Inference of Global Progress Properties for Dynamically Interleaved Multiparty Sessions

Mario Coppo[1] Mariangiola Dezani-Ciancaglini[1]
Luca Padovani[1] Nobuko Yoshida[2]

[1] Dipartimento di Informatica, Università di Torino, Italy
[2] Department of Computing, Imperial College London, UK

BEAT 2013

The problem

$$a(y).b(z).y?(x).z!\langle x\rangle$$

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

- two distinct sessions
- each session is well typed
- the system gets stuck

The problem

$$a(y).b(z).y?(x).z!\langle x\rangle \qquad y : ?\texttt{int} \qquad z : !\texttt{int}$$

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \qquad y : !\texttt{int} \qquad z : ?\texttt{int}$$

- two distinct sessions
- each session is well typed
- the system gets stuck

The “interaction” type system

If $\vdash P$, then P never gets stuck

- ☺ Bettini, Coppo, D’Antoni, De Luca, Dezani-Ciancaglini, Yoshida, **Global Progress in Dynamically Interleaved Multiparty Sessions**, CONCUR 2008
- ☹ **not syntax-directed**

Outline

1. Progress
2. Key ideas of the type system
3. Two examples
4. Remarks

Progress 1/2

$$\begin{array}{rl} \text{If} & P \rightarrow^* \mathcal{E}\,[\; s?(x).P' \;] \\ \text{Then} & \rightarrow^* \mathcal{E}'[\; s?(x).P' \mid s : m \cdot h \;] \end{array}$$

$$\begin{array}{rl} \text{If} & P \rightarrow^* \mathcal{E}\,[\; s : m \cdot h \;] \\ \text{Then} & \rightarrow^* \mathcal{E}'[\; s : m \cdot h \mid s?(x).P' \;] \end{array}$$

A process without progress

$$a(y).b(z).y?(x).z!\langle x\rangle \mid \overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

A process without progress

$$a(y).b(z).y?(x).z!\langle x\rangle \mid \overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

$$\downarrow_*$$

$$(\nu s)(\nu s')(s?(x).s'!\langle x\rangle \mid s'?(x).s!\langle c\rangle \mid s : \emptyset \mid s' : \emptyset)$$

A process without progress

$$a(y).b(z).y?(x).z!\langle x\rangle \mid \overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

$$\downarrow_*$$

$$(\nu s)(\nu s')(s?(x).s'!\langle x\rangle \mid s'?(x).s!\langle c\rangle \mid s : \emptyset \mid s' : \emptyset)$$

Progress 2/2

A **good** process that looks like a **bad** one

$$P \rightarrow^* \mathcal{E}[\ s?(x).P' \mid \overline{b}(y).s!\langle 3\rangle.Q'\ ]$$

A **bad** process that looks like a **good** one

$$c(y).(\text{a process that gets stuck})$$

Progress 2/2

A **good** process that looks like a **bad** one

$$P \rightarrow^* \mathcal{E}[\ s?(x).P' \mid \overline{b}(y).s!\langle 3\rangle.Q'\ ]$$

A **bad** process that looks like a **good** one

$$c(y).(\text{a process that gets stuck})$$

Idea

- define progress modulo **catalyzers**
- catalyzer = missing participant that never gets stuck

Consequence

- session initiation can be considered non-blocking

Interaction type system: basic ideas

1. associate processes with dependencies $a \prec b$

   "an action of service a blocks an action of service b"

2. a process is well typed if it yields no circular dependencies

Computing service dependencies

$$a(y).b(z).y?(x).z!\langle x\rangle \qquad a \prec b$$

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \qquad b \prec a$$

Service names as messages

$$a(y).b(z).y?(x).z!\langle x\rangle \qquad a \prec b$$

$$\overline{c}(t).t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

$$c(t).t!\langle a\rangle$$

Service names as messages

$$a(y).b(z).y?(x).z!\langle x\rangle \qquad a \prec b$$

$$t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

$$t!\langle a\rangle$$

Service names as messages

$$a(y).b(z).y?(x).z!\langle x\rangle \qquad a \prec b$$

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \qquad b \prec a$$

Service names as messages

$$a(y).b(z).y?(x).z!\langle x\rangle \qquad a \prec b$$

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

Idea

- identify a class of safe services even if mutually dependent
- restrict messages to services in this class

Nested services

Definition

a is a nested service if $\lambda \prec a$ implies that λ is a nested service

		Nested?
$\overline{a}(y).\overline{a}(z).z?(x).y?(x')$	$a \prec a$	✔
$\overline{a}(y).\overline{b}(z).z?(x).y?(x')$ $\mid \overline{b}(z).\overline{a}(y).y?(x).z?(x')$	$b \prec a$ $a \prec b$	✔
$\overline{a}(y).\overline{b}(z).y?(x).z?(x')$	$y \prec b$	✖

Private services

$$a(y).(\nu\, b)(b(z).z?(x).y!\langle x\rangle)$$

- no catalyzer can help starting the session on b

Private services

$$a(y).(\nu\, b)(b(z).z?(x).y!\langle x\rangle)$$

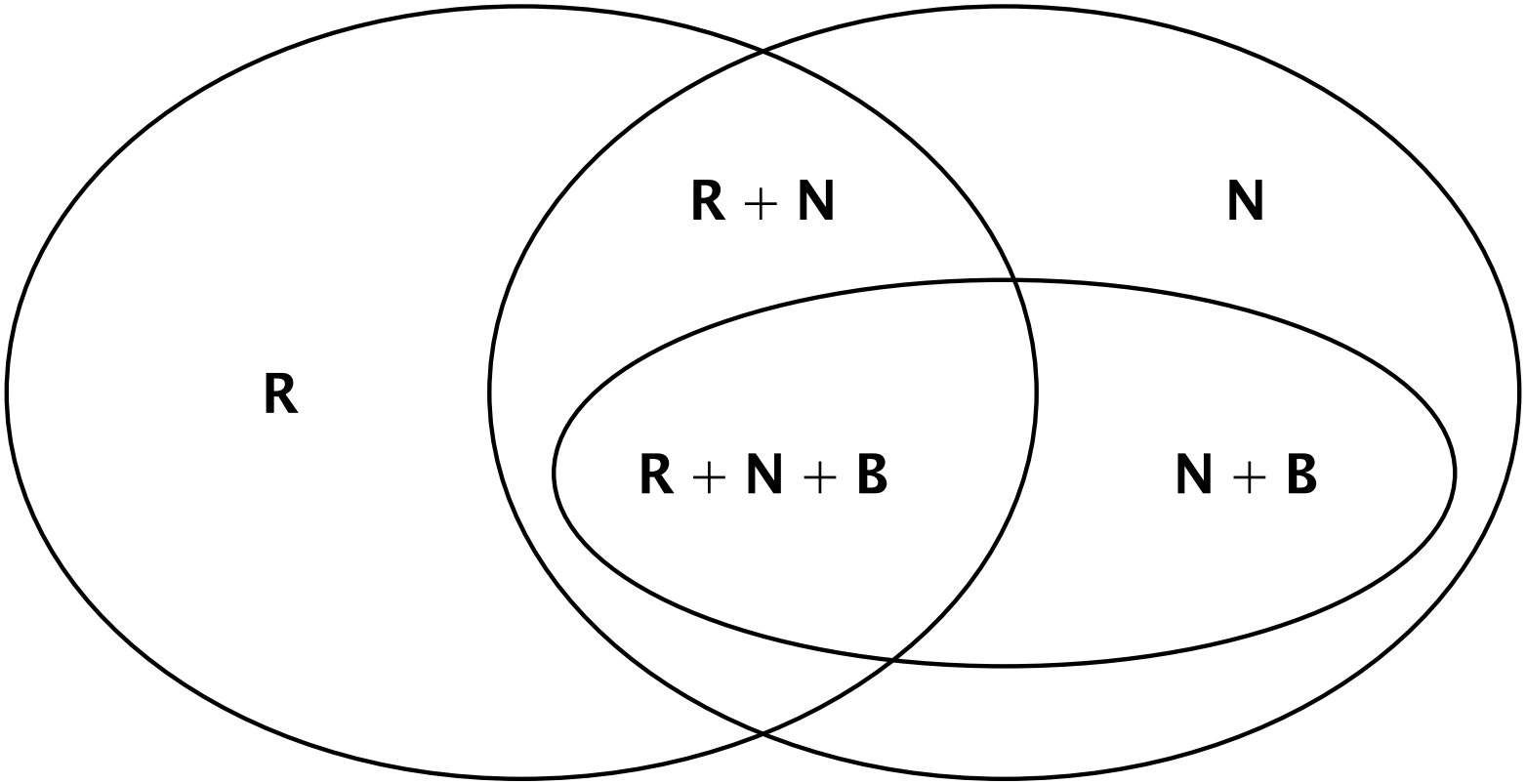
- no catalyzer can help starting the session on b

Definition

a is boundable if it is never followed by free channels

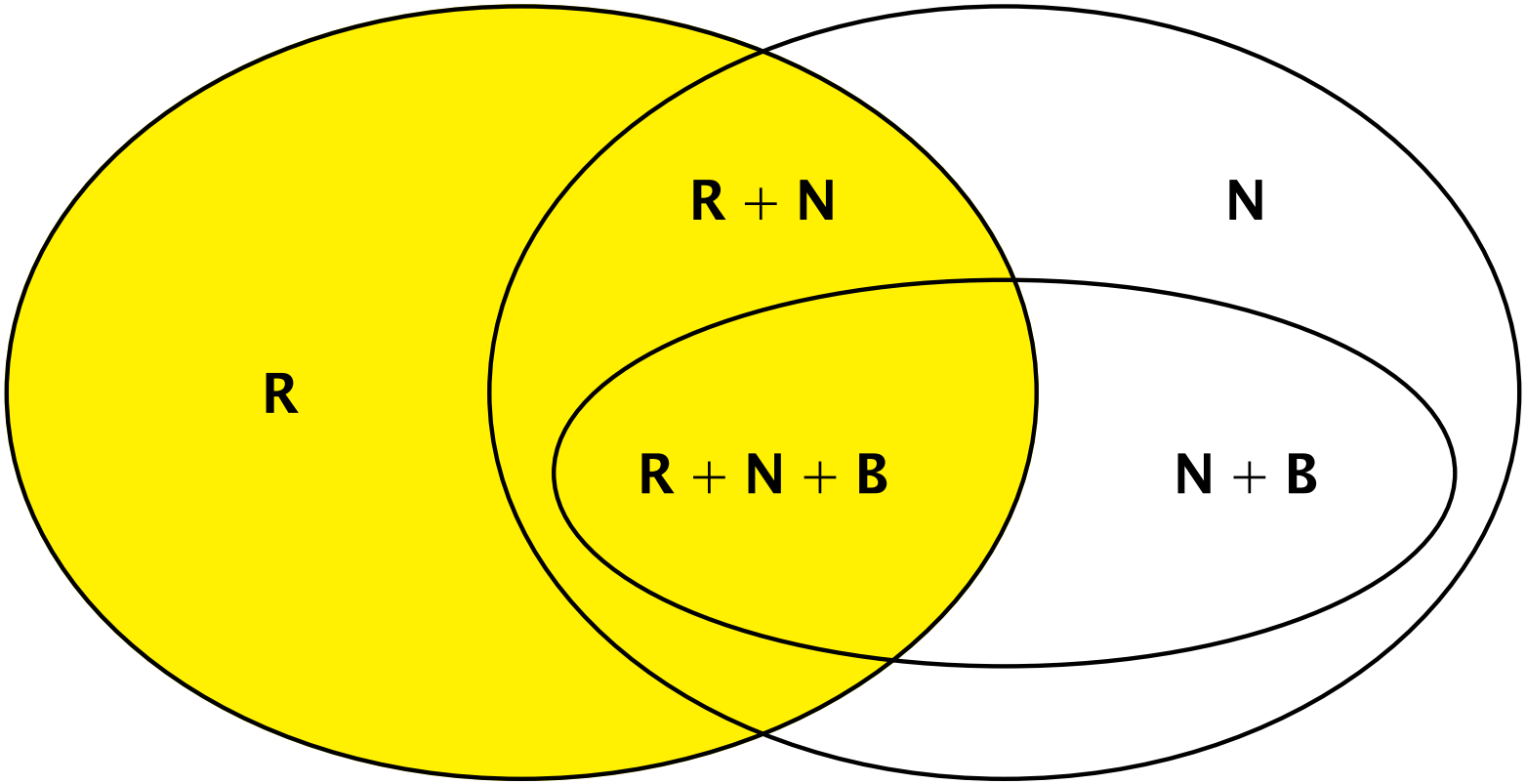
- b is nested but not boundable

Service classification



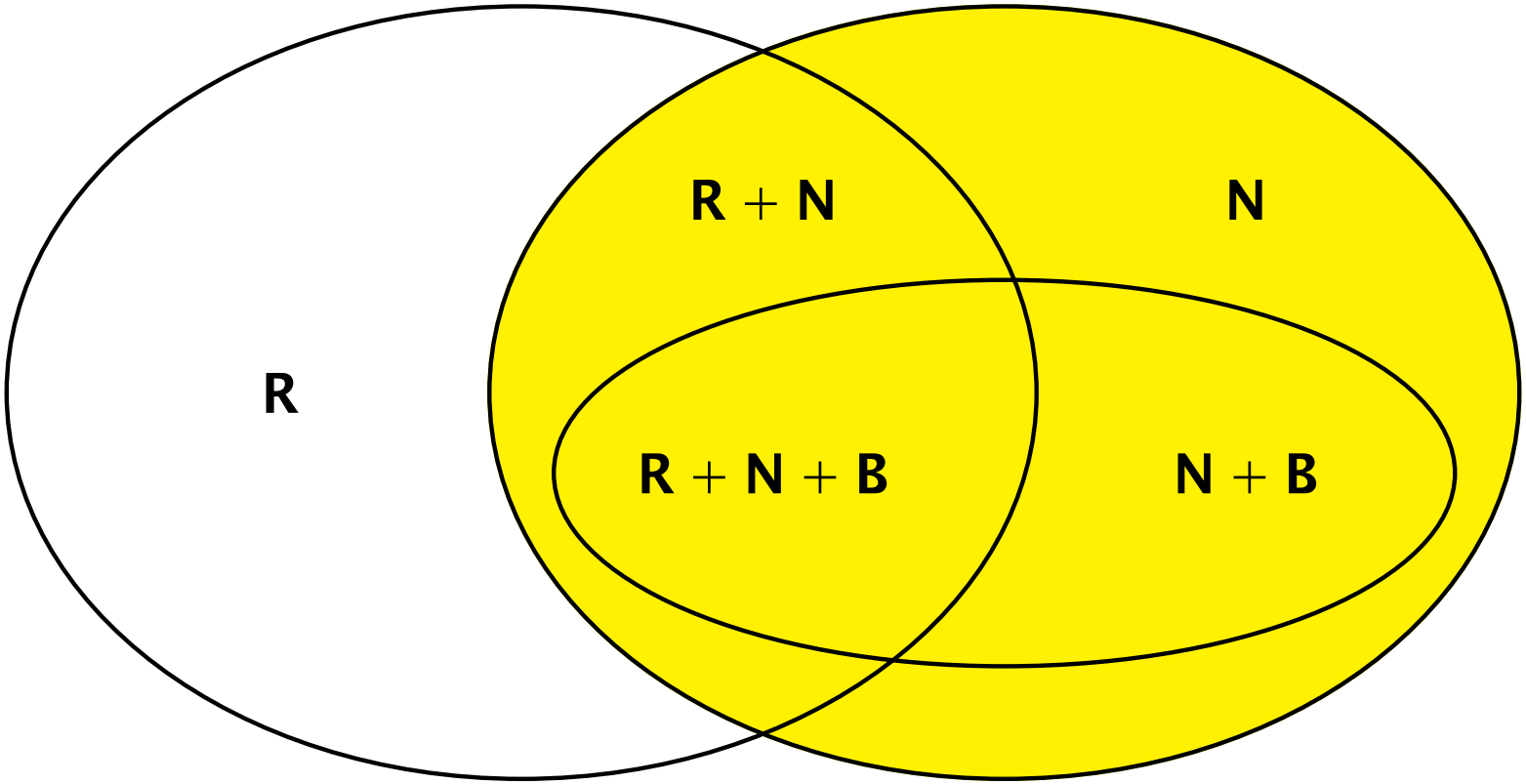
- each service can have up to three features . . .
- . . . which the interaction type system guesses

Service classification



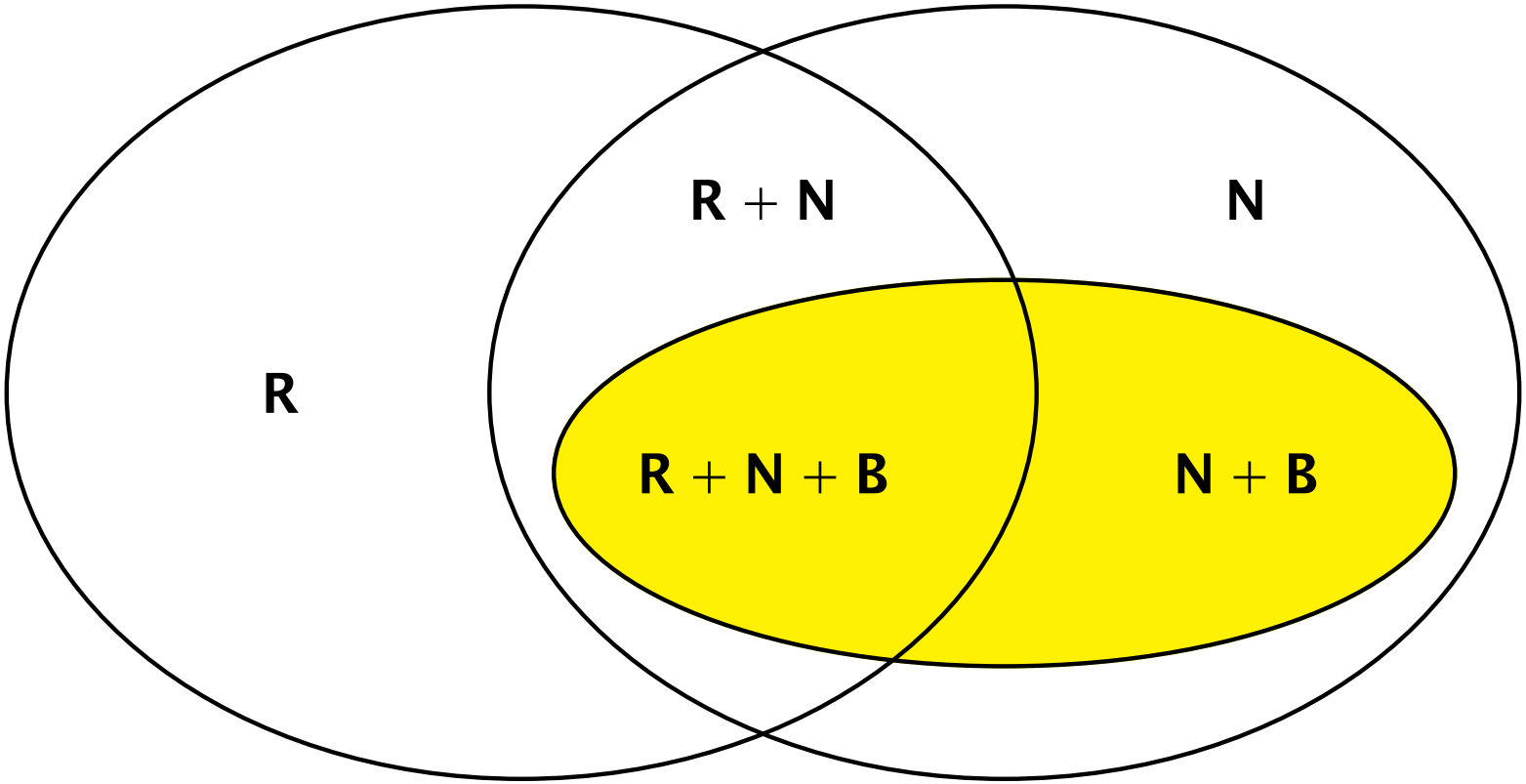
- each service can have up to three features . . .
- . . . which the interaction type system guesses

Service classification



- each service can have up to three features . . .
- . . . which the interaction type system guesses

Service classification



- each service can have up to three features . . .
- . . . which the interaction type system guesses

Algorithm judgments

$$P \Mapsto \mathsf{D}; \mathsf{R}; \mathsf{N}; \mathsf{B}$$

If. . .

$$\begin{array}{rcl} \mathsf{D}^{\infty} & \subseteq & \mathsf{N} \setminus \mathsf{R} \\ \mathsf{D} \downarrow \mathsf{N} & \subseteq & \mathsf{N} \\ \mathsf{fs}(P) & \subseteq & \mathsf{R} \cup \mathsf{N} \end{array}$$

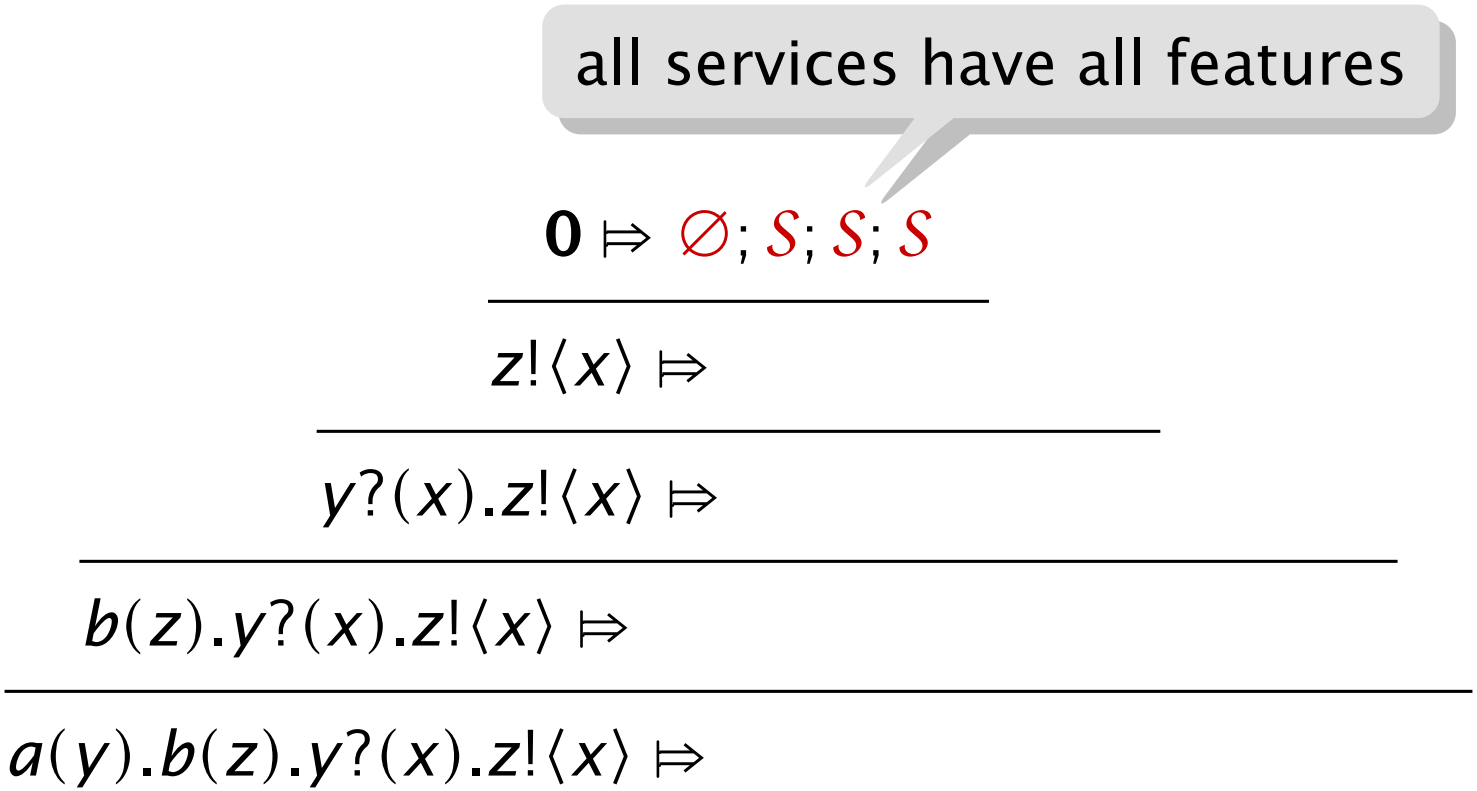
Example 1

$a(y).b(z).y?(x).z!\langle x\rangle \Mapsto$

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto}{z!\langle x\rangle \Mapsto}}{y?(x).z!\langle x\rangle \Mapsto}}{b(z).y?(x).z!\langle x\rangle \Mapsto}}{a(y).b(z).y?(x).z!\langle x\rangle \Mapsto}$$

Example 1


all services have all features
$\mathbf{0} \Vdash \emptyset; S; S; S$
$z!\langle x\rangle \Vdash$
$y?(x).z!\langle x\rangle \Vdash$
$b(z).y?(x).z!\langle x\rangle \Vdash$
$a(y).b(z).y?(x).z!\langle x\rangle \Vdash$

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Vdash \emptyset; S; S; S}{z!\langle x\rangle \Vdash \emptyset; S; S; S}}{y?(x).z!\langle x\rangle \Vdash}}{b(z).y?(x).z!\langle x\rangle \Vdash}}{a(y).b(z).y?(x).z!\langle x\rangle \Vdash}$$

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \emptyset; S; S; S}{z!\langle x\rangle \Mapsto \emptyset; S; S; S}}{y?(x).z!\langle x\rangle \Mapsto \{y \prec z\}; S; S; S}}{b(z).y?(x).z!\langle x\rangle \Mapsto}}{a(y).b(z).y?(x).z!\langle x\rangle \Mapsto}$$

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \emptyset; S; S; S}{z!\langle x\rangle \Mapsto \emptyset; S; S; S}}{y?(x).z!\langle x\rangle \Mapsto \{y \prec z\}; S; S; S}}{b(z).y?(x).z!\langle x\rangle \Mapsto \{y \prec b\}; S; S \setminus \{b\}; S \setminus \{b\}}}{a(y).b(z).y?(x).z!\langle x\rangle \Mapsto}$$

B ⊆ N

D ↓ N ⊆ N

Example 1

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \emptyset; S; S; S}{z!\langle x\rangle \Mapsto \emptyset; S; S; S}}{y?(x).z!\langle x\rangle \Mapsto \{y \prec z\}; S; S; S}}{b(z).y?(x).z!\langle x\rangle \Mapsto \{y \prec b\}; S; S \setminus \{b\}; S \setminus \{b\}}}{a(y).b(z).y?(x).z!\langle x\rangle \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\}}$$

Example 1 (cont.)

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle$$

$$a(y)\cdots \mid \overline{a}(y)\cdots \Rightarrow$$

Example 1 (cont.)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \emptyset; S; S; S}{y!\langle x\rangle \Mapsto \emptyset; S; S; S}}{z?(x).y!\langle x\rangle \Mapsto \{z \prec y\}; S; S; S}}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec a\}; S; S; S}$$

$a(y) \cdots \mid \overline{a}(y) \cdots \Mapsto$

Example 1 (cont.)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \emptyset; S; S; S}{y!\langle x\rangle \Mapsto \emptyset; S; S; S}}{z?(x).y!\langle x\rangle \Mapsto \{z \prec y\}; S; S; S}}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec a\}; S; S; S}$$

$$\dfrac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\}}{a(y)\cdots \mid \overline{a}(y)\cdots \Mapsto}$$

Example 1 (cont.)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \varnothing; S; S; S}{y!\langle x\rangle \Mapsto \varnothing; S; S; S}}{z?(x).y!\langle x\rangle \Mapsto \{z \prec y\}; S; S; S}}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec a\}; S; S; S}$$

$$\dfrac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{a}(y)\cdots \Mapsto \{b \prec a\}; S; S; S}{a(y)\cdots \mid \overline{a}(y)\cdots \Mapsto}$$

Example 1 (cont.)

$$\mathbf{0} \Mapsto \emptyset; S; S; S$$

$$y!\langle x\rangle \Mapsto \emptyset; S; S; S$$

$$z?(x).y!\langle x\rangle \Mapsto \{z \prec y\}; S; S; S$$

$$\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S$$

$$\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec a\}; S; S; S$$

$$a(y)\cdot\cdot\cdot \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{a}(\cdot)\cdot\cdot\cdot \Mapsto \{\cdot \prec a\}; S; S; S$$

$$a(y)\cdot\cdot\cdot \mid \overline{a}(y)\cdot\cdot\cdot \Mapsto \{a \prec b, b \prec a\}; S \setminus \{a, b\}; S \setminus \{b\}; S \setminus \{b\}$$

$D^{\infty} \subseteq N \setminus R$

Example 1 (cont.)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\mathbf{0} \Mapsto \emptyset; S; S; S}{y!\langle x\rangle \Mapsto \emptyset; S; S; S}}{z?(x).y!\langle x\rangle \Mapsto \{z \prec y\}; S; S; S}}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{a}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec a\}; S; S; S}$$

$$\dfrac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{a}(y)\cdots \Mapsto \{b \prec a\}; S; S; S}{a(y)\cdots \mid \overline{a}(y)\cdots \Mapsto \{a \prec b, b \prec a\}; S \setminus \{a, b\}; S \setminus \{b\}; S \setminus \{b\}}$$

Example 2

$$\overline{c}(t).t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto$$

$$a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{c}(t)\cdots \Mapsto \emptyset; S \setminus \{b\}; S; S$$

$$a(y)\cdots \mid \overline{c}(t)\cdots \Mapsto \{a \prec b\}; S \setminus \{b\}; S \setminus \{b\}; S \setminus \{b\}$$

Example 2

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto}}{t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto}}{\overline{c}(t).t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto}$$

$$\dfrac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{c}(t)\cdots \Mapsto \emptyset; S \setminus \{b\}; S; S}{a(y)\cdots \mid \overline{c}(t)\cdots \Mapsto \{a \prec b\}; S \setminus \{b\}; S \setminus \{b\}; S \setminus \{b\}}$$

Example 2

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}}{t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto}}{\overline{c}(t).t?(x).\overline{x}(y).b(z).z?(x).y!\langle x\rangle \Mapsto}$$

x must be nested, so b too

dependencies discharged

$$\dfrac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{c}(t)\cdots \Mapsto \emptyset; S \setminus \{b\}; S; S}{a(y)\cdots \mid \overline{c}(t)\cdots \Mapsto \{a \prec b\}; S \setminus \{b\}; S \setminus \{b\}; S \setminus \{b\}}$$

Example 2

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}}{\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}}{t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}}{\overline{c}(t).t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}$$

$$\dfrac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{c}(t)\cdots \Mapsto \emptyset; S \setminus \{b\}; S; S}{a(y)\cdots \mid \overline{c}(t)\cdots \Mapsto \{a \prec b\}; S \setminus \{b\}; S \setminus \{b\}; S \setminus \{b\}}$$

Example 2

$$\vdots$$

$$\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S$$

$$\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S$$

$$t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S$$

$$\overline{c}(t).t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S$$

$$\frac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{c}(t)\cdots \Mapsto \emptyset; S \setminus \{b\}; S; S}{a(y)\cdots \mid \overline{c}(t)\cdots \Mapsto \{a \prec b\}; S \setminus \{b\}; S \setminus \{b\}; S \setminus \{b\}}$$

Example 2

$$\vdots$$

$$\frac{\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \{b \prec y\}; S; S; S}{\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}$$

$$\frac{t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}{\overline{c}(t).t?(x).\overline{x}(y).\overline{b}(z).z?(x).y!\langle x\rangle \Mapsto \emptyset; S \setminus \{b\}; S; S}$$

$$\frac{a(y)\cdots \Mapsto \{a \prec b\}; S; S \setminus \{b\}; S \setminus \{b\} \quad \overline{c}(t)\cdots \Mapsto \emptyset; S \setminus \{b\}; S; S}{a(y)\cdots \mid \overline{c}(t)\cdots \Mapsto \{a \prec b\}; S \setminus \{b\}; S \setminus \{b\}; S \setminus \{b\}}$$

Result

Theorem

If $P \Mapsto \mathsf{D}; \mathsf{R}; \mathsf{N}; \mathsf{B}$, *then* P *has progress*

Proof.

The algorithm is sound and complete wrt the inference type system (cf. CONCUR 2008) □

Result

Theorem

If $P \Mapsto \mathsf{D}; \mathsf{R}; \mathsf{N}; \mathsf{B}$, *then* P *has progress*

Proof.

The algorithm is sound and complete wrt the inference type system (cf. CONCUR 2008) (for finite processes only) □

Soon to come

Inference for recursive processes

Wrap up

- static analysis for (multiparty) session interleaving
- progress $\neq$ absence of deadlock
  - diverging systems do not necessarily have progress
  - catalyzers may help reduction
- efficient inference algorithm

Future work

- many simple program patterns are **ill typed**
  - ☛ more flexible type discipline is required
- π-calculus $\neq$ **programming language**
  - ☛ richer/more compositional types are needed
- type systems for liveness properties are **complex**
  - ☛ traditional concepts/techniques (fairness, subtyping, coinductive reasoning, ...) must be revisited

A simple ill-typed process with progress

$$\begin{array}{ll}
\texttt{def } X(y,z) = y!\langle 3\rangle.z?(x).X(y,z) \texttt{ in} & b \prec a \\
\texttt{def } Y(y,z) = y?(x).z!\langle x\rangle.Y(y,z) \texttt{ in} & a \prec b \\
a(y).b(z).X(y,z) \mid \overline{a}(y).\overline{b}(z).Y(y,z) &
\end{array}$$