FM2011
17TH INTERNATIONAL SYMPOSIUM ON FORMAL METHODS
Limerick, Ireland, June 20-24,2011

Failure-Divergence Refinement of Compensating Communicating Processes

Zhenbang Chen[1], Zhiming Liu[2], Ji Wang[1]

zbchen@nudt.edu.cn

National Laboratory for Parallel and Distributed Processing, Changsha, China

International Institute for Software Technology, The United Nations University, Macau, China

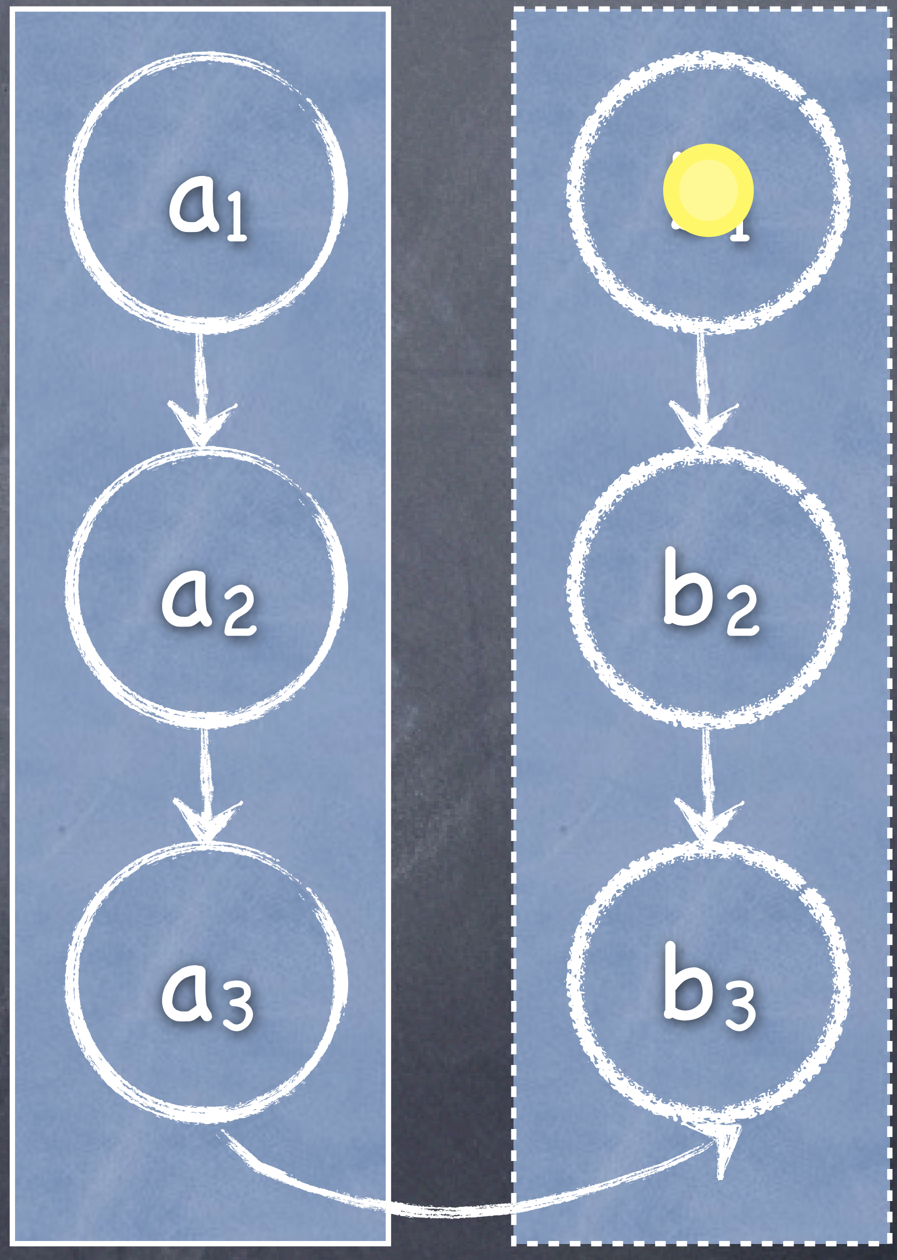
Long-Running Transactions

- Database
  - Long-lived transactions
  - Small ACID transactions
- SAGAS
  - 1987, SIGMOD
- Compensation

Compensation

In Database

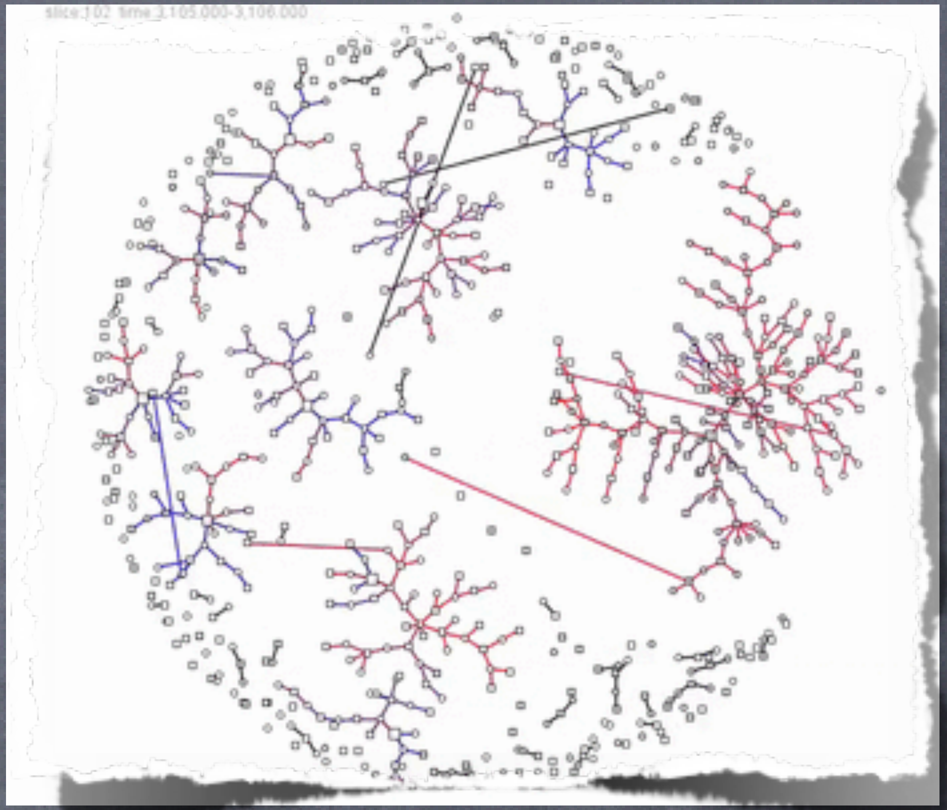
- An activity has its compensation activity
- In case of a failure, use compensations
- Atomicity and consistency



Error -> Failure

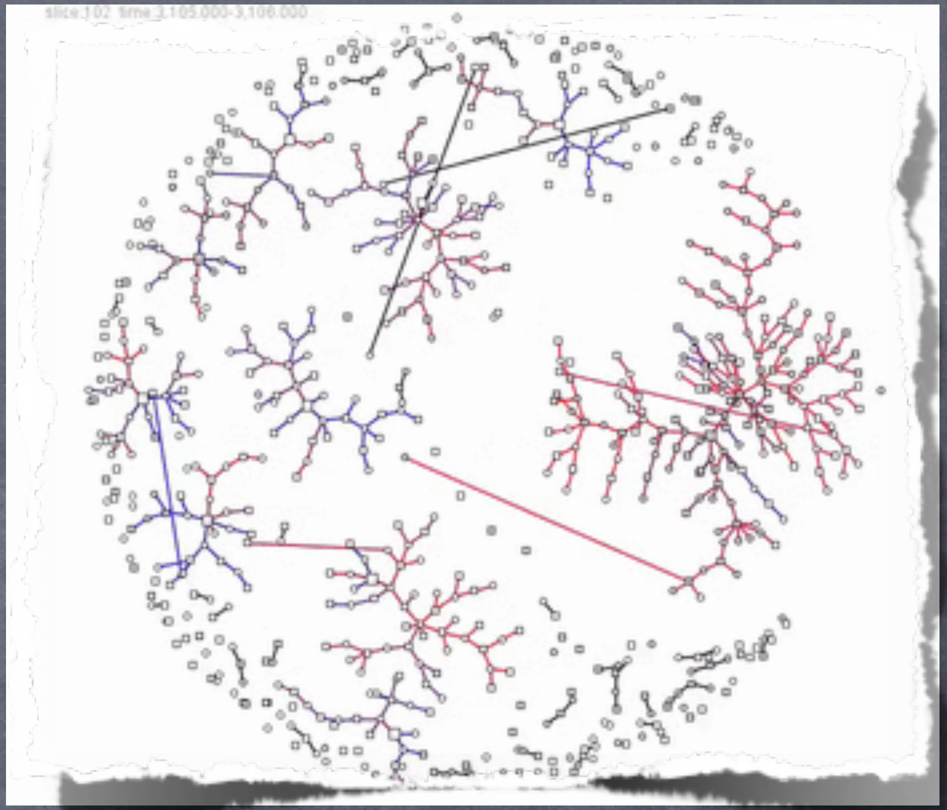
In Service Oriented Computing

- World wide distributed organizations
- Coordinate to accomplish a task



In Service Oriented Computing

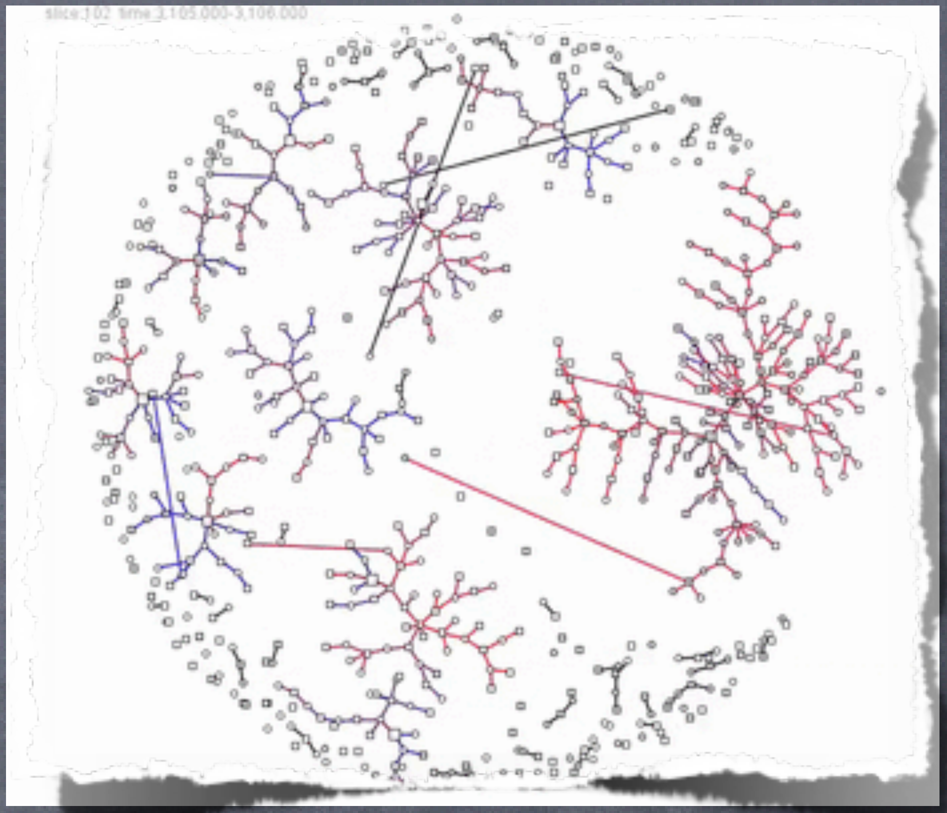
- World wide distributed organizations
- Coordinate to accomplish a task



How to ensure consistency in case of a failure?

In Service Oriented Computing

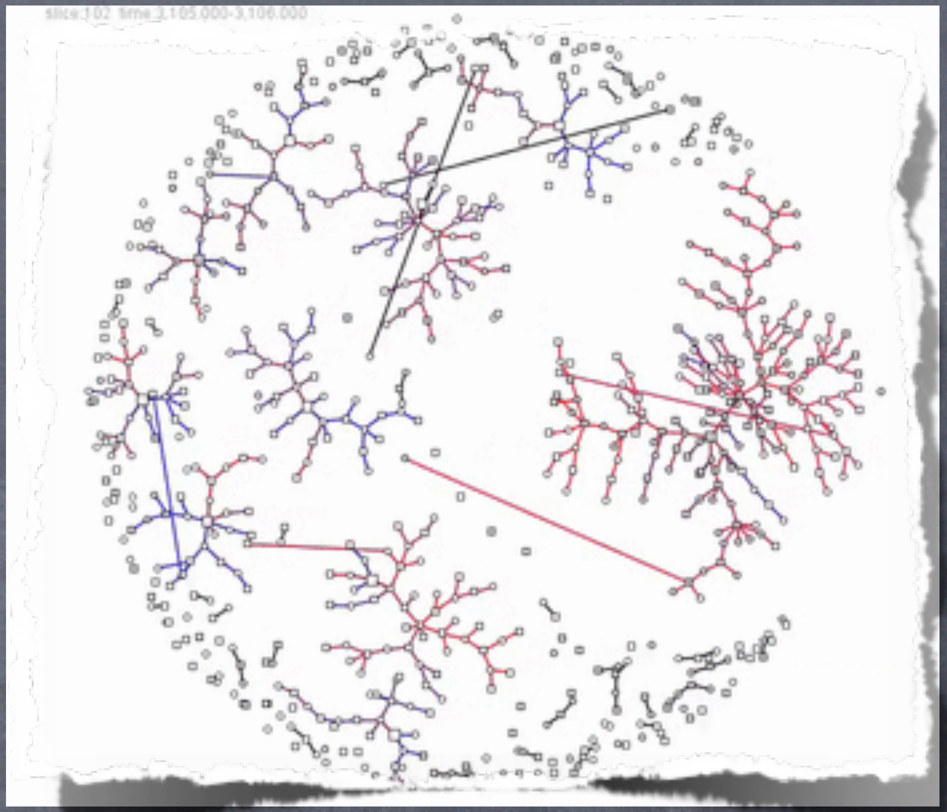
- World wide distributed organizations
- Coordinate to accomplish a task



How to ensure consistency in case of a failure?

In Service Oriented Computing

- World wide distributed organizations
- Coordinate to accomplish a task

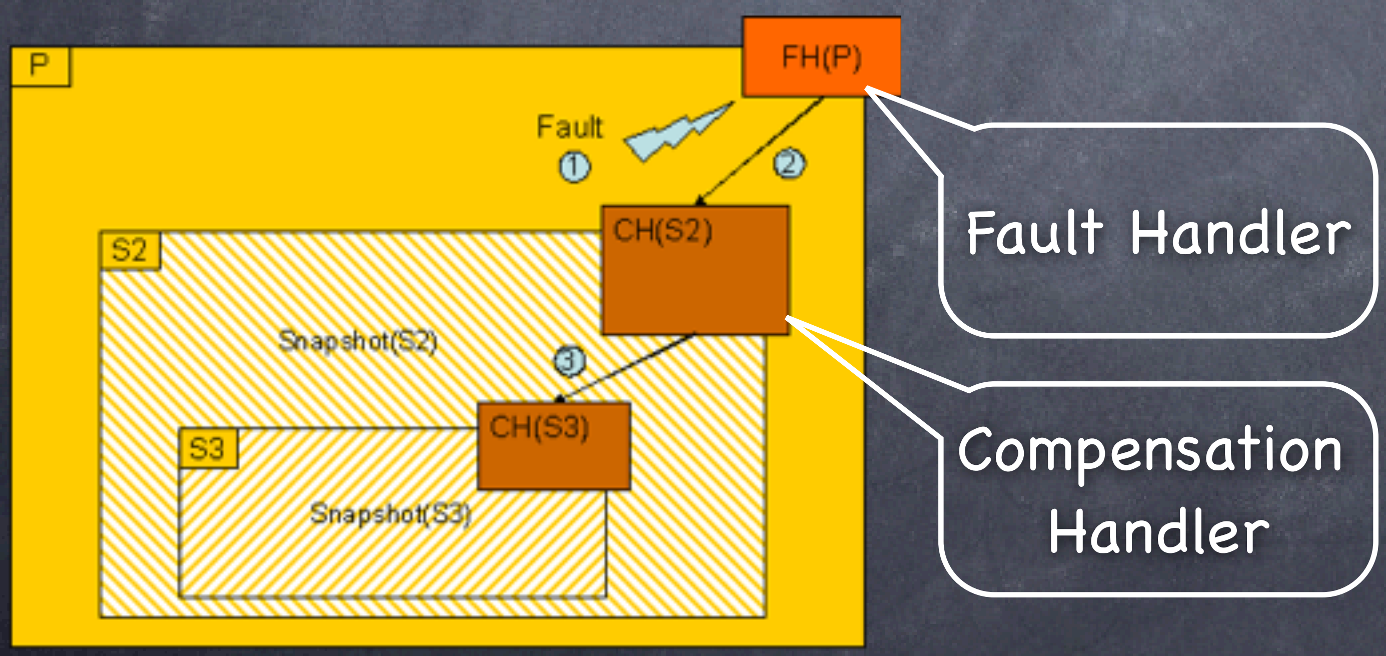


Long Running Transactions

How to ensure consistency in case of a failure?

Orchestration Programming in SOC

- WS-BPEL
  - Compensation based fault handling
  - Flexible recovery mechanisms for LRTs



Ensure an acceptive consistency of composite Web Services

WS-BPEL 2.0, OASIS Standard, 11 April 2007

Orchestration Programming in SOC

- WS-BPEL
  - Compensation based fault handling
  - Flexible recovery mechanisms for LRTs
- Formal languages
  - cCSP, StAC, SAGAs, etc.

Compensating CSP

- Process language
  - CSP extension for LRTs
  - Basic operators
- Two types of processes
  - Standard & Compensable
- Terminated trace semantics

Theoretical Issues of cCSP

- Concurrent systems
  - Non-determinism & Deadlock & Livelock
  - Synchronization & Recursion
- Formal semantics
  - Denotational model
- Refinement

Life Before

- Concurrent features
  - Non-determinism & Deadlock
- Denotational semantics
  - Trace & Stable failures
- Operational semantics

Recursion??? => no divergence

Now

- All basic concurrent features
  - Divergence for livelock
- A failure-divergence semantics
  - Standard & Compensable
  - Fixed-point theory
- Refinement w.r.t the semantics
  - Non-determinism

Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 ; a_2 \div b_2) \; ; \; \mathbf{throww}]$

Extended cCSP Syntax

$$
\begin{aligned}
P \quad ::= \quad & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \mathop{\|}_{X} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
& \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP \quad ::= \quad & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \mathop{\|}_{X} PP \mid PP \boxtimes PP \mid \\
& PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{aligned}
$$

Examples $[(a_1 \div b_1 ; a_2 \div b_2) \; ; \; \mathbf{throww}]$

a_1

b_1

Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 ; a_2 \div b_2)\ ;\ \mathbf{throww}]$

a_1 a_2

b_1 b_2

Extended cCSP Syntax

$$P \quad ::= \quad a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \mathop{\|}_{X} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid$$
$$\mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p)$$

$$PP \quad ::= \quad P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \mathop{\|}_{X} PP \mid PP \boxtimes PP \mid$$
$$PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)$$

Examples $[(a_1 \div b_1; a_2 \div b_2)$; **throww**$]$

a_1 a_2 ☹

b_1 b_2

Extended cCSP Syntax

$$
\begin{array}{lll}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 ; a_2 \div b_2)\ ;\ \mathbf{throww}]$

a_1 a_2 ☹ b_2

b_1

Extended cCSP Syntax

$$
\begin{aligned}
P \quad &::= \quad a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
&\qquad \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP \quad &::= \quad P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
&\qquad PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{aligned}
$$

Examples $[(a_1 \div b_1 ; a_2 \div b_2)$; **throww**$]$

$a_1 \quad a_2 \quad$ ☹ $\quad b_2 \quad b_1$

Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 \underset{\{a_1,a_2\}}{\parallel} a_2 \div b_2)]$

Extended cCSP Syntax

$$
\begin{array}{lll}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 \underset{\{a_1,a_2\}}{\parallel} a_2 \div b_2)]$

$a_1 \quad a_2$

$b_1 \quad b_2$

Extended cCSP Syntax

$$\begin{array}{lll} P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\ & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\ PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\ & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp) \end{array}$$

Examples $[(a_1 \div b_1 \underset{\{a_1,a_2\}}{\parallel} a_2 \div b_2)]$

$$\boxed{a_1 \underset{\{a_1,a_2\}}{\parallel} a_2}$$

b_1 b_2

Extended cCSP Syntax

$$\begin{array}{lcl} P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \triangleright P \mid [PP] \mid \\ & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\ PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\ & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp) \end{array}$$

Examples $[(a_1 \div b_1 \underset{\{a_1,a_2\}}{\parallel} a_2 \div b_2)]$

$$\boxed{a_1 \underset{\{a_1,a_2\}}{\parallel} a_2}$$

$b_1 \quad b_2$

Deadlock!!

Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \triangleright P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2)\ ;\ \mathbf{throww}]$

Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2)\ ;\ \mathbf{throww}]$

a a

b_1 b_2

Extended cCSP Syntax

$$
\begin{array}{lll}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2) \; ; \; \mathbf{throww}]$

$\boxed{a \underset{\{a\}}{\parallel} a}$

$\boxed{b_1 \underset{\{a\}}{\parallel} b_2}$

Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2)\ ;\ \mathbf{throww}]$

$a \underset{\{a\}}{\parallel} a$ ☹

$b_1 \underset{\{a\}}{\parallel} b_2$

Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
 & & \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2)\ ;\ \mathbf{throww}]$

$\boxed{a \underset{\{a\}}{\parallel} a}$ ☹

$\boxed{b_1 \underset{\{a\}}{\parallel} b_2}$

Extended cCSP Syntax

$$P \quad ::= \quad a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p)$$

$$PP \quad ::= \quad P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2) \; ; \; \textbf{throww}]$

$\boxed{a \underset{\{a\}}{\parallel} a}$ ☹ b_2

$\boxed{b_1 \underset{\{a\}}{\parallel}}$

Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2)\ ;\ \mathbf{throww}]$

Extended cCSP Syntax

$$P \quad ::= \quad a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p)$$

$$PP \quad ::= \quad P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)$$

Examples $[(a \div b_1 \underset{\{a\}}{\parallel} a \div b_2)\ ;\ \mathbf{throww}]$

Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
& & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
& & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2);\mathbf{throww}]$

Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \mathbin{\underset{X}{\parallel}} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \mathbin{\underset{X}{\parallel}} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2);\mathbf{throww}]$

a_1 a_2

b_1 b_2

Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2);\mathbf{throww}]$

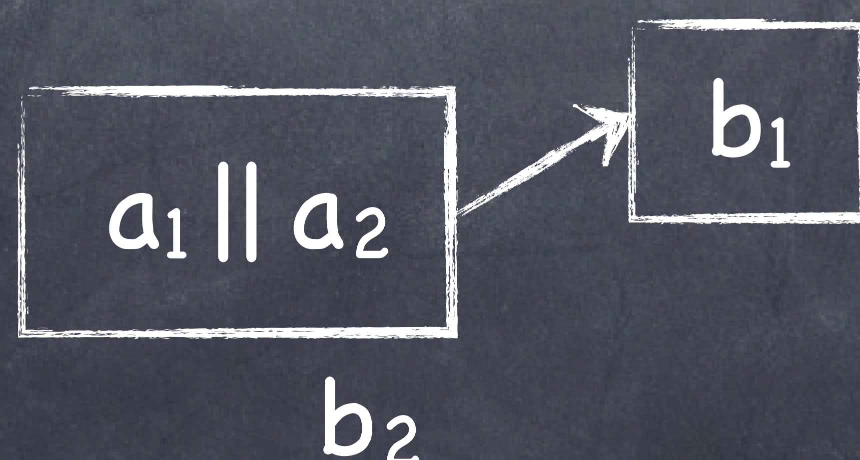
$$\boxed{a_1 \parallel a_2}$$

$b_1 \quad b_2$

Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \textbf{skip} \mid \textbf{stop} \mid \textbf{throw} \mid \textbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \textbf{skipp} \mid \textbf{throww} \mid \textbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

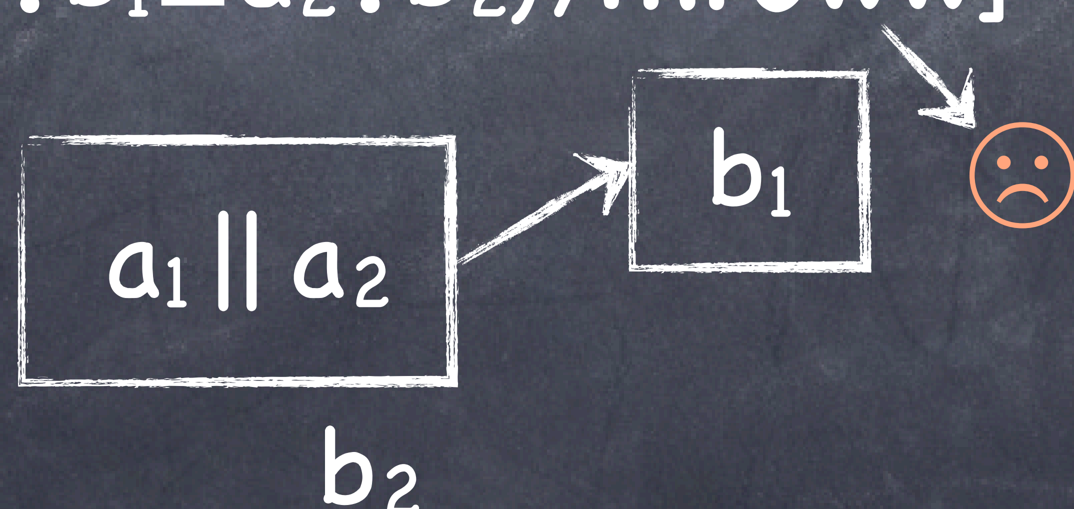
Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2); \textbf{throww}]$



Extended cCSP Syntax

$$
\begin{array}{lll}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \textbf{skip} \mid \textbf{stop} \mid \textbf{throw} \mid \textbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \textbf{skipp} \mid \textbf{throww} \mid \textbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

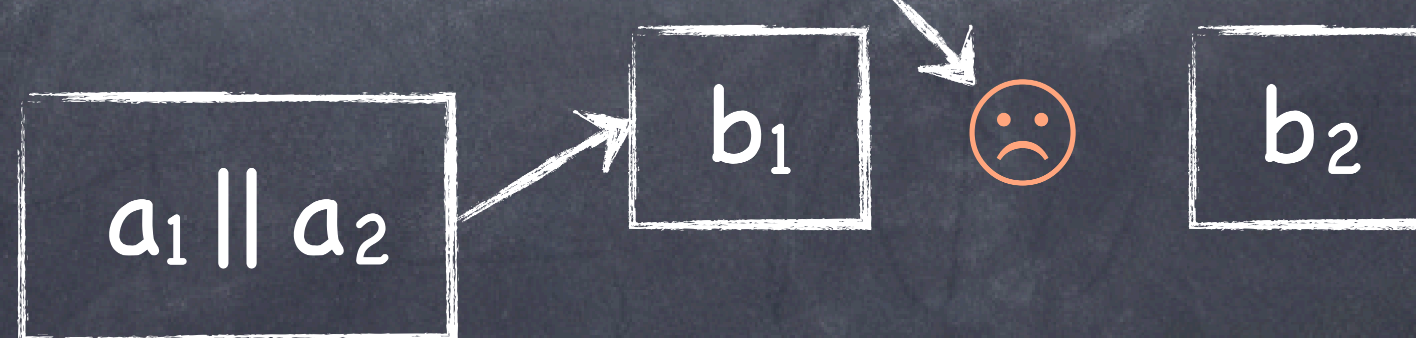
Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2);\textbf{throww}]$



Extended cCSP Syntax

$$
\begin{array}{lcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

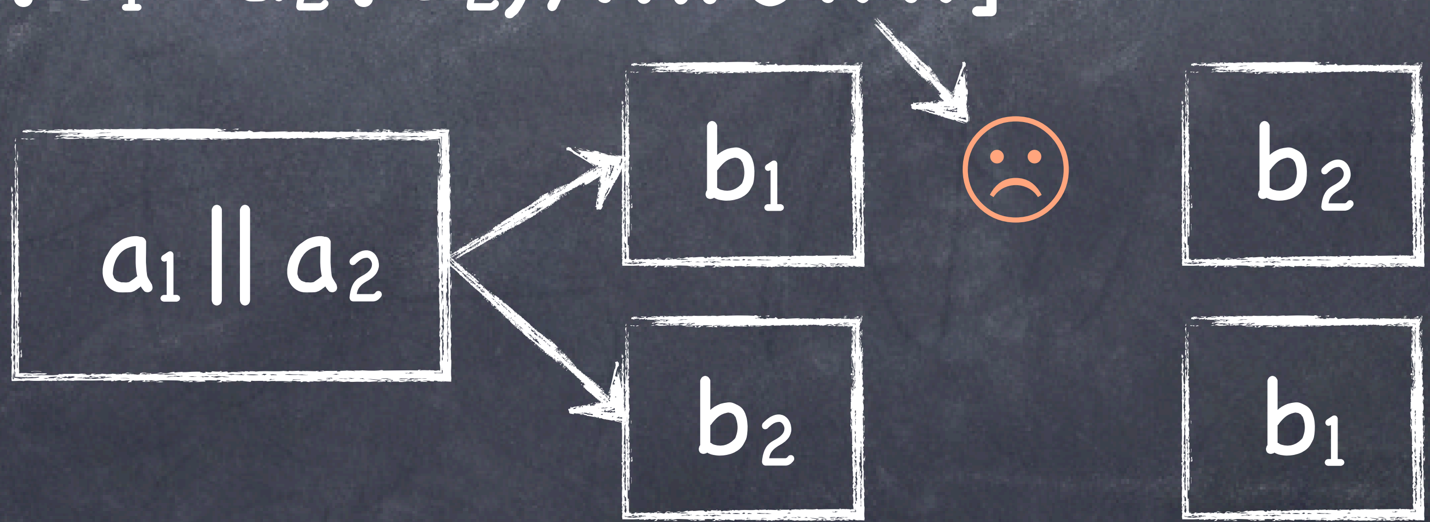
Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2); \mathbf{throww}]$



Extended cCSP Syntax

$$
\begin{array}{rcl}
P & ::= & a \mid P;P \mid P \sqcap P \mid P \Box P \mid P \underset{X}{\parallel} P \mid P \setminus X \mid P[\![R]\!] \mid P \rhd P \mid [PP] \mid \\
 & & \mathbf{skip} \mid \mathbf{stop} \mid \mathbf{throw} \mid \mathbf{yield} \mid \mu\, p.F(p) \\
PP & ::= & P \div P \mid PP;PP \mid PP \sqcap PP \mid PP \Box PP \mid PP \underset{X}{\parallel} PP \mid PP \boxtimes PP \mid \\
 & & PP \setminus X \mid PP[\![R]\!] \mid \mathbf{skipp} \mid \mathbf{throww} \mid \mathbf{yieldd} \mid \mu\, pp.FF(pp)
\end{array}
$$

Examples $[(a_1 \div b_1 \boxtimes a_2 \div b_2);\mathbf{throww}]$



Way to Go

Build a new model

Find it out

Based on an existing one

Stable failures model

Way to Go

Build a new model

Find it out

Based on an existing one

Stable failures model

Problems

- We failed on the first way
  - Compensable processes

(s, T, F)

$$\boxed{[\![PP]\!] = (T, F, C)}$$

Extension

(s, F, D)

$$\boxed{[\![PP]\!] = (F, D, C)}$$

Complete Lattice or CPO?
Refinement order? I don't know

Working Process and Final Result

- Search and tradeoff
  - Semantic model and algebraic laws
  - Refinement and fixed-point theory

$[\![PP]\!]$???

$\Downarrow$ ☺

(F, D, F^c, D^c)

(s, s', X) (s, s')

Order and Properties

$$\boxed{(F_1, D_1, F^c_1, D^c_1) \sqsubseteq_c (F_2, D_2, F^c_2, D^c_2)}$$

$$\boxed{F_1 \supseteq F_2} \wedge \boxed{D_1 \supseteq D_2} \wedge \boxed{F^c_1 \supseteq F^c_2} \wedge \boxed{D^c_1 \supseteq D^c_2}$$

- The order is easy to understand
- The domain is a CPO w.r.t the order
- The order is natural for refinement

Recursion Semantics

- The operators are continuous
- Least fixed-point semantics

$$[\![\mu\, pp.\, FF(pp)]\!] = \bigsqcup\{FF^n(div \div div) \mid n \in N\}$$

$$[\![\mu\, pp.\, (a \div b; pp)]\!] = ([\![\mu\, p.\, (a;p)]\!] ,\{\},\{\})$$

Refinement Laws

- Consistently related

$$\boxed{PP_1 \sqsubseteq_c PP_2 \Rightarrow [PP_1] \sqsubseteq [PP_2]}$$

- Reduction

$$Q_1 \sqsubseteq Q_2 \Rightarrow P \div Q_1 \sqsubseteq_c P \div Q_2$$
$$P_1 \sqsubseteq P_2 \Rightarrow P_1 \div Q \sqsubseteq_c P_2 \div Q$$

Basic Algebraic Laws

- Units and zeros

$$
\boxed{\begin{array}{c} \text{skipp} \,;\, \text{PP} = \text{PP} \\ \text{PP} \,;\, \text{skipp} = \text{PP} \\ \text{throww} \,;\, \text{PP} = \text{throww} \end{array}}
$$

- Distribution

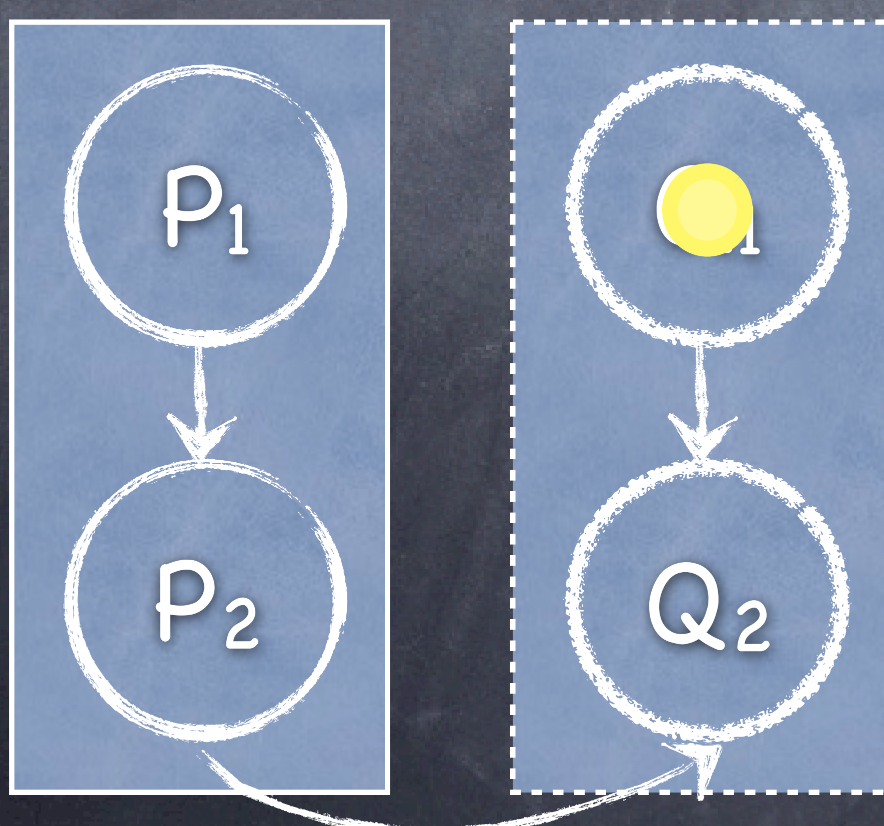
$$
\boxed{\begin{array}{l} [\text{PP} \sqcap \text{QQ}] = [\text{PP}] \sqcap [\text{QQ}] \\ P \div (Q \sqcap R) = (P \div Q) \sqcap (P \div R) \\ (P \div Q) \backslash X = (P \backslash X) \div (Q \backslash X) \end{array}}
$$

Compensation Laws (1)

- If P, P_1 and P_2 do not result in an exception

$$[P \div Q \ ; \ \mathbf{throww}] = P \ ; \ Q$$

$$[P_1 \div Q_1 \ ; \ P_2 \div Q_2 \ ; \ \mathbf{throww}] = P_1 \ ; \ P_2 \ ; \ Q_2 \ ; \ Q_1$$



The laws are still valid when P_1 is YIELD

Compensation Laws (2)

- If all the standard processes terminate successfully and do not diverge

$$[(P \div Q) \| \mathbf{throww}] = P \,;\, Q$$

$$P_1 \div Q_1 \underset{X}{\|} P_2 \div Q_2 = P_1 \underset{X}{\|} P_2 \div Q_1 \underset{X}{\|} Q_2$$

$$[(P_1 \div Q_1 \boxtimes P_2 \div Q_2) \,;\, \mathbf{throww}] = (P_1 \| P_2) \,;\, ((Q_1 \,;\, Q_2) \sqcap (Q_2 \,;\, Q_1))$$

Interruption Laws

- If all the standard processes do not diverge and terminate successfully

$[(\mathbf{yieldd}; P_1 \div Q_1; \mathbf{yieldd}; P_2 \div Q_2) || \mathbf{throww}] =$
$\mathbf{skip} \sqcap (P_1 ; Q_1) \sqcap (P_1 ; P_2 ; Q_2 ; Q_1)$

$[(\mathbf{yieldd}; P_1 \div Q_1) || (\mathbf{yieldd}; P_2 \div Q_2) || \mathbf{throww}] =$
$\mathbf{skip} \sqcap (P_1 ; Q_1) \sqcap (P_2 ; Q_2) \sqcap ((P_1 || P_2);(Q_1 || Q_2))$

yieldd must be used to specify interruption places

Conclusion & Future Work

- A semantic theory for LRTs
  - Non-determinism, deadlock and livelock
  - Design by refinement
  - Verification of LRTs
- Next step
  - Tool development for extended cCSP
  - Component-based modeling

End

Thank you!