Modular fault diagnosis in discrete-event systems with a CPN diagnoser

Yannick Pencolé, Romain Pichard, Pierre Fernbach

DISCO Team (Diagnosis and Supervisory COntrol)
CNRS-LAAS, Université de Toulouse, FRANCE

September 2, 2015
Introduction

- Fault diagnosis in discrete event systems
  - Given a discrete event system and its model, a set of anticipated faults and a sequence of observations of the system
  - Determine whether a set of faults occurred in the system
- Problem initially introduced within the automaton formalism
- **Contrib 1**: Starting from a Petri net model:
  - how to compute a *Petri net* Diagnoser:
  - as efficient as the diagnoser automaton of [Sampath 95]
  - as precise (belief state + fault)
  - that is not any kind of reachable marking graph
  - and smaller (a proper Petri Net)
- **Contrib 2**: Application: how to design a modular diagnosis system with help of this Petri net diagnoser.
- Use of Coloured Petri Net (CPN)
A DES is modelled here as:

\[ S = \langle P, T, A, \ell, \Sigma, M_0 \rangle \]

- \( \langle P, T, A, M_0 \rangle \) is a marked Petri net;
- \( \Sigma \) is the set of transition labels;
- \( \ell : T \rightarrow \Sigma \) is the label mapping.
Diagnosis problem

- $S$ be a model of a discrete event system,
- $\sigma = \sigma'.o, \sigma' \in \Sigma^*_o, o \in \Sigma_o$ be an observable sequence of the system,
- the diagnosis of $\sigma$ in $S$, denoted $\Delta(S, \sigma)$ is the maximal set $\{(M_1, F_1), \ldots, (M_n, F_n)\}$ such that:
  1. if $\sigma$ is empty, $\Delta(S, \sigma) = \{(M_0, \emptyset)\}$;
  2. if $\sigma$ is not empty, then for any $i \in \{1, \ldots, n\}$ there exists at least a firable sequence

$$M_0 \xrightarrow{t_1i} \cdots \xrightarrow{t_{ki}} M_i$$

such that

$$\bigcup_{j=1}^{k} \ell(t_{ji}) \cap \Sigma_f = F_i$$

and

$$\mathbb{P}(\ell(t_{1i}) \cdot \ell(t_{2i}) \cdots \ell(t_{ki})) = \sigma$$

with $\ell(t_{ki}) = o$.

This problem is equivalent to the one of [Sampath 1995] but based on bounded Petri nets.
Examples

- $\Delta(S, \varepsilon) = \{(2p_1, \emptyset)\}$,
- $\Delta(S, o_1) = \{(2p_2, \emptyset)\}$,
- $\Delta(S, o_2 o_2) = \{(2p_2, \{f\}), (2p_2, \emptyset), (2p_1, \{f\}), (p_1 p_2, \{f\})\}$. 
Examples : extended version

\[\Delta^+(S, \varepsilon) = \{(2p_1, \emptyset), (p_1p_2, \{f\}), (2p_2, \{f\})\},\]
\[\Delta^+(S, o_1) = \{(2p_2, \emptyset)\},\]
\[\Delta^+(S, o_2o_2) = \{(2p_2, \{f\}), (2p_2, \emptyset), (2p_1, \{f\}), (p_1p_2, \{f\})\}.$$
Classical diagnoser [Sampath 95]
How to get a proper Petri-net diagnoser?

- Classical diagnoser: a deterministic automaton based on the reachable marking graph of the model. Combinatorial Explosion.
- Petri-diagnoser:
  - is it possible to design a proper Petri net that solves the diagnosis problem
  - as precise as the Sampath’s diagnoser (belief state + possible faults)
  - as efficient as the Sampath’s diagnoser (one observable = one triggering of transitions)
Our proposal: a CPN diagnoser

- one place = one diagnosis candidate (belief state + faults)
- one structural transition = one observation type
- colours: encoding of belief state transitions
Equivalent Coloured diagnoser
Coloured diagnoser
Coloured diagnoser

\[ 2p_1 \rightarrow p_1 p_2 f \rightarrow 2p_2 \rightarrow 2p_2 f \rightarrow 2p_1 f \rightarrow p_1 p_2 \rightarrow t_{o1} \rightarrow t_{o2} \]
Coloured diagnoser
Comparative analysis

- The coloured diagnoser solves the same problem as the classical diagnoser with same efficiency.

- Graphical viewpoint:

<table>
<thead>
<tr>
<th></th>
<th>Classical</th>
<th>Coloured</th>
</tr>
</thead>
<tbody>
<tr>
<td>state representation</td>
<td>$o(2^{2</td>
<td>P</td>
</tr>
<tr>
<td>transition representation</td>
<td>$o(2^{2</td>
<td>P</td>
</tr>
</tbody>
</table>

- Colours: $o(2^{2|P| \times 2^{|\Sigma_f|}})$. 
Modular diagnosis:
- determine the module belief state + module faults
- for each module
- the module diagnosis must be globally consistent

Usually solved with a set of automata (modular diagnosers)

Proposal: Implementation of the modular diagnosis problem with ONE CPN
Notion of modules

- subset of places and transitions (usually a component or a set of components)
- shared resources: transitions only (event synchronisation, communication)
- Assumption here: shared transitions are observable (to get global-consistency [Pencolé SAFE06] for free)
- Sound decomposition of the Petri model: set of modules
Modular system

Sound decomposition
Modular diagnoser, module 1
Modular diagnoser, module 1

\[ p_0 \]

\[ d_2 \quad d_1 \quad a \]

\[ f_1 \quad p_2 \quad p_1 \]

\[ p_0 \]

\[ a \]
Modular diagnoser, module 1
Modular diagnoser, module 1
Modular diagnoser, module 1
Modular diagnoser, module 1
Modular diagnoser, module 1

\[ \begin{aligned} p_0 & \xrightarrow{d_2} p_2 \\
p_2 & \xrightarrow{d_1} p_1 \\
f_1 & \xrightarrow{a} p_1 \\
 \end{aligned} \]
Modular diagnoser, module 2
New observation : $b_1$?
Modular coloured diagnoser

Observation: \( b_1 \)

\[
\Delta^+(S, b_1) = \{(p_0, p_4, f_2), (p_0, p_3, f_2)\}
\]

\[
\Delta_{M}(S, b_1) = \Delta^+(S_1) = \{(p_0)\} \land \Delta^+(S_2) = \{(p_4, f_2), (p_3, f_2)\}
\]
Observation: $b_1$ followed by $a$

$$\Delta^+(S, b_1 a) = \{(p_1 p_3, f_2), (p_2 p_3, f_1 f_2)\}$$

$$\Delta_M(S, b_1 a) = \Delta^+(S_1) = \{(p_1), (p_2, f_1)\} \land \Delta^+(S_2) = \{(p_3, f_2)\}$$
Conclusion

- Design of a CPN diagnoser
- as precise, complete as the Sampath’s diagnoser
- but it is still a Petri-net and can be used as it
- definitely smaller in terms of place and transition (graphical viewpoint)
- as an application, modular diagnosis system
- just by synchronising shared observable transitions
- some perspectives:
  - coordination protocols [Debouk00] with CPN diagnosers.
  - discriminability analysis of the CPN net structure.
  - problem abstractions
  - deploying and embedding on hardwares (micro-controllers...)

---