Évaluation à la volée de la diagnosticabilité des systèmes à événements discrets temporisés

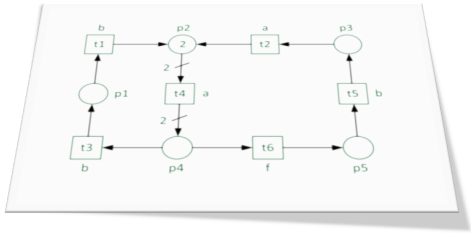
Baisi LIU, Mohamed GHAZEL, Armand TOGUYÉNI

École Centrale de Lille (EC-Lille)
Laboratoire d'Automatique, Génie Informatique et Signal (LAGIS)
Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux (IFSTTAR)

November 15, 2013

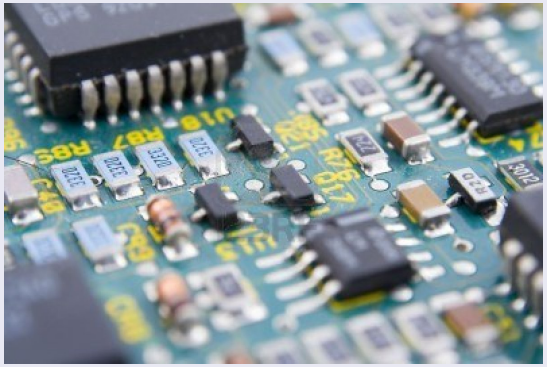
Outline

1. Introduction
   - Discrete event systems
   - Fault diagnosis of discrete event systems
   - Objectives



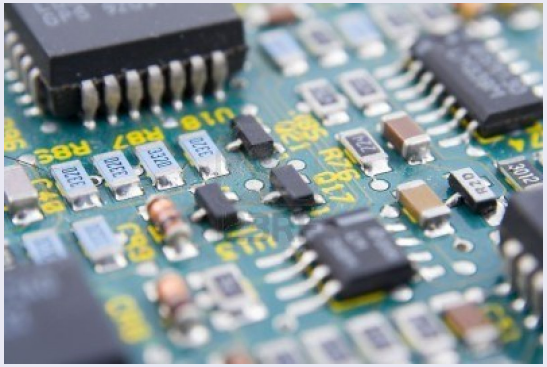
Abstraction of discrete event systems

Real systems → discrete event systems (DES)



Abstraction of discrete event systems

Real systems → discrete event systems (DES)



Abstraction of DES [Cassandras & Lafortune, 2007]

- Untimed DES
  - System behavior is described by events of logic ordering,
    e.g., $s_1 = ab$, $s_2 = ab$.
- Timed DES
  - System behavior is described by events of logic ordering + occurrence dates,
    e.g., $s_1 = (a@1)(b@5)$, $s_2 = (a@2)(b@4)$.
- Stochastic DES
  - logic ordering + occurrence dates + occurrence probability

Fault diagnosis of DES

Partial observation

- Indication of an event by sensor reading $\rightarrow$ observation
- Limitation of sensor installation $\rightarrow$ partial observation

Fault diagnosis of DES

Partial observation

- Indication of an event by sensor reading $\rightarrow$ observation
- Limitation of sensor installation $\rightarrow$ partial observation

Fault diagnosis [Lin, 1994; Sampath *et al.*, 1995]

- Diagnosability
  - The ability to diagnose any fault in finite delay (K steps / Δ time units)
  - Offline analysis
- Diagnosis
  - Detection and isolation of a fault
  - Online analysis

Fault diagnosis of DES

Partial observation

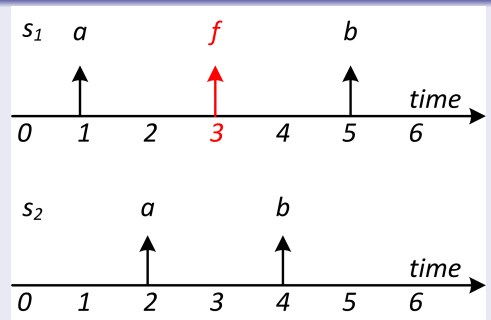
- Indication of an event by sensor reading $\rightarrow$ observation
- Limitation of sensor installation $\rightarrow$ partial observation

Fault diagnosis [Lin, 1994; Sampath *et al.*, 1995]

- Diagnosability
  - The ability to diagnose any fault in finite delay (K steps / Δ time units)
  - Offline analysis
- Diagnosis
  - Detection and isolation of a fault
  - Online analysis

From untimed to timed diagnosis

- An undiagnosable fault in untimed context may be diagnosable in timed context
- An undiagnosable fault in timed context must be undiagnosable in timed context
- Untimed context: $s_1 = s_2$, f is undiagnosable
  Timed context: $s_1 \neq s_2$, f is diagnosable



Relative research on diagnosability

Untimed diagnosability

- Sampath *et al.*, 1995
  automata, diagnoser automata, conditions for diagnosability

Untimed K-diagnosability

- Basile *et al.*, 2010; 2012
  Petri net, linear programming, conditions for diagnosability
- Cabasino *et al.*, 2012
  Petri net, verifier net, conditions for diagnosability

Timed Δ-diagnosability

- Tripakis *et al.*, 2002; Cassez et al., 2012
  timed automata, conditions for timed diagnosability
- Bouyer *et al.*, 2005
  timed automata, timed diagnosability

Problems

Can we analyze timed diagnosability using untimed approaches?

Problems

Can we analyze timed diagnosability using untimed approaches?

Timed diagnosability analysis of DES

- What are the conditions for diagnosability of timed DES?

Problems

Can we analyze timed diagnosability using untimed approaches?

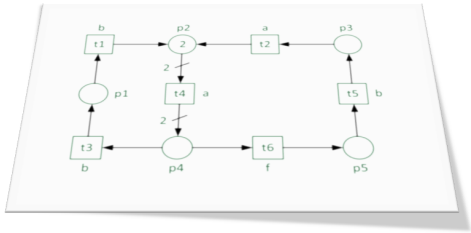
Timed diagnosability analysis of DES

- What are the conditions for diagnosability of timed DES?

Δ-diagnosability of timed DES

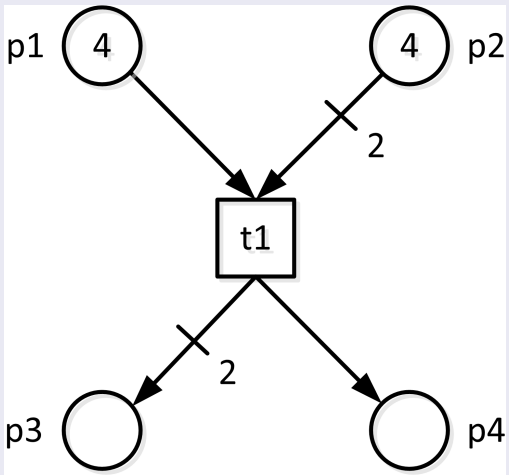
- Is a fault diagnosable under a given time delay of Δ?
- Is there a minimum Δ to ensure diagnosability?
  For $\Delta \geq \Delta_{min}$ the system is Δ-diagnosable.
  For $\Delta < \Delta_{min}$ the system is not Δ-diagnosable.

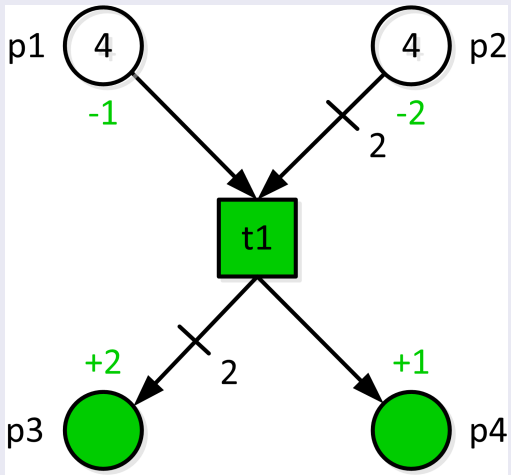
2. Labeled time Petri net and its observability
   - Petri net and its extensions
   - Observation of labeled time Petri net

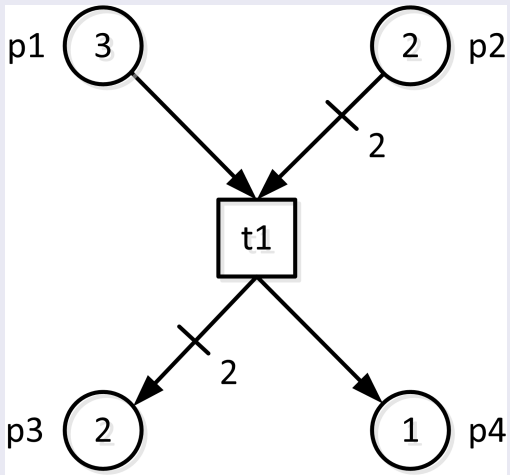


Petri net (PN) [Petri, 1962]

- Petri net $= (P, T, Pre, Post, M_0)$
  - P is the set of places;
  - T is the set of transitions;
  - Pre is the pre-incidence mapping;
  - $Post$ is the post-incidence mapping;
  - M_0 is the initial marking.



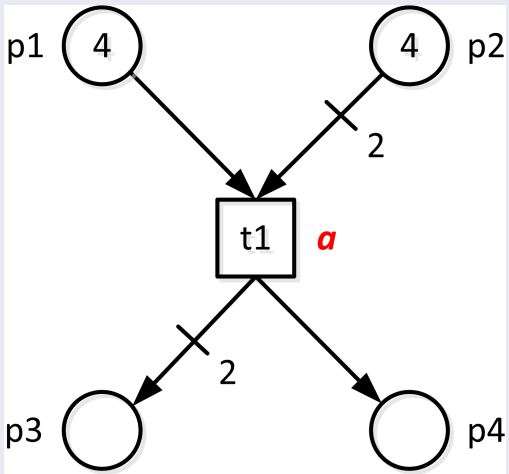


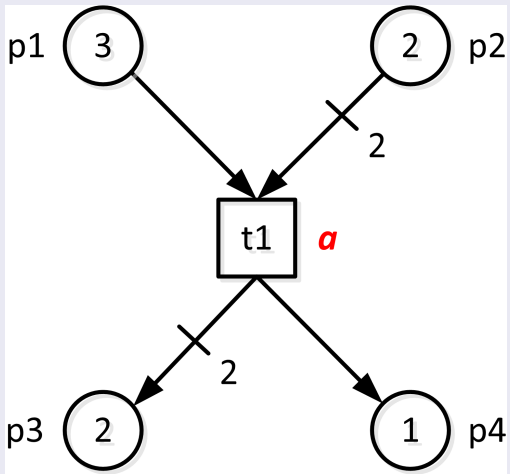


- $M_1 = M_0 + (Post - Pre) \cdot \vec{t_1}$

Labeled Petri net (LPN)

- Labeled Petri net $= (P, T, Pre, Post, M_0, \Sigma, \varphi)$
  - $(P, T, Pre, Post, M_0)$ is an ordinary Petri net;
  - Σ is the set of events;
  - φ is the labeling function $\Sigma \to T$.

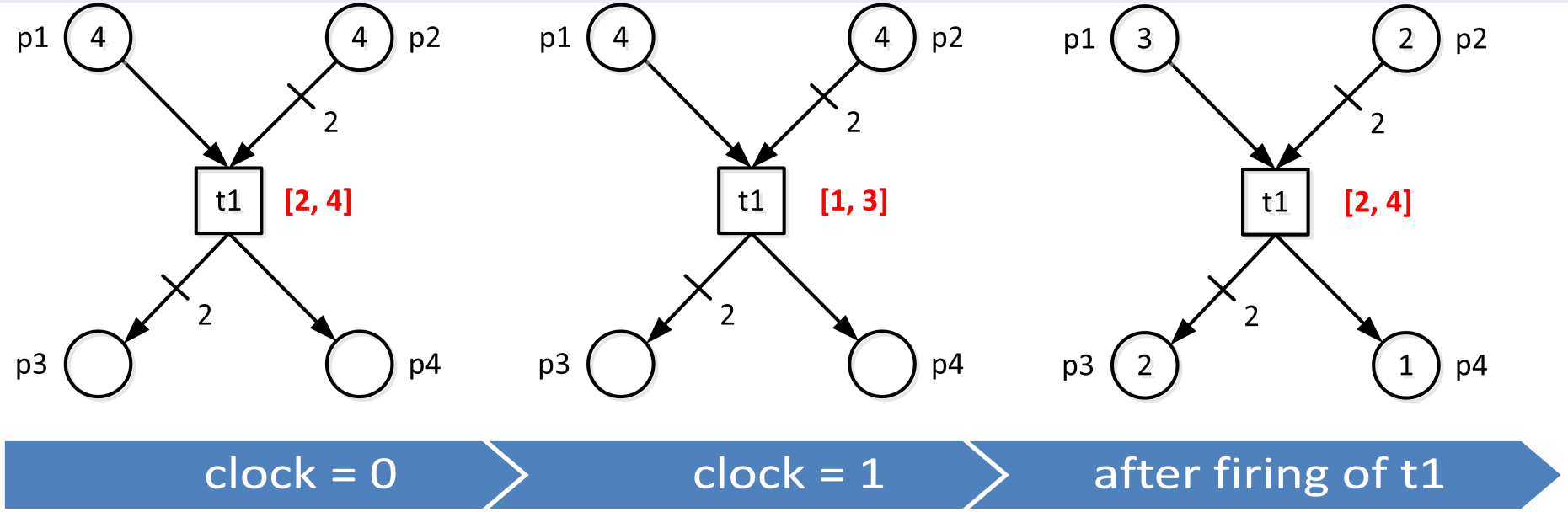




- $M_1 = M_0 + (Post - Pre) \cdot \vec{t_1}$

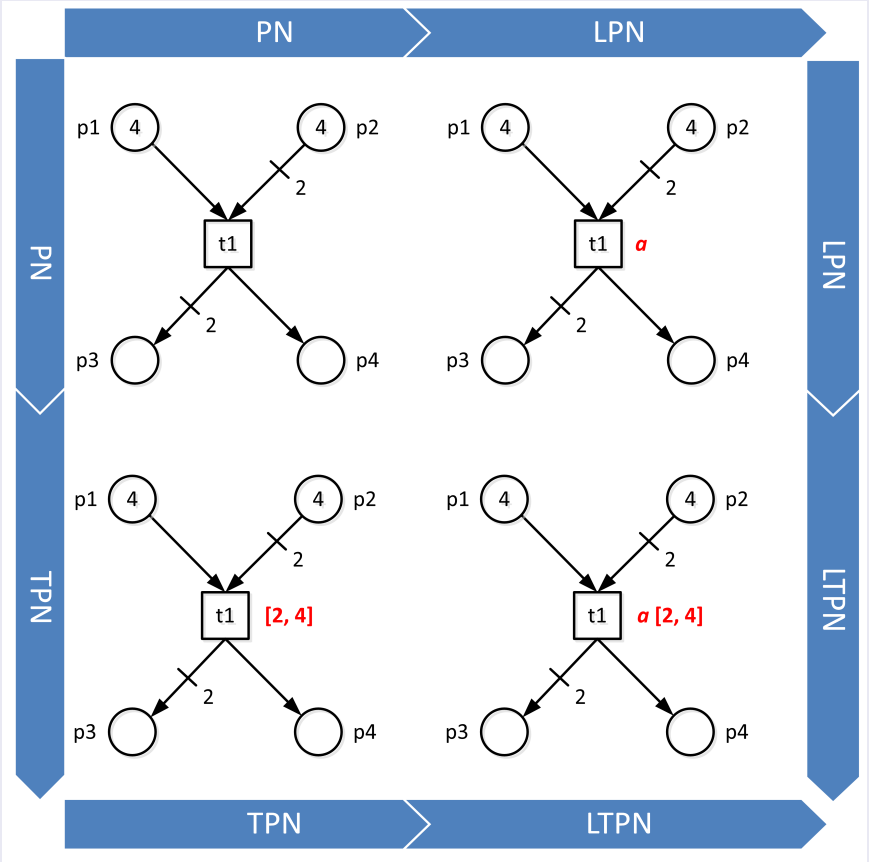
Time Petri net (TPN) [Merlin, 1974]

- Time Petri net $= (P, T, Pre, Post, M_0, SIM)$
  - $(P, T, Pre, Post, M_0)$ is an ordinary Petri net;
  - $SIM : T \to \mathbb{Q}^+ \times (\mathbb{Q}^+ \cup \{\infty\})$ is the static interval mapping.



Labeled time Petri net (LTPN)

- LTPN $= (P, T, Pre, Post, M_0, \Sigma, \varphi, SIM)$



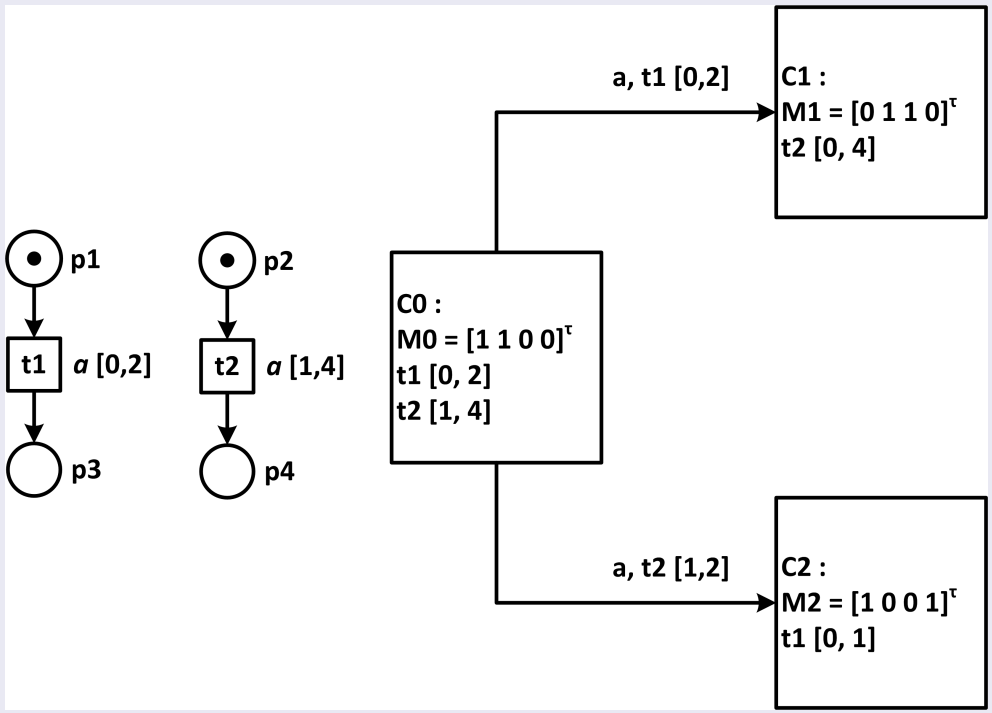
- A LTPN is a nondeterministic timed model for DES.

State class for TPN & LTPN

State class [Berthomieu, 1983]

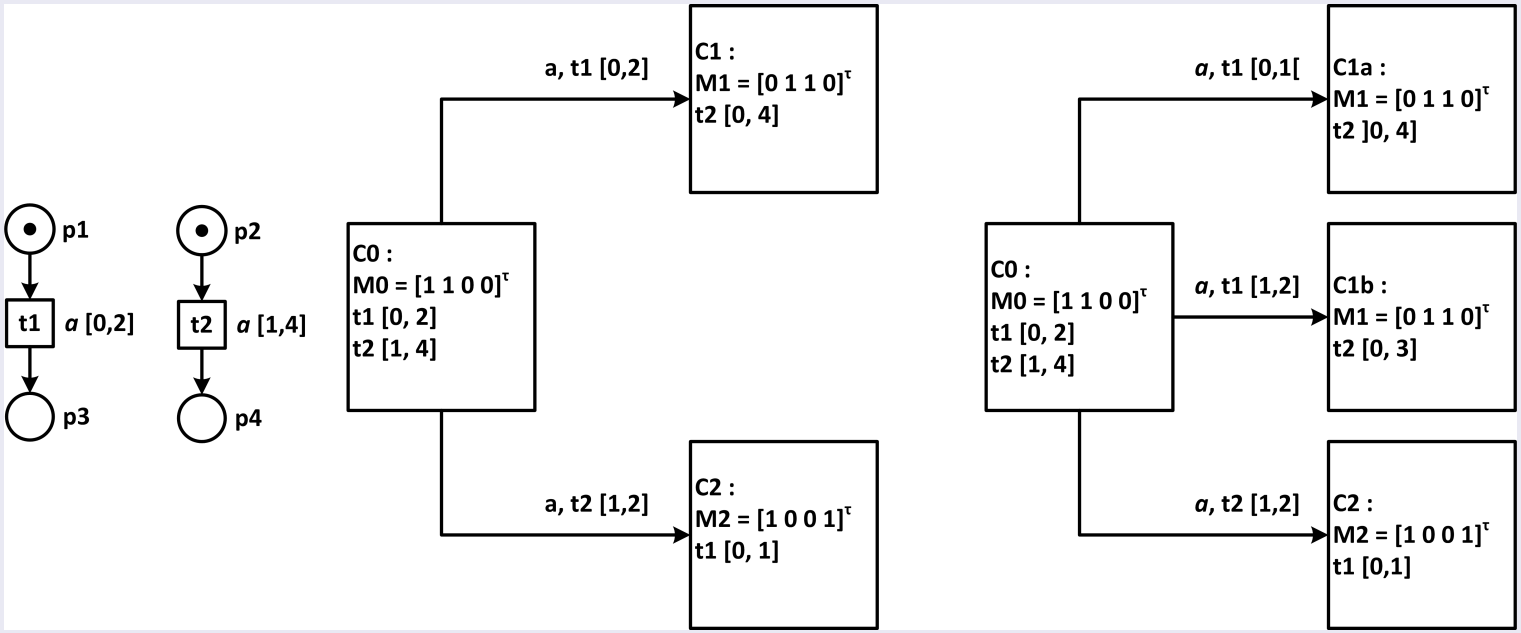
- State class $C = (M, D)$
  - M is a marking;
  - D is a firing domain;
- State class provides finite presentation for infinite state space.

Example



Overestimation in the observation for LTPN

Example



A deterministic structure for observation of LTPN

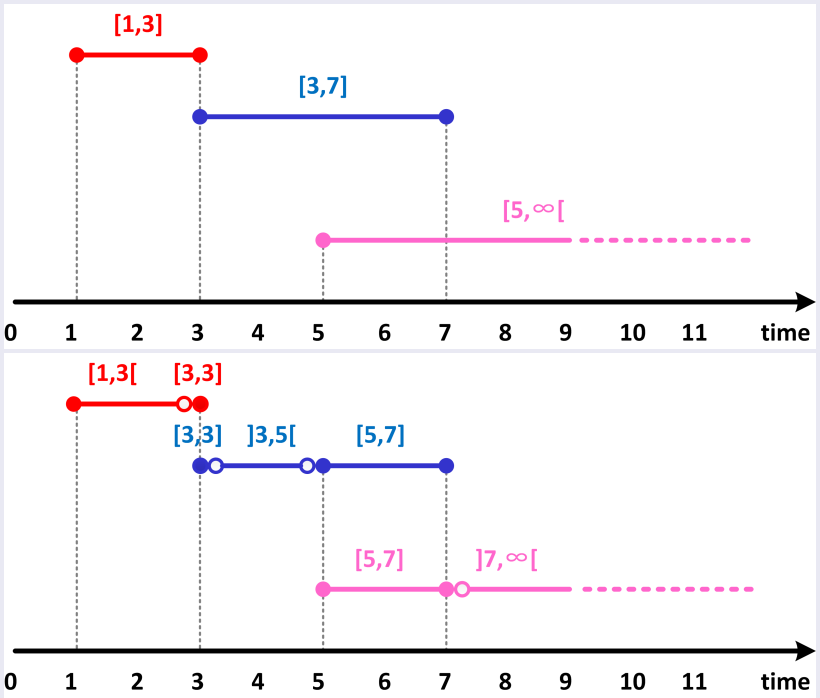
- Original state classes (firing domains) are overestimated after splitting time intervals.
- Recomputation of state classes is necessary for further analysis.

Splitting time intervals

- Untimed discrimination:
  (e_1, i_1) and (e_2, i_2) are distinguishable if $e_1 \neq e_2$,
  e.g., $a[2, 4]$ and $b[3, 5]$ are distinguishable.
- Timed discrimination:
  (e, i_1) and (e, i_2) are distinguishable if $i_1 \cap i_2 \neq \emptyset$,
  e.g., $a[2, 4]$ and $a[7, 9]$ are distinguishable.

Splitting time intervals

- Untimed discrimination:
  (e_1, i_1) and (e_2, i_2) are distinguishable if $e_1 \neq e_2$,
  e.g., $a[2, 4]$ and $b[3, 5]$ are distinguishable.
- Timed discrimination:
  (e, i_1) and (e, i_2) are distinguishable if $i_1 \cap i_2 \neq \emptyset$,
  e.g., $a[2, 4]$ and $a[7, 9]$ are distinguishable.



$$e[1, 3]; e[3, 7]; e[5, \infty[$$

$$\Downarrow$$

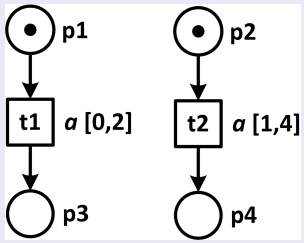
$$e[1, 3[; e[3, 3]; e]3, 5[; e[5, 7]; e]7, \infty[$$

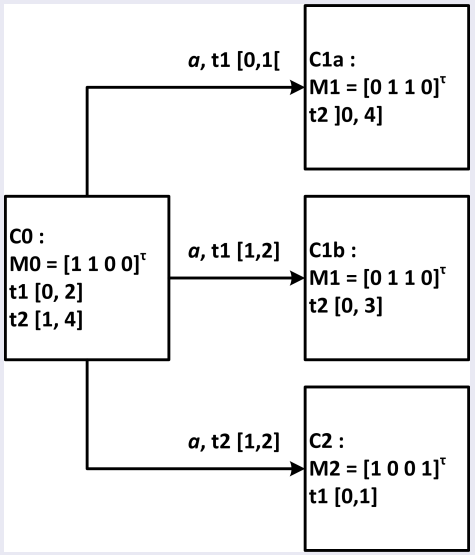
Observer for LTPN

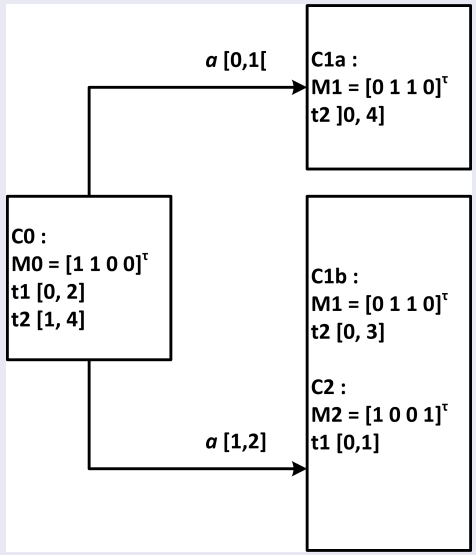
Transition between state class sets

- $X_1 \xrightarrow{(e,i)} X_2$
  - X_1: a source set of state classes;
  - (e, i): observable event e with an interval i;
  - X_2: a target set of state classes.
- An observer for LTPN deduce the current state by an event and its occurrence date.

Example

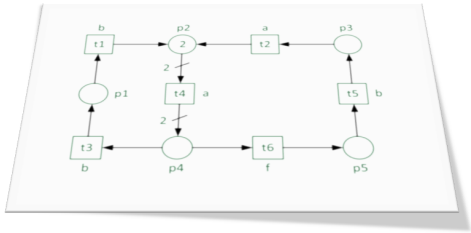






- Splitting time interval transforms a timed nondeterministic structure into a untimed deterministic one.

3. Diagnosability of labeled time Petri nets
   - Basic notations
   - Conditions for diagnosability
   - Online diagnosis



Augmented state class graph (ASC-graph)

Augmented state class (ASC)

- ASC: $x = (C, y)$
  - C is a state class;
  - y is a fault tag.
- $x' = (C', y')$ is reachable from $x = (C, y)$ upon $\sigma \in T^*$, iff
  - $C \xrightarrow{\sigma} C'$;
  - $$y' = \begin{cases} F & \text{if } (y = F) \vee (\exists\ k, \sigma^k \in T_f) \text{ where } T_f \text{ is the set of faulty transitions} \\ N & \text{otherwise} \end{cases}$$

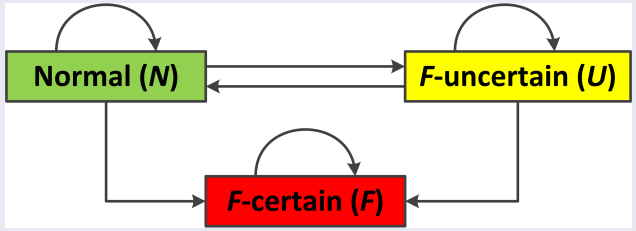
ASC-graph

- ASC-graph carries the information of both reachability and fault propagation.
- The graph structure helps to check some specific cycles (indeterminate cycles).

ASC-set graph (ASG)

ASC-set

- ASC-set is a set of ASCs reached right after an observable event.
- An ASC-set is
  - normal, if $\forall\ (C, y) \in g, y = N$ (N denotes normal);
  - F-certain, if $\forall\ (C, y) \in g, y = F$ (F denotes fault);
  - F-uncertain, otherwise.
- The transition of ASC-set $(C, y) \rightarrow (C', y')$:
  - $C \rightarrow C'$ follows the rules for classical state classes.
  - $y \rightarrow y'$ follows the rules for (permanent) fault propagation.



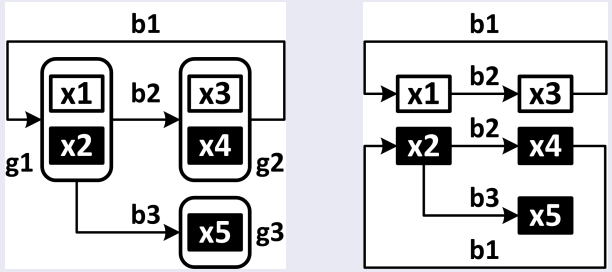
ASC-set graph (ASG)

- An ASG is a deterministic structure for diagnosability analysis.
- An ASG present the reachability and fault propagation of LTPN in untimed formation.

Conditions for diagnosability

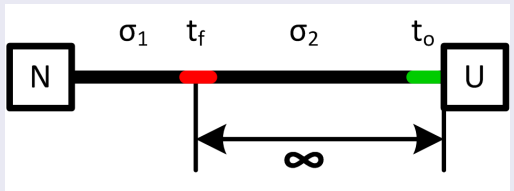
Condition 1: no indeterminate cycle

- No indeterminate cycle is the condition for diagnosability for untimed DES. [Sampath *et al.*, 1995]
- There exists "indeterminate cycle" $\Rightarrow$ the fault is undiagnosable.



Condition 2: infinite sequence duration

- The sequence duration between a fault and an F-uncertain ASC is infinite
  $\Rightarrow$ the fault is undiagnosable.
  $\sigma_1 \in T_u^*, t_f \in T_f, \sigma_2 \in T^*, t_o \in T_o, (max(SD(\sigma_2 t_o)) = \infty) \Rightarrow t_f$ is not diagnosable

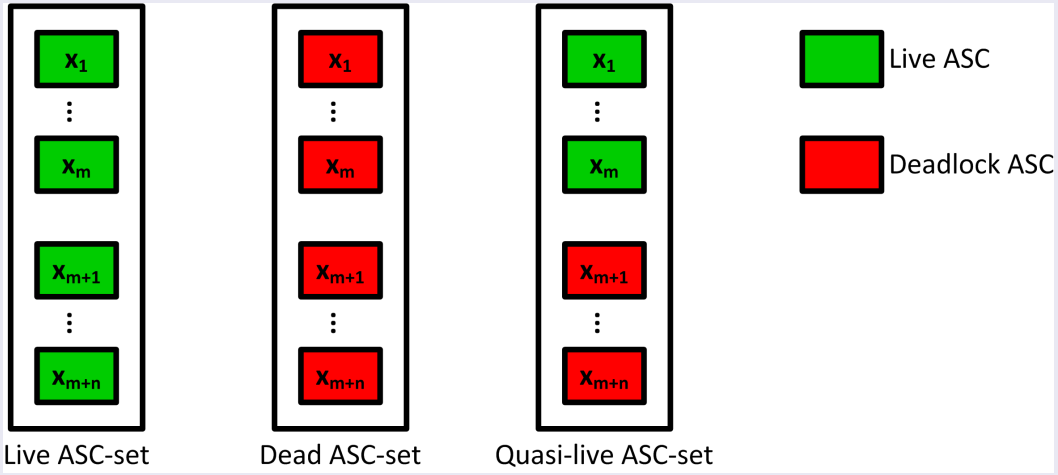


- This condition is under the condition of diagnosability in timed context.

Conditions for diagnosability

Condition 3: F-uncertain subset of ASC

- Deadlock subset of an F-uncertain ASC is F-uncertain
  $\Rightarrow$ the fault is undiagnosable.
- This condition is under the condition of unlive timed DES.



Condition for diagnosability

- !Condition 1 $\wedge$!Condition 2 $\wedge$!Condition 3
  $\Rightarrow$ the fault is diagnosable.

On the fly approach

On the fly approach

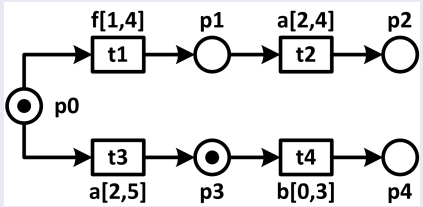
- ASC-graph and ASG are built in parallel.
  - ASC-graph is used for checking indeterminate cycles.
  - ASG is used for analyze fault propagation.
- State space is generated as necessary.

Advantage

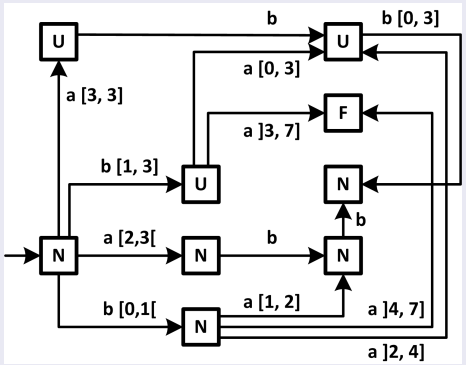
- Lower cost than state enumerative approach.
- Possible to lead the state generation by a strategy.

Online diagnosis of LTPNs

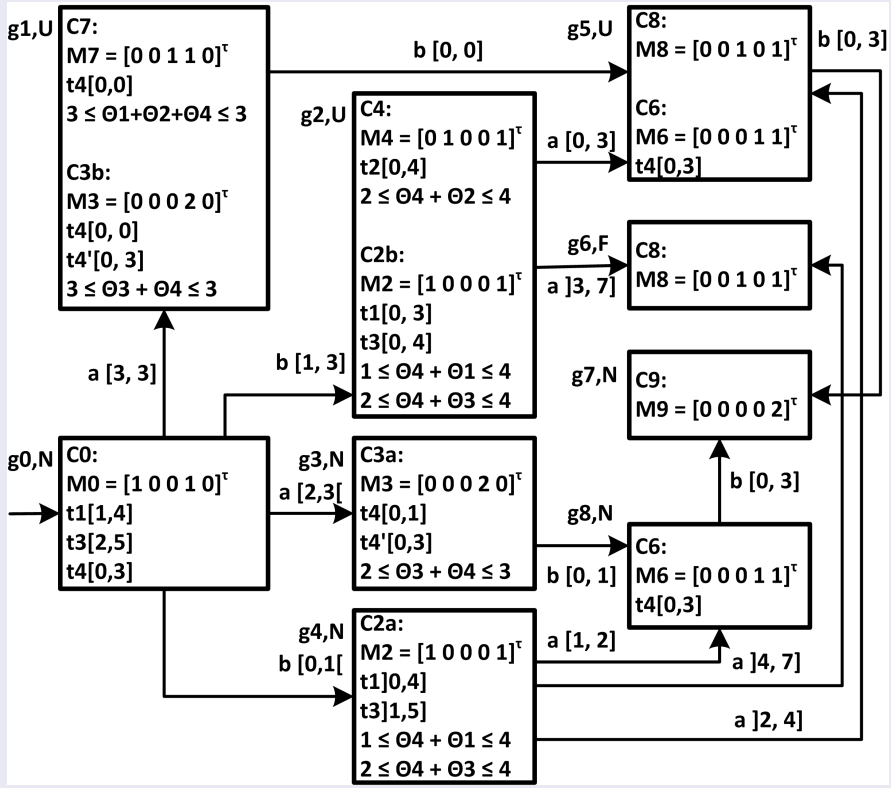
- LTPN → ASG → timed diagnoser
- Timed diagnoser reacts to a sequence of observable events and occurrence date.



LTPN → ASG

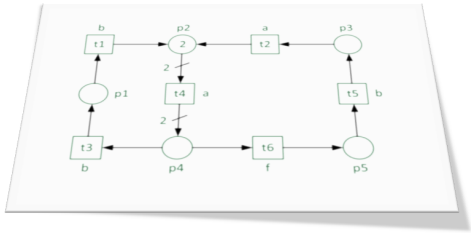


diagnoser ← ASG



- Example: $(b@2)(a@4)$ → a fault has occurred.

4 Summary
- Contributions and Current Works



Contributions

- Approach of splitting time intervals to analyze observability of LTPNs.
- Conditions for diagnosability for LTPN models.
- An on-the-fly approach to check diagnosability.

Future Works

- On-the-fly construction of ASG using heuristics.
- Diagnosability analysis using zone graph.

Thank you for your attention!