K/K_{min} diagnosability analysis in (bounded and unbounded) labeled Petri nets by means of linear algebraic optimization

Mohamed Ghazel

University Gustave Eiffel, Lille Campus
COSYS/ESTAS, F-59650 Villeneuve d'Ascq

CNAM Paris, 30th January 2025

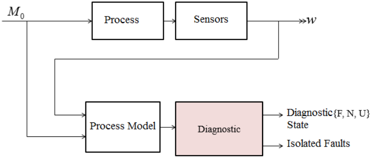
Plan

Introduction

Diagnosability and diagnosis

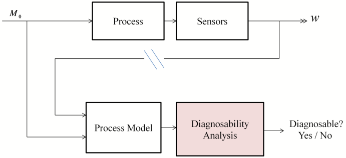
The diagnosis (Hamscher et al., 1992)

The diagnosis consists of:
- detecting the occurrence of faulty behaviors in a system
- identifying/Isolating occurred faults (which faults? in which part of the system?)
Then intervening on the system to repair it.



Diagnosability (Pencolé Y., 2008)

The ability for a system and its monitoring mechanisms to exhibit observations associated with each anticipated faulty situation.



Introduction

System Modeling: Labeled Petri Net

Petri Net (PN)

A PN is a quadruple $\mathcal{N} = (P, T, W^-, W^+)$

- P, T: finite sets consisting respectively of places and transitions;
- $W^- : P \times T \to \mathbb{N}$: pre-incidence matrix;
- $W^+ : P \times T \to \mathbb{N}$: post-incidence matrix;
- $W = W^+ - W^-$: incidence matrix of net $\mathcal{N}$.

Marked Petri net

A marked PN is a pair $< \mathcal{N}, M_0 >$ such that $\mathcal{N}$ is a PN and M_0 is the known initial marking.

Labeled Petri Net (LPN)

An LPN is a marked PN in which we associate a label with each transition in T. Let the labeling function be:

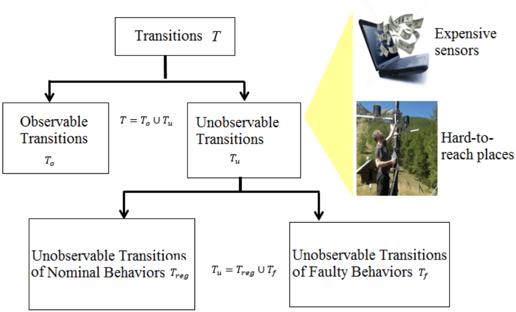
$$\mathcal{L} : T \to E \cup \{\varepsilon\}$$

Introduction

System Modeling: Partial Observability

A model = Normal behavior + Faulty behavior

Fault Modeling



Notations:

- $\mathcal{N}_o = (P, T_o, W_o^-, W_o^+)$ with $W_o^- = W^-_{|T_o}$ and $W_o^+ = W^+_{|T_o}$;
- $\mathcal{N}_u = (P, T_u, W_u^-, W_u^+)$ with $W_u^- = W^-_{|T_u}$ and $W_u^+ = W^+_{|T_u}$;
- $\varepsilon_i \in T_u$ and $t_i \in T_o$

Introduction

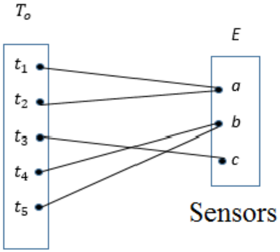
System Modeling: Indiscernible Observable Transitions

Projection Operator

$$\begin{array}{llll} P_l: & T^* & \longrightarrow & E^* \\ & \sigma & \longrightarrow & w = \mathcal{L}(P_o(\sigma)) \end{array}$$

Inverse Projection Operator

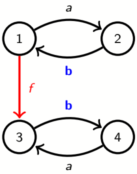
$$\begin{array}{llll} P_l^{-1}: & E^* & \longrightarrow & T^* \\ & w & \longrightarrow & P_l^{-1}(w) = \{\sigma \in T^* \mid P_l(\sigma) = w\} \end{array}$$



$P_l(t_1 t_3 t_4) = acb$
$P_l^{-1}(acb) = \{t_1 t_3 t_4, t_2 t_3 t_4, t_1 t_3 t_5, t_2 t_3 t_5\}$

Introduction

Definition of diagnosability

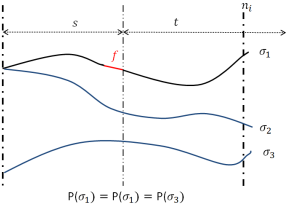


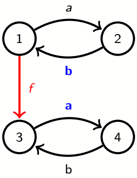
$(ab)^*$ f $(ba)^*$

$f(ba)^*$

$\Rightarrow$ **Failure f is diagnosable**

[h]





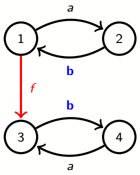
$(ab)^*$ f $(ab)^*$

$(ab)^*$

$\Rightarrow$ **Failure f is not diagnosable**

Introduction

Definition of diagnosability

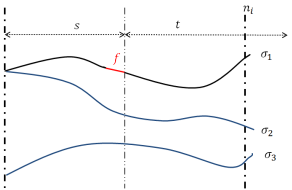


$(ab)^*\ f\ (ba)^*$

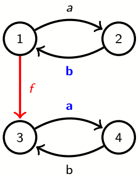
$f(ba)^*$

$\Rightarrow$ **Failure f is diagnosable**

[h]



$P(\sigma_1) = P(\sigma_1) = P(\sigma_3)$



$(ab)^*\ f\ (ab)^*$

$(ab)^*$

$\Rightarrow$ **Failure f is not diagnosable**

Diagnosability Sampath95

A live and prefix-closed language L is said to be diagnosable with respect to a projection function P and a set of faults Σ_f iff:

$$(\exists n \in \mathbb{N})\ [\forall s \in \Psi(\Sigma_f)]\ (\forall t \in L/s)\ [|t| \geq n \Rightarrow D]$$

$$\text{with } D : \omega \in P_L^{-1}[P(s.t)] \Rightarrow \Sigma_f \in \omega.$$

Introduction

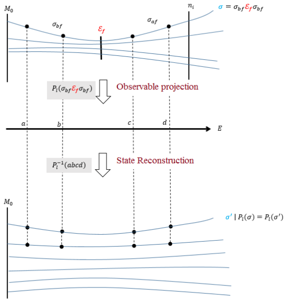
Definition of diagnosability

Diagnosability Sampath95

A live and prefix-closed language L is said to be diagnosable with respect to a projection function P and a set of faults Σ_f iff:

$$(\exists n \in \mathbb{N})\ [\forall s \in \Psi(\Sigma_f)]\ (\forall t \in L/s)\ [|t| \geq n \Rightarrow D]$$

$$\text{with } D : \omega \in P_L^{-1}[P(s.t)] \Rightarrow \Sigma_f \in \omega.$$



Introduction

K-diagnosability

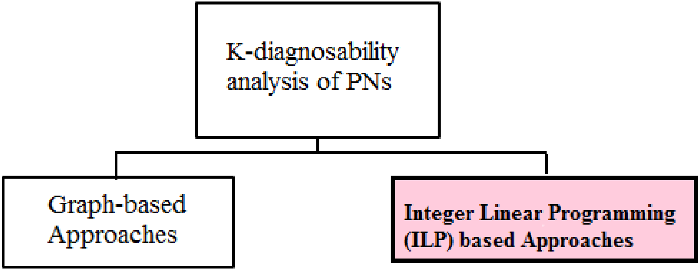
Diagnosability condition of Sampath → There exists a finite time window (without determining it) within which one can determine the occurrence of a fault

⇩

K-Diagnosability condition → One can determine the occurrence of a fault at least after K events following the first occurrence of the fault

Introduction

Motivation: Approaches based on Integer Linear optimization Problems (ILP)



Cabasino et al. 2012

Liu et al. 2017

Basile et al. 2012

Overview

Contributions & Reference works

Contributions

1. Algebraic formulation of diagnosability properties;
2. Usage of linear optimization techniques for analyzing these properties.

Objectifs :

- Advantage relatively to graph-based approaches: avoid building the state space of the Petri net ⇒ tackling combinatorial explosion
- Taking advantages of standard techniques of algebraic resolution (available tools/libraries)

Reference works:

- F. Basile, P. Chiacchio, G. De Tommasi, On K -diagnosability of Petri nets via integer linear programming, Automatica 48, 2012
- 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, 2005.

Plan

K/K_{min}-diagnosability analysis

Aim

- For our first contribution, the problem of K-diagnosability can be reformulated as follows:

> Given an LPN and a fault class T_f, for a given $K \in \mathbb{N}^*$,
> - Is T_f K-diagnosable?
> - And if so, what is the minimum value $K_{min} \leq K$ that ensures K_{min}-diagnosability of T_f?

- **The considered assumptions**

H0. The LPN does not reach a deadlock after firing a fault transition.

H1. The unobservable subnet is acyclic.

H2. A sufficient maximal length J_K of the prefixes that activate fault class T_f for the first time, is known (J_K is inspired from [Basile et al., 2012], but is different from parameter $\mathcal{J}$ in [Basile et al., 2012]).

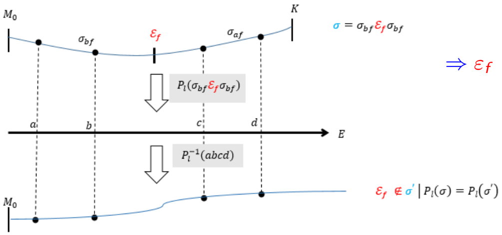
K/K_{min}-diagnosability analysis

General principle of the approach

Reformulation of K-diagnosability

An LPN is K-diagnosable with respect to a fault class T_f if and only if there does not exist any pair (σ, σ') of firing sequences such that:

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



$\Rightarrow$ ε_f is diagnosable if there does not exist such a pair (σ, σ').

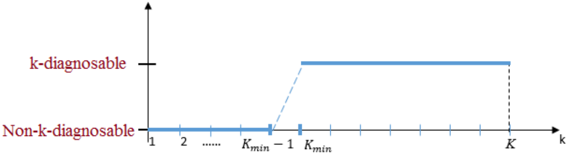
K/K_{min}-diagnosability analysis

General principle of the approach

K_{min}-diagnosability $\longrightarrow$ K-diagnosability

The K_{min}-diagnosability of a fault class T_f is defined as the determination of the minimum value K_{min} that ensures the diagnosability of T_f. K-diagnosability can be inferred as follows:

- If $K_{min} = 1$ then T_f is 1-diagnosable and there is no value $\kappa, 1 \leq \kappa \leq K$ such that T_f is not κ-diagnosable.
- If $2 \leq K_{min} \leq K$ then T_f is K_{min}-diagnosable and $\forall \kappa : 1 \leq \kappa < K_{min}$, T_f is not κ-diagnosable.



K/K_{min}-diagnosability analysis

General principle of the approach

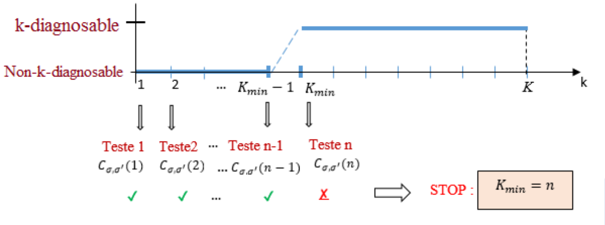
Determination of K_{min} :

Solution 1: Iterative approach

1. We assume that T_f is $K-$diagnosable and that $K \geq K_{min} \geq 2$.
2. We increment the value of κ iteratively and investigate the existence of two feasible firing sequences $\sigma, \sigma' \in T^*$ satisfying the following condition:

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

3. We stop incrementing κ as soon as the condition $C_{\sigma-\sigma'}(\kappa)$ is no longer satisfied $\Longrightarrow K_{min}$ corresponds to the last tested value of κ.



K/K_{min}-diagnosability Analysis

General principle of the approach

Disadvantage of Solution 1

A large number of iterations, especially if K_{min} is high

$\Downarrow$

Solution 2 : *Contribution* 1

Determine K_{min} in a single iteration as a solution of a linear optimization problem (and infer K-diagnosability)

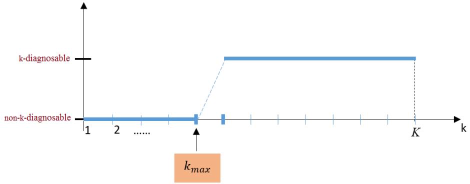
General principle of the approach

Reformulation of K and K_{min}-diagnosability

Determination of K_{min} :

Solution 2: Single ILP-based approach

$$\begin{cases} \kappa_{max} = \max_{\mathbb{N}} \kappa \\ \text{ s.t } \; C_{\sigma-\sigma'}(\kappa) \\ \kappa \in [1...K] \end{cases}$$



Therefore, K_{min} can be deduced as follows:

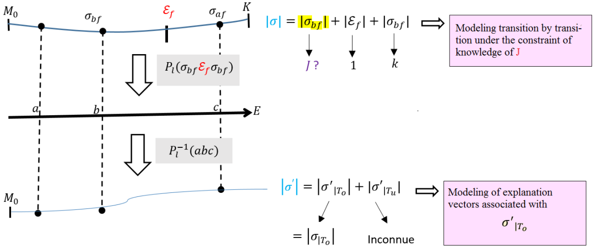
- If $\nexists \kappa$ satisfying $C_{\sigma,\sigma'}(\kappa)$, then $K_{min} = 1$.
- If $1 \leq \kappa_{max} < K$ then $K_{min} = \kappa_{max} + 1$.
- If $\kappa_{max} = K$ then T_f is not K-diagnosable.

$\Rightarrow$ 2 simultaneous outputs:

- The verdict of K-diagnosability;
- The determination of K_{min} if T_f is K-diagnosable.

K/K_{min}-diagnosability analysis

Algebraic Modeling



Proposal: Characterization of J_K

The verification of K-diagnosability of T_f, based on the condition $C_{\sigma,\sigma'}(\kappa)$ with $\kappa \in [1; K]$, can be determined while considering only a subset of prefixes in $\psi(T_f)$ of maximum length J_K defined as follows:

$$J_K = \max_{1 \leq \kappa \leq K} \min_{C_{\sigma,\sigma'}(\kappa)} |\sigma_{bf}|$$

J_K is finite even for unbounded nets $\Rightarrow$ Contribution 1 applies to both **bounded and unbounded LPNs** (cf. our Automatica paper).

Algebraic Modeling

1- Modeling Fault Sequences σ

$$\sigma = \underbrace{t^{<1>}t^{<2>} \ldots t^{<J>}}_{\sigma_{bf}} \; \underset{\downarrow \varepsilon_f}{t^{<J+1>}} \; \underbrace{t^{<J+2>} \ldots t^{<J+K+1>}}_{\sigma_{af}}$$

$\Downarrow$ $x^{<i>} = \pi(t^{<i>})$

$$X = [(x^{<1>})^T (x^{<2>})^T \ldots (x^{<J>})^T \, (x^{<J+1>})^T \, (x^{<J+2>})^T \ldots (x^{<J+K+1>})^T]^T$$

- The Marking Equations
- The Transition Firing Conditions
- At most one transition is fired at each iteration
- The fault is triggered for the first time at iteration $J+1$

$$\Rightarrow \begin{cases} -W.\displaystyle\sum_{i=1}^{j-1} x^{<i>} + W^- \cdot x^{<j>} \leq M_0; \ \forall j \in [2, J+K+1] \\ W^- \cdot x^{<1>} \leq M_0 \\ \displaystyle\sum_{l=1}^{|T|} x_l^{<j>} \leq 1 \ ; \ \forall j \in [1, J+K+1] \\ \displaystyle\sum_{j=1}^{<J>} \sum_{l=1}^{|T|} x_l^{<j>}(T_f) = 0 \\ \displaystyle\sum_{l=1}^{|T|} x_l^{<J>}(T_f) = 1 \end{cases}$$

$$\Longrightarrow \boxed{A_f^{J,K}.X \leq b_f^{J,K}}$$

K/K_{min}-diagnosability analysis

Algebraic Modeling

2- Modeling of fault-free sequences σ' such that $P_l(\sigma') = P_l(\sigma)$

$$\sigma' = \sigma'_u{}^{<1>} t'_o{}^{<1>} \sigma'_u{}^{<2>} t'_o{}^{<2>} \ldots \sigma'_u{}^{<J+K+1>} t'_o{}^{<J+K+1>}$$

$$\Downarrow \quad x'^{<i>} = \begin{pmatrix} \pi(t'_o{}^{<i>}) \\ \pi(\sigma'_u{}^{<i>}) \end{pmatrix}$$

$$X' = [(x'^{<1>})^T (x'^{<2>})^T \ldots (x'^{<J+K+1>})^T]^T$$

$$\left\{ \begin{array}{l} \text{– The Marking Equations} \\ \text{– The Firing Conditions of Observable Transitions} \\ -T_f \notin \sigma' \end{array} \right. \Rightarrow \left\{ \begin{array}{l} -W_u . \sum_{i=1}^{j} x_u{}^{<i>} - W_o . \sum_{i=1}^{j-1} x_o{}^{<i>} + W_o^- . x_o^{<j>} \leq M_0 \ , \ \forall j \in [2, J+K+1] \\ -W_u . x_u^{<1>} + W_o^- . x_o^{<1>} \leq M_0 \\ \sum_{j=1}^{<J+K+1>} \sum_{l=1}^{|T|} x_l'^{<j>}(T_f) = 0 \end{array} \right.$$

$$\Longrightarrow \boxed{A_n^{J,K} . X' \leq b_n^{J,K}}$$

Theorem (Murata, 1989)

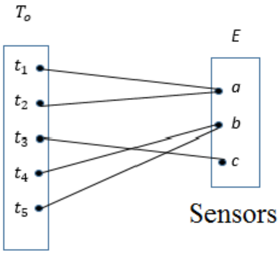
In an acyclic PN, marking M is reachable from M_0 *iff* there exists a non negative integer solution x satisfying $M = M_0 + W.x$.

$\Longrightarrow$ X' solution of $A_n^{J,K} . X' \leq b_n^{J,K}$ is the image of a firable sequence under the assumption of acyclicity of the unobservable subnet

K/K_{min}-diagnosability analysis

Algebraic Modeling

3- Modeling indistinguishability (of observable transitions)



$$\wp \cdot {x_o}^{<i>} = y^{<i>} \quad ; \; \forall i \in [1, J+K+1]$$

$$P_l(\sigma') = P_l(\sigma) \implies \wp \cdot {x_o}^{<i>} = \wp \cdot {x'_o}^{<i>} \implies \boxed{\boldsymbol{D}.X = \boldsymbol{D}.X'}$$

K/K_{min}-diagnosability analysis

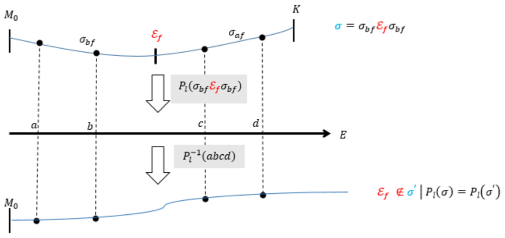
Algebraic Modeling

Final Model

Theorem

The existence of some pair of sequences (σ,σ') that satisfies $C_{\sigma-\sigma'}(\kappa), 1 \leq \kappa \leq K$ (under the assumption H1 of acyclicity) $\Longleftrightarrow$ the existence of two vectors $(X,X') \in \mathbb{N}^{(J+K+1).|T|} \times \mathbb{N}^{(J+K+1).|T|}$ satisfying the following polyhedron:

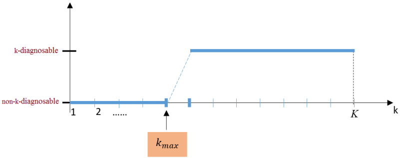
1. $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K},\ A^{J,K} = \begin{pmatrix} A_f^{J,K} & \mathbf{0} \\ \mathbf{0} & A_n^{J,K} \\ \boldsymbol{D} & -\boldsymbol{D} \\ -\boldsymbol{D} & \boldsymbol{D} \end{pmatrix}$ and $b^{J,K} = \begin{pmatrix} b_f^{J,K} \\ b_n^{J,K} \\ \mathbf{0} \\ \mathbf{0} \end{pmatrix}$
2. $\exists\sigma,\ \sigma' \in T^*$ with $\Pi(\sigma) = X, \Pi(\sigma') = X', M_0[\sigma \succ$ and $M_0[\sigma' \succ$



K/K_{min}-diagnosability analysis

Algebraic Modeling

$$
\begin{cases}
\kappa_{max} = \max\limits_{\mathbb{N}} \sum\limits_{i=J+2}^{J+K+1} c.x^{<i>} \\
\text{s.t } \; A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K} \\
\exists \sigma, \; \sigma' \in T^* \; \Pi(\sigma) = X, \Pi(\sigma') = X'
\end{cases}
$$



K/K_{min}-diagnosability analysis

Diagnosability under the assumption of acyclicity of unobservable subnet

Theorem: Necessary and Sufficient Condition for K-Diagnosability

Consider an LPN with an acyclic unobservable subnet and a fault class T_f. Given $K \in \mathbb{N}^*$, T_f is K-diagnosable **iff** at least one of the following two conditions is satisfied:

-i- $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ admits no solution, or

-ii- $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ admits a solution and $\max\limits_{\mathbb{N}}(\lambda^\top.X) < K$.

Corollary: K_{min}-diagnosability

Consider an LPN with an acyclic unobservable subnet. If the fault class T_f is K-diagnosable then T_f is K_{min}-diagnosable with K_{min} is defined as follows:

– If $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ admits no solution, then $K_{min} = 1$.

– If $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ admits a solution and $\max\limits_{\mathbb{N}}(\lambda^\top.X) < K$, then $K_{min} = \max\limits_{\mathbb{N}}(\lambda^\top.X) + 1$.

K/K_{min}-diagnosability analysis - case of cylic unobservable subnet

Diagnosability in the presence of cycles in the unobservable subnet

The considered assumptions

H0. The LPN does not reach a deadlock after firing a fault transition.

~~***H1.*** The unobservable subnet is acyclic.~~

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

Cyclic Case - peculiarity

For an LPN with a cyclic unobservable subnet, the obtained pair (X, X') may be a spurious solution.

K/K_{min}-diagnosability Analysis

Diagnosability in the presence of cycles in the unobservable subnet

Theorem: Sufficient Condition for K-Diagnosability

Consider an LPN that may contain unobservable cycles. Given a fault class T_f and a value $K \in \mathbb{N}^*$, T_f is K-diagnosable **If** at least one of the following two conditions is satisfied

-i- $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ does not admit a solution, or

-ii- $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ admits a solution and $\max\limits_{\mathbb{N}}(\lambda^\top.X) < K$.

Corollary: K_{cyc}-diagnosability

Consider an LPN that may contain unobservable cycles. If the fault class T_f is K-diagnosable, then T_f is K_{cyc}-diagnosable, where K_{cyc} is defined as follows: :

– If $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ does not admit a solution, then $K_{cyc} = K_{min} = 1$.

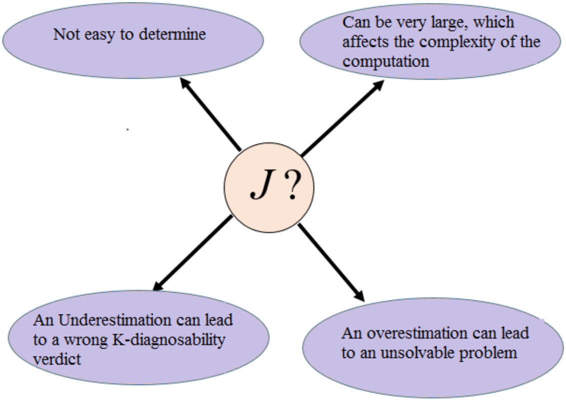
– If $A^{J,K}.\begin{pmatrix} X \\ X' \end{pmatrix} \leq b^{J,K}$ admits a solution and $\max\limits_{\mathbb{N}}(\lambda^\top.X) < K$, then $K_{cyc} = \max\limits_{\mathbb{N}}(\lambda^\top.X) + 1$.

$$K_{cyc} \in [K_{min}\ ,\ K]$$

Plan

K-diagnosability over a compacted horizon

Problem Statement



K-diagnosability over a compacted horizon

Considered assumptions

The considered assumptions:

H0. The LPN does not reach a deadlock after firing a fault transition.

~~***H1.*** The unobservable subnet is acyclic.~~

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

K-diagnosability over a compacted horizon

Solution : The compression of the count vector X corresponding to the fault sequence σ, and the count vector X' corresponding to the indistinguishable fault-free sequence σ' over the interval $[1 \dots J]$. The compressed vectors are defined as follows:

$$X = [\overbrace{(x^{<1>})^T \dots (x^{<J>})^T}^{\text{compression}} (x^{<J+1>})^T \dots (x^{<J+K+1>})^T]^T \quad \Rightarrow \quad X_c = [(x^{<1\to J>})^T (x^{<J+1>})^T \dots (x^{<J+K+1>})^T]^T$$

$$X' = [\overbrace{(x'^{<1>})^T \dots (x'^{<J>})^T}^{\text{compression}} (x'^{<J+1>})^T (x'^{<J+2>})^T \dots (x'^{<J+K+1>})^T]^T \quad \Rightarrow \quad X'_c = [(x'^{<1\to J>})^T (x'^{<J+1>})^T \dots (x^{<J+K+1>})^T]^T$$

with

$$x^{<1\to J>} = \sum_{i=1}^{J} x^{<i>} \;, \quad x'^{<1\to J>} = \sum_{i=1}^{J} x'^{<i>}$$

K-diagnosability over a compacted horizon

Algebraic Modeling

1- Modeling faulty sequences $\sigma \Rightarrow A_f^K.X_c \leq b_f^K$

2- Modeling fault-free sequences σ' $\Rightarrow A_n^K.X_c' \leq b_n^K$

3- Formulating indistinguishability between σ and $\sigma' \Rightarrow D_c.X_c = D_c.X_c'$

$\Downarrow$ **Final model**

Theorem

The existence of sequences σ, σ' satisfying $C_{\sigma-\sigma'}(\kappa), 1 \leq \kappa \leq K$
$\Longrightarrow$ the existence of two vectors $(X_c, X_c') \in \mathbb{N}^{(K+2).|T|} \times \mathbb{N}^{(K+2).|T|}$ satisfying the following polyhedron:

$$A^K.\begin{pmatrix} X_c \\ X_c' \end{pmatrix} \leq b^K$$

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

K-diagnosability over a compacted horizon

K-diagnosability condition

Theorem: Sufficient Condition for K-Diagnosability

Consider an LPN and a fault class T_f. Given $K \in \mathbb{N}^*$, T_f is K-diagnosable **If** one of the following two conditions is satisfied:

-i- $A^K.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leq b^K$ does not admit a solution, or

-ii- $A^K.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leq b^K$ admits a solution and $\max\limits_{\mathbb{N}}(\lambda_c^\top.X_c) < K$.

Corollary: K_c-diagnosability

If the sufficient condition for K-diagnosability is satisfied, then not only can we conclude that T_f is K-diagnosable, but also that it is K_c-diagnosable, where:

a) $K_c = 1$ if $A^K.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leq b^K$ does not admit a solution.

b) $K_c = \max\limits_{\mathbb{N}}(\lambda_c^\top.X_c) + 1$ if $A^K.\begin{pmatrix} X_c \\ X'_c \end{pmatrix} \leq b^K$ admits a solution $< K$.

We can also infer that:

$$\underline{K_{min} \leq K_{cyc} \leq K_c \leq K}$$

Plan

Experiments

Application: Presentation of a railway level crossing benchmark [Ghazel and Liu, WODES'2016]

Benchmark: a level crossing control system with n tracks, with 2 fault classes :

- $\{t_6\}$: early opening of the gate
- $\bigcup\{(t_{i,4}, ig)\}$: train detection failure

Evaluations: We set K to 125 and test the K/K_{min}-diagnosability of $\{t_6\}$ while incrementing the number of tracks n from 1 to 18.

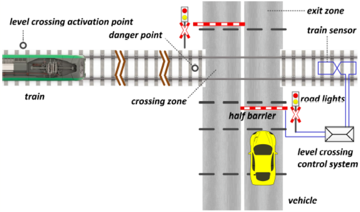


Figure: A level crossing system (single track)

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

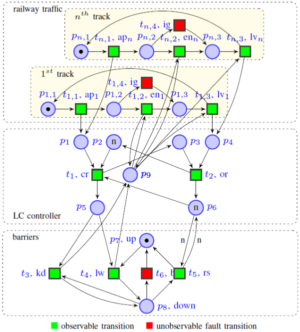
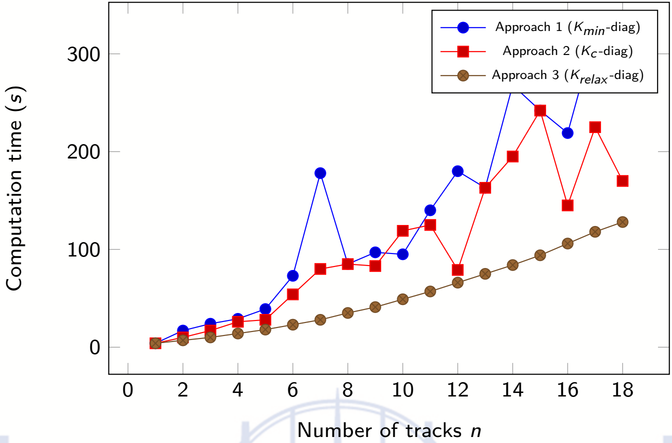


Figure: The PN model of the LC system (multi-track)

Experiments

Obtained Results

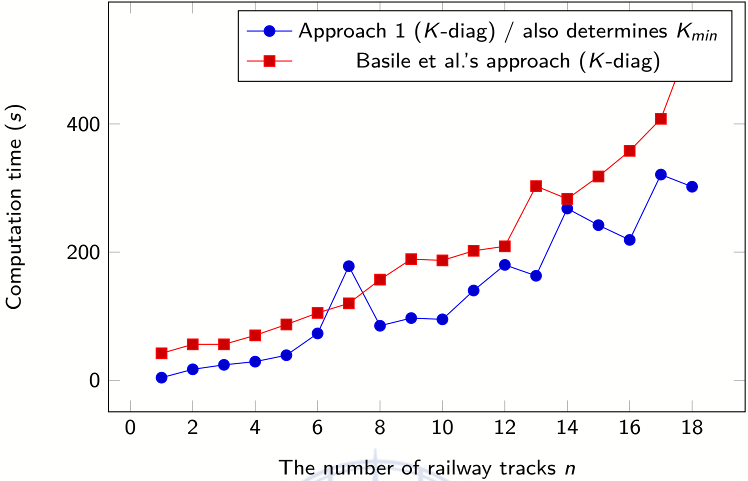
K-diag \ n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
K_{min}	7	13	19	25	31	37	43	49	55	61	67	73	79	85	91	97	103	109
K_c	7	13	19	25	31	37	43	49	55	61	67	73	79	85	91	97	103	109



N.B: Approach 3 is detailed in our WODES'2024 paper.

Experiments

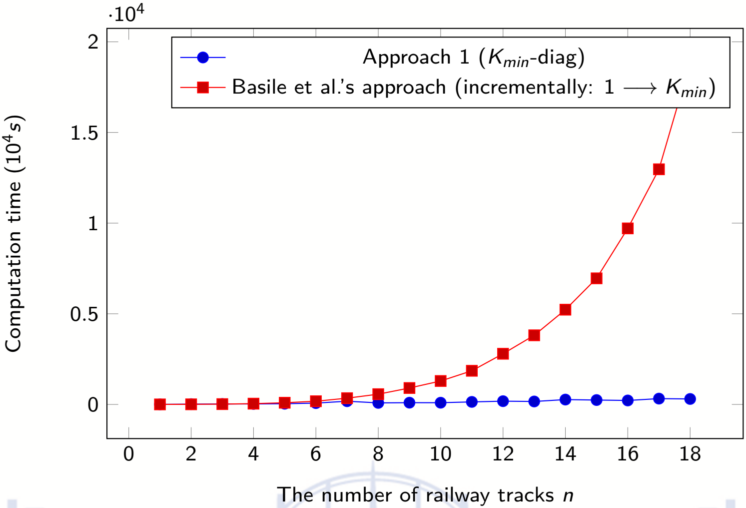
Comparative study



N.B: same value of J considered for both approaches.

Experiments

Comparative study



N.B: same value of J considered for both approaches.

Plan

Conclusion

Contributions: Two algebraic approaches based on ILP formulations for the analysis of K/K_{min}-diagnosability of DES modeled as partially observable LPN, which can be unbounded.

Conclusion

Approach 1 :

- A necessary and sufficient condition for K-diagnosability under the assumption of acyclicity of the unobservable subnet.
- If the established condition is met, the minimal value $K_{min} \leq K$ ensuring K_{min}-diagnosability is calculated simultaneously.
- A sufficient condition for K-diagnosability is established in the case of a cyclic unobservable subnet.
- In case such a condition is fulfilled, a value $K_{cyc} \leq K$ ensuring diagnosability is also determined.

Conclusion

Approach 2 :

- The elimination of parameter J, which is difficult to determine,
- The reduction of the system's size and thus the computational complexity.
- A sufficient condition for K-diagnosability over a compacted horizon is established.
- If the established condition of K-diagnosability is fulfilled, a value $K_c \leq K$ ensuring K_c-diagnosability is also determined.
- Some characterization of J (J_K) was also made (cf. paper).

Thank you for your attention

References:

- *Amira Chouchane, Mohamed Ghazel, Abderraouf Boussif, K-diagnosability analysis of bounded and unbounded Petri nets using linear optimization, Automatica, Vol. 147, 2023.*
- *Amira Chouchane, Mohamed Ghazel, An efficient algorithm for k-diagnosability analysis of bounded and unbounded petri nets, WODES'2024, Rio de Janeiro, 2024.*

Other related work:

- *Amira Chouchane, Mohamed Ghazel, Fault-prognosability, K-step prognosis and K-step predictive diagnosis in partially observed petri nets by means of algebraic techniques, Automatica, Vol. 162, 2024.*