

Diagnosability in Nonsequential Systems

Stefan Haar

Sept 2, 2010
DISC WS Berlin

Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"
- 7 Conclusion

Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"
- 7 Conclusion

Event-based Diagnosability in sequential settings

Definitions (following Sampath 1995 and many others)

- Given: a DES model : FSM, Petri net , ... with
 - transition set \mathcal{T} ,
 - observable transitions $\mathcal{O} \subseteq \mathcal{T}$,
 - unobservable transitions $\mathcal{UO} \triangleq \mathcal{T} \setminus \mathcal{O}$
 - fault transition $f \in \mathcal{UO}$
- $s \sim_{\mathcal{O}} s'$ iff $s, s' \in \mathcal{T}^*$ are mapped to the same word in \mathcal{O}^*
- $\mathcal{L} \subseteq \mathcal{T}^* (\mathcal{T}^\omega)$ is **non-diagnosable** iff there exist sequences $s_N, s_Y \in \mathcal{L}$ such that:
 1. s_Y is faulty, s_N is healthy, and $s_N \sim_{\mathcal{O}} s_Y$;
 2. moreover, s_Y with the above is arbitrarily long after the first fault, i. e. for every $k \in \mathbb{N}$ there exists a choice of $s_N, s_Y \in \mathcal{L}$ with the above properties and such that the suffix $s_{Y/\phi}$ of s_Y after the first occurrence of fault ϕ in s_Y satisfies $|s_{Y/\phi}| \geq k$.

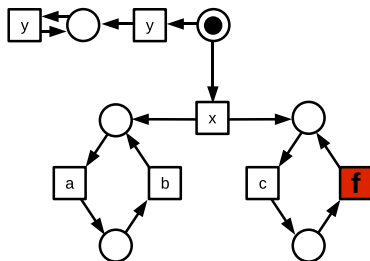
Event-based Diagnosability in sequential settings

Background

- Classical definition : Sampath et al 1995
- ... gave also verification method and characterization in terms of cycles
- Extensions to decentralized architectures, timed systems, ...
- Here: **nonsequential behaviour**
- Distributed systems exhibit **local** states and **local** behaviour
- Partial Order Techniques necessary to fight state space explosion
- **Here**: Follow PN-based **asynchronous diagnosis** with unfoldings (Benveniste, Fabre, Jard, Haar 2003)
- Focus on concurrency-related properties that interleavings miss

What Interleavings can't detect

Observation: *abababab...*



Has **f** occurred ?

Contents

- 1 Introduction
- 2 Key Concepts**
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"
- 7 Conclusion

Petri Nets

Nets

A **net** is a tuple $\mathcal{N} = (\mathcal{P}, \mathcal{T}, F)$ such that (i) $\mathcal{P}, \mathcal{T} \neq \emptyset$, (ii) $\mathcal{P} \cap \mathcal{T} = \emptyset$ (iii) $F \subseteq (\mathcal{P} \times \mathcal{T}) \cup (\mathcal{T} \times \mathcal{P})$.

With $M_0 \subseteq \mathcal{P}$, (\mathcal{N}, M_0) is a **Petri Net**.

Occurrence Net

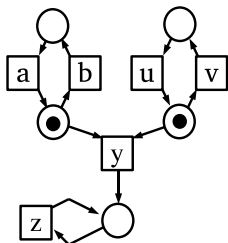
For a net $ON = (\mathcal{B}, \mathcal{E}, G)$ and $e_1, e_2 \in \mathcal{E}$, let $e_1 \#_i e_2$ iff there is $b \in \mathcal{B}$ s.th. bGe_1 and bGe_2 , and let

$$\# \triangleq \{(x_1, x_2) \mid \exists e_1, e_2 : e_1 \#_i e_2 \wedge e_j G^* x_j\}$$

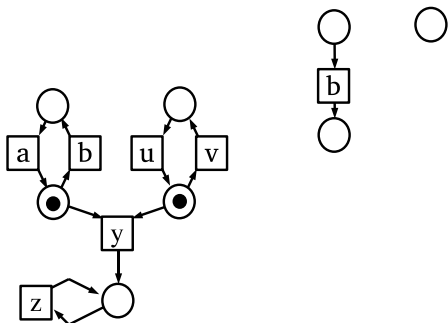
ON is an **occurrence net** if and only if it satisfies

- 1 \leq_{ON} is a partial order;
- 2 for all $b \in \mathcal{B}$, $|\bullet b| \in \{0, 1\}$;
- 3 for all $x \in \mathcal{B} \cup \mathcal{E}$, the set $[x] = \{y \in \mathcal{B} \cup \mathcal{E} \mid y \leq_{ON} x\}$ is finite;
- 4 no self-conflict, i.e. no $x \in \mathcal{B} \cup \mathcal{E}$ such that $x \#_{ON} x$;
- 5 the set \mathbf{c}_0 of \leq_{ON} -minimal nodes is contained in \mathcal{B} and finite.

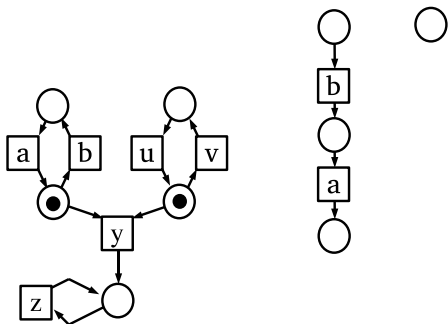
Occurrence semantics for Petri Nets: Unfoldings



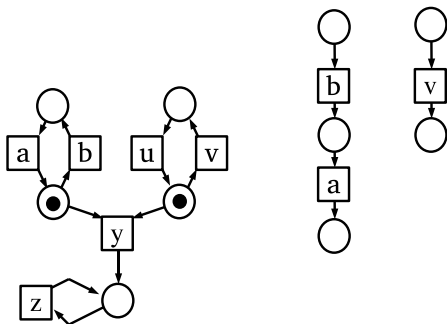
Occurrence semantics for Petri Nets: Unfoldings



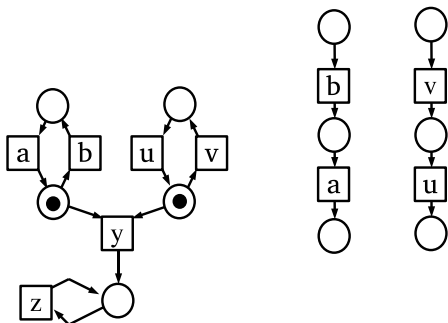
Occurrence semantics for Petri Nets: Unfoldings



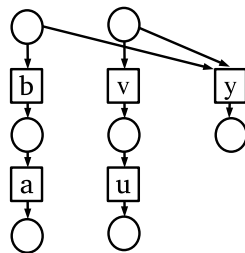
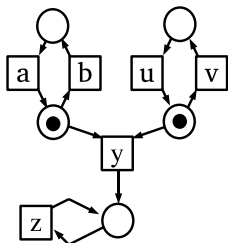
Occurrence semantics for Petri Nets: Unfoldings



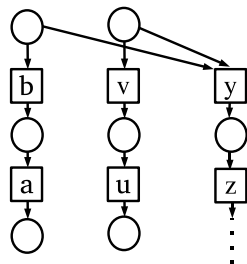
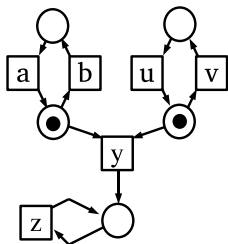
Occurrence semantics for Petri Nets: Unfoldings



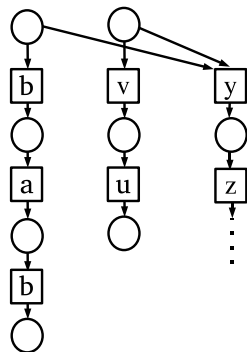
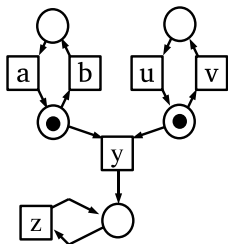
Occurrence semantics for Petri Nets: Unfoldings



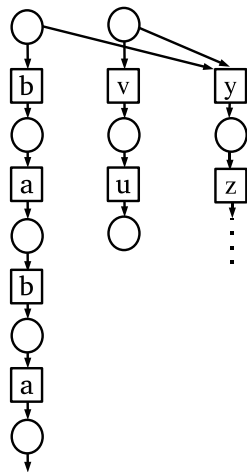
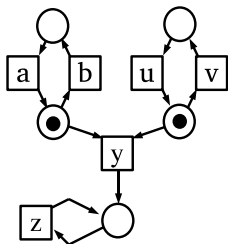
Occurrence semantics for Petri Nets: Unfoldings



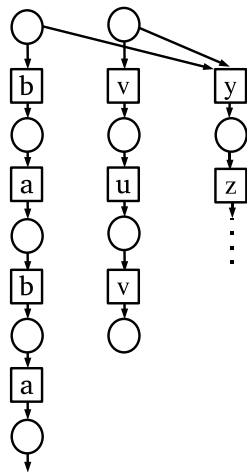
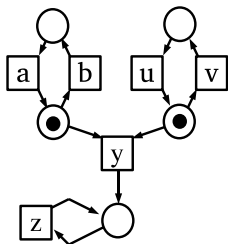
Occurrence semantics for Petri Nets: Unfoldings



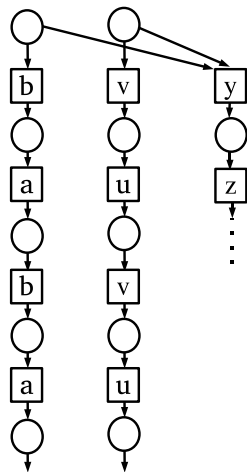
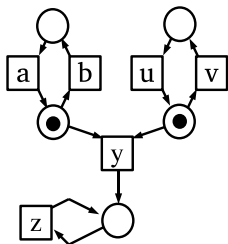
Occurrence semantics for Petri Nets: Unfoldings



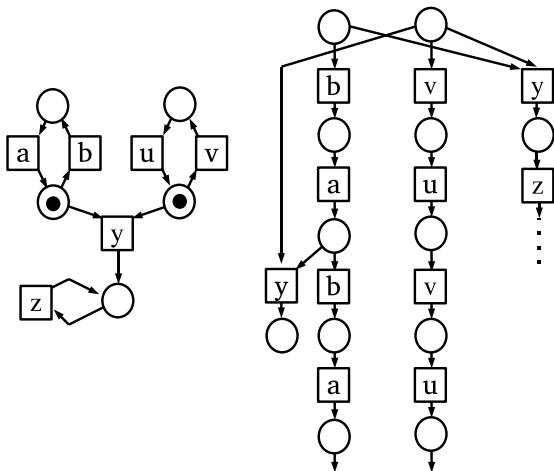
Occurrence semantics for Petri Nets: Unfoldings



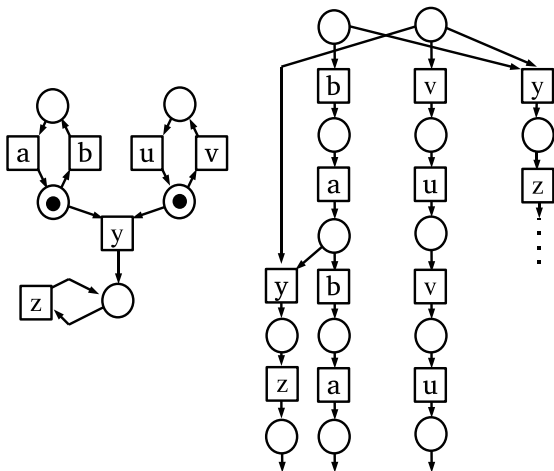
Occurrence semantics for Petri Nets: Unfoldings



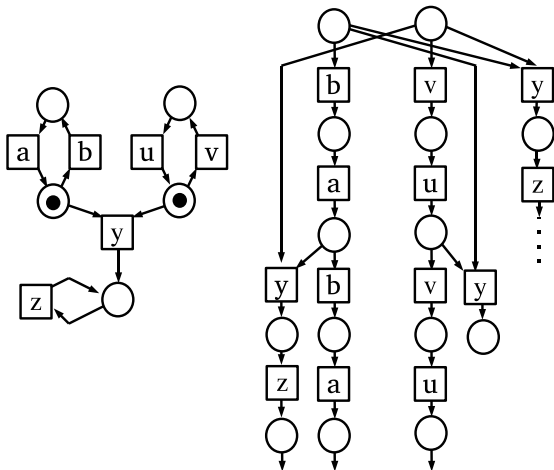
Occurrence semantics for Petri Nets: Unfoldings



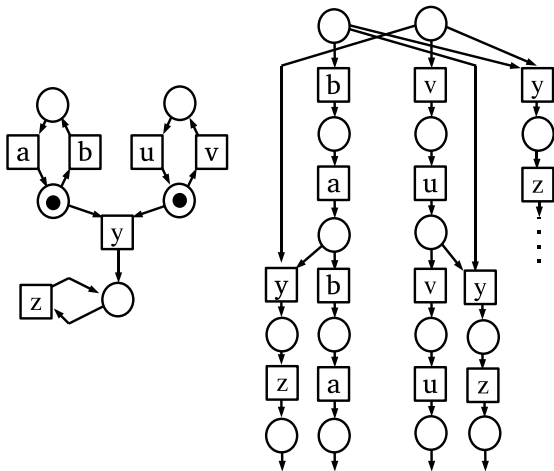
Occurrence semantics for Petri Nets: Unfoldings



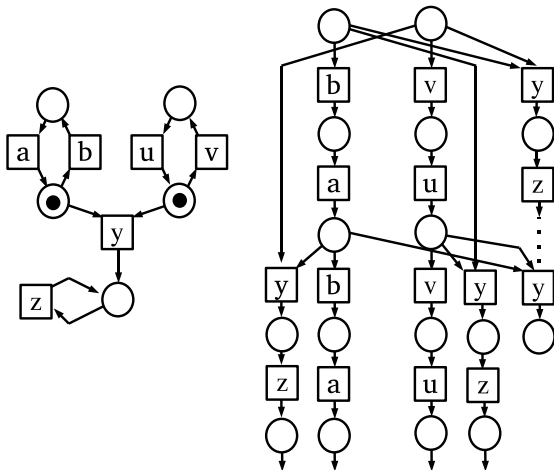
Occurrence semantics for Petri Nets: Unfoldings



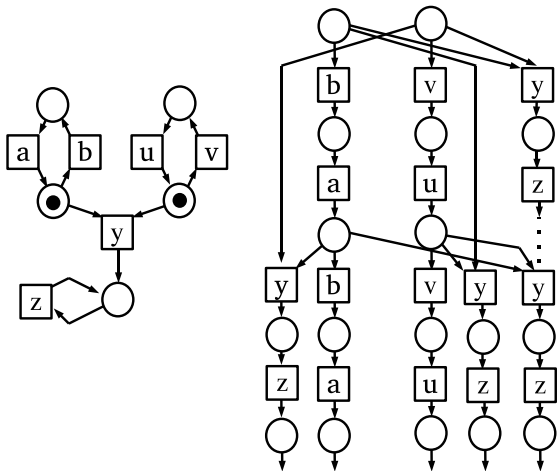
Occurrence semantics for Petri Nets: Unfoldings



Occurrence semantics for Petri Nets: Unfoldings



Occurrence semantics for Petri Nets: Unfoldings



Event Structures

Event Structures

A (labeled) prime event structure is a tuple PES = $(E, \leq, \#, \lambda)$ s.th.

- 1 $E = \text{supp}(\text{PES}) \neq \emptyset$ support, or set of events,
- 2 $\leq \subseteq E \times E$ a partial order with finite causes:

$$\forall e \in E : |\{e' \in E \mid e' \leq e\}| < \infty, \quad (1)$$

- 3 $\# \subseteq E \times E$ irreflexive symmetric conflict relation with heredity:

$$\forall e, e', e'' \in E : e \# e' \wedge e' \leq e'' \Rightarrow e \leq e'', \quad (2)$$

- 4 $\lambda : E \rightarrow \mathbb{A}$ total labelling.

Special Cases

- "Forgetting" places in an occurrence net yields a PES
- Computation tree semantics of PN is a concurrency-free PES

Special Sub-Structures

Prefixes

A **prefix** of PES = $(E, \leq, \#, \lambda)$ is a subset $Pref \subseteq E$ that is **causally closed**, i.e. $\forall e, e' \in E$

$$\left. \begin{array}{l} e \in Pref \\ e' < e \end{array} \right\} \Rightarrow e' \in Pref$$

Configurations

A prefix κ of PES is called a **configuration** iff κ is **conflict-free**, i.e.

$$\left. \begin{array}{l} e \in \kappa \\ e' \# e \end{array} \right\} \Rightarrow e' \notin \kappa$$

Note:

Configurations correspond 1-1 to nonsequential behaviours, i.e. they are **generalized words** (see Mazurkiewicz traces etc...)

Heights in Event Structures

Definitions

Weight function $\mu : E \rightarrow [0, +\infty)$

$$\underline{\mathcal{H}}(\emptyset) \triangleq 0$$

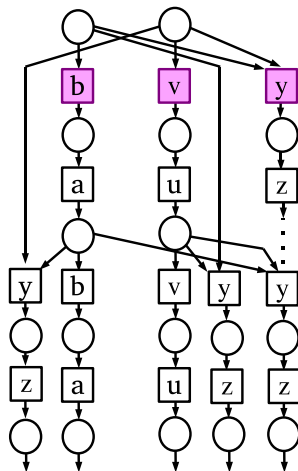
$$\underline{\mathcal{H}}(e) \triangleq \mu(e) + \max_{e' < e} (\underline{\mathcal{H}}(e'))$$

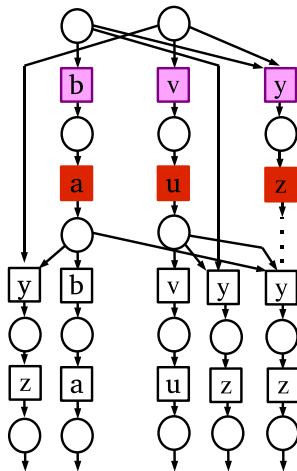
For a prefix $Pref$,

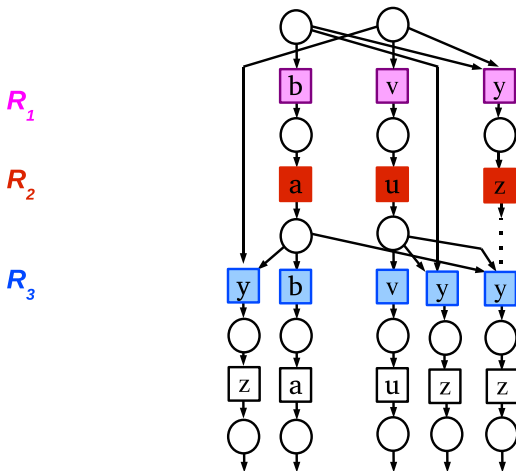
$$\underline{\mathcal{H}}(Pref) \triangleq \sup \{ \underline{\mathcal{H}}(e) \mid e \in Pref \}$$

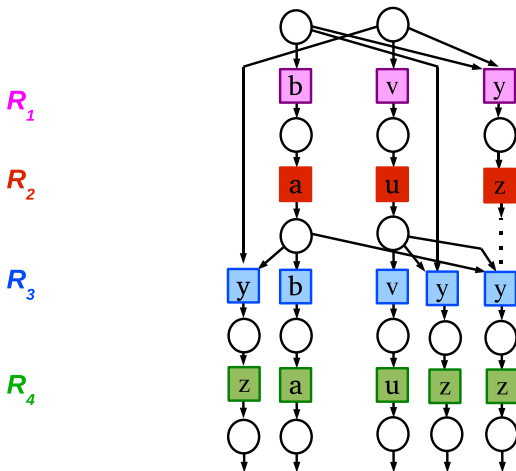
Unit Prefix of height $n \in \mathbb{N}$:

$$\begin{aligned} \mathcal{R}_n &\triangleq \{ e \mid \underline{\mathcal{H}}(e) \leq n \} \\ &= \bigcup_{\underline{\mathcal{H}}(Pref) \leq n} Pref \end{aligned}$$

Counting Height: $\mu \equiv 1$ R_1 

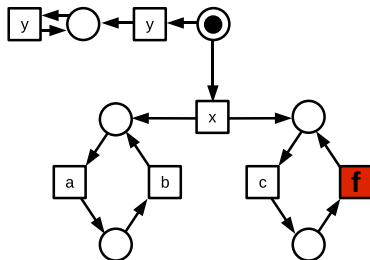
Counting Height: $\mu \equiv 1$ R_1 R_2 

Counting Height: $\mu \equiv 1$ 

Counting Height: $\mu \equiv 1$ 

What Interleavings can't detect

Observation: *abababab...*



Has **f** occurred ?

Lower and Upper Heights

Definitions

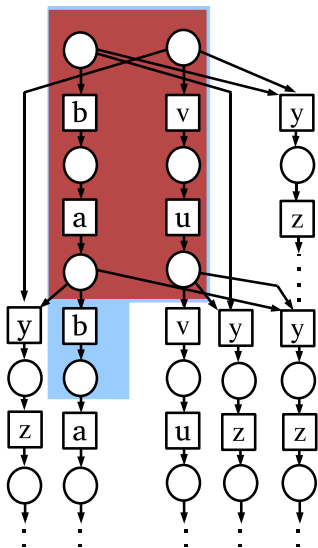
Fix any configuration κ .

- The **upper height** $\underline{\mathcal{H}}(\kappa)$ is its "prefix height"

$$\underline{\mathcal{H}}(\kappa) \triangleq \sup \{ \underline{\mathcal{H}}(e) \mid e \in \kappa \}$$

- **Lower height** $\overline{\mathcal{H}}(\kappa)$: biggest n such that $\kappa \cap \mathcal{R}_n$ is **maximal** in \mathcal{R}_n
- $\overline{\mathcal{H}}(\bullet)$ measures the "uniform parallel progress" in κ
- κ is **progressive** iff $\underline{\mathcal{H}}(\kappa) = \overline{\mathcal{H}}(\kappa)$

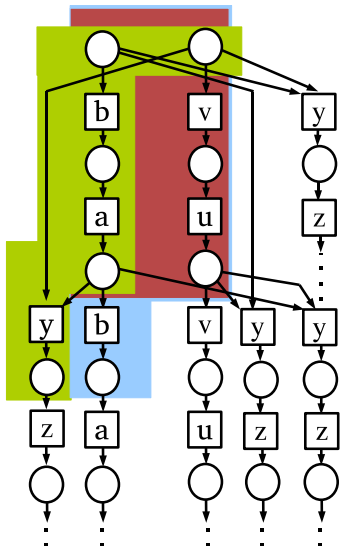
Progress



NOT progressive

Progressive

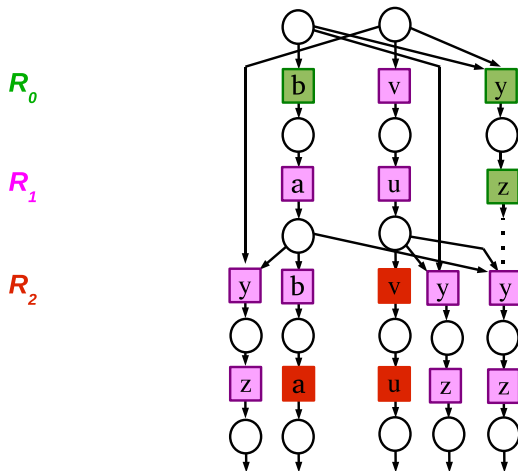
Progress



NOT progressive

Progressive

Progressive

Observable Height: $\mu \equiv 1_{\{a,v\}}$ 

Weak and Strong Diagnosability

- \mathcal{N} a safe Petri net, L (L_{PROG}) its (progressive) configurations,
 - $\lambda : \mathcal{T} \rightarrow A \cup \{\varepsilon\}$ an alarm labeling.
 - $UO \triangleq \lambda^{-1}(\varepsilon)$ the **invisible** and $O \triangleq \mathcal{T} \setminus UO$ the **visible** transitions;
 - $\phi \in UO$ the **fault** transition.
- \mathcal{N} is **strongly diagnosable** iff there is $n \in \mathbb{N}$ such that for any **faulty** $\kappa_\phi \in L_{PROG}$, extension κ of κ_ϕ ($\kappa_\phi \sqsubseteq \kappa$), and **any** $\kappa' \in L$,

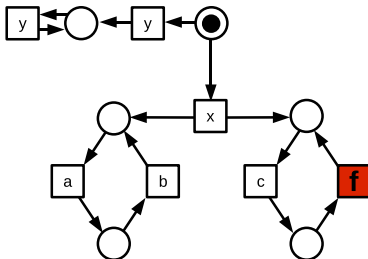
$$\left. \begin{array}{l} \overline{\mathcal{H}}(\kappa) \geq \overline{\mathcal{H}}(\kappa_\phi) + n \\ \kappa \sim_O \kappa' \end{array} \right\} \Rightarrow \kappa' \text{ faulty.}$$

- \mathcal{N} is **weakly diagnosable** iff there is $n \in \mathbb{N}$ such that for any **faulty** $\kappa_\phi \in L_{PROG}$, **progressive** extension κ of κ_ϕ , and **any** $\kappa' \in L_{PROG}$,

$$\left. \begin{array}{l} \underline{\mathcal{H}}(\kappa) \geq \underline{\mathcal{H}}(\kappa_\phi) + n \\ \kappa \sim_O \kappa' \end{array} \right\} \Rightarrow \kappa' \text{ faulty.}$$

What Interleavings can't detect

not strongly diagnosable



... but weakly diagnosable !

Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)**
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"
- 7 Conclusion

Pseudo-Metrics and Topology (WODES 2010)

- Suppose μ is invariant under label (\mathbb{A} -)isomorphisms. Then so are the μ -heights $\mathcal{H}_\mu^*(\bullet)$ and $\mathcal{H}_\mu(\bullet)$; therefore, so is

$$\Psi_\mu(\kappa) \triangleq 2^{-\mathcal{H}_\mu(\kappa)}.$$

- With $\mathbf{K}_1 \sqcap \mathbf{K}_2$ the \subseteq -maximal prefix of \mathbf{K}_1 such that \mathbf{K}_2 has an \mathbb{A} -isomorphic prefix, define:

$$\mathbf{d}_\mu(\kappa_1, \kappa_2) \triangleq \Psi_\mu(\mathbf{K}_1 \sqcap \mathbf{K}_2).$$

- Denote the associated topology as \mathfrak{T}^μ .

Observability and Diagnosability

Definitions

- Let $\text{PES} = (E, \leq, \#, \lambda)$ a labeled PES with $\lambda : E \rightarrow \mathbb{A}$,
- $\eta : \mathbb{A} \rightarrow \mathbb{O}$ a partial mapping into **observation alphabet** \mathbb{O} ,
- $E_\eta \triangleq \{e \mid \eta(\lambda(e)) \downarrow\}$ the **visible** events, and
- $E_\varepsilon \triangleq \{e \mid \eta(\lambda(e)) \uparrow\}$ the **invisible** events.
- With $\mu \equiv \mathbb{1}_{E_\eta}$ obtain **visible height** $\mathcal{H}_\eta(\bullet)$, and **visible metric** $\mathbf{d}_\eta(\bullet, \bullet)$.
- Call PES **observable** iff for all κ ,

$$\mathcal{H}(\kappa) = +\infty \quad \Rightarrow \quad \mathcal{H}_\eta(\kappa) = +\infty.$$

- **Fault** $\phi \in \eta^{-1}(\{\varepsilon\})$
- κ is **faulty** iff $\kappa \cap \lambda^{-1}(\phi) \neq \emptyset$, otherwise **healthy**.

Topological View

Observability and Diagnosability

- Let Ω_F (Ω_{NF}) be the set of faulty (healthy) runs.
- Ω_F is open in \mathfrak{T} ...
- ... but in general neither open nor closed in \mathfrak{T}_η .

N vs F

Fault ϕ is

- **eventually F-diagnosable** for (PES, η) iff Ω_F is open in \mathfrak{T}_η , and
- **eventually N-diagnosable** for (PES, η) iff Ω_{NF} is open in \mathfrak{T}_η .

What for ?

- Unified framework for sequential and PO semantics
- Basis for characterization of more complex properties (to do):
Monitorability, asynchronous controllability, ...
- To do : Add measure , e. g. probability

Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification**
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"
- 7 Conclusion

Invariants

Incidence matrix + Net invariants

- $\mathbf{N} : (\mathcal{P} \times \mathcal{T}) \rightarrow \{-1, 0, 1\}$

$$\mathbf{N}(p, t) \triangleq \begin{cases} 0 & : (pFtFp) \vee \neg(pFt \vee tFp) \\ 1 & : (pFt) \wedge \neg(tFp) \\ -1 & : (tFp) \wedge \neg(pFt) \end{cases} .$$

- **Marking Equation Lemma:** If $\sigma \in \mathcal{T}^*$ and $M \xrightarrow{\sigma} M'$

$$M' = M + \mathbf{N}\bar{\sigma}.$$

- A **\mathcal{T} -invariant** (**\mathcal{T} -semiflow**) of N is a rational-valued solution of $\mathbf{N} \cdot x = 0$; it reproduces M , i.e. $M \xrightarrow{\sigma} M$.
- Violations of **strong diagnosability** correspond to indeterminate \mathcal{T} -semiflows ; more is known, see Giua et al.
- does not allow to check for **weak** diagnosability

Diagnosability Verification

Net unfoldings

Approach by Madalinski, Dague and Nouioua:

- Construct a verifier by $V \triangleq \mathcal{N} \times \mathcal{N}'$ with synchronization on alarm labels of **visible transitions**
- Check whether there exists an infinite run of V on which ϕ occurs, but not ϕ'
- Feasible by use of complete prefix with cutoff criterion "same marking, same fault occurrence vector"
- Extension to **weak diagnosability** : in progress

Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis**
- 6 Exploring "reveals"
- 7 Conclusion

WIP (DISC): Probabilistic Diagnosis

- With R. Boel, E. Fabre et al: extension of stochastic diagnosis (Thorsley/Teneketzis) to Petri nets
- Formalizing PO properties :WIP
- Adapt (?) / develop verification procedures

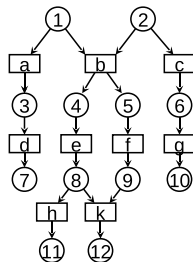
Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"**
- 7 Conclusion

Presenting *Reveals* \triangleright and Facets

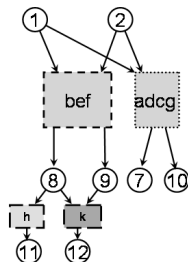
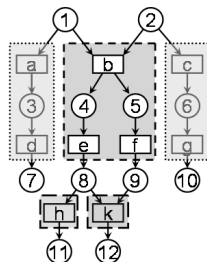
- $a \triangleright c$ (read: a reveals c)
 - iff $\#[c] \subseteq \#[a]$
 - iff occurrence of a implies **inevitable** occurrence of c
- Relation \triangleright computable

Facets: symmetric components (or SCCs) of \triangleright
 \rightarrow *Abstraction*



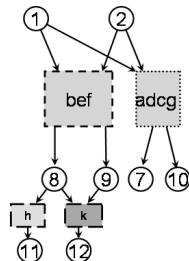
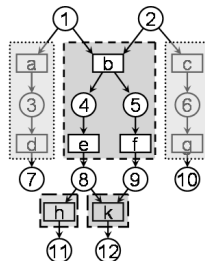
Presenting *Reveals* \triangleright and Facets

- $a \triangleright c$ (read: a reveals c)
 - iff $\#[c] \subseteq \#[a]$
 - iff occurrence of a implies **inevitable** occurrence of c
- Relation \triangleright computable (on bounded prefix)
- **Facets**: symmetric components (or SCCs) of \triangleright
 \rightarrow *Abstraction*



Qualitative Diagnosability (CDC 2008+2009, TAC 2010)

- \mathcal{N} is q -diagnosable iff the sublanguage of facet-closed configurations is diagnosable
- ... i. e. iff the facet abstraction is (ordinary) diagnosable
- Often, need only one visible label per facet
- Facet labels may give quick checks for q -diagnosability



Contents

- 1 Introduction
- 2 Key Concepts
- 3 Pseudometrics and Topology (WODES 2010)
- 4 Diagnosability Verification
- 5 Probabilistic Diagnosis
- 6 Exploring "reveals"
- 7 Conclusion**

Partial Order Diagnosis: An active field

New properties and tasks

- Strong diagnosability implies weak diagnosability, but ..
- does not look "left and right" into concurrent components
- **Weak diagnosis** blends diagnosis of the past and prognosis of the inevitable future: Weakly diagnosed ϕ *cannot be prevented*
- Topological perspective available
- New **Reveals** relation on event structures
- **q**-diagnosability
- TBD/WIP
 - probabilistic diagnosis
 - distribution
 - control, asynchronous games