Diagnosis (09)
Uncertainties on the Observations

Alban Grastien
alban.grastien@rsise.anu.edu.au
Uncertainties on the Observations

- Partial order
- Loss of observations
- Sensor or channel failures
- Uncertainty on the message
- Masking

Monitoring system
Modelling Uncertainties in the System

Solution
Each communication channel between the system to diagnose and the monitoring system is modelled as a component of the system.

Problems
- A single buffer for one observation on a component that can emit $k$ different observations requires $k$ states: the size of the global model is multiplied by $k$ for only one buffer!
- We usually have information about delays between emissions and receptions of observations: do we have to use timed automata?
- We do not want to diagnose the communication channels (otherwise, they would be part of the system).
Partially Ordered Sets

Partial Order

A partially ordered set is a pair $\langle E, \prec \rangle$ so that:

- $\forall e \in E, \ e \n prec \ e$
- $\forall e_1 \in E, \forall e_2 \in E, \ e_1 \prec e_2 \Rightarrow e_2 \n prec \ e_1$
- $\forall e_1 \in E, \forall e_2 \in E, \forall e_3 \in E, \ e_1 \prec e_2 \land e_2 \prec e_3 \Rightarrow e_1 \prec e_3$

Pencolé et al.

- The observations are a partial order set.
- A state of the diagnosis automaton is a pair $\langle s, o \rangle$ where $s$ is a possible state of the system and $o$ is a possible prefix of a sequence compatible with the observations.
Example

Possible Sequences

- $\langle o_1, o_1, o_2, o_1, o_3 \rangle$
- $\langle o_1, o_2, o_1, o_1, o_3 \rangle$
- $\langle o_2, o_1, o_1, o_1, o_3 \rangle$
Deals both with partial order and uncertain observations

Observations

- The observation (without s) is a partially ordered set of observation fragments.
- An observation fragment $N$ has a subset of $O \cup \{\emptyset\}$:
  - if $e \in N$, then $e$ is one of the observable events that possibly generated the observation fragment.
  - if $\emptyset \in N$, then possibly no observable event generated the observation fragment.
Example

Observation

Index Space
Diagnosis

- A Silent Closure of $s$ is the sub automaton that can be reached from the state $s$ with unobservable transitions.

- A Diagnosis State is a pair $\langle s, I \rangle$ where $s$ is a system state and $I$ is an index.

- There is a transition from $\langle s, I \rangle$ to $\langle s', I' \rangle$ labeled by $e$ if:
  - there exists a state $s''$ in the silent closure of $s$ so that there is a transition from $s''$ to $s'$ labeled by $e$, and
  - there is a transition from $I$ to $I'$ labeled by $e$ on the index space.

- Moreover, with each state is associated a diagnosis (a set of sets of fault modes).
Observation Automaton

- $OBS = \langle Q, E, T, I, F \rangle$
- Each trajectory on $OBS$ ending in a state $F$ is a possible sequence of emitted observations consistent with the observations received.
What You Can Model With Automata

- Partial Order
- Uncertainty
- Loss of observations
- Sensor failure
- Masking
Let $A_1 = \langle Q_1, E_1, T_1, I_1, F_1 \rangle$ and $A_2 = \langle Q_2, E_2, T_2, I_2, F_2 \rangle$ be two automata. The synchronisation $A_1 \otimes A_2$ is an automaton $A = \langle Q, E, T, I, F \rangle$ so that:

- $Q = Q_1 \times Q_2$
- $E = E_1 \cup E_2$
- $T = \{ \langle \langle s_1, s_2 \rangle, e, \langle s'_1, s'_2 \rangle \rangle \mid$
  
  \hspace{1cm} (e \in E_1 \land \langle s_1, e, s'_1 \rangle \in T_1) \lor (e \notin E_1 \land s_1 = s'_1) \land$
  
  \hspace{1cm} (e \in E_2 \land \langle s_2, e, s'_2 \rangle \in T_2) \lor (e \notin E_2 \land s_2 = s'_2) \}$
- $I = I_1 \times I_2$
- $F = F_1 \times F_2$
Diagnosis by Observation Automaton

- $MOD$ is an automaton that models the system (all the states are final)
- $OBS$ is the observation automaton
- the diagnosis automaton is defined by $MOD \otimes OBS$

When the diagnosis automaton is computed, the diagnosis can be easily retrieved