Solving Diagnosability of Hybrid Systems via Abstraction and Discrete-Event Techniques:

Alban Grastien, Louise Travé-Massuyès, and Vicenç Puig

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.

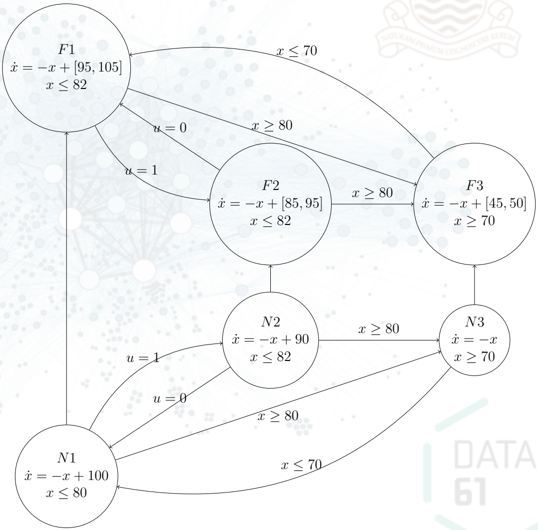
Our Contributions

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

An Example



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

Outline

General Idea

$H \longrightarrow$ Diagnosability undecidable

Diagnosability decidable

D_H^∞

D_H^∞ diagnosable $\Rightarrow$ H diagnosable

Discretisation from H to D_H^∞

How to compute D_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

Discernibility

Definition

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)

Indicators

Definition

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

Discernibility and Indicators

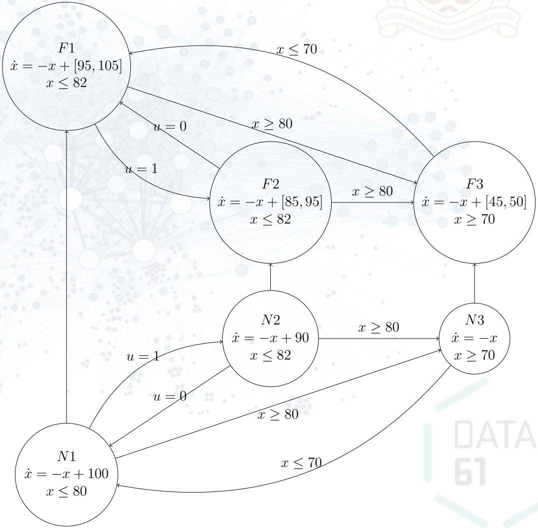
If an indicator

- 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:

$$\begin{aligned} 1 &: \text{the indicator is always satisfied in this mode} \\ -1 &: \text{the indicator is never satisfied in this mode} \\ 0 &: \text{the indicator is sometimes satisfied in this mode} \end{aligned}$$

	$N1$	$N2$	$N3$	$F1$	$F2$	$F3$
$indi_1$	1			0		
$indi_2$		1				
$indi_3$			1			
$indi_4$	1			1		
$indi_5$					1	
$indi_6$						1

(-1s not represented)

Example

Discernibility (4/4)

Indiscernibility matrix:

- two modes are discernible if

$$\{L(m_1, indi), L(m_2, indi)\} = \{-1, 1\}$$

for some indicator $indi$

	$N1$	$N2$	$N3$	$F1$	$F2$	$F3$
$N1$	1			1		
$N2$		1				
$N3$			1			
$F1$	1			1		
$F2$					1	
$F3$						1

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)

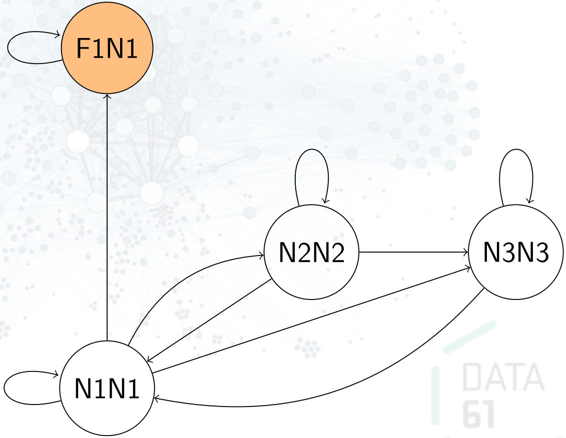
A counter-example is a cycle in the twin plant that is

- reachable,
- and ambiguous.

Theorem: If there is no counter-example the DES is diagnosable

Twin Plant for D_H^∞

Running Example



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

  $\Rightarrow$ eventually the system must leave mode $N1$
  $\{N1\}$ is ephemal

The ephemeral sets include:

- $\{N1, N2\}$
- $\{N3\}$
- $\{F1, F2\}$
- $\{F3\}$.

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)

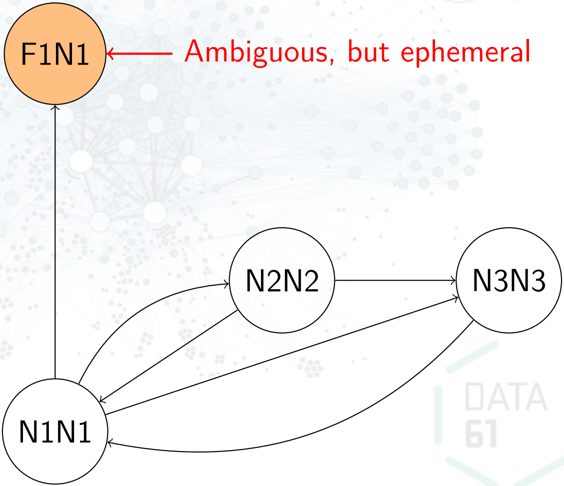
A counter-example is a cycle in the twin plant that is

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

Theorem: The DES is diagnosable iff there is no counter-example

Twin Plant for D_H^∞

Running Example



Outline

Running Example

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

Incremental Approach

Concluding Remarks

Motivation

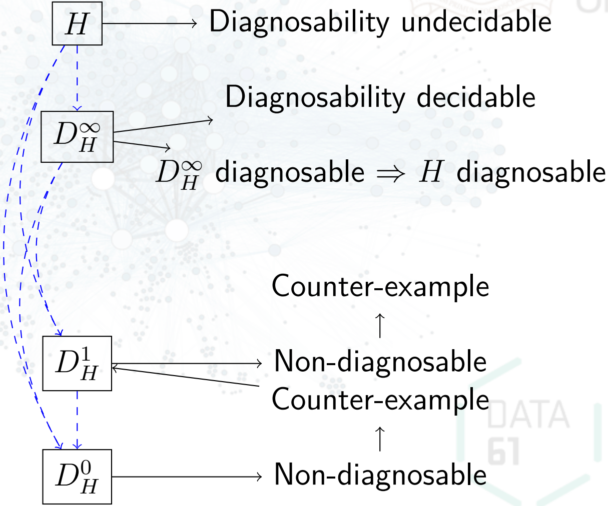
Why Use Incremental Approach?

- 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

$$\begin{tikzcd} \boxed{H} \arrow[r] \arrow[d, dashed] & \text{Diagnosability undecidable} \\ \boxed{D_H^\infty} \arrow[r] \arrow[dr] & \text{Diagnosability decidable} \\ & D_H^\infty \text{ diagnosable} \Rightarrow H \text{ diagnosable} \end{tikzcd}$$

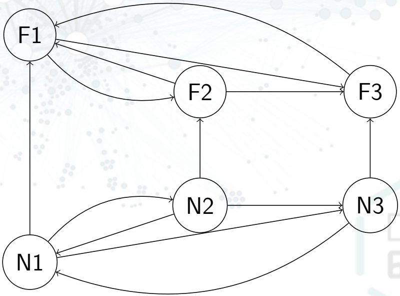
General Idea



0. Maximal Abstraction: D_H^0

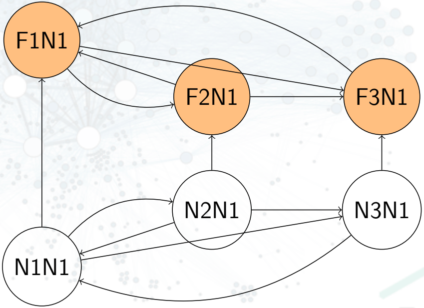
How to Compute D_H^0:

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



0. Twin Plant

Running Example



If the system generates the following faulty behaviour:

$$b_{\mathrm{F}} = N1 \rightarrow F1(\rightarrow F1)^{\infty}$$

then the diagnoser might believe that what is happening is:

$$b_{\mathrm{N}} = N1 \rightarrow N1(\rightarrow N1)^{\infty}$$

0. Negating the Counter Example

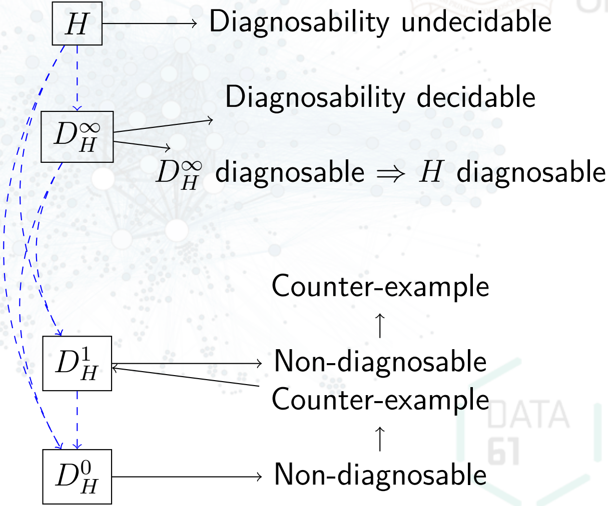
Critical Pair (reminder):

- $b_{\mathrm{F}} = N1 \to F1(\to F1)^{\infty}$
- $b_{\mathrm{N}} = N1 \to N1(\to N1)^{\infty}$

Answer:

- $\{F1\}$ is ephemeral, therefore the counter example is not valid.

Back to the General Idea

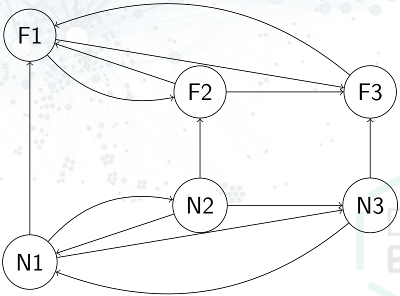


1. New Abstraction: D_H^1

Running Example

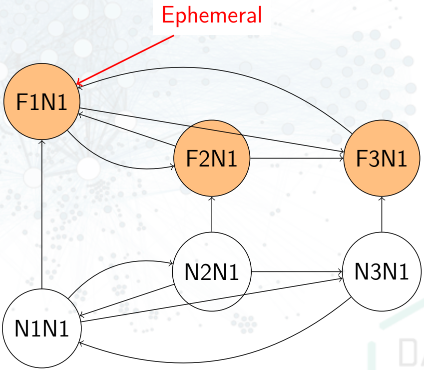
Known ephemeral sets

- $\{F1\}$



1. Twin Plant

Running Example



1. Counter Example

Running Example

If the system generates the following faulty behaviour:

$$b_{\mathrm{F}} = N1 \to F1 \to F2(\to F1 \to F2)^{\infty}$$

then the diagnoser might believe that what is happening is:

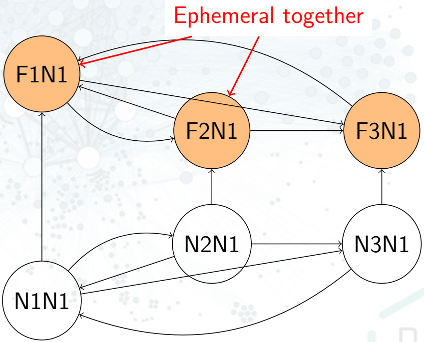
$$b_{\mathrm{N}} = N1 \to N1 \to N1(\to N1 \to N1)^{\infty}$$

Answer:

- It can be shown that $\{F1, F2\}$ is ephemeral.

2. Twin Plant

Running Example



2. Discernibility

Running Example

If the system generates the following faulty behaviour:

$$b_{\mathrm{F}} = N1 \to F1 \to F2 \to F3(\to F1 \to F2 \to F3)^{\infty}$$

then the diagnoser might believe that what is happening is:

$$b_{\mathrm{N}} = N1 \to N1 \to N1 \to N1(\to N1 \to N1 \to N1)^{\infty}$$

Answer:

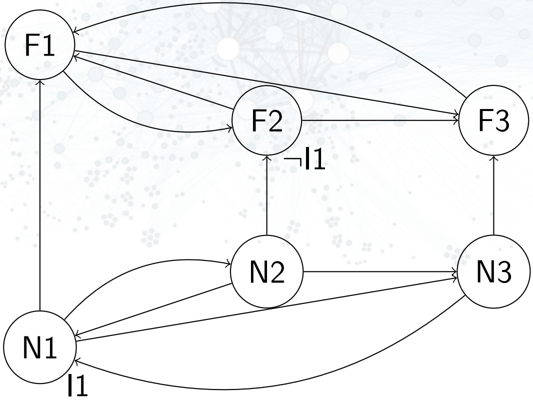
- Indicator $I1$ always discern $N1$ from $F2$

3. New Abstraction: D_H^3

Running Example

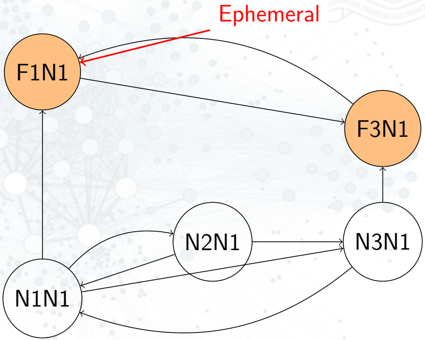
Known ephemeral sets

- $\{F1, F2\}$



3. New Twin Plant: D_H^3

Running Example



New counter example:

- $b_{\mathrm{F}} = N1 \to F1 \to F2 \to F3(\to F1 \to F2 \to F3)^{\infty}$
- $b_{\mathrm{N}} = N1 \to N1 \to N2 \to N1(\to N1 \to N2 \to N1)^{\infty}$

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 infere *ephemerality* properties
  - we infere *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^∞ not diagnosable" does not imply "H not diagnosable".
  What can we do if D_H^∞ is not diagnosable ?

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