Asynchronous Diagnosis and *leadsto* in Occurrence Nets

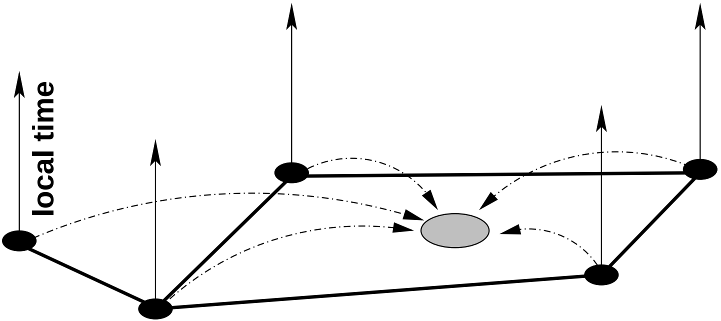
Stefan Haar
INRIA Saclay + LSV
France

January 28, 2009

Contents

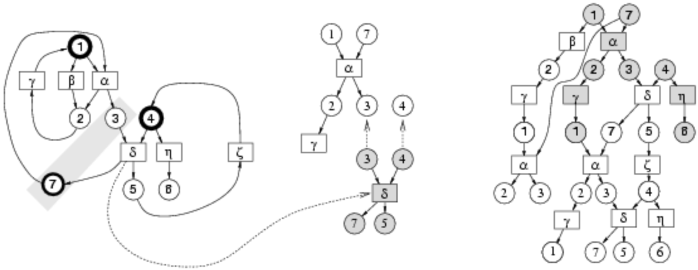
Contents

Fault Diagnosis for Networks



Centralized Diagnoser observes asynchronous alarm streams

Unfoldings and Diagnosis (BFHJ 2003)



Unfoldings: from PNs to ONs

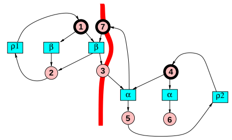
Let $ON = (\mathcal{B}, \mathcal{E}, G, \mathbf{c}^*)$, and $\leqslant \;:=\; G^*$, $< \;:=\; G^+$; set

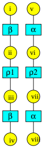
- $e_1 \,\#_m\, e_2$ iff ${}^\bullet e_1 \cap {}^\bullet e_2 \neq \emptyset$
- $x_1 \,\#\, x_2$ iff $\exists\, e_1, e_2 : \; (e_1 \#_m e_2) \wedge (e_1 \leqslant x_1) \wedge (e_2 \leqslant x_2)$
- x_1 **co** x_2 iff neither $(x_1 \leqslant x_2)$ nor $(x_2 < x_1)$ nor $(x_1 \# x_2)$

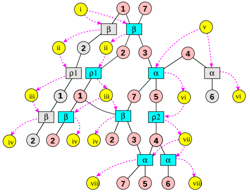
ON is an occurrence net iff:

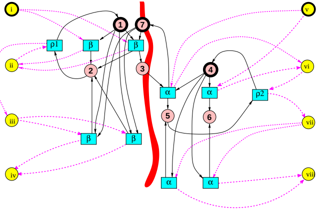
- No self-conflict: $\forall x \in \mathcal{B} \cup \mathcal{E} : \neg[x \# x]$;
- $\leqslant$ is a partial order: $\forall x \in \mathcal{B} \cup \mathcal{E} : \neg[x < x]$;
- $\forall x \in \mathcal{B} \cup \mathcal{E} : |\{x' \mid x' < x\}| < \infty$;
- no backward branching: $\forall b \in \mathcal{B} : |{}^\bullet b| \leq 1$.
- $\mathbf{c}^* := \min(ON) \subseteq \mathcal{B}$.
- **Configuration:** conflict free, downward closed set $\mathbf{c}^* \subseteq \kappa \subseteq \mathcal{B} \cup \mathcal{E}$;
- **Run:** $\subseteq$-maximal configuration ω

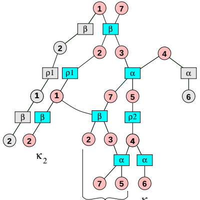
Unfoldings and Diagnosis











Unfoldings and Diagnosis

$\mathbf{C} \in \mathbf{diag}(\mathcal{A})$ iff

$$\exists\ \overline{\mathbf{C}} \in \mathbf{config}(\mathcal{U}_{\mathcal{N}\times\mathcal{A}}) : \mathbf{proj}_{\mathcal{N}}(\overline{\mathbf{C}}) = \mathbf{C},\ \ \mathbf{proj}_{\mathcal{A}}(\overline{\mathbf{C}}) = \mathcal{A}.$$

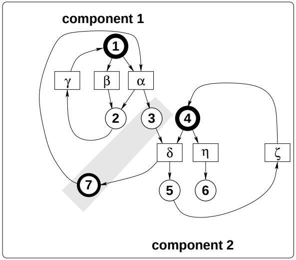
Further Fun

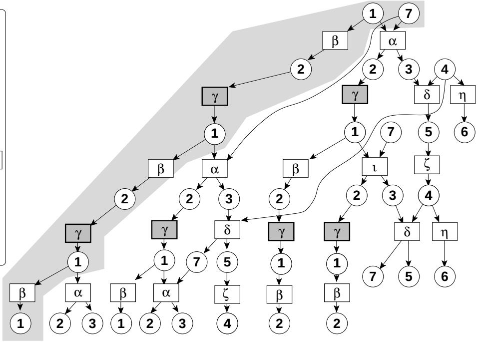
- Distribution
- Dynamic topologies
- Probability of asynchronous runs
- Latencies, nonmonotonicity in timed systems
- **Observability:** do there exist silent cycles ?
- **Diagnosability:** Can fault occurrence be determined after a bounded 'time' ? In particular, do there exist undeterminate cycles ?

Contents

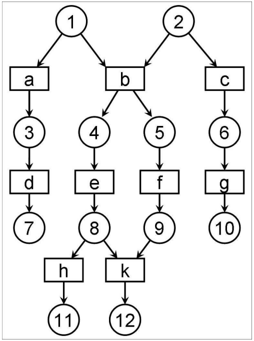
leadsto relation ▷

Motivation: ensure Observability





leadsto relation ▷



$$\forall\, \omega : \quad k \in \omega \Rightarrow e \in \omega \Rightarrow b \in \omega$$

$$a \in \omega \iff \neg(b \in \omega) \iff c \in \omega$$

$$\forall\, \omega : e \in \omega \iff f \in \omega$$

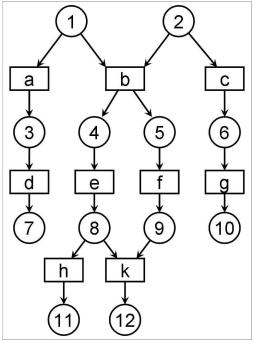
leadsto relation $\triangleright$

- In *ON*, set

$$
\begin{aligned}
\#[x] &:= \{x' \mid x\#x'\} \\
\#_\mu[x] &:= \{y \mid x\#y \ \wedge \ \forall\, z : z < y \Rightarrow \neg(z\#x)\}
\end{aligned}
$$

- x **leads to** y, written $x \triangleright y$, iff $\#[x] \supseteq \#[y]$.
- **THM:** $x \triangleright y$ holds iff for all runs ω $x \in \omega \Rightarrow y \in \omega$, i. e. $x < y \Rightarrow y \triangleright x$.
- But $y \triangleright x$ compatible also with $y < x$ and y **co** x
- $< \subseteq \triangleright^{-1}$
- $\triangleright[x]$ is a configuration.

leadsto relation ▷



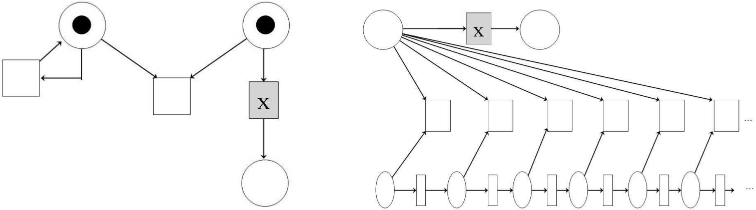
$$\triangleright[h] = \{b, e, f, h\} \quad , \quad \triangleright[k] = \{b, e, f, k\}$$
$$\triangleright[a] = \triangleright[d] = \triangleright[c] = \triangleright[g] \quad = \quad \{a, d, c, g\}$$

leadsto relation

- Theorem: For $\rhd$, it suffices to inspect $\#_\mu[\bullet]$:

$$\#[x] \quad = \quad \{z' \mid \exists y \in \#_\mu[x] : \; y \leqslant z\}.$$

- Caveat: $\#_\mu[x]$ is not necessarily finite:



Safe nets allow to compute ▷

In $\mathcal{U}_{\mathcal{N}}$, $\mathcal{N}$ safe, we have:

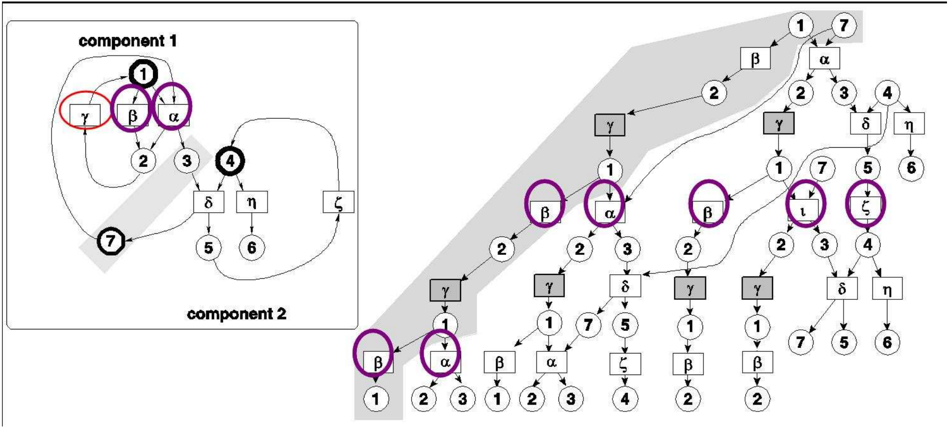
Define *round*(x) to be the minimal n such that x is in the nth complete prefix $\mathcal{U}_n$.

Theorem: For all $n \in \mathbb{N}$ and $\neg(x \triangleright y)$, there exists a **leadsto witness** in $\mathcal{U}_{m+K-1}$, i.e. z such that

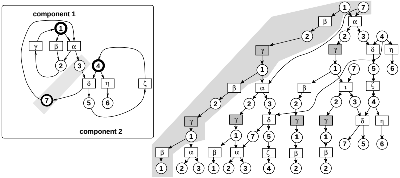
$$z \# y \quad \wedge \quad \neg\,(z \# x).$$

Here, $m = \min(round(x), round(y))$ and K is the number of $\mathcal{N}'$s reachable markings.

Example revisited: Lifting $\triangleright$ to $\mathcal{N}$



Example revisited: Lifting $\rhd$ to $\mathcal{N}$

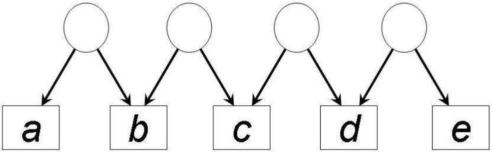


$\rhd_{\mathcal{N}}$	α	β	γ	δ	η	ζ
α	+	−	+	−	−	−
β	−	+	+	−	−	−
γ	−	−	+	−	−	−
δ	+	−	−	+	−	+
η	−	−	−	−	+	−
ζ	+	−	+	+	−	+

▷ is 'superadditive'

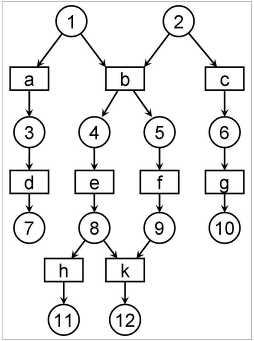
Extend ▷ to sets of events:

$$\triangleright[\{a,e\}] = \{a,c,e\} \neq \triangleright[a] \cup \triangleright[e] = \{a,e\}$$



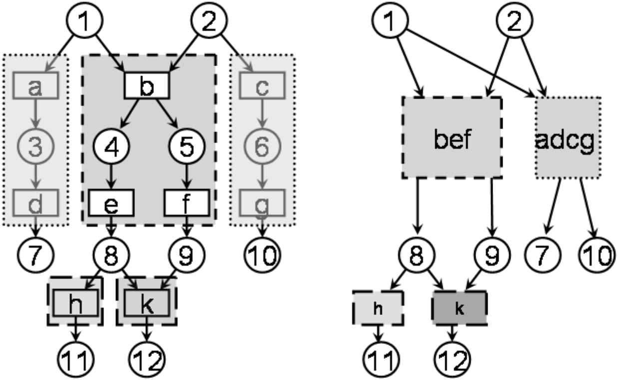
Contents

When ▷ holds both ways



$$\triangleright[b] = \triangleright[e] = \triangleright[f] = \{b, e, f\}$$

Facets



Facets and their properties

Call **facet** any strongly connected component δ of $\triangleright$. Then:

- δ is $\#$-free
- δ is **convex**: $x \ < \ y \ < \ z$ and $x, z \in \delta$ imply $y \in \delta$
- $b^\bullet \cap \delta(b) \neq \emptyset \Rightarrow |b^\bullet| = 1$.
- Maximal nodes in δ are conditions
- Facets are abstractions, and the set of facets Δ is an AES and an ON
- $x \mapsto \delta(x)$ preserves runs
- Allow e.g. for *qualitative* diagnosability analysis

Contents

Results and Outlook

- *leadsto* relation effectively computable
- $\triangleright$ formalizes occurrence dependencies under progress and information content of configurations
- Structures search for minimal observability : which events must be visible to allow control, diagnosis, verification, ...
- Large unfoldings can be reduced by facet abstraction if only eventual occurrence matters
- Facet abstraction preserves set of runs
- Todo :
  - Improve bounds on $\#_\mu[\bullet]$-computation
  - Read nets
  - Check properties + morphisms of *extended PES* $(E, \leqslant, \#, \triangleright)$

Results and Outlook

To Do

- Refine *diagnosis* procedure
- Improve bounds on $\#_\mu[\bullet]$-computation
- Read nets
- Check properties + morphisms of *extended PES* $(E, \leqslant, \#, \triangleright)$
- Logics