True Concurrency, Logic and Verification

Paolo Baldan
University of Padova

joint work with
Silvia Crafa, Alberto Carraro

Outline

- Behavioural theory for true concurrency. Why?
- From behavioural equivalences to a **behavioural logics for true concurrency**
- Some open questions

Why?

True concurrency, why?

- True concurrency only as an **abstraction**
- A concurrent program executes in single-processor machines (interleaving)
  - No longer true since some time ...
  - Distributed systems, multi-processors, multi-core

True concurrency, why?

- True concurrency **not observable**

$a \parallel b$

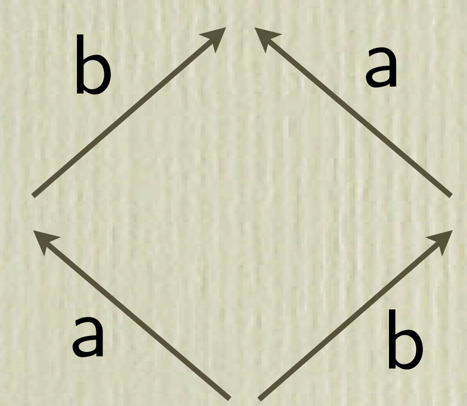
$ab + ba$

True concurrency, why?

- True concurrency **not observable**

$a \parallel b$

$ab + ba$



True concurrency, why?

- True concurrency **not observable**
  - might be, but even if not directly observable it is there
  - essential/convenient for characterising properties like parallelism, races, interferences, information-flow, ...

Example: Non-interference

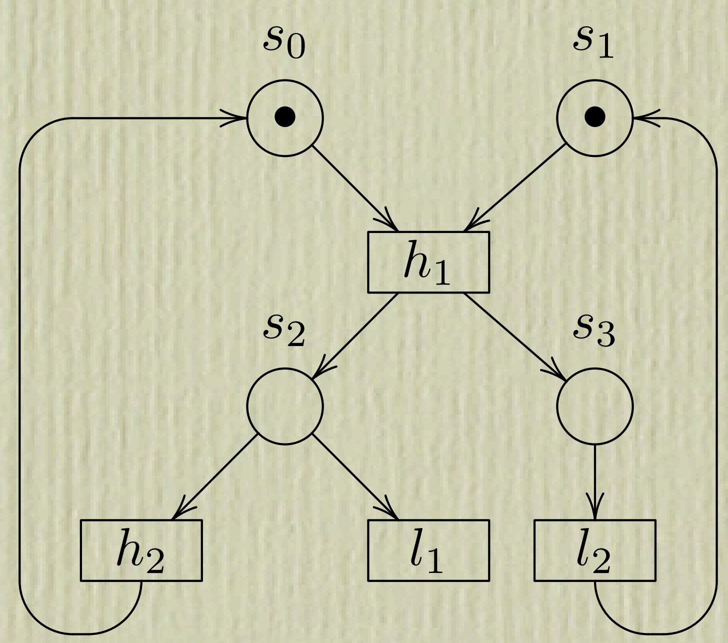
- E.g. **Non-interference** [Goguen,Meseguer]
  - hierarchy on actions (e.g., simplest low - high)
  - a system is **secure** when activity at **high** level is not visible at **low** level

Example: Non-interference

- E.g. **Non-interference** [Goguen,Meseguer]
  - hierarchy on actions (e.g., simplest low - high)
  - a system is **secure** when activity at **high** level is not visible at **low** level
- (B)**NDC** (Non-Deducibility on Composition)

$$\forall H. \quad Sys \sim_{low} Sys \mid H$$

Non interference



- Petri nets
  [Busi, Gorrieri],
  [Best,Darondeau,Gorrieri]

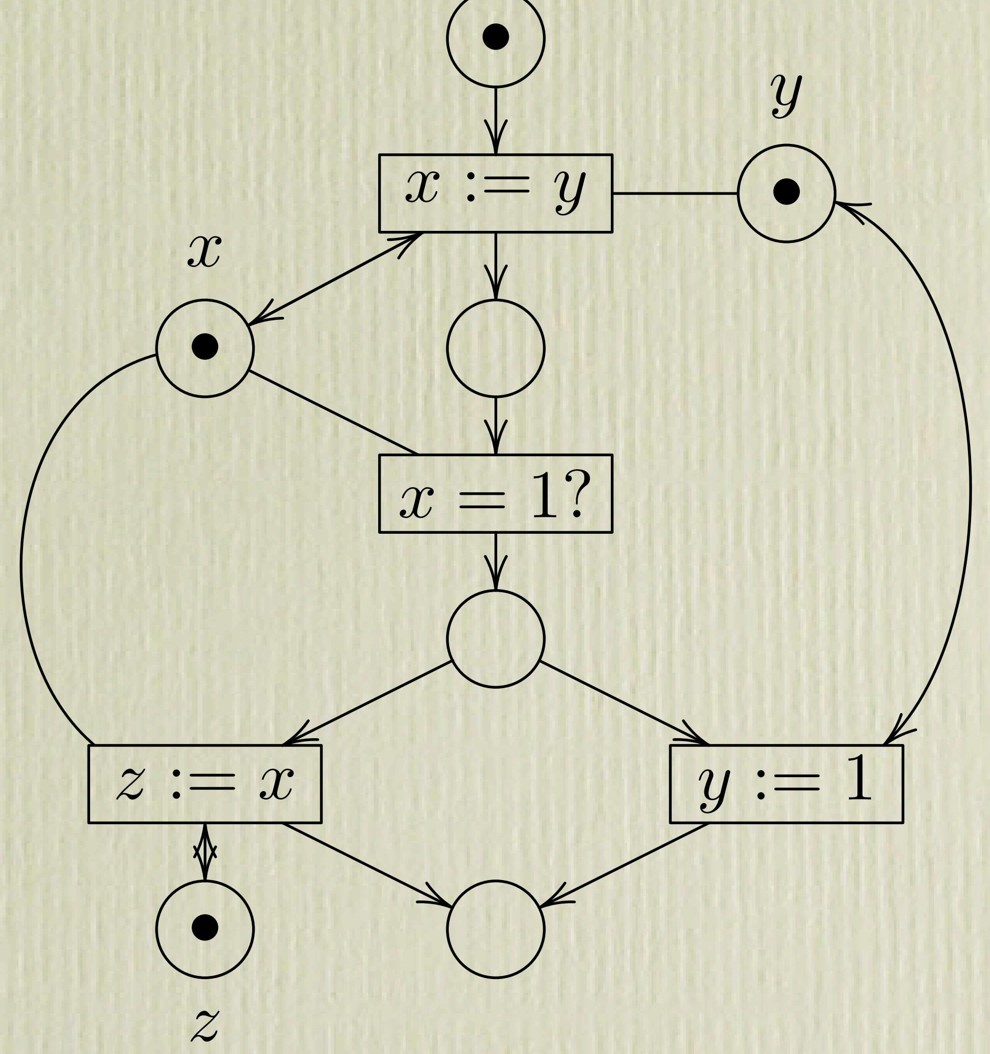
$$\forall H. \quad N \sim_{low} N \mid H$$

- Expressible as the absence of certain **causal dependencies** from ***H*** to ***L*** [PN'14]

Example: Atomicity check

- Concurrent language with shared memory
- Translation into Petri nets

x := *y*;
if (*x* = 1) then *z* := *x*
else *y* := 1;



Example: Atomicity check

- Atomicity assertion

atomic{
  $x := y$;
  if ($x = 1$) then $z := x$
    else $y := 1$;
}

- Reduced to the absence of a triple of events

$$e_1 \leq e \leq e_1'$$

with ***e_1*, *e_1'*** in the **atomic block**, while ***e*** **outside**

[Farzan, Madhusan, ...]

Reversible systems

- When a system is reversible, an action could be reversed only after its causal consequences
- **Causality** and **concurrency** come naturally into play in observational theories of **reversible systems**

{Ulidowski's talk}

True concurrency, why?

- Even though you are still not interested ...
- Properties expressible in an interleaving semantics can be possibly **expressed** and **checked** much more efficiently using a true concurrent models
    - Eg. Deadlocks, hazards, LTL on prefixes of the unfolding {McMillan], {Esparza], {Vogler], ...

Operational models & Behavioural equivalences

Event structures

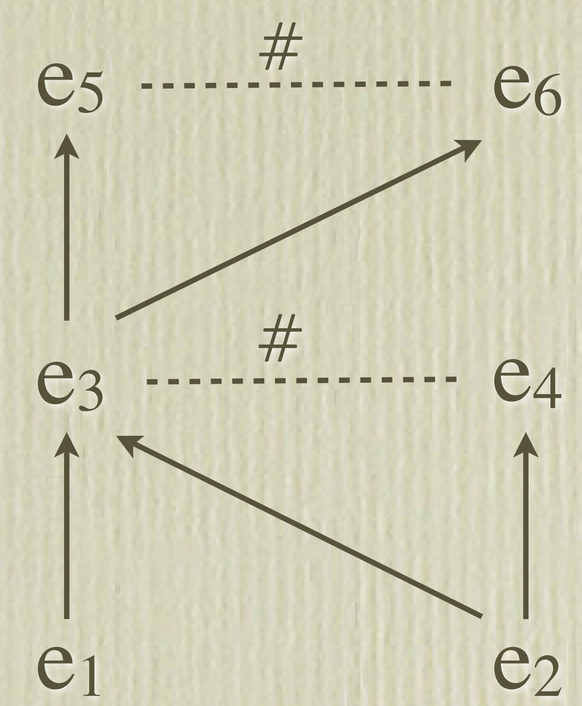
$(E, \leq, \#, \lambda)$

$$
\begin{tikzcd}
e_5 \arrow[rr, dash, dashed, "\#"] & & e_6 \\
e_3 \arrow[u] \arrow[urr] \arrow[rr, dash, dashed, "\#"] & & e_4 \\
e_1 \arrow[u] & & e_2 \arrow[ull] \arrow[u]
\end{tikzcd}
$$

[Nielsen,Plotkin, Winskel]

Event structures

$(E, \leq, \#, \lambda)$



- E events

[Nielsen,Plotkin, Winskel]

Event structures

$(E, \leq, \#, \lambda)$

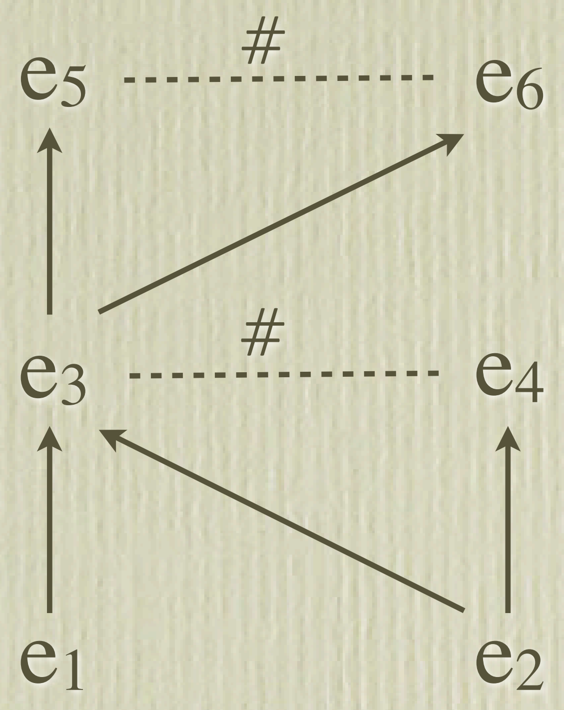
$$\begin{tikzcd}
e_5 \arrow[r, dashed, no head, "\#"] & e_6 \\
e_3 \arrow[u] \arrow[ur] \arrow[r, dashed, no head, "\#"] & e_4 \\
e_1 \arrow[u] & e_2 \arrow[ul] \arrow[u]
\end{tikzcd}$$

- E events
- ≤ causality

[Nielsen,Plotkin, Winskel]

Event structures

$(E, \leq, \#, \lambda)$

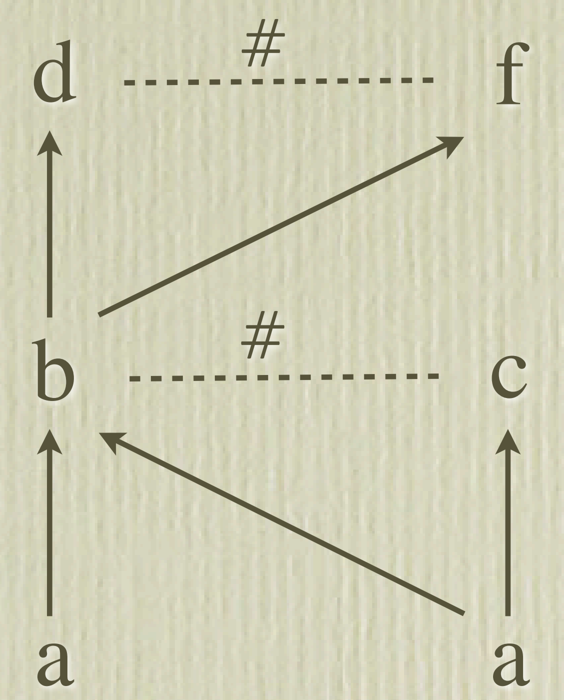


- E events
- $\leq$ causality
- # conflict

[Nielsen,Plotkin, Winskel]

Event structures

$(E, \leq, \#, \lambda)$



- E events
- ≤ causality
- # conflict

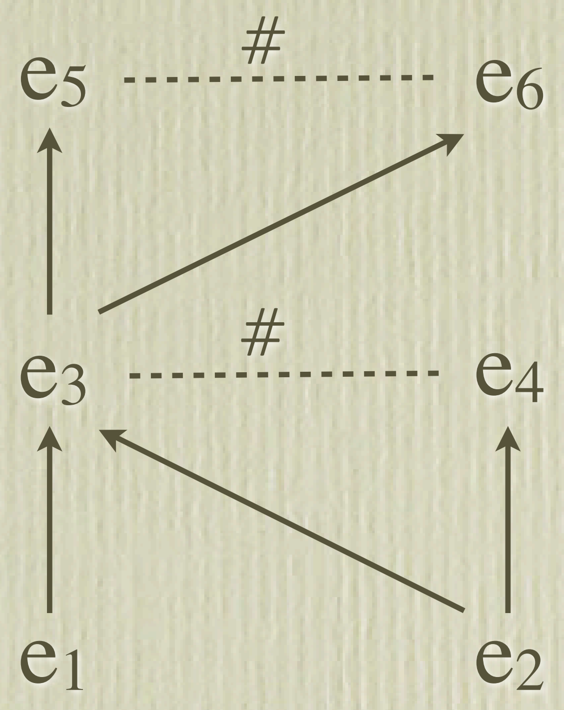
[Nielsen,Plotkin, Winskel]

Event structures

$(E, \leq, \#, \lambda)$

Computations as **configurations**

(causally closed, conflict-free)

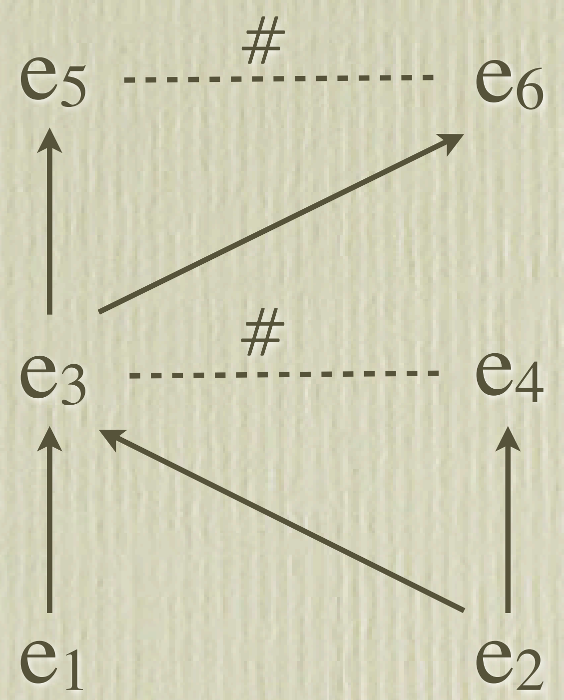


Event structures

$(E, \leq, \#, \lambda)$

Computations as **configurations**

(causally closed, conflict-free)



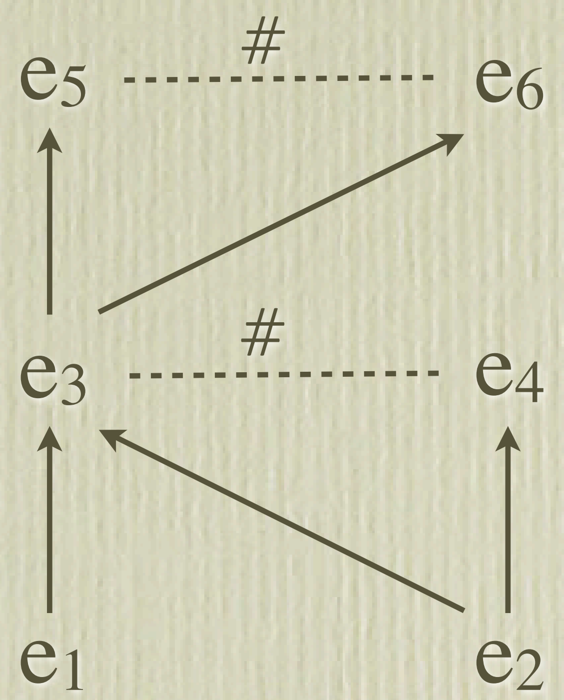
$$\emptyset \xrightarrow{\{e_1\}} \{e_1\} \xrightarrow{\{e_3\}} \{e_1, e_3\}$$

Event structures

$(E, \leq, \#, \lambda)$

Computations as **configurations**

(causally closed, conflict-free)



$$\emptyset \xrightarrow{\{e_1\}} \{e_1\} \xrightarrow{\{e_3\}} \{e_1, e_3\}$$

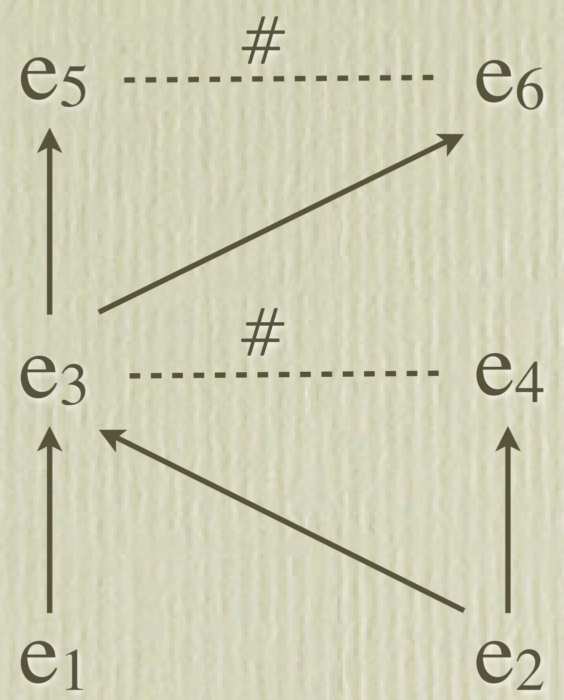
$$\emptyset \xrightarrow{\{e_1, e_2\}} \{e_1, e_2\} \xrightarrow{\{e_3, e_5\}} \{e_1, e_2, e_3, e_5\}$$

Event structures

(E, ≤, #, λ)

Computations as **configurations**

(causally closed, conflict-free)



$$\emptyset \xrightarrow{\{e_1\}} \{e_1\} \xrightarrow{\{e_3\}} \{e_1, e_3\}$$

$$\emptyset \xrightarrow{\{e_1, e_2\}} \{e_1, e_2\} \xrightarrow{\{e_3, e_5\}} \{e_1, e_2, e_3, e_5\}$$

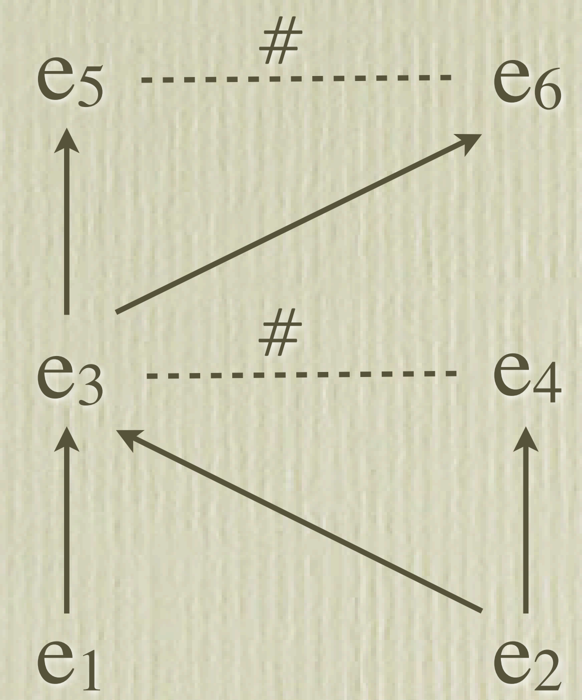
step

Event structures

(E, ≤, #, λ)

Computations as **configurations**

(causally closed, conflict-free)



$$\emptyset \xrightarrow{\{e_1\}} \{e_1\} \xrightarrow{\{e_3\}} \{e_1, e_3\}$$

$$\emptyset \xrightarrow{\{e_1,e_2\}} \{e_1, e_2\} \xrightarrow{\{e_3,e_5\}} \{e_1, e_2, e_3, e_5\}$$

step

pomset

Behavioural equivalence

- Defined on top of the operational model, taking different observations ...

True concurrent spectrum

hereditary history-preserving bisimilarity

interleaving bisimilarity

[van Glabbeek, Goltz]

True concurrent spectrum

hereditary history-preserving bisimilarity

$\downarrow$

history-preserving bisimilarity

interleaving bisimilarity

[van Glabbeek, Goltz]

True concurrent spectrum

hereditary history-preserving bisimilarity

↓

history-preserving bisimilarity

↓

pomset bisimilarity

interleaving bisimilarity

[van Glabbeek, Goltz]

True concurrent spectrum

hereditary history-preserving bisimilarity

↓

history-preserving bisimilarity

↓

pomset bisimilarity

↓

step bisimilarity

↓

interleaving bisimilarity

[van Glabbeek, Goltz]

Behavioural Logic?

Interleaving world

(interleaving) bisimilarity

trace equivalence

[van Glabbeek's LTBT spectrum]

Interleaving world

(interleaving) bisimilarity ⟺ Hennessy-Milner logic

$$\varphi ::= \top \mid \langle a \rangle \varphi \mid \neg \varphi \mid \varphi \wedge \varphi$$

trace equivalence

[van Glabbeek's LTBT spectrum]

Interleaving world

(interleaving) bisimilarity

Hennessy-Milner logic

$\varphi ::= \top \mid \langle a \rangle \varphi \mid \neg \varphi \mid \varphi \wedge \varphi$

trace equivalence

[van Glabbeek's LTBT spectrum]

Interleaving world

(interleaving) bisimilarity ⇔ Hennessy-Milner logic
$\varphi ::= \top \mid \langle a \rangle \varphi \mid \neg \varphi \mid \varphi \wedge \varphi$

simulation equivalence ⇔ $\varphi ::= \top \mid \langle a \rangle \varphi \mid \varphi \wedge \varphi$

trace equivalence

[van Glabbeek's LTBT spectrum]

Interleaving world

(interleaving) bisimiliarity ⟺ Hennessy-Milner logic $\varphi ::= \top \mid \langle a \rangle \varphi \mid \neg \varphi \mid \varphi \wedge \varphi$

simulation equivalence ⟺ $\varphi ::= \top \mid \langle a \rangle \varphi \mid \varphi \wedge \varphi$

trace equivalence

[van Glabbeek's LTBT spectrum]

Interleaving world

(interleaving) bisimilarity ⟷ Hennessy-Milner logic $\varphi ::= \top \mid \langle a \rangle \varphi \mid \neg \varphi \mid \varphi \wedge \varphi$

simulation equivalence ⟷ $\varphi ::= \top \mid \langle a \rangle \varphi \mid \varphi \wedge \varphi$

trace equivalence ⟷ $\varphi ::= \top \mid \langle a \rangle \varphi$

[van Glabbeek's LTBT spectrum]

Logics for true concurrency

- [DeNicola-Ferrari 90]
  Framework for several temporal logics.
  Pomset bis. and weak hp-bis.

- [Hennessy-Stirling 85, Nielsen-Clausen 95]
  Charaterise hhp-bis with past-tense/back step modalities (no autoconcurrency)

- [Bradfield-Froschle 02, Gutierrez 09]
  Modal logics for action independence/causality
  Captures hp-bis.

- ....

A logic for true concurrency

$$\varphi ::= \top \mid \langle \mathsf{a} \rangle \varphi \mid \neg\varphi \mid \varphi \wedge \varphi$$

A logic for true concurrency

$$\varphi ::= \top \ \mid \langle \mathsf{a} z \rangle \varphi \ \mid \ \neg\varphi \ \mid \ \varphi \wedge \varphi$$

A logic for true concurrency

$$\varphi ::= \top \mid \langle \mathbf{x}, \overline{\mathbf{y}} < \mathsf{a} z \rangle \varphi \mid \neg \varphi \mid \varphi \wedge \varphi$$

A logic for true concurrency

$$\varphi ::= \top \ \mid \ (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}z)\varphi \ \mid \langle z \rangle \varphi \ \mid \ \neg \varphi \ \mid \ \varphi \wedge \varphi$$

A logic for true concurrency

$$\varphi ::= \top \mid (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}z)\varphi \mid \langle z \rangle \varphi \mid \neg\varphi \mid \varphi \wedge \varphi$$

Interpreted over event structures

$$C \models_\eta \varphi$$

A logic for true concurrency

$$\varphi ::= \top \mid (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}z)\varphi \mid \langle z \rangle \varphi \mid \neg\varphi \mid \varphi \wedge \varphi$$

Interpreted over event structures

$$C \models_\eta \varphi$$

configuration
state of the computation

A logic for true concurrency

$$\varphi ::= \top \;\mid\; (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}z)\varphi \;\mid \langle z \rangle \varphi \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi$$

Interpreted over event structures

$$C \models_{\eta} \varphi$$

configuration
state of the computation

describes some futures
for C

A logic for true concurrency

$$\varphi ::= \top \;\mid\; (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}z)\varphi \;\mid \langle z \rangle \varphi \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi$$

Interpreted over event structures

$$C \models_\eta \varphi$$

configuration
state of the computation

describes some futures
for C

$$\eta : Var \to E$$

records the events
bound to variables

Semantics

$C \models_\eta (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a} z)\varphi$

exists an event e in the future of C s.t.

$\eta(\mathbf{x}) < e,\ \eta(\mathbf{y}) \| e,\ \lambda(e) = \mathsf{a}$ and $C \models_{\eta[z \mapsto e]} \varphi$

Semantics

$C \models_\eta (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}z)\varphi$

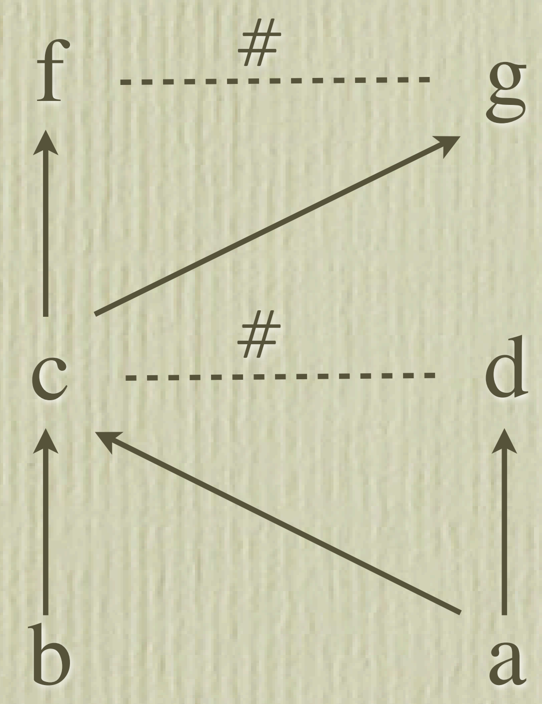
exists an event e in the future of C s.t.

$\eta(\mathbf{x}) < e,\ \eta(\mathbf{y}) \,||\, e,\ \lambda(e) = \mathsf{a}$ and $C \models_{\eta[z \mapsto e]} \varphi$

$C \models_\eta \langle z \rangle \varphi$

if $C \xrightarrow{\eta(z)} C'$ and $C' \models_\eta \varphi$

Examples

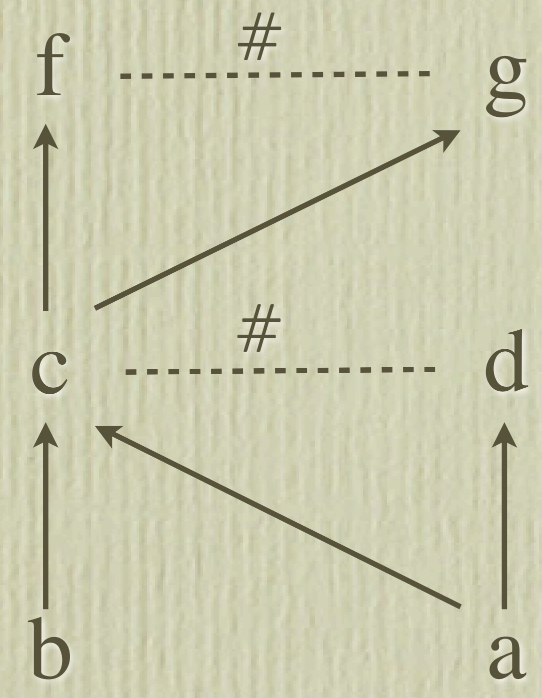


Examples

$$\begin{tikzcd}
f \arrow[r, dash, dashed, "\#"] & g \\
c \arrow[u] \arrow[ur] \arrow[r, dash, dashed, "\#"] & d \\
b \arrow[u] & a \arrow[ul] \arrow[u]
\end{tikzcd}$$

$$\emptyset \models_{\emptyset} (\mathsf{c}x)\top$$

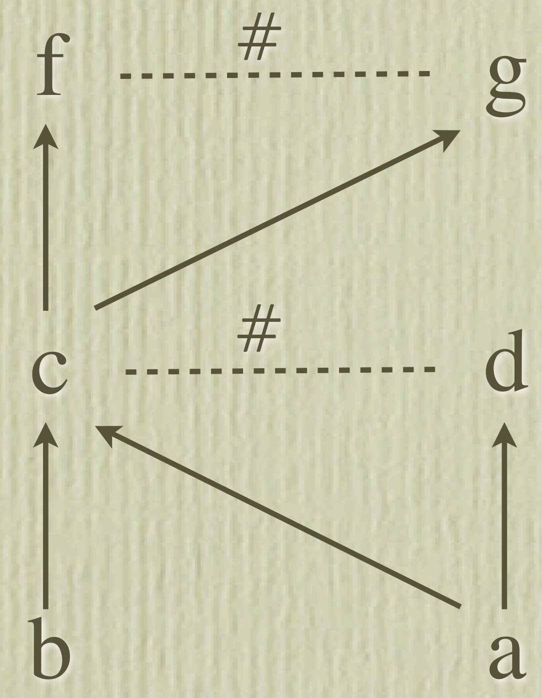
Examples



$\emptyset \models_{\emptyset} (\mathsf{c}x)\top$

$\emptyset \models_{\emptyset} (\mathsf{c}x)\top \;\wedge (\mathsf{d}y)\top$

Examples

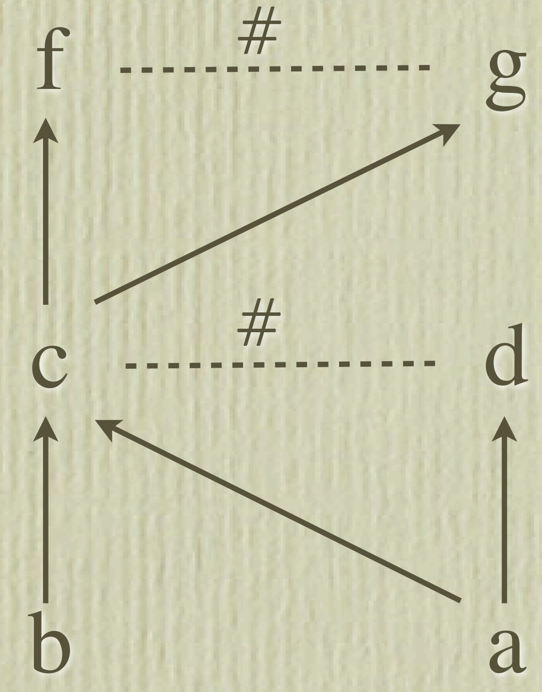


$$\emptyset \models_{\emptyset} (\mathsf{c}x)\top$$

$$\emptyset \models_{\emptyset} (\mathsf{c}x)\top \ \wedge (\mathsf{d}y)\top$$

$$\emptyset \not\models_{\emptyset} (\mathsf{c}x)\langle x\rangle\top$$

Examples

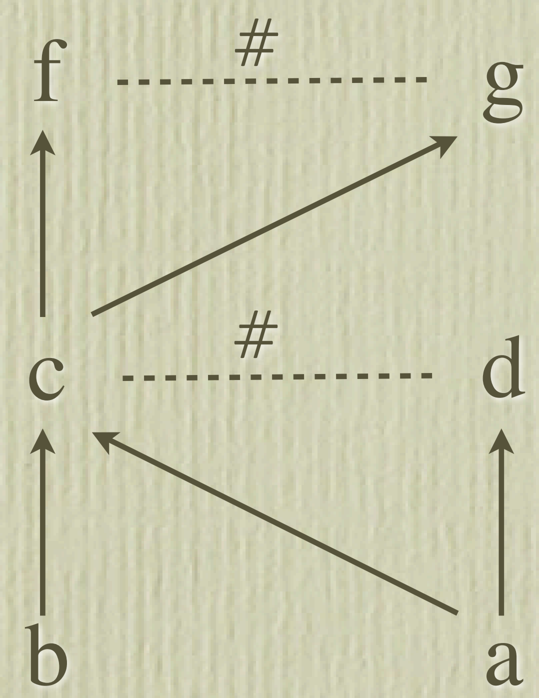


Examples

$$\begin{tikzcd} f \arrow[r, dash, dashed, "\#"] & g \\ c \arrow[u] \arrow[ur] \arrow[r, dash, dashed, "\#"] & d \\ b \arrow[u] & a \arrow[ul] \arrow[u] \end{tikzcd}$$

$$\emptyset \models_{\emptyset} (\mathsf{a}x)\langle x\rangle(x < \mathsf{d}y)\langle y\rangle\top$$

Examples



$$\emptyset \models_{\emptyset} (\mathsf{a}x)\langle x\rangle(x < \mathsf{d}y)\langle y\rangle\top$$

$$\emptyset \not\models_{\emptyset} (\mathsf{a}x)\langle x\rangle(x < \mathsf{d}y)\langle y\rangle(\mathsf{c}z)\top$$

Examples

$$
\begin{tikzcd}
\mathrm{f} \arrow[r, dash, dashed, "\#"] & \mathrm{g} \\
\mathrm{c} \arrow[u] \arrow[ur] \arrow[r, dash, dashed, "\#"] & \mathrm{d} \\
\mathrm{b} \arrow[u] & \mathrm{a} \arrow[ul] \arrow[u]
\end{tikzcd}
$$

$$\emptyset \models_{\emptyset} (\mathsf{a}x)\langle x\rangle(x < \mathsf{d}y)\langle y\rangle\top$$

$$\emptyset \not\models_{\emptyset} (\mathsf{a}x)\langle x\rangle(x < \mathsf{d}y)\langle y\rangle(\mathsf{c}z)\top$$

$$\emptyset \models_{\emptyset} (\mathsf{a}x)(\bar{x} < \mathsf{b}y)(\mathsf{c}z)\langle x\rangle\langle y\rangle\langle z\rangle\top$$

A logic for hhp-bisimilarity

Theorem: Logical equivalence is hhp-bisimilarity

$$\forall\varphi.\ (\mathbf{E}_1 \models \varphi \quad \Leftrightarrow \quad \mathbf{E}_2 \models \varphi) \qquad \text{iff} \qquad \mathbf{E}_1 \sim_{hhp} \mathbf{E}_2$$

A logic for hhp-bisimilarity

Theorem: Logical equivalence is hhp-bisimilarity

$$\forall \varphi.\ (\mathbf{E}_1 \models \varphi \quad \Leftrightarrow \quad \mathbf{E}_2 \models \varphi) \qquad \text{iff} \qquad \mathbf{E}_1 \sim_{hhp} \mathbf{E}_2$$

Fragments of the logics corresponds to **coarser equivalences** in the true concurrent spectrum

Abbreviations

- **Immediate execution**

$$\langle\!| \mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z |\!\rangle\, \varphi$$

$$(\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z)\langle z\rangle\, \varphi$$

Abbreviations

- **Immediate execution**

$$\langle\!| \mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z |\!\rangle\, \varphi$$

$$(\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z)\langle z \rangle\, \varphi$$

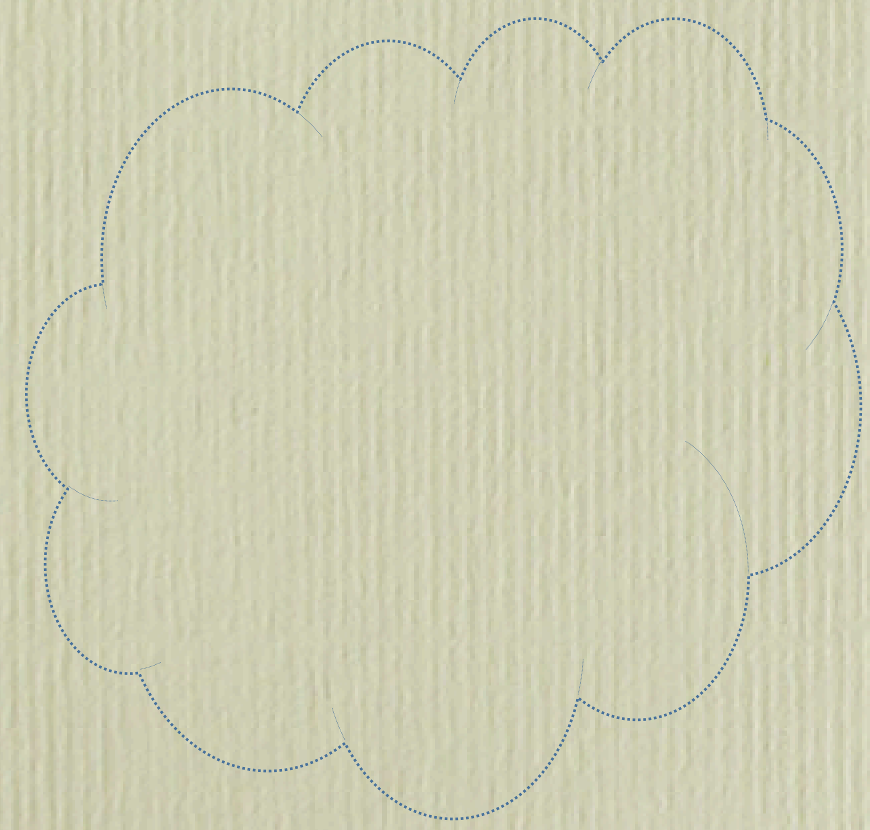
- **Step**

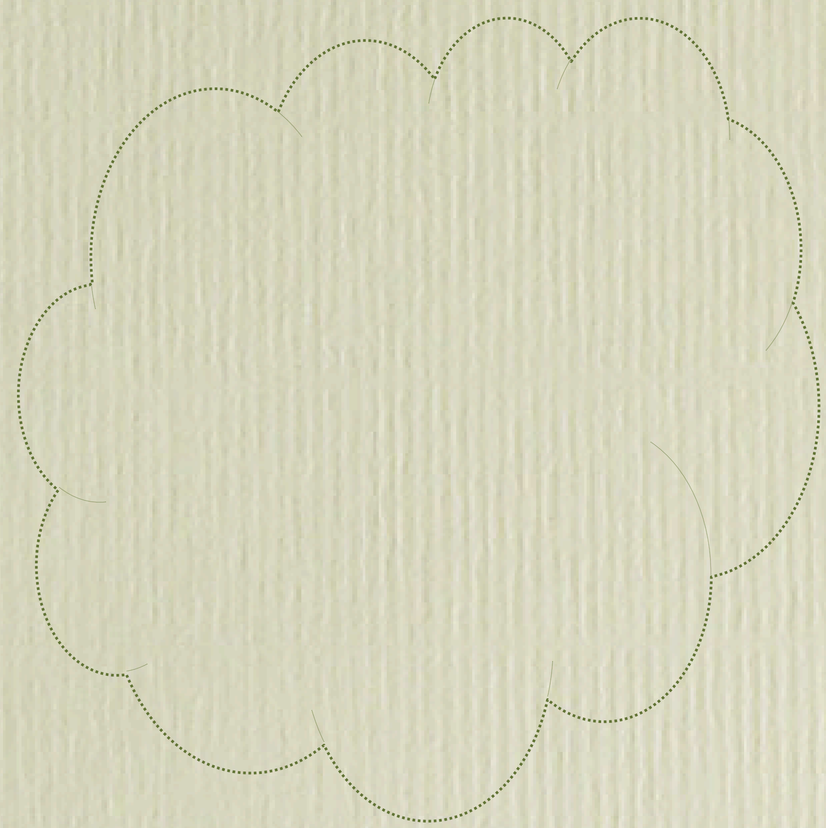
$$(\langle\!| \mathbf{a} z |\!\rangle \otimes \langle\!| \mathbf{b} z' |\!\rangle)\varphi$$

$$\langle\!| \mathsf{a} z |\!\rangle \langle\!| \bar{z} < \mathsf{b} z' |\!\rangle \varphi$$

Step Bisimilarity

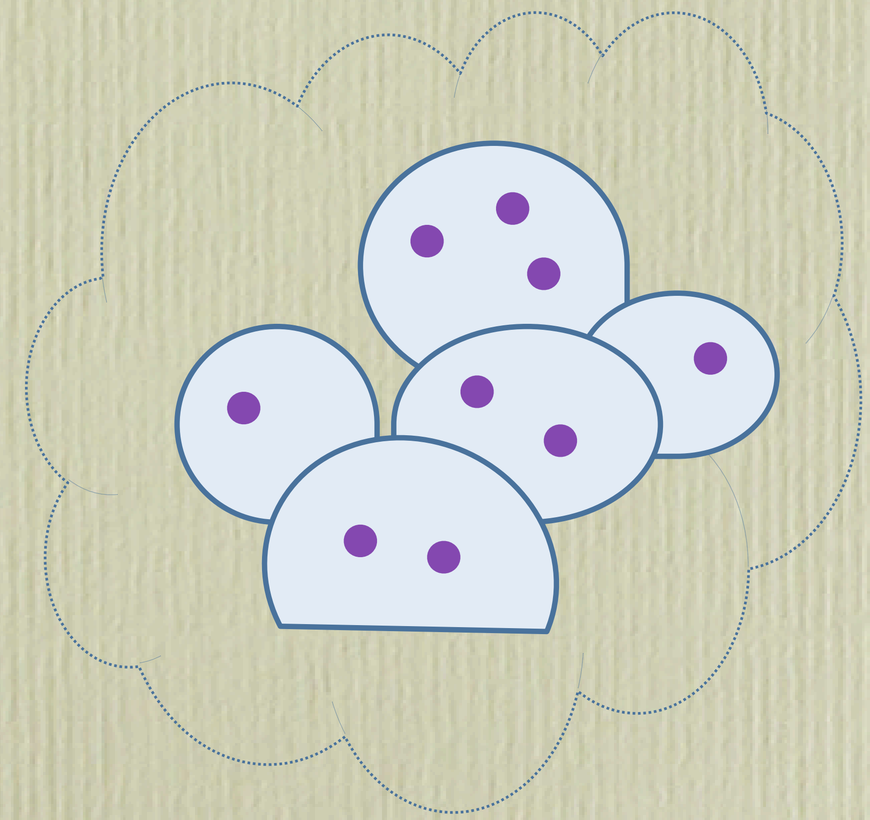
- Step transitions: observes concurrency

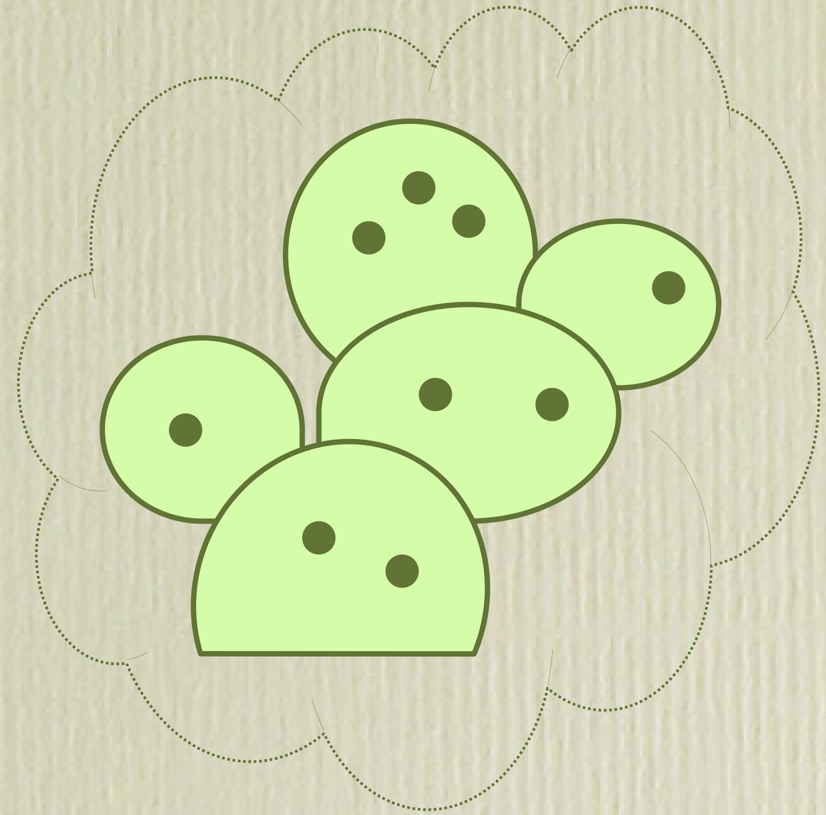




Step Bisimilarity

- Step transitions: observes concurrency





Step Bisimilarity

$$\varphi \ ::= \ (\langle\!|\mathsf{a_1}\, x_1|\!\rangle \otimes \cdots \otimes \langle\!|\mathsf{a_n}\, x_n|\!\rangle)\ \varphi \ \mid \ \varphi \wedge \varphi \ \mid \ \neg\varphi \ \mid \ \mathsf{T}$$

Step Bisimilarity

$$\varphi \;::=\; (\langle\!|\, \mathsf{a}_1\, x_1 \,|\!\rangle \otimes \cdots \otimes \langle\!|\, \mathsf{a}_n\, x_n \,|\!\rangle)\; \varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \neg\varphi \;\mid\; \mathsf{T}$$

$$\begin{tikzcd} b \arrow[d, no head] & a \arrow[d, no head] \\ a \arrow[r, dotted, no head] & b \end{tikzcd}$$

$$a \qquad b$$

Step Bisimilarity

$$\varphi \;::=\; (\langle\!|\mathsf{a}_1\, x_1|\!\rangle \otimes \cdots \otimes \langle\!|\mathsf{a_n}\, x_n|\!\rangle)\ \varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \neg\varphi \;\mid\; \mathsf{T}$$

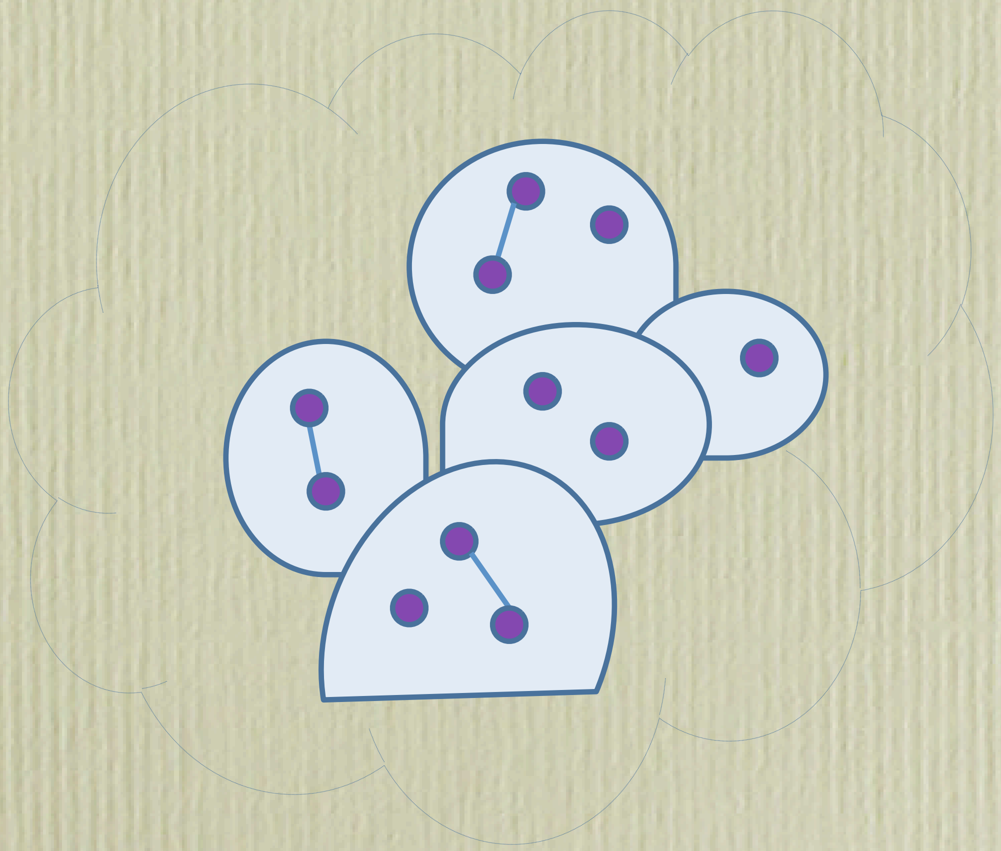
$$\begin{tikzcd} b \arrow[d, dash] & a \arrow[d, dash] \\ a \arrow[r, dotted, dash] & b \end{tikzcd} \quad \not\models \quad (\langle\!|\mathsf{a}\, z|\!\rangle \otimes \langle\!|\mathsf{b}\, z'|\!\rangle)\mathsf{T} \quad \Dashv \quad \begin{array}{cc} a & b \end{array}$$

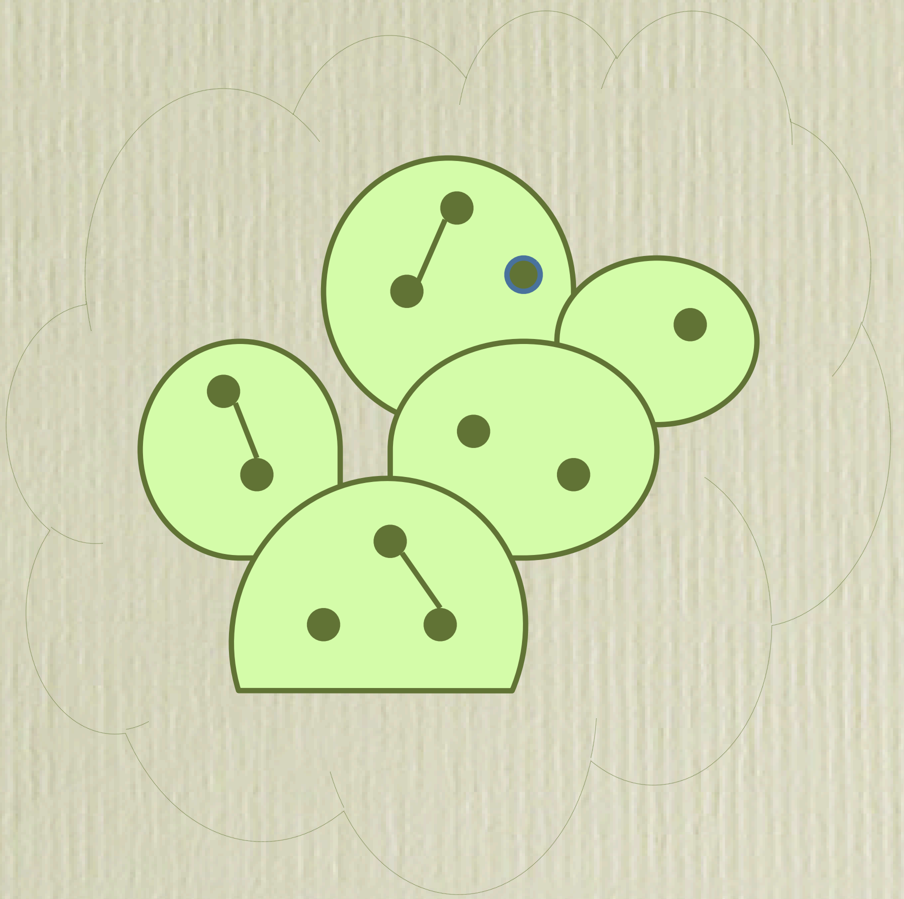
Pomset bisimilarity

- Observes also causality

Pomset bisimilarity

- Observes also causality





Pomset Bisimilarity

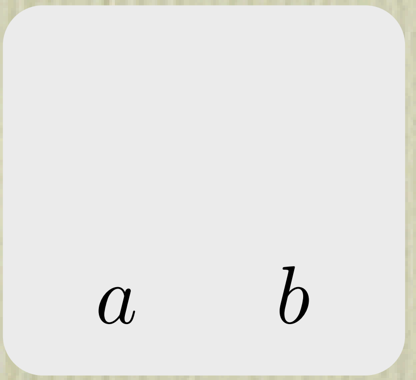
$$\varphi \;::=\; \langle\!|\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z|\!\rangle\, \varphi \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \mathsf{T}$$

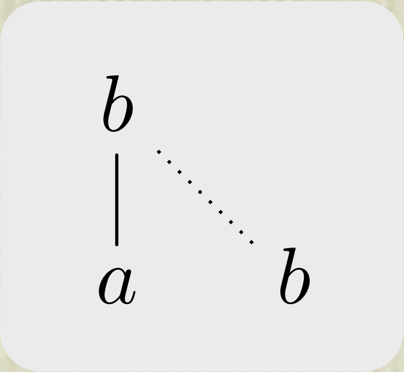
propositional connectives only on closed subformulae

Pomset Bisimilarity

$$\varphi \;::=\; \langle\!|\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z|\!\rangle\, \varphi \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \mathsf{T}$$

propositional connectives only on closed subformulae

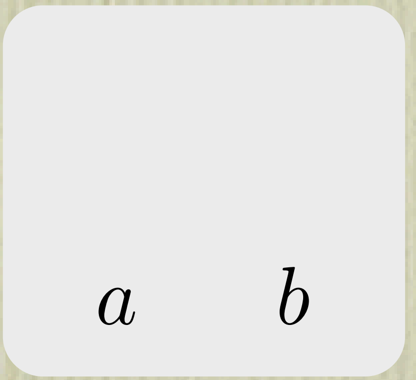




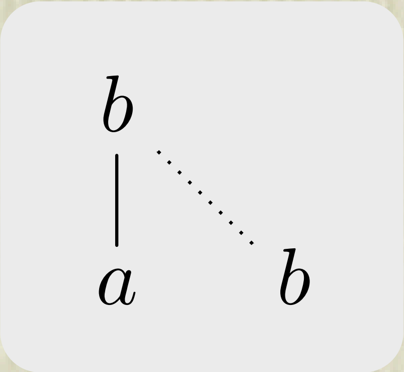
Pomset Bisimilarity

$$\varphi \ ::= \ \langle\!|\, \mathbf{x}, \bar{\mathbf{y}} < \mathsf{a}\, z \,|\!\rangle\, \varphi \ \mid \ \neg\varphi \ \mid \ \varphi \wedge \varphi \ \mid \ \mathsf{T}$$

propositional connectives only on closed subformulae



$$\not\models \quad \langle\!|\mathsf{a}\, x|\!\rangle \langle\!| x < \mathsf{b}\, y |\!\rangle \mathsf{T} \quad \Dashv$$

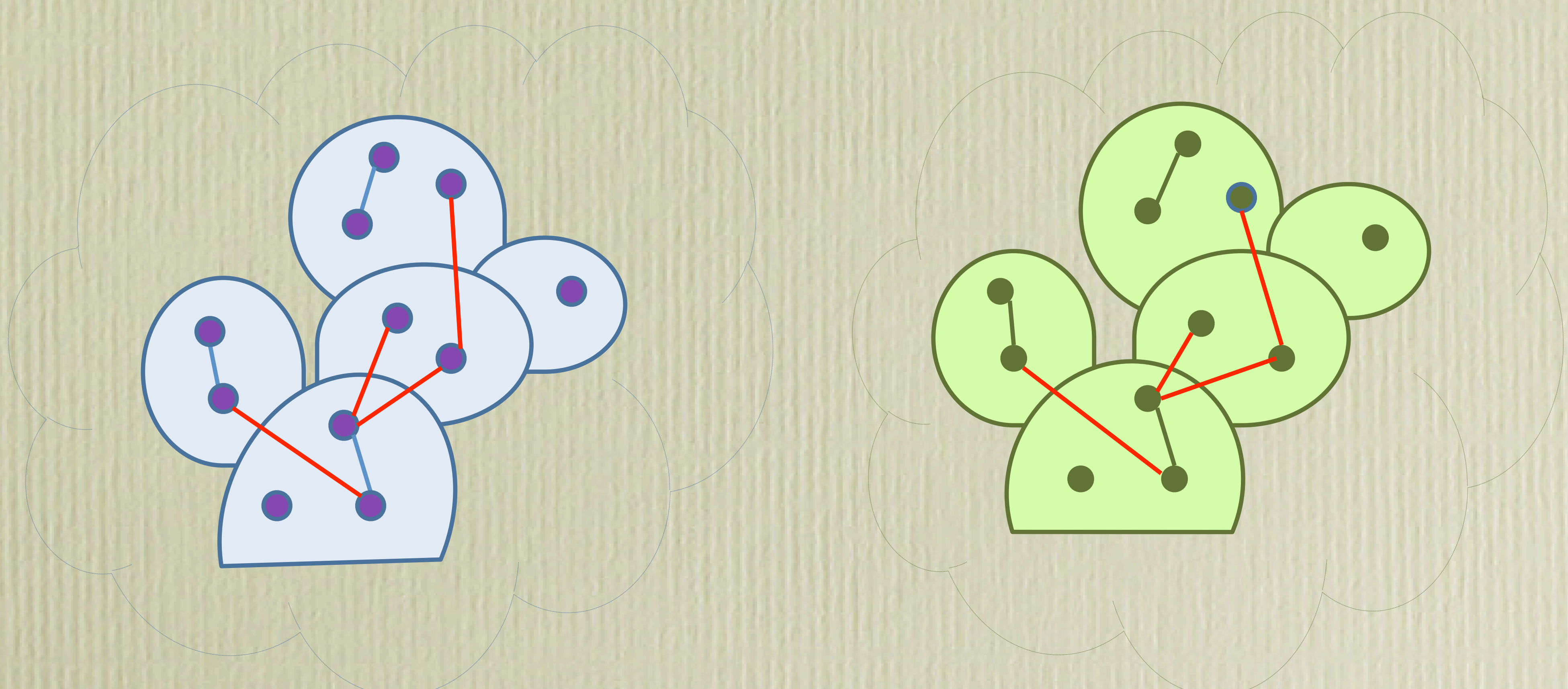


History-preserving Bisim

- An event of a system must be simulated by an event of the other with the same history (causal links)

History-preserving Bisim

- An event of a system must be simulated by an event of the other with the same history (causal links)



History Preserving Bisim

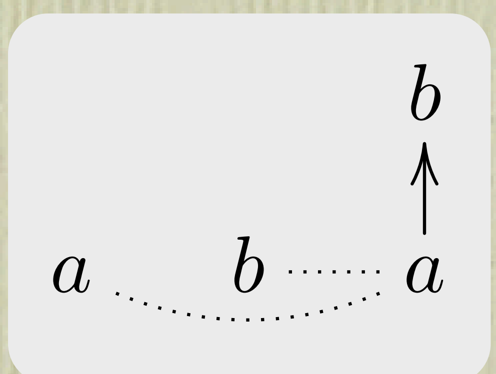
$$\varphi \;\; ::= \;\; \langle\!| \mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z |\!\rangle\, \varphi \;\;|\;\; \neg\varphi \;\;|\;\; \varphi \wedge \varphi \;\;|\;\; \mathsf{T}$$

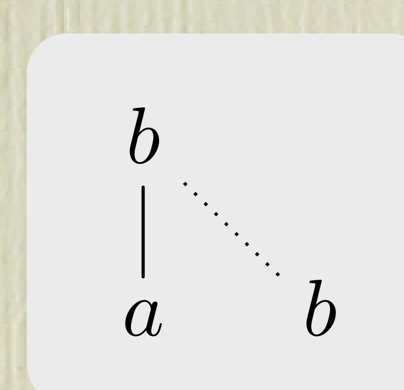
~~connectives only on closed formulae~~

History Preserving Bisim

$$\varphi \;::=\; \langle\!|\mathbf{x}, \bar{\mathbf{y}} < \mathsf{a}\, z|\!\rangle\, \varphi \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \mathsf{T}$$

~~connectives only on closed formulae~~

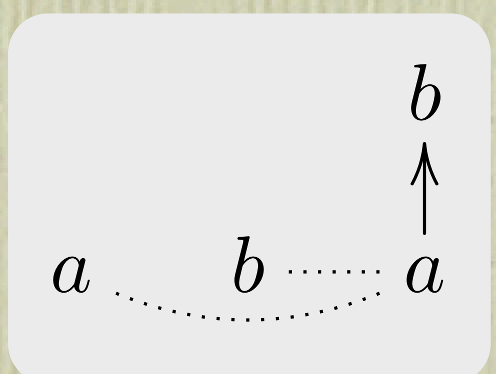




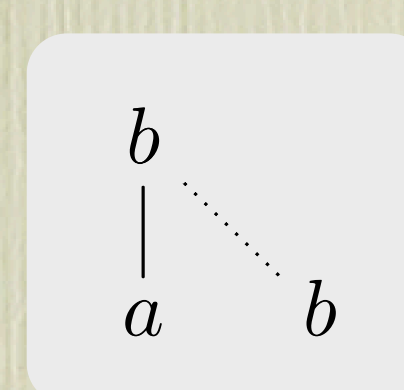
History Preserving Bisim

$$\varphi \;::=\; \langle\!|\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z|\!\rangle\, \varphi \;\mid\; \neg\varphi \;\mid\; \varphi \wedge \varphi \;\mid\; \mathsf{T}$$

~~connectives only on closed formulae~~



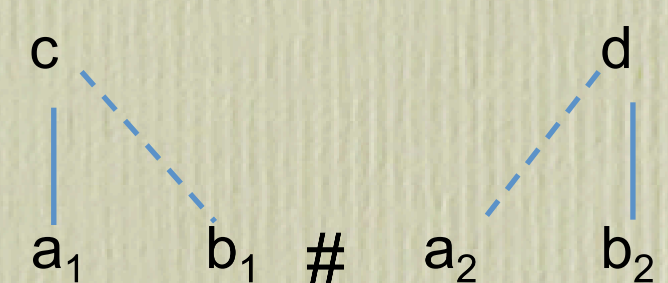
$$\not\models \quad \langle\!|\mathsf{a}\, x|\!\rangle(\langle\!|\overline{x} < \mathsf{b}\, y|\!\rangle \mathsf{T} \wedge \langle\!|x < \mathsf{b}\, z|\!\rangle \mathsf{T}) \quad =\!\!|$$



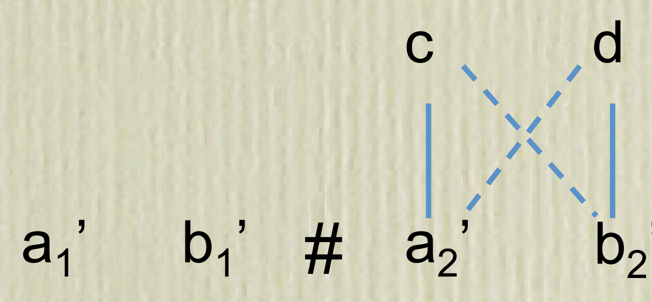
Hereditary HP-bisim.

- Matching between events in the simulation does not depend on the order of concurrent events (which can thus be reversed)!

Event Id Logic
[Phillips,Ulidowski]



$\not\sim_{hhp}$



$$((\mathsf{a}x) \otimes (\mathsf{b}y))((x < \mathsf{c}z) \wedge (y < \mathsf{d}z'))\top$$

Adding recursion

- In order to have an expressive specification logic

$$\varphi \;::=\; \mathsf{T} \;\mid\; \varphi \wedge \varphi \;\mid\; \neg\varphi \;\mid\; (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z)\,\varphi \;\mid\; \langle z \rangle\, \varphi \;\mid\; X(\mathbf{x}) \;\mid\; \mu X(\mathbf{x}).\varphi$$

Adding recursion

- In order to have an expressive specification logic

$$\varphi \;::=\; \mathsf{T} \;\mid\; \varphi \wedge \varphi \;\mid\; \neg\varphi \;\mid\; (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z)\,\varphi \;\mid\; \langle z \rangle\, \varphi \;\mid\; X(\mathbf{x}) \;\mid\; \mu X(\mathbf{x}).\varphi$$

- Invariant φ

$$\nu X.(\varphi \wedge [\![\mathsf{Act}]\!] X)$$

Adding recursion

- In order to have an expressive specification logic

$$\varphi \ ::= \mathsf{T} \ \mid \ \varphi \wedge \varphi \ \mid \ \neg\varphi \ \mid \ (\mathbf{x}, \overline{\mathbf{y}} < \mathsf{a}\, z)\, \varphi \ \mid \ \langle z \rangle\, \varphi \ \mid$$
$$X(\mathbf{x}) \ \mid \ \mu X(\mathbf{x}).\varphi$$

- Invariant φ

$$\nu X.(\varphi \wedge [\![\mathsf{Act}]\!] X)$$

- Eventually φ

$$\mu X.(\varphi \vee (\langle\!|\mathsf{Act}\,|\!\rangle \mathsf{T} \wedge [\![\mathsf{Act}\,]\!] X)$$

Further examples

- There is a causal chain of ***b***-labelled events ending with an ***a***-labelled event

$$\langle\!|\, \mathsf{b}\, x \,|\!\rangle\, (\mu X(x).(\langle\!|\, x < \mathsf{a}\, z \,|\!\rangle \mathsf{T} \vee \langle\!|\, x < \mathsf{b}\, y \,|\!\rangle\, X(y)))$$

Further examples

- There is a causal chain of ***b***-labelled events ending with an ***a***-labelled event

$$\langle\!|\, \mathsf{b}\, x \,|\!\rangle\, (\mu X(x).(\langle\!|\, x < \mathsf{a}\, z \,|\!\rangle \mathsf{T} \vee \langle\!|\, x < \mathsf{b}\, y \,|\!\rangle\, X(y)))$$

- There is a sequence of steps "***a*** in parallel with ***b***", and finally an ***a***-labelled event:

$$\mu X.(\langle\!|\, \mathsf{a}\, x \,|\!\rangle \mathsf{T} \vee (\langle\!|\, \mathsf{a}\, y \,|\!\rangle \otimes \langle\!|\, \mathsf{b}\, z \,|\!\rangle) X)$$

Further examples

- A high event is never a cause for a low event
- An atomic block is never causally interleaved with an external action
- ...

Model-checking?

- **Model-checking** is **decidable** on **regular** event structures
- Not obvious $\neg(\mathsf{a}x)\neg(x < \mathsf{a}y)\top$
- By reduction to [Madhusan]
- More direct technique? Unfolding prefixes?

Satisfiability?

- Not obvious: no **finite model property**
- Internalized in a Guarded Fragment of FOL {Andreka, van Benthem, and Nemeti}
- Decidable with a transitive operator {Kieronski}, undecidable with two
- GF + fixed point {Gradel-Walukiewicz}

Simpler logic?

$$\varphi ::= \top \mid (\mathsf{a}z)\varphi \mid \langle z\rangle\varphi \mid \neg\varphi \mid \varphi\wedge\varphi$$

- No explicit reference to causality/concurrency
- The logic traces the **history of events in time** (can only check for identity/labels)
- Connection with HD-automata/nominal automata

Connection with HD-automata?

- Encoding of any event structure **E** into an HD-automata **H(E)**

H(E) ~ H(E') iff **E** *hhp-bisimilar* to **E'**

- Proof via logic (two PES satisfy the same formulae iff the corresponding automata do)
- With a finite horizon (bounded lookup) one gets **effective approximations of hhp-bisimilarity**

Open problem

Can true concurrent models be of use for analysing true concurrent systems?