A pomset semantics for choreographies

José Proença

DCC-talks, 15 May 2024

2011
PhD @ CWI
Amsterdam (NL)

Coordination

Formal methods

Concurrency

Software Engineering

2005
Lic. @ UMinho
Braga

Mathematics &
Computer Science

2015
Postdoc @
KU Leuven (BE)

Programming languages
Variability

Wireless Sensor Netw.
Reactive programming

2019
Postdoc @
INESC TEC
Braga

Softw. Architectures
Design Calculi

From Feb’19
Postdoc @ CISTER
From Set’23
Assistant prof. @ DCC

Formal methods

Component-based systems

Concurrency theory

Coordination **models**

Distributed **algorithms**

Using SAT solvers

Compositional **semantics**
- Automata based
- Constraint based
- Calculus based

ABS programming **language**

Variability models

Domain specific **languages**

Category theory

Type systems

Wireless sensor networks

Verification (Model checking, Dynamic Logic)

Reactive **programming**

Real-time systems

Hybrid systems

Critical systems

*Ready-to-use **formal tools***

2005 2010 2015 2020

Nowadays...

Real-time systems + industrial partners

- Modelling of "coordinators" in real-time OS
- Model checking many variations made easier

Hybrid programs

- Lince tool
- ICTAC

```
// Cruise control
p:=0; v:=2;
while true do {
  if v<=10
  then p'=v,v'=5  for 1
  else p'=v,v'=-2 for 1
}
```

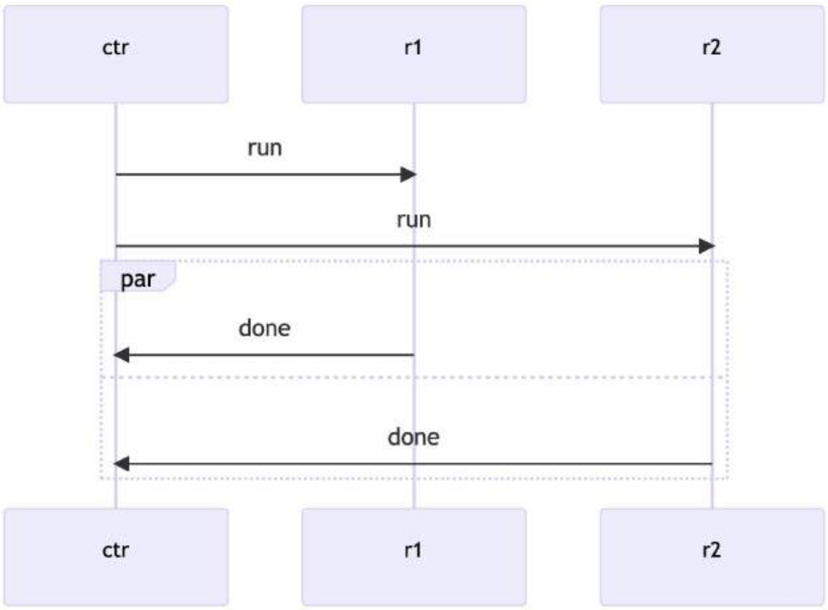
Team Automata

- (Multi) synchronisation of automata
- Communication properties
- Different setting: dynamic logic, variability, realisability, ...
- FM, ICTAC

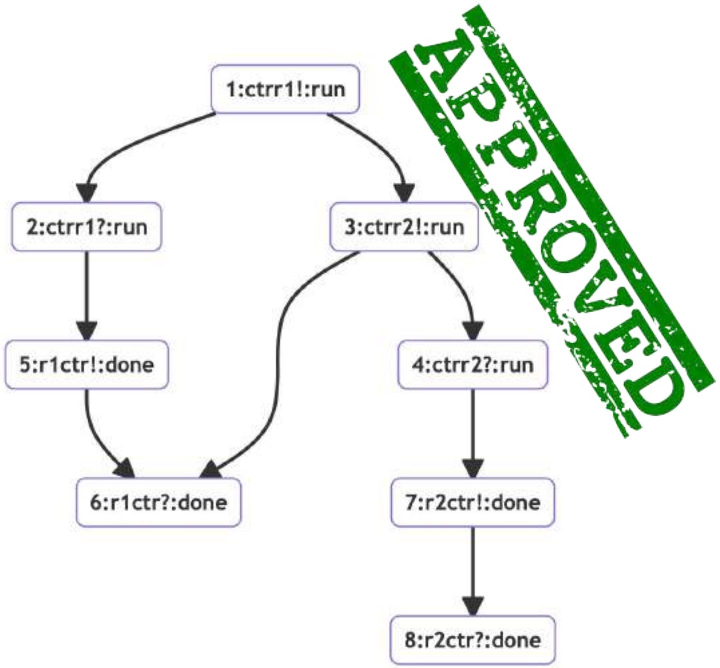
Choreographies

- Multi-party session types
- "Formal" message sequence charts
- **Pomsets**
- ECOOP, ISOLA

This talk: pomsets



Choreographies



(Branching) pomsets

Realisability

Joint work with

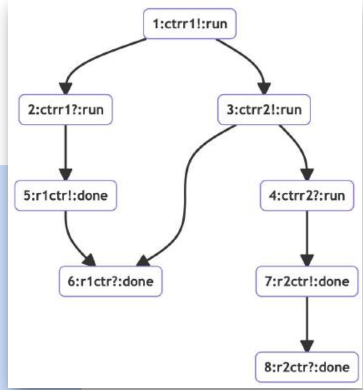
Sung-Shik Jongmans

Luc Edixhoven

CWI

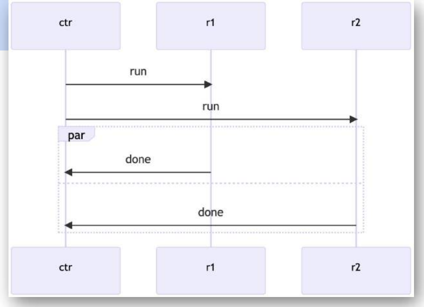
Universiteit Leiden

Outline



Choreographies

- What is a system of communicating agents



Pomsets

- What is a pomset
- Semantics as a set of pomsets
- Semantics as a **branching pomset**

Realisability via pomsets

- Local view of the behaviour
- **Realisable**:
  composed local beh. = **global beh.**
- Goal: Infer realisability from sufficient conditions over the global view

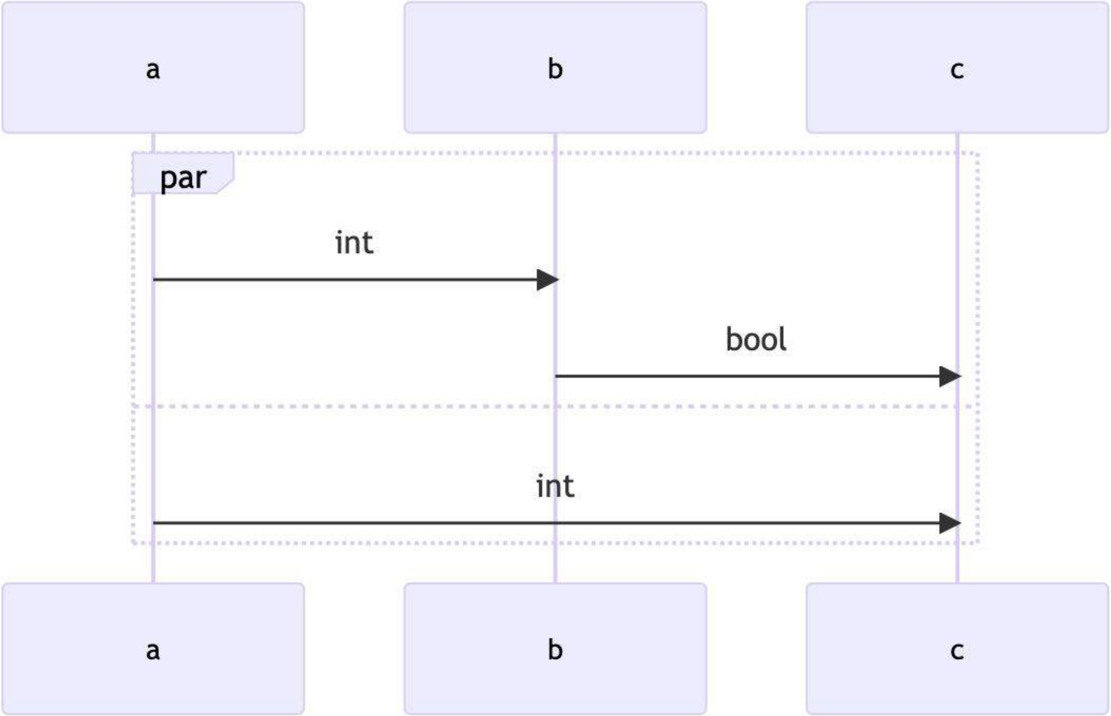
Choreographies

$(a \to b{:}\mathrm{int}\ ;\ b \to c{:}\mathrm{bool})\ \ ||\ \ a \to c{:}\mathrm{int}$

Alice communicates an integer to **Bob**,
after which **Bob** communicates a boolean to **Carol**.
Simultaneously, **Alice** communicates an integer to **Carol**.

Choreographies

$(a \rightarrow b : \text{int} \; ; \; b \rightarrow c : \text{bool}) \;\; || \;\; a \rightarrow c : \text{int}$



Mostly standard semantics

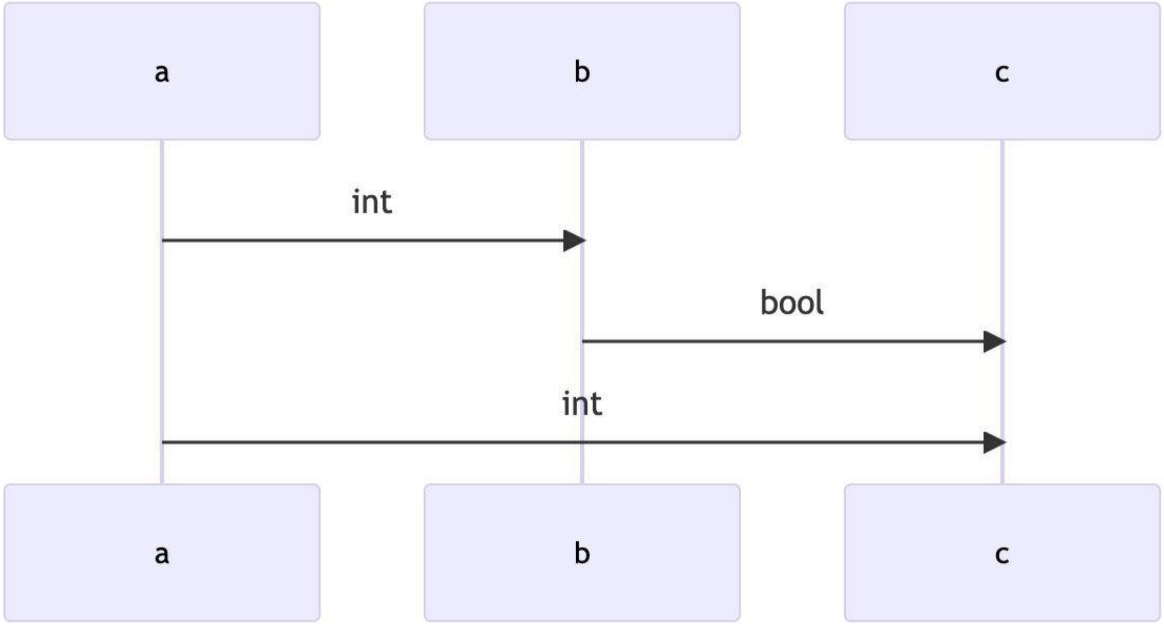
$$
\begin{aligned}
c ::= \;& \mathbf{1} \\
\mid\;& a{\to}b{:}x \\
\mid\;& ab?x \\
\mid\;& c \,;\, c \\
\mid\;& c + c \\
\mid\;& c \parallel c \\
\mid\;& c^*
\end{aligned}
$$

(Mostly) Standard Semantics

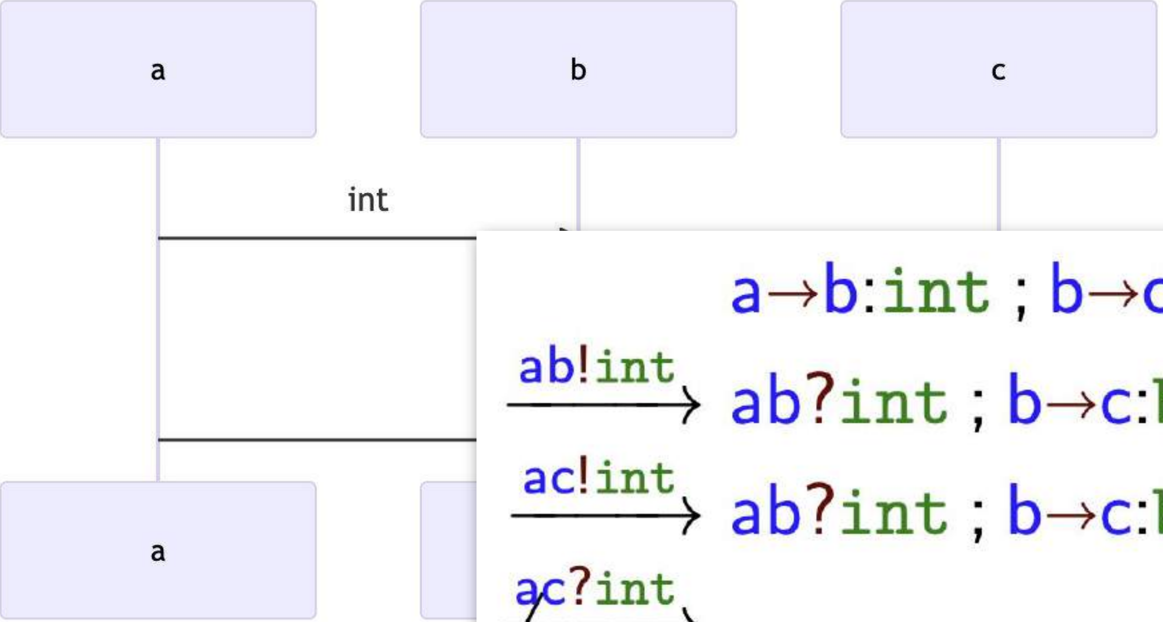
$$
\begin{aligned}
c ::= \;& \mathbf{1} \\
\mid\;& a \to b : x \\
\mid\;& ab?x \\
\mid\;& c \,;\, c \\
\mid\;& c + c \\
\mid\;& c \parallel c \\
\mid\;& c^*
\end{aligned}
$$

$$
\begin{aligned}
& (a \to b:\mathtt{int} \,;\, b \to c:\mathtt{bool}) \parallel a \to c:\mathtt{int} \\
\xrightarrow{ac!\mathtt{int}}\; & (a \to b:\mathtt{int} \,;\, b \to c:\mathtt{bool}) \parallel ac?\mathtt{int} \\
\xrightarrow{ab!\mathtt{int}}\; & (ab?\mathtt{int} \,;\, b \to c:\mathtt{bool}) \parallel ac?\mathtt{int} \\
\xrightarrow{ab?\mathtt{int}}\; & b \to c:\mathtt{bool} \parallel ac?\mathtt{int} \\
\xrightarrow{bc!\mathtt{bool}}\; & bc?\mathtt{bool} \parallel ac?\mathtt{int} \\
\xrightarrow{ac?\mathtt{int}}\; & bc?\mathtt{bool} \\
\xrightarrow{bc?\mathtt{bool}}\; & \mathbf{1}
\end{aligned}
$$

Weak sequential composition



Weak sequential composition



$$\mathtt{a}{\to}\mathtt{b}{:}\mathtt{int}\ ;\ \mathtt{b}{\to}\mathtt{c}{:}\mathtt{bool}\ ;\ \mathtt{a}{\to}\mathtt{c}{:}\mathtt{int}$$

$$\xrightarrow{\mathtt{ab!int}}\ \mathtt{ab?int}\ ;\ \mathtt{b}{\to}\mathtt{c}{:}\mathtt{bool}\ ;\ \mathtt{a}{\to}\mathtt{c}{:}\mathtt{int}$$

$$\xrightarrow{\mathtt{ac!int}}\ \mathtt{ab?int}\ ;\ \mathtt{b}{\to}\mathtt{c}{:}\mathtt{bool}\ ;\ \mathtt{ac?int}$$

$$\not\xrightarrow{\mathtt{ac?int}}$$

Partial termination
(Rensink and Wehrheim 2001)

If $c_1 \xrightarrow{\checkmark_\ell} c_1'$ and $c_2 \xrightarrow{\ell} c_2'$ then $c_1 \,;\, c_2 \xrightarrow{\ell} c_1' \,;\, c_2'$

- If c_1 is independent of the subject of ℓ then $c_1 \xrightarrow{\checkmark_\ell} c_1$.
- If c_1 can resolve choices to be independent of the subject of ℓ then $c_1 \xrightarrow{\checkmark_\ell} c_1'$.
- Otherwise $c_1 \stackrel{\checkmark_\ell}{\not\rightarrow}$.

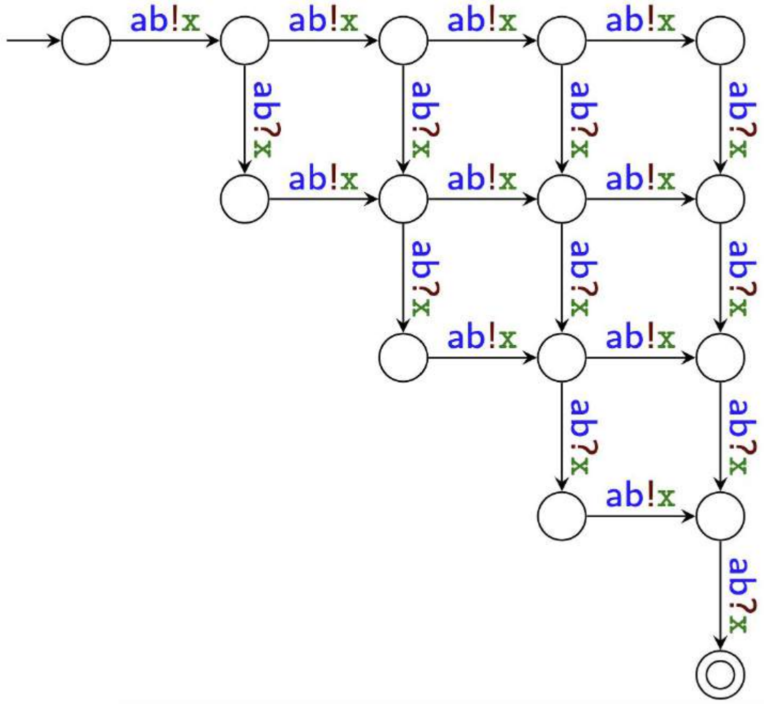
Partial termination: *allowing actions*

- $\mathtt{ab?int} \,;\, \mathtt{b{\to}c{:}bool} \xrightarrow{\checkmark \mathtt{ac!int}} \mathtt{ab?int} \,;\, \mathtt{b{\to}c{:}bool}$
- $\mathtt{ab?int} \,;\, \mathtt{b{\to}c{:}bool} \not\xrightarrow{\checkmark \mathtt{ac?int}}$

- $\mathtt{a{\to}b{:}x} + \mathtt{a{\to}c{:}x} \xrightarrow{\checkmark \mathtt{ad?x}} \mathtt{a{\to}b{:}x} + \mathtt{a{\to}c{:}x}$
- $\mathtt{a{\to}b{:}x} + \mathtt{a{\to}c{:}x} \xrightarrow{\checkmark \mathtt{ba!x}} \mathtt{a{\to}c{:}x}$
- $\mathtt{a{\to}b{:}x} + \mathtt{a{\to}c{:}x} \not\xrightarrow{\checkmark \mathtt{ba?x}}$

How big is the state-space?

$a \to b{:}x\ ;\ a \to b{:}x\ ;\ a \to b{:}x\ ;\ a \to b{:}x$

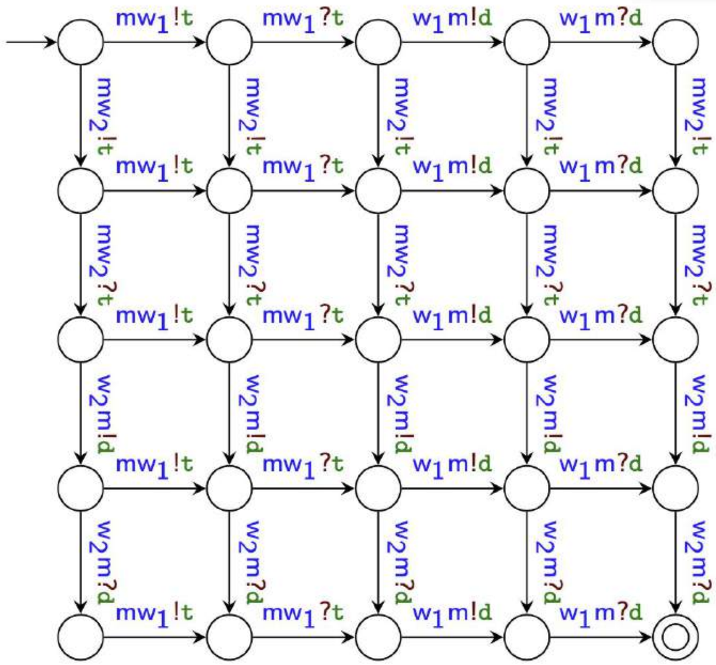


\# states:

$O(n^2)$

How big is the state-space?

$$(m \to w_1 : t \; ; \; w_1 \to m : d) \parallel (m \to w_2 : t \; ; \; w_2 \to m : d)$$

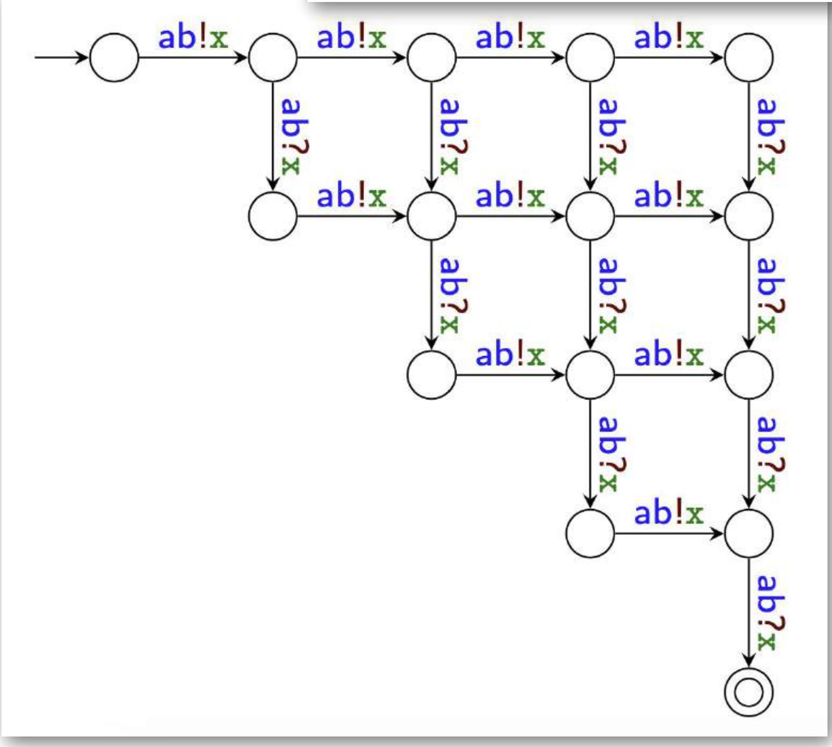


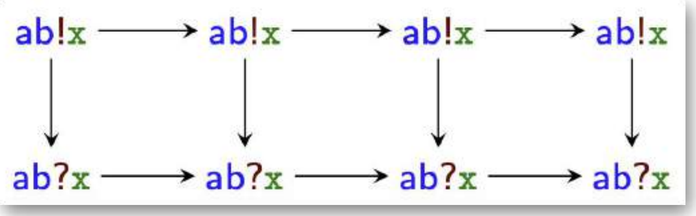
\# states:

$O(5^n)$

Pomsets: more compact?

a→b:x ; a→b:x ; a→b:x ; a→b:x





Partially **o**rdered **m**ulti**set** *(Pratt 1986)*

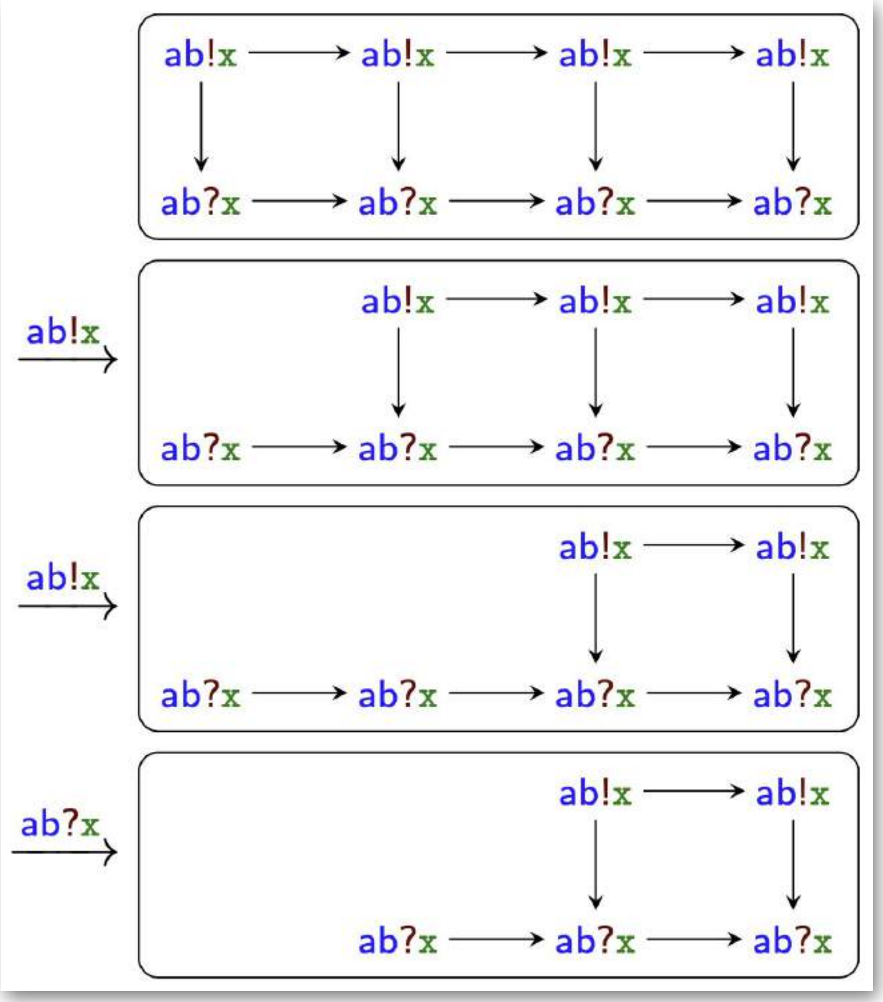
$$a \to b{:}x \;;\; a \to b{:}x \;;\; a \to b{:}x \;;\; a \to b{:}x$$

$$
\begin{array}{ll}
\langle \{e_1, \ldots, e_8\}, & O(n) \\
\quad \{e_i \leq e_j \mid i \leq j \wedge (j \text{ is even} \vee i \text{ is odd})\}, & O(n^2) \\
\quad e_i \mapsto \begin{cases} ab!x & \text{if } i \text{ is odd} \\ ab?x & \text{if } i \text{ is even} \end{cases} \quad \rangle & O(n)
\end{array}
$$

$$
\begin{tikzcd}
e_1 \arrow[r] \arrow[d] & e_3 \arrow[r] \arrow[d] & e_5 \arrow[r] \arrow[d] & e_7 \arrow[d] \\
e_2 \arrow[r] & e_4 \arrow[r] & e_6 \arrow[r] & e_8
\end{tikzcd}
\qquad
\begin{tikzcd}
ab!x \arrow[r] \arrow[d] & ab!x \arrow[r] \arrow[d] & ab!x \arrow[r] \arrow[d] & ab!x \arrow[d] \\
ab?x \arrow[r] & ab?x \arrow[r] & ab?x \arrow[r] & ab?x
\end{tikzcd}
$$

Semantics

All traces that follow the causal dependencies between events



Another example

$$(\mathsf{m}{\rightarrow}\mathsf{w}_1{:}\mathsf{t}\ ;\ \mathsf{w}_1{\rightarrow}\mathsf{m}{:}\mathsf{d}) \parallel (\mathsf{m}{\rightarrow}\mathsf{w}_2{:}\mathsf{t}\ ;\ \mathsf{w}_2{\rightarrow}\mathsf{m}{:}\mathsf{d})$$

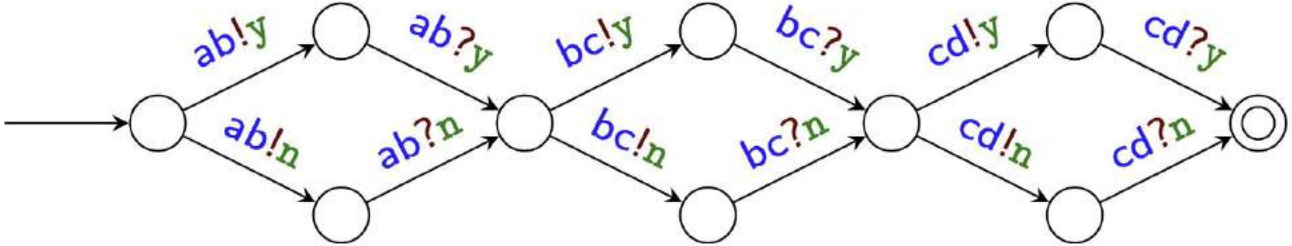
$$\begin{array}{ll}
\langle \{e_1, \ldots, e_8\}, & O(n) \\
\quad \{e_i \leq e_j \mid i \leq j \wedge i \equiv j \bmod 2\}, & O(n^2) \\
\quad \{e_1 \mapsto \mathsf{mw_1!t}, \ldots, e_8 \mapsto \mathsf{w_2m?d}\}\rangle & O(n)
\end{array}$$

$$\begin{array}{ccccccc}
e_1 & \longrightarrow & e_3 & \longrightarrow & e_5 & \longrightarrow & e_7 \\
e_2 & \longrightarrow & e_4 & \longrightarrow & e_6 & \longrightarrow & e_8
\end{array}$$

$$\begin{array}{ccccccc}
\mathsf{mw_1!t} & \longrightarrow & \mathsf{mw_1?t} & \longrightarrow & \mathsf{w_1m!d} & \longrightarrow & \mathsf{w_1m?d} \\
\mathsf{mw_2!t} & \longrightarrow & \mathsf{mw_2?t} & \longrightarrow & \mathsf{w_2m!d} & \longrightarrow & \mathsf{w_2m?d}
\end{array}$$

Choices – the dark side

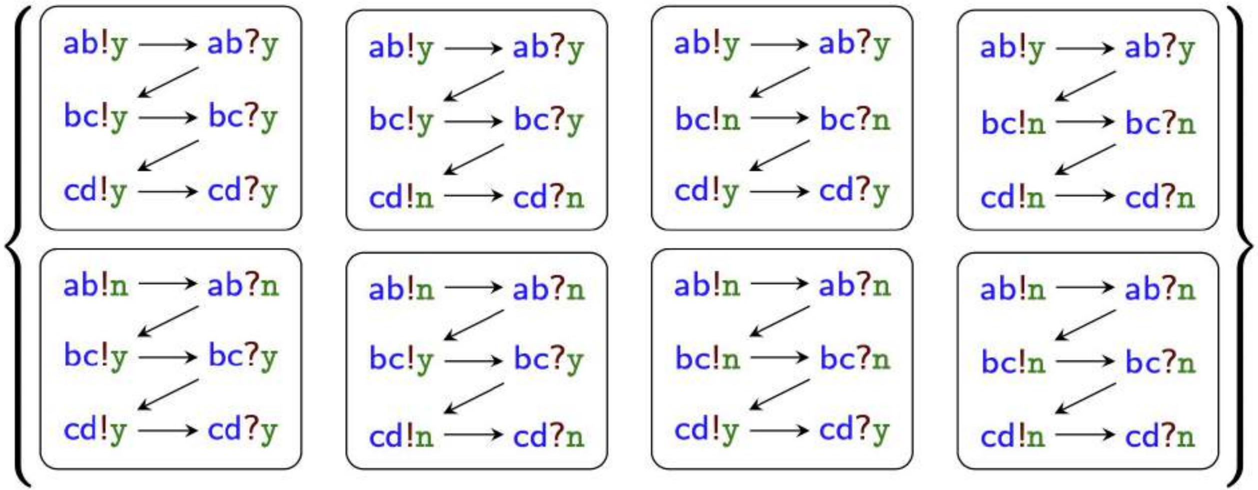
$$(\mathsf{a}{\to}\mathsf{b}{:}\mathtt{y} + \mathsf{a}{\to}\mathsf{b}{:}\mathtt{n}) \;;\; (\mathsf{b}{\to}\mathsf{c}{:}\mathtt{y} + \mathsf{b}{\to}\mathsf{c}{:}\mathtt{n}) \;;\; (\mathsf{c}{\to}\mathsf{d}{:}\mathtt{y} + \mathsf{c}{\to}\mathsf{d}{:}\mathtt{n})$$



$O(n)$ states

Choices – the dark side

$$(a{\to}b{:}y + a{\to}b{:}n) \,;\, (b{\to}c{:}y + b{\to}c{:}n) \,;\, (c{\to}d{:}y + c{\to}d{:}n)$$

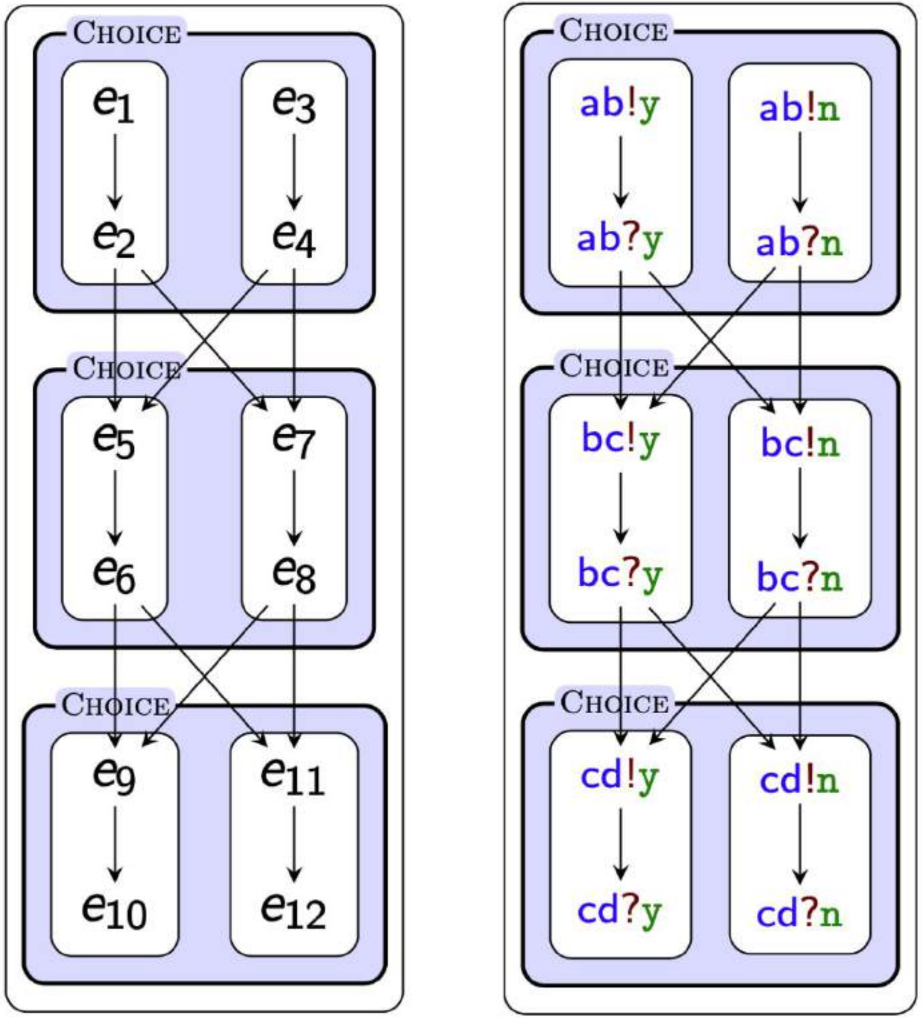


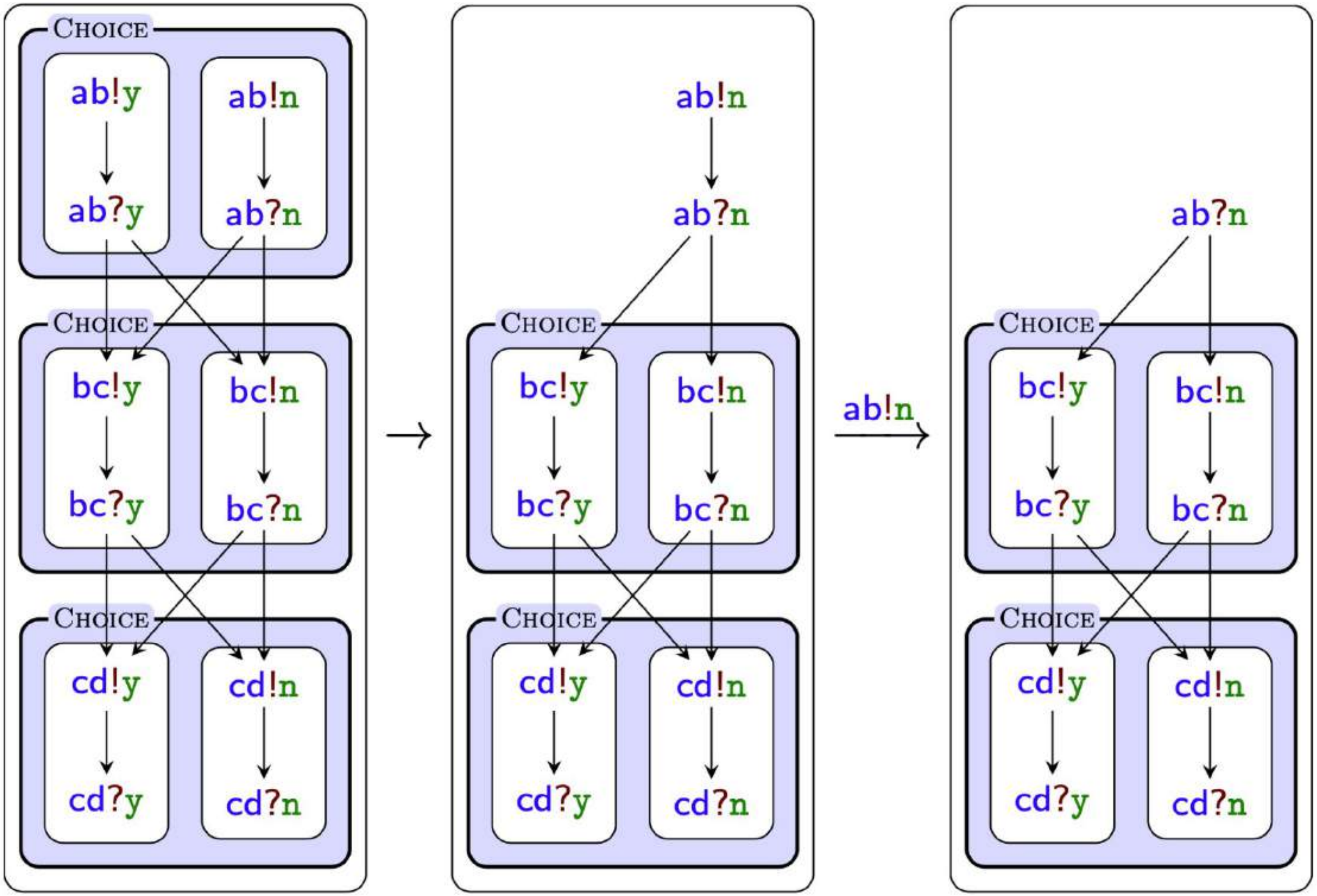
$O(2^n)$ pomsets

Branching pomsets *(to the rescue)*

$$\mathcal{B} ::= \{\mathcal{C}_1, \ldots, \mathcal{C}_n\}$$
$$\mathcal{C} ::= e \mid \{\mathcal{B}_1, \mathcal{B}_2\}$$

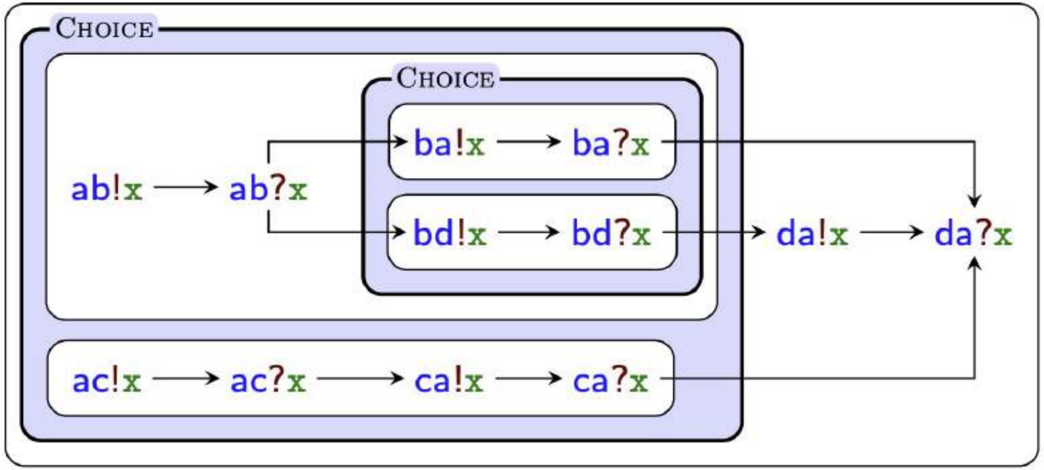
Here: $\mathcal{B} = \{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3\}$, where
$\mathcal{C}_1 = \{\{e_1, e_2\}, \{e_3, e_4\}\}$,
$\mathcal{C}_2 = \{\{e_5, e_6\}, \{e_7, e_8\}\}$ and
$\mathcal{C}_3 = \{\{e_9, e_{10}\}, \{e_{11}, e_{12}\}\}$.

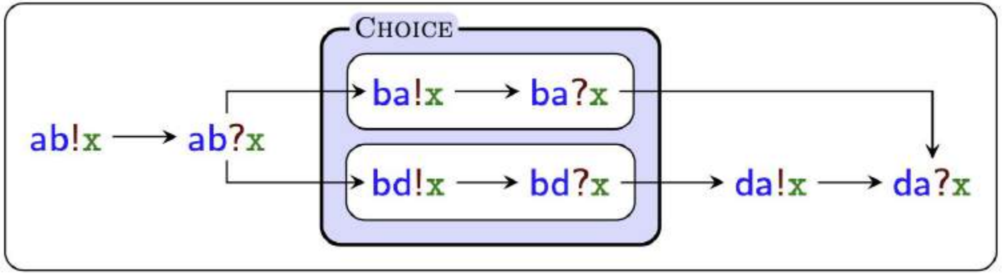




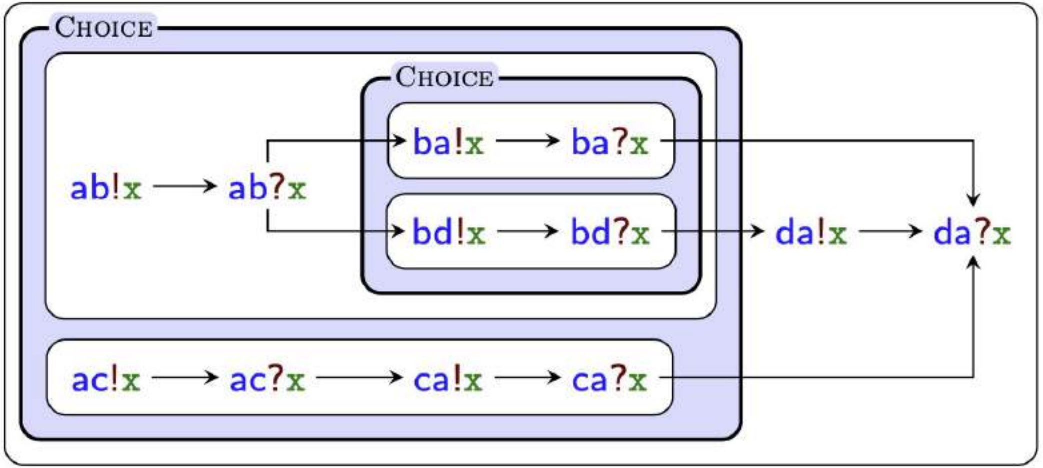
CHOICE
ab!y
ab?y
ab!n
ab?n
CHOICE
bc!y
bc?y
bc!n
bc?n
CHOICE
cd!y
cd?y
cd!n
cd?n
ab!n
ab?n
CHOICE
bc!y
bc?y
bc!n
bc?n
CHOICE
cd!y
cd?y
cd!n
cd?n
ab!n
ab?n
CHOICE
bc!y
bc?y
bc!n
bc?n
CHOICE
cd!y
cd?y
cd!n
cd?n

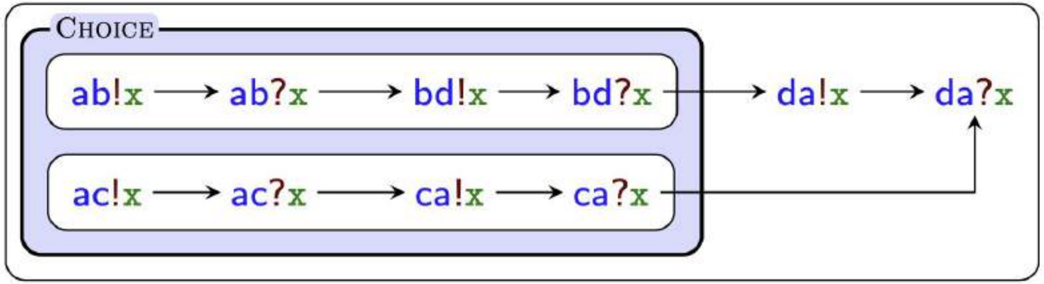
Refining: resolving choices



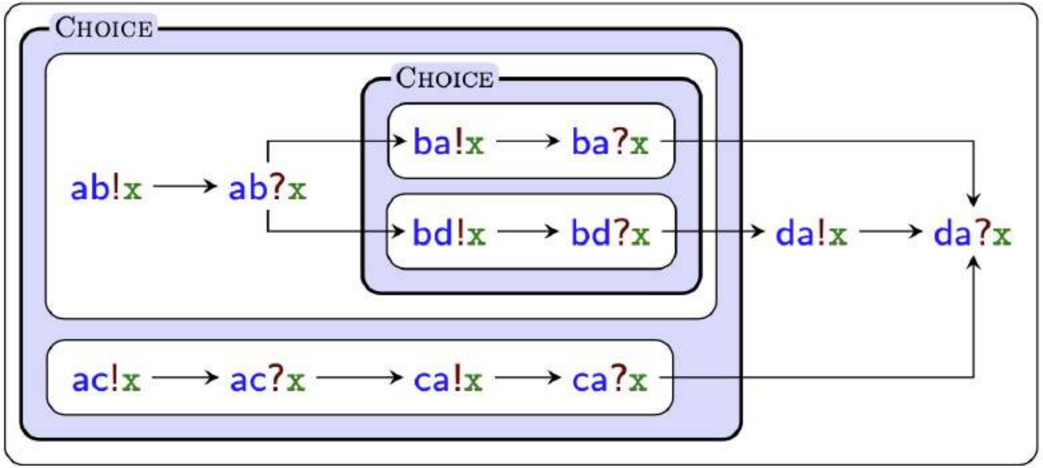


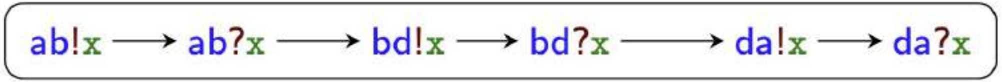
Refining: resolving choices



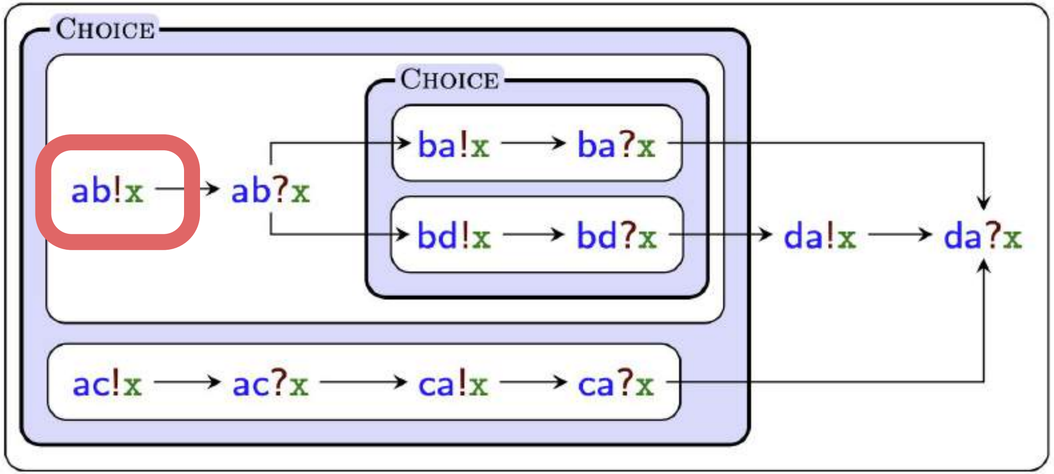


Refining: resolving choices

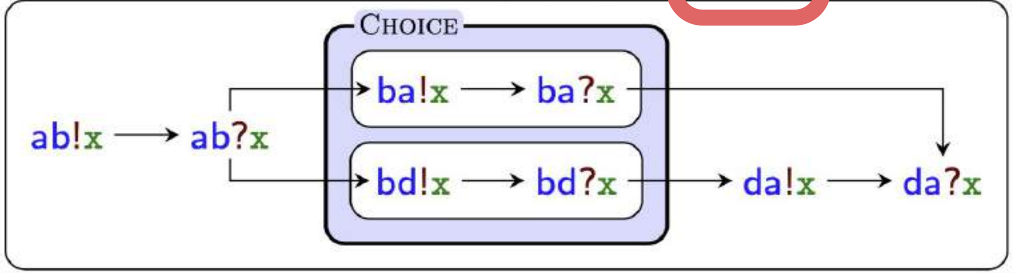




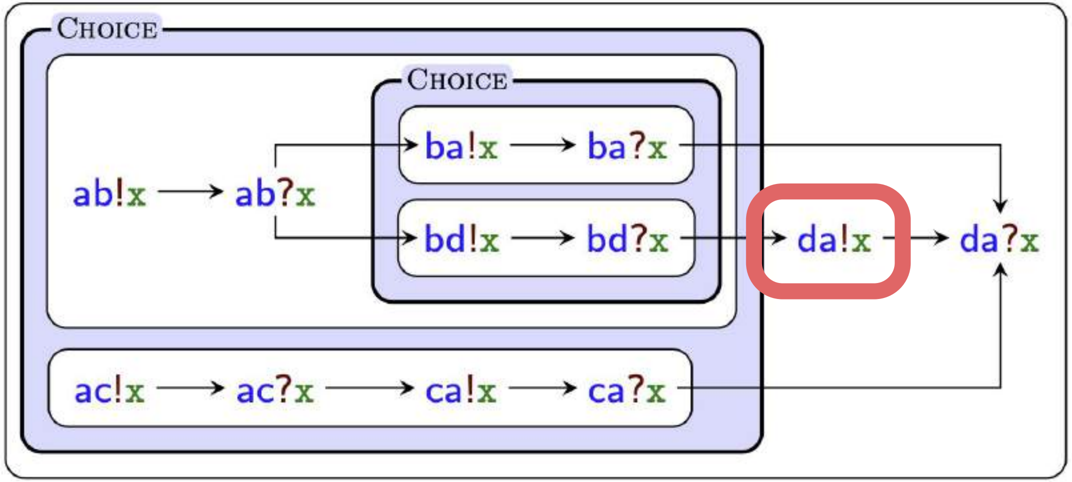
Enabling: *maximal* refinement wrt “e”



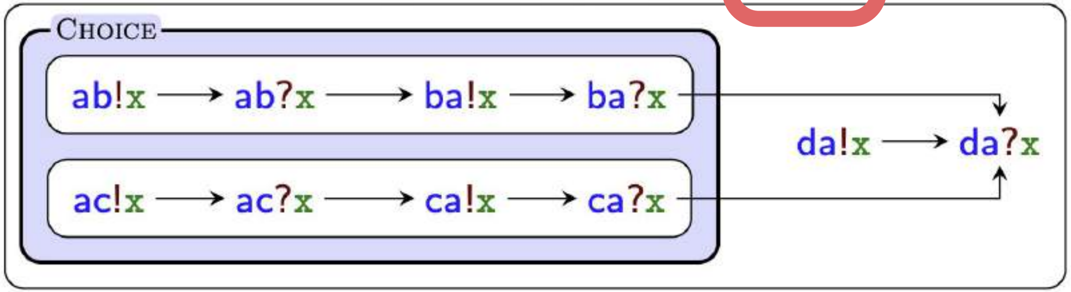
Enabling e_1 ($\lambda(e_1)$ = ab!x)



Enabling: *maximal* refinement wrt "e"



Enabling e_{11} ($\lambda(e_{11})$ = da!x)



From choreographies to B-Pomsets

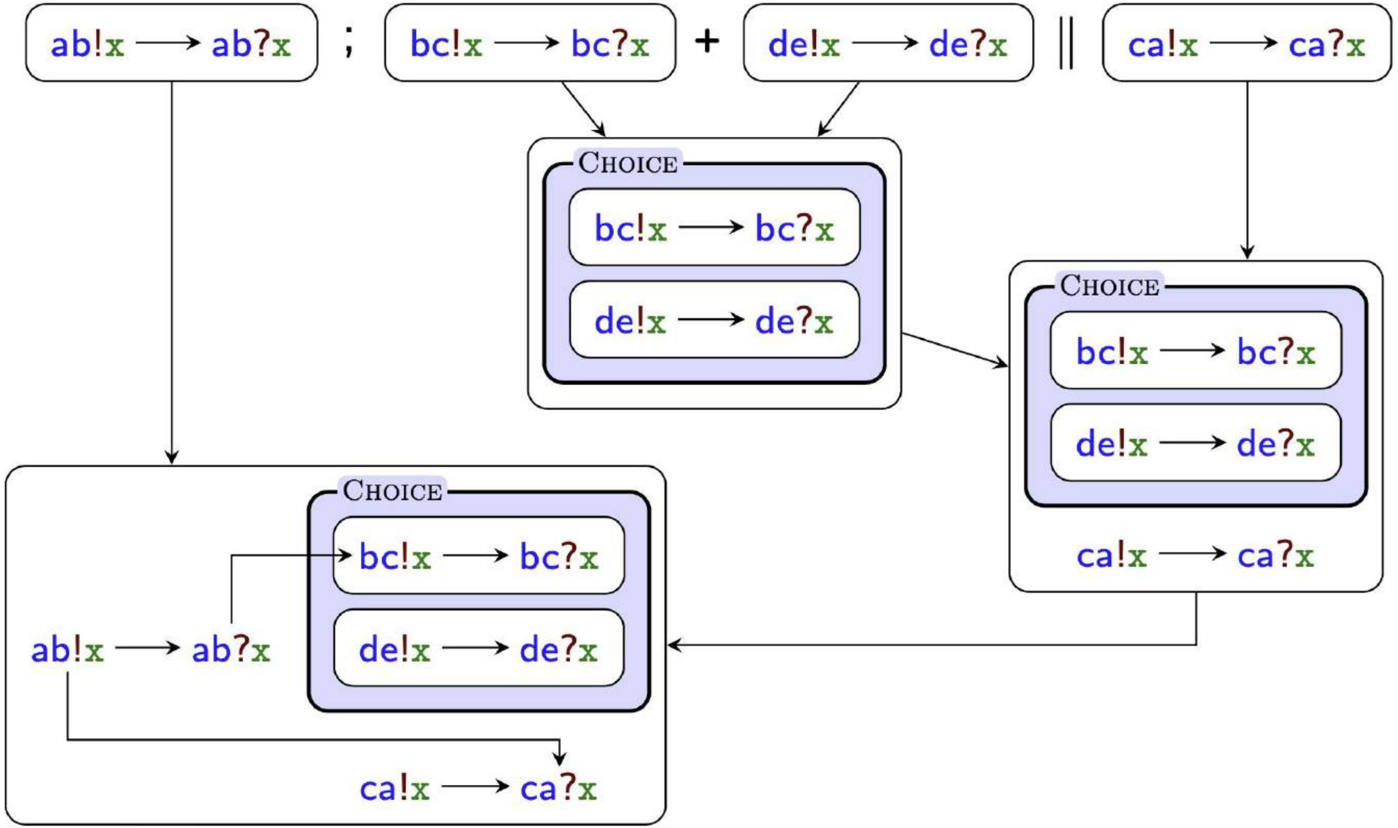
$$[\![a \to b : x \;;\; ((b \to c : x + d \to e : x) \parallel c \to a : x)]\!]$$

From choreographies to B-Pomsets

$$[\![a \to b : x \ ; \ ((b \to c : x + d \to e : x) \ \| \ c \to a : x)]\!]$$

$$\boxed{ab!x \longrightarrow ab?x} \ ; \ \boxed{bc!x \longrightarrow bc?x} + \boxed{de!x \longrightarrow de?x} \ \| \ \boxed{ca!x \longrightarrow ca?x}$$

From choreographies to B-Pomsets



From choreographies to B-Pomsets

Theorem

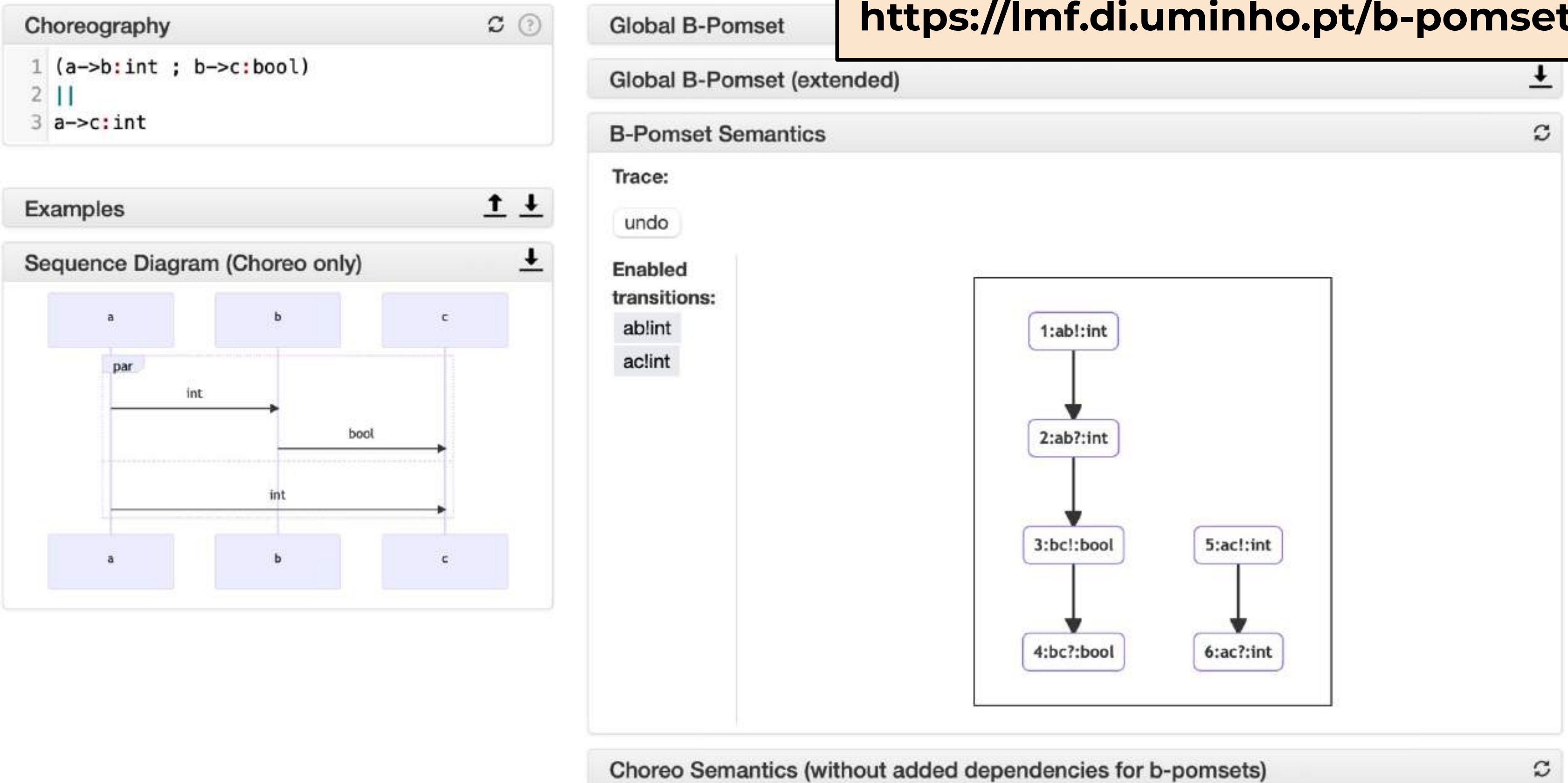
If [...] then choreography c is bisimilar to branching pomset $[\![c]\!]$.

Lemma

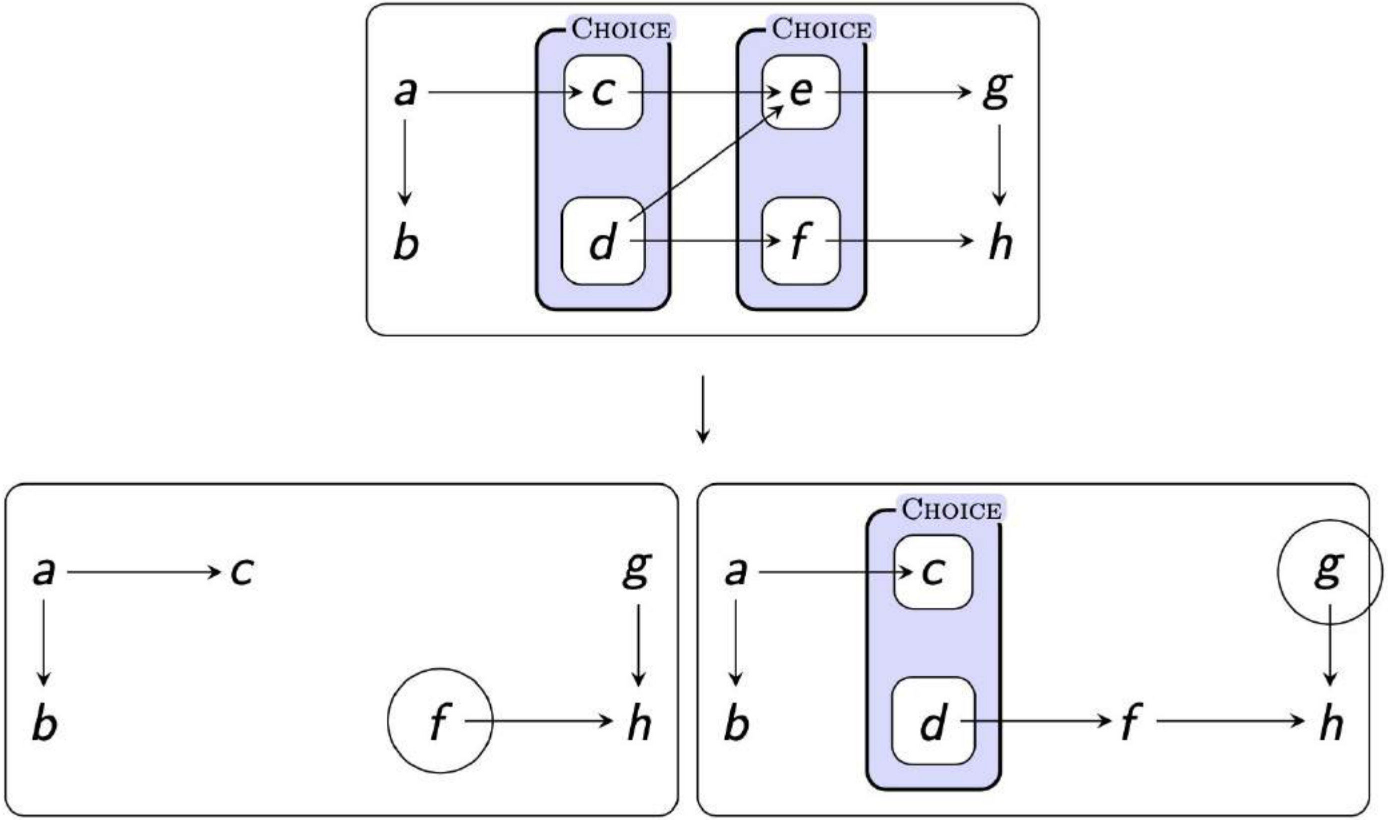
If [...] and $c_2 \xrightarrow{\ell} c_2'$ and $[\![c_2]\!] \xrightarrow{\ell} [\![c_2']\!]$ then $c_1 \xrightarrow{\surd_\ell} c_1'$ if and only if $[\![c_1 \, ; \, c_2]\!]$ can enable the corresponding event e.

Tool support

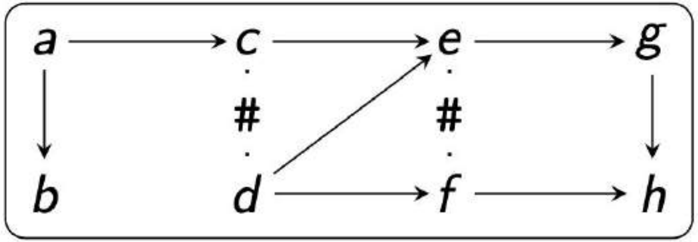
https://lmf.di.uminho.pt/b-pomset



B-Pomsets are not choreographies



B-Pomsets are similar to **Event Structures**

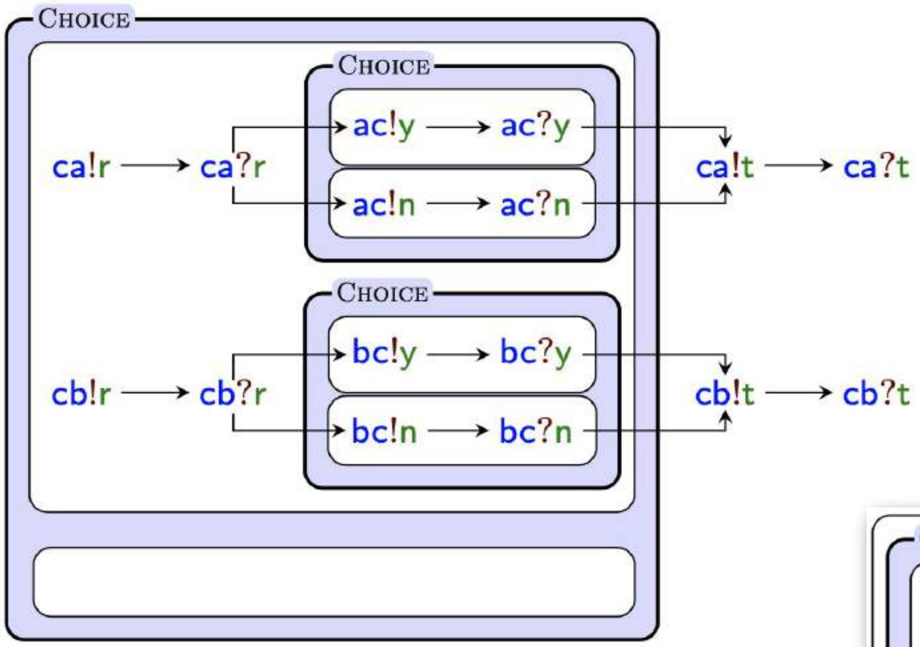


- add <u>conflict relation</u>; two conflicting events may not occur together in the same execution

  above: $\{(c, d), (e, f)\}$

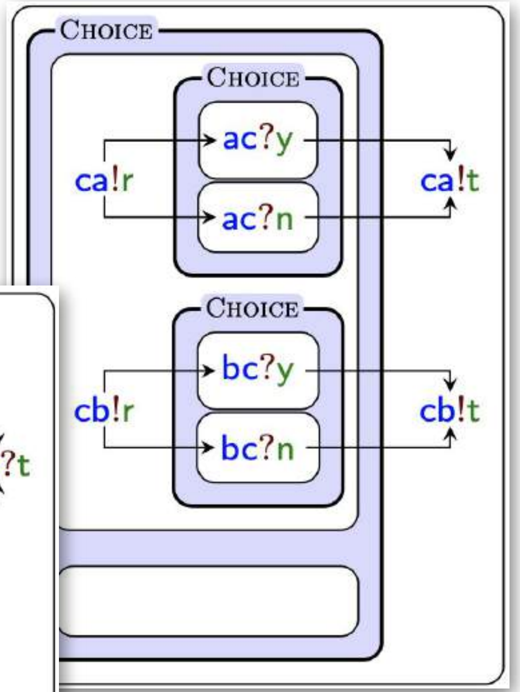
- most classes of event structures define variations on causality and/or conflicts

Realisability

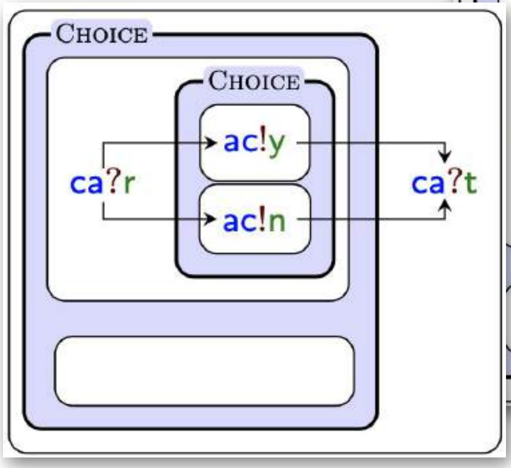


Global B-Pomset

Carol



Alice



Checking realisability of B-Pomsets

Well-Branched

- Every choice has a "leader"

Tree-like

- "Arrows" cannot "leave" choices

Well-Channeled

- "*Sends*" and "*receives*" of the same agents must be in the same order

Choreographic

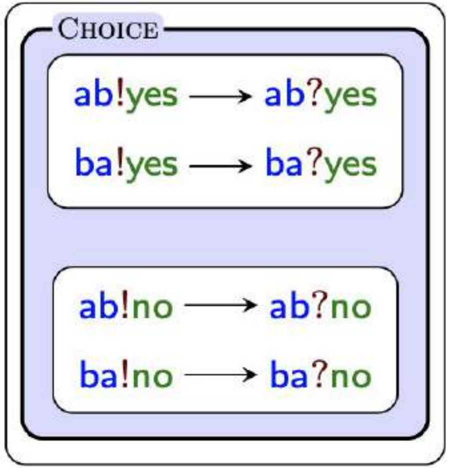
- It represents "some" choreography

Realisable

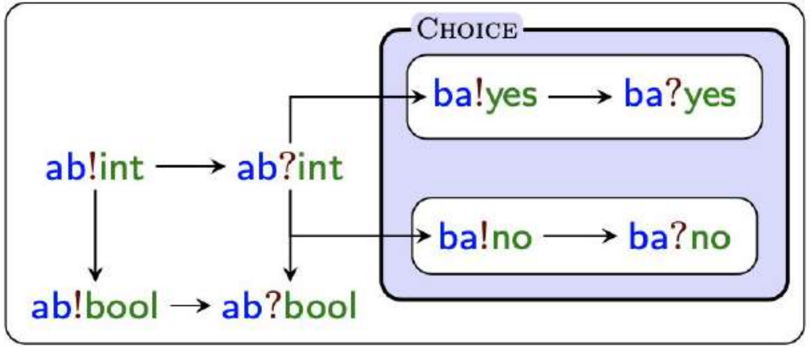
inspired by multiparty session types

Examples

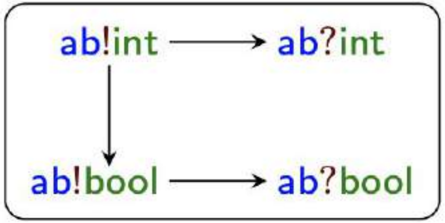
R_f =



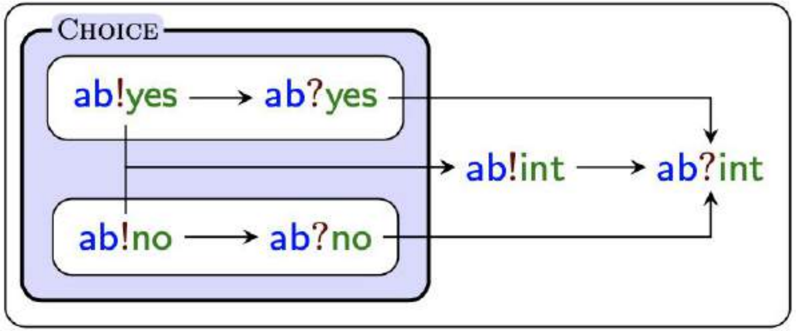
R_g =



R_h =



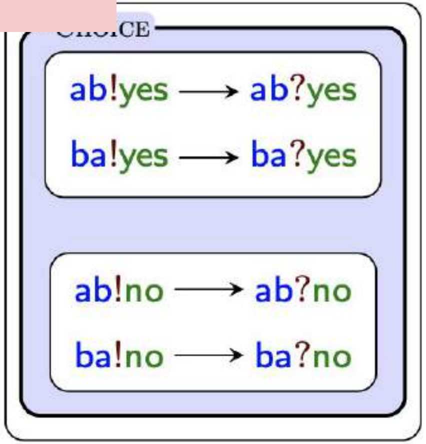
R_i =



Examples

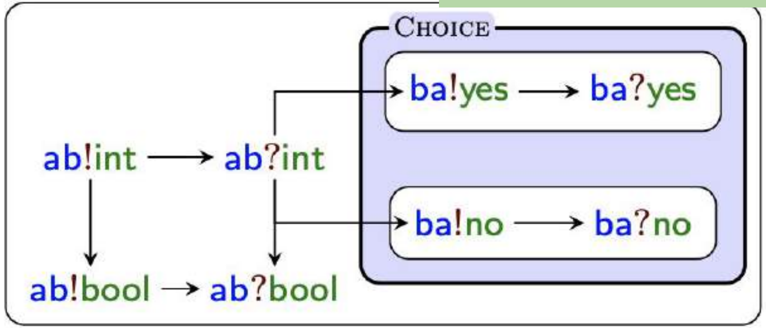
ill-branched

R_f =

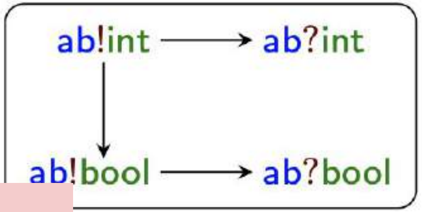


OK

R_g =

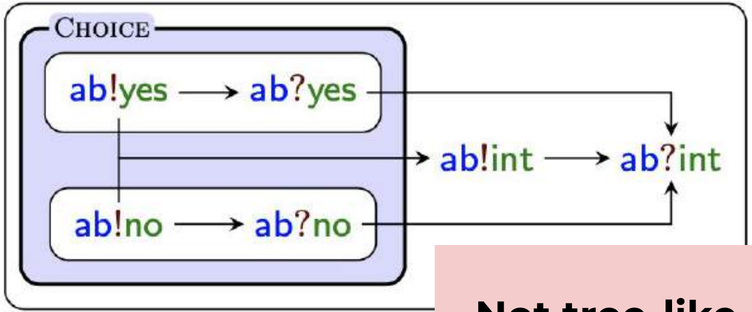


R_h =



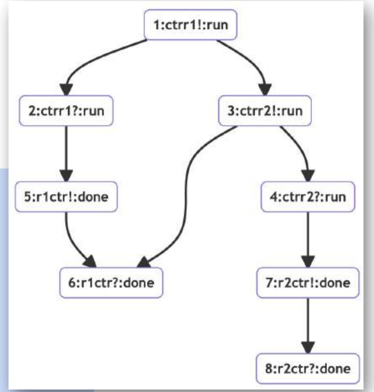
ill-channelled

R_i =



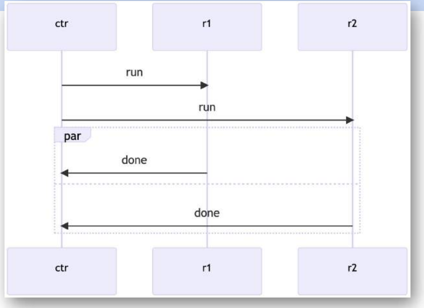
Not tree-like

Wrap up



Choreographies

- What is a system of communicating agents (asynchronous)



Pomsets

- What is a pomset
- Semantics as a set of pomsets
- Semantics as a **branching pomset**

Event Structures & Realisability

- **Realisable**: **composed local beh.** = **global beh.**
- Sufficient conditions for realisability