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

F. Basile\textsuperscript{1}  P. Chiacchio\textsuperscript{1}  G. De Tommasi\textsuperscript{2}

\textsuperscript{1}Università di Salerno, Italy  
\textsuperscript{2}Università di Napoli “Federico II”, Italy

IFAC SAFEPROCESS 2009, Barcelona, Spain
1. Preliminaries

2. Motivation

3. Contribution
   - Examples

4. Ongoing works
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
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\textsuperscript{th} IEEE CDC, Boel and Jiroveanu, 16\textsuperscript{th} Symp. Math Theory Networks Syst.).

Explosion of the state space estimation
Fault diagnosis and prognosis in Petri Nets by using a single generalized marking estimation

Preliminaries

Explosion of the state space estimation

\[ m_0 = \begin{bmatrix} 2 & 0 & 0 & 2 & 0 & 0 & 0 \end{bmatrix}^T \] - \( t_1 \) fires.
Unobservable Reach (as called in Genc and Lafortune)

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

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

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

$$\mu = [1 \ 2 \ 0 \ 2 \ 0 \ 0 \ -1]^T.$$ 

As far as the fault diagnosis is concerned, $\mu$ 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

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)

\[ \mu_0 = m_0 = [0 \ 0 \ 1 \ 1]^T \]

\( t_1, t_2, t_3 \) 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
After the firing of $\sigma = t_2$, the generalized marking estimation becomes $\mathbf{\mu}_1 = [-1 \ 0 \ 1 \ 1]^T$.
The negative component of $\mathbf{\mu}_1$ means that either $t_4$ or $t_5$ should have fired in order to explain the observed firing.
If \( t_3 \) does not fire, it is impossible to find any sufficiently long continuation of \( \sigma \) 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).
Let $\Sigma(\mu_1)$ be the set of all the possible firing count vectors $\epsilon$ corresponding to sequences of unobservable transitions enabled under $\mu_1$,

$$\max_{\epsilon \in \Sigma(\mu_1)} \epsilon(t_{f_2}) = 0,$$

meaning that the fault $t_{f_2}$ has not occurred for sure (and it cannot occur in the future).
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.
If the firing of $t_1$ is observed $\mu_2 = \mu_0$ is reached we erroneously get

$$\max_{\epsilon \in \Sigma(\mu_2)} \epsilon(t_{f_2}) = 1,$$

meaning that $t_{f_2}$ may occur.
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


\( N = (P, T, \text{Pre}, \text{Post}) \) 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 \( s \).

\( Pr^{-1}_L \) is the inverse projection operator defined as

\[
Pr^{-1}_L(r) = \{ s \in L \ \text{s.t.} \ Pr(s) = r \}.
\]

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

\[
\Psi(\tau_{f_i}) = \{ s \dot{t} \in L \ \text{s.t.} \ \dot{t} = \tau_{f_i} \}.
\]
Diagnosable language - Definition

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

$$\forall \ t_f \ni h_i \in \mathbb{N} \text{ such that the following holds}$$

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

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

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

$$r \in Pr_{L}^{-1}(Pr(sq)) \Rightarrow t_f_i \in r.$$
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
\[
\min_{\epsilon \in \Sigma(N,\mu)} \epsilon(t_{f_i}) > 0,
\]
with $\mu_0[z] \mu$, 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

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

with $\mu_0[\beta]|\mu''$, 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
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\textsuperscript{th} IEEE ETFA, Sep. 2009).
Fault diagnosis and prognosis in Petri Nets by using a single generalized marking estimation

Ongoing works

... The End

Thank you!