Fault diagnosis and prognosis in Petri Nets by using a single generalized marking estimation

F. Basile[1] P. Chiacchio[1] G. De Tommasi[2]

[1]Università di Salerno, Italy

[2]Università di Napoli "Federico II", Italy

IFAC SAFEPROCESS 2009, Barcelona, Spain

Outline

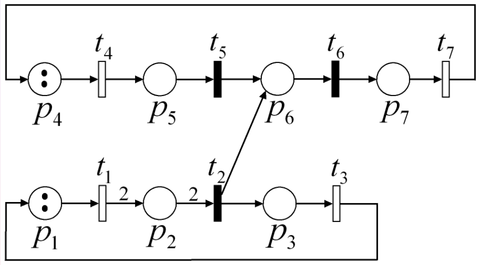
Backgrounds

- Fault detection for DES has been issued since the mid 80s, and it is still an *hot topic*
- The standard approach is based on the *diagnoser* automata (Sampath et al., IEEE Trans. Aut. Contr., 1995)
- All possible unobservable events that may occur from a given state have to be considered
- A number of approaches based on a Petri net (PN) models have been proposed

Backgrounds (cont'd)

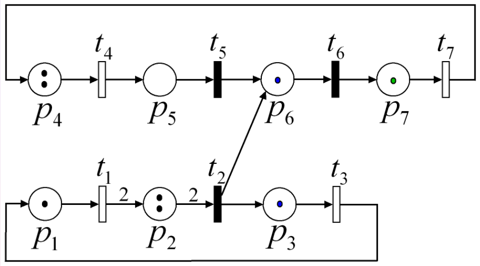
- In the PNs framework, a possible approach to fault diagnosis provides to associate the faults to unobservable transitions
- These approaches need to estimate the current state of the net (Genc and Lafortune, IEEE Trans. Automat. Sci. Eng., 2007 – Giua and Seatzu, 44^{th} IEEE CDC, Boel and Jiroveanu, 16^{th} Symp. Math Theory Networks Syst.)
- Explosion of the state space estimation

Explosion of the state space estimation



$\mathbf{m}_0 = \begin{bmatrix} 2 & 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^{\mathrm{T}}$ - t_1 fires.

Explosion of the state space estimation



Unobservable Reach (as called in Genc and Lafortune)

$\mathbf{m}_1 = \begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^T$

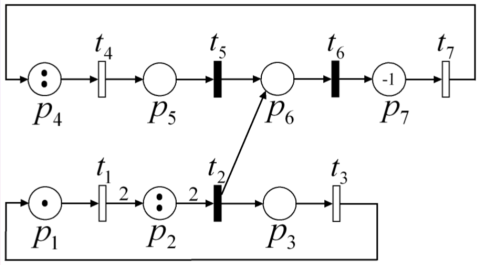
$\mathbf{m}_2 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 1 & 0 \end{bmatrix}^T$ - if t_2 has fired

$\mathbf{m}_3 = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}^T$ - if t_2 and t_6 have fired

A unique PN state estimation: the generalized marking

- In (Basile et al, WODES 2008) the authors have introduced generalized markings to avoid state space explosion.
- Generalized markings can have negative components
- The negative components record how many tokens are missing in the input places of observable transitions, whose firings have not been explained yet.
- Using the generalized marking the fault diagnosis problem is formulated in terms of ILP problems
- Given the *local* representation of the state in PNs, for each fault the ILPs are solved on a subnet which is *smaller* than the whole plant model.

Generalized marking: example



If t_7 fires we reach

$$\boldsymbol{\mu} = \begin{bmatrix} 1 & 2 & 0 & 2 & 0 & 0 & -1 \end{bmatrix}^{\mathrm{T}}.$$

As far as the fault diagnosis is concerned, $\boldsymbol{\mu}$ stores in a compact way all the needed information about the state space estimation.

Fault detection algorithm: remarks

- The problem of diagnosability, i.e. to decide a priori if a given fault can be detected, is not addressed by the proposed algorithm.
- It is assumed that the fault events - assumed to be unobservable - can be detected.
- The proposed approach is mainly aimed to improve the efficiency in terms of memory requirements.

Motivation

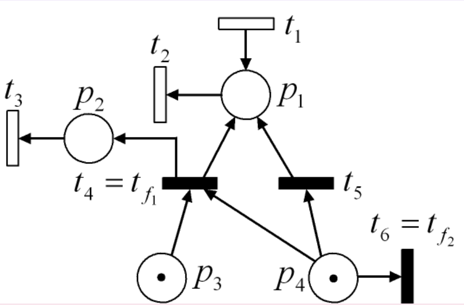
Motivation

We had the feeling that diagnosability was sufficient to perform *diagnosis* using a single generalized marking estimation, but we must prove that!

Remark

Diagnosability is obviously necessary!

Motivation (cont'd)



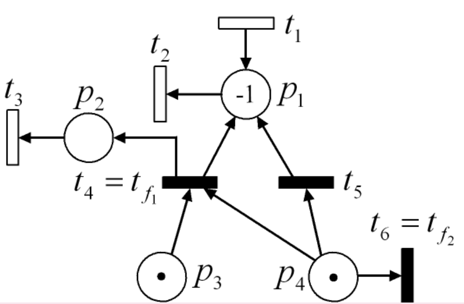
$\mu_0 = \mathbf{m}_0 = [0\ 0\ 1\ 1]^T$

t_1 , t_2 , t_3 are observable transitions

t_4 , t_5 and t_6 are unobservable transitions

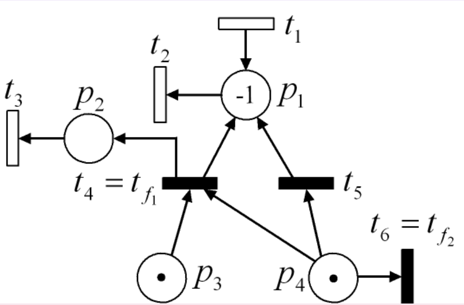
$t_4 = t_{f_1}$ and $t_6 = t_{f_2}$ model faults

Motivation



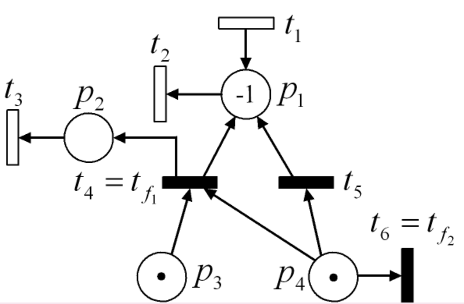
After the firing of $\sigma = t_2$, the generalized marking estimation becomes $\boldsymbol{\mu}_1 = [-1\ 0\ 1\ 1]^T$.
The negative component of $\boldsymbol{\mu}_1$ means that either t_4 or t_5 should have fired in order to explain the observed firing.

Motivation - (cont'd)



If t_3 does not fire, it is impossible to find any sufficiently long continuation of σ that permits to distinguish between the firing of t_4 and t_5, then the language associated with the net is not diagnosable (we will show that it is also not detectable).

Motivation - (cont'd)

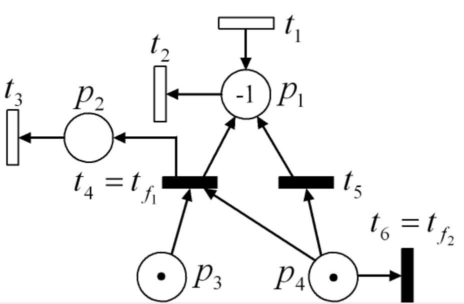


Let $\boldsymbol{\Sigma}(\boldsymbol{\mu}_1)$ be the set of all the possible firing count vectors $\boldsymbol{\epsilon}$ corresponding to sequences of unobservable transitions enabled under $\boldsymbol{\mu}_1$,

$$\max_{\boldsymbol{\epsilon}\in\boldsymbol{\Sigma}(\boldsymbol{\mu}_1)} \boldsymbol{\epsilon}(t_{f_2}) = 0\,,$$

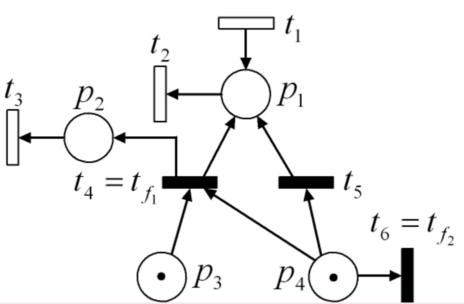
meaning that the fault t_{f_2} has not occurred for sure (and it cannot occur in the future).

Motivation - (cont'd)



Moreover t_{f_2} cannot occur anymore, since either t_4 or t_5 has fired, disabling t_{f_2} without any possibility to enabled it once again.

Motivation - (cont'd)



If the firing of t_1 is observed $\boldsymbol{\mu}_2 = \boldsymbol{\mu}_0$ is reached we erroneously get

$$\max_{\epsilon \in \boldsymbol{\Sigma}(\boldsymbol{\mu}_2)} \epsilon(t_{f_2}) = 1\,,$$

meaning that t_{f_2} may occur.

Contribution

We have found the conditions under which a single g-marking estimation can be used to distinguish both

- between "a fault has occurred for sure" and "a fault may not have occurred" (*diagnosis*)
- between "a fault may have occurred/occur" and "a fault has not occurred for sure" (*prognosis*)

Preliminaries

The notion of detectable prefix-closed and live language is given starting from the definition of diagnosability given in Sampath et al., IEEE Trans. Aut. Contr. 2005.

- $N = (P, T, \mathbf{Pre}, \mathbf{Post})$ is a net with $T = T_{uo} \cup T_o$, and $T_f \subseteq T_{uo}$.
- $\bar{s}$ is the prefix-closure of any trace $s \in T^*$. We denote by L/s the post-language of L after s.
- $Pr : T^* \mapsto T_o^*$ is the usual projection which "erases" the unobservable events in a trace s.
- Pr_L^{-1} is the inverse projection operator defined as

$$Pr_L^{-1}(r) = \left\{s \in L \text{ s.t. } Pr(s) = r\right\}.$$

- If $\dot{t}$ is the final event of trace s, we define

$$\Psi(t_{f_i}) = \left\{s\dot{t} \in L \text{ s.t. } \dot{t} = t_{f_i}\right\}.$$

Diagnosable language - Definition

A prefix-closed and live language L is said to be diagnosable w.r.t. T_f if

$$\forall\ t_{f_i}\ \exists\ h_i \in \mathbb{N} \text{ such that the following holds}$$

$$\forall\ s \in \Psi(t_{f_i}) \text{ and } \forall\ q \in L/s$$

$$||q|| \geq h_i \Rightarrow D$$

where $||q||$ is the length of trace q, and the diagnosability condition D is

$$r \in Pr_L^{-1}\big(Pr(sq)\big) \Rightarrow t_{f_i} \in r\,.$$

Let s be any trace generated by the system that ends in a failure event t_{f_i}, and let q be any sufficiently long continuation of s. Condition D implies that along every continuation q of s it is possible to detect the occurrence of t_{f_i} with a finite delay, specifically in at most h_i transitions of the system after s.

Detectable language

Definition

A prefix-closed and live language L is said to be detectable w.r.t. T_{uo} if it is diagnosable w.r.t. T_{uo}.

Remarks

- detectability implies diagnosability
- undetectability does not necessarily implies undiagnosability
- undiagnosability implies undetectability

Main result - 1

Theorem

Let L be diagnosable w.r.t. T_f. If $s \in \Psi(t_{f_i})$ then exists $q \in L/s$, such that

$$\min_{\epsilon \in \mathbf{\Sigma}(N,\boldsymbol{\mu})} \epsilon(t_{f_i}) > 0\,,$$

with $\boldsymbol{\mu}_0[z\rangle\boldsymbol{\mu}$, and $z = Pr(sq)$.

Main result - 2

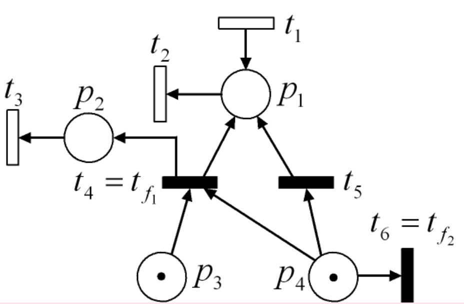
Theorem

Let L be detectable w.r.t. T_{uo}. If s is a sequence which enables the firing of t_{f_i} and $t_{f_i} \notin s$, then it exists $h \in \mathbb{N}$ such that for all sequences $q \in L/s$ whose firing does not enable t_{f_i}, and $||q|| > h$, $t_{f_i} \notin q$, it holds that

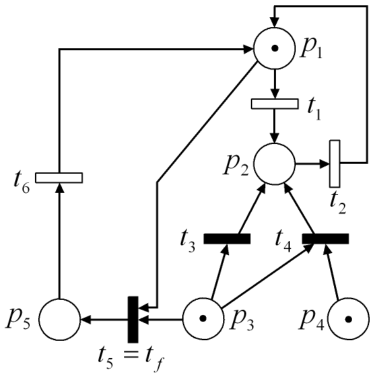
$$\max_{\boldsymbol{\epsilon} \in \boldsymbol{\Sigma}(N, \boldsymbol{\mu}'')} \boldsymbol{\epsilon}(t_{f_i}) = 0\,,$$

with $\boldsymbol{\mu}_0[\beta\rangle\boldsymbol{\mu}''$, and $\beta = Pr(sq)$.

Undiagnosable and undetectable net

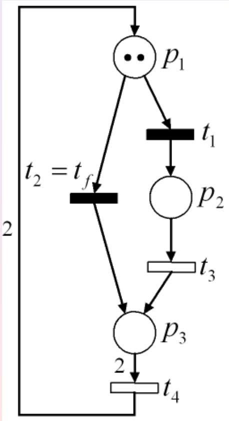


Diagnosable and undetectable net



- It is still not possible to distinguish between the firing of t_3 and t_4, hence the language is undetectable.
- The language is diagnosable. Indeed after the firing of t_f all the possible continuations are given by $\ldots t_f t_6 (t_1 t_2)^*$.

Detectable net



Ongoing works

- An updated version of the fault detection algorithm based on g-markings, which includes the present results, has been published in Basile et al., IEEE Trans. Aut. Contr., Apr. 2009
- We have proposed a new approach for fault diagnosis based on ILPs without using the g-markings (see Basile et al., IFAC DCSD 2009, Jun. 2009). In this case the detectability assumption is no more needed
- We are now working on the identification issue to face the problem of fault diagnosis when the fault are not modeled (see Basile et al., 14^{th} IEEE ETFA, Sep. 2009)

. . . The End

Thank you!