^+ = W_{|T_o}^+$. Similarly, the unobservable subnet is denoted as $\mathcal{N}_u = (P, T_u, W_u^-, W_u^+)$, with $W_u^- = W_{|T_u}^-$, and $W_u^+ = W_{|T_u}^+$.
The *labeling function*, denoted as $\mathcal{L} : T \rightarrow E \cup \{\varepsilon\}$, assigns to each transition $t \in T$ either a label in E if $t \in T_o$, or ε if $t \in T_u$. An LPN system, represented as $\mathcal{N}_\mathcal{L} = (\mathcal{N}, M_0, E, \mathcal{L})$, consists of a Petri net $\mathcal{N}$ with a known initial marking M_0 and a finite set of events E that are assigned to its transitions as labels, by means of the labelling function $\mathcal{L}$. The extension of $\mathcal{L}$ to transition sequences is denoted as $\mathcal{L} : T^* \rightarrow \{E \bigcup \{\varepsilon\}\}^*$. The projection of $\sigma \in T^*$ in the set of observable labels E^* is denoted by $P_l(\sigma)$ and is defined as $P_l(\sigma) = \mathcal{L}(P_o(\sigma))$. The inverse projection operator, denoted as $P_l^{-1}(w), w \in E^*$, is defined as: $P_l^{-1}(w) = \{\sigma \in T^* \mid P_l(\sigma) = w\}$. Function $\pi_E : E^* \rightarrow \mathbb{N}^{|E|}$ assigns to any word $w \in E^*$ a vector $y = \pi_E(w) \in \mathbb{N}^{|E|}$, where each component $\pi_E(w)^i, 1 \leqslant i \leqslant |E|$, corresponds to the number of occurrences of the i^{th} label in E within w. The set of sequences that enable fault class T_f *for the first time* is defined as $\psi(T_f) = \{\sigma \in T^* |(\ T_f \notin \sigma) \wedge (\exists\, \varepsilon_f \in T_f :\ M_0[\sigma\varepsilon_f\ \succ)\}$.

2.2 LPN structure

In the considered LPN, the set of transitions is partitioned as $T = T_o \uplus T_u$, where T_o (resp. T_u) is the set of observable (resp. unobservable) transitions. The set of unobservable transitions is, in turn, 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 be partitioned into r disjoint subsets ($T_f = \bigcup_{i=1}^{r} F_i$) that represent the different fault classes. Without loss of generality and for the sake of clarity, one single fault class (T_f), is considered in this paper. A sequence $\sigma \in T^*$ is said to be faulty if it contains at least one fault transition of T_f (*i.e.*, $\exists\ \varepsilon_f \in T_f$ such that $\varepsilon_f \in \sigma$). In the remainder of the paper, we say that *fault class T_f occurred* to mean that some fault transition $\varepsilon_f \in T_f$ has fired.

In this paper, for K-diagnosability analysis, we consider the following assumptions:
H0) the considered LPN does not reach a deadlock after firing any fault transition, and
H1) the unobservable subnet is acyclic.

2.3 K/K_{min}-diagnosability of an LPN

***Definition** 1. (K-diagnosability of a fault class)* A fault class T_f in an LPN is K-diagnosable for some given integer $K \in \mathbb{N}^*$, if the following holds:
$(\forall \sigma_{bf} \in \psi(T_f))(\forall \sigma_{af} | M_0[\sigma_{bf}\varepsilon_f\sigma_{af}\ \succ ; \varepsilon_f \in T_f) :$
$|\sigma_{af}| \geqslant K \Rightarrow Diag$
where the diagnosability condition is defined as:
$Diag : \sigma \in P_l^{-1}[P_l(\sigma_{bf}\sigma_{af})] \Rightarrow T_f \in \sigma.$

A corollary problem arises in the case when K-diagnosability is confirmed. Namely, it consists to determine a minimum value $K_{min} \leqslant K$ that ensures (K_{min}-)diagnosability.

2.4 Algebraic approach for K/K_{min}-diagnosability analysis in Chouchane et al. (2023)

In the present paper, we build upon our work discussed in Chouchane et al. (2023), which addresses K and K_{min}-diagnosability in LPNs.

A. Principle.

The principle of the approach is as follows: *Given an LPN and a fault class T_f, the K/K_{min}-diagnosability analysis problem can be rephrased as follows: is there $K_{min} \leqslant K$ such that T_f is K_{min}-diagnosable and T_f is not $(K_{min}-1)$-diagnosable?* If so, T_f is K_{min}-diagnosable and therefore K-diagnosable.

To determine K_{min}, we proceed as follows: we assume that there exists some value $\kappa, 1 \leqslant \kappa \leqslant K$, such that T_f is not κ-diagnosable. Hence, we determine the maximum value of κ, denoted as κ_{max} (if it does exist) such that there exit two feasible firing sequences $\sigma, \sigma' \in T^*$ fulfilling the following condition denoted as $C_{\sigma-\sigma'}(\kappa)$:

$$C_{\sigma-\sigma'}(\kappa) : \begin{cases} \sigma = \sigma_{bf}\varepsilon_f\sigma_{af}, \sigma_{bf} \in \psi(T_f), \varepsilon_f \in T_f, \\ |\sigma_{af}| = \kappa; \\ T_f \notin \sigma'; \\ P_l(\sigma) = P_l(\sigma'). \end{cases}$$

Therefore, the following verdict can be inferred:

- If $\nexists \kappa$ verifying $C_{\sigma-\sigma'}(\kappa)$, then $K_{min} = 1$.
- If $1 \leqslant \kappa_{max} < K$ then $K_{min} = \kappa_{max} + 1$.
- If $\kappa_{max} = K$ then T_f is not K-diagnosable.

B. Algebraic model.

In Chouchane et al. (2023), in order to establish a necessary and sufficient condition for K-diagnosability, an algebraic model is developed for formulating sequences σ and σ' that satisfy condition $C_{\sigma-\sigma'}(\kappa)$ for some value $\kappa, 1 \leqslant \kappa \leqslant K$. To achieve this goal, it is essential to characterize the length of the sequences within $\psi(T_f)$, *i.e.*, which enable fault class T_f for the first time, without the need to explicitly determine the entire set. In Chouchane et al. (2023), a necessary and sufficient condition for

$K-$diagnosability was established for bounded and unbounded LPNs using ILP techniques. The main idea of the technique developed in Chouchane et al. (2023) will be summarized in what follows, so that the contribution developed in the present paper be self-contained. Note that, similarly to the work in Basile et al. (2012) and the recent approach in Basile et al. (2023) discussing initial state opacity analysis, in Chouchane et al. (2023) we considered the following assumption:

H2) A sufficient maximal length J of the prefixes that activate fault class T_f, for the first time, is known.

Modeling the faulty sequence:
Let us assume that fault class T_f is K_{min}-diagnosable with $K_{min} > 1$, then there exists at least one firable sequence $\sigma = \sigma_{bf}\varepsilon_f\sigma_{af}$ from M_0 such that:

- $\sigma_{bf} = t^{<1>}t^{<2>}\dots t^{<J>}$ with $t^{<i>} \in (T \setminus T_f) \cup \{\zeta\}$ for all $i \in [\![1, J]\!]$, where ζ stands for the empty step sequence;
- $\varepsilon_f = t^{<J+1>} \in T_f$;
- $\sigma_{af} = t^{<J+2>}, \dots, t^{<J+K_{min}>}$ with $t^{<i>} \in T$ for all $i \in [\![J+2, J+K_{min}]\!]$; and
- there exists at least one fault-free sequence $\sigma' \in (T \setminus T_f)^*$ enabled from M_0, such that $P_l(\sigma) = P_l(\sigma')$.

In fact, since $K_{min} \leqslant K$ is not known a priori, we expand the firing sequence σ_{af} over horizon $J+K+1$ by taking $t^{<J+K_{min}+1>}, \cdots, t^{<J+K+1>}$ as empty step sequences in case $K_{min} < K$. Therefore, we can write $\sigma = t^{<1>}t^{<2>}\cdots t^{<J+K+1>}$, where for $i \in [\![1, J+K+1]\!]$ $t^{<i>}$ may 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 $x_u^{<i>} = \pi_{T_u}(t^{<i>})$, yielding $x^{<i>} = [(x_o^{<i>})^\top \ (x_u^{<i>})^\top]^\top$. Consequently, we get the following set of constraints:

$$\begin{cases} W^- \cdot x^{<1>} \leqslant M_0 \\ -W.\sum_{i=1}^{j-1} x^{<i>} + W^- \cdot x^{<j>} \leqslant M_0 \ ; \forall j \in [\![2, J+K+1]\!] & (a) \\ 0 \leqslant c.x^{<j>} \leqslant 1, \forall j \in [\![1, J+K+1]\!] & (b) \\ \sum_{i=1}^{J} c_f.x^{<i>} = 0 & (c) \\ c_f.x^{<J+1>} = 1 & (d) \\ c.x^{<j>} - c.x^{<j+1>}, \forall j \in [\![J+2, J+K]\!] & (e) \\ 1 \leqslant \sum_{i=J+2}^{J+K+1} c.x^{<i>} \leqslant K & (f) \end{cases} \quad (1)$$

where c is a row vector of $1'$s of dimension $|T|$ and 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.

Constraints (a) arise from the firing conditions of transitions $t^{<1>}, \dots, t^{<J+K+1>}$ respectively. Constraints (b) stipulate that, during each iteration $< j >$ from $< 1 >$ to $< J+K+1 >$, no more than one transition can be fired. Constraint (c) ensures that no fault transition of fault class T_f occurs from iteration $< 1 >$ to iteration $< J >$. Constraint (d) specifies that the initial appearance of a fault transition in T_f takes place at the $(J+1)^{th}$ iteration. Constraints (e) dictate that, within iterations $< J+2 >$ to $< J+K+1 >$, the count vector remains at 1 until the $< J+K_{min}+1 >^{th}$ iteration, where it irrevocably switches to 0 and stays at 0 until the final iteration $< J+K+1 >$. Constraint (f) stipulates that the faulty sequence σ includes a minimum of one transition and a maximum of K transitions after the first occurrence of the fault class.

Remark** 1.* Under ***H0, system (1) is satisfied *iff* there exists a feasible faulty sequence σ with a maximum of K transition firings upon the first occurrence of fault class T_f. In fact, (1) corresponds to the state equation that describes a faulty sequence σ (with $|\sigma| \leqslant J+K+1$)), accounting for at most one transition firing per iteration (Theorem 3 in Chouchane et al. (2023)).

Modeling the fault-free sequence
Now that faulty sequence σ has been formally defined, let us assume the existence of a corresponding non-faulty indistinguishable sequence (w.r.t. T_f) σ', such that $P_l(\sigma) = P_l(\sigma') = w$. Given that σ comprises at most $J+K+1$ transitions, we can deduce that $|w| \leqslant J+K+1$. Hence, we can represent w as $w = l^{<1>}l^{<2>}\dots l^{<J+K+1>}$, where $l^{<i>}$ denotes the label produced at iteration $< i >$, which may be either a label in E or the empty step label. Let $\sigma_o^{'} = P_o(\sigma')$, and let $\sigma_o^{'}$ as $\sigma_o^{'} = t_o^{'<1>}t_o^{'<2>}\dots t_o^{'<J+K+1>}$ where $t_o^{'<i>} \in \mathcal{L}^{-1}(l^{<i>})$ if $l^{<i>} \in E$, and the empty sequence otherwise. Consider the unobservable sequences (explanations) $\sigma_u^{'<1>}, \sigma_u^{'<2>}, \dots, \sigma_u^{'<J+K+1>}$ that are coherent with transitions $t_o^{'<1>}, t_o^{'<2>}, \dots, t_o^{'<J+K+1>}$, respectively. The firing count vector of the fault-free sequence $\sigma^{'}$ can then be written as $\sigma^{'} = \sigma_u^{'<1>}t_o^{'<1>}\sigma_u^{'<2>}t_o^{'<2>}\dots\sigma_u^{'<J+K+1>}t_o^{'<J+K+1>}$.

Let $x^{'<i>} = ((x_o^{'<i>})^\top \ (x_u^{'<i>})^\top)^\top$ be the firing count vector of $\sigma_u^{'<i>}t_o^{'<i>}$ where $x_o^{'<i>} = \pi_{T_o}(t_o^{'<i>})$ and $x_u^{'<i>} = \pi_{T_u}(\sigma_u^{'<i>})$. The following set of constraints can therefore be derived:

$$\begin{cases} -W_u.x_u^{'<1>} + W_o^-.x_o^{'<1>} \leqslant M_0 \\ -W_u.\sum_{i=1}^{j} x_u^{'<i>} - W_o.\sum_{i=1}^{j-1} x_o^{'<i>} + W_o^-.x_o^{'<j>} \\ \qquad \leqslant M_0; \forall j \in [\![2, J+K+1]\!] & (f) \\ \sum_{i=1}^{J+K+1} c_f.x^{'<i>} = 0 & (g) \end{cases} \quad (2)$$

Constraints (f) stem from the firing conditions, while constraint (g) dictates that sequence θ must be devoid of any fault transitions.

Remark** 2.* Under hypotheses ***H0 and ***H1***, equation (2) is satisfied if and only if there exists some feasible fault-free sequence σ'. In fact, in a PN with an acyclic unobservable subnet, every positive solution of state equation $M = M_0 + W.x$ corresponds to a count vector of an actual feasible firing sequence (Theorem 1 in Chouchane et al. (2023)).

Let us now establish the relationship between $x_o{}^{<i>}$ and $y^{<i>}$, $i \in [\![1, J]\!]$ where $y^{<i>}$ represents the count vector of the observed label associated with the i^{th} iteration. To achieve this, let us consider the arrangement of T_o and E as $\{t_1, \cdots, t_{|T_o|}\}$ and $\{\ell_1, \cdots, \ell_{|E|}\}$, respectively. Let $\wp \in \{0,1\}^{|E|\times|T_o|}$ be the labeling matrix, where the general term $\wp_{qr}$ is defined as follows for $q \in [\![1, |T_o|]\!]$ and $r \in [\![1, |E|]\!]$:

$$\begin{cases} \wp_{qr} = 1 \text{ if } \mathcal{L}(t_r) = \ell_q \\ \wp_{qr} = 0 \text{ otherwise} \end{cases} \quad (3)$$

Hence, $y^{<i>} = \wp \cdot {x_o}^{<i>}$ for all $i \in [\![1, J+K+1]\!]$. The two sequences σ and σ' have the same observable projection, hence the following relationship can be stated:

$$\wp \cdot {x_o}^{<i>} = \wp \cdot {x_o}'^{<i>} \ ; \forall i \in [\![1, J+K+1]\!] \quad (4)$$

Final model

Let us define $X, X' \in \mathbb{N}^{(J+K+1).|T|}$, count vectors of sequences σ and σ', respectively, as follows:

$$\begin{aligned} X &= \left((x^{<1>})^\top \ (x^{<2>})^\top \ \dots \ (x^{<J+K+1>})^\top \right)^\top \\ X' &= \left((x'^{<1>})^\top \ (x'^{<2>})^\top \ \dots \ (x'^{<J+K+1>})^\top \right)^\top \end{aligned} \quad (5)$$

Based on Remarks 1 and 2, the existence of a pair $(\sigma, \sigma') \in C(\kappa)$ under assumptions ***H0*** and ***H1*** is equivalent to the existence of a pair of vectors $(X, X') \in \mathbb{N}^{(J+K+1).|T|} \times \mathbb{N}^{(J+K+1).|T|}$ satisfying the following relation:

$$A. \begin{pmatrix} X \\ X' \end{pmatrix} \leqslant b \quad (6)$$

where A and b are easily inferred from (1), (2) and (4).

C. Necessary and sufficient condition for K−diagnosability.

Let us denote by κ_{max} the cost function of the following optimization problem when system (6) is feasible:

$$\begin{cases} \max\limits_{\mathbb{N}} (\lambda^\top . X) \text{ such that } (6) \\ X, X' \in \mathbb{N}^{(J+K+1).|T|} \end{cases} \quad (7)$$

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

A necessary and sufficient condition for K-diagnosability, based on (7), can be succinctly expressed as follows:

Theorem** 1.* (Chouchane et al. (2023)). Consider an LPN under hypotheses ***H0 and ***H1***, and fault class T_f. T_f is K-diagnosable, $K \in \mathbb{N}^*$, **iff** either of the two following conditions holds:
-i- (7) has no solution, or
-ii- (7) admits a solution and $\max(\lambda^\top . X) < K$

Corollary** 1.* (Chouchane et al. (2023)). 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 (7) has no solution,
– $K_{min} = \max(\lambda^\top . X) + 1$, otherwise.

3. K-DIAGNOSABILITY ANALYSIS BASED ON THE RELAXATION OF ILP PROBLEM IN $\mathbb{R}$

Solving ILP problems is computationally expensive, known to be NP-hard with exponential complexity in the number of variables (Garey and Johnson (1982); Von zur Gathen and Sieveking (1978)). To enhance the resolution efficiency, we adopt ILP problem relaxation in this paper, allowing solutions to take real values in $\mathbb{R}$. Moreover, as stated earlier, implementing the technique discussed in Section 2 requires determining a value for parameter J, which could be high depending on the net structure, hence directly impacting the ILP problems to be solved. The technique discussed in the sequel does not involve parameter J.

3.1 Algebraic model on a compact horizon

To establish the ILP formulation for K-diagnosability analysis as in Chouchane et al. (2023), it is necessary to determine an optimal value for J, which poses challenges and may be computationally demanding. In this paper, we propose an algebraic formulation of the K-diagnosability feature that eliminates the need for J, significantly reducing the problem size. Indeed, the vectors from iteration $< 1 >$ to $< J >$ are compressed into one single iteration $< 1 \rightarrow J >$. A sufficient condition for K-diagnosability can then be derived while relaxing the resolution of the formulated optimization problem in $\mathbb{R}$.

A. Modeling the faulty sequence.

The compression of the count vector X corresponding to the faulty sequence σ (defined as in Section (2.4.B)) 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 defined as follows:

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

while $x^{<J+1>}, \dots, x^{<J+K+1>}$ remain unchanged compared to X. It should be recalled that J does not intervene in the developed formulation under relaxation, but is kept in the notation just for the sake of clarity, to be aligned with the notations employed in Section 2.3. In fact, here indexes $< 1 \rightarrow J >, < J+1 > ... < J+K+1 >$ correspond to the 1st, 2nd ...(2+K)th components of X_c, respectively. The same remark applies in the subsequent formulae.

Based on system (1), the established model of the faulty sequence σ under horizon compression while replacing $\sum\limits_{i=1}^{J} x^{<i>}$ by $x^{<1\rightarrow J>}$, is defined as follows:

$$\begin{cases} -W.x^{<1\rightarrow J>} + W^- \cdot x^{<J+1>} \leqslant M_0 \\ -W.x^{<1\rightarrow J>} - W. \sum\limits_{i=J+1}^{j-1} x^{<i>} + W^- \cdot x^{<j>} \leqslant M_0; \\ \forall j \in [\![J+2, J+K+1]\!] \\ 0 \leqslant c.x^{<j>} \leqslant 1 \ ; \ \forall j \in [\![J+1, J+K+1]\!] \\ c_f.x^{<1\rightarrow J>} = 0 \\ c_f.x^{<J+1>} = 1 \\ c.x^{<j>} - c.x^{<j+1>} \geqslant 0 \ ; \forall j \in [\![J+2; J+K]\!] \\ 1 \leqslant \sum\limits_{i=J+2}^{J+K+1} c.x^{<i>} \leqslant K \end{cases} \quad (8)$$

B. Modeling the fault-free sequence.

The compression of the count vector X' of the fault-free sequence σ' (defined as in Section (2.4.B)) 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:

$$x'^{<1\rightarrow J>} = \sum_{i=1}^{J} x'^{<i>} = \begin{pmatrix} x_o'^{<1\rightarrow J>} \\ x_u'^{<1\rightarrow J>} \end{pmatrix} = \begin{pmatrix} \sum\limits_{i=1}^{J} x_o'^{<i>} \\ \sum\limits_{i=1}^{J} x_u'^{<i>} \end{pmatrix} \quad (9)$$

while $x'^{<J+1>}, \ldots, x'^{<J+K+1>}$ remain unchanged. The model of fault-free sequence σ' under horizon compression satisfies the following constraints:

$$\begin{cases} -W_u.x_u^{'<1\to J>} + W_o^-.x_o^{'<1\to J>} - W_u.x_u^{'<J+1>} + \\ \qquad W_o^-.x_o^{'<J+1>} \leqslant M_0 \\ -W_u.x_u^{'<1\to J>} + W_o^-.x_o^{'<1\to J>} - W_u.\sum_{i=J+1}^{j} x_u^{'<i>} - W_o. \\ \sum_{i=J+1}^{j-1} x_o^{'<i>} + W_o^-.x_o^{'<j>} \leqslant M_0; \forall j \in [\![J+2, J+K+1]\!] \\ c_f.x'^{<1\to J>} + \sum_{i=J+1}^{J+K+1} c_f.x'^{<i>} = 0 \\ \wp \cdot {x_o}^{<1\to J>} = \wp \cdot {x_o}'^{<1\to J>} \\ \wp \cdot {x_o}^{<i>} = \wp \cdot {x_o}'^{<i>} \ ; \forall i \in [\![J+1, J+K+1]\!] \end{cases} \tag{10}$$

C. Final model.

According to (8) and (10), if there exists a couple of sequences $(\sigma, \sigma') \in C(\kappa)$ where $1 \leqslant \kappa \leqslant K$ under hypothesis ***H0*** and ***H1***, 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 relation:

$$A_c.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leqslant b_c \tag{11}$$

where A_c and b_c can be easily deduced.

3.2 Main results

Let us consider the following optimization problem:

$$\begin{cases} \max\limits_{\mathbb{N}} (\lambda_c^\top.X_c) \\ A_c.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leqslant b_c;\ X_c, X'_c \in \mathbb{N}^{(2+K).|T|} \end{cases} \tag{12}$$

with $\lambda = \begin{pmatrix} \mathbf{0}_{1\times 2.|T|} & c\ c\ \cdots\ c \end{pmatrix}^\top \in \mathbb{N}^{(2+K).|T|}$ and c is as defined in (1). The relaxation of ILP problem (12) can be defined as follows:

$$\begin{cases} \max\limits_{\mathbb{R}} \lambda_c^\top.X_c \\ A_c.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leqslant b_c;\ X_c, X'_c \geqslant \mathbf{0}; X_c, X'_c \in \mathbb{R}^{(K+2).|T|} \end{cases} \tag{13}$$

The relaxed model (13) neglects the integer nature of the count vectors. At this stage, the objective is to establish a sufficient condition for K-diagnosability based on system (13), and determine a value $K_{relax} \leqslant K$ that ensures K_{relax}-diagnosability. First, let us recall the following lemma that establishes the relation between the cost functions respectively of an ILP problem and its corresponding relaxed problem. It should be noted that for $x \in \mathbb{R}$, $\lfloor x \rfloor$ denotes the integer part of x.

***Lemma** 2.* (Liao and Devadas (1997)).
Let $\{\max\limits_{\mathbb{Z}}(c^\top.x) | A.x \leqslant b\}$ and $\{\max\limits_{\mathbb{R}}(c^\top.x) | A.x \leqslant b\}$ be respectively the cost functions of an ILP problem and its relaxation in $\mathbb{R}$. Therefore, $\max\limits_{\mathbb{R}}(c^\top.x) \geqslant \lfloor \max\limits_{\mathbb{R}}(c^\top.x) \rfloor \geqslant \max\limits_{\mathbb{Z}}(c^\top.x)$.

From Lemma 2 and considering both optimization problems (12) and (13), we can state that:

$$\max_{\mathbb{R}}(\lambda_c^\top.X_c) \geqslant \lfloor \max_{\mathbb{R}}(\lambda_c^\top.X_c) \rfloor \geqslant \max_{\mathbb{N}}(\lambda_c^\top.X_c) \tag{14}$$

Using relation (14), the following sufficient condition for K-diagnosability can be established based on (13).

Theorem** 3.* Consider an LPN that fulfills assumptions ***H0 and ***H1*** and consider some fault class T_f. For a fixed $K \in \mathbb{N}^*$, T_f is K-diagnosable **if** either of the following two conditions is fulfilled:
-i- (13) has no solution, or
-ii- (13) admits a solution in $\mathbb{R}$ and $\max\limits_{\mathbb{R}}(\lambda_c^\top.X_c) < K$

Proof. i- (13) has no solution in $\mathbb{R}$ implies that (12) has no solution in $\mathbb{N}$. Therefore, (7) has no solution either. Thus, according to Theorem 1 and Corollary 1, T_f is K-diagnosable and in particular 1-diagnosable.
ii- If (13) admits a solution and $\max(\lambda_c^\top.X_c) < K$, then according to (14), for $\kappa = \lfloor \max\limits_{\mathbb{R}}(\lambda_c^\top.X_c) \rfloor + 1 \leqslant K$, there does not exist any pair of vectors (X_c, X'_c) satisfying (11). In other terms, for $\kappa = \lfloor \max\limits_{\mathbb{R}}(\lambda_c^\top.X_c) \rfloor + 1 \leqslant K$, there does not exist any pair $(\sigma, \sigma') \in C(\kappa)$ and hence T_f is K_{relax}-diagnosable with $K_{relax} = \lfloor \max\limits_{\mathbb{R}}(\lambda_c^\top.X_c) \rfloor + 1 \leqslant K$. Obviously, T_f is K-diagnosable.

***Corollary** 2.* If the sufficient condition stated in proposition 3 holds, then we can conclude not only that T_f is K-diagnosable but also that it is K_{relax}-diagnosable with:
– $K_{relax} = 1$ if (13) has no solution,
– $K_{relax} = \lfloor \max\limits_{\mathbb{R}}(\lambda^\top.X) \rfloor + 1$ if $\max\limits_{\mathbb{R}}(\lambda^\top.X_c) < K$ in (13).

We can also state that:

$$K_{min} \leqslant K_{relax} \leqslant K \tag{15}$$

***Remark** 3.* The K-diagnosability test, as well as the determination of a potentially lower value $K_{relax} \leqslant K$ (in case K-diagnosability is fulfilled), can be performed in a polynomial time in $2|T|(K+2) \times (K+2).(2|P| + 2|T| + |E| + 3) + 5$. Indeed, some linear programming algorithms of polynomial complexity are available, such as, for instance, the Karmarkar algorithm Karmarkar (1984).

4. EXPERIMENTAL RESULTS

In this section, we conduct experiments to assess theefficiency of the discussed technique. We employ the railway benchmark proposed in Ghazel and Liu (2016), addressing a level crossing system that encompasses n railway tracks (where n is a variable). To experimentally evaluate the developed technique and compare it with the ILP-based approaches for K-diagnosability analysis, defined in Chouchane et al. (2023) and Basile et al. (2012), we implemented a Matlab® code for the approach discussed in the current paper, and used to Matlab code of the techniques in Chouchane et al. (2023) and Basile et al. (2012). The experiments were conducted on a dual-core Intel(R) Xeon(R) CPU with a clock speed of 3.30 GHz each and 32 GB of RAM. We set the value of K to 125 and assessed the K-diagnosability of fault transition t_6 while varying the number of tracks n from 1 to 18, thereby increasing the model size. It should be noted that only the approaches in Chouchane et al. (2023) and Basile et al. (2012) require parameter J. The results are showcased in

n	J	ILP-based approach in Basile et al. (2012)				ILP-based approach in Chouchane et al. (2023)		Relaxation based approach	
		K-diag?	$T(s)$ [1]	K_{min}-diag	$T(s)$	K-diag?/K_{min}	$T(s)$	K-diag?/K_{relax}	$T(s)$
1	3	YES	62	7	3	YES / 7	4	YES / 7	4
2	6	YES	31	13	7	YES / 13	16	YES / 13	6
3	9	YES	59	19	16	YES / 19	105	YES / 19	8
4	12	YES	70	25	36	YES / 25	55	YES / 25	11
5	15	YES	100	31	36	YES / 31	57	YES / 31	16
6	18	YES	108	37	36	YES / 37	107	YES / 37	20
7	21	YES	145	43	320	YES / 43	1399	YES / 43	26
8	24	YES	211	49	559	YES / 49	145	YES / 49	34
9	27	YES	334	55	898	YES / 55	195	YES / 55	46
10	30	YES	224	61	1286	YES / 61	195	YES / 61	71
11	33	YES	325	67	3084	YES / 67	277	YES / 67	91
12	36	YES	352	73	4716	YES / 73	439	YES / 73	106
13	39	YES	109	79	7330	o.m		YES / 79	148
14	42	YES	157	85	10931			YES / 85	276
15	45	o.m		o.t				YES / 91	251
16	48							YES / 97	270
17	51	(out of memory)		(> 2 hours)				YES / 103	272

Table 1. Obtained results for the 3 approaches

Table 1. As it can be seen from the numerical results, the advantages of the relaxation technique presented in the present work are clear from the computed execution times and required memory. Furthermore, it is worth noting that the values obtained for K_{relax} are rigorously identical to the corresponding values of K_{min} across the various analyzed models. It is, however, important to emphasize that this alignment is not ensured in general, given the relationship among K, K_{min}, and K_{relax} for K-diagnosable models, where $K_{min} \leqslant K_{relax} \leqslant K$.

5. CONCLUSION

In this paper, we establish a sufficient condition for K-diagnosability in both bounded and unbounded LPNs. The methodology relies on an algebraic formulation of the problem in the form of a polyhedron constructed within a compact horizon. We employ the technique of relaxation (in $\mathbb{R}$) of an ILP problem for conducting K-diagnosability analysis. To evaluate the performance and efficiency of the introduced methodology, some experiments have been conducted on a railway benchmark, illustrating the advantages of the proposed technique.

In future work, we will focus on the sensor placement problem in connection with the K-diagnosability issue.

REFERENCES

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

Basile, F., De Tommasi, G., and Motta, C. (2023). Assessment of initial-state-opacity in live and bounded labeled petri net systems via optimization techniques. *Automatica*, 152, 110911.

Basile, F., De Tommasi, G., and Sterle, C. (2015). Sensors selection for K-diagnosability of Petri nets via integer linear programming. In *23rd Mediterranean Conference on Control and Automation*, 168–175. IEEE.

Boccia, M., Sforza, A., and Sterle, C. (2020). Simple pattern minimality problems: integer linear programming formulations and covering-based heuristic solving approaches. *INFORMS Journal on Computing*, 32(4), 1049–1060.

Cabasino, M.P., Giua, A., Lafortune, S., and Seatzu, C. (2012). A new approach for diagnosability analysis of Petri nets using verifier nets. *IEEE Transactions on Automatic Control*, 57(12), 3104–3117.

Chouchane, A., Ghazel, M., and Boussif, A. (2023). K-diagnosability analysis of bounded and unbounded petri nets using linear optimization. *Automatica*, 147, 110689.

Garey, M.R. and Johnson, D.S. (1982). Computers and intractability: A guide to the theory of NP-completeness. *SIAM Review*, 24(1), 90–91.

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

Karmarkar, N. (1984). A new polynomial-time algorithm for linear programming. In *Proceedings of the 16th annual ACM symposium on Theory of computing*, 302–311.

Lancia, G. and Serafini, P. (2021). Computational complexity and ilp models for pattern problems in the logical analysis of data. *Algorithms*, 14(8), 235.

Liao, S. and Devadas, S. (1997). Solving covering problems using LPR-based lower bounds. In *Proceedings of the 34th annual Design Automation Conference*, 117–120.

Liu, B., Ghazel, M., and Toguyeni, A. (2017). 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.

Von zur Gathen, J. and Sieveking, M. (1978). A bound on solutions of linear integer equalities and inequalities. *Proceedings of the American Mathematical Society*, 72(1), 155–158.

Zhu, G., Feng, L., Li, Z., and Wu, N. (2021). An efficient fault diagnosis approach based on integer linear programming for labeled petri nets. *IEEE Transactions on Automatic Control*, 66(5), 2393–2398.