Diagnosis of Discrete-Event Systems

Alban Grastien

Australian Government
Department of Broadband, Communications and the Digital Economy
Australian Research Council

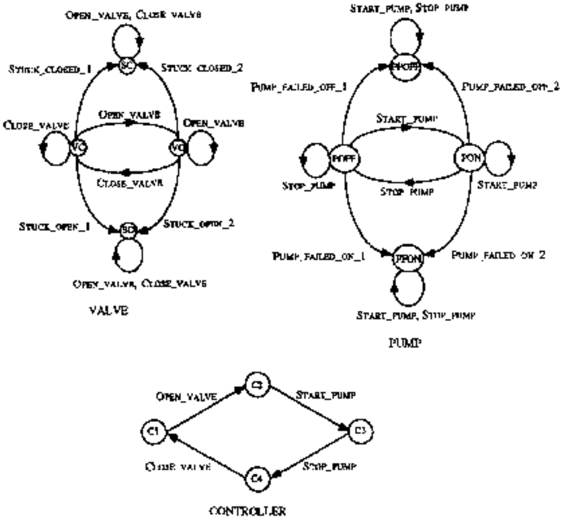
NICTA Funding and Supporting Members and Partners

Discrete-Event Systems

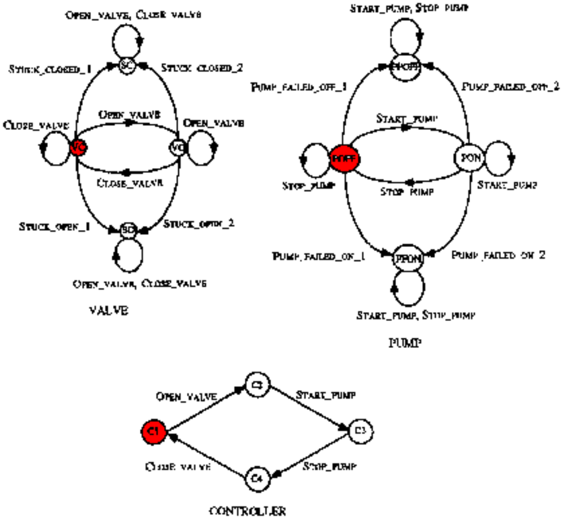
Systems that are

1. dynamic (the state of the system changes over time)
2. modeled at a discrete level (no continuous variable)

Example: HVAC

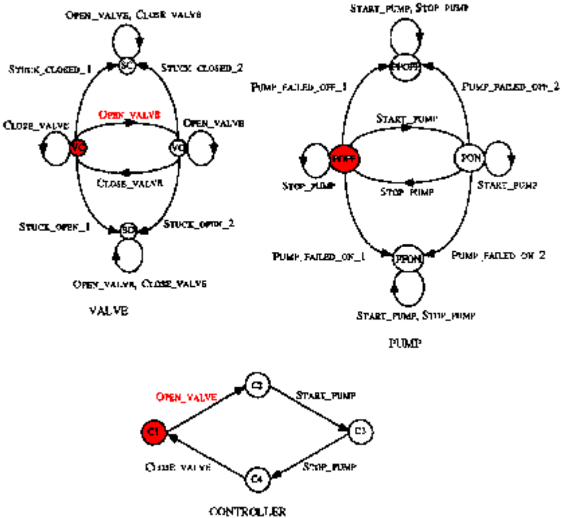


Example: HVAC



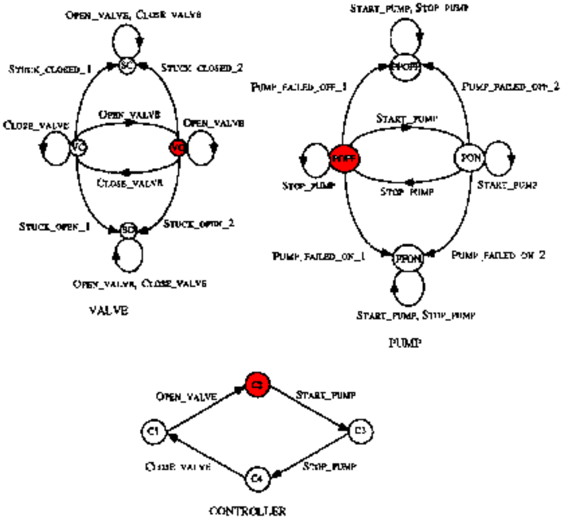
State of the system

Example: HVAC



Occurrence
of event
`Open valve`

Example: HVAC



New state

Language Framework

Let Σ be the set of events:

- a behaviour is a word on Σ (sequence of events, called trajectory): $\beta \in \Sigma\star$
- the model is a language: $\mathcal{L}_M \subseteq \Sigma\star$

Example:

- $\Sigma = \{a, b, c\}$
- $\beta = aaca$
- $\mathcal{L}_M = \{a, aa, ab, aac, abc, acc, aaca, abca, abcc \ldots\}$

Some events $\Sigma_o \subseteq \Sigma$ of events are observable
(sensors, commands, alarms, etc.)

When an observable event occurs, it is recorded.

The observation of a trajectory is the projection of the trajectory over the observable events (eliminate the unobservable events of the trajectory)

$$obs(traj) \in \Sigma_o\star$$

Fault

A subset of unobservable events $\Sigma_f \subseteq (\Sigma \setminus \Sigma_o)$ are called faulty

The "faulty state" of a trajectory is the set of faulty events that occur on the trajectory:

$$\delta(\mathit{traj}) \subseteq \Sigma_f$$

System execution traj^* (unknown)

Diagnosis problem:

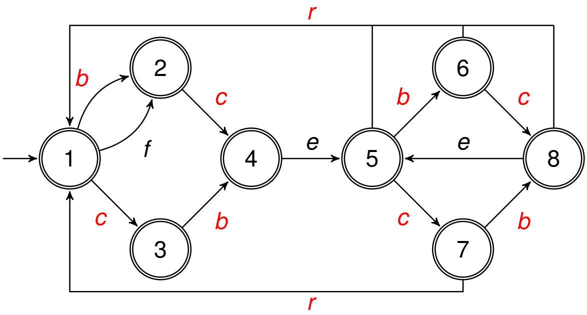
$$P = \langle \mathcal{L}_M, \Sigma_o, \mathit{obs}(\mathit{traj}^*), \Sigma_f \rangle$$

Diagnosis of DES: $\delta(\mathit{traj}^*)$ (impossible to find, in general)

Assuming the model is complete ($\mathit{traj} \in \mathcal{L}_M$),
then $\delta(\mathit{traj}^*) \in \Delta(P)$ where

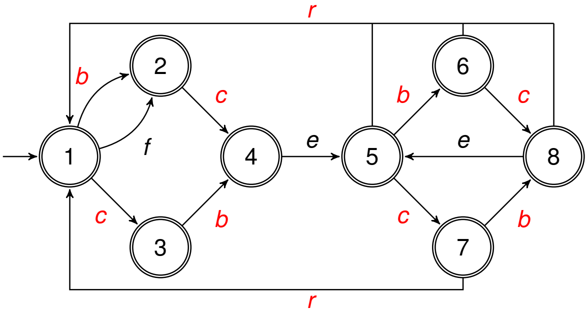
$$\Delta(P) = \{F \subseteq \Sigma_f \mid \exists \mathit{traj} \in \mathcal{L}_M.\ \mathit{obs}(\mathit{traj}) = \mathit{obs}(\mathit{traj}^*) \wedge \delta(\mathit{traj}) = F\}$$

Examples



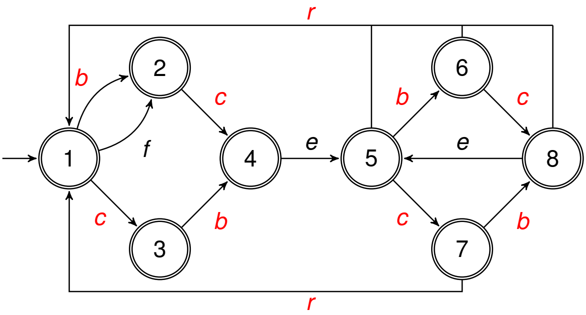
- $traj^* = bcebc$
- Observation: *bcbc*
- $\delta(traj^*) = \emptyset$

Examples



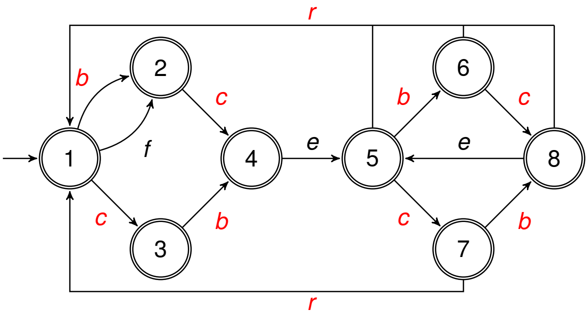
- $traj^* = bcebc$
- Observation: *bcbc*
- $\delta(traj^*) = \emptyset$
- Nominal: $traj_N = bcebc$
- Faulty: no faulty $traj_F$!
- $\Delta = \{\emptyset\}$

Examples



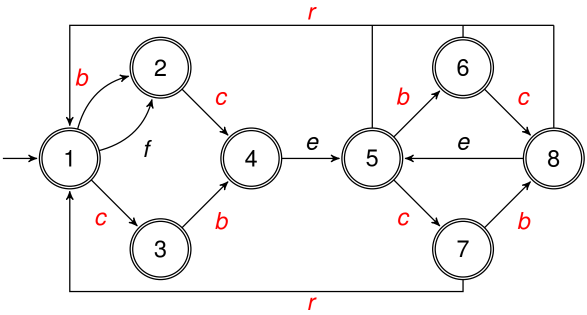
- $traj^* = fcebc$
- Observation: *cbc*
- $\delta(traj^*) = \{F\}$

Examples



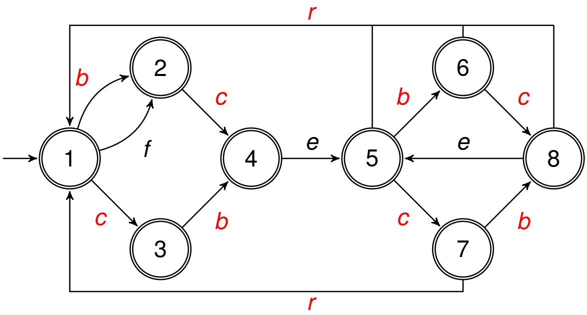
- $traj^* = fcebc$
- Observation: *cbc*
- $\delta(traj^*) = \{F\}$
- Nominal: $traj_N = cbec$
- Faulty: $traj_F = fcebc$
- $\Delta = \{\emptyset, \{F\}\}$

Examples



- $traj^* = fcecb$
- Observation: *ccb*
- $\delta(traj^*) = \{F\}$

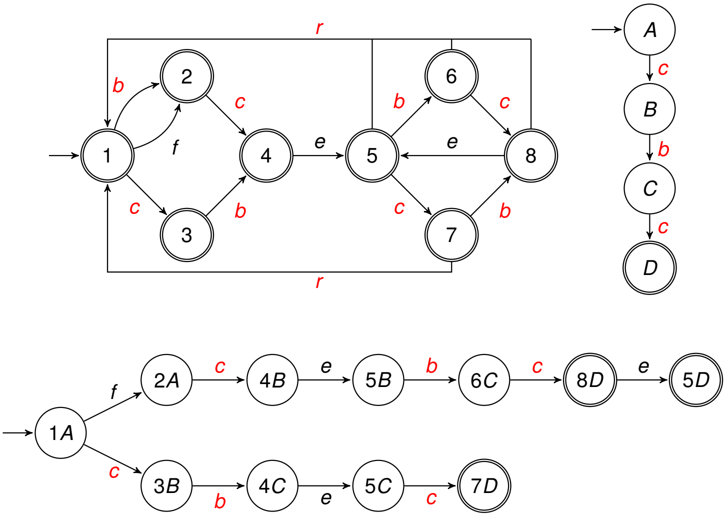
Examples



- $traj^* = fcecb$
- Observation: *ccb*
- $\delta(traj^*) = \{F\}$
- Nominal: no nominal $traj_N$
- Faulty: $traj_F = fcecb$
- $\Delta = \{\{F\}\}$

How to Compute the Diagnosis

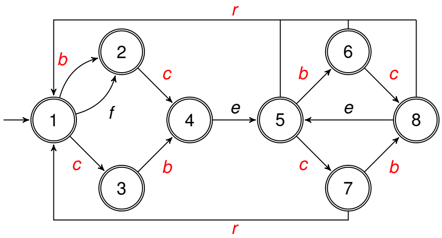
- Represent the observation as an automaton
- Synchronise the model and the observation
- Check whether one/all trajectories contains a faulty event



r
b
2
c
f
1
4
e
5
b
6
c
e
8
c
3
b
c
7
b
r
A
c
B
b
C
c
D
f
2A
c
4B
e
5B
b
6C
c
8D
e
5D
1A
c
3B
b
4C
e
5C
c
7D

Symbolic Representation of States

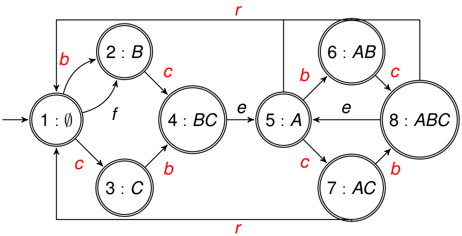
State Variables



Define a set V of Boolean properties (state variables) such that each state of the DES is associated with a different set of properties.

Symbolic Representation of States

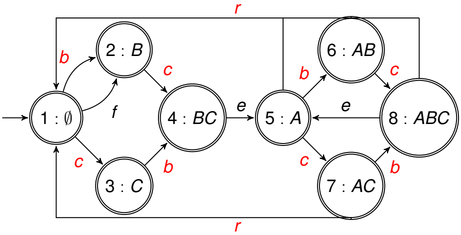
State Variables



Define a set V of Boolean properties (state variables) such that each state of the DES is associated with a different set of properties.

Here: $V = \{A, B, C\}$

	1	2	3	4	5	6	7	8
A					Y	Y	Y	Y
B		Y		Y		Y		Y
C			Y	Y			Y	Y

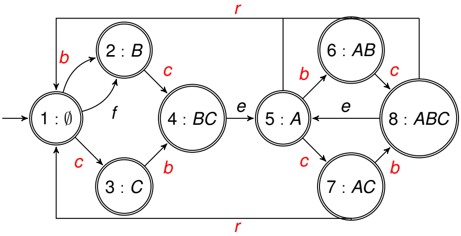


A state is represented by a propositional formula:

- $\Phi_1 = \neg A \wedge \neg B \wedge \neg C$
- $\Phi_2 = \neg A \wedge B \wedge \neg C$
- $\Phi_3 = \neg A \wedge \neg B \wedge C$
- $\Phi_4 = \neg A \wedge B \wedge C$
- $\Phi_5 = A \wedge \neg B \wedge \neg C$
- $\Phi_6 = A \wedge B \wedge \neg C$
- $\Phi_7 = A \wedge \neg B \wedge C$
- $\Phi_8 = A \wedge B \wedge C$

Symbolic Representation of States

Set of States Representation



A set of states is represented by the disjunction of the representations of states.

E.g.:

- $\Phi_{\{1\}} = \Phi_1 = \neg A \wedge \neg B \wedge \neg C$
- $\Phi_{\{1,3\}} = \Phi_1 \vee \Phi_3 = (\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C) = \neg A \wedge \neg B$
- $\Phi_{\{1,3,5,7\}} = \Phi_1 \vee \Phi_3 \vee \Phi_5 \vee \Phi_7 = \neg B$

Symbolic Representation of States

Operations on Sets (of States)

1. Union $S_1 \cup S_2$

Symbolic Representation of States

Operations on Sets (of States)

1. Union $S_1 \cup S_2$ $\Phi_{S_1} \vee \Phi_{S_2}$
2. Intersection $S_1 \cap S_2$

Symbolic Representation of States

Operations on Sets (of States)

1. Union $S_1 \cup S_2$ — $\Phi_{S_1} \vee \Phi_{S_2}$
2. Intersection $S_1 \cap S_2$ — $\Phi_{S_1} \wedge \Phi_{S_2}$
3. (Relative) Complement $Q \setminus S$

Symbolic Representation of States

Operations on Sets (of States)

1. Union $S_1 \cup S_2$ $\Phi_{S_1} \vee \Phi_{S_2}$
2. Intersection $S_1 \cap S_2$ $\Phi_{S_1} \wedge \Phi_{S_2}$
3. (Relative) Complement $Q \setminus S$ $\Phi_Q \wedge \neg\Phi_S$
4. Emptiness $S \stackrel{?}{=} \emptyset$

Symbolic Representation of States

Operations on Sets (of States)

1. Union $S_1 \cup S_2$ — $\Phi_{S_1} \vee \Phi_{S_2}$
2. Intersection $S_1 \cap S_2$ — $\Phi_{S_1} \wedge \Phi_{S_2}$
3. (Relative) Complement $Q \setminus S$ — $\Phi_Q \wedge \neg \Phi_S$
4. Emptiness $S \stackrel{?}{=} \emptyset$ — $\Phi_S \stackrel{?}{\equiv} \bot$
5. Inclusion $S_1 \stackrel{?}{\subseteq} S_2$

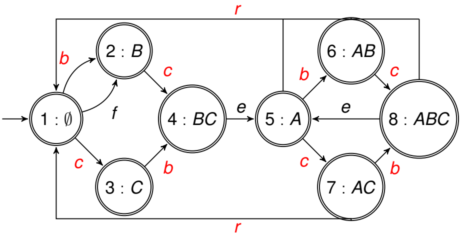
1. Union $S_1 \cup S_2$ — $\Phi_{S_1} \vee \Phi_{S_2}$
2. Intersection $S_1 \cap S_2$ — $\Phi_{S_1} \wedge \Phi_{S_2}$
3. (Relative) Complement $Q \setminus S$ — $\Phi_Q \wedge \neg\Phi_S$
4. Emptiness $S \stackrel{?}{=} \emptyset$ — $\Phi_S \stackrel{?}{\equiv} \bot$
5. Inclusion $S_1 \stackrel{?}{\subseteq} S_2$ — $\Phi_{S_1} \wedge \neg\Phi_{S_2} \stackrel{?}{\equiv} \bot$
6. Overlap $S_1 \cap S_2 \stackrel{?}{=} \emptyset$

Symbolic Representation of States

Operations on Sets (of States)

1. Union $S_1 \cup S_2$ — $\Phi_{S_1} \vee \Phi_{S_2}$
2. Intersection $S_1 \cap S_2$ — $\Phi_{S_1} \wedge \Phi_{S_2}$
3. (Relative) Complement $Q \setminus S$ — $\Phi_Q \wedge \neg\Phi_S$
4. Emptiness $S \stackrel{?}{=} \emptyset$ — $\Phi_S \stackrel{?}{\equiv} \bot$
5. Inclusion $S_1 \stackrel{?}{\subseteq} S_2$ — $\Phi_{S_1} \wedge \neg\Phi_{S_2} \stackrel{?}{\equiv} \bot$
6. Overlap $S_1 \cap S_2 \stackrel{?}{=} \emptyset$ — $\Phi_{S_1} \wedge \Phi_{S_2} \stackrel{?}{\equiv} \bot$

Symbolic Representation of Transitions



- Create "next" (primed) properties: $V' = \{A', B', C'\}$
- Create event variables: $V_\Sigma = \{b, c, r, e\}$

Transition $\langle 1, b, 2 \rangle$:

- $(\neg A \wedge \neg B \wedge \neg C) \wedge (b \wedge \neg c \wedge \neg r \wedge \neg e) \wedge (\neg A' \wedge B' \wedge \neg C')$

All transitions of event b:

- $(A \leftrightarrow A') \wedge (\neg B \wedge B') \wedge (C \leftrightarrow C') \wedge (b \wedge \neg c \wedge \neg r \wedge \neg e)$

Set of transitions labeled by event e

Set of transitions labeled by event e

$$\Phi_T \wedge e$$

Set of transitions labeled by an event $e \in \Sigma'$

Set of transitions labeled by event e

$$\Phi_T \wedge e$$

Set of transitions labeled by an event $e \in \Sigma'$

$$\Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right)$$

Subset of transitions from τ originating from a state of S

Set of transitions labeled by event e

$$\Phi_T \wedge e$$

Set of transitions labeled by an event $e \in \Sigma'$

$$\Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right)$$

Subset of transitions from τ originating from a state of S

$$\Phi_\tau \wedge \Phi_S$$

Set of targets of a set τ of transitions

Set of transitions labeled by event e

$$\Phi_T \wedge e$$

Set of transitions labeled by an event $e \in \Sigma'$

$$\Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right)$$

Subset of transitions from τ originating from a state of S

$$\Phi_\tau \wedge \Phi_S$$

Set of targets of a set τ of transitions

$$(\exists V.\ \exists V_\Sigma.\ \Phi_\tau)\,[V'/V]$$

1. The set of states reached from S through a single transition labeled by an event of Σ'

1. The set of states reached from S through a single transition labeled by an event of Σ'

$$\left(\exists V.\, \exists V_{\Sigma}.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e\right) \wedge \Phi_S\right)[V'/V]$$

2. The set of states reached from S through exactly two transitions labeled by events of Σ'

1. The set of states reached from S through a single transition labeled by an event of Σ'

$$\left(\exists V.\, \exists V_{\Sigma}.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e\right) \wedge \Phi_S\right)[V'/V]$$

2. The set of states reached from S through exactly two transitions labeled by events of Σ'

$$\left(\exists V.\, \exists V_{\Sigma}.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e\right) \wedge \left(\exists V.\, \exists V_{\Sigma}.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e\right) \wedge \Phi_S\right)[V'/V]\right.$$

1. The set of states reached from S through a single transition labeled by an event of Σ'

$$\left(\exists V.\ \exists V_\Sigma.\ \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right) \wedge \Phi_S \right) [V' / V]$$

3. The set of states reached from S through zero or one transition labeled by an event of Σ'

Symbolic Representation of Automata

1. The set of states reached from S through a single transition labeled by an event of Σ'

$$\left(\exists V.\ \exists V_\Sigma.\ \Phi_T \wedge \left(\bigvee_{e\in\Sigma'} e\right) \wedge \Phi_S\right)[V'/V]$$

3. The set of states reached from S through zero or one transition labeled by an event of Σ'

$$\Phi_S \vee \left(\exists V.\ \exists V_\Sigma.\ \Phi_T \wedge \left(\bigvee_{e\in\Sigma'} e\right) \wedge \Phi_S\right)[V'/V]$$

The set of states reached from S through any number of transitions labeled by events of Σ'

The set of states reached from S through any number of transitions labeled by events of Σ'

$$\mu Z.\Phi_S \vee \left(\exists V.\, \exists V_\Sigma.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right) \wedge Z \right) [V'/V]$$

Symbolic Representation of Automata

The set of states reached from S through any number of transitions labeled by events of Σ'

$$\mu Z.\Phi_S \vee \left(\exists V.\, \exists V_\Sigma.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right) \wedge Z \right) [V'/V]$$

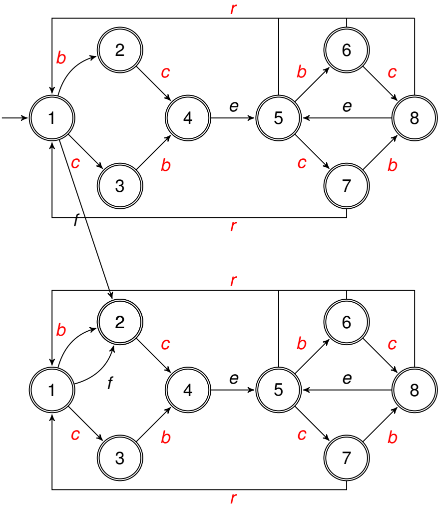
Implementation

$\Phi := \Phi_S$
$\Phi' := \Phi$
repeat
  $\Phi := \Phi'$
  $\Phi' := \Phi \vee \left(\exists V.\, \exists V_\Sigma.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma'} e \right) \wedge \Phi \right) [V'/V]$
until $\Phi = \Phi'$

Create 2^n copies of the model, where n is the number of faults

Let $Q_{obs(traj^*)}$ be the set of states q such that $I \xrightarrow{obs(traj^*)} q$, then

$$F \in \Delta(obs(traj^*)) \Leftrightarrow Q_F \cap Q_{obs(traj^*)} \neq \emptyset$$



r
b
2
c
6
b
c
1
4
e
5
e
8
c
b
c
b
3
7
f
r
r
b
2
c
6
b
c
1
f
4
e
5
e
8
c
b
c
b
3
7
r

NICTA

- Initial set S_0^+ of states:
  - $\{I\}$
- Set S_0^- of states before first observation:
  - Set of states reached from S_0^+ through unobservable transitions
- Set S_1^+ of states after first observation:
  - Set of states reached from S_0^- through a transition labeled by o_1

...

- Set S_i^+ of states after ith observation:
  - Set of states reached from S_{i-1}^- through a transition labeled by o_i
- Set S_i^- of states before $i+1$th observation:
  - Set of states reached from S_i^+ through unobservable transitions

Is the fault set F part of the diagnosis?

$S := \{I\}$
for all Observation fragment o_i from $obs(traj^*)$ **do**
  $S := \{q' \in Q \mid \exists w \in (\Sigma \setminus \Sigma_o)\star\,.\ \exists q \in S.\ q \xrightarrow{w} q'\}$
  $S := \{q' \in Q \mid \exists q \in S.\ q \xrightarrow{o} q'\}$.
end for
return $S \cap Q_F \overset{?}{\neq} \emptyset$

Is the fault set F part of the diagnosis?

$\Phi := \Phi_I$
for all Observation fragment o_i from $obs(traj^*)$ **do**
$\quad \Phi := \mu Z.\Phi \vee \left(\exists V.\, \exists V_\Sigma.\, \Phi_T \wedge \left(\bigvee_{e \in \Sigma \setminus \Sigma_o} e\right) \wedge Z\right)[V'/V]$
$\quad \Phi := (\exists V.\, \exists V_\Sigma.\, \Phi_T \wedge o \wedge \Phi)\,[V'/V]$
end for
return $\Phi \wedge \Phi_F \overset{?}{\not\equiv} \bot$