MeFoSyLoMa 11/7/2014

Weak Fairness is So Revealing !

Stefan Haar

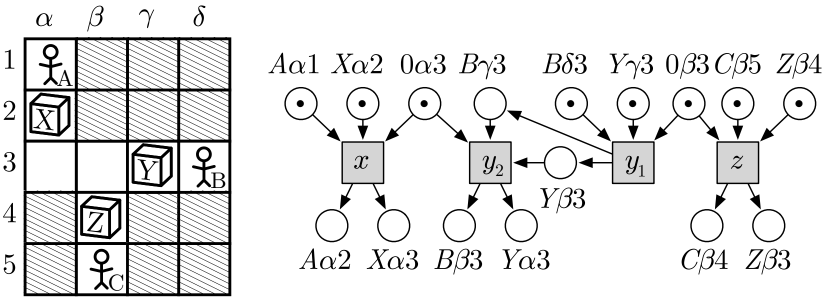
INRIA and LSV, CNRS and ENS Cachan

with S. Balaguer, Th. Chatain, V. Germanos, C. Kern, V. Khomenko, C. Rodriguez, S. Schwoon . . .

July 11, 2014

Weak Fairness is So Revealing !

Some actions reveal one another

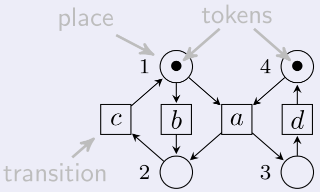


z prevents y_1 ... and therefore makes x inevitable:

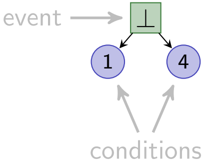
$$z \textbf{ reveals } x \quad : \quad z \rhd x$$

Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

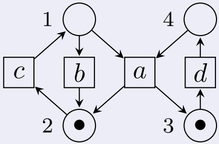


Process: representation of a non-sequential run as a partial order.

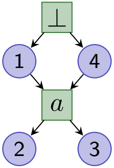


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

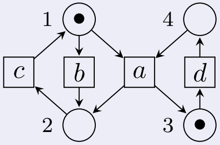


Process: representation of a non-sequential run as a partial order.

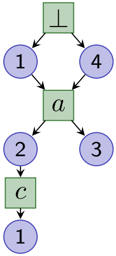


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

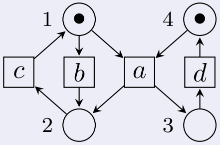


Process: representation of a non-sequential run as a partial order.

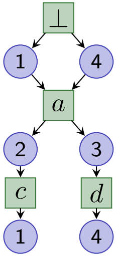


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

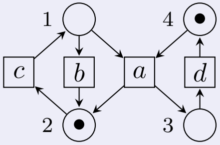


Process: representation of a non-sequential run as a partial order.

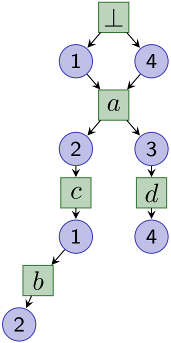


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

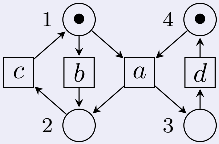


Process: representation of a non-sequential run as a partial order.



Petri nets, Processes, Branching Processes and Unfoldings

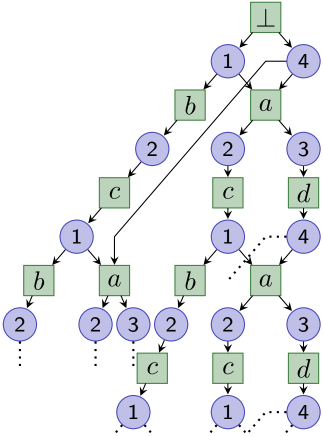
Petri net:



Process: representation of a non-sequential run as a partial order.

Branching process: representation of several runs.

Unfolding: maximal branching process.

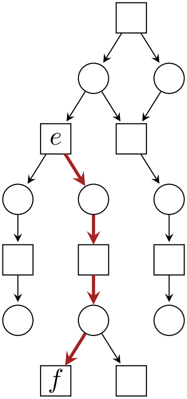


Nets and Structural Relations

The structure of a net induces three relations over its nodes:

Causality $\leq$

$e \leq f \quad \overset{def}{\Leftrightarrow} \quad e\ F^*\ f$ (directed path from e to f)



$e \leq f$

Nets and Structural Relations

The structure of a net induces three relations over its nodes:

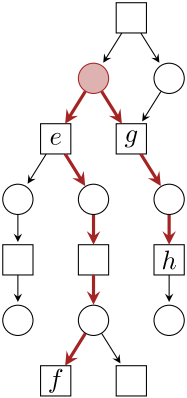
Causality $\leq$

$e \leq f \overset{def}{\Leftrightarrow} e\ F^*\ f$ (directed path from e to f)

Conflict $\#$

$e \#_d g \overset{def}{\Leftrightarrow} e \neq g \wedge {}^\bullet e \cap {}^\bullet g \neq \emptyset$

$f \# h \overset{def}{\Leftrightarrow} \exists e \leq f, g \leq h : e \#_d g$



$e \#_d g$

$f \# h$

Nets and Structural Relations

The structure of a net induces three relations over its nodes:

Causality $\leq$

$e \leq f \quad \overset{def}{\Leftrightarrow} \quad e\ F^*\ f$ (directed path from e to f)

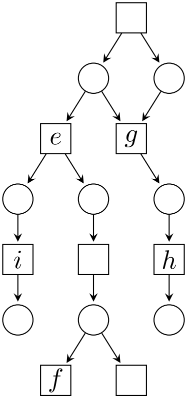
Conflict $\#$

$e \#_d g \overset{def}{\Leftrightarrow} \quad e \neq g \wedge {}^\bullet e \cap {}^\bullet g \neq \emptyset$

$f \# h \overset{def}{\Leftrightarrow} \quad \exists e \leq f, g \leq h : e \#_d g$

Concurrency co

$f\ co\ i \quad \overset{def}{\Leftrightarrow} \quad \neg(i \# f) \wedge \neg(i \leq f) \wedge \neg(f \leq i)$



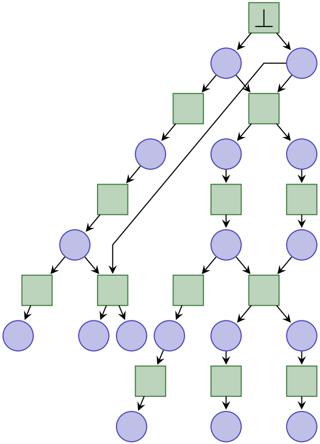
$f\ co\ i$

Occurrence Nets [Nielsen, Plotkin, Winskel, 1980]

Definition (Occurrence net)

An *occurrence net* (ON) is a net (B, E, F) where B and E are the sets of *conditions* and *events*, and which satisfies:

1. no self-conflict,
2. acyclicity
3. finite causal pasts: $\forall e \in E$, $\lceil e \rceil \stackrel{def}{=} \{e' : e' \leq e\}$ is finite.
4. no backward branching for conditions,
5. $\perp \in E$ is the only $\leq$-minimal node (event $\perp$ creates the initial conditions).



Weak Fairness in PNs

Spoilers

Let $t \in T$. The set of t's *spoilers* is

$$spoil(t) \stackrel{def}{=} \{t' \in T \mid {}^\bullet t' \cap {}^\bullet t \neq \emptyset\}.$$

Note : $t \in spoil(t)$!

Weak Fairness (Vogler 1995)

Infinite run $\sigma = t_1 t_2 \ldots \in T^\infty$ of N, with marking sequence $m_1 m_2 \ldots$, is *weakly fair for* $t \in T$ if and only if for all $i \in \mathbb{N}$,

$$m_i \xrightarrow{t} \quad \Rightarrow \quad \exists\, j > i : \; t_j \in spoil(t).$$

σ is *weakly fair* iff it is w.f. for all $t \in T$.

Theorem

σ is weakly fair iff it is the interleaving of some maximal run ω of N.

Configurations and Runs

Definitions (Configurations and Runs of an ON)

A *configuration* is a set ω of events which is

- causally closed: $\forall e \in \omega, \lceil e \rceil \subseteq \omega$,
- conflict free: $\forall e \in \omega, \#[e] \cap \omega = \emptyset$.

A run is *maximal* iff it is maximal w.r.t. $\subseteq$.

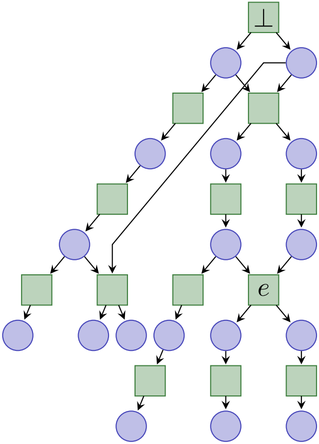
Notation

Ω denotes the set of *maximal runs*.

Interpretation

Ω gives exactly the *weakly fair* (nonsequential) executions:

- No transition remains enabled for ever (i.e. without firing, or being disabled by a conflicting transition): *weak fairness*



Configurations and Runs

Definitions (Configurations and Runs of an ON)

A *configuration* is a set ω of events which is

- causally closed: $\forall e \in \omega, \lceil e \rceil \subseteq \omega$,
- conflict free: $\forall e \in \omega, \#[e] \cap \omega = \emptyset$.

A run is *maximal* iff it is maximal w.r.t. $\subseteq$.

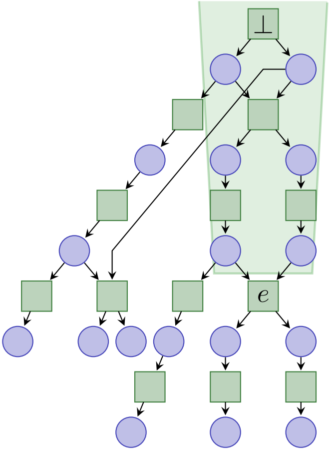
Notation

Ω denotes the set of *maximal runs*.

Interpretation

Ω gives exactly the *weakly fair* (nonsequential) executions:

- No transition remains enabled for ever (i.e. without firing, or being disabled by a conflicting transition): *weak fairness*



Configurations and Runs

Definitions (Configurations and Runs of an ON)

A *configuration* is a set ω of events which is

- causally closed: $\forall e \in \omega, \lceil e \rceil \subseteq \omega$,
- conflict free: $\forall e \in \omega, \#[e] \cap \omega = \emptyset$.

A run is *maximal* iff it is maximal w.r.t. $\subseteq$.

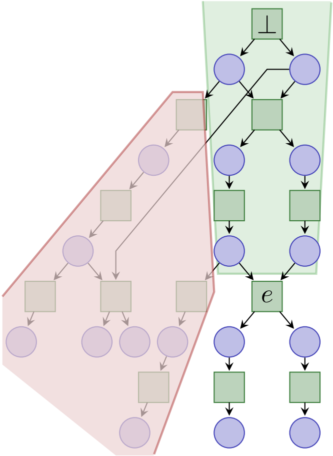
Notation

Ω denotes the set of *maximal runs*.

Interpretation

Ω gives exactly the *weakly fair* (nonsequential) executions:

- No transition remains enabled for ever (i.e. without firing, or being disabled by a conflicting transition): *weak fairness*



Structural relations vs logical relations

- The structural relations imply *logical dependencies* between event occurrences:
  - $a \leq b \Rightarrow (\forall \omega \in \Omega, b \in \omega \Rightarrow a \in \omega)$,
  - $a \# b \Leftrightarrow \forall \omega \in \Omega, \{a, b\} \nsubseteq \omega$,
- Some logical dependencies ("if a then b") implied by weak fairness cannot be expressed by the structural relations.

Structural relations vs logical relations

- The structural relations imply *logical dependencies* between event occurrences:
  - $a \leq b \Rightarrow (\forall \omega \in \Omega, b \in \omega \Rightarrow a \in \omega)$,
  - $a \# b \Leftrightarrow \forall \omega \in \Omega, \{a, b\} \not\subseteq \omega$,
- Some logical dependencies ("if a then b") implied by weak fairness cannot be expressed by the structural relations.

Here

- Formalization of logical dependencies in a *relational framework* with *reveals* relations $\triangleright$ and $\twoheadrightarrow$
- Reduction of Occurrence nets by contracting *facets*
- Concurrency vs Independence : *tight nets*
- Connection with diagnosis under partial observation

Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

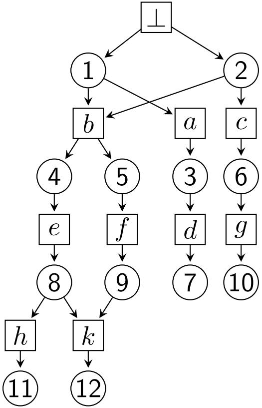
Event e *reveals event* f, *written* $e \triangleright f$, *iff* $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Causal closure

$\forall x, y \in E, x \leq y \Rightarrow y \triangleright x$

$d \triangleright a$,
$h \triangleright \perp$,
$a \triangleright d$
because of weak fairness,
$a \triangleright c$
because for any maximal run ω,

$$\begin{aligned} a \in \omega \quad &\Rightarrow \quad b \notin \omega \\ &\Rightarrow \quad c \in \omega \text{ (weak fairness)} \end{aligned}$$



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Causal closure

$\forall x, y \in E, x \leq y \Rightarrow y \triangleright x$

$d \triangleright a$,

$h \triangleright \perp$,

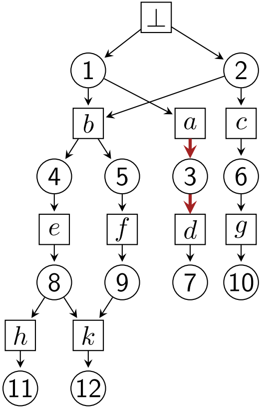
$a \triangleright d$

because of weak fairness,

$a \triangleright c$

because for any maximal run ω,

$$a \in \omega \quad \Rightarrow \quad b \notin \omega$$
$$\Rightarrow \quad c \in \omega \text{ (weak fairness)}$$



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Causal closure

$\forall x, y \in E, x \leq y \Rightarrow y \triangleright x$

$d \triangleright a$,

$h \triangleright \perp$,

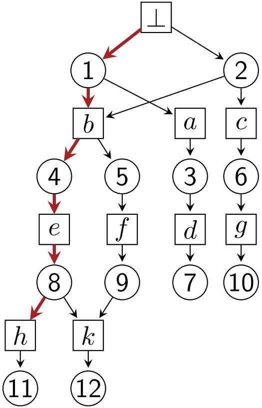
$a \triangleright d$

because of weak fairness,

$a \triangleright c$

because for any maximal run ω,

$$\begin{aligned} a \in \omega &\Rightarrow b \notin \omega \\ &\Rightarrow c \in \omega \text{ (weak fairness)} \end{aligned}$$



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Causal closure

$\forall x, y \in E, x \leq y \Rightarrow y \triangleright x$

$d \triangleright a$,

$h \triangleright \perp$,

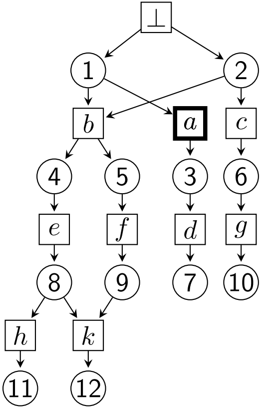
$a \triangleright d$

because of weak fairness,

$a \triangleright c$

because for any maximal run ω,

$$\begin{aligned} a \in \omega &\Rightarrow b \notin \omega \\ &\Rightarrow c \in \omega \text{ (weak fairness)} \end{aligned}$$



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Causal closure

$\forall x, y \in E, x \leq y \Rightarrow y \triangleright x$

$d \triangleright a$,

$h \triangleright \perp$,

$a \triangleright d$

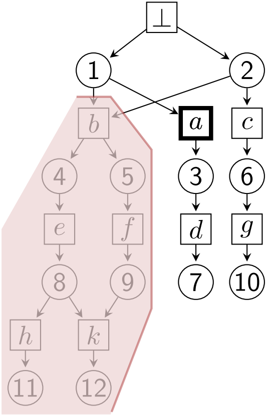
because of weak fairness,

$a \triangleright c$

because for any maximal run ω,

$a \in \omega \quad \Rightarrow \quad b \notin \omega$

$\quad\quad\quad \Rightarrow \quad c \in \omega$ (weak fairness)



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Lemma

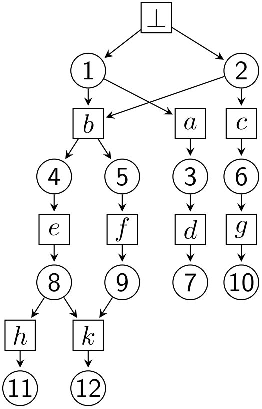
Lemma: Characterization of Ω by $\#$ A set of events ω is a maximal run iff

$$\forall a \in E, a \notin \omega \Leftrightarrow \#[a] \cap \omega \neq \emptyset$$

where $\#[e] \stackrel{def}{=} \{f \in E \mid f \# e\}$.

Characterization of $\triangleright$ by $\#$

$\forall e, f \in E, e \triangleright f \Leftrightarrow \#[f] \subseteq \#[e]$
i.e. any event that could prevent the occurrence of f is prevented by the occurrence of e.



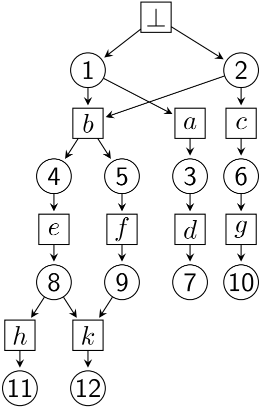
Reveals Relation

Definition (Reveals relation $\triangleright$)

Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Properties

- $\triangleright$ is reflexive and transitive, but it is not antisymmetric in general.
- The conflict relation ($\#$) is inherited under $\triangleright^{-1}$: $g \triangleright a \wedge a \# b \Rightarrow g \# b$.



Computing $\triangleright$: Finding witnesses [HKS 2011]

Definition

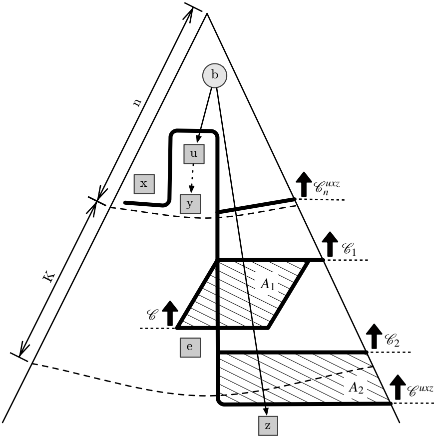
Let U_M be the first complete finite prefix of (N, M), and K_M the height of U_M; then set

$$K := \max_{M \in \mathcal{R}(M_0)} K_M.$$

Theorem [HKS 2011]

For any two events x, y such that $\neg(x \triangleright y)$, there exists an event z such that

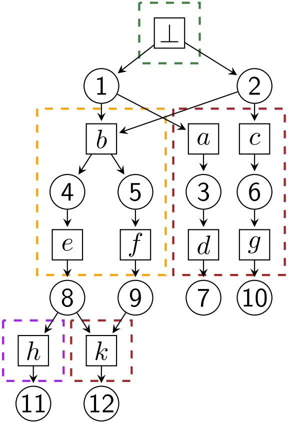
$$\begin{array}{rcl} z & \# & y \\ \neg(z & \# & x) \\ \mathbf{h}(z) & \leq & K + \max(\mathbf{h}(x), \mathbf{h}(y)) \end{array}$$



Facets Abstraction [H2010,BCH2011]

Definition (Facets)

A facet of an ON is an equivalence class of $\sim = \triangleright \cap \triangleright^{-1}$.



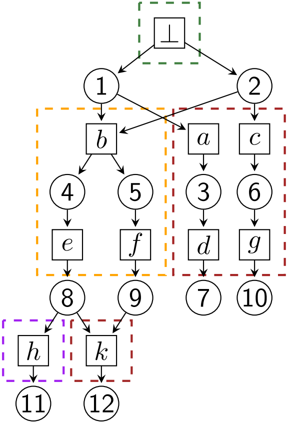
Facets Abstraction [H2010,BCH2011]

Definition (Facets)

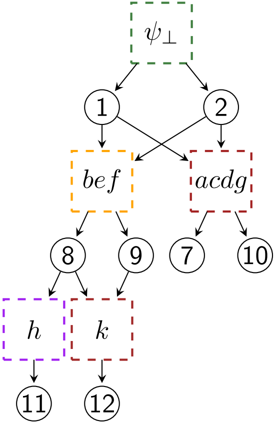
A facet of an ON is an equivalence class of $\sim = \triangleright \cap \triangleright^{-1}$.

Definition (Reduced ON)

A reduced ON is an ON (B, Ψ, F) such that $\forall \psi_1, \psi_2 \in \Psi$, $\psi_1 \sim \psi_2 \Leftrightarrow \psi_1 = \psi_2$.



facets can be contracted into events



Binary Relations on Ψ and Reduced Nets [H2010,BCH2011]

The causality ($\leq$), conflict ($\#$), concurrency (co) and reveals ($\triangleright$) relations naturally extend to Ψ.

Lemma

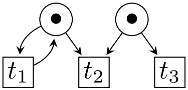
Lemma 1 $\triangleright$ *is a partial order on* Ψ *(*$\triangleright$ *is antisymmetric by definition of a reduced ON).*

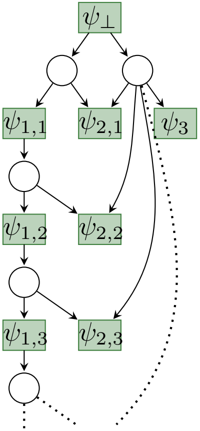
$(\Psi, \triangleright^{-1}, \#)$ is an event structure

- $\triangleright^{-1}$ is a partial order, ✓
- The set $\{\psi' \mid \psi \triangleright \psi'\}$ is not always finite, ✗
- $\#$ is inherited under $\triangleright^{-1}$. ✓

Infinite Revealed Set [BCH2011]

For a facet ψ, the set $\{\psi' \mid \psi \triangleright \psi'\}$ may not be finite.





$\psi_3 \triangleright \psi_{1,i},\ \forall i \in \mathbb{N}^*$

Binary Relations on Ψ [BCH2011]

The causality ($\leq$), conflict ($\#$), concurrency (co) and reveals ($\triangleright$) relations naturally extend to Ψ.

Lemma

Lemma 1 $\triangleright$ is a partial order on Ψ ($\triangleright$ is antisymmetric by definition of a reduced ON).

Lemma

Lemma 2 For any finite reduced ON (B, Ψ, F), $(\Psi, \triangleright^{-1}, \#)$ is a prime event structure since:

- *$\triangleright^{-1}$ is a partial order,*
- *$\forall \psi \in \Psi$, the set $\{\psi' \mid \psi \triangleright \psi'\}$ is finite,*
- *$\#$ is inherited under $\triangleright^{-1}$.*

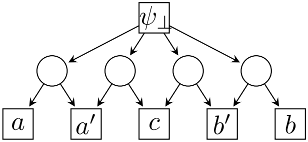
Concurrency vs Logical Independency [BCH2011]

- $\#$, $\leq$ and co are mutually exclusive.

Structural relations and logical dependencies

- $a \# b \Leftrightarrow$ for any run ω, $\{a, b\} \not\subseteq \omega$.
- $a \leq b \Rightarrow$ for any run ω, $b \in \omega \Rightarrow a \in \omega$ $(b \triangleright a)$,
- Does a co b mean a and b are logically independent ?

  No, they can be related by $\triangleright$.

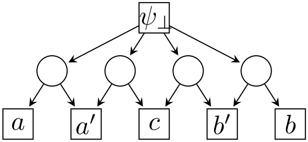


c co a and $c \triangleright a$

a co b and a ind b.

Concurrency vs Logical Independency [BCH2011]

- $\#$, $\leq$ and co are mutually exclusive.



Structural relations and logical dependencies

- $a \# b \Leftrightarrow$ for any run ω, $\{a, b\} \not\subseteq \omega$.
- $a \leq b \Rightarrow$ for any run ω, $b \in \omega \Rightarrow a \in \omega$ $(b \triangleright a)$,
- Does a co b mean a and b are logically independent ?
  No, they can be related by $\triangleright$.

c co a and $c \triangleright a$
a co b and a ind b.

Independency relation ind

$$\forall a, b \in \Psi, \quad a \; ind \; b \quad \overset{def}{\Leftrightarrow} \quad \neg(a \# b) \wedge \neg(b \triangleright a) \wedge \neg(a \triangleright b)$$
$$\Leftrightarrow \quad a \; co \; b \wedge \neg(b \triangleright a) \wedge \neg(a \triangleright b)$$

- $\#$, $\triangleright$ and ind are also mutually exclusive.

Minimal $\rhd$ and $\#$ [BCH2011]

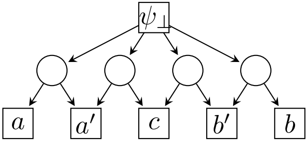
Immediate conflict relation $\#_i$

$$a \,\#_i\, b \overset{def}{\Leftrightarrow} a \,\#\, b \wedge \nexists c : \begin{array}{l} (c \neq a \wedge a \rhd c \wedge c \,\#\, b) \vee \\ (c \neq b \wedge b \rhd c \wedge c \,\#\, a) \end{array}$$

Immediate reveals relation $\rhd_i$

Transitive reduction of $\rhd$: let $a \rhd_i b \overset{def}{\Leftrightarrow}$ iff

- $a \rhd b$ and $a \neq b$
- for all c: $a \rhd c \rhd b \Rightarrow c \in \{a, b\}$



$$\Omega = \{\{\psi_\perp, a, b, c\}, \{\psi_\perp, a, b'\}, \{\psi_\perp, a', b\}, \{\psi_\perp, a', b'\}\}$$

$\neg(c \,\#_i\, a')$ since $c \rhd a$ and $a \,\#\, a'$
$\neg(c \rhd_i \psi_\perp)$ since $c \rhd a$ and $a \rhd \psi_\perp$

Remarks

- $\rhd = \rhd_i^*$,
- $\# = (\rhd_i^{-1})^* \circ \#_i \circ \rhd_i^*$ ($\rhd$-inheritance of $\#$),
- Therefore $\rhd_i$ and $\#_i$ define Ω (characterization of Ω by $\#$).

"Tightening" a Reduced ON [BCH2011]

Tight net

A tight net is a reduced ON (B, Ψ, F) such that $\forall a, b \in \Psi$, $a \rhd b \Leftrightarrow b \leq a$.

Violations of tightness

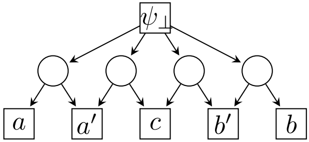
$a, b \in \Psi$ such that

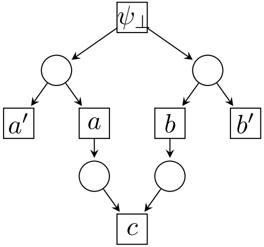
- $a \; co \; b$
- $a \rhd b$

Net Surgery

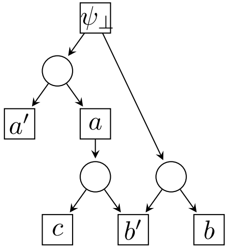
Add a condition from b to a for all a, b such that

- $a \; co \; b$
- $a \rhd_i b$





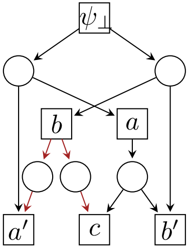
Another Example for Tightening [BCH2011]



$\mathcal{N}$

Constraints

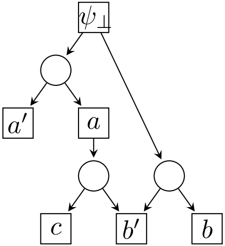
$$\begin{array}{lll} a & \#_i & a' \\ b & \#_i & b' \\ \\ a & \triangleright_i & \psi_\perp \\ b & \triangleright_i & \psi_\perp \\ c & \triangleright_i & a \\ c & \triangleright_i & b \\ a' & \triangleright_i & b \\ b' & \triangleright_i & a \end{array}$$



$\mathcal{N}'$

$$\Omega = \big\{\{\psi_\perp, a, b, c\}, \{\psi_\perp, a, b'\}, \{\psi_\perp, a', b\}\big\}$$

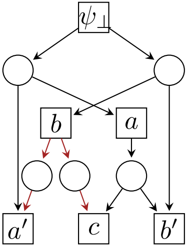
Another Example for Tightening [BCH2011]



$\mathcal{N}$

Constraints

$$
\begin{array}{lll}
a & \#_i & a' \\
b & \#_i & b' \\
\\
a & \triangleright_i & \psi_\perp \\
b & \triangleright_i & \psi_\perp \\
c & \triangleright_i & a \\
c & \triangleright_i & b \\
a' & \triangleright_i & b \\
b' & \triangleright_i & a
\end{array}
$$



$\mathcal{N}'$

$$\Omega = \big\{\{\psi_\perp, a, b, c\}, \{\psi_\perp, a, b'\}, \{\psi_\perp, a', b\}\big\}$$

Definition (Tight net)

A tight net is a reduced ON (B, Ψ, F) *such that* $\forall a, b \in \Psi$, $a \triangleright b \Leftrightarrow b \leq a$.

Weak Fairness is So Revealing !

Reveal Your Faults: Partial observation and Diagnosis

Assumptions

- Possible behaviours well-known
- Current execution only partially visible

Goal:

- Determine, from partial observations,
  whether some invisible event (fault) has occurred.

Sequential Semantics Misses a Point

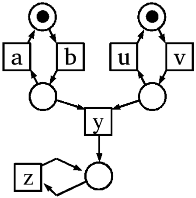
Suppose that

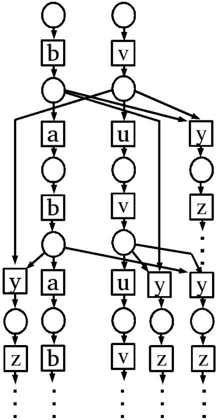
- $T_O = \{b, y\}$
- $\Phi = \{v\}$

v will be correctly diagnosed if y occurs. What if not ? If

$$bbbbbb\ldots$$

is observed, what do we infer about v ?



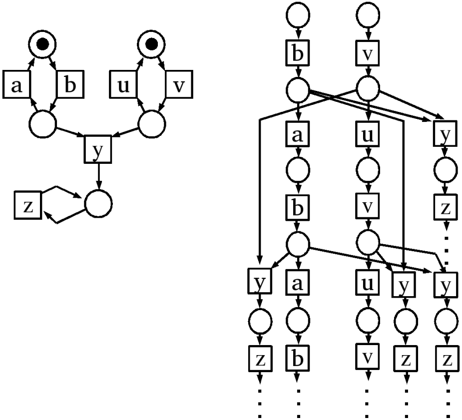


It's about weak fairness !

Still with

- $T_O = \{b, y\}$
- $\Phi = \{v\}$

the only way for the system to do b^ω is to be *unfair* to v: always enabled, never fired
HERE: diagnosis under weak fairness



Extended Reveals+Diagnosis

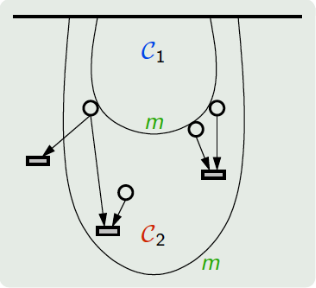
Application

- $A \twoheadrightarrow B$ iff ρ's *containing* A must *hit* B
- Used for *weak diagnosis*:
  Given an observation pattern α, are *all* weakly fair extensions of explanations of α faulty ?

Lemma

There is ω weakly-fair and fault-free iff there are configurations $\mathcal{C}_1, \mathcal{C}_2$ such that:

1. $\mathcal{C}_1 \subseteq \mathcal{C}_2$
2. $mark(\mathcal{C}_1) = mark(\mathcal{C}_2)$
3. $\mathcal{C}_1$ enables $e \Rightarrow spoilers(e) \cap \mathcal{C}_2 \neq \emptyset$
4. $\mathcal{C}_2$ is fault-free



Weak Diagnosis Framework

Setup

- Safe PN $N = (P, T, F, M_0)$ with unfolding $\mathcal{U}_N = (B, E, G, m_0, f)$ and labelling $\lambda : T \to \mathcal{A} \cup \{\varepsilon\}$
- $T_{ubs} \stackrel{def}{=} \lambda^{-1}(\{\varepsilon\})$, $T_{obs} \stackrel{def}{=} T \backslash T_{ubs}$, $E_{ubs} \stackrel{def}{=} f^{-1}(T_{ubc})$, $E_\phi \stackrel{def}{=} f^{-1}(\{\phi\})$etc.
- Assume observations are *Labeled Partial Orders (LPO)* $lpo(C) = (S_C, <_C, \lambda_C)$ over $\mathcal{A}$
- $obs(C) \stackrel{def}{=} compat(lpo(C))$: the lpo's *compatible* with $lpo(C)$, i.e. labeled order extensions of $lpo(C)$.
- C *explains observation pattern* α iff $\alpha \in obs(C)$
- $expl(\alpha) : \{C \mid \alpha \in obs(C)\}$

Weak Diagnosis

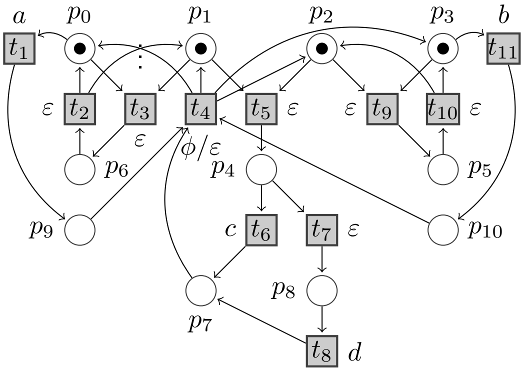
Observation pattern α *weakly diagnoses* fault ϕ iff

$$C \in expl(\alpha) \quad \Rightarrow \quad C \twoheadrightarrow E_\phi$$

Example

Observation pattern α *weakly diagnoses* fault ϕ iff

$$C \in expl(\alpha) \quad \Rightarrow \quad C \twoheadrightarrow E_\phi$$

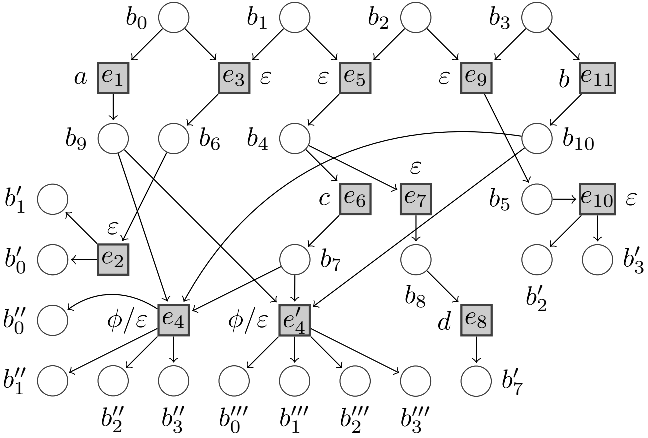


Example

Any α containing $\{a, b\}$ or intersecting $\{c, d\}$ (weakly) diagnoses ϕ since, e.g.,

$$\{e_1, e_{11}\} \rightharpoonup \{e_4, e_4'\} \subseteq E_\phi$$

$$\{e_6\} \rightharpoonup \{e_4, e_4'\} \quad , \quad \{e_8\} \rightharpoonup \{e_4, e_4'\}$$



Solving the weak diagnosis problem

Weak Diagnosis Problem

Need to decide:

$$C \in expl(\alpha) \quad \overset{???}{\Longrightarrow} \quad C \twoheadrightarrow E_\phi \qquad\qquad (*)$$

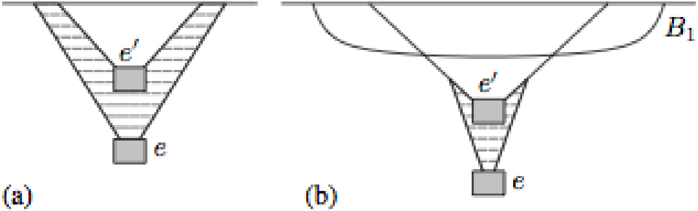
Reduction

To check $(*)$, assume w.l.o.g. $C = \perp$

Summary

- *Bounded* prefixes suffice to compute all succinct explanations
- Complete finite prefixes can be enriched by finitely many spoilers to exhibit witnesses for "non-diagnosis" (if they exist)

Towards weak diagnosis



- Take a *marking-complete* prefix B_1
- Stop unfolding at *sp-cutoff events*: any e such that there is $e' < e$ satisfying, for $D \stackrel{def}{=} [e]\backslash[e']$,
  - $f({}^\bullet D \backslash D^\bullet) = f(D^\bullet \backslash {}^\bullet D)$
  - $B_1 \cap {}^\bullet D = \emptyset$

  I.e. e and e' spoil exactly the same events enabled by configurations from B_1.

Decision method

Prefixes needed

- P_α: contains all *succinct* explanations of α
- P^1: marking-complete
- P^2: contains all *non-sp-cutoffs*; $P^1 \sqsubseteq P^2$

ALL ARE FINITE !!

Encoding in SAT

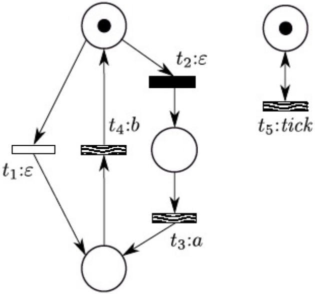
$$config(l, \mathcal{P}) \stackrel{def}{=} \Big(\bigwedge_{e \in E} \bigwedge_{e' \in {}^{\bullet\bullet}e} (v_e^l \Rightarrow v_{e'}^l) \Big) \quad \wedge$$

$$\Big(\bigwedge_{c \in B, \{e_1, \ldots, e_n\} = c^\bullet} amo(v_{e_1}^l, \ldots, v_{e_n}^l) \Big) \quad \wedge \quad \Big(\bigwedge_{c \in B} v_c^l \Leftrightarrow \big(\bigwedge_{e \in {}^\bullet c} v_e^l \wedge \bigwedge_{e \in c^\bullet} \neg v_e^l \big) \Big)$$

- Similarly : configuration containment, reachability, enabling, spoiling, explanation,...
- Diagnosis checkable with SAT solvers

Weak Fairness is So Revealing !

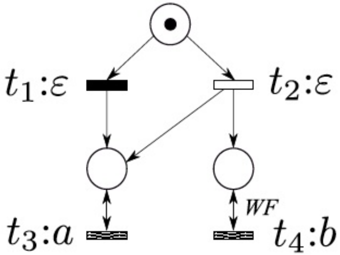
Checking Diagnosability under WF [ACSD 2014]



Effect of concurrent component on the right

- Only t_5 destroys diagnosability
- Once t_3 is WF, net is diagnosable

A non-WF-Diagnosable Net ...



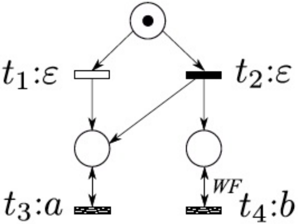
Def: WF-diagnosability

An LPN is WF-diagnosable iff each infinite WF execution σ containing a fault has a finite prefix $\hat{\sigma}$ such that every infinite WF execution r with $\lambda(\hat{\sigma}) \sqsubseteq \lambda(r)$ contains a fault.

Note:

Fault Transition depicted in black

. . . becomes WF-diagnosable with a different fault



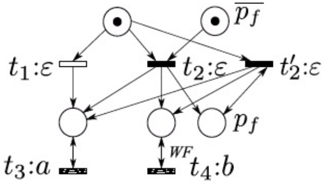
Def: WF-diagnosability

An LPN is WF-diagnosable iff each infinite WF execution σ containing a fault has a finite prefix $\hat{\sigma}$ such that every infinite WF execution r with $\lambda(\hat{\sigma}) \sqsubseteq \lambda(r)$ contains a fault.

Note:

Fault Transition depicted in black

Checking WF-Diagnosability: Fault Tracking Net



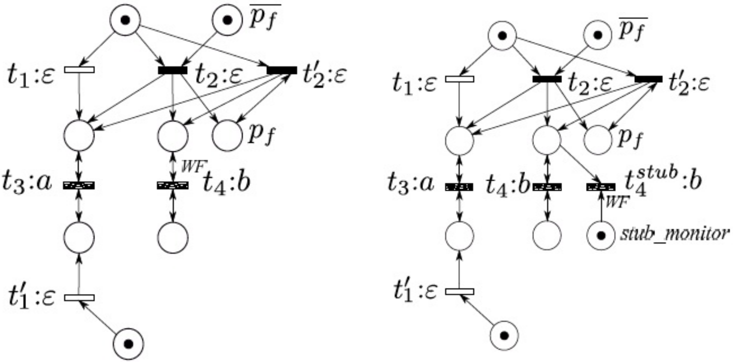
FTN

- Extend N with

Note:

FTN bisimilar to N

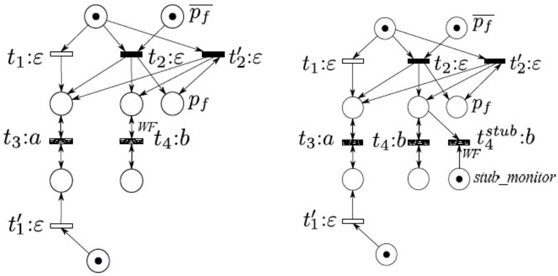
Checking WF-Diagnosability: Verifier Net



Verifier 1

- Synchronize FTN N_{Ft} with copy N'_{Ft} of itself on observable transitions
- Remove from product all observable transitions of N_{Ft} .
- Remove from Ns all observable and fault transitions of N'_{Ft}.
- Call the resulting net V.
- N is diagnosable iff $diag = \Box\overline{p_f}$ holds in V

Checking WF-Diagnosability: Verifier Net



Verifier 2

- Synch FTN N_{Ft} with copy N'_{Ft} of itself on obs; fused transitions non-WF
- Turn all observable transitions of N_{Ft} into stubs.
- Remove all observable and fault transitions of N'_{Ft}; all remaining transitions from $N'_{Ft}$are non-WF
- Call the resulting net V_{WF}.
- N is diagnosable iff $diag = \Box\overline{p_f} \vee \neg stub\_monitor$ holds in V_{WF}

Weak Fairness is So Revealing !

Conclusion

Weak Fairness

- Impact on semantics captured by structural relations
- Exploited in diagnosis ...
- ... and diagnosability

Temporal vs. logical view of event structures

- $(\leq, \#, co)$ vs $(\triangleright, \#$ and $ind)$
- Extended reveals $\twoheadrightarrow$

To Do

- Link with Opacity / Non-interference
- Use in Control / Test / ... ?
- Extend to contextual, timed, probabilistic models . . .

THANKS !