On-time diagnosis of discrete event systems

Aditya Mahajan and Demosthenis Teneketzis

Dept. of EECS,
University of Michigan,
Ann Arbor, MI. USA.

WODES 2008, May 30, 2008.

Fault Diagnosis in DES

1. Asymptotic (accuracy is critical; delay is important but not critical)

2. On-time (delay is critical; accuracy is important but not critical)

Most of the literature on diagnosis of DES has concentrated on asymptotic fault diagnosis.

Contribution of this paper

- Formulate on-time fault diagnosis as a minimax optimization problem.

- Use decision theory to provide a solution methodology.

Modelling questions

- What do we mean by "time"?
- What should the diagnoser/monitor do?
- How do we model performance?

When it is time to take a decision but the monitor is not sure that a fault has occurred, it will **make mistakes.**

Preliminaries

Language, Monitor, and Costs

Language

- Language L is prefix-closed, **finite, and bounded**

$$\mathsf{L} = \mathsf{L}_\mathsf{T} \cup \mathsf{L}_{\mathsf{NT}}$$

- Terminal Strings: $\mathsf{L}_\mathsf{T} \coloneqq \{s \in \mathsf{L} : \mathsf{L} \setminus s \neq \emptyset\}$
- Non-terminal Strings: $\mathsf{L}_{\mathsf{NT}} \coloneqq \mathsf{L} \setminus \mathsf{L}_\mathsf{T}$.

- Event Set $\Sigma = \Sigma_o \cup \Sigma_{uo} \implies$ natural projections.
- Observable events: Σ_o
- Unobservable events: Σ_{uo}.
- Fault event $f \in \Sigma_{uo}$.

Monitor

- Observes $P(L)$
- Upon observing an event, the monitor can:
  - **raise an alarm**, $\Longrightarrow$ the system is shut down immediately.
  - **do nothing**, $\Longrightarrow$ the system continues to operate.
- Monitoring policy $g : P(L) \to \{0, 1\}$
- Monitored sub-language $L|_g$

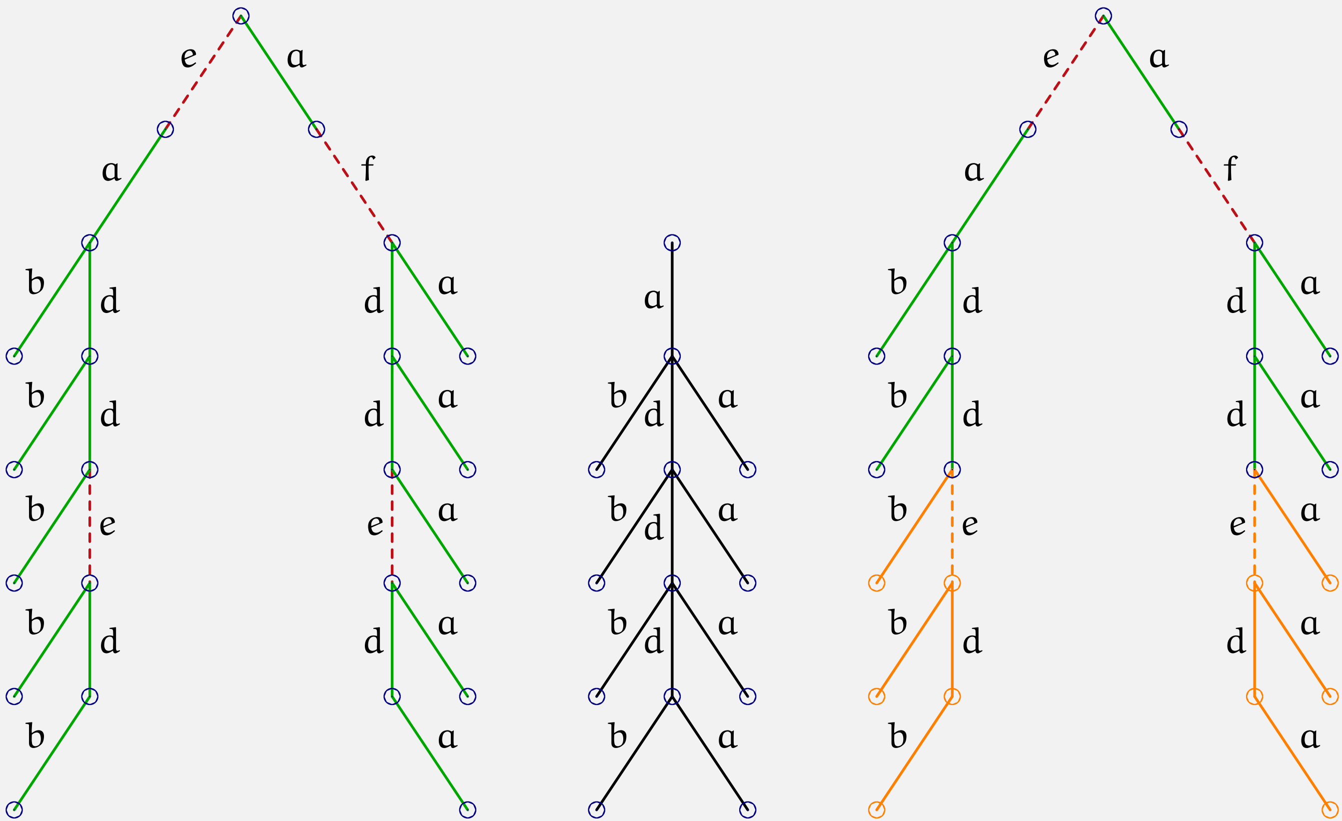
Sub-language where the system can stop

- Monitor raises an alarm $\Longrightarrow$ system stops in $L^S_{NT} \cup L^S_T$

$$L^S_{NT} = \{s \cdot \sigma \in L_{NT} : \sigma \in \Sigma_o\}, \qquad L^S_T = \{s \cdot \sigma \in L_T : \sigma \in \Sigma_o\}$$

- Monitor does not raise an alarm $\Longrightarrow$ system stops in L_T
- System can stop in $L^S = L^S_{NT} \cup L_T$
- For any g, $(L|_g)_T \subseteq L^S$

Example



Language L

P(L)

$L|_g$ for $g(add) = 1$

Quantifying timeliness

- After a fault has occurred, each event incurs a cost c.
- System is stopped in a non-faulty state $\Longrightarrow$ false alarm penalty of H_{NT}.
- System executes a terminal trace in a faulty state $\Longrightarrow$ additional terminal penalty of H_T.

Cost of stopping

- For $s \in L$, let
  - $\tau(s)$ be the first stage when a fault occurs in s.
  - n be the "length" of s
- for $s \in L_{NT}^{S}$, $C(s) = \begin{cases} (n - \tau(s))c, & \text{if } s \text{ contains a fault,} \\ H_{NT}, & \text{otherwise;} \end{cases}$
- for $s \in L_T$, $C(s) = \begin{cases} (n - \tau(s))c + H_T, & \text{if } s \text{ contains a fault,} \\ 0, & \text{otherwise.} \end{cases}$

Problem Formulation

The on-time diagnosis problem

- **Given**
  - Prefix-closed, finite, and bounded language L,
  - Observable events Σ_o, unobservable events Σ_{uo}, and fault event f
  - Cost c, fault alarm penalty H_{NT}, and a terminal penalty H_T.
- **Define**
  - $\mathcal{G}$ family of functions from $P(L)$ to $\{0, 1\}$
  - Performance of a monitoring policy $g \in \mathcal{G}$

$$\mathcal{J}(g) \coloneqq \max_{s \in (L|_g)_T} C(s).$$

- **Choose**
  - A monitoring rule $g^* \in \mathcal{G}$ to minimize $\mathcal{J}(g)$

$$\mathcal{J}^* = \mathcal{J}(g^*) = \min_{g \in \mathcal{G}} \max_{s \in (L|_g)_T} C(s)$$

Centralized minimax optimization problem
Can be solved by dynamic programming

Some Notation

- $Q(t) \coloneqq \{s \cdot \sigma \in P^{-1}(t) : \sigma \in \Sigma_o\}$
- $Q_T(t) \coloneqq P^{-1}(t) \cap L_T$

Optimal monitoring rule

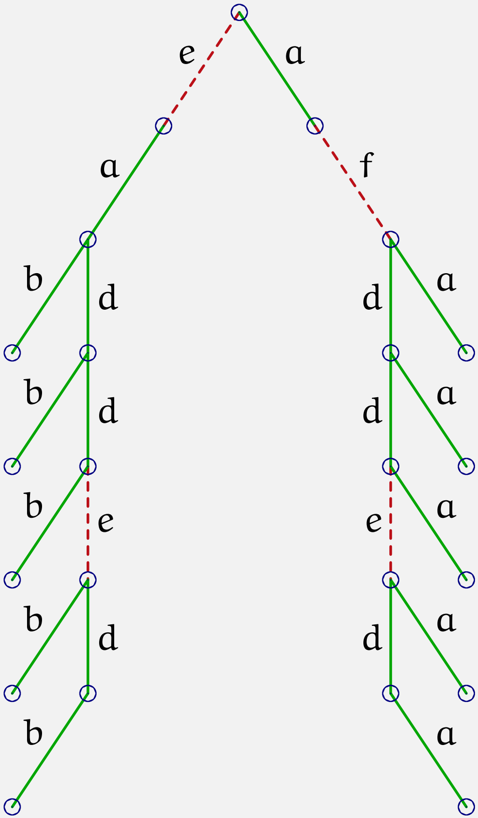
- For $t \in (P(L))_T$

$$\underbrace{V(t)}_{\substack{\text{minimum}\\\text{worst case}\\\text{cost to go at } t}} = \min\Big\{ \underbrace{\max_{s \in Q(t)} C(s)}_{\substack{\text{worst case cost}\\\text{of stopping}}}, \underbrace{\max_{s \in Q_T(t)} C(s)}_{\substack{\text{worst case cost}\\\text{of continuing}}} \Big\}$$

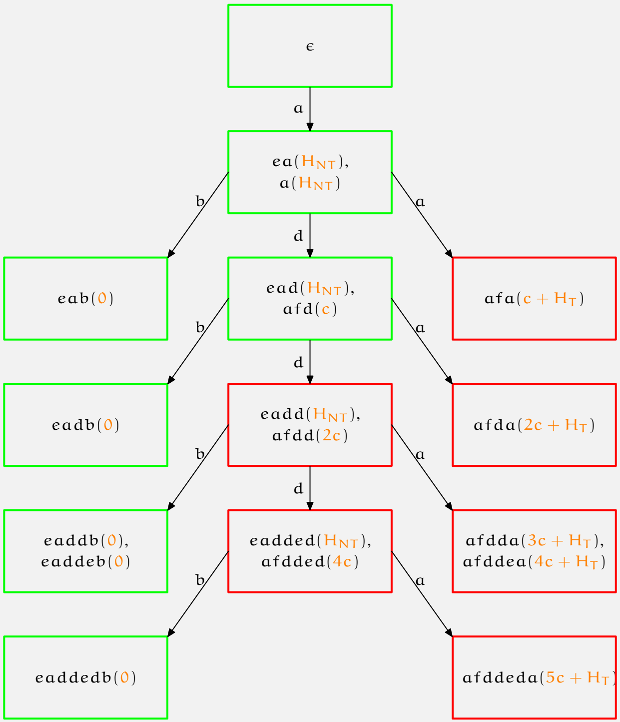
- For $t \in (P(L))_{NT}$, let $O_C(t) \coloneqq \{e \in \Sigma : t \cdot e \in P(L)\}$, and

$$\underbrace{V(t)}_{\substack{\text{minimum}\\\text{worst case}\\\text{cost to go at } t}} = \min\Big\{ \underbrace{\max_{s \in Q(t)} C(s)}_{\substack{\text{worst case cost}\\\text{of stopping}}}, \underbrace{\max\Big\{\max_{s \in Q_T(t)} C(s), \max_{e \in O_C(t)} V(t \cdot e)\Big\}}_{\text{worst case cost of continuing}} \Big\}$$

Example



Language L



Optimal monitor for

$H_T = c$, $H_{NT} = 3c$

Relaxing some modelling assumptions

- **Live** languages

  Should be possible. Working on the details.

- Generalized costs

  Use a trace dependent cost in the paper

- Generalized projections

  Use **prefix-preserving** projections in the paper

Summary

- Formulate and solve on-time fault diagnosis problem.
- Penalize false alarm and (trace dependent) amount of delay in fault detection.
- Equivalent to a minimax optimization problem.

Thank you