Solving Diagnosability of Hybrid Systems via Abstraction and Discrete-Event Techniques:
Alban Grastien, Louise Travé-Massuyès, and Vicenç Puig

www.csiro.au
Diagnosability of Hybrid Systems

Problem Definition

A **hybrid system** is a system that involves both continuous (state) and discrete (mode) dynamics.

We assume a strong-fault model (some knowledge on the faulty behaviour).

A system is **diagnosable** if the occurrence of every fault can always be detected and identified by an observer.
Our Contributions

Diagnosability of HS with DES Techniques:

• We discretise the system.

• We use DES techniques to prove diagnosability.

• We use an incremental approach to identify the minimal amount of information necessary for diagnosability.
Outline

Running Example

Discretisation of Hybrid Systems
  The General Idea
  Discernibility
  Ephemerality
  Diagnosability of DES

Incremental Approach

Concluding Remarks
An Example

Observations: $y = x, \dot{y} = \dot{x}$
Outline

Running Example

Discretisation of Hybrid Systems
   The General Idea
   Discernibility
   Ephemerality
   Diagnosability of DES

Incremental Approach

Concluding Remarks
General Idea

Diagnosability undecidable

$\Rightarrow$

Diagnosability decidable

$D_H^\infty$ diagnosable $\Rightarrow H$ diagnosable
Discretisation from $H$ to $D^\infty_H$

How to compute $D^\infty_H$:

- Keep the set of modes and transitions (including loops on every mode)

- Compute **discernibility** between modes (discretise the observation)

- Compute **ephemerality** of sets of modes
Two modes $m_1$ and $m_2$ are **discernible** if the observations always allow to determine that you are not in $m_2$ when you are in $m_1$ (and vice-versa)
An **indicator** is a constraint on the observable variables.

Three possible interactions between a mode and an indicator:
- the indicator *always* holds in the mode
- the indicator *never* holds in the mode
- the indicator *sometimes* holds in the mode
If an indicator
• always holds in $m_1$ and
• never holds in $m_2$
then $m_1$ and $m_2$ are discernible.
Example

Discernibility (1/4)

Observations: $y = x$, $\dot{y} = \dot{x}$
Example
Discernibility (2/4)

- \( indi_1: \dot{y} + y = 100 \) (derived from mode \( N1 \))
- \( indi_2: \dot{y} + y = 90 \) (mode \( N2 \))
- \( indi_3: \dot{y} + y = 0 \) (mode \( N3 \))
- \( indi_4: \dot{y} + y \in [95, 105] \) (mode \( F1 \))
- \( indi_5: \dot{y} + y \in [85, 89] \) (mode \( F2 \))
- \( indi_6: \dot{y} + y \in [45, 50] \) (mode \( F3 \))
Example
Discernibility (3/4)

Indicator function:

1: the indicator is always satisfied in this mode
−1: the indicator is never satisfied in this mode
0: the indicator is sometimes satisfied in this mode

<table>
<thead>
<tr>
<th></th>
<th>N1</th>
<th>N2</th>
<th>N3</th>
<th>F1</th>
<th>F2</th>
<th>F3</th>
</tr>
</thead>
<tbody>
<tr>
<td>indi₁</td>
<td>1</td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>indi₂</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>indi₃</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>indi₄</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>indi₅</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>indi₆</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

(−1s not represented)
Example

Discernibility (4/4)

Indiscernibility matrix:

- two modes are discernible if

\[ \{L(m_1, \text{indi}), L(m_2, \text{indi})\} = \{-1, 1\} \]

for some indicator \( \text{indi} \)

<table>
<thead>
<tr>
<th></th>
<th>( N1 )</th>
<th>( N2 )</th>
<th>( N3 )</th>
<th>( F1 )</th>
<th>( F2 )</th>
<th>( F3 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( N1 )</td>
<td>1</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>( N2 )</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( N3 )</td>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>( F1 )</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>( F2 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>( F3 )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

a 1 indicates that the modes are not discernible
Diagnosability of DES

Twin Plant:
• Make a copy $D'$ of $D$
• Remove the faulty modes of $D'$
• Synchronise $D$ with $D'$ (mode-based observations: remove discernible pairs)

A counter-example is a cycle in the twin plant that is
• reachable,
• and ambiguous.

Theorem: If there is no counter-example the DES is diagnosable
Twin Plant for $D_H^\infty$

Running Example

A. Grastien, L. Travé-Massuyès, and V. Puig

Diagnosability of HS via DES
Ephemerality

Issue:

• The discretisation inserts loops on every mode: how do we model the fact that the system cannot stay in this mode?

Definition:

• A set of modes is **ephemeral** if the system cannot stay forever in this set of modes
Ephemerality

Running Example

- In mode $N1$, 
  - Derivative: $\dot{x} = 100 - x \geq 20$
  - Invariant: $x \leq 80$

$\Rightarrow$ eventually the system must leave mode $N1$

{$N1$} is ephemal
Ephemerality
Running Example

- In mode $N_1$,
  - Derivative: $\dot{x} = 100 - x \geq 20$
  - Invariant: $x \leq 80$

$\Rightarrow$ eventually the system must leave mode $N_1$

$\{N_1\}$ is ephemeral

The ephemeral sets include:

- $\{N_1, N_2\}$
- $\{N_3\}$
- $\{F_1, F_2\}$
- $\{F_3\}$. 
Diagnosability of DES $D$

Theory

Twin Plant:

- Make a copy $D'$ of $D$
- Remove the faulty modes of $D'$
- Synchronise $D$ with $D'$ (mode-based observations: remove discernible pairs)

A counter-example is a cycle in the twin plant that is

- reachable,
- fair (non-ephemeral),
- and ambiguous.

Theorem: The DES is diagnosable iff there is no counter-example
Twin Plant for $D_H^\infty$

Running Example

Ambiguous, but ephemeral
Outline

Running Example

Discretisation of Hybrid Systems
  The General Idea
  Discernibility
  Ephemerality
  Diagnosability of DES

Incremental Approach

Concluding Remarks
Motivation

Why Use Incremental Approach?

- Computing all indicators is expensive
  - They are exponentially many
  - Many indicators are useless/redundant

- Computing the ephemeral sets is expensive

- Using all indicators during diagnosis is expensive
  - We want to identify the indicators that are helpful
General Idea

$H \quad \rightarrow \quad \text{Diagnosability undecidable}$

Diagnosability decidable

$D^\infty_H \quad \rightarrow \quad D^\infty_H \text{ diagnosable} \Rightarrow H \text{ diagnosable}$

Counter-example $D^\infty_1$ Non-diagnosable

Counter-example $D^\infty_0$ Non-diagnosable

A. Grastien, L. Travé-Massuyès, and V. Puig

Diagnosability of HS via DES

24/39
General Idea

- Diagnosability undecidable
  - $D_H^\infty$ diagnosable $\Rightarrow H$ diagnosable
- Diagnosability decidable
  - Counter-example
    - $D_H^1$ non-diagnosable
    - Counter-example
      - $D_H^0$ non-diagnosable
0. Maximal Abstraction: $D^0_H$

How to Compute $D^0_H$:

- Keep the modes and transitions (including loops)
- Ignore state dynamics and guards
- No indiscernibility, no ephemerality
0. Twin Plant

Running Example

A. Grastien, L. Travé-Massuyès, and V. Puig

Diagnosability of HS via DES
If the system generates the following faulty behaviour:

\[ b_F = N1 \rightarrow F1(\rightarrow F1)^\infty \]

then the diagnoser might believe that what is happening is:

\[ b_N = N1 \rightarrow N1(\rightarrow N1)^\infty \]
Critical Pair (reminder):

- \( b_F = N1 \rightarrow F1(\rightarrow F1)^\infty \)
- \( b_N = N1 \rightarrow N1(\rightarrow N1)^\infty \)

Answer:

- \( \{F1\} \) is ephemeral, therefore the counter example is not valid.
Back to the General Idea

Diagnosability undecidable

Diagnosability decidable

$D_H^\infty$ diagnosable $\Rightarrow H$ diagnosable

Counter-example

Non-diagnosable

Counter-example

Non-diagnosable

A. Grastien, L. Travé-Massuyès, and V. Puig
Diagnosability of HS via DES
1. New Abstraction: $D^1_H$

Running Example

Known ephemeral sets

• $\{F1\}$
1. Twin Plant

Running Example

Ephemeral

Diagram of the Twin Plant running example with nodes and connections.
1. Counter Example

Running Example

If the system generates the following faulty behaviour:

\[ b_F = N1 \rightarrow F1 \rightarrow F2(\rightarrow F1 \rightarrow F2)^\infty \]

then the diagnoser might believe that what is happening is:

\[ b_N = N1 \rightarrow N1 \rightarrow N1(\rightarrow N1 \rightarrow N1)^\infty \]

Answer:

- It can be shown that \( \{F1, F2\} \) is ephemeral.
2. Twin Plant

Running Example

Diagram:

- Ephemeral together

Nodes: F1N1, F2N1, F3N1, N1N1, N2N1, N3N1
2. Discernibility

Running Example

If the system generates the following faulty behaviour:

$$b_F = N1 \rightarrow F1 \rightarrow F2 \rightarrow F3(\rightarrow F1 \rightarrow F2 \rightarrow F3)\infty$$

then the diagnoser might believe that what is happening is:

$$b_N = N1 \rightarrow N1 \rightarrow N1 \rightarrow N1(\rightarrow N1 \rightarrow N1 \rightarrow N1)\infty$$

Answer:
- Indicator $I1$ always discern $N1$ from $F2$
3. New Abstraction: $D^3_H$

Running Example

**Known ephemeral sets**

- $\{F1, F2\}$
3. New Twin Plant: $D_H^3$

Running Example

New counter example:

- $b_F = N1 \rightarrow F1 \rightarrow F2 \rightarrow F3(\rightarrow F1 \rightarrow F2 \rightarrow F3)^\infty$
- $b_N = N1 \rightarrow N1 \rightarrow N2 \rightarrow N1(\rightarrow N1 \rightarrow N2 \rightarrow N1)^\infty$

etc.
Outline

Running Example

Discretisation of Hybrid Systems
   The General Idea
   Discernibility
   Ephemerality
   Diagnosability of DES

Incremental Approach

Concluding Remarks
Summarising the Approach

- To check diagnosability of hybrid systems, we discretise the hybrid model:
  - we keep the list of modes
  - we keep the list of transitions
  - we infer *ephemerality* properties
  - we infer *discernibility* properties between modes

- We compute a subset of these properties sufficient for diagnosability $\rightarrow$ near-optimal observability
Extensions

• Ephemerality and discernibility.
  How to compute these properties?

• "$D_H^\infty$ not diagnosable" does not imply "$H$ not diagnosable".
  What can we do if $D_H^\infty$ is not diagnosable?

• Symbolic tools.
  Using BDDs to verify diagnosability of networks of systems
  with $> 2^{100}$ modes.