An Efficient Approach for Diagnosability and Diagnosis of DES Based on Labeled Petri Nets - Untimed and Timed Contexts

Baisi Liu

Supervisors

Armand Toguyéni, Mohamed Ghazel

09/04/2014

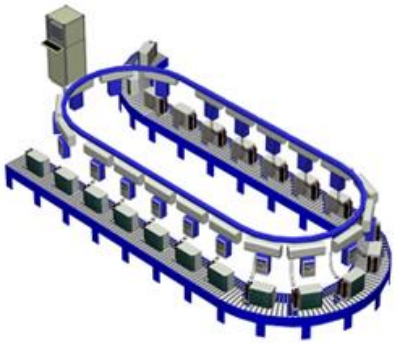
Outline

- Introduction
- Fault diagnosis of DES in untimed context
- Fault diagnosis of DES in timed context
- Conclusions & perspectives

Introduction

- Context
- Problems & objectives

Discrete event system (DES)



DES = Discrete-state Event-driven System

Untimed modeling → (More information / More complex) → Timed modeling

Fault diagnosis

- Partial observation

Constraints for sensor installation

- Technical constraints
- Maintenance
- Availability
- Cost
- …

It is necessary to develop efficient monitoring techniques to overcome the partial observability on system behavior.

Fault diagnosis

- Partial observation
- Diagnosis
  - To deduce, online, the occurrence of an unobservable fault and its type using observable events.
- Diagnosability

Sampath et al., 1995

Definition 1: A prefix-closed and live language L is said to be diagnosable with respect to the projection P and with respect to the partition Π_f on Σ_f if the following holds

$$(\forall i \in \Pi_f)(\exists n_i \in \mathbb{N})[\forall s \in \Psi(\Sigma_{fi})](\forall t \in L/s)$$
$$[||t|| \geq n_i \Rightarrow D]$$

where the diagnosability condition D is

$$\omega \in P_L^{-1}[P(st)] \Rightarrow \Sigma_{fi} \in \omega.$$

Fault diagnosis

- Partial observation
- Diagnosis
  - To deduce, online, the occurrence of an unobservable fault and its type using observable events.
- Diagnosability
  - The ability to diagnose any fault in a finite delay after its occurrence.
- K/Δ-diagnosability
  - The ability to diagnose any fault in a finite delay of K/Δ after its occurrence.
  - To find the minimum K/Δ to ensure diagnosability is of interest.

Objective

- To tackle the combinatorial explosion problem in the diagnoser approach
- To develop a technique to cover all the main problems in both untimed and timed contexts:
  - K-/Δ-/classic diagnosability, K_{min}/Δ_{min}, online diagnosis
- Independency from the way the behavior model has been obtained

Hypotheses

- Input model
  - Labeled Petri net (LPN) for untimed context
  - Labeled time Petri net (LTPN) for timed context
    - Expressiveness
    - compact representation

- We take the classic hypotheses:
  - The models are live and bounded.
  - Absence of feasible cycle of unobservable transitions
  - Faults are permanent.
  - $\Sigma = \Sigma_o \cup \Sigma_u$
  - $\Sigma_f \subseteq \Sigma_u$
  - $\Sigma_f = \cup \Sigma_{Fi}$

Contributions

I. Fault diagnosis of DES in an untimed context using labeled Petri nets (LPNs)

II. Fault diagnosis of DES in a timed context using labeled time Petri nets (LTPNs)

Problems

- Diagnosability: Is the system diagnosable?
- K/Δ-diagnosability: Is the system diagnosable in a given finite delay of K/Δ after the occurrence of fault?
- K_{min}/Δ_{min}: If the system is diagnosble, what is the minimum K/Δ to ensure diagnosability?
- Online diagnosis

I. Fault diagnosis of DES in untimed context

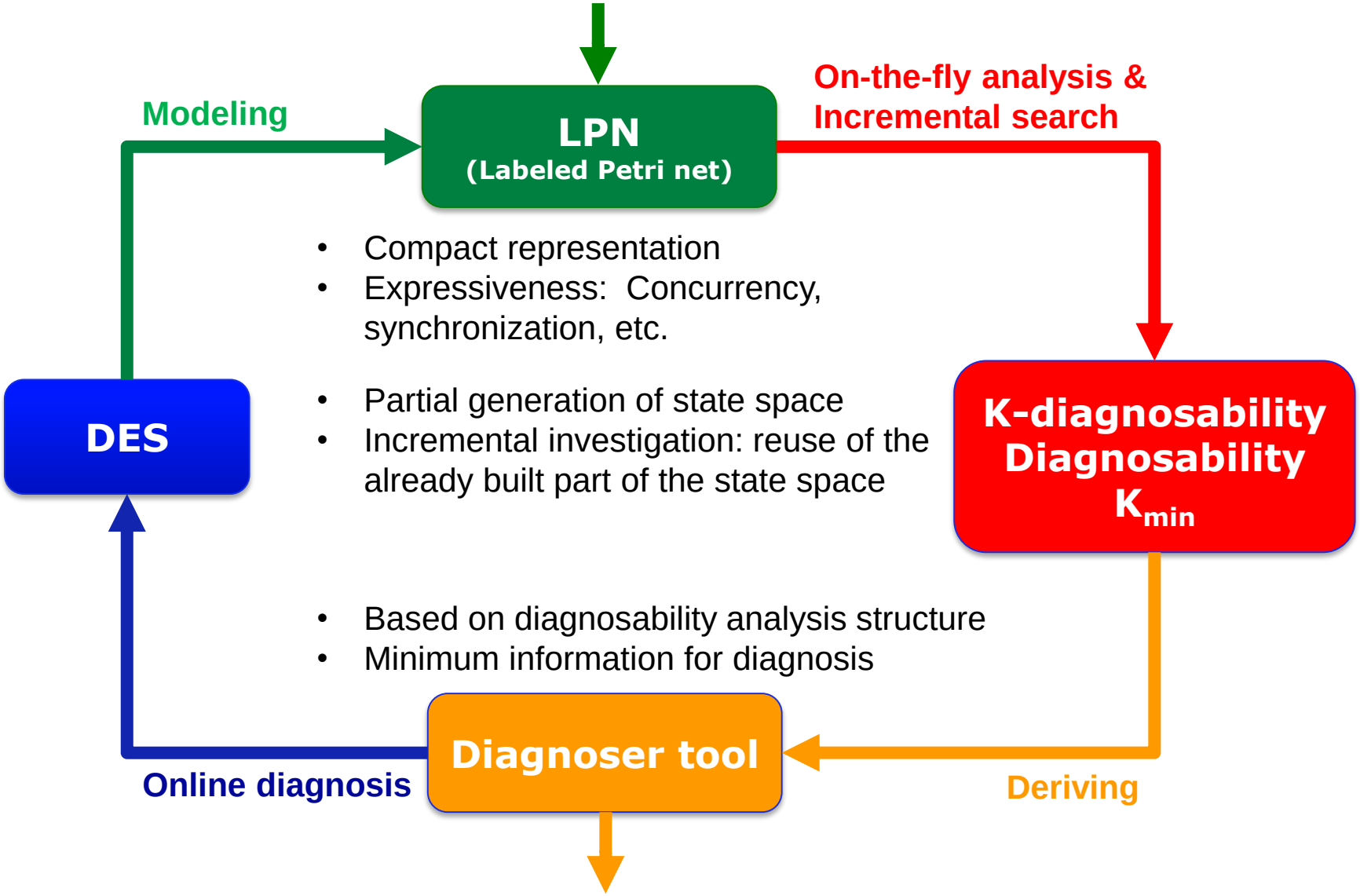
- Motivations
- K-diagnosability
- Diagnosability based on K-diagnosability analysis
- Online diagnosis
- Comparative results

State of the art – untimed diagnosis

Contribution	Model	Diagnosability	K-diagnosability	K_{min}	Technique
Sampath et al.,1995	automata	√			Diagnoser
Jiang et al.,	automata	√			Twin-plant
Yoo et al.	automata	√			Verifier automata
Cabasino et al.	Petri net (PN)	√	√		Verifier PN, BRG
Basile et al.	PN		√		Integer linear programming (ILP)
Our contribution	**PN**	**√**	**√**	**√**	**On-the-fly & Incremental analysis**

- Automata-based approaches suffer from combinatorial explosion problem.
- Existing PN-based approaches focus on certain aspects.
- On-the-fly and incremental technique help to integrate K-/classic dignosability, K_{min} and online diagnosis.

Idea

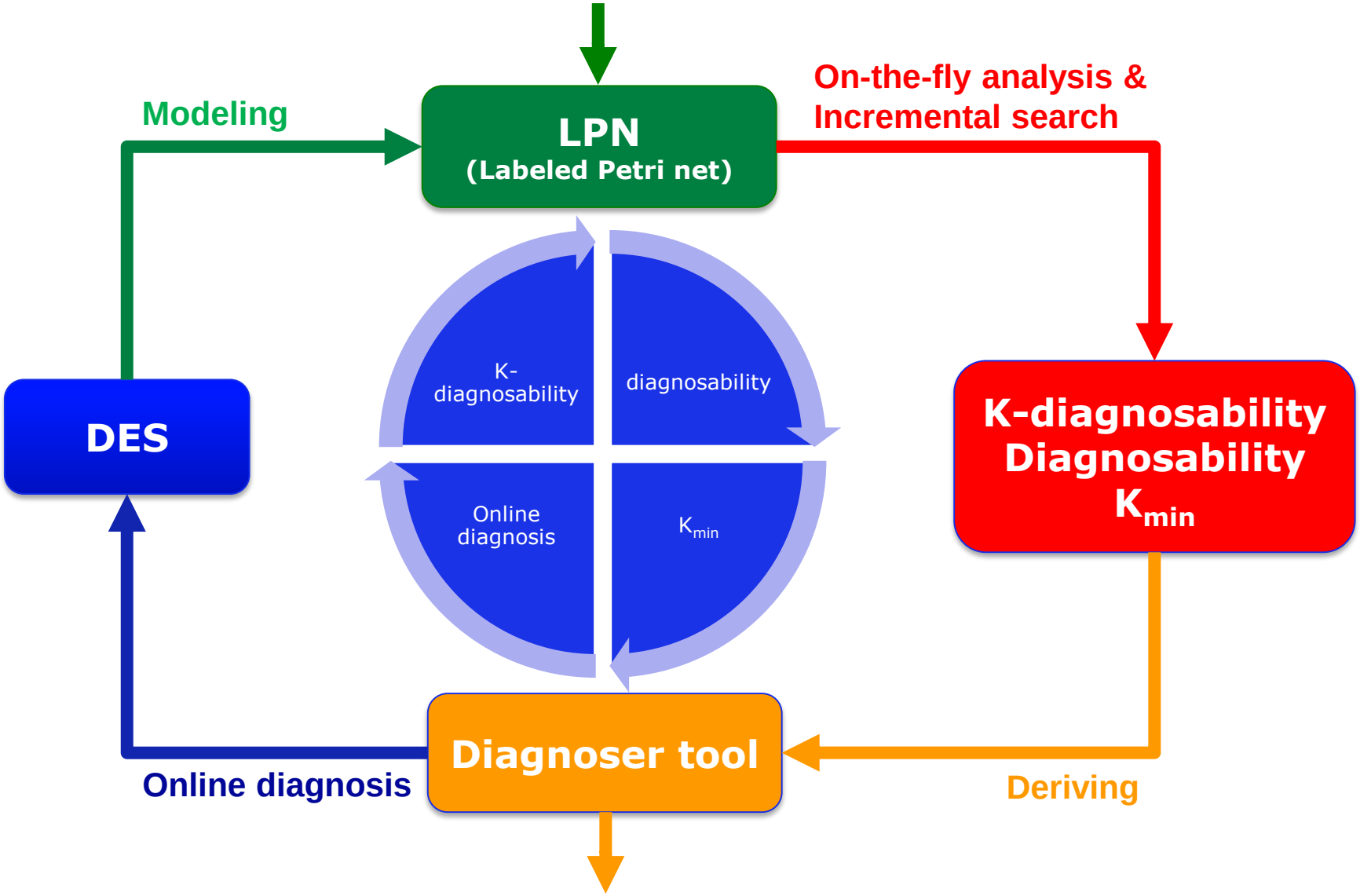


- Compact representation
- Expressiveness: Concurrency, synchronization, etc.

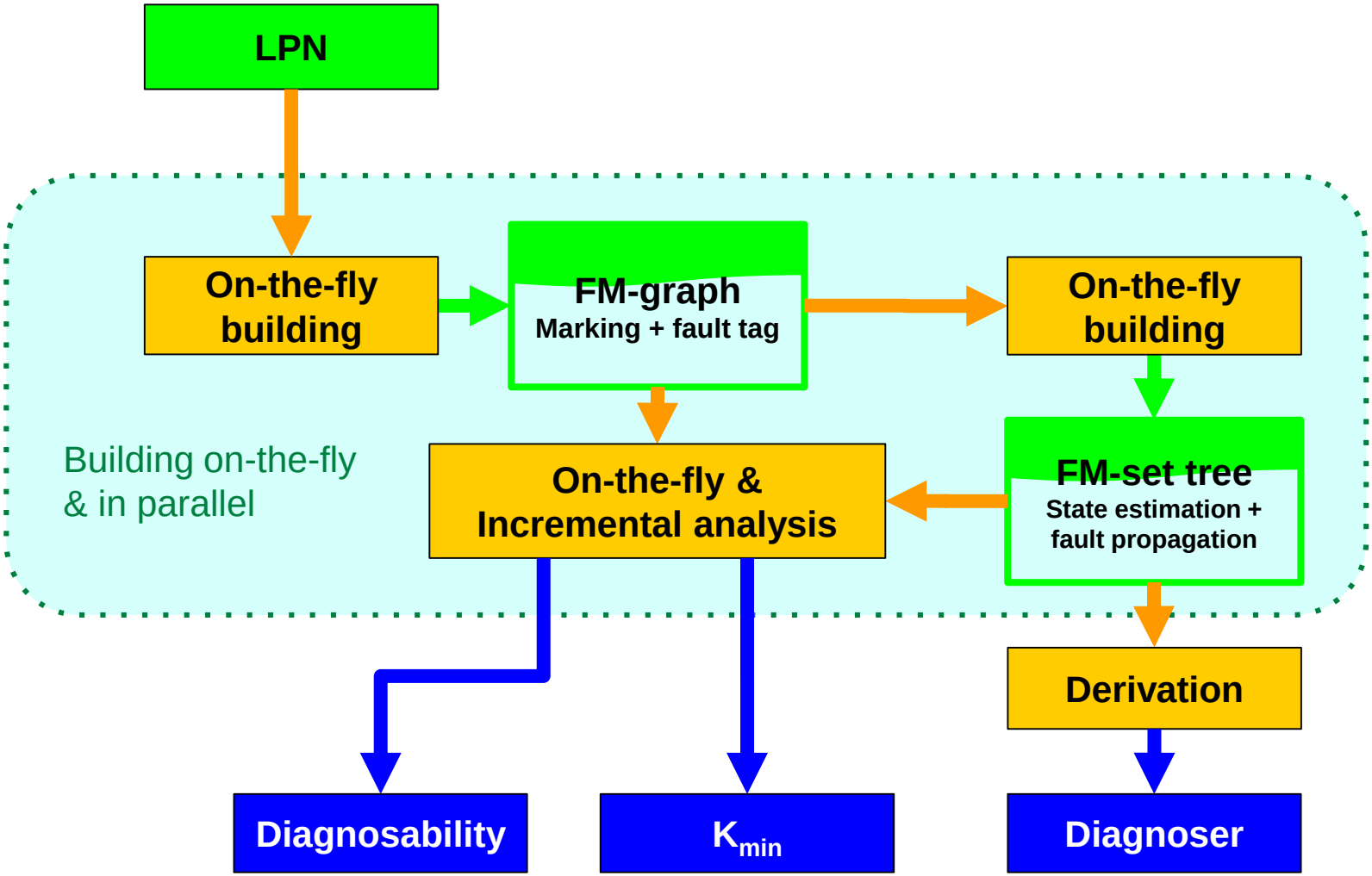
- Partial generation of state space
- Incremental investigation: reuse of the already built part of the state space

- Based on diagnosability analysis structure
- Minimum information for diagnosis

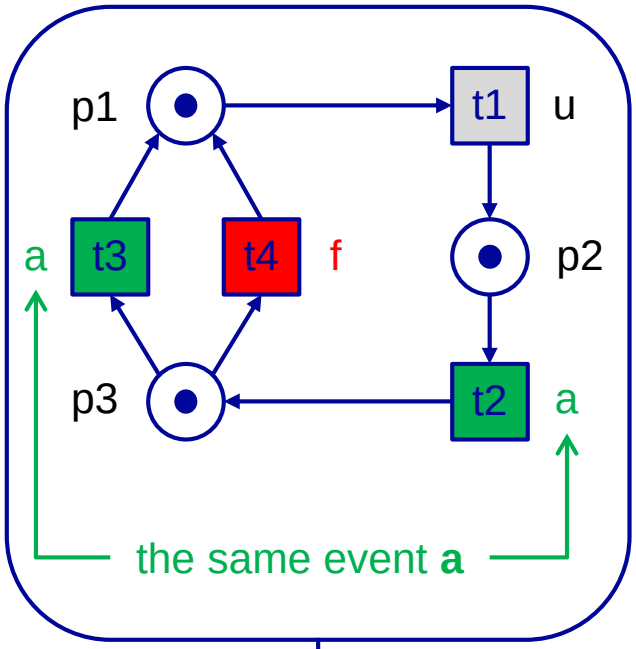
Idea

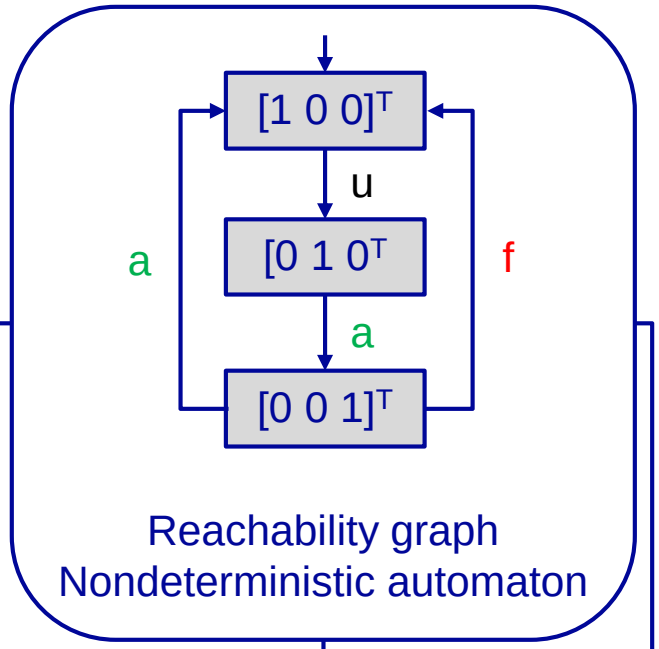

Modeling
LPN
(Labeled Petri net)
On-the-fly analysis &
Incremental search
DES
K-
diagnosability
diagnosability
Online
diagnosis
K_{min}
K-diagnosability
Diagnosability
K_{min}
Diagnoser tool
Online diagnosis
Deriving

On-the-fly & incremental analysis



LPN approach vs. classic approaches



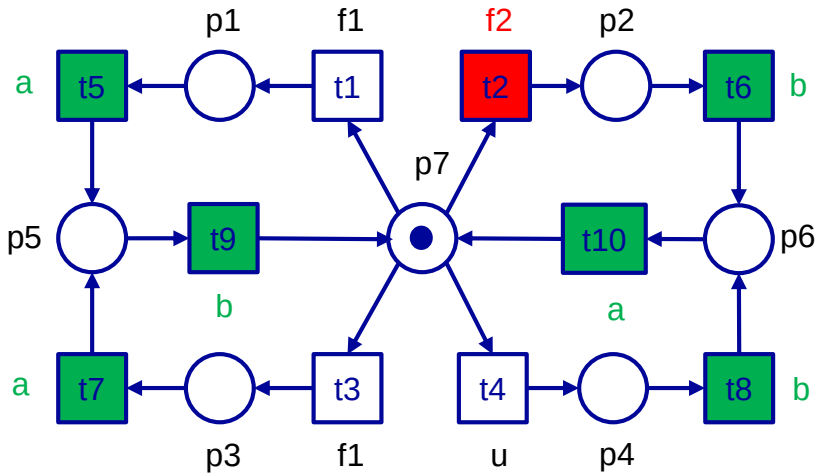


on-the-fly analysis & incremental search

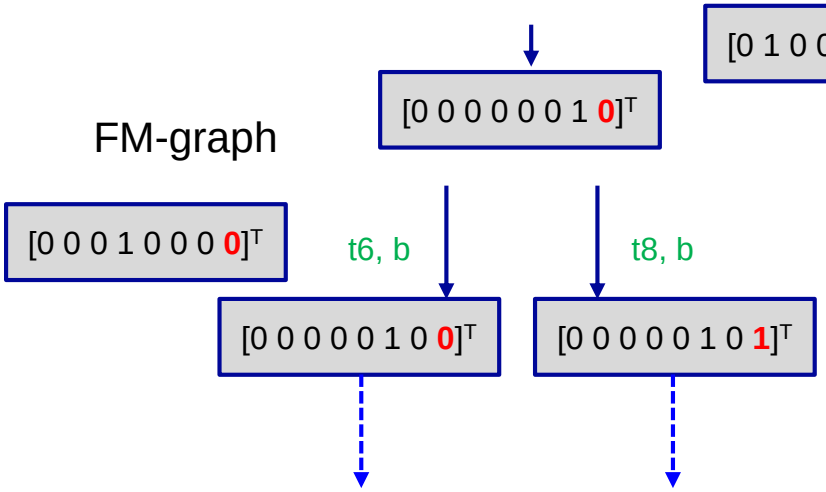
A priori building of the whole state space

diagnosability analysis

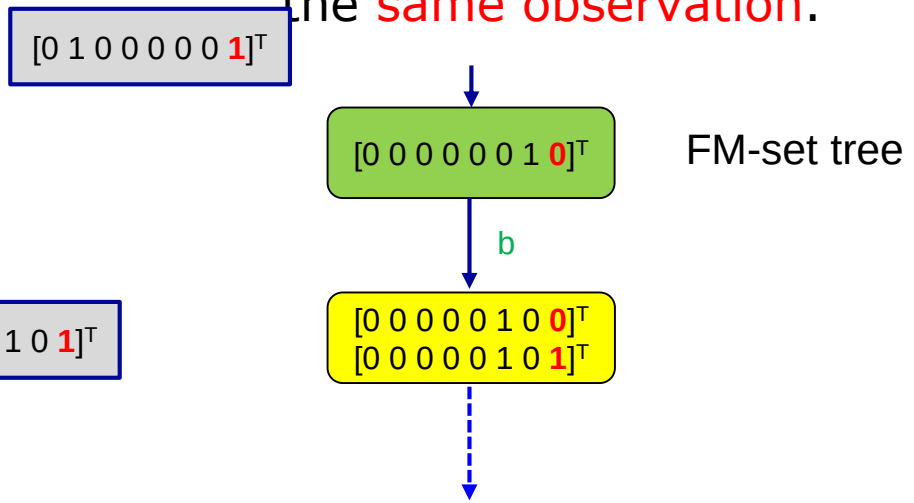
Fault marking (FM) & FM-set



- FM = marking + fault tag
  - 0 = no occurrence of fault
  - 1 = a fault has occurred
- An FM-set is the set of FMs that reachable from FM_0 by the same observation.



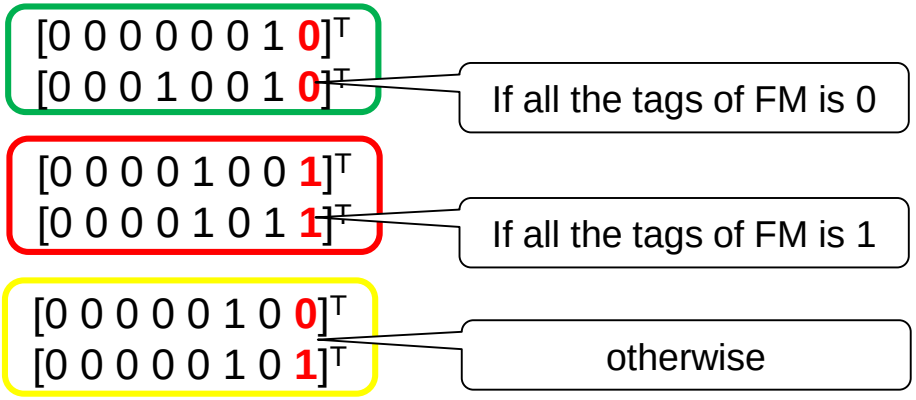
Reachability graph + fault propagation



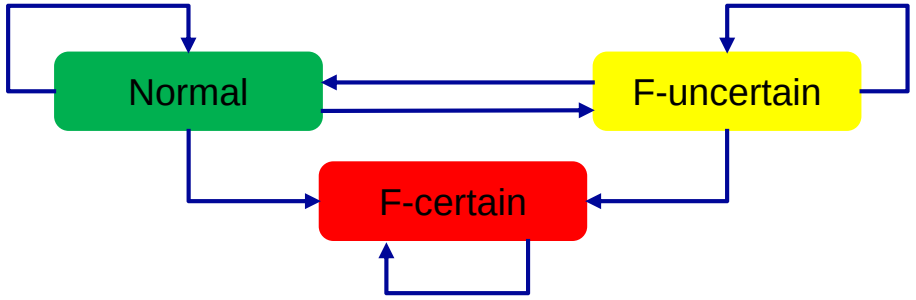
State estimation + fault propagation

Fault tag of FM-set

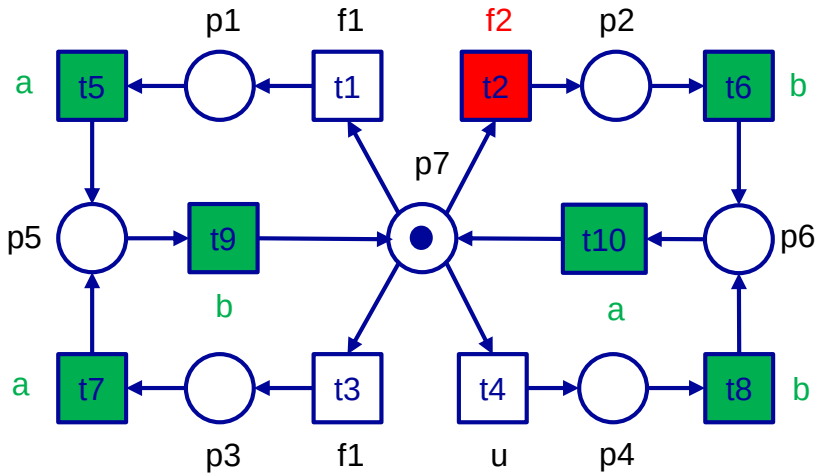
- Fault tag of FM-set to estimate the occurrence of fault
  - [Sampath, Cabasino, …]
  - Normal (N)
  - F-certain (F)
  - F-uncertain (U)

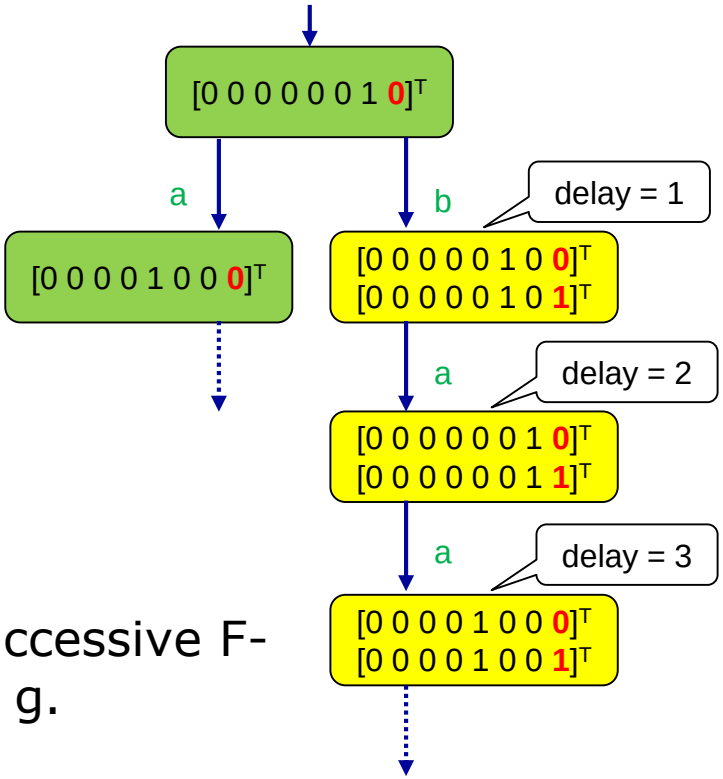


- Fault tag propagation
  - Faults are permanent.



Delay value of FM-set

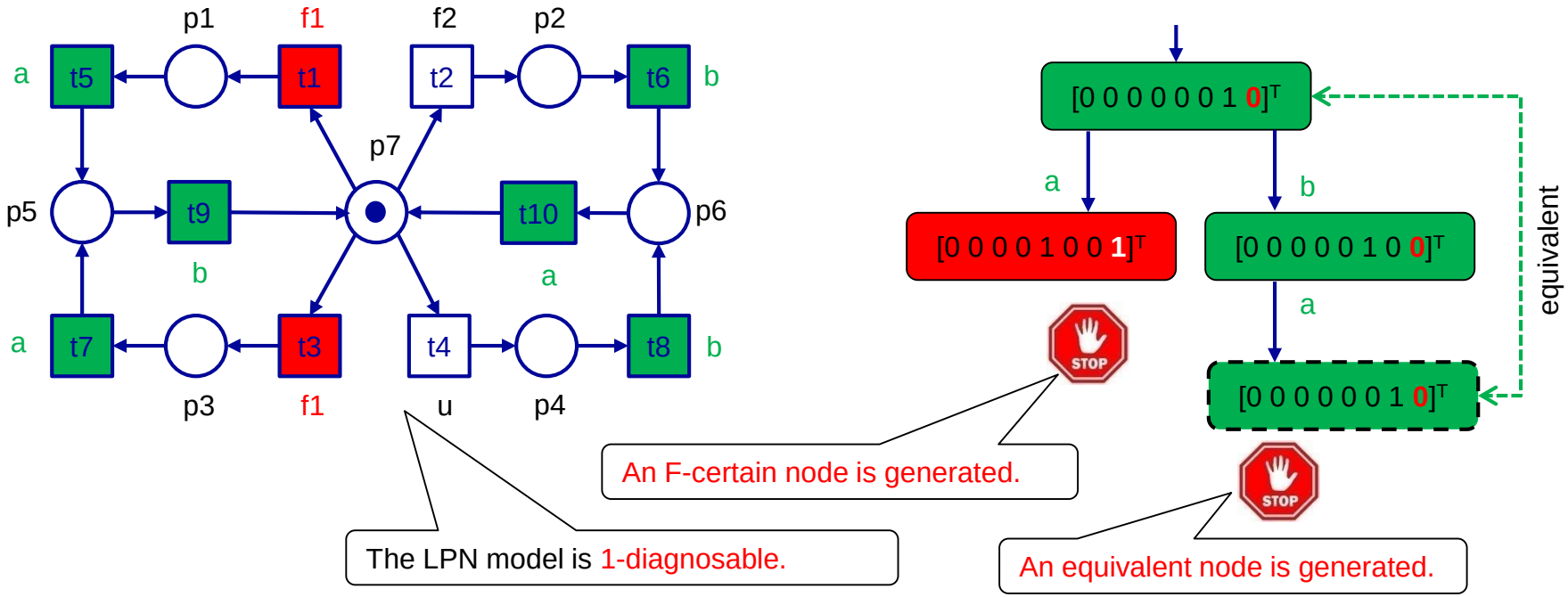




- Delay(g) is the maximum number of successive F-uncertain FM-sets after a fault for node g.

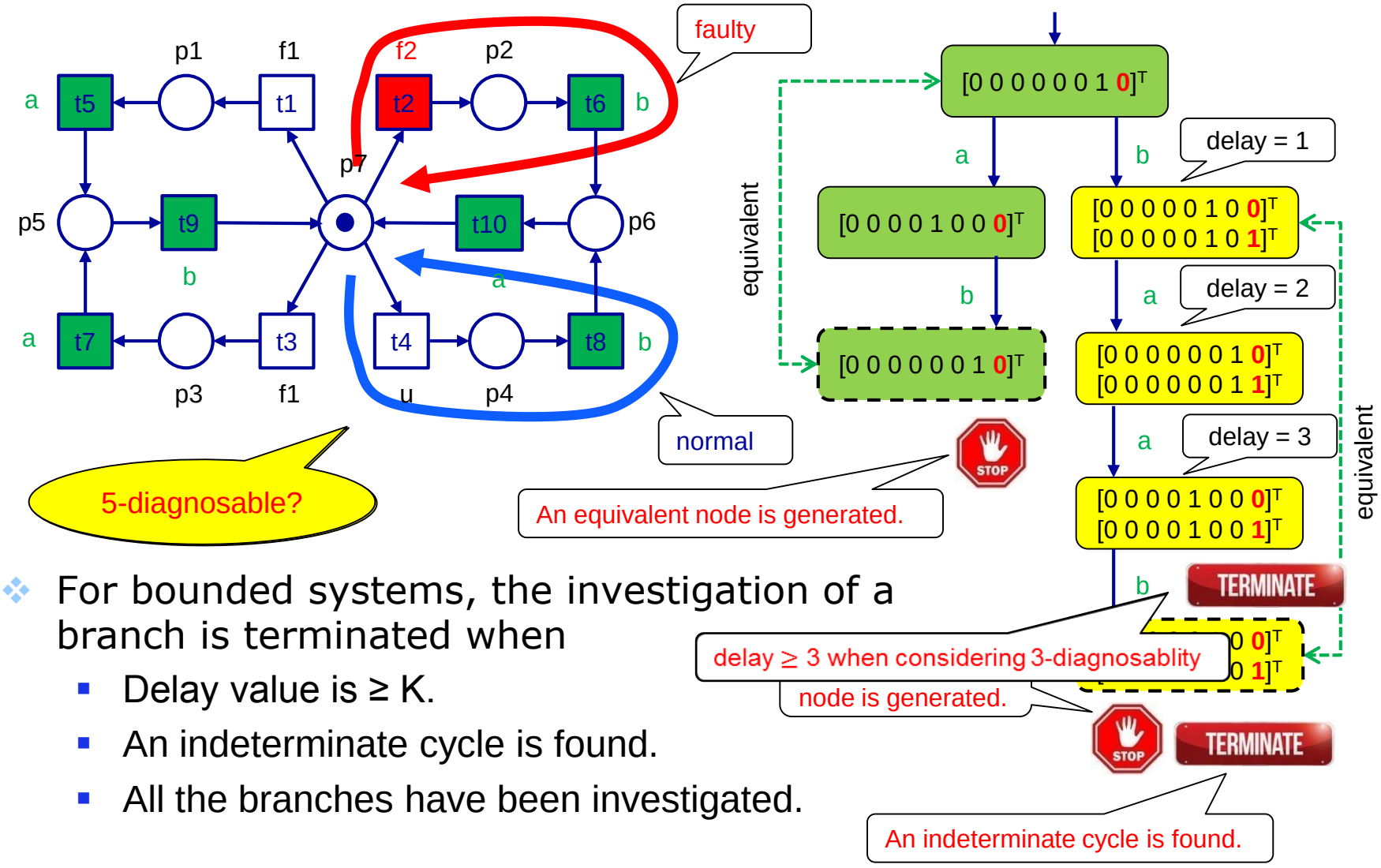
- Delay value is useful when
  - Investigating K-diagnsoability;
  - Finding K_{min} if the system is diagnosable.

On-the-fly checking K-diagnosability



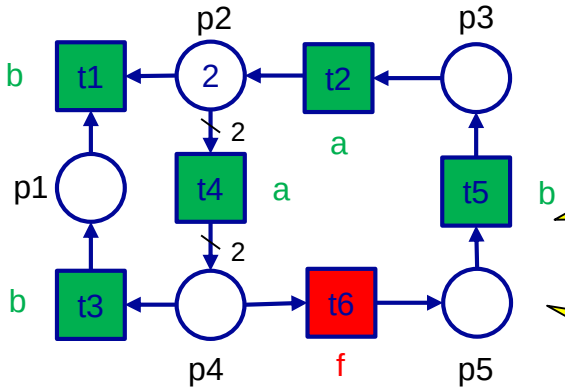
- The FM-set tree is investigated based on depth-first search.
- For bounded LPN, the building of FM-set tree branch can be stopped when
  - An F-certain FM-set is generated;
  - An equivalent FM-set is generated.

On-the-fly checking K-diagnosability



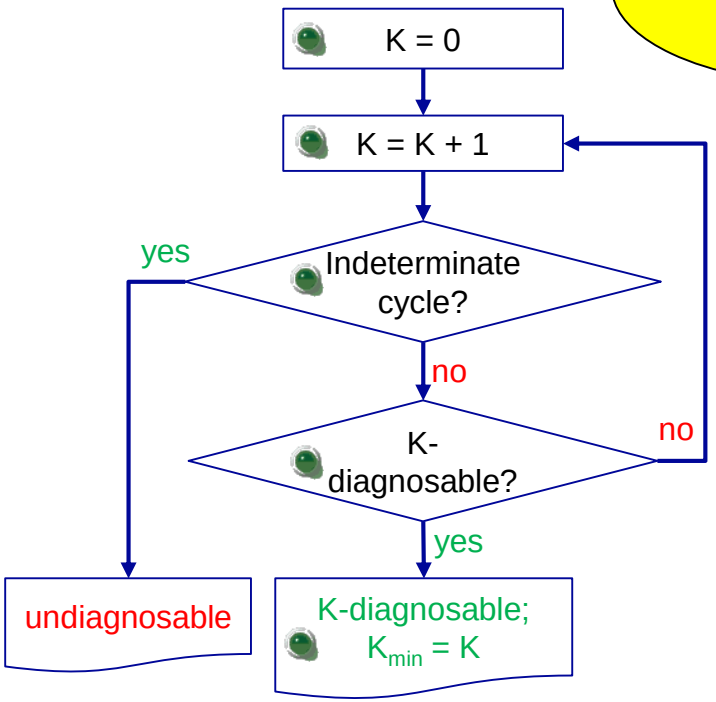
- For bounded systems, the investigation of a branch is terminated when
  - Delay value is ≥ K.
  - An indeterminate cycle is found.
  - All the branches have been investigated.

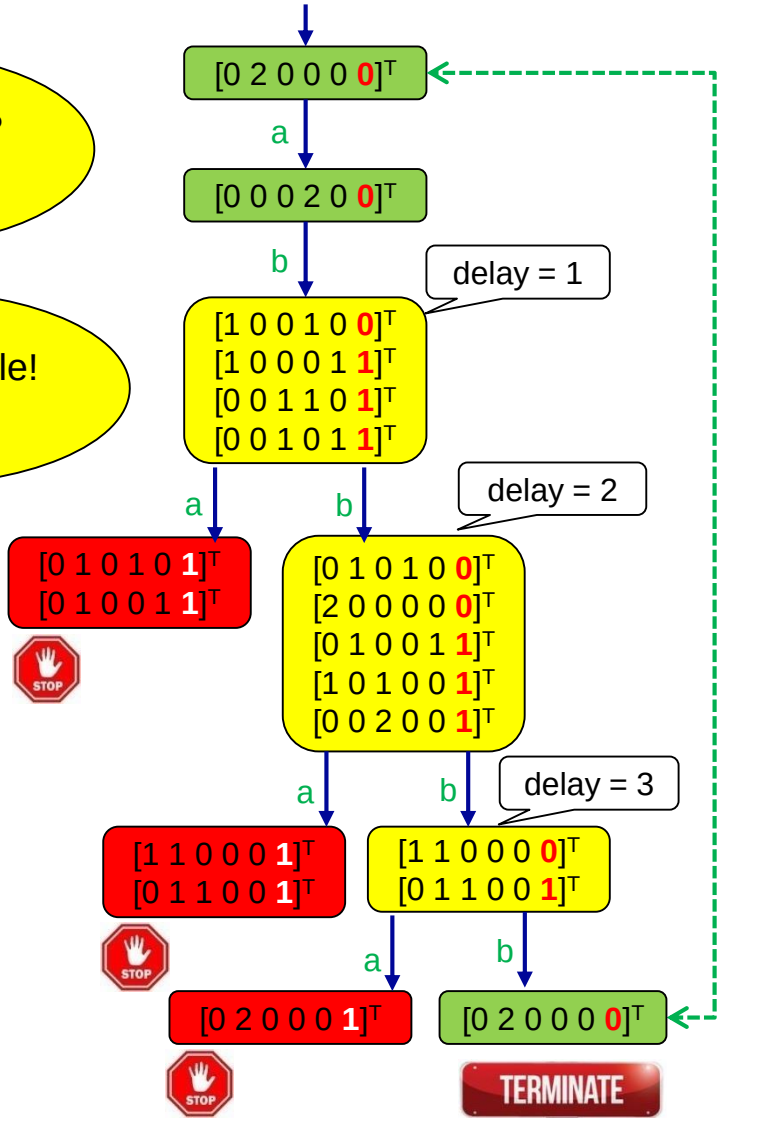
Checking diagnosability & searching K_{min}



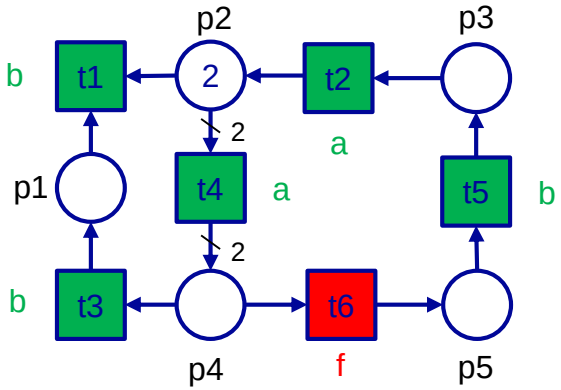
Diagnosable?
K_{min}?

4-Diagnosable!
K_{min} = 4

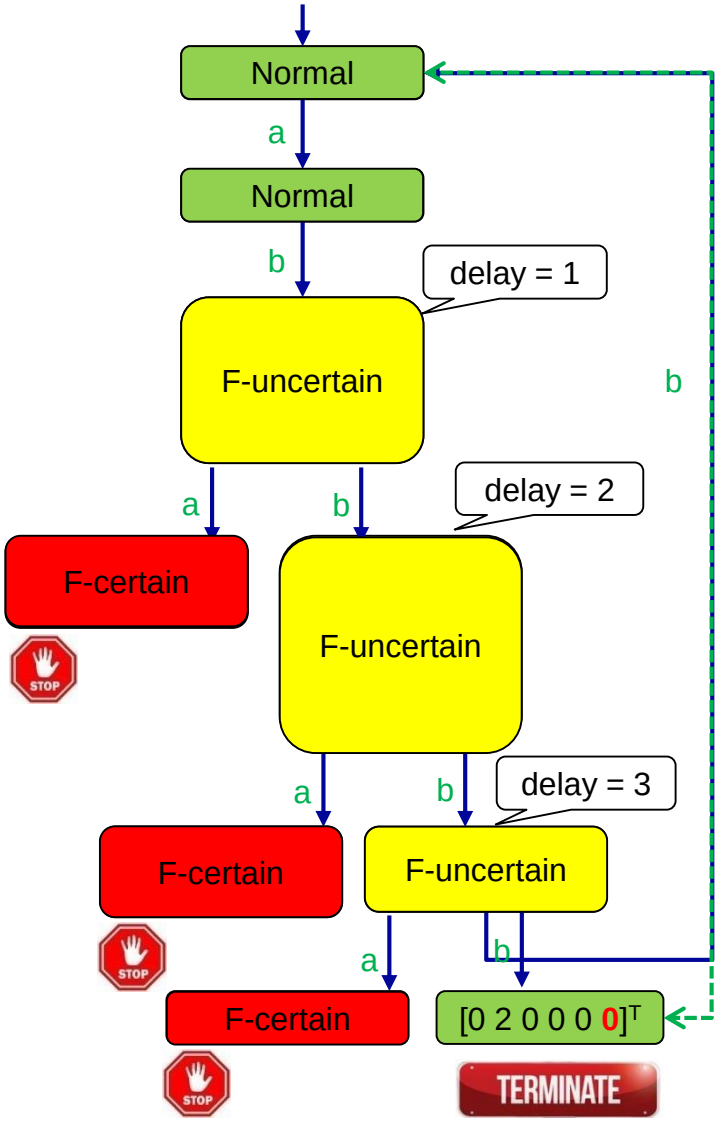




Online diagnosis



- An online diagnoser can be derived from FM-set tree.
- Low memory cost



Algorithms and Complexity

- Recursive algorithm to investigate classic diagnosability based on K-diagnosability analysis
- Complexity: the same level as that of diagnoser approach (in the worst case).
- Efficiency in terms of time and memory: partial generation of the state space.

Algorithm 3 Checking K-diagnosability by on-the-fly building of FM-graph and FM-set tree in parallel

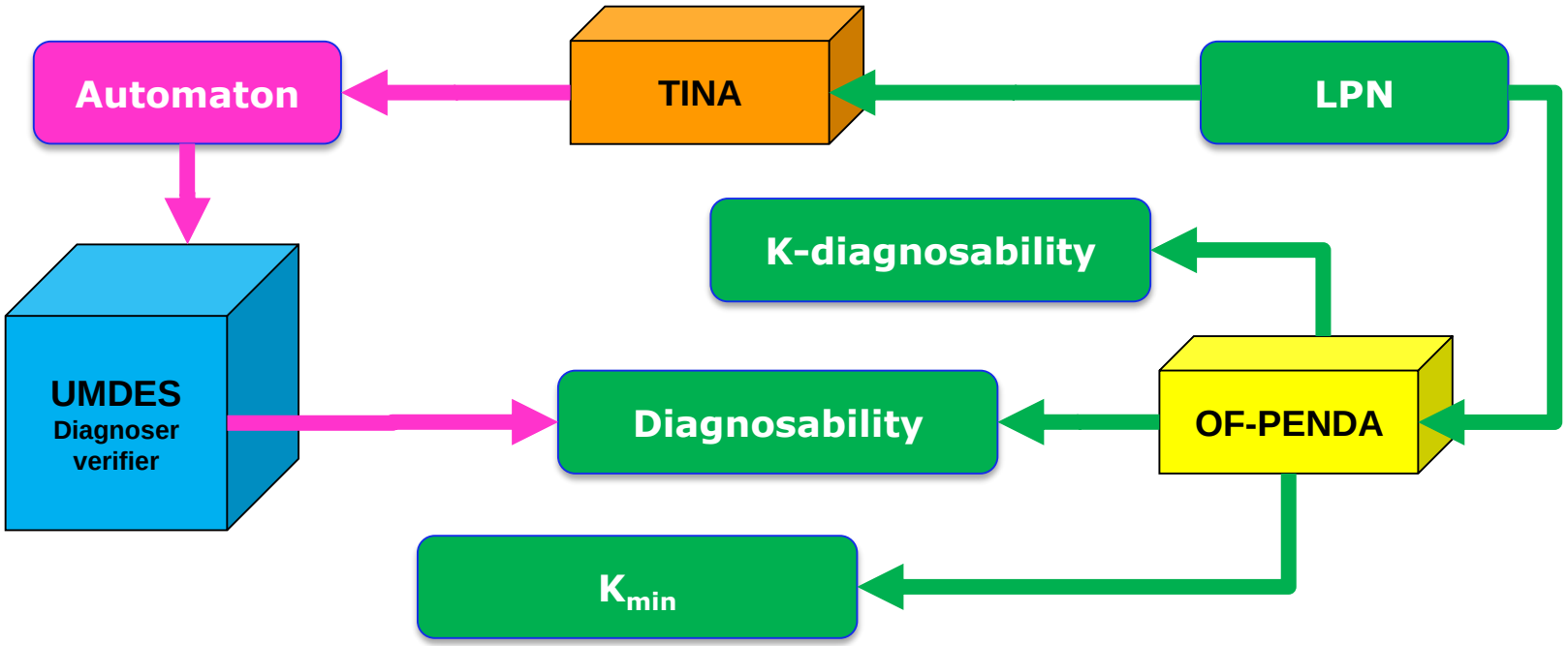
Input: an FM-set x in the FM-set tree $\mathcal{T}$, and K relative to K-diagnosability;
Output: a triple $(\mathcal{T}', y, n)$, where $\mathcal{T}'$ is the FM-set tree generated after running KDiag function, y is the FM-set where the generation of an FM-set tree branch stops and n is the K-diagnosability verdict;
function KDiag$(\mathcal{T}, x, K)$
  for all $e \in \Sigma_o$ **do**
    $x' \leftarrow$ NextFMSet(x, e) ; ▷ x' is the child node of x.
    update $\mathcal{T}$ to $\mathcal{T}'$ by adding x' from x upon e;
    if $(x' \neq \emptyset) \wedge [tag(x') = N]$ **then**
      if $(\forall\, x'' \in \mathcal{X}_u)(x' \neq x'')$ **then** ▷ No equivalent node already exists.
        $\mathcal{X}_u \leftarrow \mathcal{X}_u \cup \{x'\}$;
        $(\mathcal{T}'', y, n) \leftarrow$ KDiag$(\mathcal{T}', x', K)$;
        if $n \neq 1$ **then**
          return $(\mathcal{T}'', y, n)$;
    if $(x' \neq \emptyset) \wedge [tag(x') = U]$ **then**
      if $delay(x') = K$ **then**
        return $(\mathcal{T}', x', 0)$; ▷ 0 denotes that N_L is not K-diagnosable.
          ▷ However, it may be K'-diagnosable for $K' > K$.
      else
        if $(\exists\, x'' \in \mathcal{X}_u)(x'' = x')$ **then**
          if x' is in an indeterminate cycle **then** ▷ Use of function
            ▷ *path_exists* from the library *digraph* [Rushton, 2012].
            return $(\mathcal{T}', x', -1)$; ▷ -1 denotes N_L is not
              ▷ (K-)diagnosable due to the indeterminate cycle.
          else if $delay(x') > delay(x'')$ **then**
            $d \leftarrow delay(x') - delay(x'')$;
            if UpdDelay$(x'', d, K) =$ FALSE **then**
              return $(\mathcal{T}', x', 0)$; ▷ cf. Algorithm 5.
          else
            $\mathcal{X}_u \leftarrow \mathcal{X}_u \cup \{x'\}$;
            $(\mathcal{T}'', y, n) \leftarrow$ KDiag$(\mathcal{T}', x', K-1)$;
            if $n \neq 1$ **then return** $(\mathcal{T}'', y, n)$;
  return $(\mathcal{T}', x', 1)$; ▷ 1 denotes that N_L is K-diagnosable.

Algorithm 6 Checking diagnosability

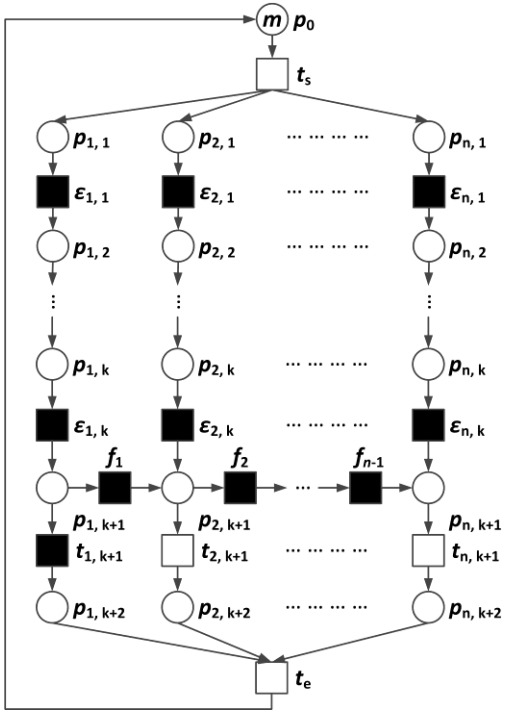
Input: $N_L = (P, T, Pre, Post, M_0, \Sigma, \varphi), T_o, T_f$;
Output: diagnosability verdict and $(\mathcal{T}', K_{min})$ if N_L is diagnosable;
$y \leftarrow x_0$;
$K \leftarrow 0$;
$n \leftarrow 0$;
$\mathcal{T}' \leftarrow$ the initial FM-set tree which contains only x_0;
while $n = 0$ **do** ▷ If N_L is not K-diagnosable.
  $K \leftarrow K + 1$;
  $x \leftarrow y$;
  $\mathcal{T} \leftarrow \mathcal{T}'$;
  $(\mathcal{T}', y, n) \leftarrow$ KDiag$(\mathcal{T}, x, K)$; ▷ cf. Algorithm 3.
if n = 1 **then**
  return $(\mathcal{T}', K)$; ▷ N_L is K_{min}-diagnosable where $K_{min} = K$.
    ▷ $\mathcal{T}'$ is used for building the diagnoser, cf. Section 4.5.
else ▷ If $n = -1$.
  return 0; ▷ N_L is not diagnosable.

OF-PENDA software tool

- OF-PENDA
  - = **O**n-the-**F**ly **PE**tri-**N**et-based **D**iagnosability **A**nalyser
  - Command line software developed using C++
  - Construction of marking graph, FM-graph, FM-set graph



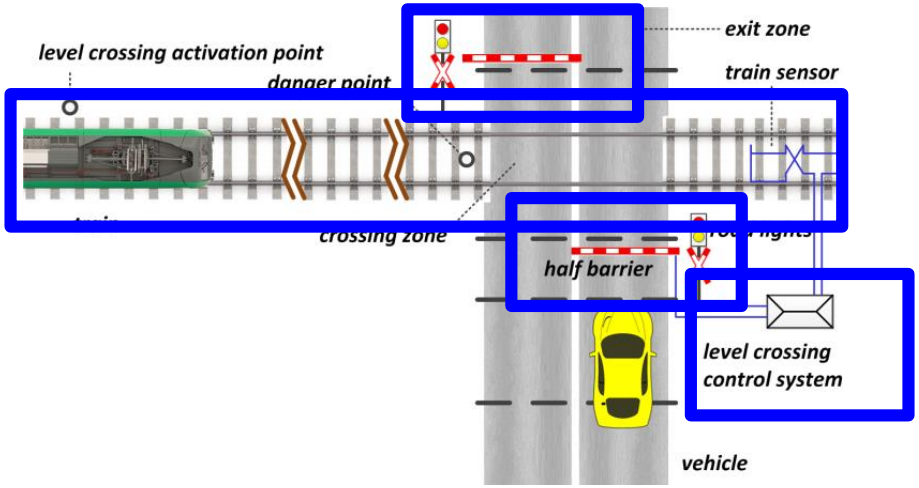
Application to WODES benchmark

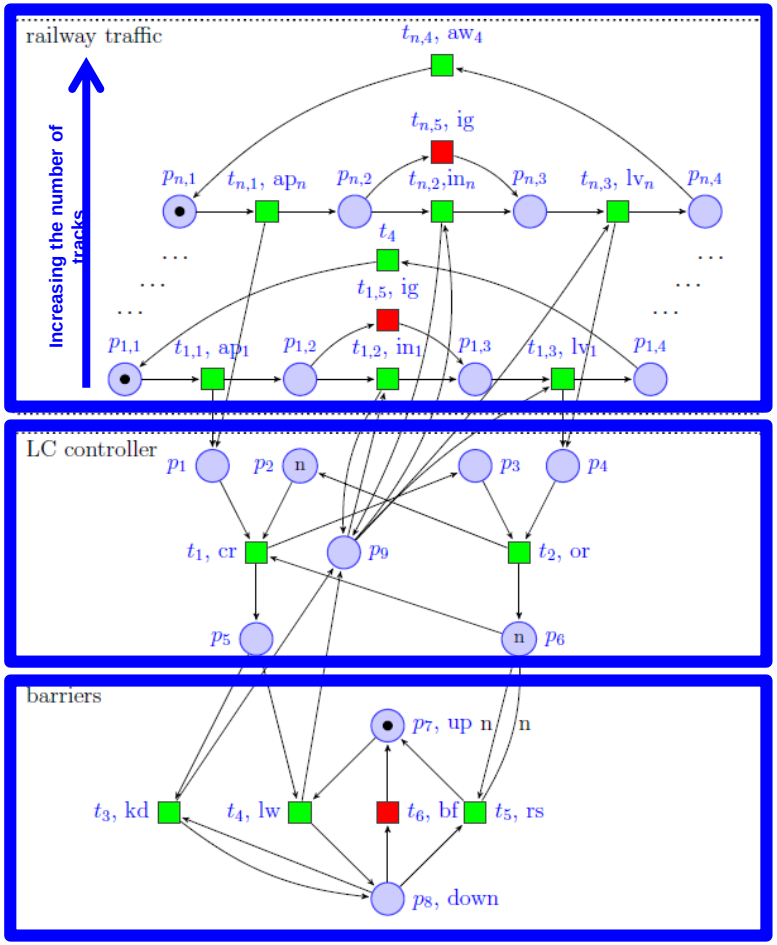


m	n	k	$\|R\|$	$\|N\|$	$\|Diag\|$	$\|\mathcal{X}_v\|$	D_D	D_O	K
1	2	1	15	8	4	3	Yes	Yes	2
1	2	2	24	10	4	3	Yes	Yes	2
1	2	3	35	12	4	3	Yes	Yes	2
1	2	4	48	14	4	3	Yes	Yes	2
1	3	1	80	52	10	6	Yes	Yes	3
1	3	2	159	90	10	6	Yes	Yes	3
1	3	3	274	138	10	6	Yes	Yes	3
1	3	4	431	196	10	6	Yes	Yes	3
1	4	1	495	367	29	17	Yes	Yes	4
1	4	2	1200	822	29	17	Yes	Yes	4
1	4	3	2415	1533	o.t.	17	o.t.	Yes	4
1	4	4	4320	2554	o.t.	17	o.t.	Yes	4
1	5	1	3295	2607	o.t.	66	o.t.	Yes	5
1	5	2	9691	o.t.	o.t.	o.t.	o.t.	o.t.	o.t.
2	2	1	96	68	20	9	No	No	8
2	2	2	237	137	o.t.	9	o.t.	No	8
2	3	1	1484	801	20	12	No	No	11
2	3	2	5949	2746	o.t.	12	o.t.	No	11
2	4	1	28203	8795	o.t.	15	o.t.	No	14
2	4	2	180918	o.t.	o.t.	o.t.	o.t.	o.t.	o.t.
3	2	1	377	290	66	12	No	No	11
3	3	1	12048	5165	o.t.	16	o.t.	No	15
3	4	1	484841	o.t.	o.t.	o.t.	o.t.	o.t.	o.t.

- WODES benchmark [Giua2007]
  - Diagnosability verdict
  - Diagnosable when m = 1
  - Live when n = 1

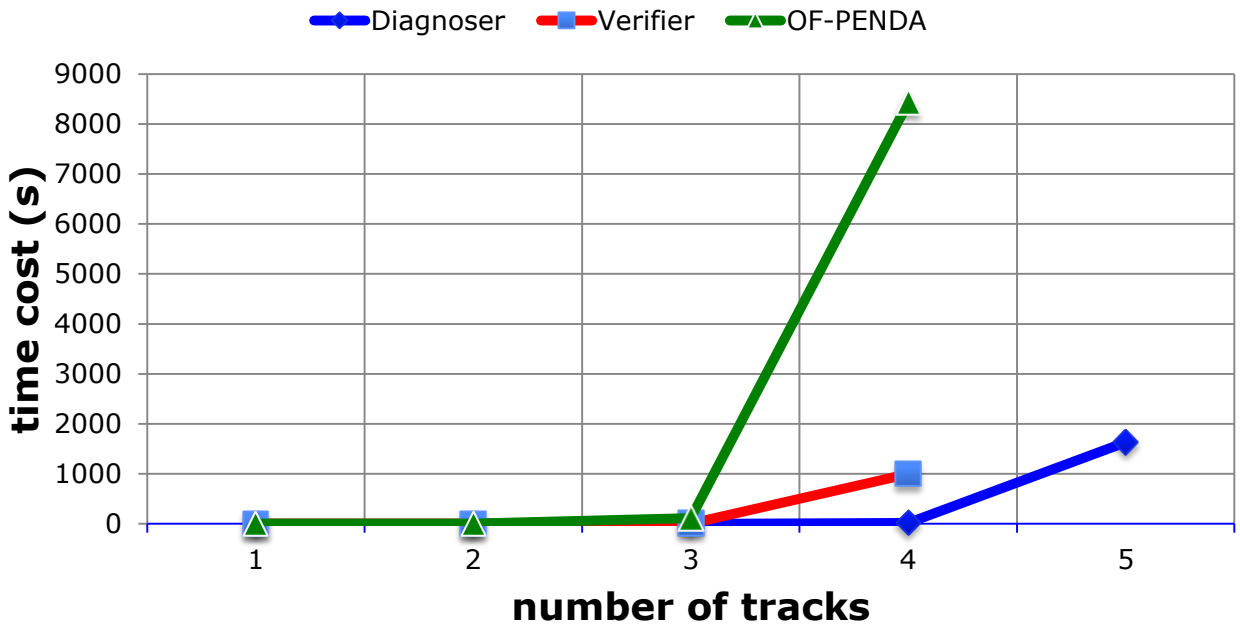
Level crossing (LC) benchmark





- Level crossing benchmark
  - Two types of faults: diagnosable and undiagnosable faults
  - Live and bounded
  - Model size increases with *n*.

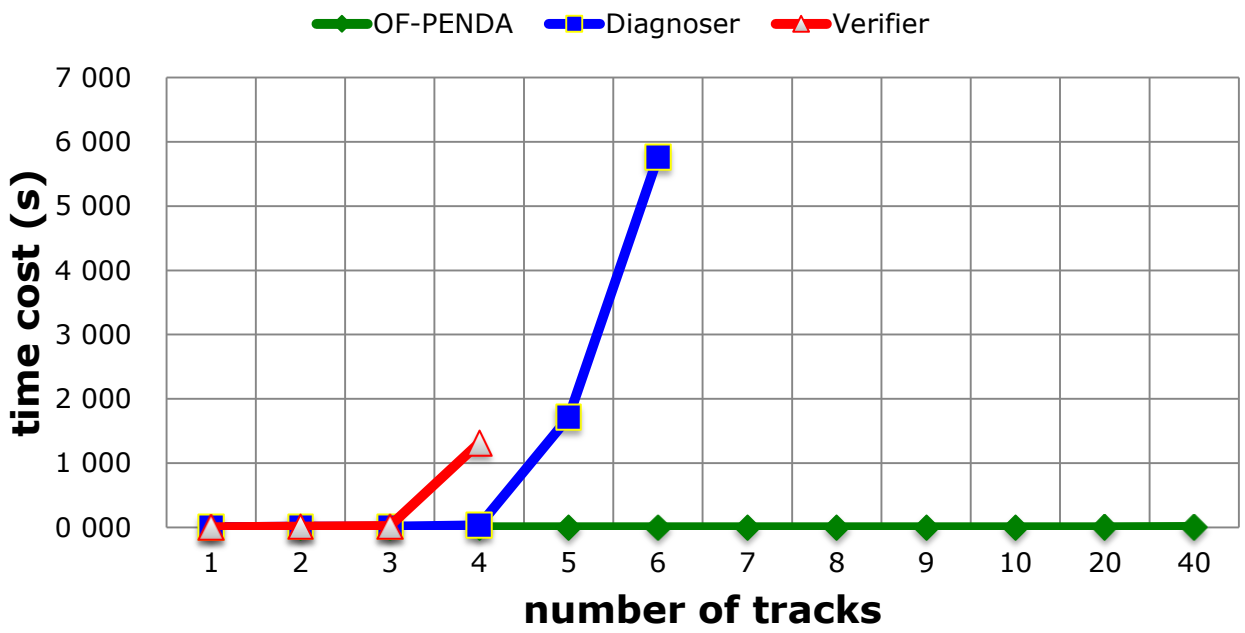
Comparative result on Σ_{F1}



n	Size of .aut file by TINA
1	655b
2	11KB
3	128KB
4	1.2MB
5	9.9MB
6	74.8MB
7	518.6MB
8	>16GB

- Σ_{F1} is diagnosable

Comparative result on Σ_{F2}



- Σ_{F2} is undiagnosable

II. Fault diagnosis of DES in timed context

- Time splitting technique
- Diagnosability analysis
- Online diagnosis

State of the art – timed diagnosis

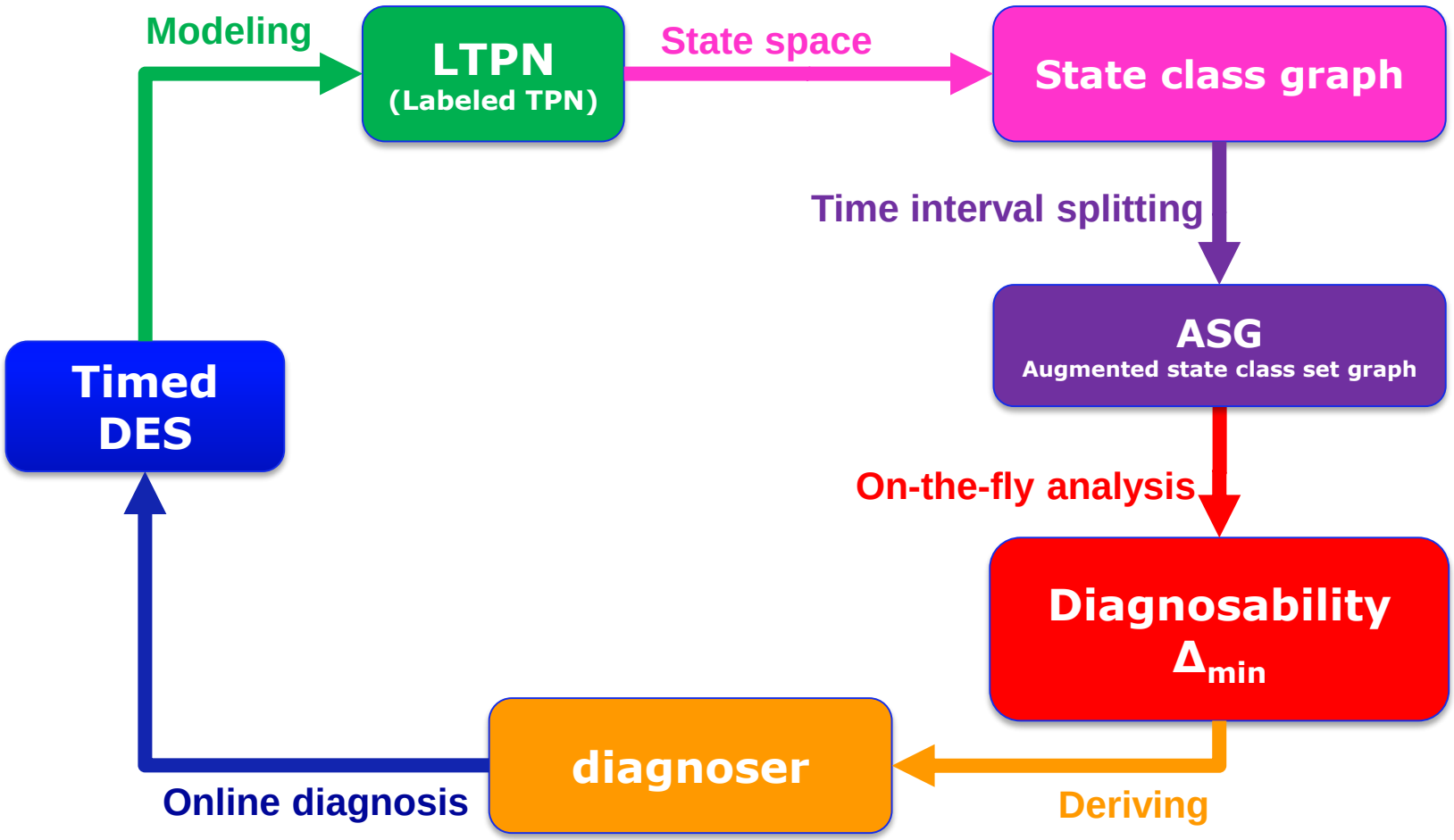
Authors	TA	TPN/LTPN	Diagnosis	Diagnosability	Δ-diagnosability
Tripakis et al.	√		√	√	√
Ghazel et al.		√	√		
Boel et al.		√	√		
Our contribution		**√**	**√**	**√**	**√**

- Timed automata (TA) based approach
  - A priori building of the state space
  - Combinatorial explosion
- Time Petri net based approach
  - Expressiveness
  - Overcome combinatorial explosion
- Our contribution is the **first** to discuss diagnosability using TPN.

Objectives

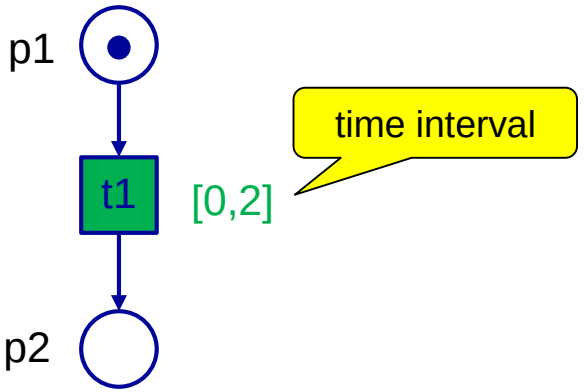
- Objective
  - Overcome the combinatorial explosion problem
- Problems
  - Is it possible to analyze diagnosability in timed context using untimed analysis techniques?
    - Time interval splitting technique for LTPN
  - When is a timed DES diagnosble?
    - Necessary and sufficient conditions for diagnosability of LTPN
  - What is the minimum Δ to ensure diagnosability?
    - On-the-fly analysis of diagnosability

Solution

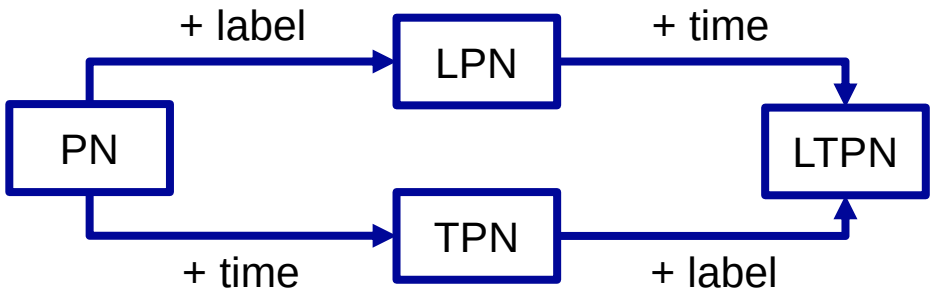

Modeling
LTPN
(Labeled TPN)
State space
State class graph
Time interval splitting
ASG
Augmented state class set graph
On-the-fly analysis
Diagnosability
Δ_{min}
Deriving
diagnoser
Online diagnosis
Timed
DES

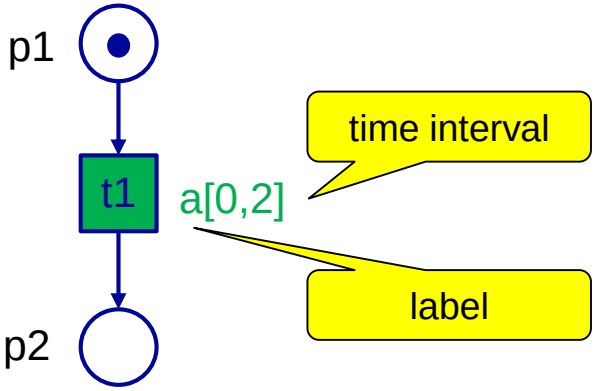
Time Petri net (TPN) & labeled TPN (LTPN)

- TPN
  - Transition firing: immediate
  - Firing date belongs to time interval
  - Strong semantic



- LTPN
  - The same label can assign to different transitions
  - Nondeterministic structure

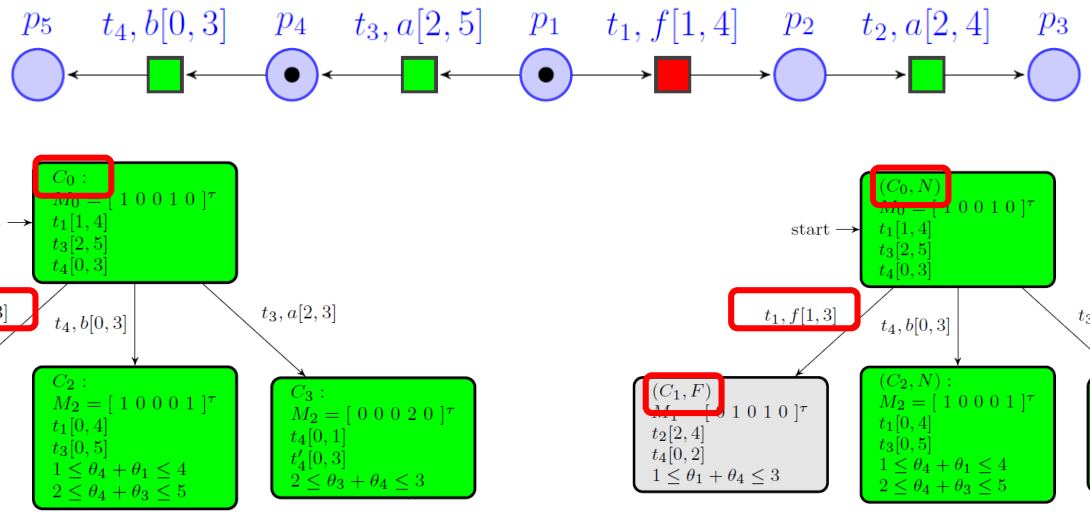




Augmented state class (ASC)

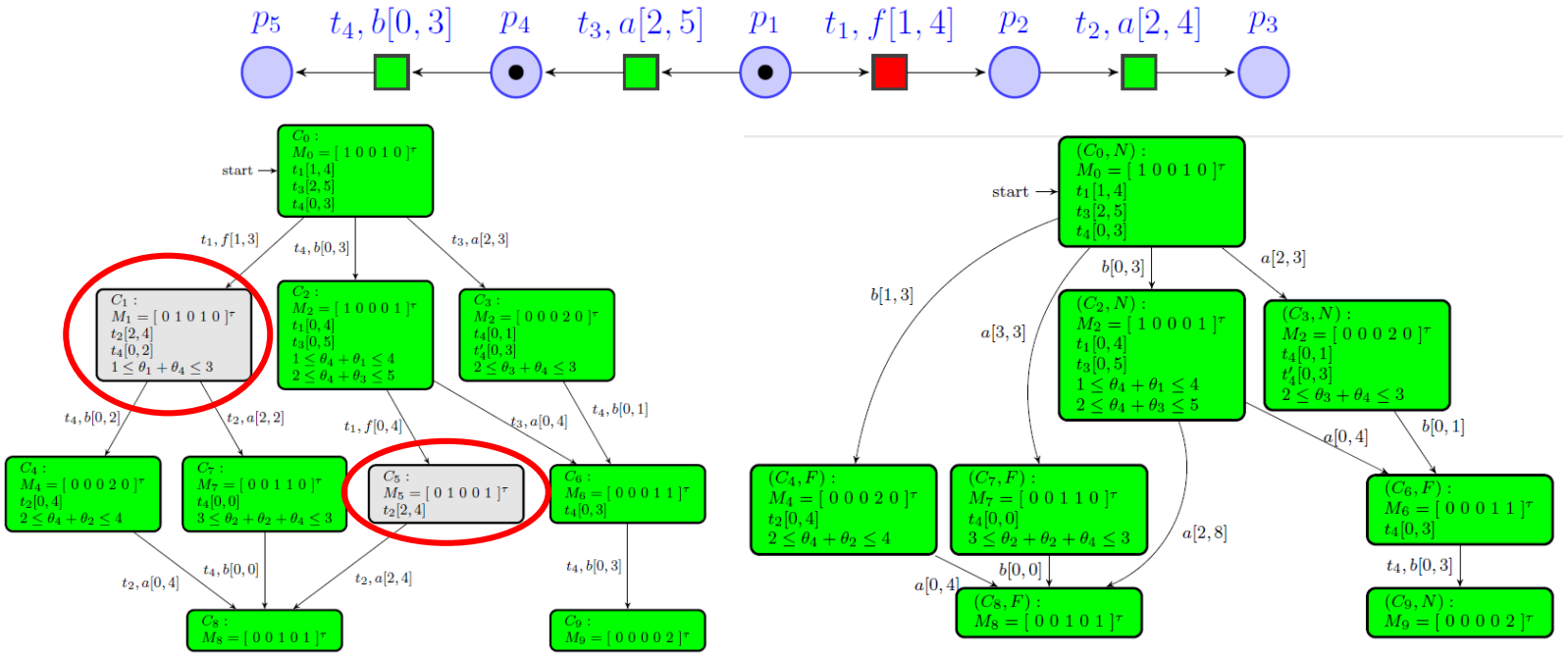
Untimed PN	Time PN (TPN)
Marking (state)	State class
State representation using the same marking	

LPN	LTPN
FM = marking + fault tag	ASC = state class + fault tag
state + fault tag	

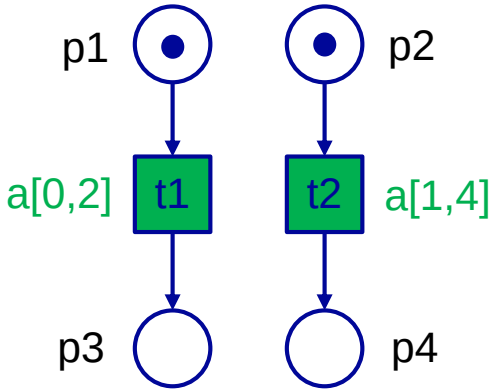


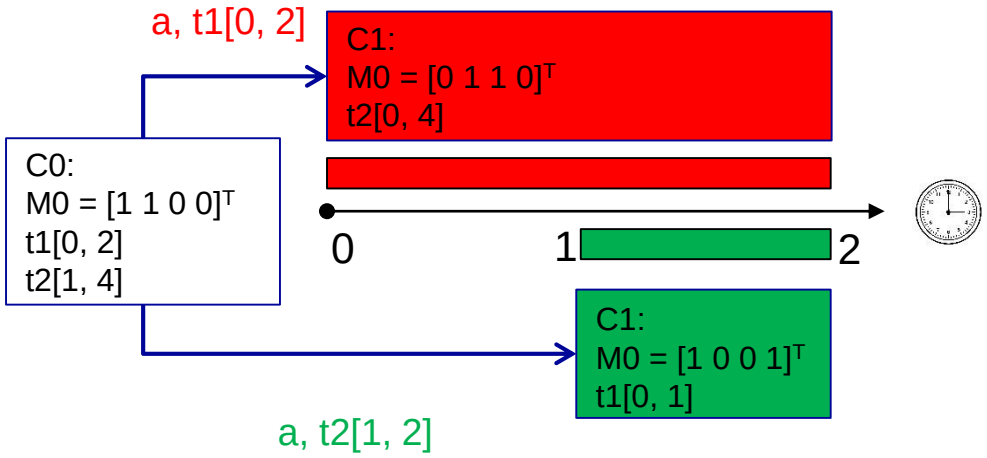
ASC-graph

LPN	LTPN
FM-graph = FM reachability + fault tag	ASC-graph = state class reachability + fault tag
Reachability graph + fault tag	

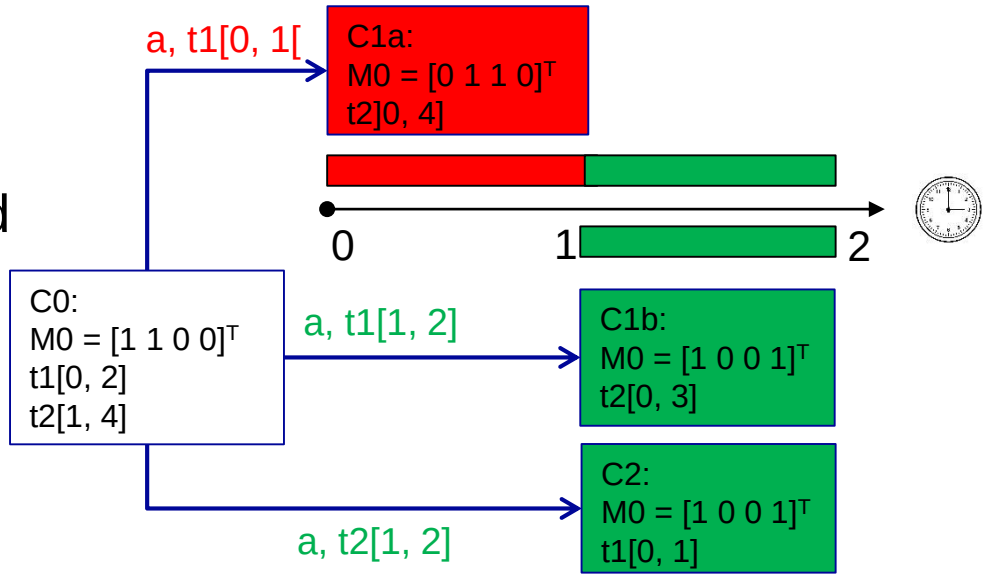


Nondeterminism of LTPN

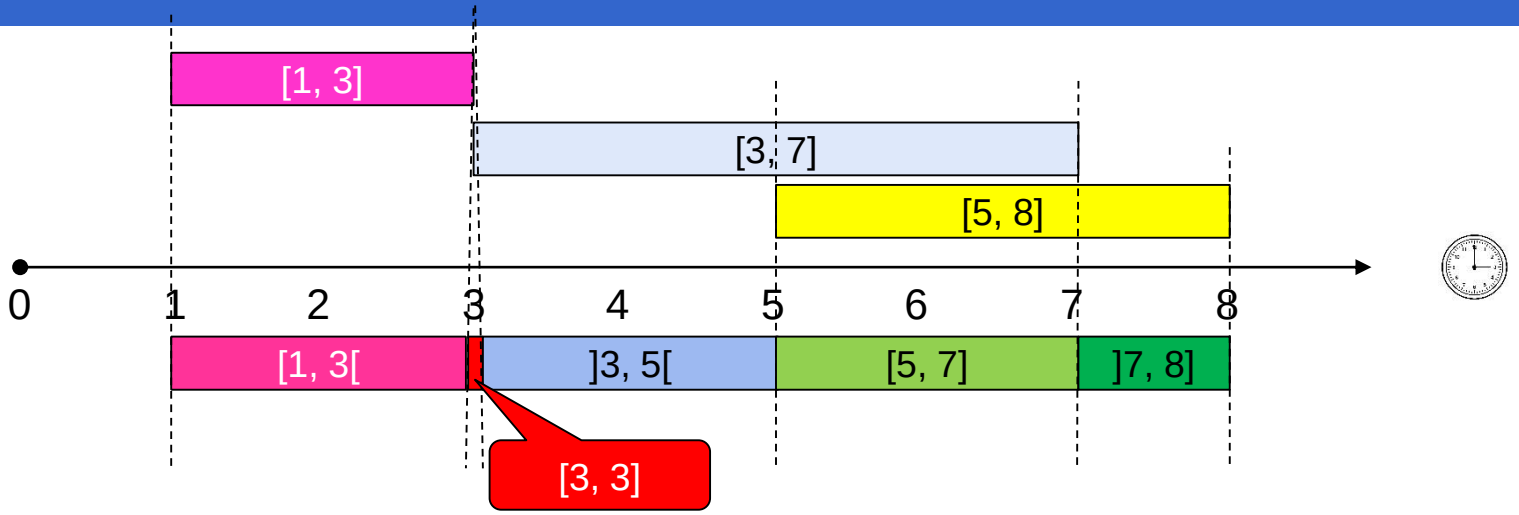




- Nondeterminism
  - Empty transition (reduced by sequence duration)
  - Output with the same label & the same firing date



Time interval splitting (TIS)



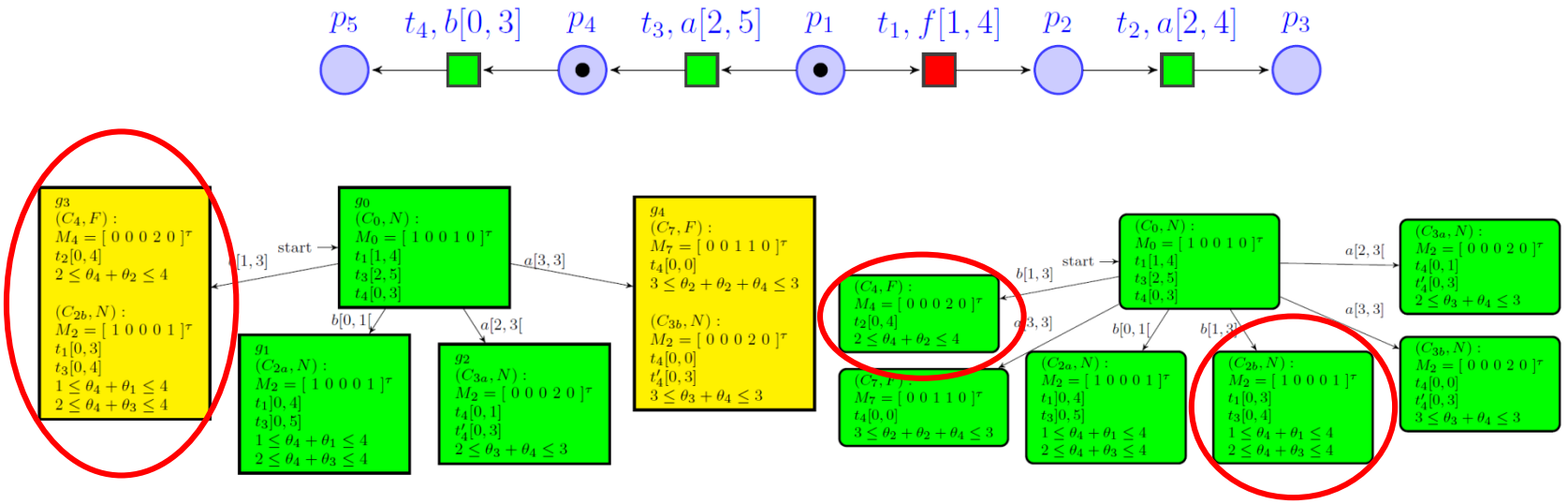
Definition *Given a finite time interval set A, the* basic interval set (BIS) *of A, denoted by $BIS(A)$, is a set of disjoint nonempty time intervals β_j subject to:*

1. $\forall\ k \neq j, \beta_k \cap \beta_j = \emptyset$;
2. $\forall\ \alpha \in A, \exists\ \beta_1, \beta_2, \cdots, \beta_m \in BIS(A)$, *such that* $\alpha = \bigcup_{j=1}^{m} \beta_j$;
3. $\forall\ \beta_1, \beta_2 \in BIS(A), \beta_1 \neq \beta_2, \exists\ \alpha \in A$, *such that* $\beta_1 \cap \alpha = \emptyset, \beta_2 \cap \alpha \neq \emptyset$.

- The BIS of a finite interval set if **finite** & **unique**.
- Timed analysis can be transformed into **untimed** analysis.

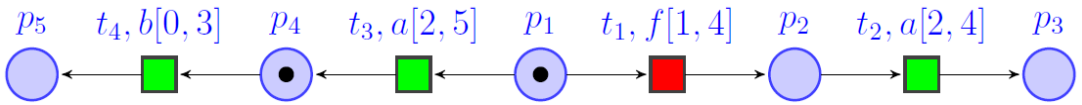
ASC-set

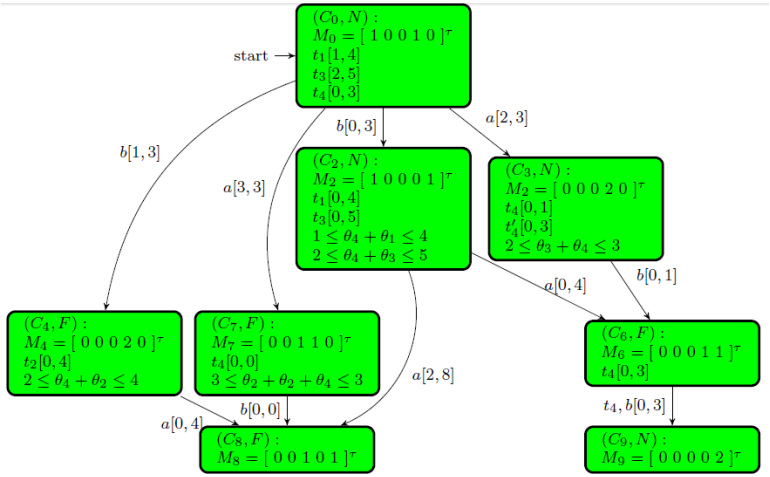
LPN	LTPN
FM-set = A set of FMs relative to the same observation	ASC-set = A set of ASCs relative to the same observation
A set of states relative to the same observation	

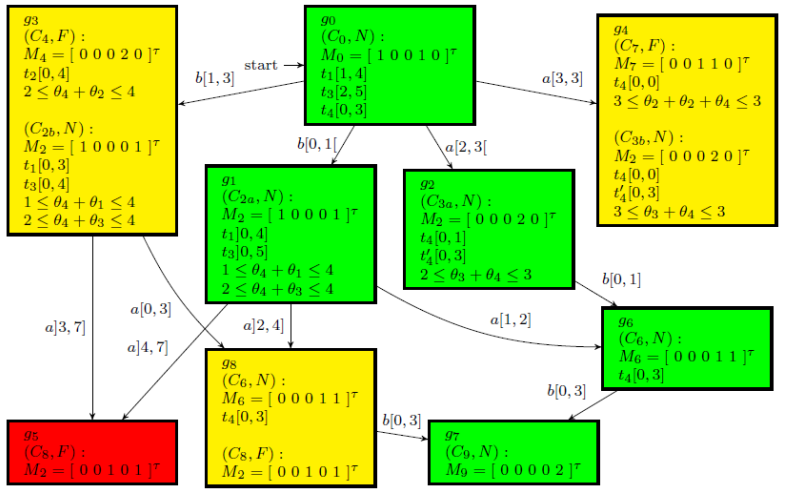


ASC-set graph (ASG)

LPN	LTPN
FM-set tree = FM-set reachability + fault propagation	ASG = ASC-set reachability + fault propagation
State estimation + fault propagation	

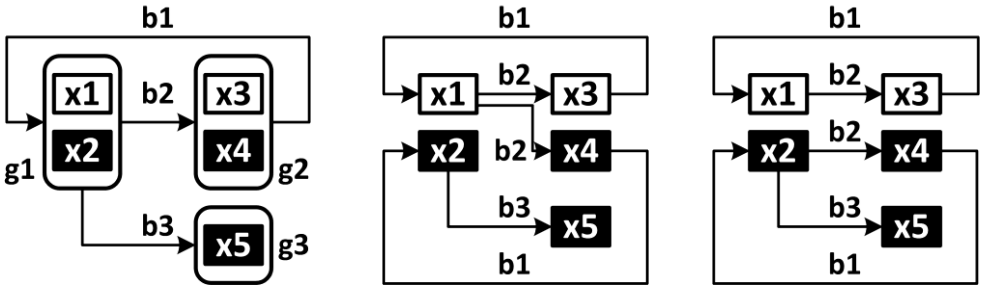




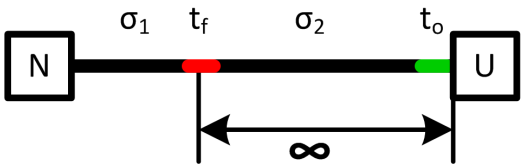


Conditions for undiagnosability

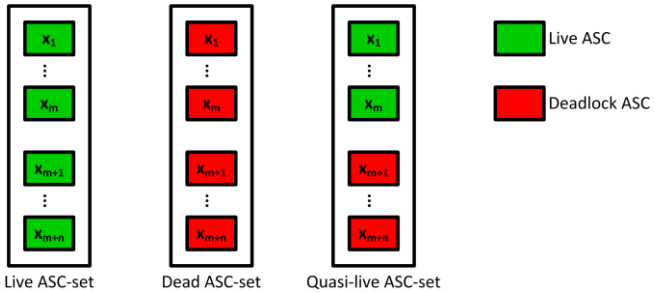
- Condition 1: existence of indeterminate cycle



- Condition 2: infinite sequence duration before F-uncertain node



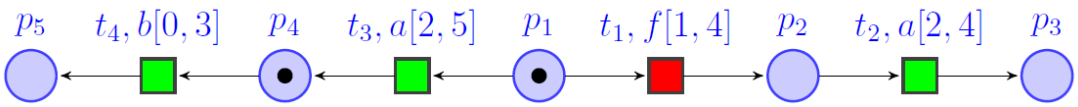
- Condition 3: dead F-uncertain subset of ASC

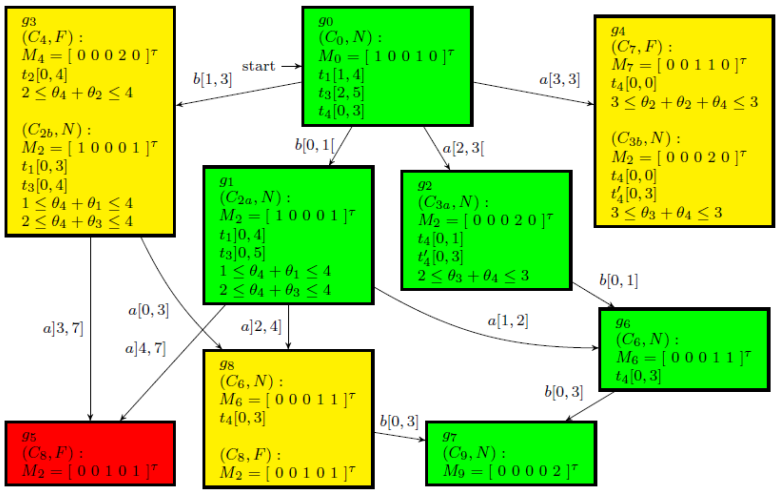


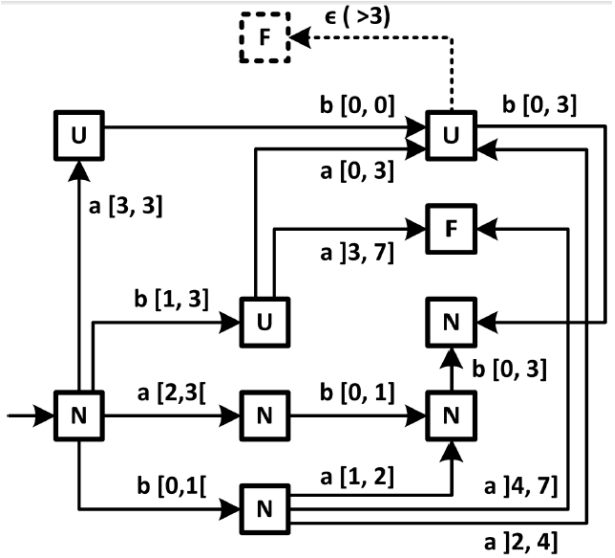
Stopping condition	Discision
Indeterminate cycle	undiagnosable
Infinite duration after a fault	
Specified dead subset of ASC	

Online diagnosis

- Online diagnoser
  - Derived from the ASG
  - Deterministic structure







Conclusions & perspectives

Conlusions

- Fault diagnosis of DES in untimed context
  - Analysis using partial generation of the state space
  - Integration of K-, classic diagnosability and diagnosis analysis
  - Search K_{min} for diagnosable systems
- Fault diagnosis of DES in timed context
  - Time interval splitting technique untimed context
  - Transformation of LTPN to untimed structure
  - Necessary and sufficient conditions for diagnosability
  - Efficient on-the-fly approach to tackle combinatorial explosion

Perspectives

- Fault diagnosis of DES in untimed context
  - K_{opt}: optimal bound for search K_{min}.
  - Application of on-the-fly and incremental approach to verifier approach.

- Fault diagnosis of DES in timed context
  - Δ_{opt}: optimal bound for searching Δ_{min}.
  - Zone graph technique.

Publications

- **Liu, B.**, Ghazel, M., & Toguyeni, A. *Diagnosis of Labeled Time Petri Nets Using Time Interval Splitting*. The 19th IFAC World Congress (IFAC-WC 2014), 2014.

- **Liu, B.**, Ghazel, M., & Toguyeni, A. *Toward an Efficient Approach for Diagnosability Analysis of DES modeled by Labeled Petri Nets.* The 13th European Control Conference (ECC'14), 2014.

- **Liu, B.**, Ghazel, M., & Toguyéni, A. *Évaluation à la volée de la diagnosticabilité des systèmes à événements discrets temporisés*. Journal Européen des Systèmes Automatisés (JESA), édition spéciale MSR'13. 2013.

- **Liu, B.**, Ghazel, M., & Toguyeni, A. *K-diagnosability of labeled Petri nets*. 9ème édition de la conférence MAnifestation des JEunes Chercheurs en Sciences et Technologies de l'Information et de la Communication (MajecSTIC 2012), 2012.

An Efficient Approach for Diagnosability and Diagnosis of DES Based on Labeled Petri Nets - Untimed and Timed Contexts

Baisi Liu

Supervisors

Armand Toguyéni, Mohamed Ghazel

09/04/2014