GLOBALLY GOVERNED SESSION SEMANTICS

Dimitrios Kouzapas

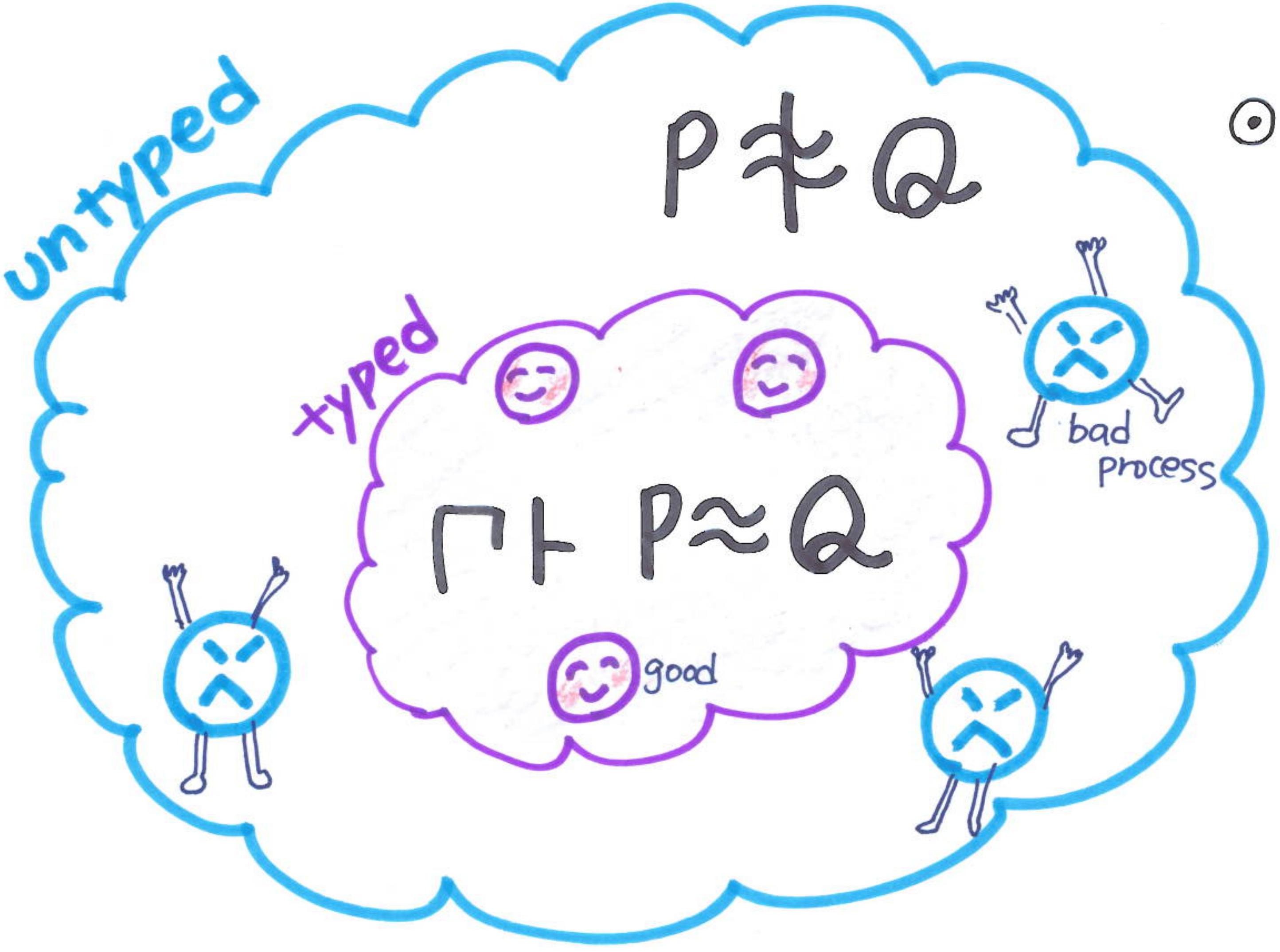
Glasgow

Nobuko Yoshida

Imperial College London

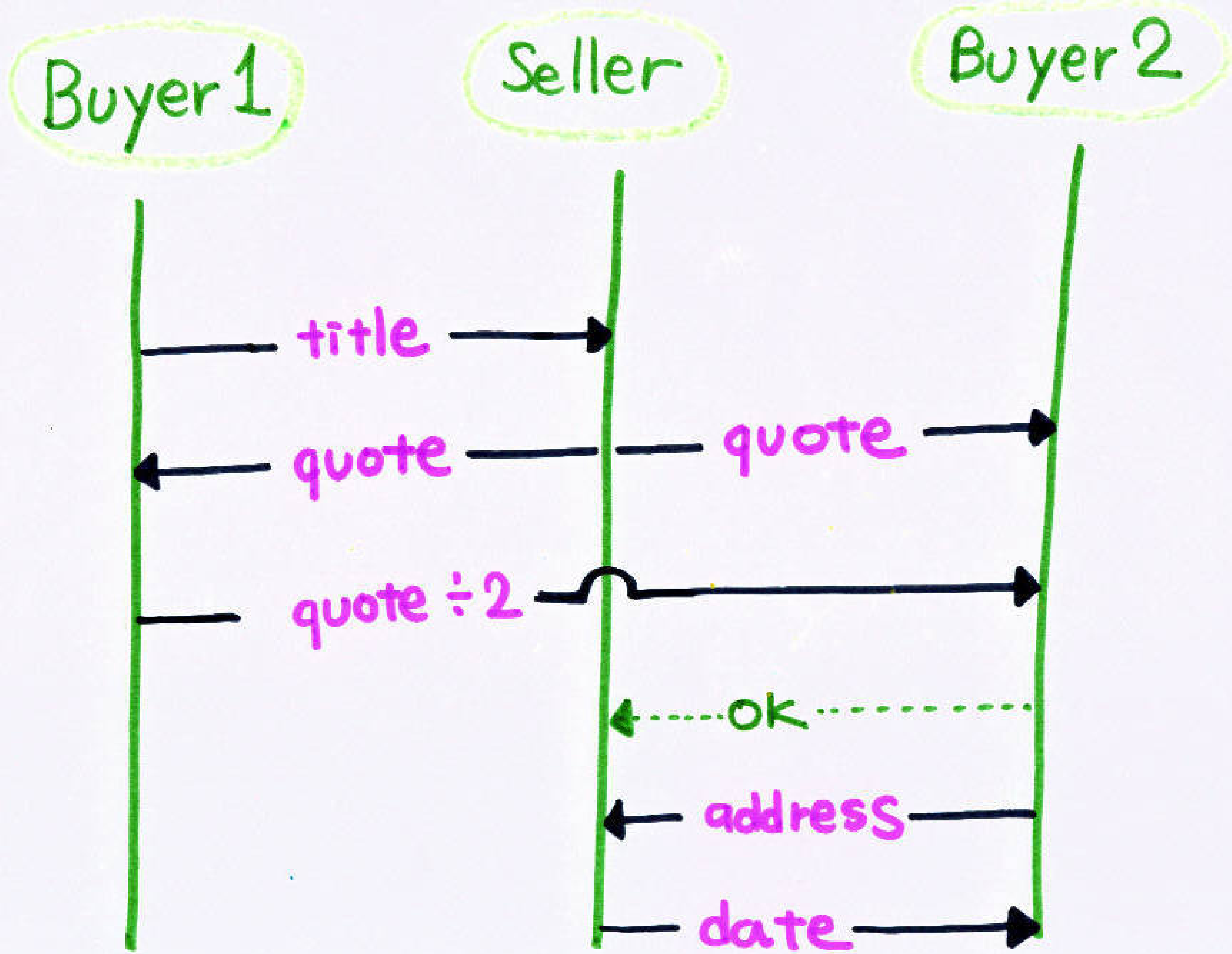
Typed Semantics in π 1991 →

IO-subtyping, Linear types, Secure Information Flow, …

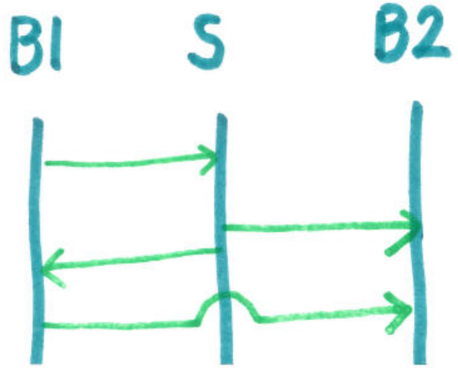


- Correctness of Encoding
- Limit environments Γ
  ⟹ Equate <u>more</u> processes
- Compositional

Multiparty Session Types



Multiparty Session Types [Honda, Yoshida, Carbone 2008]



G

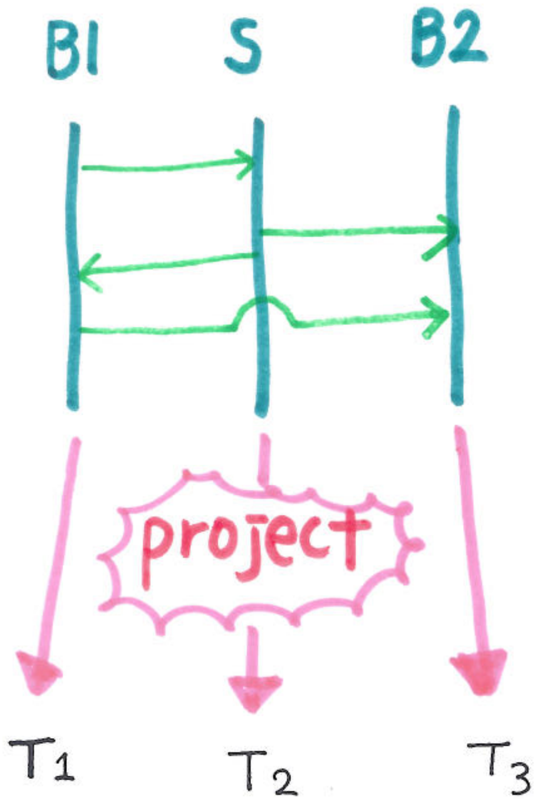
$B1 \to S$ Int.

$S \to B2$ Char

STEP 1

Write Global Type

Multiparty Session Types [Honda, Yoshida, Carbone 2008]



G: $B1 \to S$ Int.

$S \to B2$ Char

T: $B_1 ?$ Int. $B_2 !$ Char

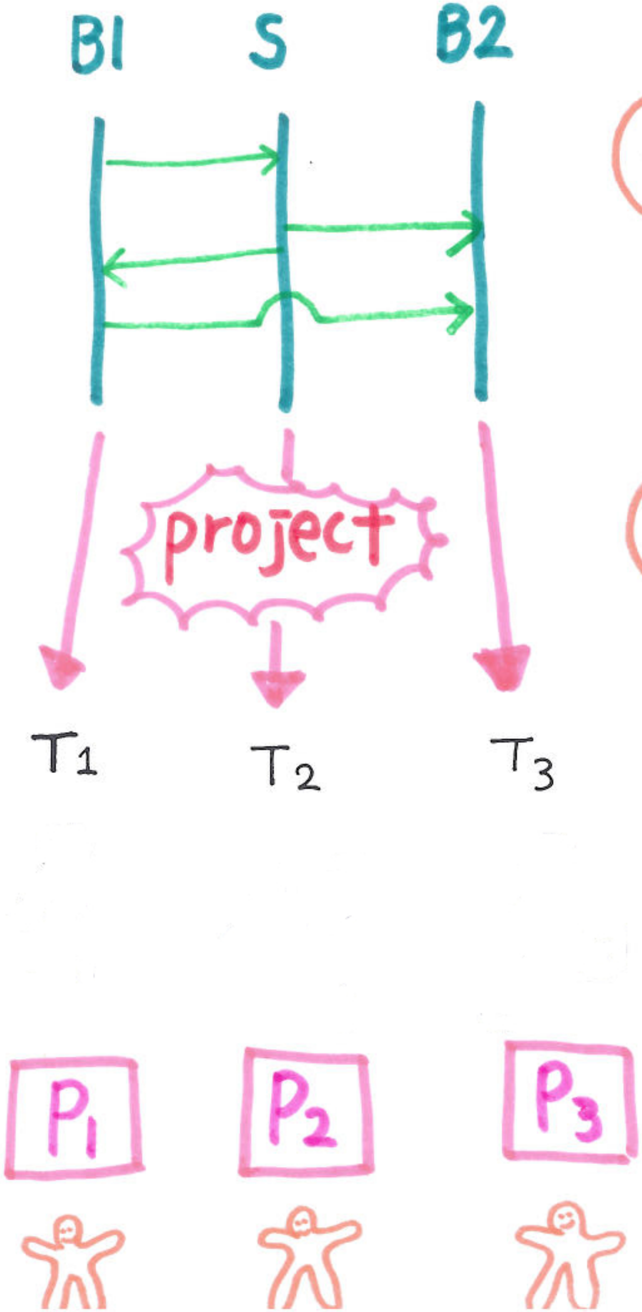
STEP 1

Write Global Type

STEP 2

Project to Local Types

Multiparty Session Types [Honda, Yoshida, Carbone 2008]



G $B1 \rightarrow S$ Int.

$S \rightarrow B2$ Char

T $B_1 ? \mathrm{Int}. B_2 ! \mathrm{Char}$

P $B_1 ?(x). B_2 ! \langle \text{"apple"} \rangle$

STEP 1

Write Global Type

STEP 2

Project to Local Type

STEP 3

- Static Check
- Generate Code
- Run-time Check

Multiparty Session Types

- Participants agreed with global protocols

- Many Multiparty Sessions can interleave

for a single point application

with each message clearly identifiable as belonging to a specific session

Multiparty Session Bisimulations

Standard Multiparty Session Bisimulations $\approx_s$

$$\Gamma \vdash P \triangleright \Delta$$

Shared Env

Session channels Env

Governed Multiparty Session Bisimulations $\approx_g$

$$E, \Gamma \vdash P \triangleright \Delta$$

Global Type Env

a mapping from session to global types

$s_1 : G_1,\ s_2 : G_2,\ \ldots,\ s_n : G_n$

Governed Bisimulations

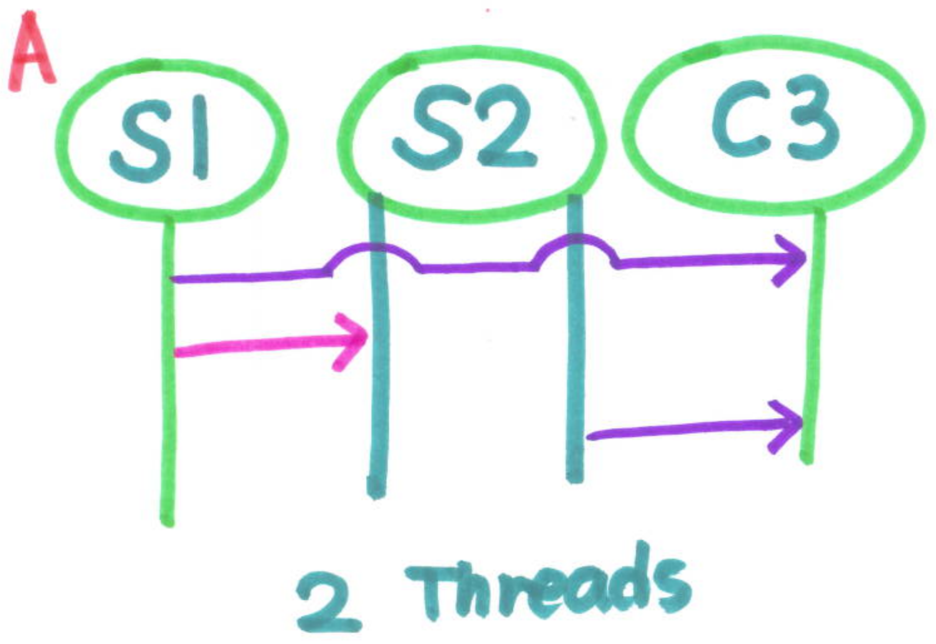
? Compositional? Coincides with Contextual Equiv?

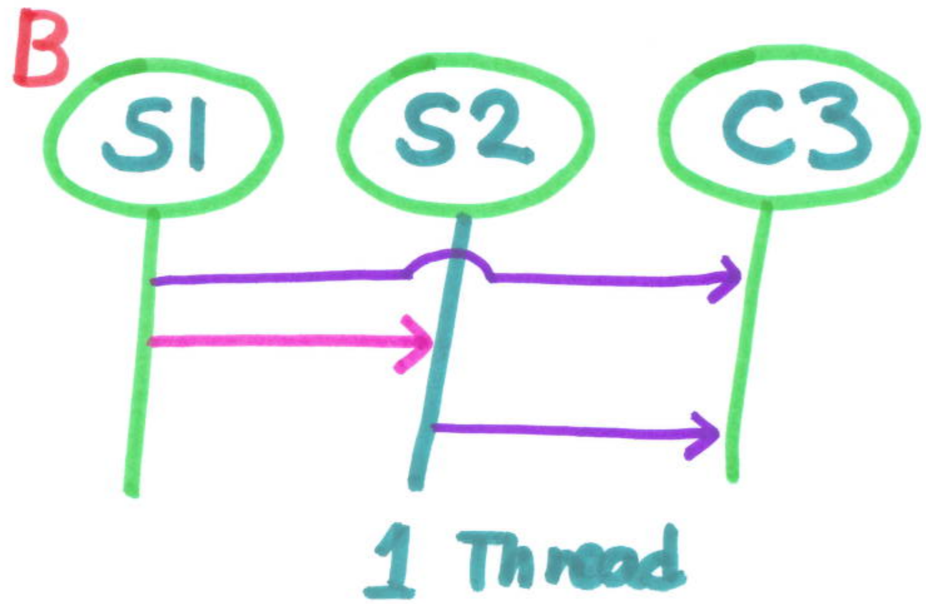
? What is a difference between $\approx_s$ and $\approx_g$?

? Under what condition $\approx_s$ and $\approx_g$ can coincide?

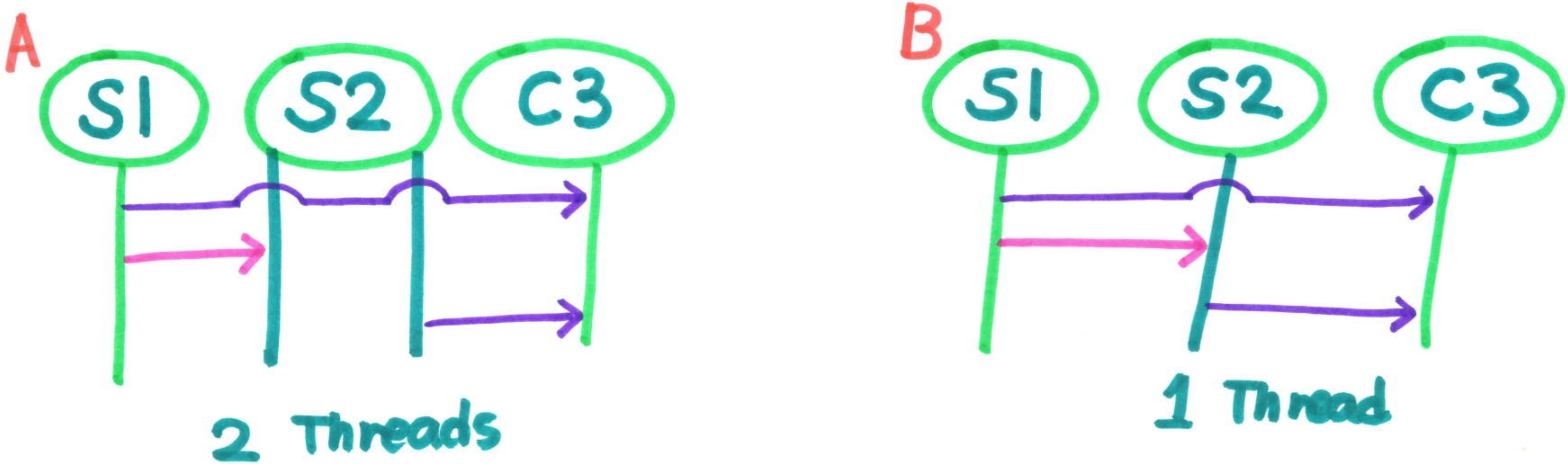
? Applications?

Example Resource Management





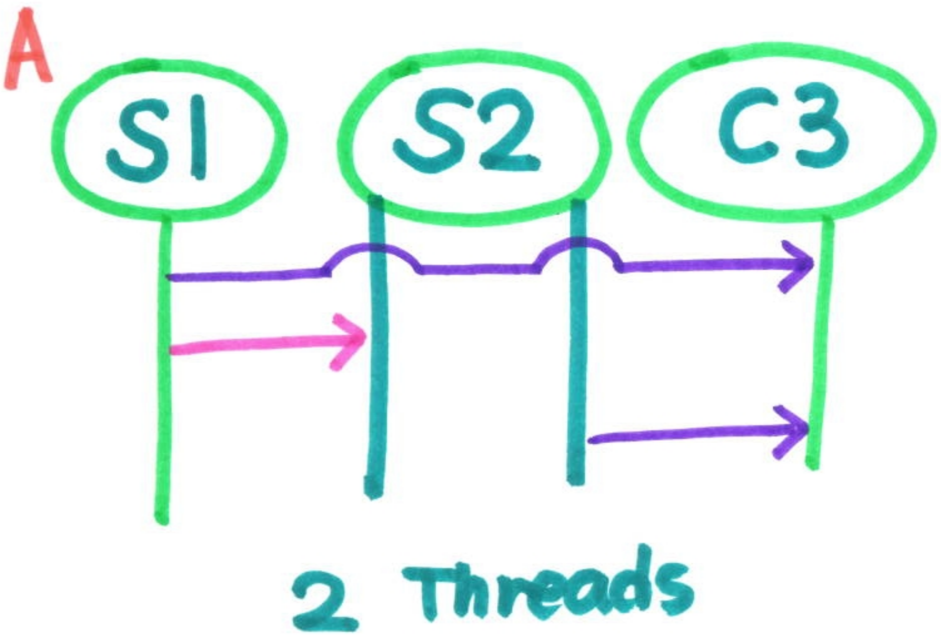
Example Resource Management

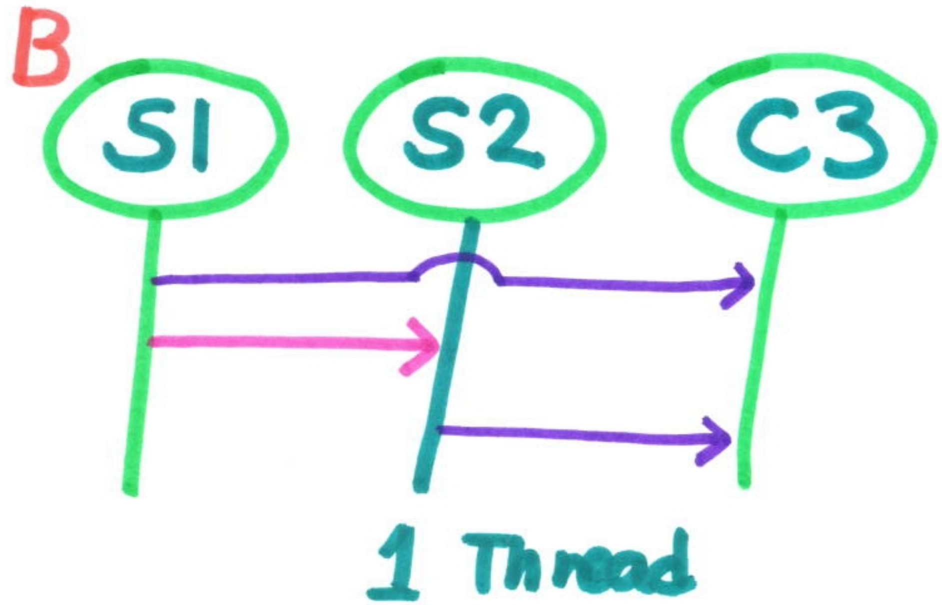


$$G1 = 1 \to 3 : \langle Nat \rangle . 2 \to 3 : \langle Nat \rangle . \text{end}$$

$$G2 = 1 \to 2 : \langle Bool \rangle . \text{end}$$

Example Resource Management





$$P1 = s[1][3]!\langle v\rangle;\ \underline{s'[1][2]}!\langle w\rangle$$

$$P2 = \underline{s'[2][1]}?(x);0 \mid \underline{s[2][3]!\langle v'\rangle};0$$ 2 Threads

$$R = \underline{s'[2][1]?}(x);\ \underline{s[2][3]!\langle v'\rangle};\ 0$$ 1 Thread

$$?\ P_1 \mid P_2 \approx_g P_1 \mid R$$

Standard Semantics

$$P_1 \mid P_2 \not\approx_s P_1 \mid R$$

$$P_1 \mid P_2 \xrightarrow{s[2][3]!\langle v' \rangle} \qquad\qquad P_1 \mid R \not\xrightarrow{s[2][3]!\langle v' \rangle}$$

$$P1 = s[1][3]!\langle v \rangle ; \underline{s'[1][2]}!\langle w \rangle$$

$$P2 = \underline{s'[2][1]}?(x) ; 0 \mid \underline{s[2][3]!\langle v' \rangle ; 0}$$

2 Threads

$$R = \underline{s'[2][1]?}(x) ; \underline{s[2][3]!\langle v' \rangle ;} 0$$

1 Thread

Standard Semantics

$$P_1 \mid P_2 \not\approx_s P_1 \mid R$$

$$P_1 \mid P_2 \xrightarrow{s[2][3]!\langle v' \rangle} \qquad P_1 \mid R \;\not\xrightarrow{s[2][3]!\langle v' \rangle}$$

Governed Semantics

$$P_1 \mid P_2 \approx_g P_1 \mid R$$

$$P_1 \mid P_2 \;\not\xrightarrow{s[2][3]!\langle v \rangle} \qquad P_1 \mid R \;\not\xrightarrow{s[2][3]!\langle v \rangle}$$

$$G1 = 1 \to 3 : \langle Nat \rangle .\ 2 \to 3 : \langle Nat \rangle .\ end$$

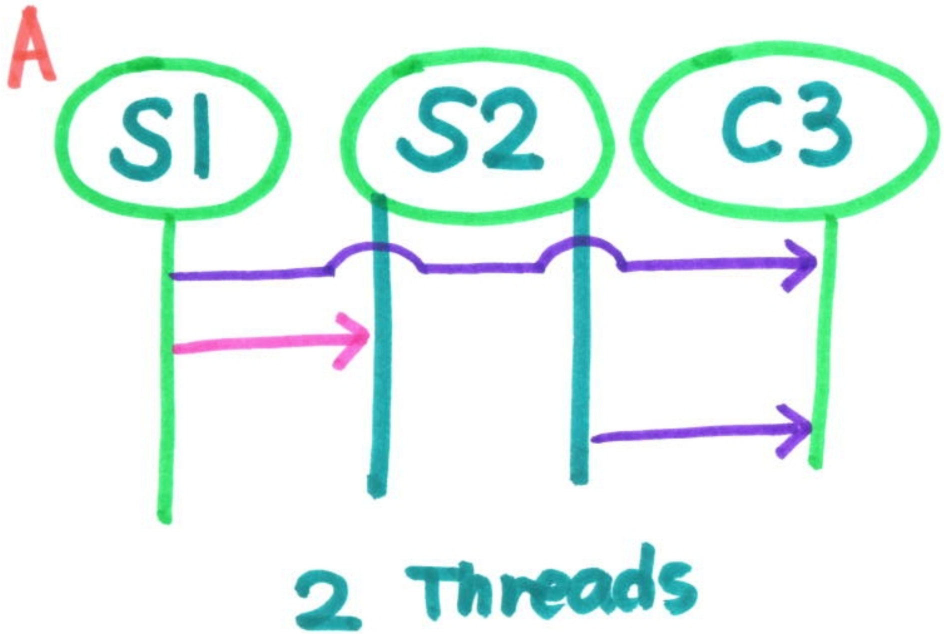
$$G2 = 1 \to 2 : \langle Bool \rangle .\ end$$

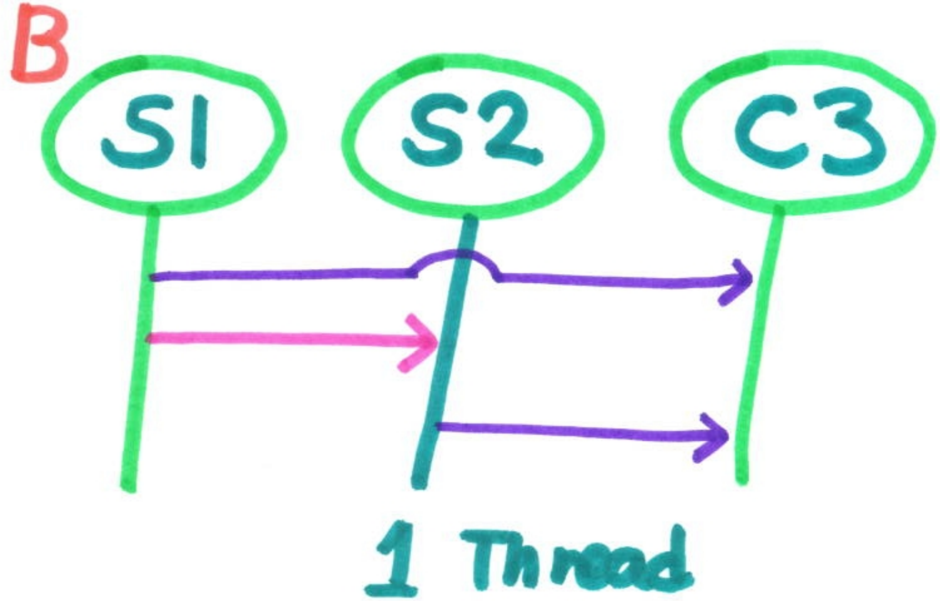
$$P1 = s[1][3]!\langle v \rangle ;\ s'[1][2]!\langle w \rangle$$

$$P2 = s'[2][1]?(x);0 \mid s[2][3]!\langle v' \rangle ; 0$$ 2 Threads

$$R = s'[2][1]?(x);\ s[2][3]!\langle v' \rangle ; 0$$ 1 Thread

Example Resource Management

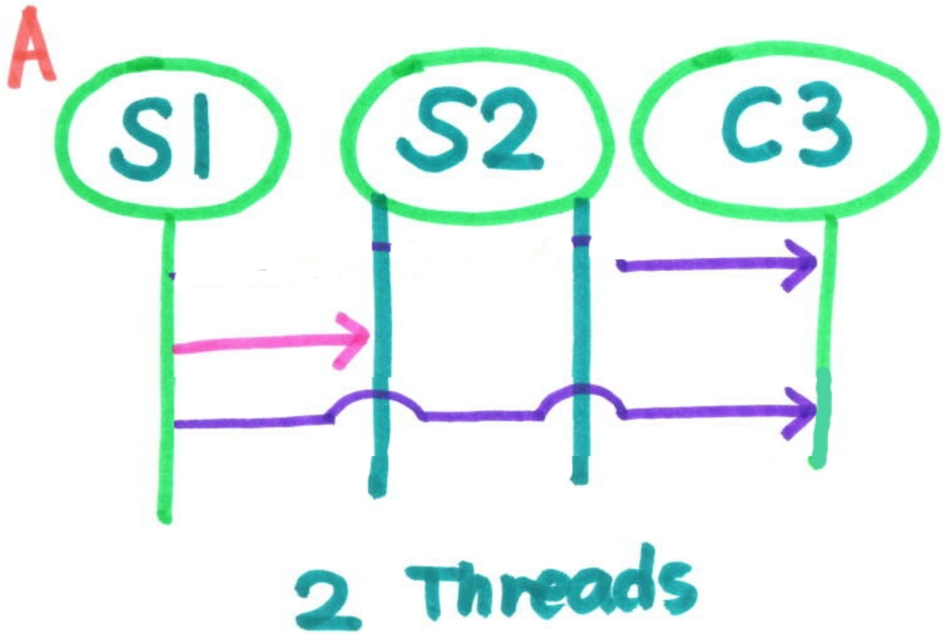


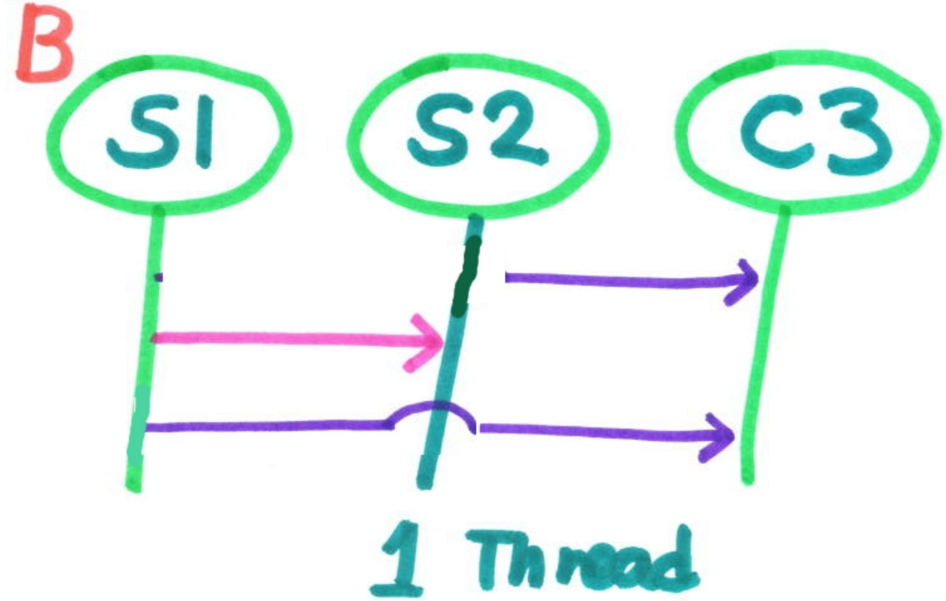


$G1 = 1 \to 3 : \langle Nat \rangle . 2 \to 3 : \langle Nat \rangle . end$

$G2 = 1 \to 2 : \langle Bool \rangle . end$

Example Resource Management





$G2 = 1 \to 2 : \langle Bool \rangle . end$

$G3 = 2 \to 3 : \langle Nat \rangle . 1 \to 3 : \langle Nat \rangle . end$

Standard Semantics

$P_1 \mid P_2 \not\approx_s P_1 \mid R$

$P_1 \mid P_2 \xrightarrow{s[2][3]!\langle v' \rangle}$ $\qquad$ $P_1 \mid R \not\xrightarrow{s[2][3]!\langle v' \rangle}$

Governed Semantics

$P_1 \mid P_2 \not\approx_g P_1 \mid R$

$P_1 \mid P_2 \xrightarrow{s[2][3]!\langle v' \rangle}$ $\qquad$ $P_1 \mid R \not\xrightarrow{s[2][3]!\langle v' \rangle}$

$G3 = 2 \to 3 : \langle Nat \rangle . 1 \to 3 : \langle Nat \rangle . \mathrm{end}$

$G2 = 1 \to 2 : \langle Bool \rangle . \mathrm{end}$

$P1 = s[1][3]!\langle v \rangle ; \underline{s'[1][2]}!\langle w \rangle$

$P2 = \underline{s'[2][1]?}(x) ; 0 \mid s[2][3]!\langle v' \rangle ; 0$ $\qquad$ 2 Threads

$R = \underline{s'[2][1]?}(x) ; s[2][3]!\langle v' \rangle ; 0$ $\qquad$ 1 Thread

Syntax and Semantics

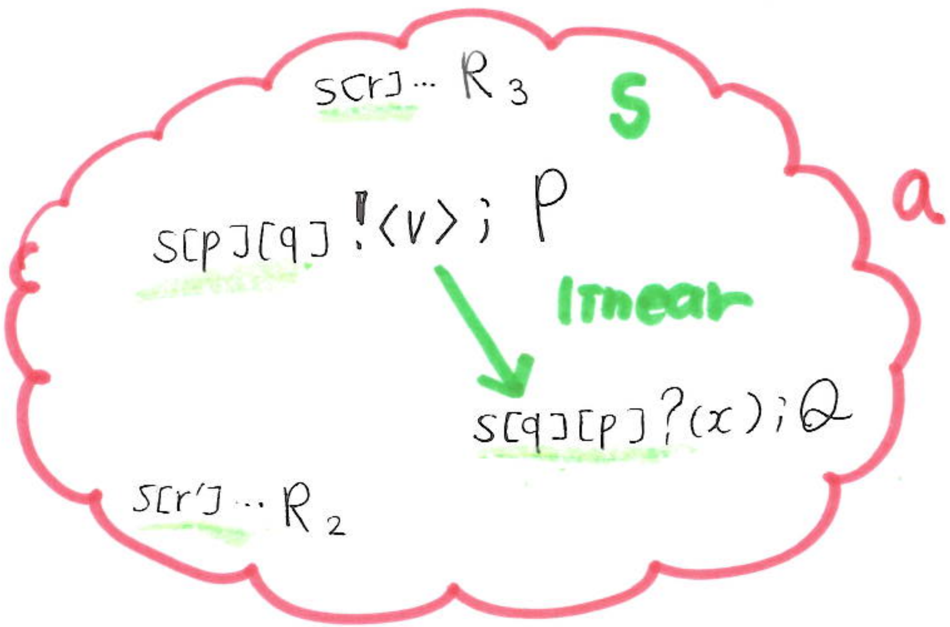
$p \cdots\cdots$ participants
$q \cdots\cdots$

$$a[1](x).\ P_1 \mid a[2](x).\ P_2 \mid \cdots \mid \bar{a}[n](x).\ P_n$$

$$\longrightarrow (\nu s)\left(P_1\{s[1]/x\} \mid P_2\{s[2]/x\} \mid \cdots \mid P_n\{s[n]/x\}\right)$$

$$s[p][q]!\langle e\rangle; P \mid s[q][p]?(x); Q \longrightarrow P \mid Q\{v/x\} \quad (e \downarrow v)$$

$$s[p][q] \oplus l_k; P \mid s[q][p] \& \{l_i : P_i\}_{i \in I} \longrightarrow P \mid P_k$$



Global Types

$$
\begin{aligned}
G ::= \;& p \to q : \langle U \rangle . G' \\
\mid\;& p \to q : \{ l_i . G_i \}_{i \in I} \\
\mid\;& \mu t . G \\
\mid\;& t \\
\mid\;& \mathrm{end}
\end{aligned}
$$

$$
U ::= \mathrm{bool} \mid G \mid T
$$

Local Types

$$
\begin{aligned}
T ::= \;& [q]!\langle U \rangle ; T' \\
\mid\;& [p]?\langle U \rangle ; T' \\
\mid\;& [q] \oplus \{ l_i . T_i \} \\
\mid\;& [p] \,\&\, \{ l_i . T_i \} \\
\mid\;& \mu t . T \\
\mid\;& t \\
\mid\;& \mathrm{end}
\end{aligned}
$$

Global Types

$$G ::= p \to q : \langle U \rangle . G' \mid p \to q : \{l_i . G_i\}_{i \in I} \mid \mu t . G \mid t \mid \mathsf{end}$$

$G \upharpoonright p$

Local Types

$$T ::= [q]\,!\langle U \rangle ; T' \mid [p]\,?\langle U \rangle ; T' \mid [q] \oplus \{l_i . T_i\} \mid [p]\,\&\{l_i . T_i\} \mid \mu t . T \mid t \mid \mathsf{end}$$

$$U ::= \mathsf{bool} \mid G \mid T$$

Global Types

$$G ::= p \to q : \langle U \rangle . G'$$
$$\mid\ p \to q : \{ l_i . G_i \}_{i \in I}$$
$$\mid\ \mu t . G$$
$$\mid\ t$$
$$\mid\ \mathtt{end}$$

$$U ::= \mathtt{bool} \mid G \mid T$$

$G \upharpoonright q$

Local Types

$$T ::= [q]!\langle U \rangle ; T'$$
$$\mid\ [p]?\langle U \rangle ; T'$$
$$\mid\ [q] \oplus \{ l_i . T_i \}$$
$$\mid\ [p] \& \{ l_i . T_i \}$$
$$\mid\ \mu t . T$$
$$\mid\ t$$
$$\mid\ \mathtt{end}$$

Part 1 : Standard $\approx_s$

Judgement $\boxed{\Gamma \vdash P \triangleright \Delta}$

Shared Env — Session Env

$u : S,\ u' : S', \ldots$ — $c : T,\ c' : T' \ldots$

Labels

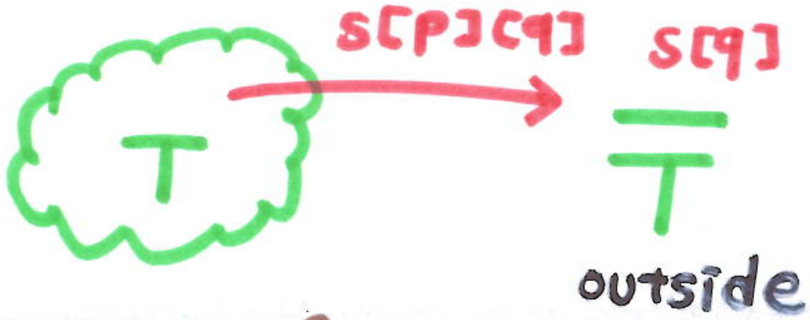
$$
\begin{aligned}
\boxed{\ell} ::= \;& \bar{a}[A](s) \mid a[A](s) \\
\mid\;& s[p][q]!\langle v \rangle \mid s[p][q]!(a) \\
\mid\;& s[p][q]!(s'[q']) \mid s[p][q]?\langle v \rangle \\
\mid\;& s[p][q] \oplus \ell \mid s[p][q] \& \ell \mid \tau
\end{aligned}
$$

Untyped LTS $\boxed{P \xrightarrow{\ell} P'}$

$$(\Gamma, \Delta) \xrightarrow{\ell} (\Gamma', \Delta')$$

if $\Gamma \vdash v : U \qquad s[q] \notin \mathrm{dom}(\Delta)$

then $(\Gamma,\ \Delta \cdot s[p] : [q]!\langle U \rangle ; T) \xrightarrow{s[p][q]!\langle v \rangle} (\Gamma,\ \Delta \cdot s[p] : T)$



$$\Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} \Gamma' \vdash P' \triangleright \Delta'$$

if $\Gamma \vdash P \triangleright \Delta$ and $P \xrightarrow{\ell} P'$ and $(\Gamma, \Delta) \xrightarrow{\ell} (\Gamma', \Delta')$

and $\Gamma' \vdash P' \triangleright \Delta'$

Synchronous Multiparty Session Bisimulation

$\Gamma \vdash P_1 \triangleright \Delta_1 \; \mathcal{R} \; \Gamma \vdash P_2 \triangleright \Delta_2$ with $\Delta_1 \leftrightarrow \Delta_2$

1. $\Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} \Gamma' \vdash P_1' \triangleright \Delta_1'$

$\Rightarrow \Gamma \vdash P_2 \triangleright \Delta_2 \stackrel{\hat{\ell}}{\Longrightarrow} \Gamma' \vdash P_2' \triangleright \Delta_2'$

and $\Gamma \vdash P_1' \triangleright \Delta_1' \; \mathcal{R} \; \Gamma \vdash P_2' \triangleright \Delta_2'$

2. $\mathcal{R}$ symmetric

max relation

$\approx_s$

$\boxed{\textbf{Theorem 1}}$ $\quad \cong_s \; = \; \approx_s$

sound and completeness

typed barbed reduction closed congruence

Part 2 Governed Bisimulation

1 E witness

2 $E \xrightarrow{\lambda} E'$ LTS

3 $E, \Gamma \vdash P \triangleright \Delta$ judgement

4 $E, \Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} E', \Gamma' \vdash P' \triangleright \Delta'$ LTS

by $(E, \Gamma, \Delta) \xrightarrow{\ell} (E', \Gamma', \Delta')$ LTS of Envs

5. $E_1, \Gamma_1 \vdash P_1 \triangleright \Delta_1 \; \mathcal{R} \; E_2, \Gamma_2 \vdash P_2 \triangleright \Delta_2$ a typed relation

Part 2 Governed Bisimulation

$E ::= \phi$
$\quad | \; E \cdot s : G$

1 E witness

2 $E \xrightarrow{\lambda} E'$ LTS

3 $E, \Gamma \vdash P \triangleright \Delta$ judgement

4 $E, \Gamma \vdash P \triangleright \Delta \xrightarrow{\ell} E', \Gamma' \vdash P' \triangleright \Delta'$ LTS

by $(E, \Gamma, \Delta) \xrightarrow{\ell} (E', \Gamma', \Delta')$ LTS of Envs

5. $E_1, \Gamma_1 \vdash P_1 \triangleright \Delta_1 \; \mathcal{R} \; E_2, \Gamma_2 \vdash P_2 \triangleright \Delta_2$ a typed relation

LTS $(E, \Gamma, \Delta) \xrightarrow{\ell} (E', \Gamma', \Delta')$

$$[\mathrm{Out}]\ \frac{E \xrightarrow{s:p\to q:U} E' \quad \Gamma \vdash v : U \quad (\Gamma, \Delta) \xrightarrow{s[p][q]!\langle v\rangle} (\Gamma', \Delta')}{(E, \Gamma, \Delta) \xrightarrow{s[p][q]!\langle v\rangle} (E', \Gamma', \Delta')}$$

Judgement $E, \Gamma \vdash P \triangleright \Delta$

if $\exists E'.\ E \xrightarrow{\tilde{\lambda}}{}^{*} E'$ and $\boxed{\Delta \subseteq \mathrm{proj}(E')}$

a witness is coherent with Δ

LTS $E_1, \Gamma_1 \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} E_2, \Gamma_2 \vdash P_2 \triangleright \Delta_2$

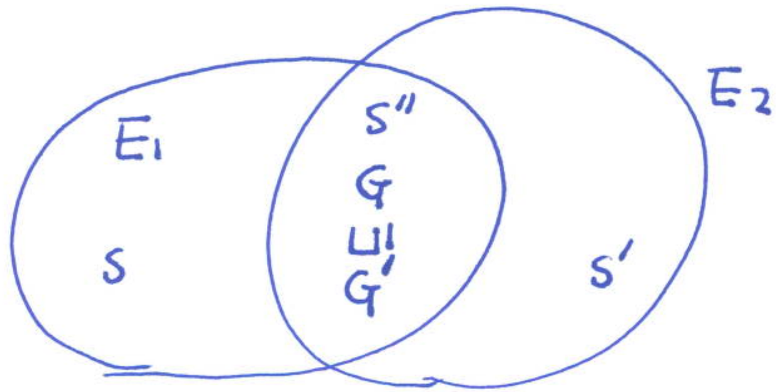
if $P_1 \xrightarrow{\ell} P_2 \wedge (E_1, \Gamma_1, \Delta_1) \xrightarrow{\ell} (E_2, \Gamma_2, \Delta_2)$

$\wedge\ E_2, \Gamma_2 \vdash P_2 \triangleright \Delta_2$

Configuration Relation

$E_1, \Gamma \vdash P_1 \triangleright \Delta_1 \;\mathcal{R}\; E_2, \Gamma \vdash P_2 \triangleright \Delta_2$

if $E_1 \sqcup E_2$ defined



we take <u>a longer</u> global type

Governed Bisimulation $\approx_g$

$E, \Gamma \vdash P_1 \triangleright \Delta_1 \; \mathcal{R} \; P_2 \triangleright \Delta_2$

1. $E, \Gamma \vdash P_1 \triangleright \Delta_1 \xrightarrow{\ell} E_1', \Gamma' \vdash P_1' \triangleright \Delta_1'$

   $E, \Gamma \vdash P_2 \triangleright \Delta_2 \stackrel{\hat{\ell}}{\Longrightarrow} E_2', \Gamma' \vdash P_2' \triangleright \Delta_2'$

   s.t. $E_1' \sqcup E_2', \Gamma \vdash P_1' \triangleright \Delta_1' \; \mathcal{R} \; P_2' \triangleright \Delta_2'$

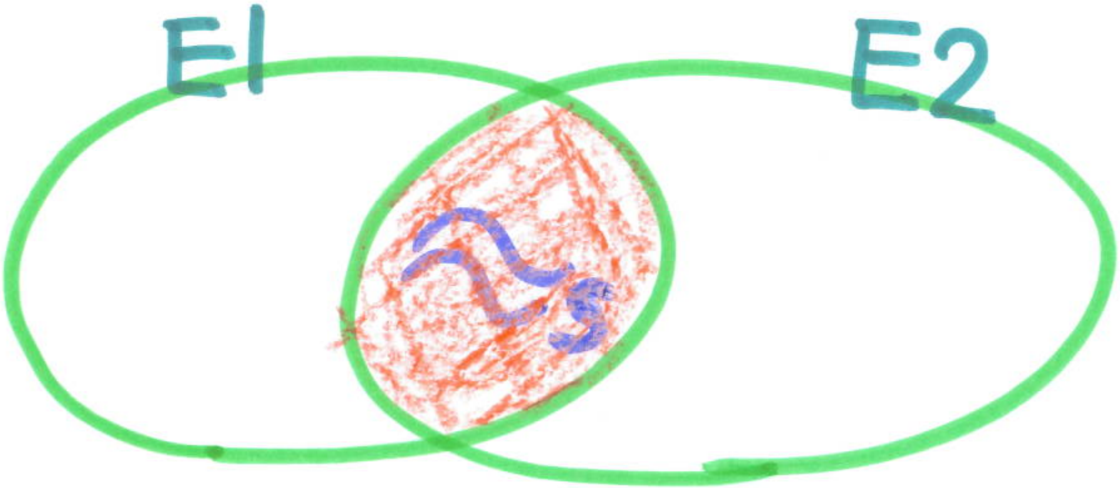
2. $\mathcal{R}$ is symmetric

Theorem 2 $\quad \cong_g \; = \; \approx_g$

soundness and completeness

Theorem 3

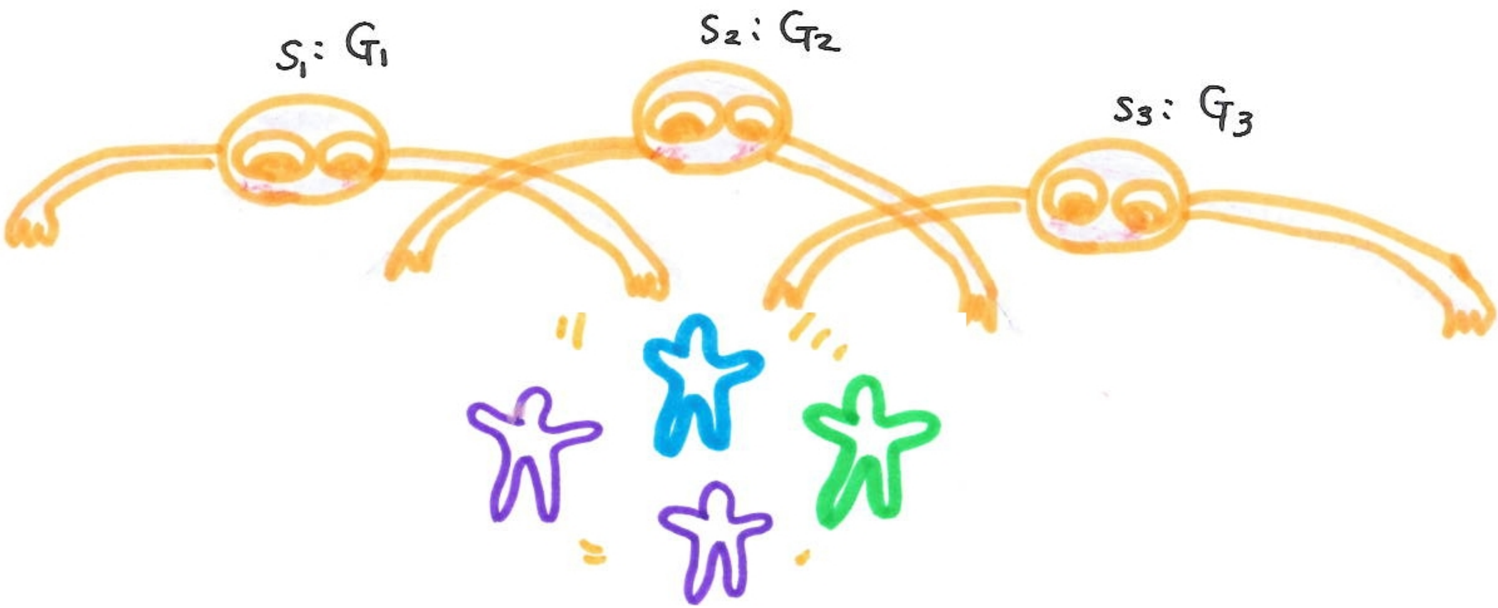
- If for all E $\quad$ $E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$
  then $\Gamma \vdash P_1 \triangleright \Delta_1 \approx_s P_2 \triangleright \Delta_2$
- If $\Gamma \vdash P_1 \triangleright \Delta_1 \approx_s P_2 \triangleright \Delta_2$
  then for all E $\quad$ $E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$



Theorem 4 (coincidence)

no interleaved sessions

Assume P_1 and P_2 are simple. If there exists E s.t. $E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$, then $\Gamma \vdash P_1 \triangleright \Delta_1 \approx_s P_2 \triangleright \Delta_2$



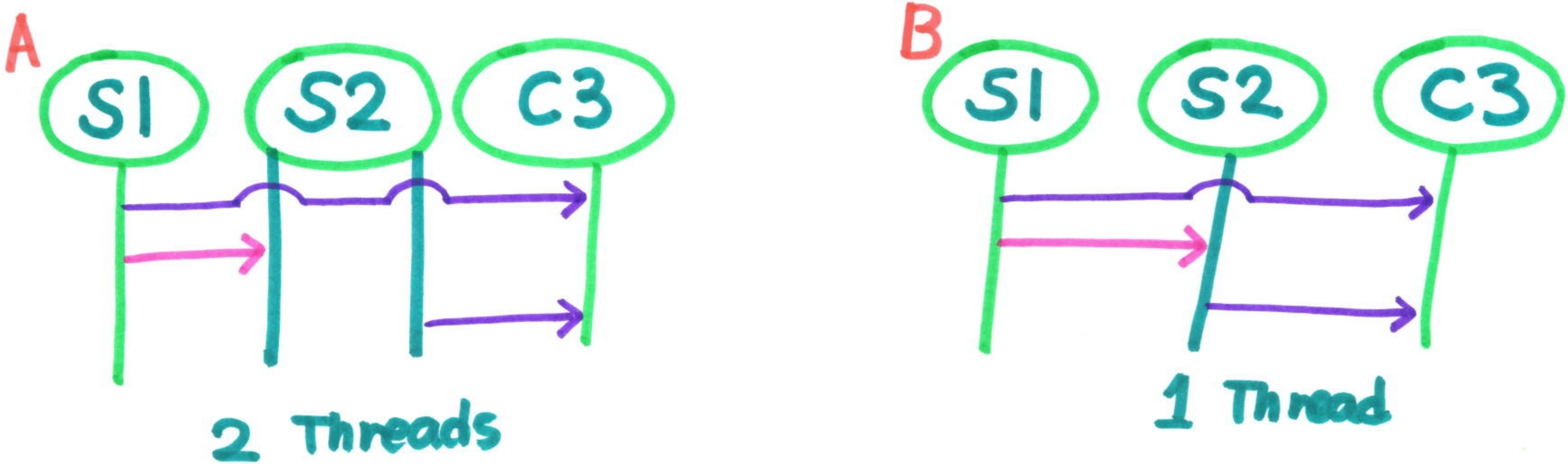
Theorem 4 (coincidence)

no interleaved sessions

Assume P_1 and P_2 are simple. If there exists E s.t. $E, \Gamma \vdash P_1 \triangleright \Delta_1 \approx_g P_2 \triangleright \Delta_2$, then

$$\Gamma \vdash P_1 \triangleright \Delta_1 \approx_s P_2 \triangleright \Delta_2$$

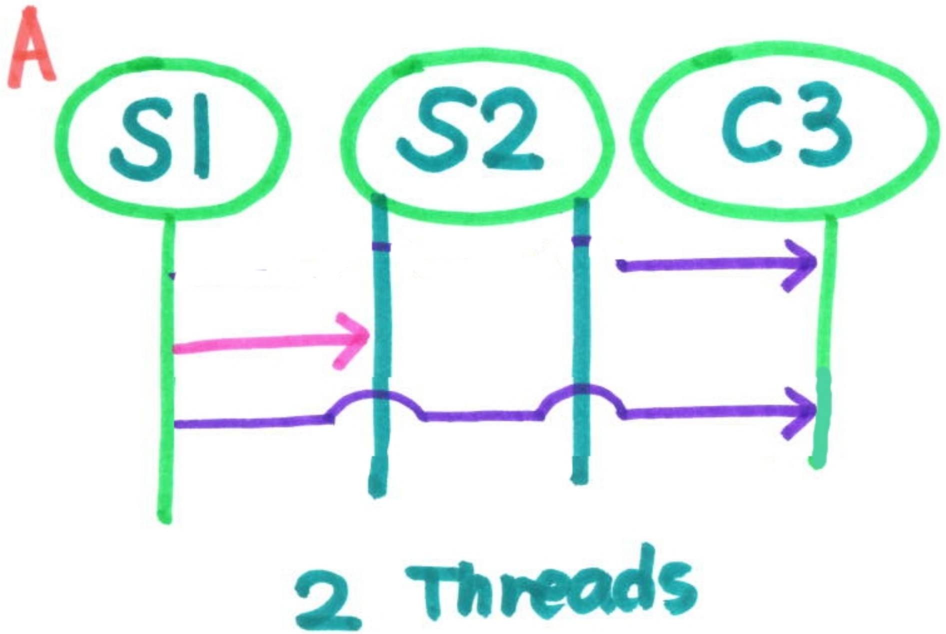
Example Resource Management

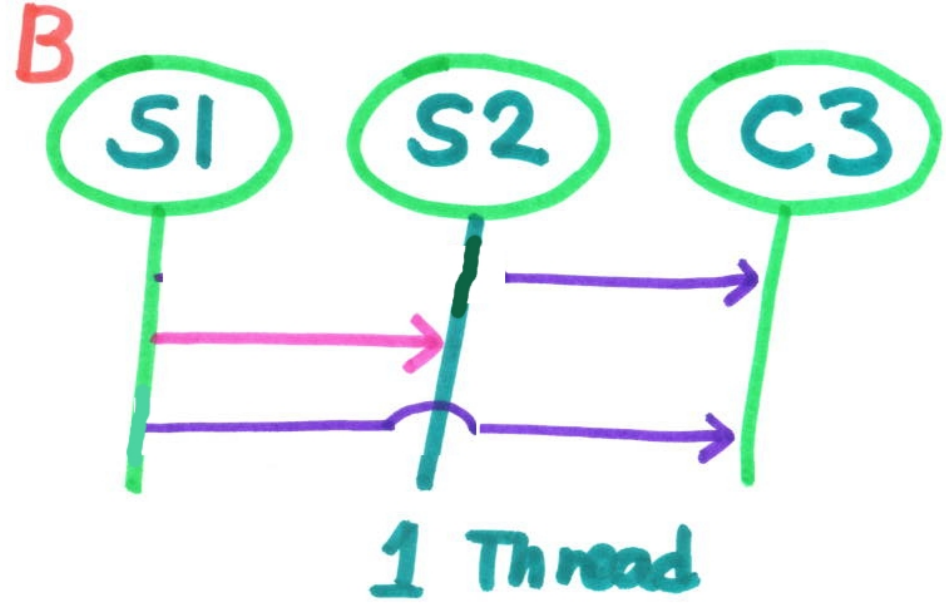


$$G1 = 1 \to 3 : \langle Nat \rangle . 2 \to 3 : \langle Nat \rangle . \mathrm{end}$$

$$G2 = 1 \to 2 : \langle Bool \rangle . \mathrm{end}$$

Example Resource Management





$$G2 = 1 \to 2 : \langle Bool \rangle . end$$

$$G3 = 2 \to 3 : \langle Nat \rangle . 1 \to 3 : \langle Nat \rangle . end$$

Reasoning

$$E_1 = \begin{array}{l} s : 1 \to 3 : \langle \mathsf{Nat} \rangle .\ \underline{2 \to 3 : \langle \mathsf{Nat} \rangle} .\ \mathsf{end} \\ s' : 1 \to 2 : \langle \mathsf{Bool} \rangle .\ \mathsf{end} \end{array}$$

$$E_2 = \begin{array}{l} s : \underline{2 \to 3 : \langle \mathsf{Nat} \rangle} .\ 1 \to 3 : \langle \mathsf{Nat} \rangle .\ \mathsf{end} \\ s' : 1 \to 2 : \langle \mathsf{Bool} \rangle .\ \mathsf{end} \end{array}$$

$$E_1, \Gamma \vdash P_1 \mid P_2 \triangleright \Delta \qquad E_1, \Gamma \vdash P_1 \mid R \triangleright \Delta$$

$$E_2, \Gamma \vdash P_1 \mid P_2 \triangleright \Delta \qquad E_2, \Gamma \vdash P_1 \mid R \triangleright \Delta$$

$$E_1 \not\xrightarrow{2 \to 3} \qquad\qquad E_2 \xrightarrow{2 \to 3}$$

Reasoning

$$E_1 = s: 1 \to 3: \langle Nat \rangle . \underline{2 \to 3: \langle Nat \rangle} . \mathsf{end}$$
$$\quad\quad s': 1 \to 2: \langle Bool \rangle . \mathsf{end}$$

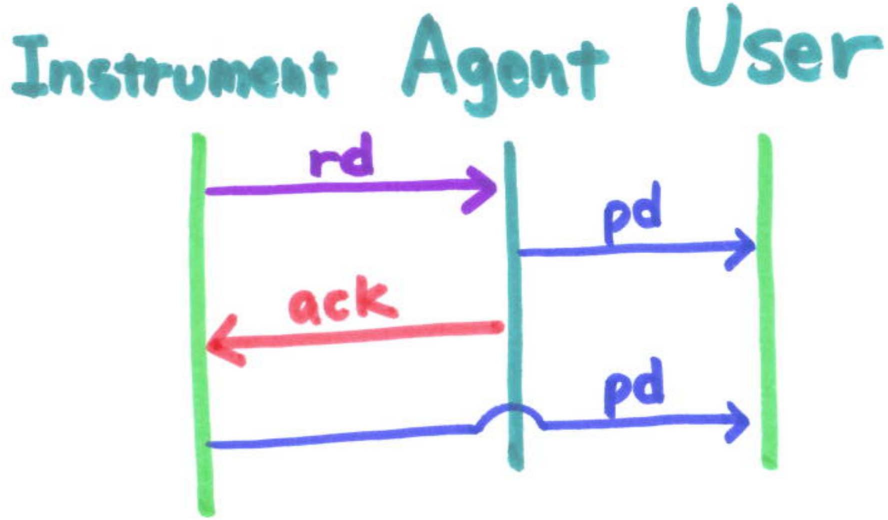
$$E_2 = s: \underline{2 \to 3: \langle Nat \rangle} . 1 \to 3: \langle Nat \rangle . \mathsf{end}$$
$$\quad\quad s': 1 \to 2: \langle Bool \rangle . \mathsf{end}$$

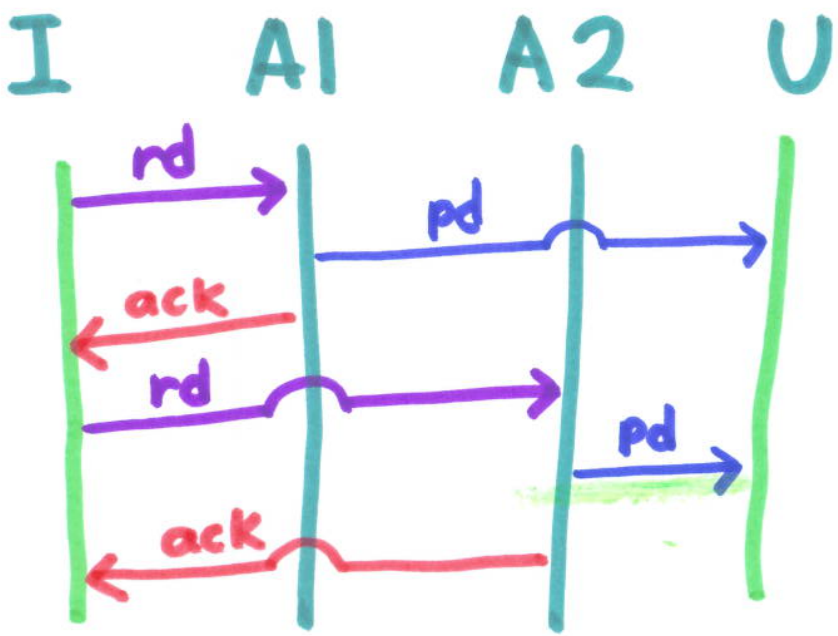
$$E_1, \Gamma \vdash P_1 \mid P_2 \triangleright \Delta \approx_g E_1, \Gamma \vdash P_1 \mid R \triangleright \Delta$$

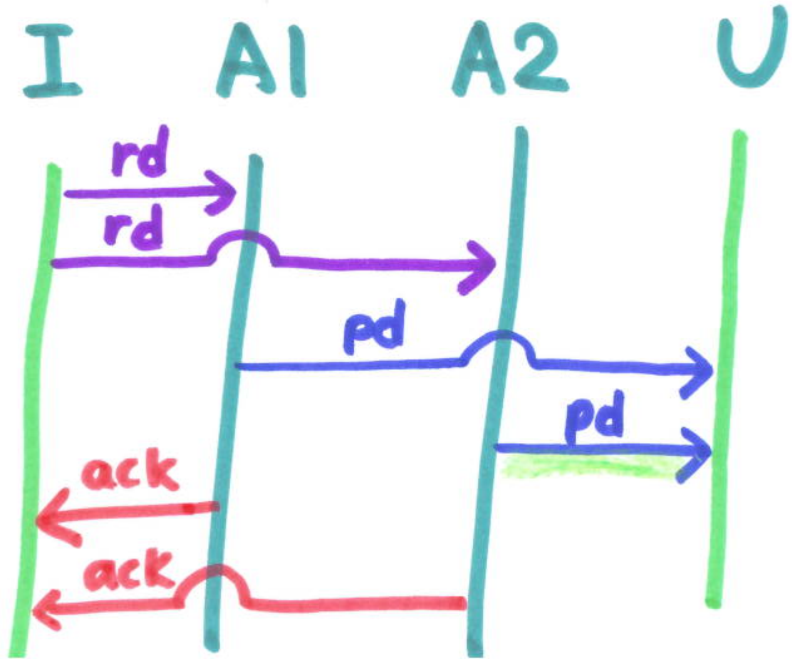
$$E_2, \Gamma \vdash P_1 \mid P_2 \triangleright \Delta \not\approx_g E_2, \Gamma \vdash P_1 \mid R \triangleright \Delta$$

$$E_1 \not\xrightarrow{2 \to 3} \qquad\qquad E_2 \xrightarrow{2 \to 3}$$

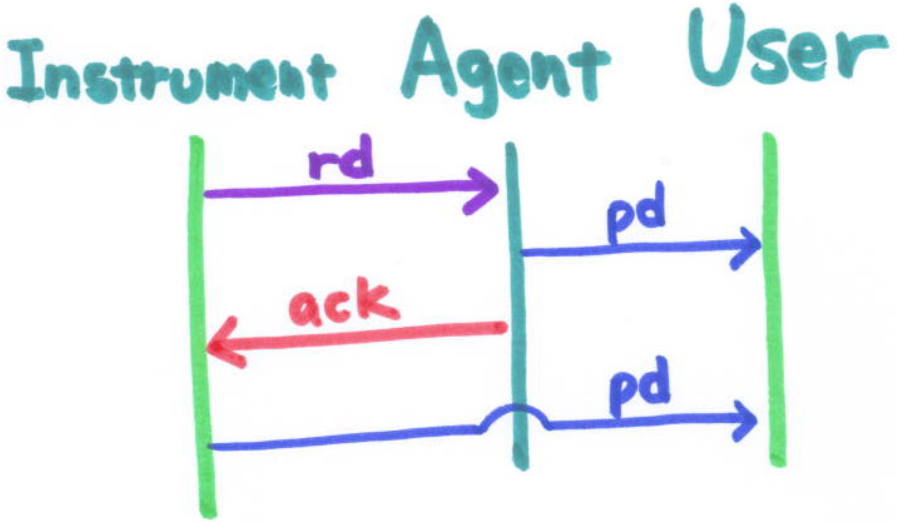
Usecase : UC. R2. 13 "Acquire Data from Instrument" from Ocean Observatories Initiative (OOI)



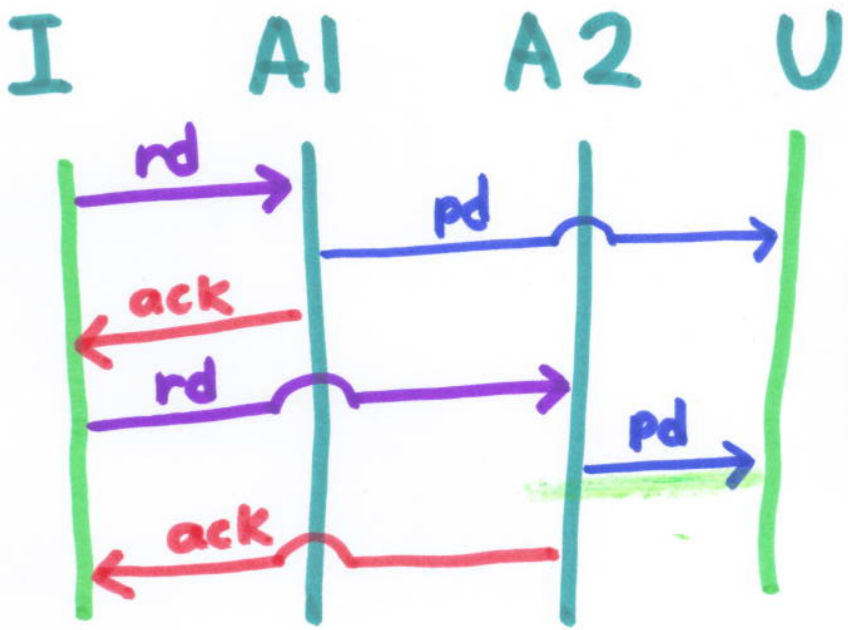




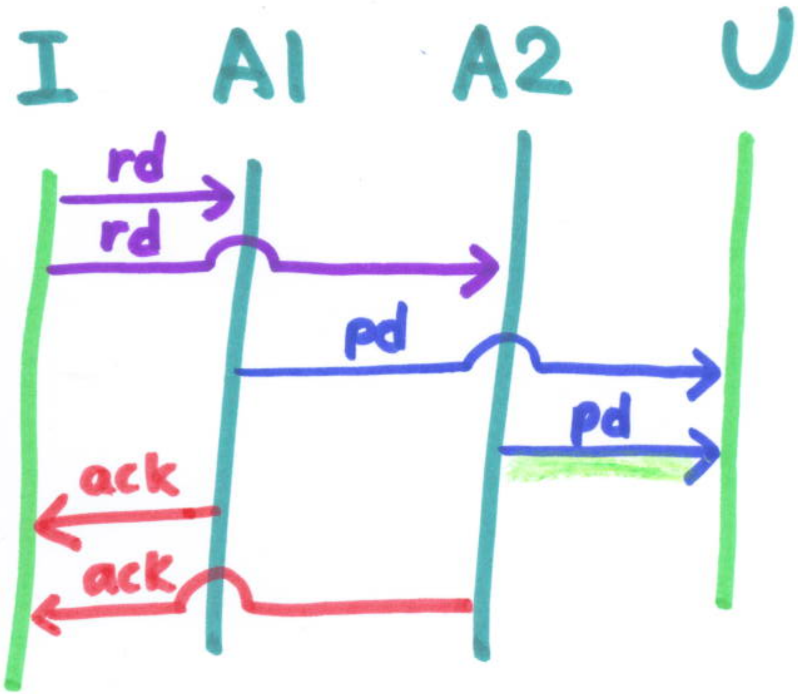
Usecase : UC.R2.13 "Acquire Data from Instrument" from Ocean Observatories Initiative (OOI)



$A1 \to U : \langle pd \rangle.$
$A2 \to U : \langle pd \rangle.$
end



$\approx_g$



Conclusions

- We define a standard multiparty session bisimulation $\approx_s$ and the governed bisimulation $\approx_g$ and prove both are compositional and coincide with reduction closed semantics.
- We show when $\approx_s$ and $\approx_g$ coincide and differ
- We apply $\approx_g$ to a real usecase for a large scale cyberinfrustructure.

Related Work

1. Binary Asynchronous Eventful Session Semantics
   FORTE/FMOODS '11, MSCS, DK's PhD Thesis

2. Environment Bisimulation
   Hennessy & Rathke '04 dictator ⟷ coordinator

Future Work

- Asynchronous Semantics
  $E \xrightarrow{\ell} E'$ (modular)

- Tool · Semantic Correspondence

Reduction-closed congruence

Barb

$\Gamma \vdash P \triangleright \Delta \downarrow s[p][q]$ $\quad P \equiv (\nu\, \tilde{a}\tilde{s})(s[p][q]!\langle v\rangle; R \mid Q)$

if $\quad s \notin \tilde{s} \quad \underline{s[q] \notin \mathrm{dom}(\Delta)}$

$\Gamma \vdash P \triangleright \Delta \downarrow a$ $\quad P \equiv (\nu\, \tilde{a}\tilde{s})(\bar{a}[n](x).R \mid Q)$

if $\quad a \notin \tilde{a}$

$\mathcal{R}$ is reduction-closed congruence if

1. $\Gamma \vdash P_1 \triangleright \Delta_1 \Downarrow m$ iff $\Gamma \vdash P_2 \triangleright \Delta_2 \Downarrow m$
2. Whenever $\Gamma \vdash P_1 \triangleright \Delta_1 \,\mathcal{R}\, P_2 \triangleright \Delta_2$ holds, $P_1 \twoheadrightarrow P_1'$ implies $P_2 \twoheadrightarrow P_2'$ and $\Gamma \vdash P_2 \triangleright \Delta_2$ with $\Gamma \vdash P_1' \triangleright \Delta_1' \,\mathcal{R}\, P_2' \triangleright \Delta_2'$
3. $\mathcal{R}$ is a congruence

$\cong_s$ max relation

Witness $E ::= \emptyset \mid E \cdot s{:}G$

LTS $E \xrightarrow{\lambda} E'$

$$\lambda ::= s : p \to q : U \mid s : p \to q : l$$

- $s : p \to q : \langle U \rangle . G \xrightarrow{s : p \to q : U} G$

- $$\frac{s : G \xrightarrow{\lambda} s : G' \qquad p, q \notin \lambda}{s : p \to q : \langle U \rangle . G \xrightarrow{\lambda} s : p \to q : \langle U \rangle . G'}$$