ECE 641
Advanced Topics in Supervisory Control for Discrete Event Systems

Lecture 3

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: Language Specification

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 $p : \Sigma^\star \rightarrow \Sigma_{\mathrm{o}}^\star$
- Prefix-closed specification $K \subseteq L(G)$: $K = \overline{K}$
  $\rightarrow$ Specification automaton $C = (Y, \Sigma, \gamma, y_0, Y_{\mathrm{m}})$ with $L(C) = K$

Remarks

- $p(L(G))$ is the language that can be seen from the plant
- K represents the correct system behavior
  $\rightarrow L(G) \setminus K$ represents faulty system behavior

Diagnosability: Language Specification

Illustration

Gap 1

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnosability: Definition

Definition

Let G model a DES, let $\Sigma_o \subseteq \Sigma$ be a set of observable events and let $K = \overline{K} \subseteq L(G)$ be a specification language. K is language-diagnosable w.r.t. G and the natural projection $p : \Sigma^\star \to \Sigma_o^\star$ if

$$(\exists n \in \mathbb{N})(\forall s \in L(G) \setminus K)(\forall st \in L(G), |t| \geq n \text{ or } st \text{ deadlocks}) \Rightarrow (\forall u \in p^{-1}p(st) \cap L(G), u \notin K). \quad (1)$$

Remarks

- Critical strings are $s \in L(G) \setminus K$
- If a faulty extension st leads to deadlock, all strings with the same projection should be faulty
- For all faulty extensions st that are longer than a bound n, all strings with the same projection should be faulty

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnosability: Example

Illustration

Gap 2

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Definition

Extended Specification Automaton $\overline{C} = (\overline{X}, \Sigma, \overline{\gamma}, \overline{y}_0, \overline{Y}_{\mathrm{m}})$

- Initial state: $\overline{y}_0 = y_0$
- State set: $\overline{Y} = Y \cup \{F\}$
- Transition relation:

$$\forall y \in Y \text{ and } \forall \sigma \in \Sigma \text{ such that } \gamma(y, \sigma)! : \overline{\gamma}(y, \sigma) = \gamma(y, \sigma)$$

$$\forall y \in y \text{ and } \forall \sigma \in \Sigma \text{ such that } \neg\gamma(y, \sigma)! : \overline{\gamma}(y, \sigma) = F$$

$$\forall \sigma \in \Sigma : \overline{\gamma}(F, \sigma) = F$$

Remarks

- $\overline{C}$ is equal to C extended by a new state F
- Every transition that is not defined in C leads to the state F in $\overline{C}$
- Every string that leads to state F is faulty

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Extended Specification Automaton

Illustration

Gap 3

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Offline Computation

Plant Automaton with Fault Label

- Compute synchronous composition $R = (Z, \Sigma, \alpha, z_0, Z_\mathrm{m}) = G||\overline{C}$
  $\Rightarrow L(R) = L(G)$
  $\Rightarrow$ Each state of R is a pair (x, y) with $x \in X$ and $y \in \overline{Y}$
  $\Rightarrow$ A state $z = (x, y) \in Z$ belongs to a faulty string if $y = F$

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

- Compute D using R
- Initial state
  - $o_0 = UR(z_0)$
- Transitions from any state $o \in O$ with observation $\sigma \in \Sigma_\mathrm{o}$
  - $\mu(o, \sigma) = OR(o, \sigma)$

Remarks

- D is called an "observer" automaton of R

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Example

Illustration

Gap 4

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Example

Illustration

Gap 5

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Properties

States

- Each state of D is a subset of $X \times \overline{Y}$
  $\Rightarrow D$ has up to $2^{|X|\cdot|\overline{Y}|}$ states

Fault Detection

- If no entry of a diagnoser state o has component $F \Rightarrow$ no fault
- If all entries of a diagnoser state o have component $F \Rightarrow$ fault
- 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 component F
  - One that only has states without component F

Diagnoser: Properties

Illustration

Gap 6

Diagnoser: Diagnosability Test

Indeterminate Deadlock

- Uncertain state o in D such that at least one entry deadlocks in R

Diagnosability Condition

- Assume that G does not have any unobservable cycles. K is language-diagnosable for G and $p : \Sigma^\star \rightarrow \Sigma_o^\star$ if and only if the diagnoser automaton D neither contains indeterminate cycles nor indeterminate deadlocks.

Remark

- This diagnosability notion allows to deal with deadlocks
- The absence of unobservable cycles can be removed (see Exercise)
- There is a more efficient verification algorithms in the literature

  Yoo, T.-S., Garcia, H. E. (2008). Diagnosis of behaviors of interest in partially observed discrete-event systems. System & Control Letters, 57(12), 1023–1029.

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Properties

Illustration

Gap 7

Klaus Schmidt
Department of Electronic and Communication Engineering – Çankaya University

Diagnoser: Properties

Illustration

Gap 8

Relation to Event Diagnosis: Explanation

Event Diagnosis

- Plant G and fault event f

Language Specification

- $K = L(G) \cap (\Sigma \setminus \{f\})^{\star}$

$\Rightarrow$ Event diagnosis problem can easily be converted into a language diagnosis problem

Example

Gap 9

Decentralized Diagnosis: Basics

Components

- Plant automaton G
- Specification automaton C; specification $K = L(C)$
- Multiple diagnosers $D_1, \ldots, D_m$ with different observations $\Sigma_{\mathrm{o},1}, \ldots, \Sigma_{\mathrm{o},m}$
- Projections $p_i : \Sigma^\star \to \Sigma_{\mathrm{o},i}^\star$ for $i = 1, \ldots, m$

Illustration

Gap 10

Decentralized Diagnosis: Definition

Diagnosis Task

- Detect each faulty string by at least one of the diagnosers

Definition (Co-diagnosability)

Let G be a DES over the alphabet Σ, let $K = \overline{K} \subseteq L(G)$ be a prefix-closed specification language and assume m local sites with their projections p_i, $i = 1, \ldots, m$. K is co-diagnosable for G and p_i, $i = 1, \ldots, m$ if

$$(\exists n \in \mathbb{N})(\forall s \in L(G) - K)(\forall st \in L(G) \text{ s.t. } |t| \geq n \text{ or } st \text{ deadlocks})$$
$$\Rightarrow (\exists i \in \{1, \ldots, m\})(\forall u_i \in M_i^{-1} M_i(st) \cap L(G), u_i \notin K)$$

Remark

- Co-diagnosability holds if each faulty string is detected by at least one diagnoser

Decentralized Diagnosis: Example

Illustration

Gap 11

Decentralized Diagnosis: Summary

Verification

W. Qiu, R. Kumar, Decentralized failure diagnosis of discrete event systems, Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on 36 (2) (2006) 384–395.

Related Work

- Studies on decentralized diagnosis in event diagnosis framework

  R. Debouk, D. Teneketzis, Coordinated decentralized protocols for failure diagnosis of discrete-event systems, Discrete Event Dynamic Systems: Theory and Applications 10 (2000) 33–86.
- Studies on decentralized diagnosis for modular systems

  C. Zhou, R. Kumar, R. Sreenivas, Decentralized modular diagnosis of concurrent discrete event systems, in: WODES, 2008, pp. 388–393.
- Studies on decentralized diagnosis using abstractions

  Schmidt, K.: Abstraction-based Verification of Co-diagnosability for Discrete Event Systems, Automatica, vol. 46, pp. 1489-1494, 2010.