Model Checking under Refinement-closed Notions of Fairness and Its Application

David M. Williams, Joeri de Ruiter and Wan Fokkink

VU University Amsterdam
Radboud University Nijmegen
Eindhoven University of Technology

ICTAC

26 September 2012

Table of contents

Motivation

Any verification using model-based techniques
is only as good as the model of the system.

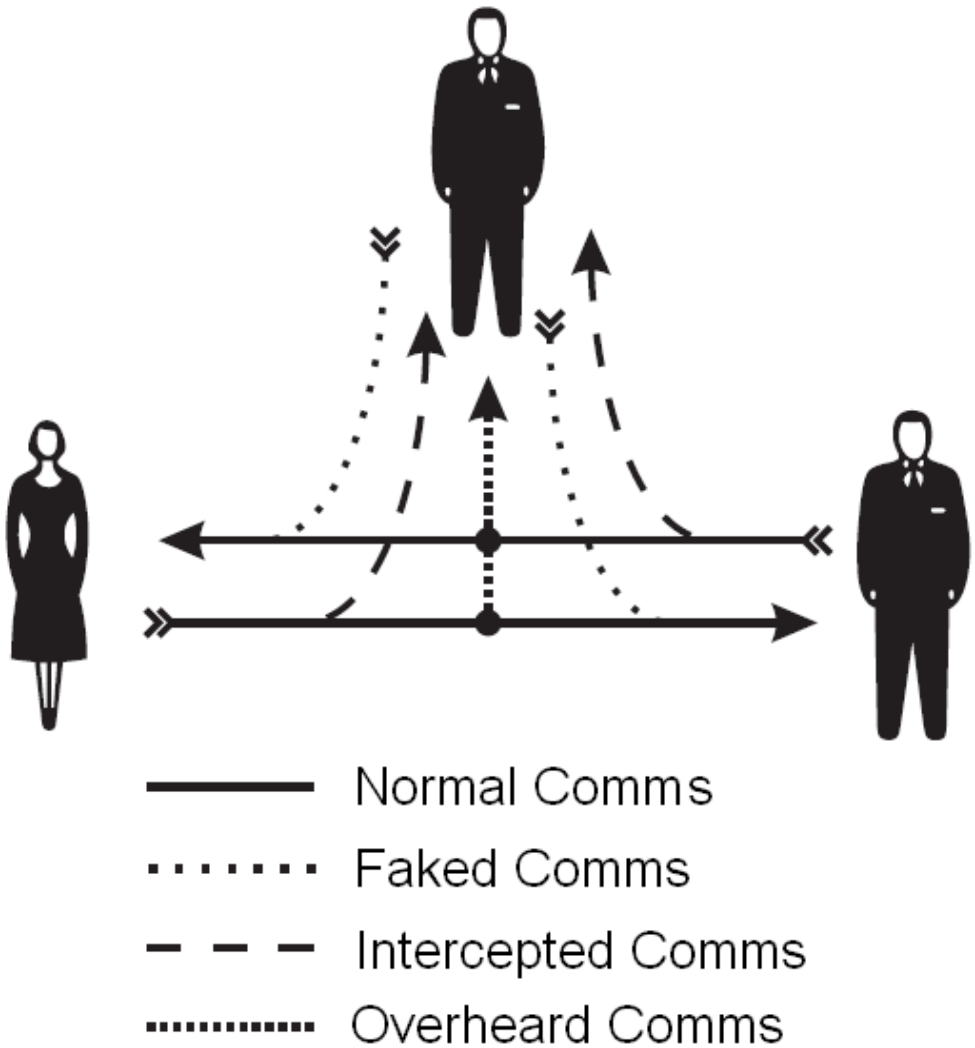
Motivation

Any verification using model-based techniques
is only as good as the model of the system.



Our verification approach relates properties of the model
to properties of the system along a refinement chain.

Motivation


Normal Comms
Faked Comms
Intercepted Comms
Overheard Comms

Model Checking CSP

Refinement Checking

$$\frac{S \sqsubseteq_{\mathcal{M}} P \qquad P \sqsubseteq_{\mathcal{M}} Q}{S \sqsubseteq_{\mathcal{M}} Q}$$

Tool Support: FDR or PAT

LTL Model Checking

$$\frac{P \models \phi \qquad P \sqsubseteq_{\mathcal{M}} Q}{Q \models \phi}$$

Tool Support: ProB or PAT

Model Checking CSP

Refinement Checking

$$\frac{S \sqsubseteq_{\mathcal{M}} P \qquad P \sqsubseteq_{\mathcal{M}} Q}{S \sqsubseteq_{\mathcal{M}} Q}$$

Tool Support: FDR or PAT

LTL Model Checking

$$\frac{P \models \phi \qquad P \sqsubseteq_{\mathcal{M}} Q}{Q \models \phi}$$

Tool Support: ProB or PAT

Model Checking CSP

Refinement Checking

$$\frac{S \sqsubseteq_{\mathcal{M}} P \qquad P \sqsubseteq_{\mathcal{M}} Q}{S \sqsubseteq_{\mathcal{M}} Q}$$

Tool Support: FDR or PAT

LTL Model Checking

$$\frac{P \models \phi \qquad P \sqsubseteq_{\mathcal{M}} Q}{Q \models \phi}$$

Tool Support: ProB or PAT

LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid a \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi \mid \Diamond \phi \mid \Box \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid |a| \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi \mid \Diamond \phi \mid \Box \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi \ \&\ \psi \mid \phi \ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{X}\ \phi \mid \mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$

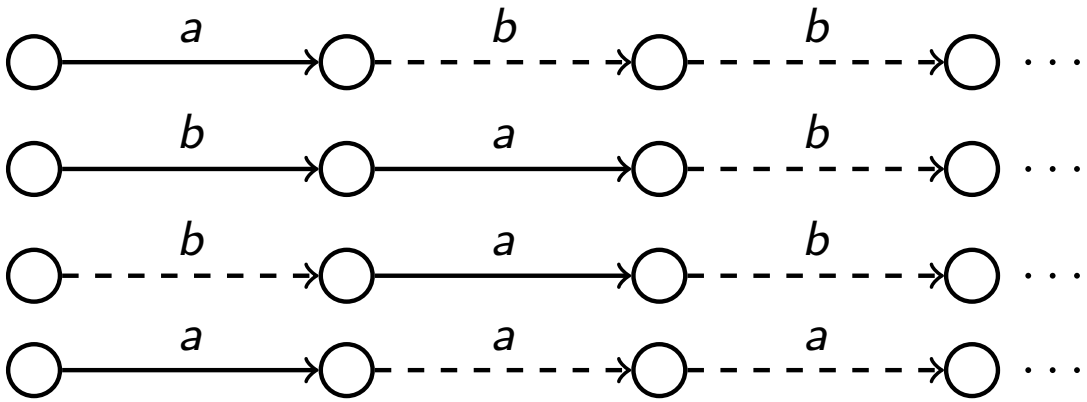
LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid |a| \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi | \Diamond \phi | \Box \phi | \psi \mathcal{U} \phi \mid \phi \mathcal{R} \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi \ \&\ \psi \mid \phi \ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{X}\ \phi \mid \mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$



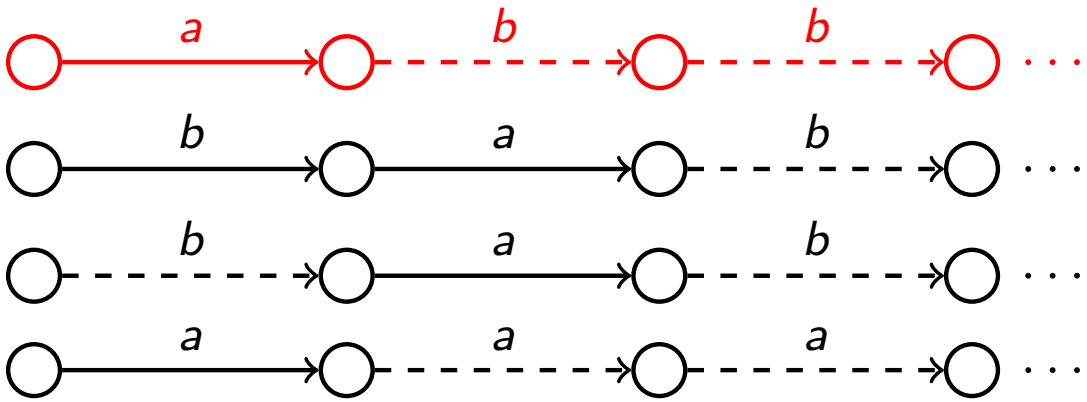
LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid a \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi \mid \Diamond \phi \mid \Box \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid \mathsf{e}(a) \mid \mathsf{deadlock} \mid$$
$$\phi \ \&\ \psi \mid \phi \ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{X}\ \phi \mid \mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$



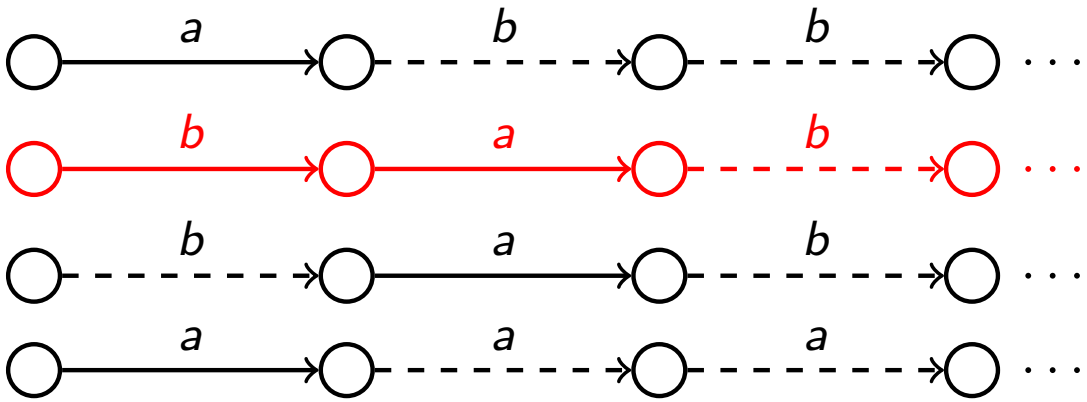
LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid |a| \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi \mid \Diamond \phi \mid \Box \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi \ \&\ \psi \mid \phi \ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{X}\ \phi \mid \mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$



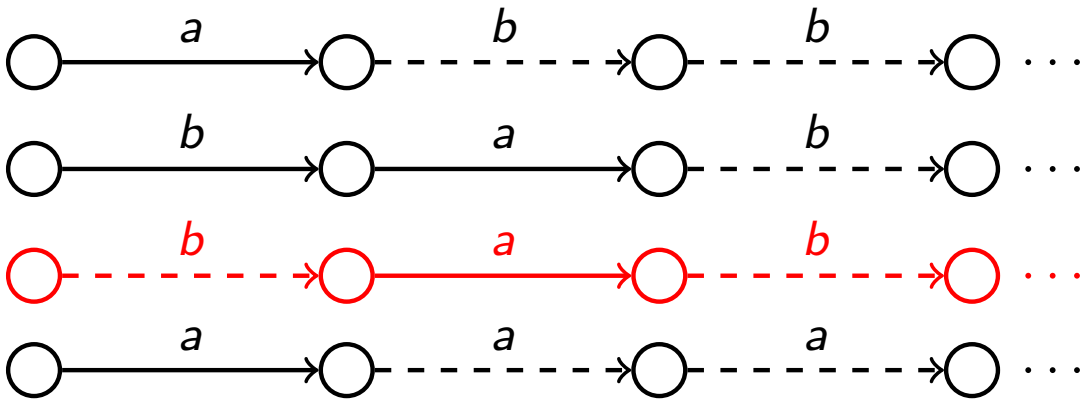
LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid |a| \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi \mid \Diamond \phi \mid \Box \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi \ \&\ \psi \mid \phi \ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{X}\ \phi \mid \mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$



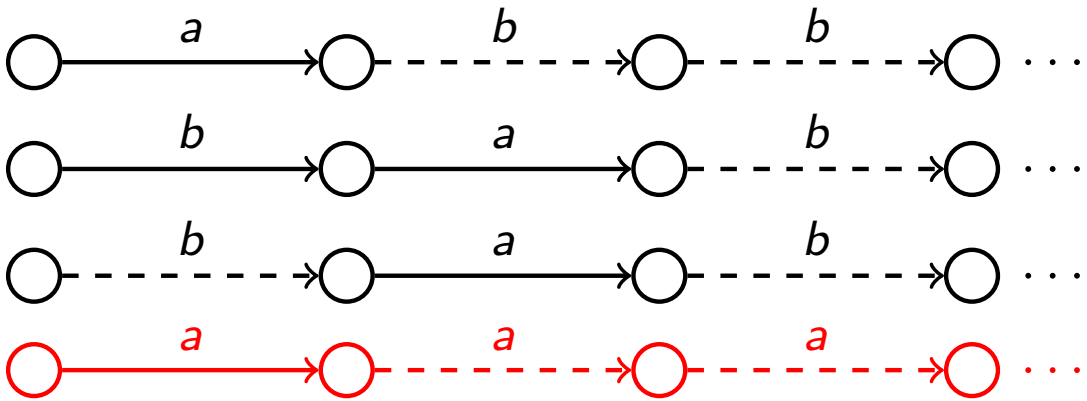
LTL for CSP

Lowe's Temporal Logic

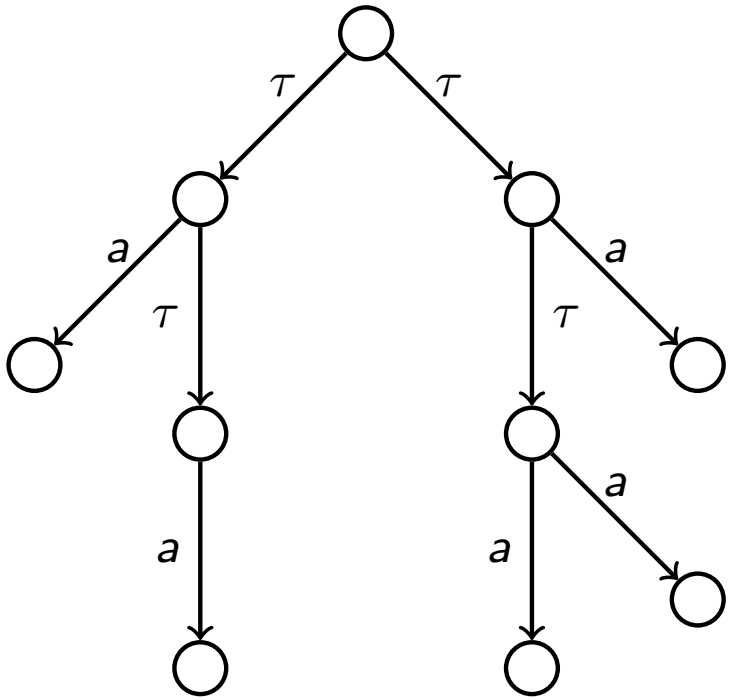
$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid |a| \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\bigcirc \phi | \Diamond \phi | \Box \phi | \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi \ \&\ \psi \mid \phi \ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{X}\ \phi \mid \mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$



Lowe's *a* and *available a*

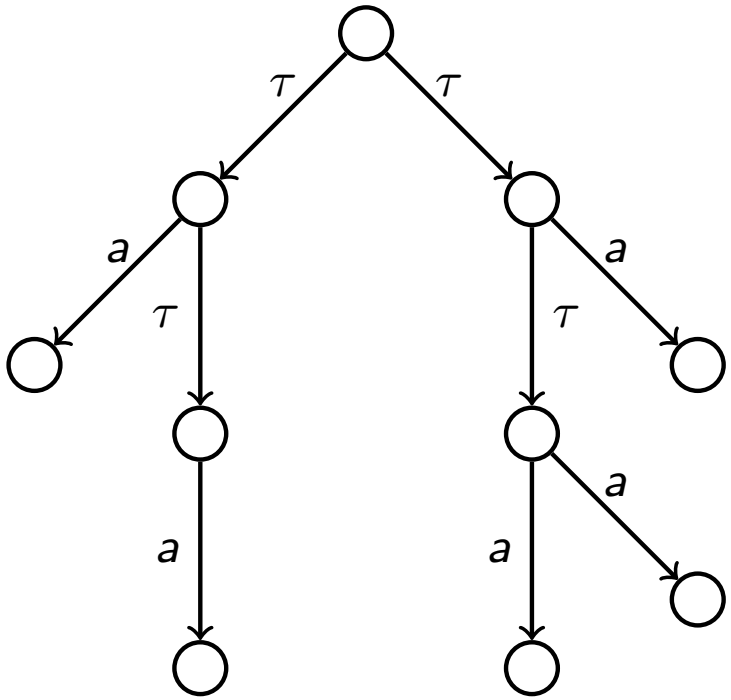


Lowe's *a*

The next visible event is guaranteed to be an *a*

$a \rightarrow$ [tau] U [a]

Lowe's *a* and *available a*

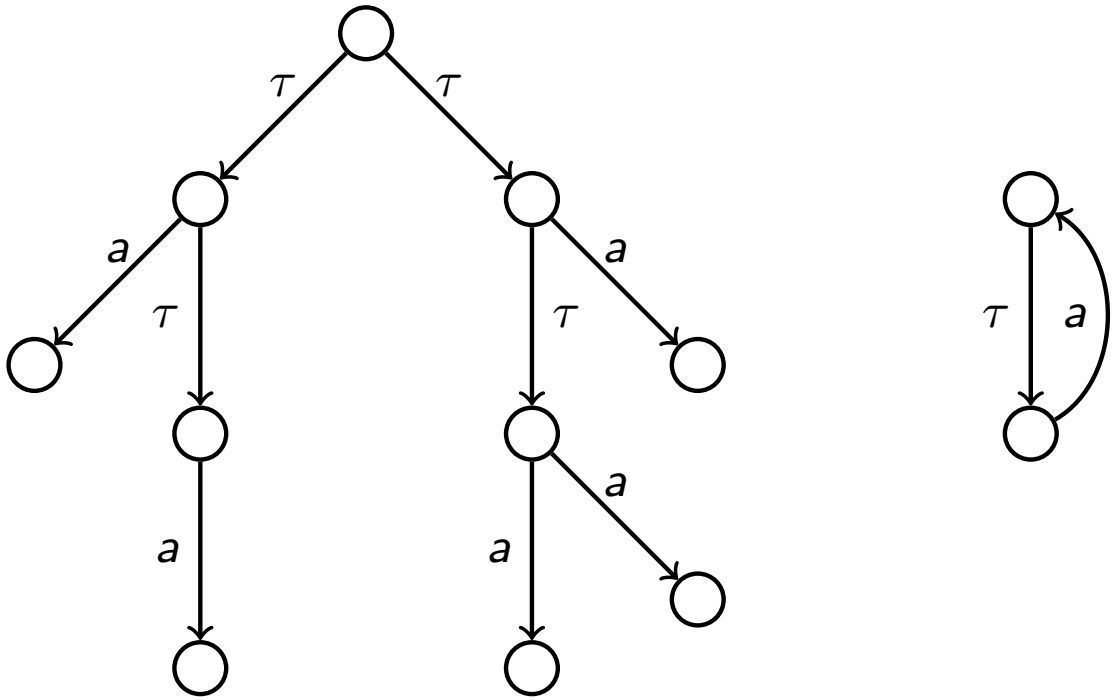


Lowe's *a*

The next visible event is guaranteed to be an *a*

$a \rightarrow$ [tau] U [a]

Lowe's *a* and *available a*

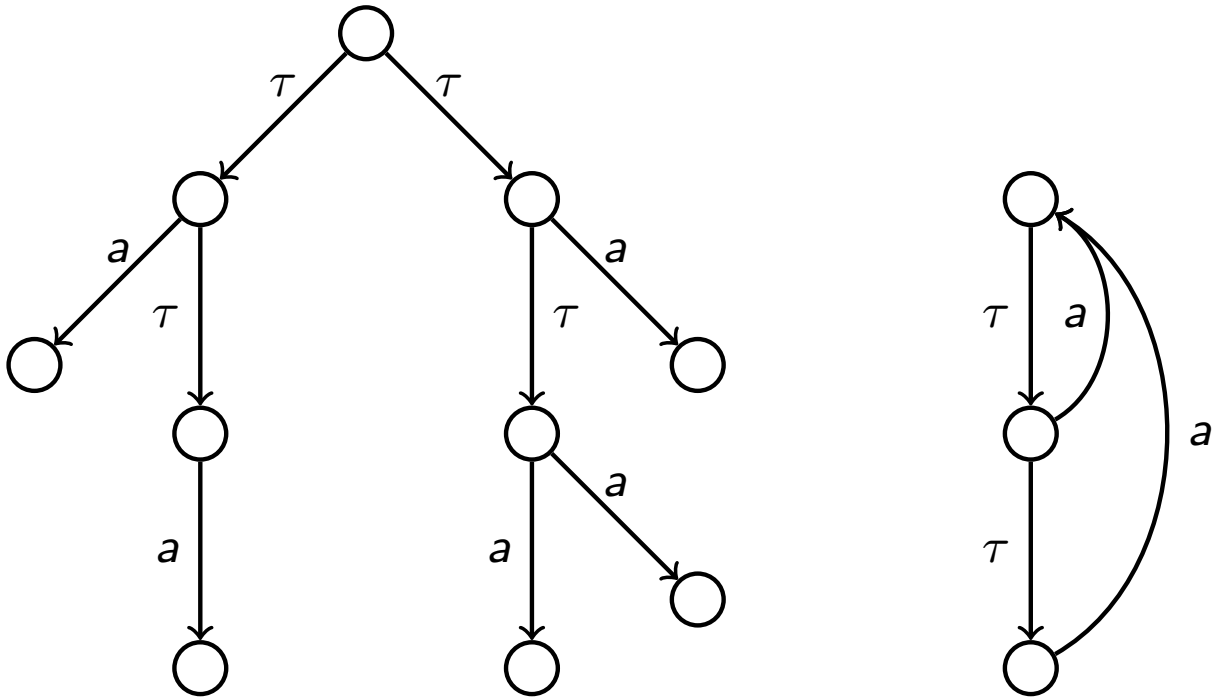


Lowe's *a*

The next visible event is guaranteed to be an *a*

$a \rightarrow$ [tau] U [a]

Lowe's *a* and *available a*

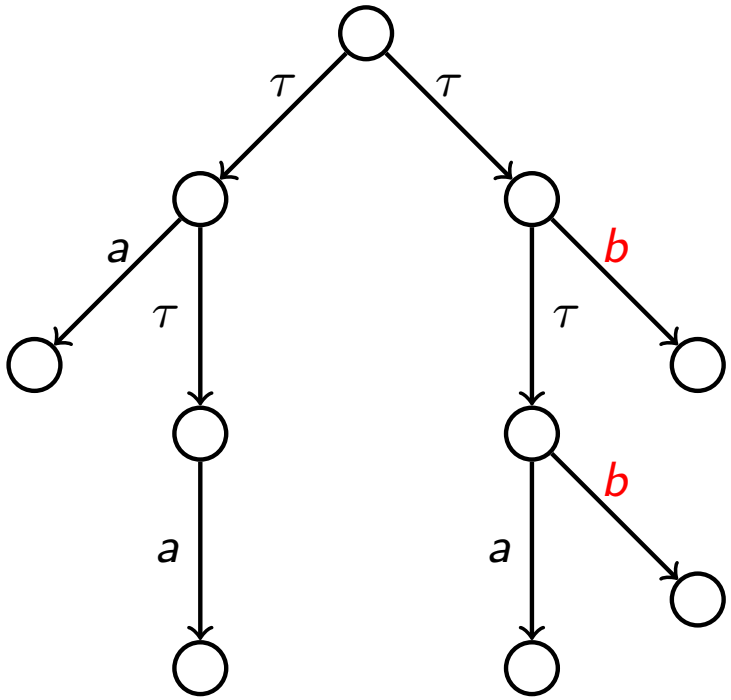


Lowe's *a*

The next visible event is guaranteed to be an *a*

$a \rightarrow$ [tau] U [a]

Lowe's *a* and *available a*

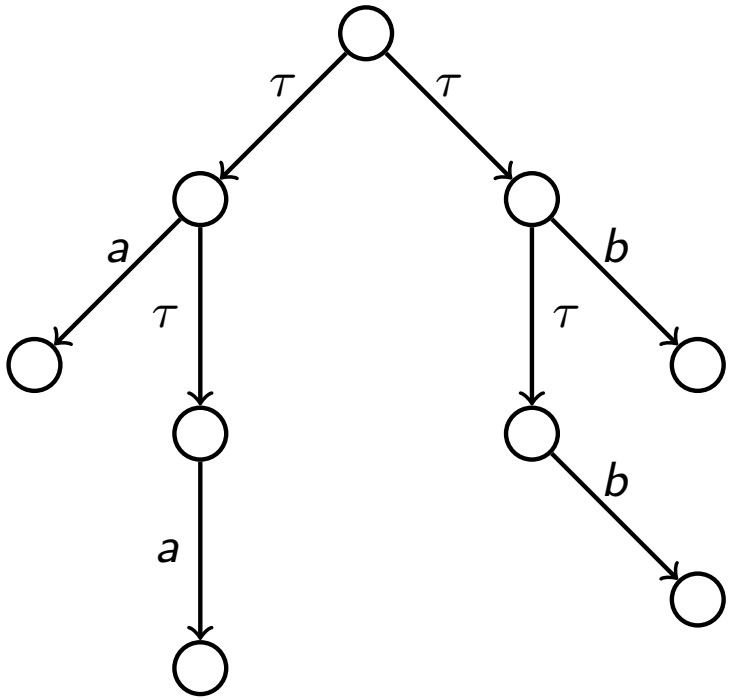


Lowe's *available a*

Whenever the process stabilises before performing its first visible event, an *a* is enabled

available a → [tau] U ((e(tau) & not [tau]) or (e(a) & not e(tau)))

Lowe's *a* and *available a*



Lowe's *available a*

Whenever the process stabilises before performing its first visible event, an *a* is enabled

available a → [tau] U ((e(tau) & not [tau]) or (e(a) & not e(tau)))

LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid a \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\Diamond \phi \mid \Box \phi \mid \bigcirc \phi \mid \psi \mathcal{U} \phi \mid \phi \mathcal{R} \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi\ \&\ \psi \mid \phi\ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi => \psi \mid$$
$$\mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \mathsf{X}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$

LTL for CSP

Lowe's Temporal Logic

$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid a \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\Diamond \phi \mid \Box \phi \mid \bigcirc \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi,\psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi\ \&\ \psi \mid \phi\ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \mathsf{X}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$

a → [tau] U [a]
available a → [tau] U ((e(tau) & not [tau]) or (e(a) & not e(tau)))

LTL for CSP

Lowe's Temporal Logic

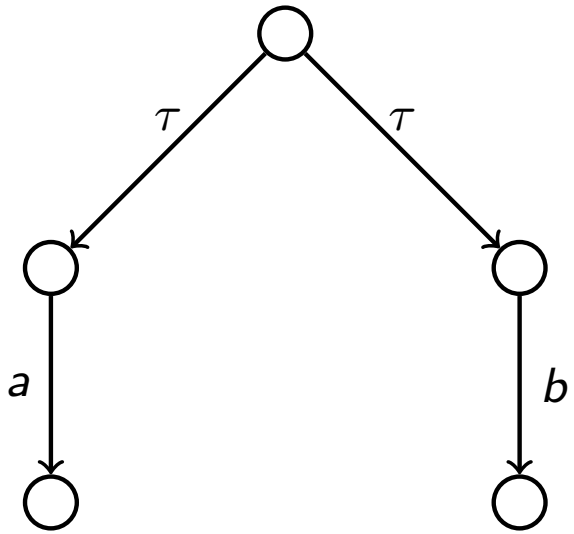
$$\phi, \psi ::= \mathit{true} \mid \mathit{false} \mid a \mid \mathit{available}\ a \mid \mathit{deadlocked} \mid$$
$$\phi \wedge \psi \mid \phi \vee \psi \mid \neg \phi \mid \phi \Rightarrow \psi \mid$$
$$\Diamond \phi \mid \Box \phi \mid \bigcirc \phi \mid \psi \,\mathcal{U}\, \phi \mid \phi \,\mathcal{R}\, \psi \qquad \text{where } a \in \Sigma$$

ProB's Temporal Logic

$$\phi, \psi ::= \mathsf{true} \mid \mathsf{false} \mid [a] \mid e(a) \mid \mathsf{deadlock} \mid$$
$$\phi\ \&\ \psi \mid \phi\ \mathsf{or}\ \psi \mid \mathsf{not}\ \phi \mid \phi \Rightarrow \psi \mid$$
$$\mathsf{F}\ \phi \mid \mathsf{G}\ \phi \mid \mathsf{X}\ \phi \mid \phi\ \mathsf{U}\ \psi \mid \psi\ \mathsf{R}\ \phi \qquad \text{where } a \in \Sigma \cup \{\tau\}$$

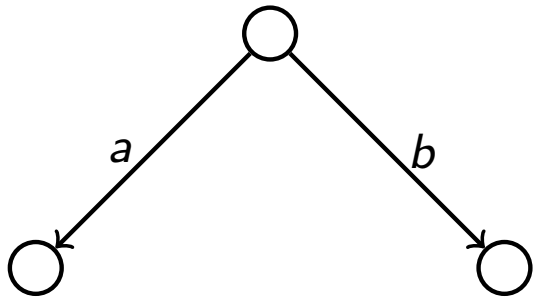
a	$\rightarrow$ [tau] U [a]
available a	$\rightarrow$ [tau] U ((e(tau) & not [tau]) or (e(a) & not e(tau)))
deadlocked	$\rightarrow$ [tau] U deadlock
$\bigcirc\phi$	$\rightarrow$ [tau] U (deadlock or (not [tau] & X ϕ))

Finite Traces vs. Stable Failures



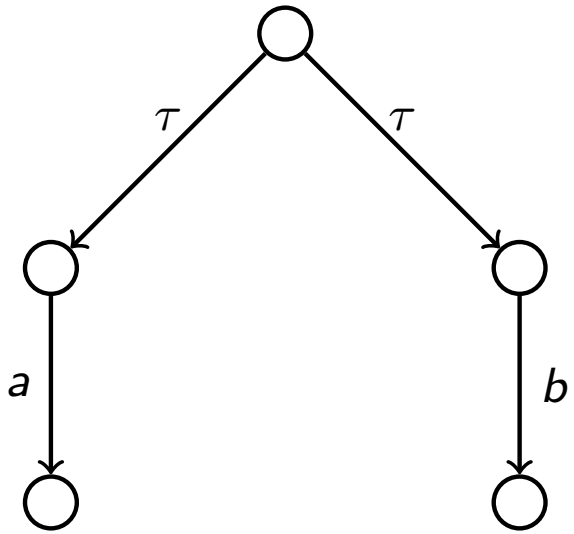
a $\rightarrow$ *Stop* $\sqcap$ *b* $\rightarrow$ *Stop*

$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



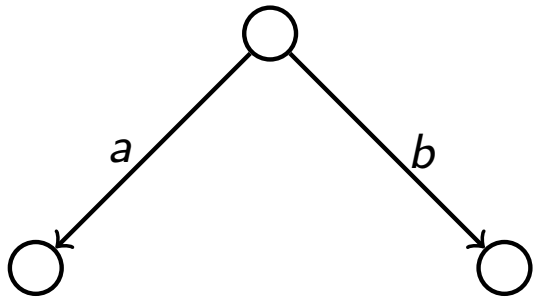
a $\rightarrow$ *Stop* $\Box$ *b* $\rightarrow$ *Stop*

Finite Traces vs. Stable Failures



$a \to Stop \sqcap b \to Stop$

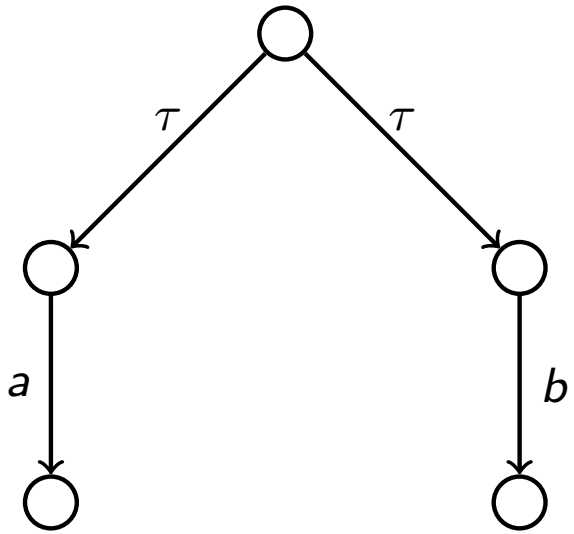
$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



$a \to Stop \;\Box\; b \to Stop$

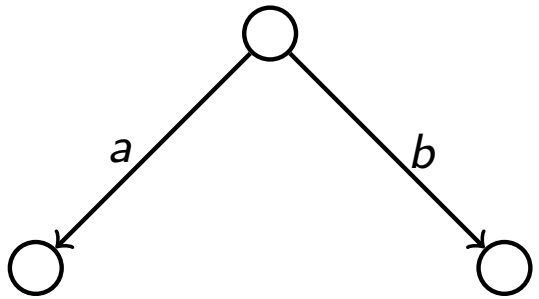
$\langle\rangle, \langle a\rangle, \langle b\rangle$

Finite Traces vs. Stable Failures



a $\rightarrow$ *Stop* $\sqcap$ *b* $\rightarrow$ *Stop*

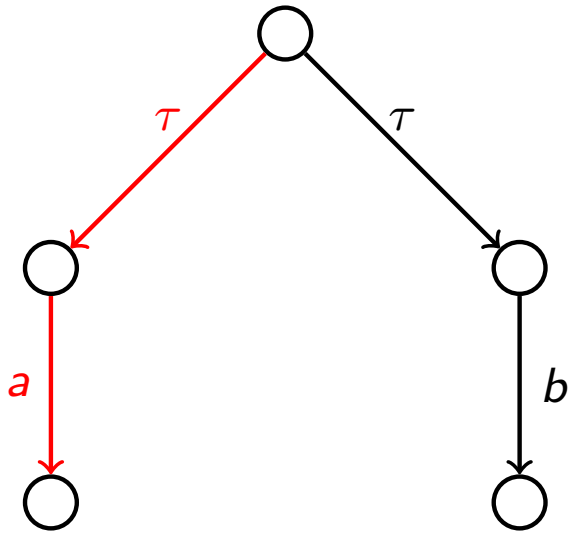
$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



a $\rightarrow$ *Stop* $\Box$ *b* $\rightarrow$ *Stop*

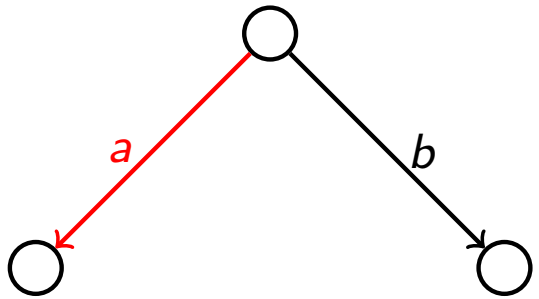
$\langle\rangle, \langle a\rangle, \langle b\rangle$
$(\langle a\rangle, \Sigma), (\langle b\rangle, \Sigma)$

Finite Traces vs. Stable Failures



$a \rightarrow Stop \sqcap b \rightarrow Stop$

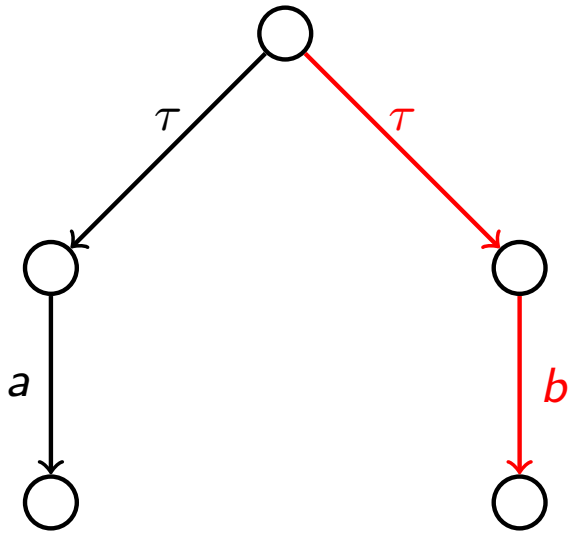
$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



$a \rightarrow Stop \;\Box\; b \rightarrow Stop$

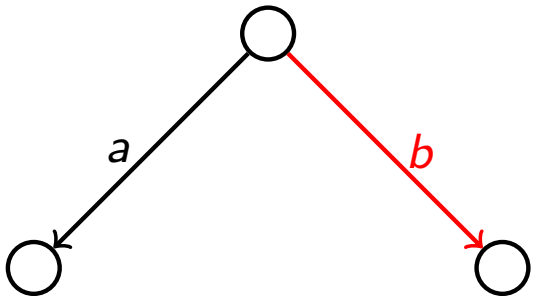
$\langle\rangle, \langle a\rangle, \langle b\rangle$
$(\langle a\rangle, \Sigma), (\langle b\rangle, \Sigma)$

Finite Traces vs. Stable Failures



$a \to Stop \sqcap b \to Stop$

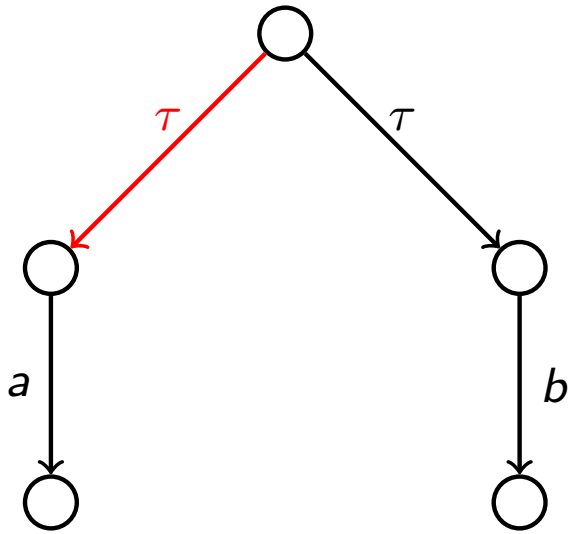
$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



$a \to Stop \;\Box\; b \to Stop$

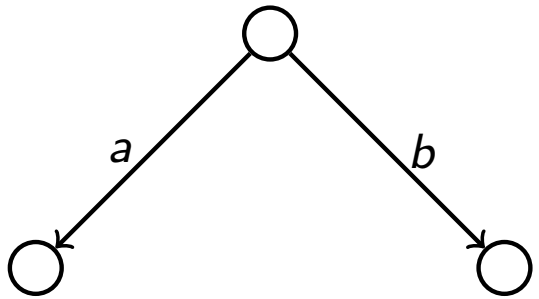
$\langle\rangle, \langle a\rangle, \langle b\rangle$
$(\langle a\rangle, \Sigma), (\langle b\rangle, \Sigma)$

Finite Traces vs. Stable Failures



$a \to Stop \sqcap b \to Stop$

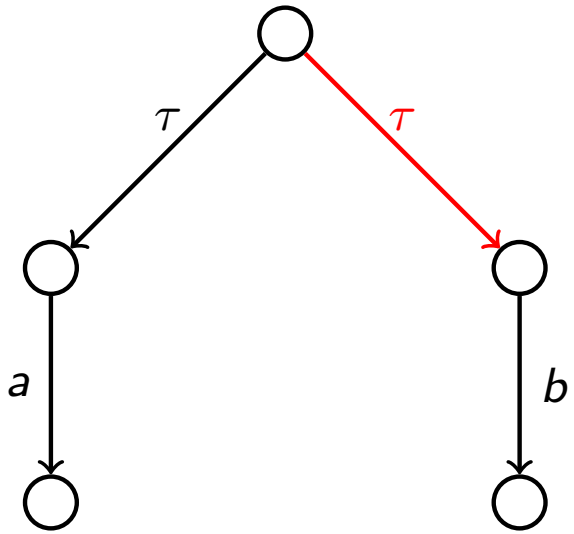
$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



$a \to Stop \;\Box\; b \to Stop$

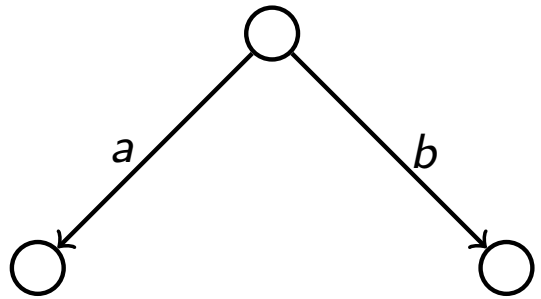
$\langle\rangle, \langle a\rangle, \langle b\rangle$
$(\langle a\rangle, \Sigma), (\langle b\rangle, \Sigma)$
$(\langle\rangle, \{b\}), (\langle\rangle, \{a\})$

Finite Traces vs. Stable Failures



a $\rightarrow$ *Stop* $\sqcap$ $b \rightarrow$ *Stop*

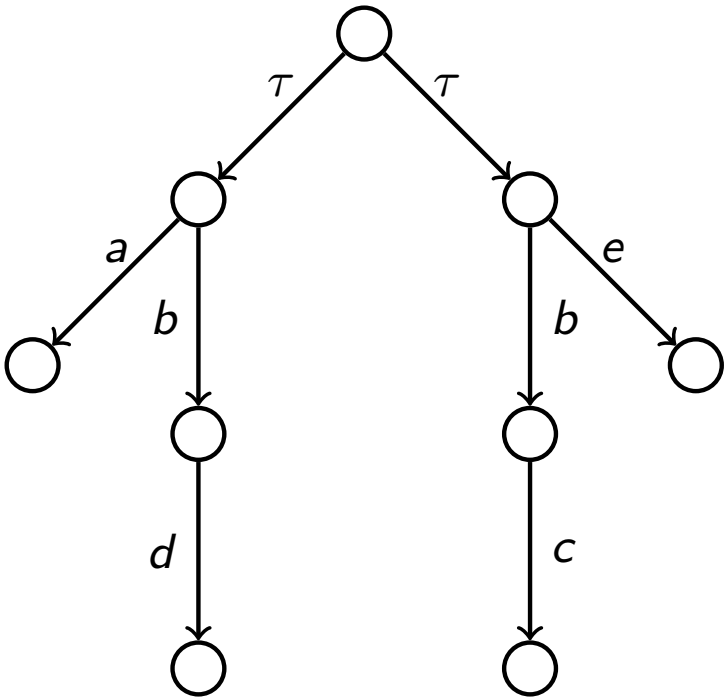
$=_{\mathcal{T}}$
$\neq_{\mathcal{F}}$
$\sqsubseteq_{\mathcal{F}}$



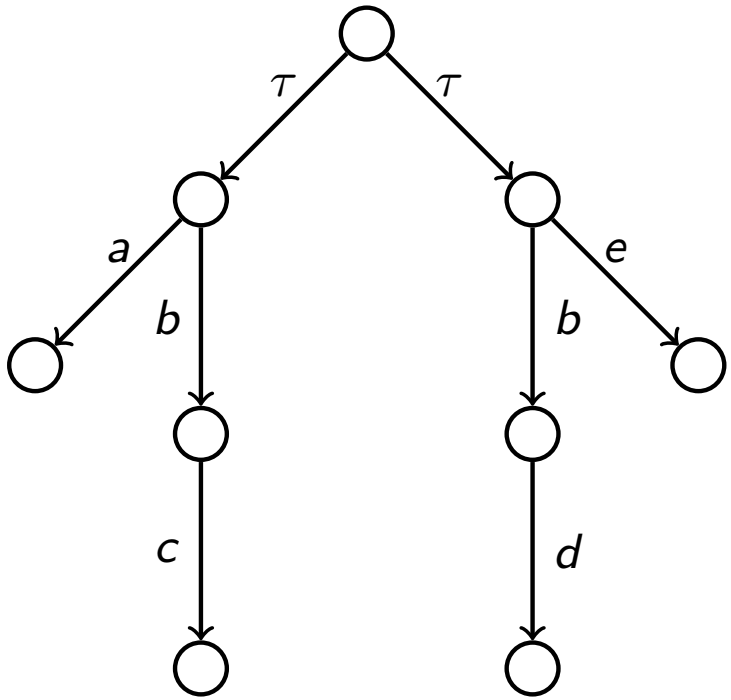
a $\rightarrow$ *Stop* $\Box$ $b \rightarrow$ *Stop*

$\langle\rangle, \langle a\rangle, \langle b\rangle$
$(\langle a\rangle, \Sigma), (\langle b\rangle, \Sigma)$
$(\langle\rangle, \{b\}), (\langle\rangle, \{a\})$

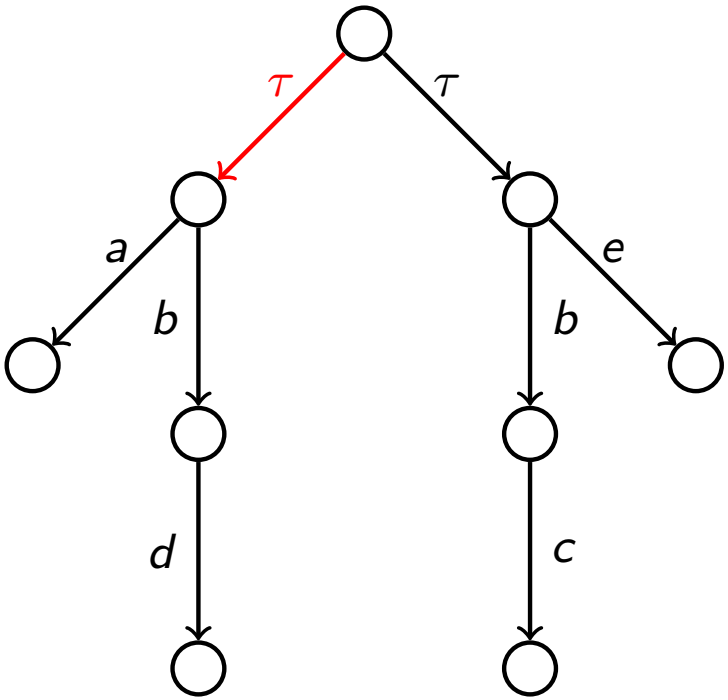
Stable Failures vs. Refusal Traces



$$=_{\mathcal{F}}$$
$$\neq_{\mathcal{RT}}$$
$$\not\sqsubseteq_{\mathcal{RT}}$$
$$\not\sqsupseteq_{\mathcal{RT}}$$



Stable Failures vs. Refusal Traces

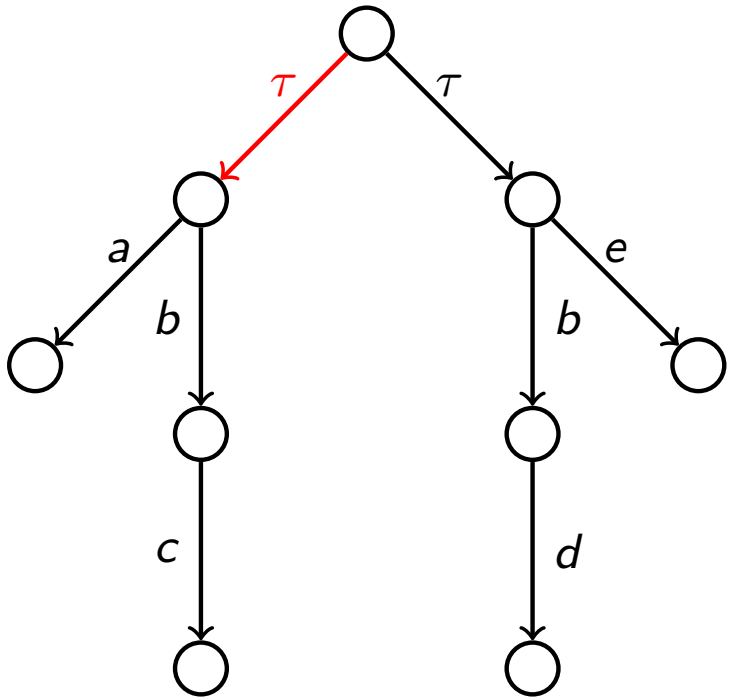


$=_{\mathcal{F}}$

$\neq_{\mathcal{RT}}$

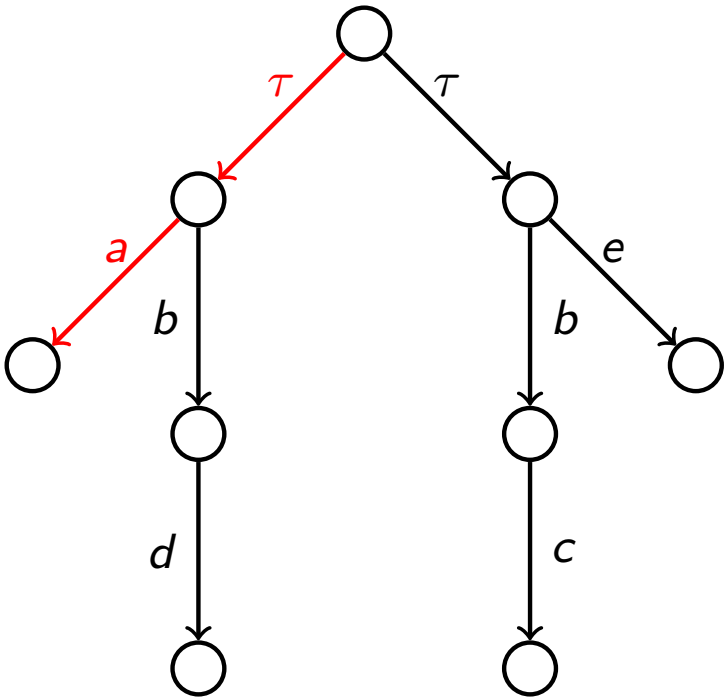
$\not\sqsubseteq_{\mathcal{RT}}$

$\not\sqsupseteq_{\mathcal{RT}}$



$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

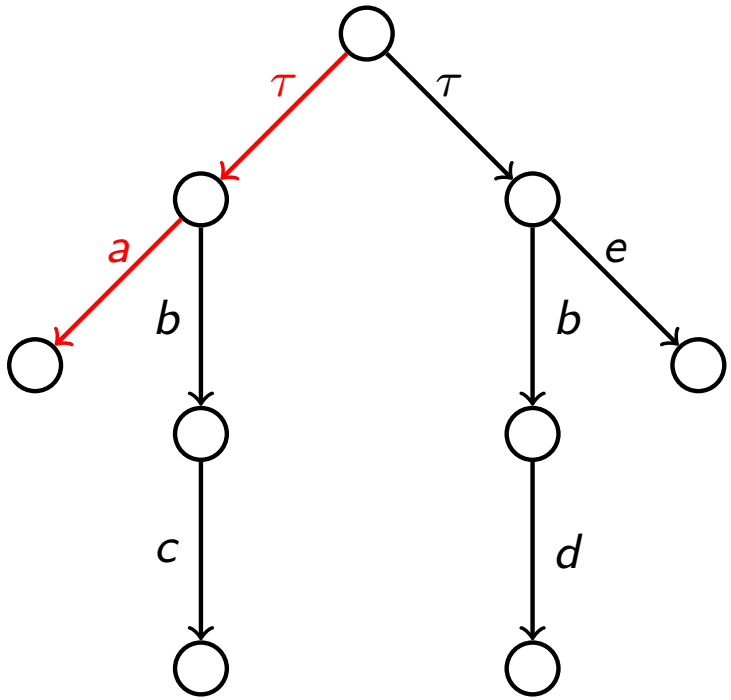


$=_{\mathcal{F}}$

$\neq_{\mathcal{RT}}$

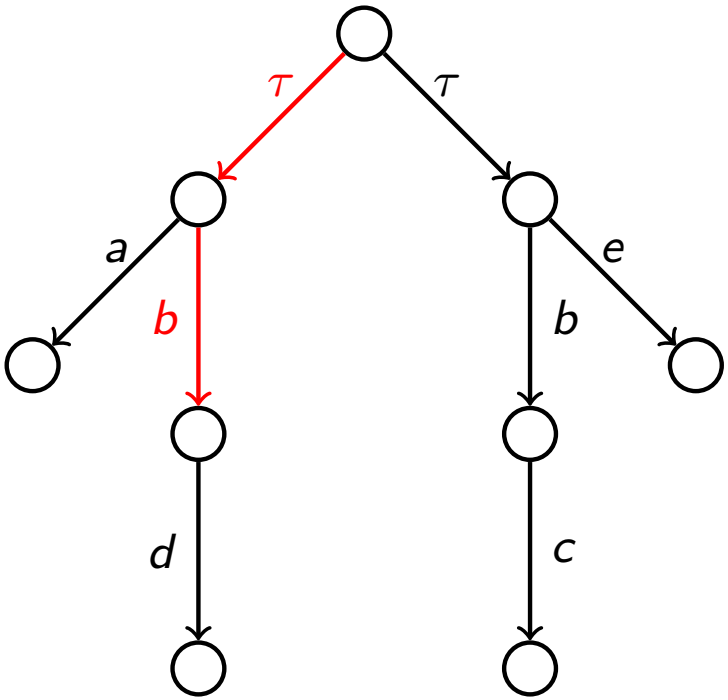
$\not\sqsubseteq_{\mathcal{RT}}$

$\not\sqsupseteq_{\mathcal{RT}}$

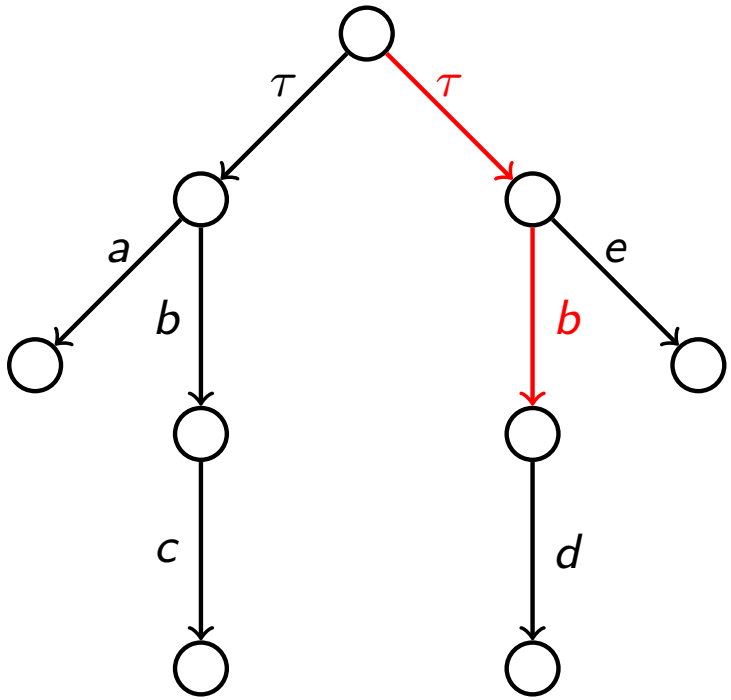


$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

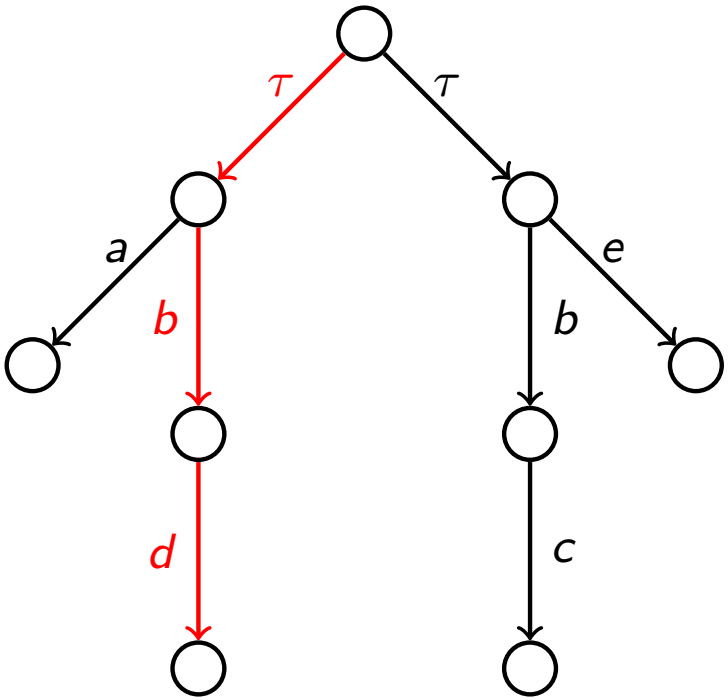


$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$

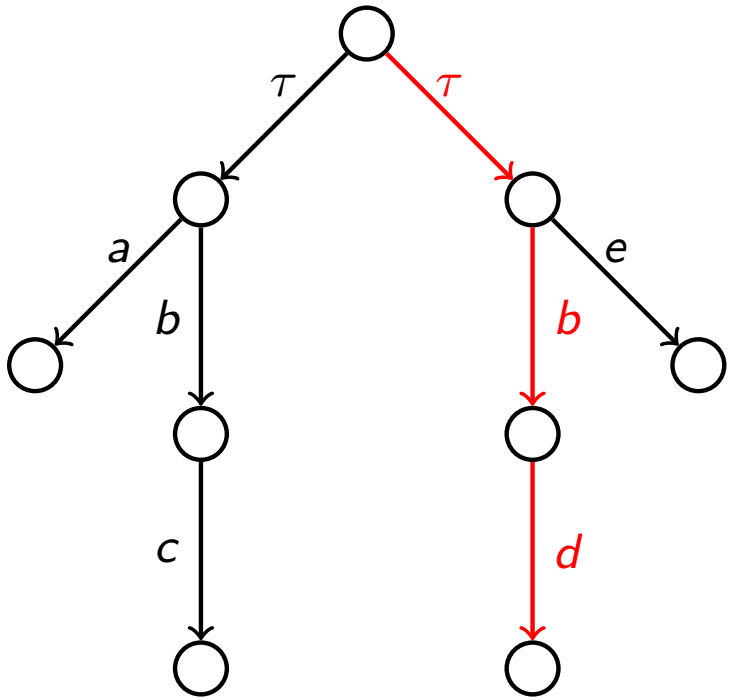


$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

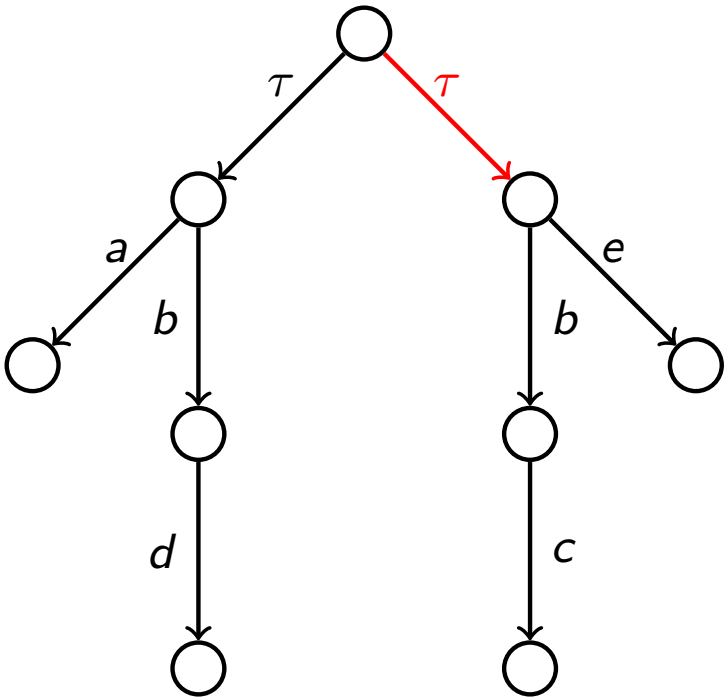


$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$

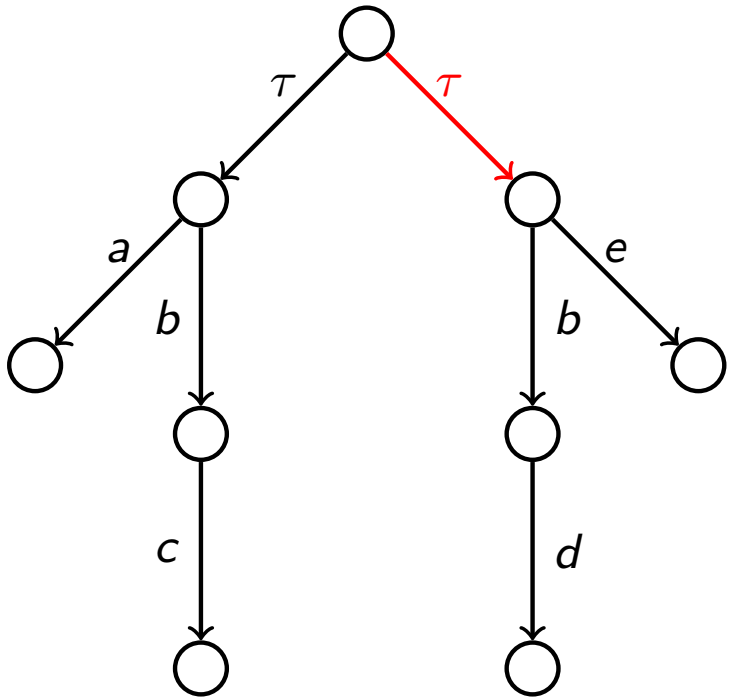


$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

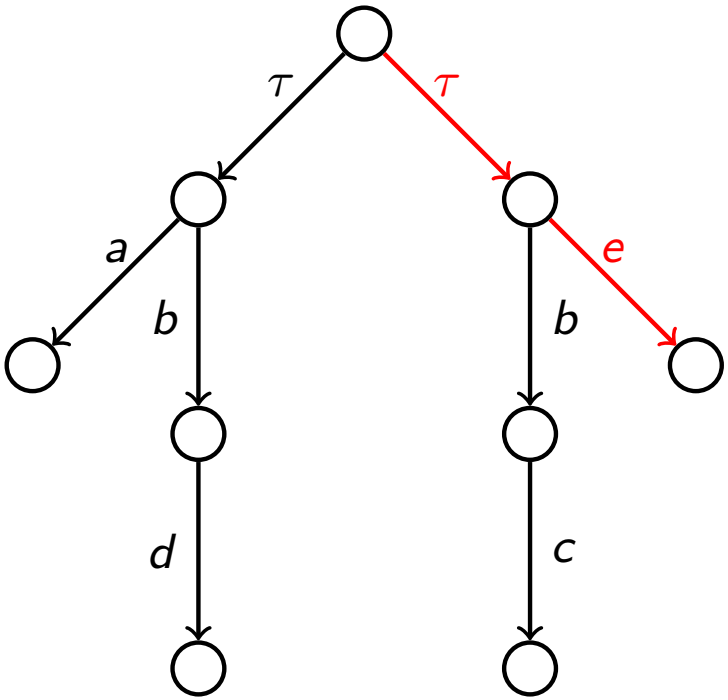


$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$

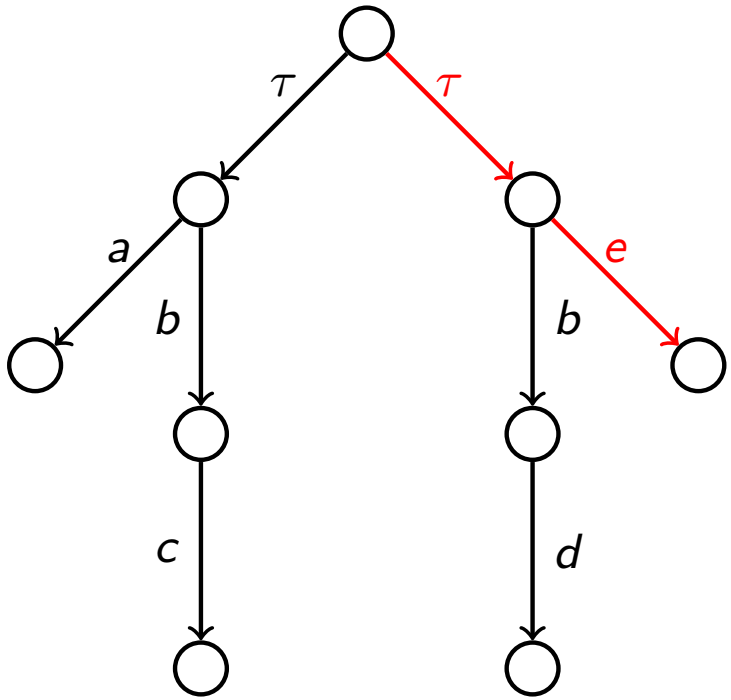


$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$
$(\langle\rangle, \{a, c, d\})$, $(\langle e\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, d, e\})$, $(\langle b, c\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

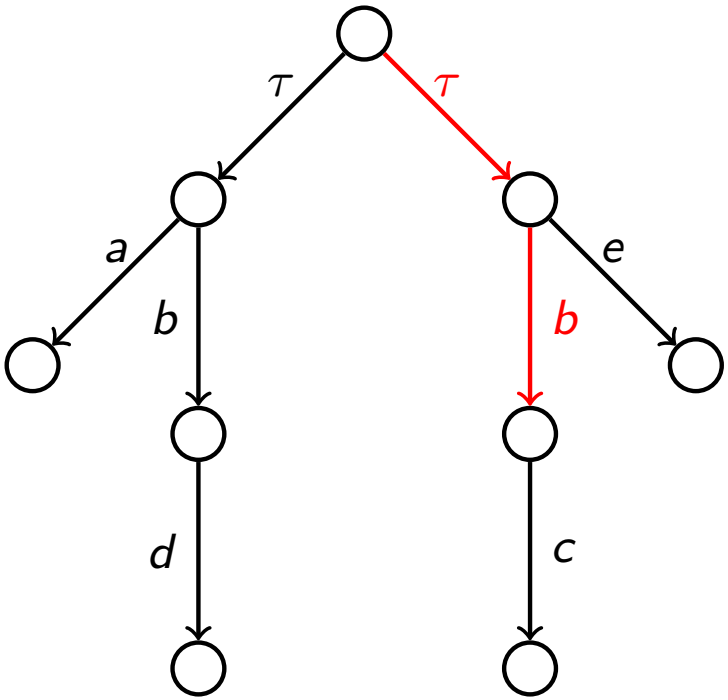


$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$

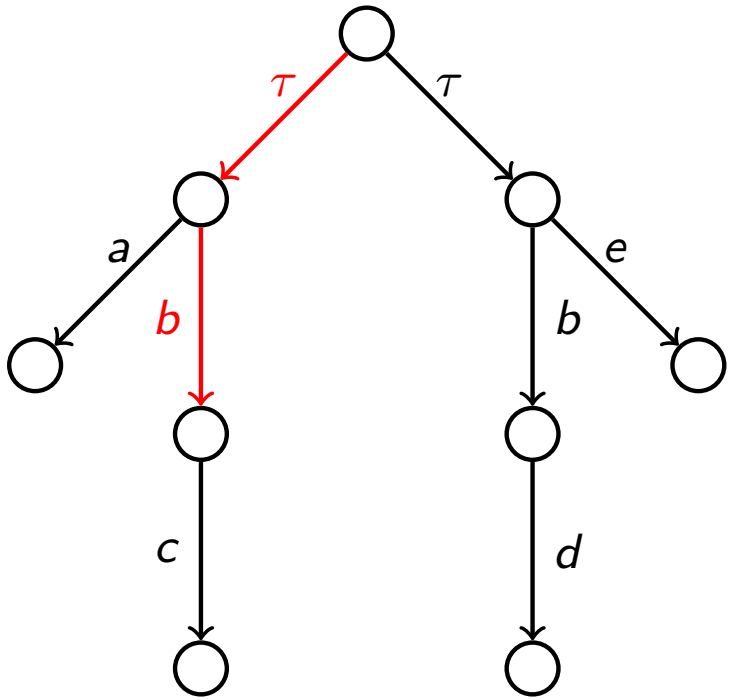


$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$
$(\langle\rangle, \{a, c, d\})$, $(\langle e\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, d, e\})$, $(\langle b, c\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

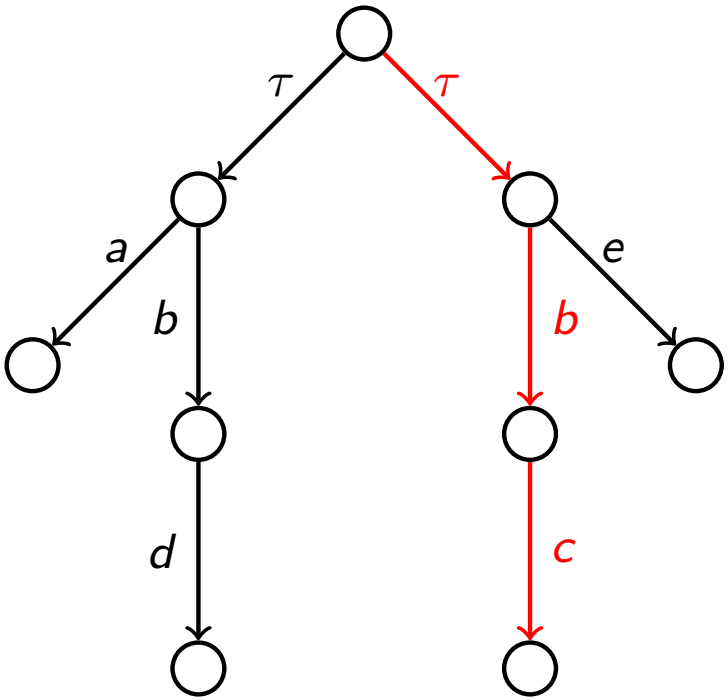


$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$

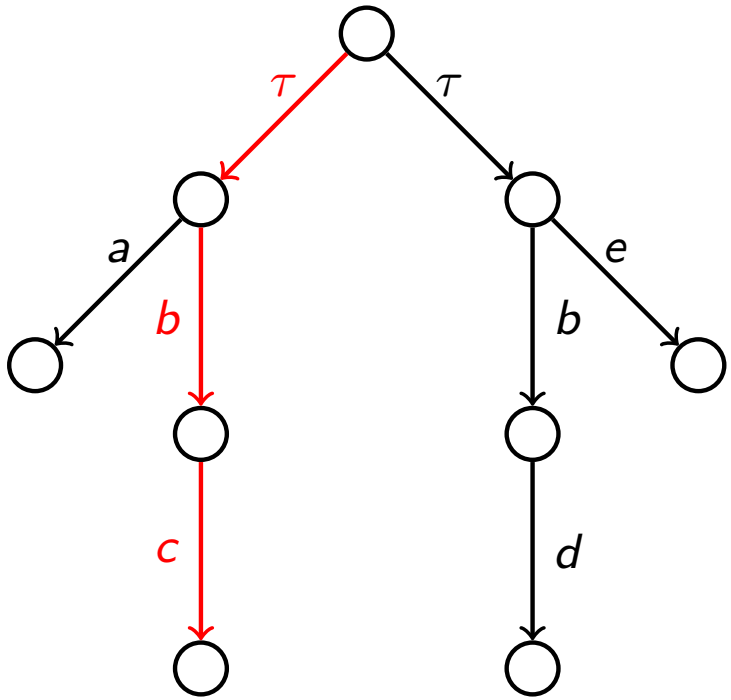


$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$
$(\langle\rangle, \{a, c, d\})$, $(\langle e\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, d, e\})$, $(\langle b, c\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

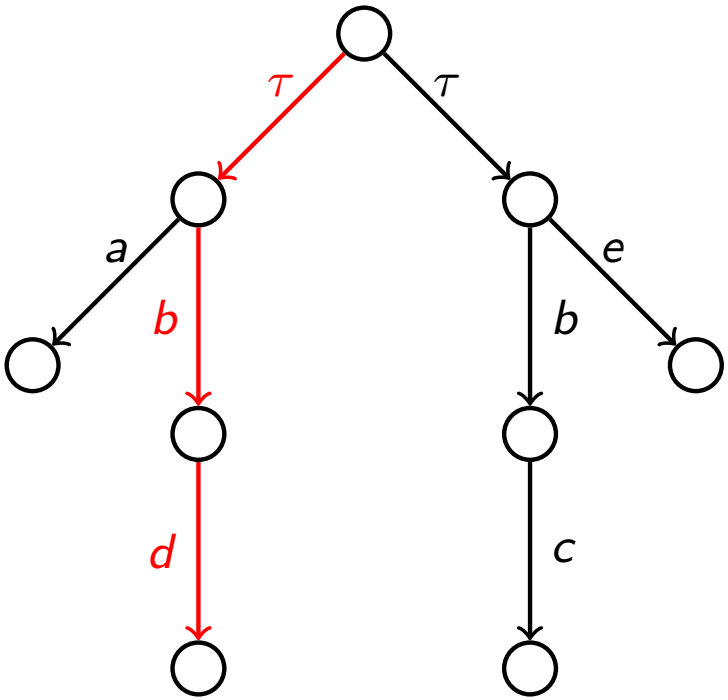


$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$



$(\langle\rangle, \{c, d, e\})$, $(\langle a\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, c, e\})$, $(\langle b, d\rangle, \Sigma)$
$(\langle\rangle, \{a, c, d\})$, $(\langle e\rangle, \Sigma)$, $(\langle b\rangle, \{a, b, d, e\})$, $(\langle b, c\rangle, \Sigma)$

Stable Failures vs. Refusal Traces

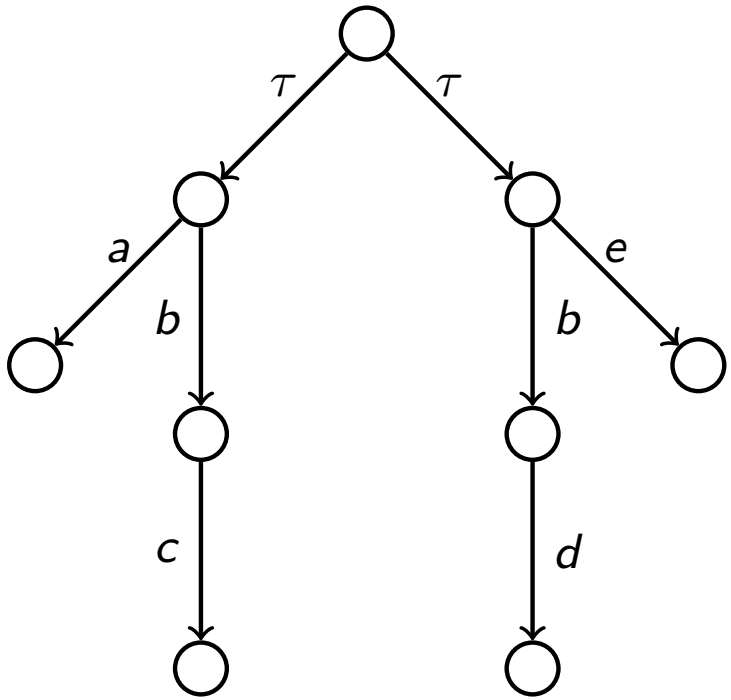


$=_{\mathcal{F}}$

$\neq_{\mathcal{RT}}$

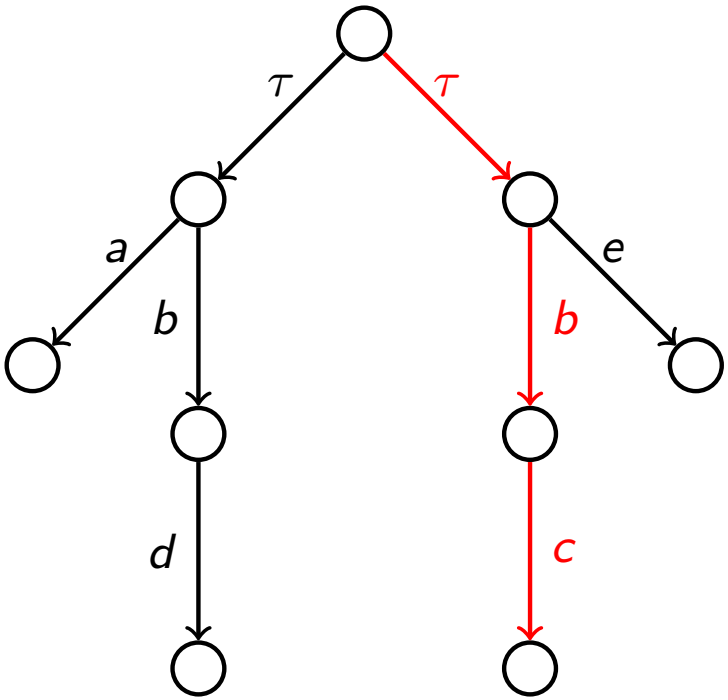
$\not\sqsubseteq_{\mathcal{RT}}$

$\not\sqsupseteq_{\mathcal{RT}}$



$\langle \{c, d, e\}, b, \{a, b, c, e\}, d, \Sigma \rangle, \langle \{a, c, d\}, b, \{a, b, d, e\}, c, \Sigma \rangle$

Stable Failures vs. Refusal Traces

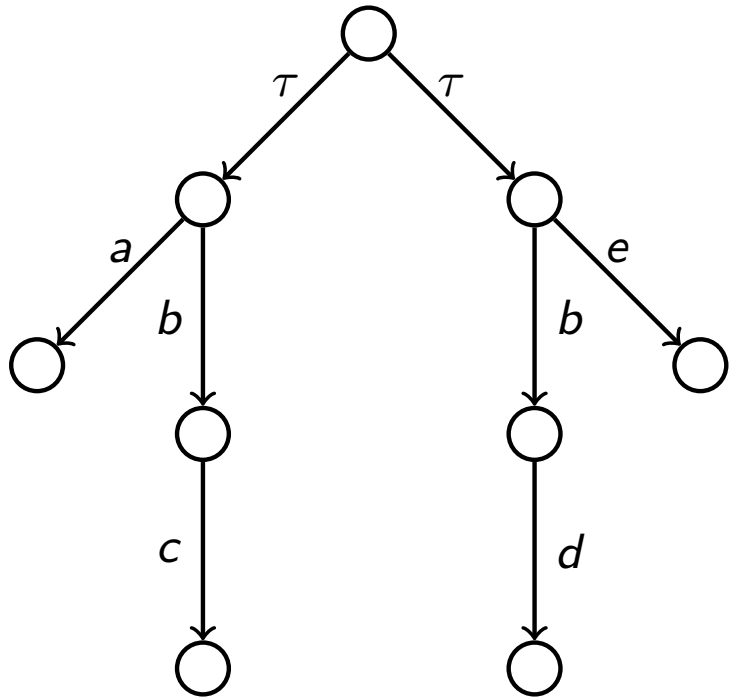


$=_{\mathcal{F}}$

$\neq_{\mathcal{RT}}$

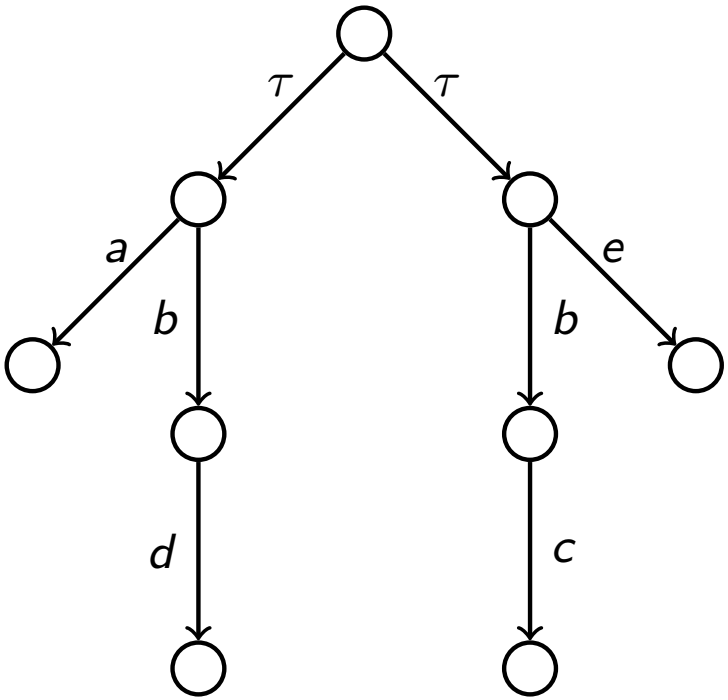
$\not\sqsubseteq_{\mathcal{RT}}$

$\not\sqsupseteq_{\mathcal{RT}}$



$\langle \{c, d, e\}, b, \{a, b, c, e\}, d, \Sigma \rangle, \langle \{a, c, d\}, b, \{a, b, d, e\}, c, \Sigma \rangle$

Stable Failures vs. Refusal Traces

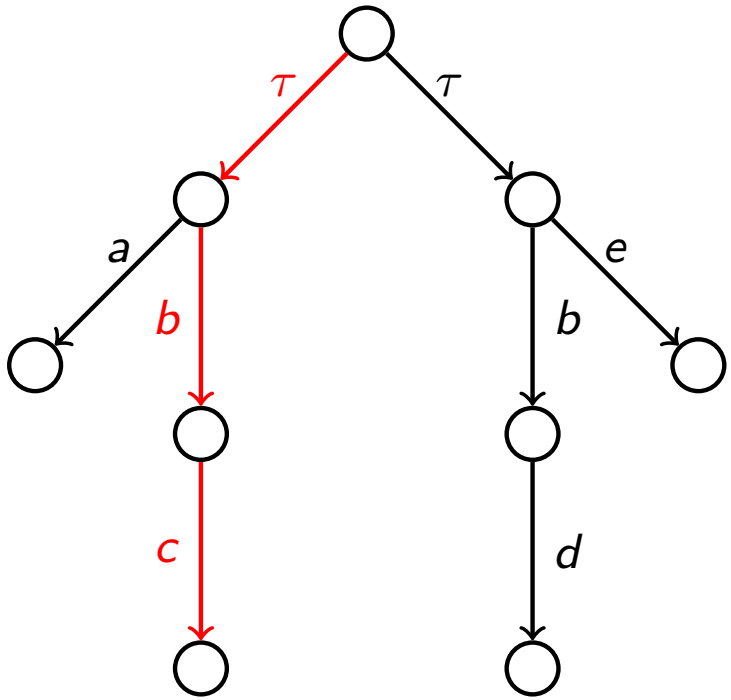


$=_{\mathcal{F}}$

$\neq_{\mathcal{RT}}$

$\not\sqsubseteq_{\mathcal{RT}}$

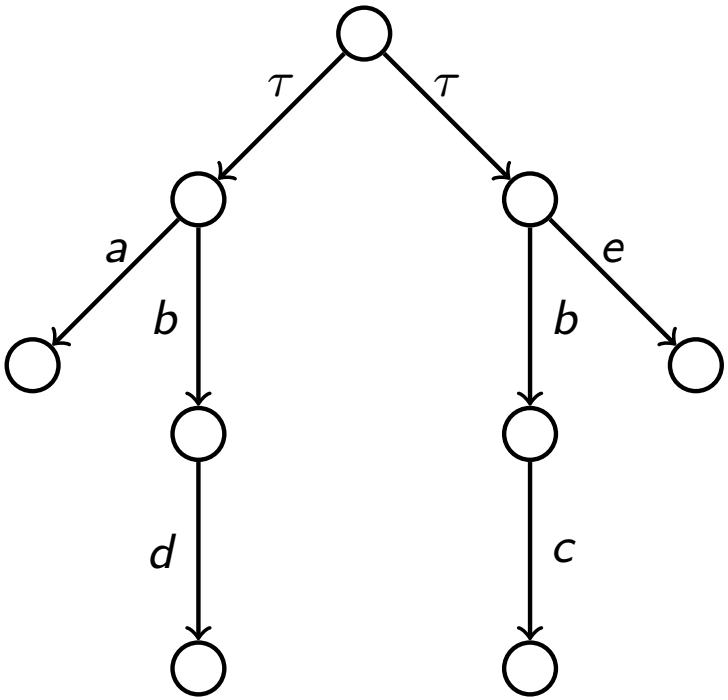
$\not\sqsupseteq_{\mathcal{RT}}$



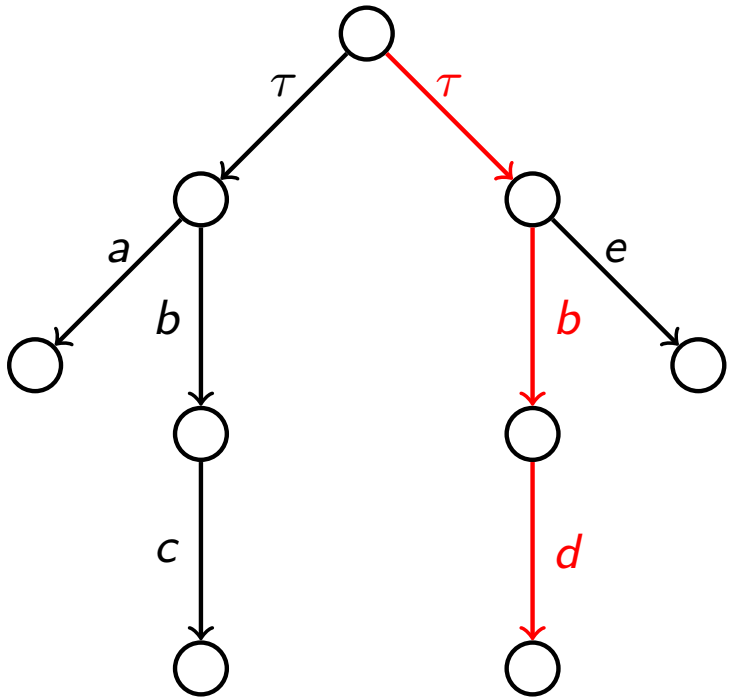
$\langle \{c, d, e\}, b, \{a, b, c, e\}, d, \Sigma \rangle, \langle \{a, c, d\}, b, \{a, b, d, e\}, c, \Sigma \rangle$

$\langle \{c, d, e\}, b, \{a, b, d, e\}, c, \Sigma \rangle, \langle \{a, c, d\}, b, \{a, b, c, e\}, d, \Sigma \rangle$

Stable Failures vs. Refusal Traces



$=_{\mathcal{F}}$
$\neq_{\mathcal{RT}}$
$\not\sqsubseteq_{\mathcal{RT}}$
$\not\sqsupseteq_{\mathcal{RT}}$



$\langle \{c, d, e\}, b, \{a, b, c, e\}, d, \Sigma \rangle, \langle \{a, c, d\}, b, \{a, b, d, e\}, c, \Sigma \rangle$
$\langle \{c, d, e\}, b, \{a, b, d, e\}, c, \Sigma \rangle, \langle \{a, c, d\}, b, \{a, b, c, e\}, d, \Sigma \rangle$

Model Checking CSP

Refinement Checking

$$\frac{S \sqsubseteq_{\mathcal{M}} P \qquad P \sqsubseteq_{\mathcal{M}} Q}{S \sqsubseteq_{\mathcal{M}} Q}$$

Tool Support: FDR or PAT

LTL Model Checking

$$\frac{P \models \phi \qquad P \sqsubseteq_{\mathcal{RT}} Q}{Q \models \phi}$$

Tool Support: ProB and FDR

Fairness

Weak Event Fairness

$$WEF = \bigwedge_{x \in \Sigma} (\Diamond \Box \, enabled\, x \Rightarrow \Box \Diamond x)$$

A constantly often enabled event shall occur infinitely often

Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \, enabled\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often

Fairness

Weak Event Fairness

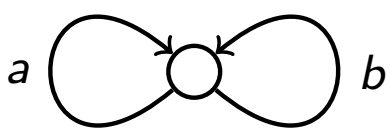
$$WEF = \bigwedge_{x \in \Sigma} (\Diamond \Box \, enabled\, x \Rightarrow \Box \Diamond x)$$

A constantly often enabled event shall occur infinitely often

Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \, enabled\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often



Fairness

Weak Event Fairness

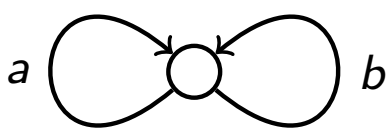
$$WEF = \bigwedge_{x \in \Sigma} (\Diamond \Box \, enabled\, x \Rightarrow \Box \Diamond x)$$

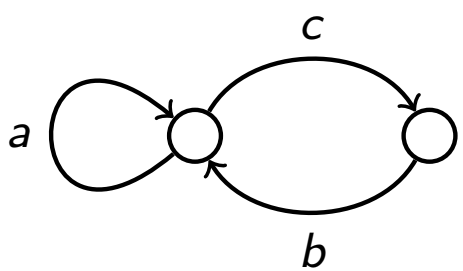
A constantly often enabled event shall occur infinitely often

Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \, enabled\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often





Fairness

Weak Event Fairness

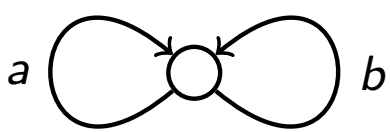
$$WEF = \bigwedge_{x \in \Sigma} (\Diamond \Box \, enabled\, x \Rightarrow \Box \Diamond x)$$

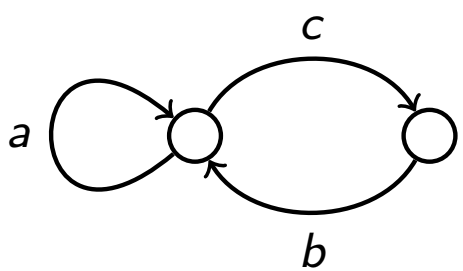
A constantly often enabled event shall occur infinitely often

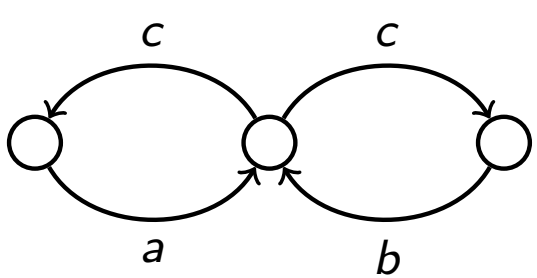
Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \, enabled\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often







Fairness

Weak Event Fairness

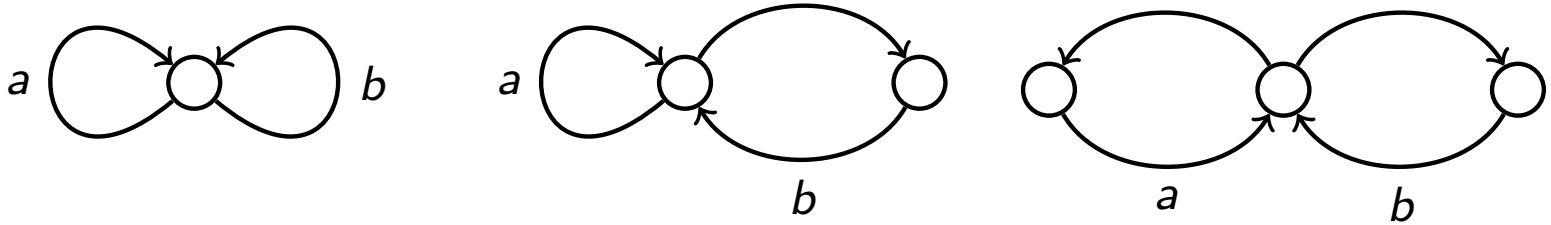
$$WEF = \bigwedge_{x \in \Sigma} (\Diamond \Box \, enabled\, x \Rightarrow \Box \Diamond x)$$

A constantly often enabled event shall occur infinitely often

Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \, enabled\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often



Fairness

Weak Event Fairness

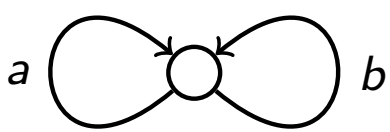
$$WEF = \bigwedge_{x \in \Sigma} (\Diamond \Box \, available\, x \Rightarrow \Box \Diamond x)$$

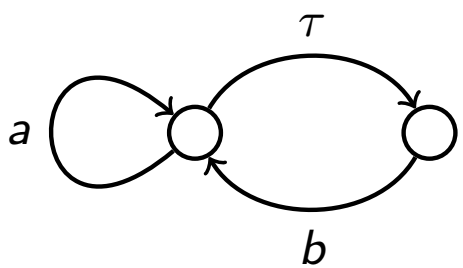
A constantly often enabled event shall occur infinitely often

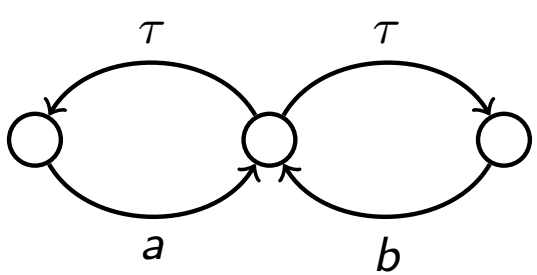
Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \, available\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often







Model Checking CSP

Refinement Checking

$$\frac{S \sqsubseteq_{\mathcal{M}} P \qquad P \sqsubseteq_{\mathcal{M}} Q}{S \sqsubseteq_{\mathcal{M}} Q}$$

Tool Support: FDR or PAT

LTL Model Checking

$$\frac{P \models \phi \qquad P \sqsubseteq_{\mathcal{RT}} Q}{Q \models \phi}$$

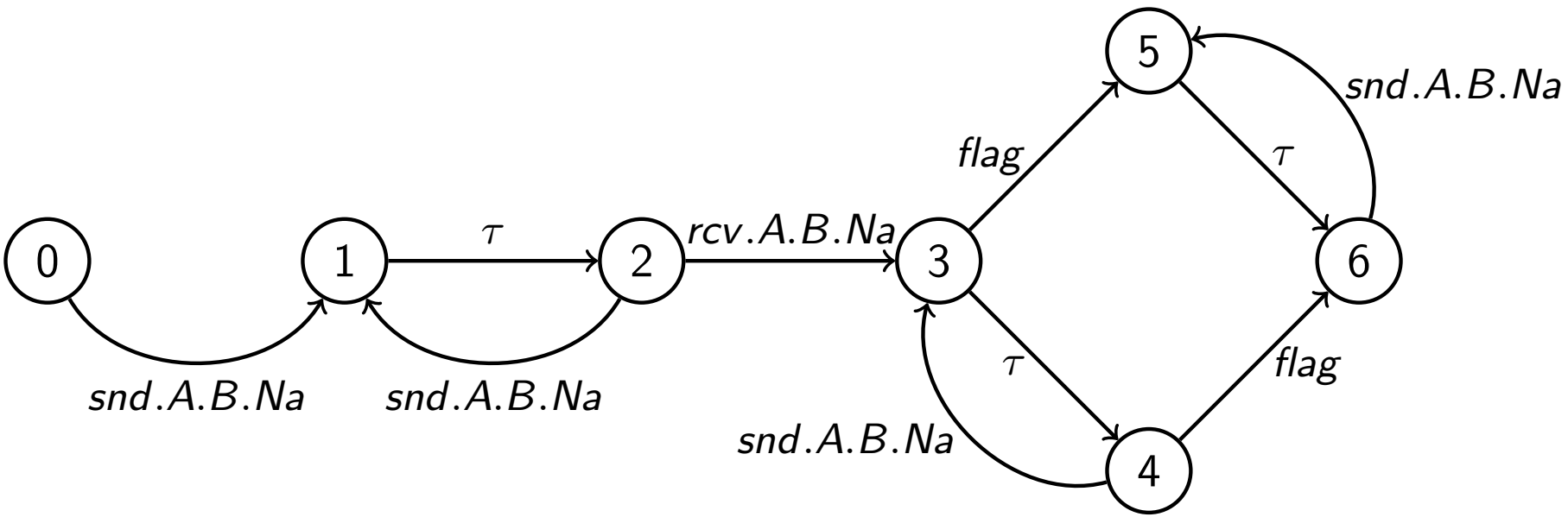
Tool Support: ProB and FDR

Application to Fair Exchange Protocols

$$SND_2 = snd.A.B.Na \rightarrow SND_2$$
$$RCV_2 = rcv.A.B.Na \rightarrow flag \rightarrow Stop$$
$$SYS_2 = (SND_2 \;|||\; RCV_2) \underset{\{|snd,rcv|\}}{\|} Spy^{L\dagger}$$

Application to Fair Exchange Protocols

$$SND_2 = snd.A.B.Na \rightarrow SND_2$$
$$RCV_2 = rcv.A.B.Na \rightarrow flag \rightarrow Stop$$
$$SYS_2 = (SND_2 \;|||\; RCV_2) \underset{\{|snd,rcv|\}}{\|} Spy^{L\dagger}$$



Conclusion

Refinement Checking

$$\frac{S \sqsubseteq_{\mathcal{M}} P \qquad P \sqsubseteq_{\mathcal{M}} Q}{S \sqsubseteq_{\mathcal{M}} Q}$$

Tool Support: FDR or PAT

LTL Model Checking

$$\frac{P \models \phi \qquad P \sqsubseteq_{\mathcal{RT}} Q}{Q \models \phi}$$

Tool Support: ProB and FDR

Future Work - Scaling the Approach

Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \mathit{available}\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often

$$((\Box \Diamond \mathit{available}\, \mathit{snd}.A.B.Na \Rightarrow \Box \Diamond \mathit{snd}.A.B.Na)$$
$$\bigwedge (\Box \Diamond \mathit{available}\, \mathit{rcv}.A.B.Na \Rightarrow \Box \Diamond \mathit{rcv}.A.B.Na))$$
$$\Rightarrow \Box \Diamond \mathit{flag}$$

Future Work - Scaling the Approach

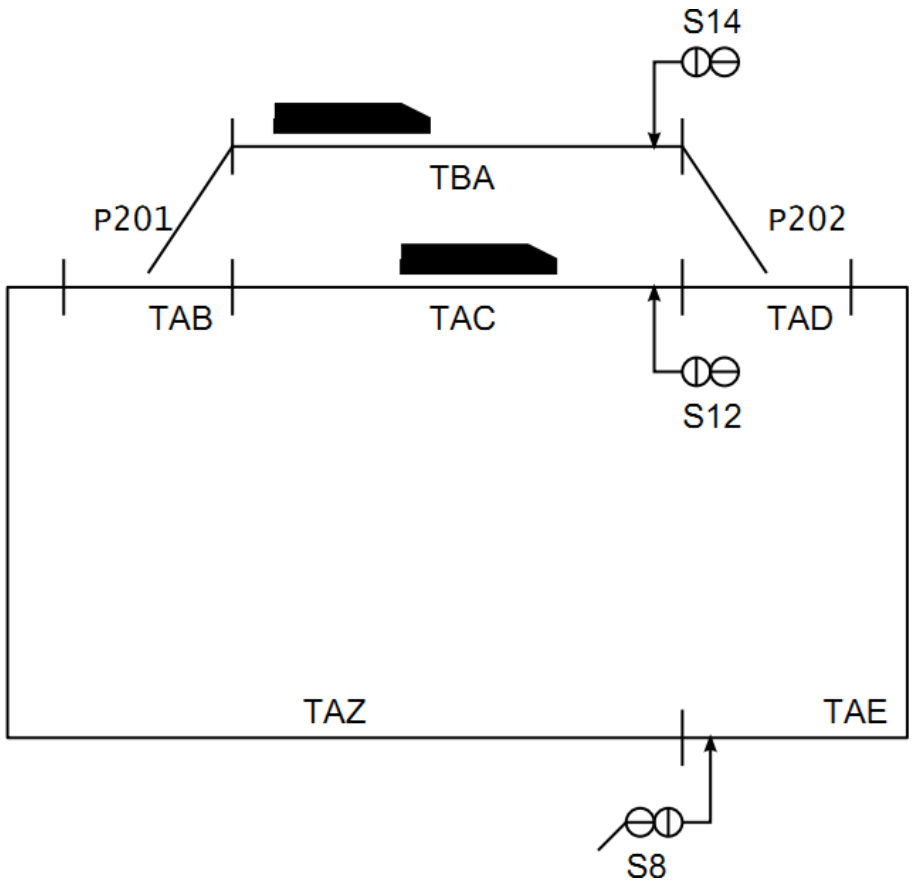
Strong Event Fairness

$$SEF = \bigwedge_{x \in \Sigma} (\Box \Diamond \mathit{available}\, x \Rightarrow \Box \Diamond x)$$

An infinitely often enabled event shall occur infinitely often

$$\begin{aligned}
&((\Box \Diamond \mathit{available}\, \mathit{snd}.A.B.Na \Rightarrow \Box \Diamond \mathit{snd}.A.B.Na) \\
&\bigwedge (\Box \Diamond \mathit{available}\, \mathit{rcv}.A.B.Na \Rightarrow \Box \Diamond \mathit{rcv}.A.B.Na) \\
&\bigwedge (\Box \Diamond \mathit{available}\, \mathit{snd}.A.B.Na' \Rightarrow \Box \Diamond \mathit{snd}.A.B.Na') \\
&\bigwedge (\Box \Diamond \mathit{available}\, \mathit{rcv}.A.B.Na' \Rightarrow \Box \Diamond \mathit{rcv}.A.B.Na')) \\
&\Rightarrow \Box \Diamond \mathit{flag}
\end{aligned}$$

Applications



Conclusion

Any verification using model-based techniques
is only as good as the model of the system.



Our verification approach relates properties of the model to properties of the system along a refinement chain.