KOSMOS workshop

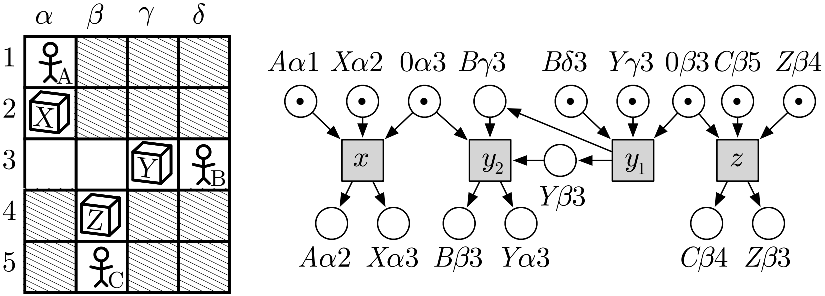
Concurrency Issues

MExICo Team

INRIA and LSV, CNRS and ENS Cachan

November 27, 2013

Some actions reveal one another

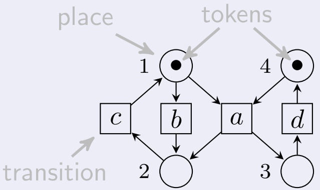


z prevents y_1 ... and therefore makes x inevitable:

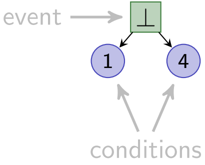
$$z \textbf{ reveals } x \quad : \quad z \triangleright x$$

Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

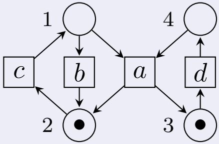


Process: representation of a non-sequential run as a partial order.

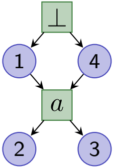


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

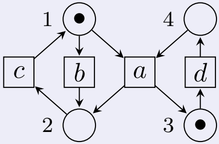


Process: representation of a non-sequential run as a partial order.

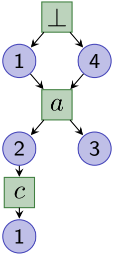


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

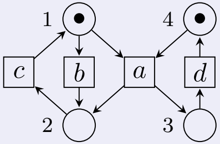


Process: representation of a non-sequential run as a partial order.

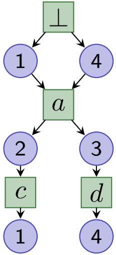


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

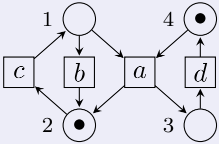


Process: representation of a non-sequential run as a partial order.

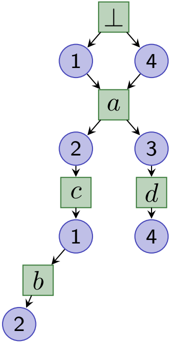


Petri nets, Processes, Branching Processes and Unfoldings

Petri net:

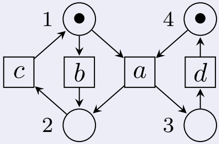


Process: representation of a non-sequential run as a partial order.



Petri nets, Processes, Branching Processes and Unfoldings

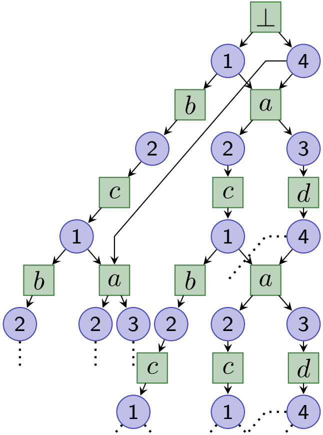
Petri net:



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

Branching process: representation of several runs.

Unfolding: maximal branching process.

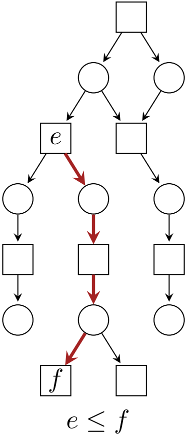


Nets and Structural Relations

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)



Nets and Structural Relations

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

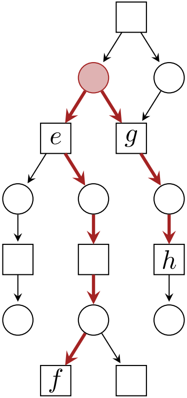
Causality $\leq$

$e \leq f \overset{def}{\Leftrightarrow} e\ F^*\ f$ (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 $\leq$

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

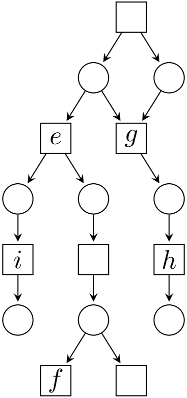
Conflict $\#$

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

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

Concurrency co

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



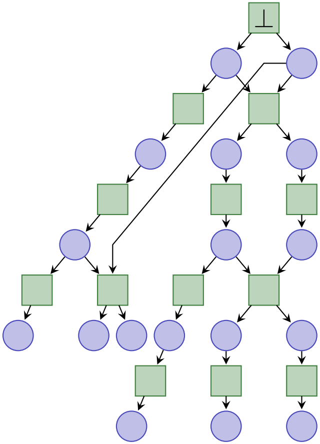
$f \; co \; i$

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. $\bot \in E$ is the only $\leq$-minimal node (event $\bot$ creates the initial conditions).



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. $\subseteq$.

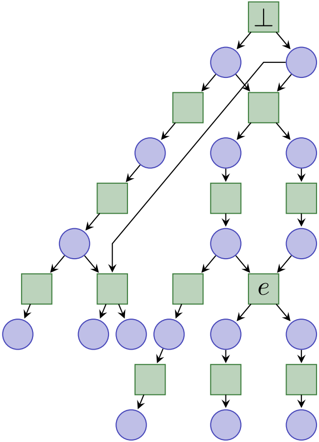
Notation

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): *progress assumption*



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. $\subseteq$.

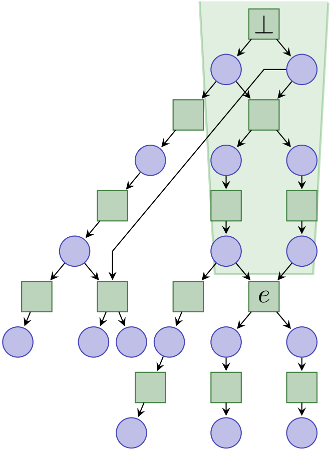
Notation

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): *progress assumption*



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. $\subseteq$.

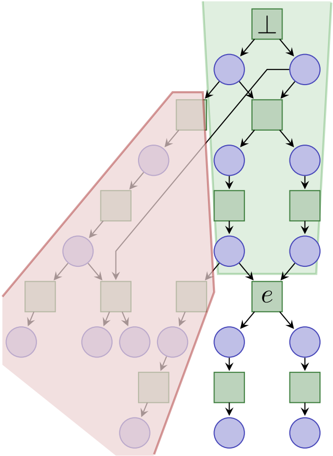
Notation

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): *progress assumption*



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.

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

Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

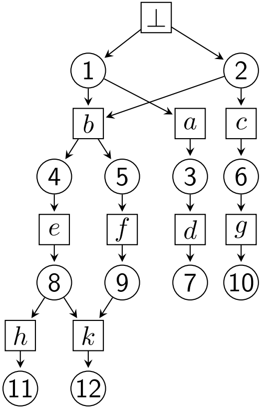
Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

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 the progress assumption,
$a \triangleright c$
because for any maximal run ω,

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



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

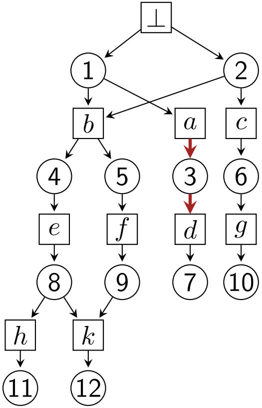
Event e reveals event f, written $e \triangleright f$, iff $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

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 the progress assumption,
$a \triangleright c$
because for any maximal run ω,

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



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

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

$d \triangleright a$,

$h \triangleright \perp$,

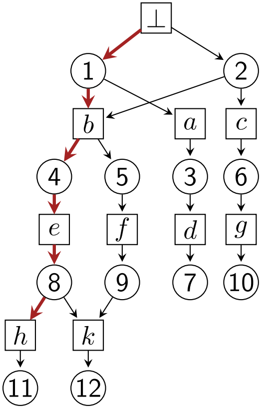
$a \triangleright d$

because of the progress assumption,

$a \triangleright c$

because for any maximal run ω,

$$a \in \omega \quad \Rightarrow \quad b \notin \omega$$
$$\Rightarrow \quad c \in \omega \text{ (progress assumption)}$$



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

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

$d \triangleright a$,

$h \triangleright \bot$,

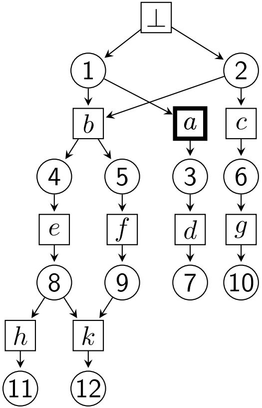
$a \triangleright d$

because of the progress assumption,

$a \triangleright c$

because for any maximal run ω,

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



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

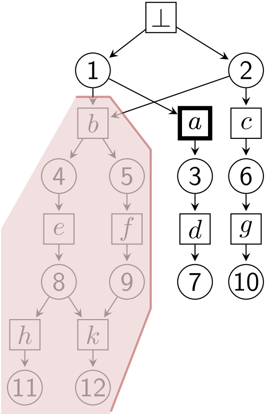
Event e *reveals event* f*, written* $e \triangleright f$*, iff* $\forall \omega \in \Omega, (e \in \omega \Rightarrow f \in \omega)$.

Causal closure

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

$d \triangleright a$,
$h \triangleright \bot$,
$a \triangleright d$
    because of the progress assumption,
$a \triangleright c$
    because for any maximal run ω,

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



Reveals Relation [Haar, 2010]

Definition (Reveals relation $\triangleright$)

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

Lemma

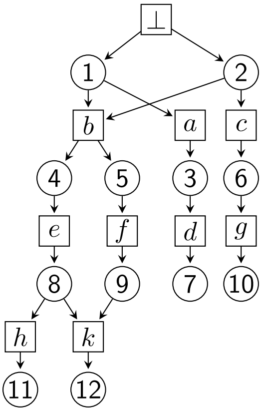
Lemma: Characterization of Ω by $\#$ A set of events ω is a maximal run iff

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

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.



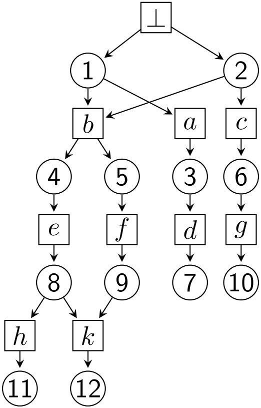
Reveals Relation

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 $\rhd$: Finding witnesses [HKS 2011]

Definition

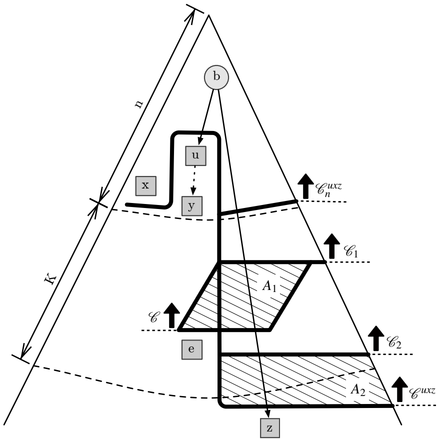
Let U_M be the first complete finite prefix of (N, M), and K_M the height of U_M; then set

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

Theorem [HKS 2011]

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

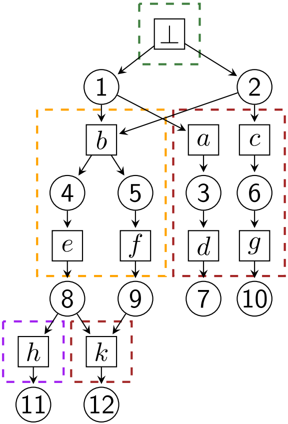
$$\begin{array}{rcl} z & \# & y \\ \neg(z & \# & x) \\ \mathbf{h}(z) & \leq & K + \max(\mathbf{h}(x), \mathbf{h}(y)) \end{array}$$



Facets Abstraction [H2010,BCH2011]

Definition (Facets)

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



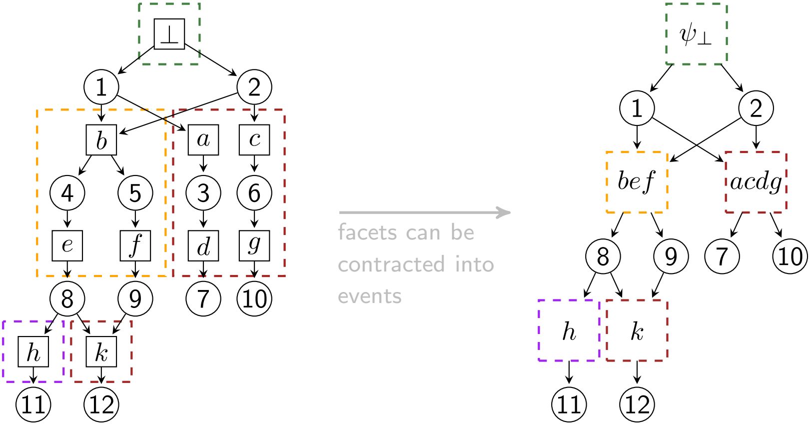
Facets Abstraction [H2010,BCH2011]

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 $\forall \psi_1, \psi_2 \in \Psi$, $\psi_1 \sim \psi_2 \Leftrightarrow \psi_1 = \psi_2$.



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

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

Lemma

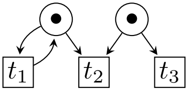
Lemma 1 $\triangleright$ is a partial order on Ψ ($\triangleright$ is antisymmetric by definition of a reduced ON).

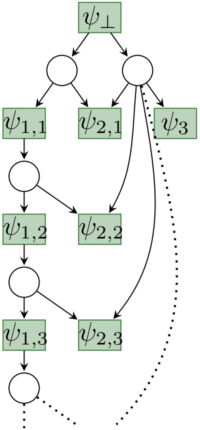
$(\Psi, \triangleright^{-1}, \#)$ is an event structure

- $\triangleright^{-1}$ 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).

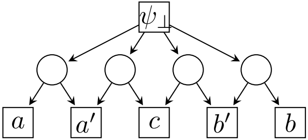
Lemma

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

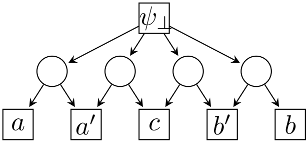
- $a \# b \Leftrightarrow$ for any run ω, $\{a, b\} \not\subseteq \omega$.
- $a \leq b \Rightarrow$ for any run ω, $b \in \omega \Rightarrow a \in \omega$ $(b \triangleright a)$,
- Does a co b mean a and b are logically independent ?

  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, $b \in \omega \Rightarrow a \in \omega$ $(b \rhd a)$,
- Does $a\ co\ b$ mean a and b are logically independent ?

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

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

Independency relation ind

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

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

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

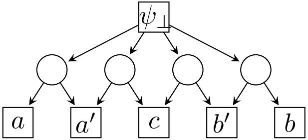
Immediate conflict relation $\#_i$

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

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 $\forall a, b \in \Psi$, $a \triangleright b \Leftrightarrow b \leq a$.

Violations of tightness

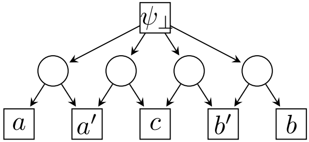
$a, b \in \Psi$ such that

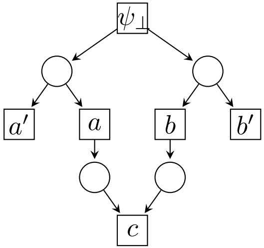
- $a\ co\ b$
- $a \triangleright b$

Net Surgery

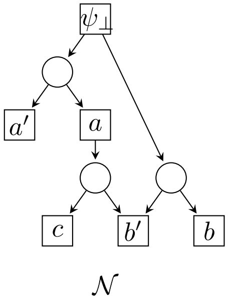
Add a condition from b to a for all a, b such that

- $a\ co\ b$
- $a \triangleright_i b$



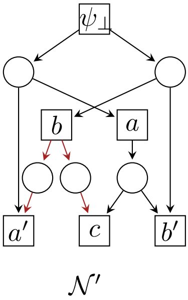


Another Example for Tightening [BCH2011]



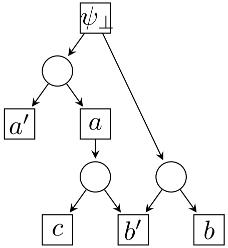
Constraints

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



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

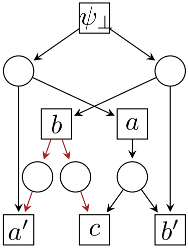
Another Example for Tightening [BCH2011]



$\mathcal{N}$

Constraints

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



$\mathcal{N}'$

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

Definition (Tight net)

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

Reveal Your Faults: Partially observation and Diagnosis

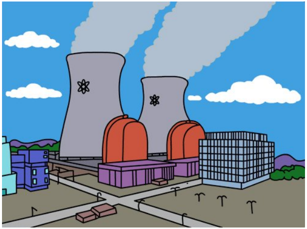
Assumptions

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

Goal:

- Determine, from partial observations,
  whether a certain event (fault) has happened in the past.

Note on Active Diagnosis



- A system with an *ambiguous* pair of runs is not diagnosable
- In that case: Compute *control*
  - based on past observations
  - so that faults manifest themselves through observations

Our Results

- Memory Consumption down from $2^{2^{O(n)}}$ to
  - $2^{O(n^2)}$ with minimal diagnosis delay
  - $2^{O(n)}$ with twice the minimal delay
- Computational complexity shown *optimal*

Sequential Semantics Misses a Point

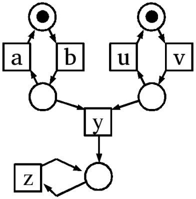
Suppose that

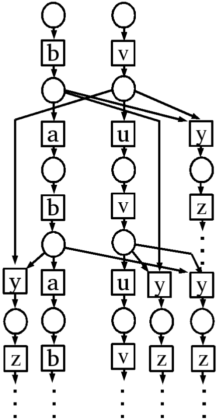
- $T_O = \{b, y\}$
- $\Phi = \{v\}$

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

$$bbbbbb\ldots$$

is observed, what do we infer about v ?



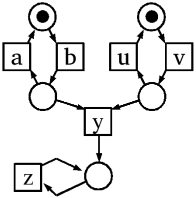


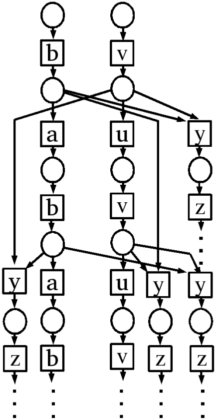
It's about weak fairness !

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

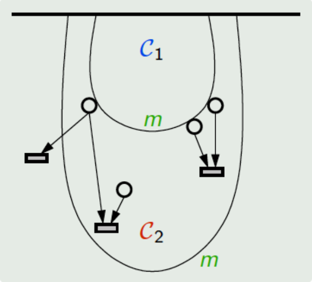
Application

- $A \twoheadrightarrow B$ 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



Observe and Derive: perspectives

Temporal vs. logical view of event structures

- Causality ($\leq$), conflict ($\#$), concurrency (co) vs
- reveals ($\triangleright$) , $\#$ and ind

Extended reveals relation $\twoheadrightarrow$

$A \twoheadrightarrow B \overset{def}{\Leftrightarrow} \forall \omega \in \Omega : [A \subseteq \omega \Rightarrow B \cap \omega \neq \emptyset]$

- Allows to express all boolean properties of $\Omega \rightarrow$ Logic ERL [BCH2011]
- Exploit in diagnosis (ACSD 2013)

To Do

- Improve Diagnosis; exploit in verification, e.g. *diagnosability*
- Probabilities
- develop a measure of "freedom of choice"
- Extend to contextual, timed, probabilistic models ...
- Connect with *logics* $\rightarrow$ coming up