ECE 641
Advanced Topics in Supervisory Control for Discrete Event Systems

Lecture 2

Associate Prof. Dr. Klaus Schmidt

Department of Mechatronics Engineering – Çankaya University

PhD Course in Electronic and Communication Engineering
Credits (3/0/3)
Course webpage: http://ece641.cankaya.edu.tr/

Diagnosability: Unobservable Events

Given

- Automaton G over alphabet Σ
- Unobservable events Σ_{uo} and observable events Σ_{o}
  $\rightarrow \Sigma = \Sigma_{\mathrm{uo}} \cup \Sigma_{\mathrm{o}}$
- Natural projection $p : \Sigma^\star \rightarrow \Sigma_{\mathrm{o}}^\star$
- Fault event $f \in \Sigma_{\mathrm{uo}}$

Remarks

- Unobservable events model events that happen in the plant but cannot be seen (for example faults)
- $p(L(G))$ is the language that can be seen from the plant
- Occurrence of f indicates that a fault happened
  $\rightarrow L(G) \cap (\Sigma \setminus \{f\})^\star$ represents the correct behavior

Diagnosability: Unobservable Events

Illustration

Gap 1

Diagnosability: Faults and Failures

Fault

A fault is a defect in a system

Fault Types

- Transient faults: These occur once and then disappear.
- Intermittent faults: Fault occurs, then vanishes again, reoccurs, etc.
- Permanent faults: Fault continues to exist until the faulty component is repaired or replaced.

Failure

A failure is an instance in time when a system displays behavior that is contrary to its specification

Remark

- Faults and failures are considered as different concepts
- Not every fault leads to a failure

Diagnosability: Diagnosis Problems

Fault Diagnosis

Given G, Σ_{uo}, p and f, determine a diagnoser that detects if the fault f happened based on the observations from the plant

Diagnosability

Given G, Σ_{uo}, p and f determine if the occurrence of the fault f can be detected by a diagnoser after a bounded delay of event occurrences

Remarks

- A diagnoser is a system that observes what happens in the plant and decides if a fault occurred or not
- Diagnosability is a property that determines if all plant faults can be detected by a diagnoser
- If a system is diagnosable, there is a diagnoser that detects all plant faults after a bounded delay

Diagnosability: Diagnosis Problems

Illustration

Gap 2

Diagnosability: Definition for Permanent Faults

Definition

Let G model a DES and let $\Sigma_{\mathrm{o}} \subseteq \Sigma$ be a set of observable events. Assume that G is live and has no cycles of unobservable events. The fault event f is diagnosable for G and the natural projection $p : \Sigma^\star \to \Sigma_{\mathrm{o}}^\star$ if

$$(\exists n \in \mathbb{N}) \quad (\forall s \in L(G) \cap (\Sigma \setminus \{f\})^\star f)(\forall st \in L(G)),$$
$$|t| \geq n \Rightarrow (\forall u \in p^{-1}p(st) \cap L(G), u \in (\Sigma \setminus \{f\})^\star f \Sigma^\star).$$

Remarks

- Critical strings are $s \in L(G) \cap (\Sigma \setminus \{f\})^\star f$ that contain the fault f
  $\Rightarrow$ We write $f \in s$ for such strings
- For all faulty extensions st that are longer than a bound n, all strings with the same projection should be faulty
  $\Rightarrow$ The fault can be detected if all strings that belong to the observation $p(st)$ are faulty

Diagnosability: Example

Illustration

Gap 3

Diagnoser: Basics

Explanation

- A diagnoser observes the plant behavior and determines if a fault happened or not
- Diagnoser can either be computed offline or can compute fault decisions online

Illustration

Gap 4

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Definitions

Plant

- Consider automaton $G = (X, \Sigma, \delta, x_0, X_{\mathrm{m}})$, unobservable events $\Sigma_{\mathrm{uo}}^{\star}$

Unobservable Reach

- For each state $x \in X$

$$UR(x) = \{x' \in X | \exists u \in \Sigma_{\mathrm{uo}}^{\star} \text{ such that } \delta(x, u) = x'\}$$

$\Rightarrow$ All states that can be reached from x without any observation

One-step Reach

- For each state set $X' \subseteq X$ and $\sigma \in \Sigma \setminus \Sigma_{\mathrm{uo}}$

$$OR(X', \sigma) = \{x \in X | \exists x' \in X' \text{ and } u \in \Sigma_{\mathrm{uo}}^{\star}\sigma\Sigma_{\mathrm{uo}}^{\star} \text{ such that } \delta(x', u) = x\}$$

$\Rightarrow$ All states that can be reached from X' with observation σ

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: One-Step Reach

Illustration

Gap 5

Diagnoser: Offline Computation

Diagnoser Automaton $D = (O, \Sigma_{\rm o}, \mu, o_0, O_{\rm m})$

- Initial state
  - $o_0 = UR(x_0)$
  - For each state $x \in o_0$ such that $\exists u \in \Sigma_{\rm uo}^\star$ with $\delta(x_0, u) = x$ and $f \notin u$: Attach a label N (normal) to x
  - For each state $x \in o_0$ such that $\exists u \in \Sigma_{\rm uo}^\star$ with $\delta(x_0, u) = x$ and $f \in u$: Attach a label F (faulty) to x
  - If $x \in o_0$ is reached by both faulty and non-faulty strings, there is an entry $(x\mathrm{N})$ and an entry $(x\mathrm{F})$ in o_0.
- Transitions from any state $o \in O$ with observation $\sigma \in \Sigma_{\rm o}$
  - $\mu(o, \sigma) = OR(o, \sigma)$
  - For each state $x \in \mu(o, \sigma)$ such that $\exists u \in \Sigma_{\rm uo}^\star \sigma \Sigma_{\rm uo}^\star$ with $f \notin u$ and $(x'\mathrm{N}) \in o$ with $\delta(x', u) = x$, Attach the label N to x
  - For each state $x \in \mu(o, \sigma)$ such that $x = \delta(x', u)$ for some $u \in \Sigma_{\rm uo}^\star \sigma \Sigma_{\rm uo}^\star$ and either $f \in u$ or $(x'\mathrm{F}) \in o$: Attach F to x

Diagnoser: Example

Illustration

Gap 6

Diagnoser: Example

Illustration

Gap 7

Diagnoser: Properties

States

- Each state of D is a subset of $X \times \{\mathrm{N}, \mathrm{F}\}$
  $\Rightarrow D$ has up to $2^{|X|+1}$ states

Fault Detection

- If all entries of a diagnoser state o have label N, no fault happened
- If all entries of a diagnoser state o have label F, fault happened
- Otherwise, we are not sure if fault happened $\Rightarrow$ uncertain state

Uncertain Cylce in D

- Cycle with uncertain diagnoser states

Indeterminate Cycle in D

- Uncertain cycle such that there are two corresponding cycles in G
  - One that only has states with label F
  - One that only has states with label N

Diagnoser: Properties

Illustration

Gap 8

Diagnoser: Diagnosability Test

Diagnosability Condition

- f is diagnosable for G and $p : \Sigma^\star \rightarrow \Sigma_o^\star$ if and only if the diagnoser automaton D does not contain indeterminate cycles

Remark

- Diagnosability test is of “exponential complexity”
- There are more efficient verification algorithms in the literature

S. Jiang, Z. Huang, V. Chandra, R. Kumar, A polynomial algorithm for testing diagnosability of discrete-event systems, IEEE Transactions on Automatic Control 46 (8) (2001) 1318–1321.

T.-S. Yoo, S. Lafortune, Polynomial time verification of diagnosability of partially observed discrete-event systems, IEEE Transactions on Automatic Control 47 (9) (2002) 1491–1495.

On-line Diagnosis

- Construct each diagnoser state after observation of an event σ

Diagnoser: Properties

Illustration

Gap 9