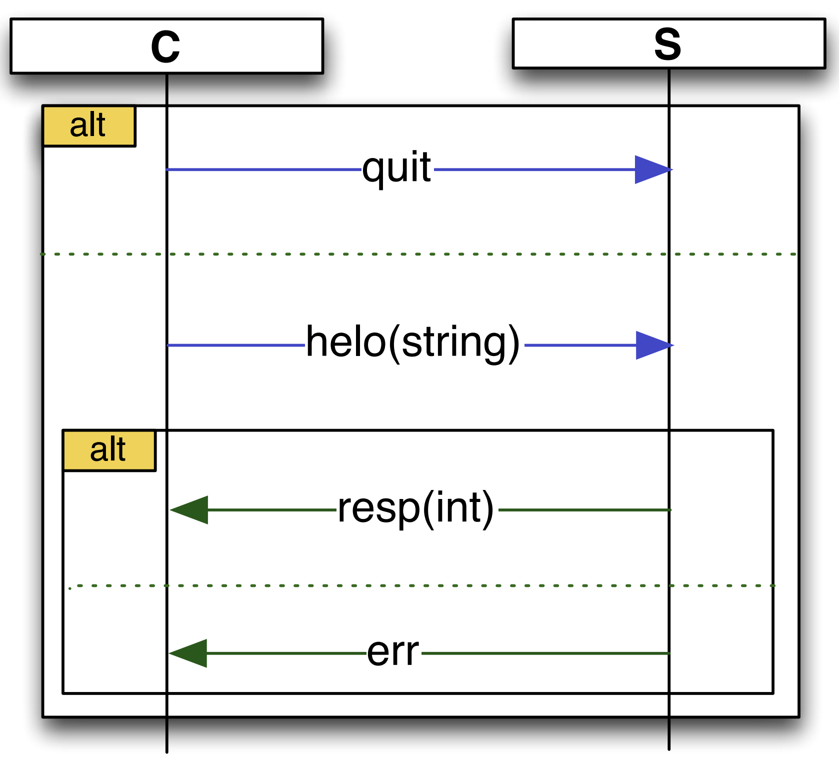
Resolving Non-Determinism in Choreographies

to appear in ESOP 2014

Laura Bocchi
Imperial College London
with Hernán Melgratti (University of Buenos Aires) & Emilio Tuosto (University of Leicester)

Choreography vs Realisation

"Using the Web Services Choreography specification, a contract containing a global definition of the common ordering conditions and constraints under which messages are exchanged, is produced [...]. Each party can then use the global definition to build and test solutions that conform to it. The global specification is in turn realised by combination of the resulting local systems [...]" [WS-CDL]



[Post Office Protocol (POP2), rfc 937]

Partial vs Complete Realisation

Choreography as a constraint

partial realisation

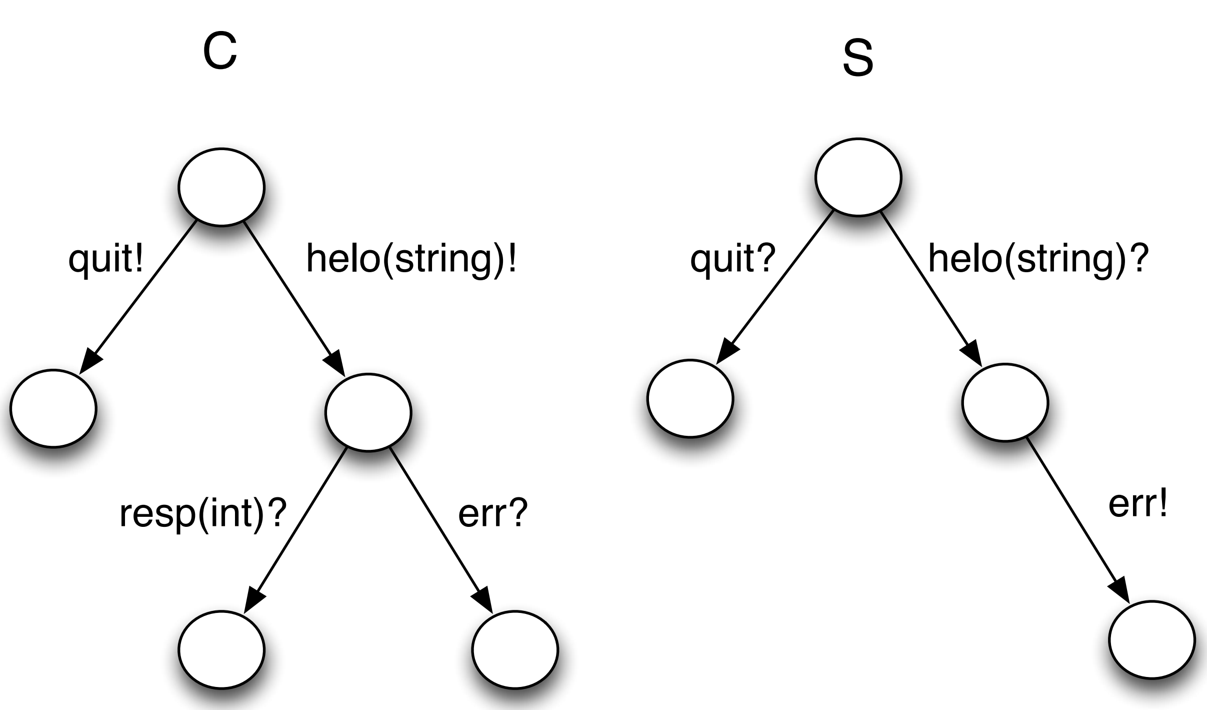
exhibits some of the some of the interaction sequences specified in the choreography

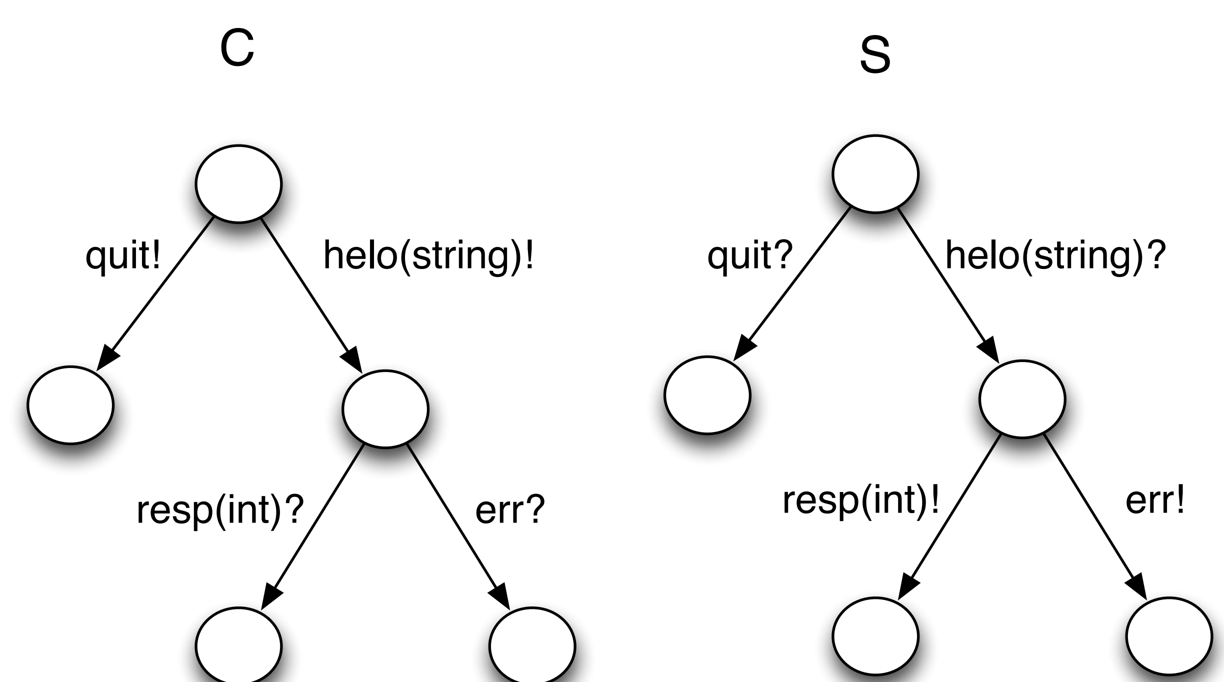
Choreography as an obligation

complete realisation

is able to exhibit all interaction sequences

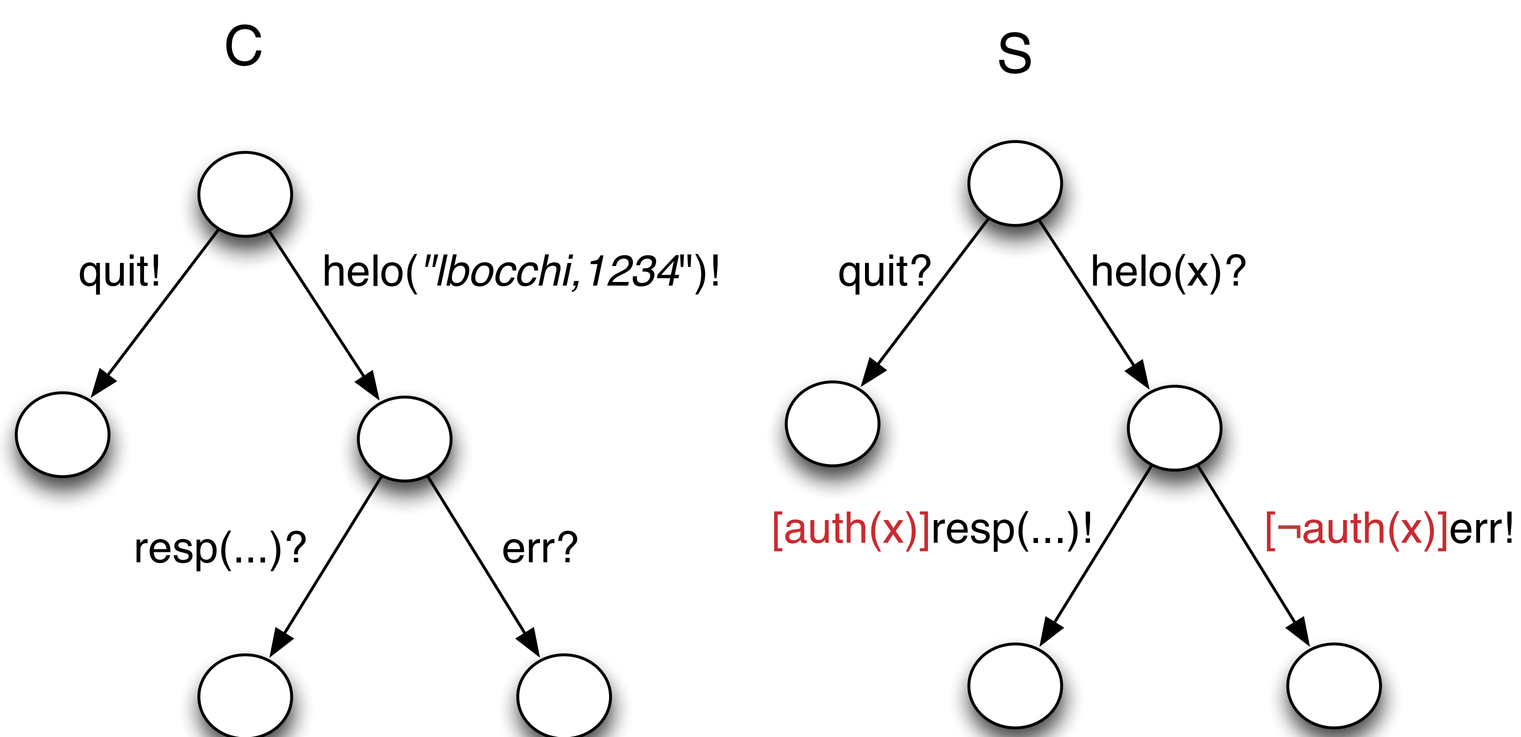
[Su, Bultan, Fu, WSFM'07]
[Lohmann, Wolf, ICSOC'11]
[Castagna, Dezani-Ciancaglini, Padovani, FORTE'11]





The Problem

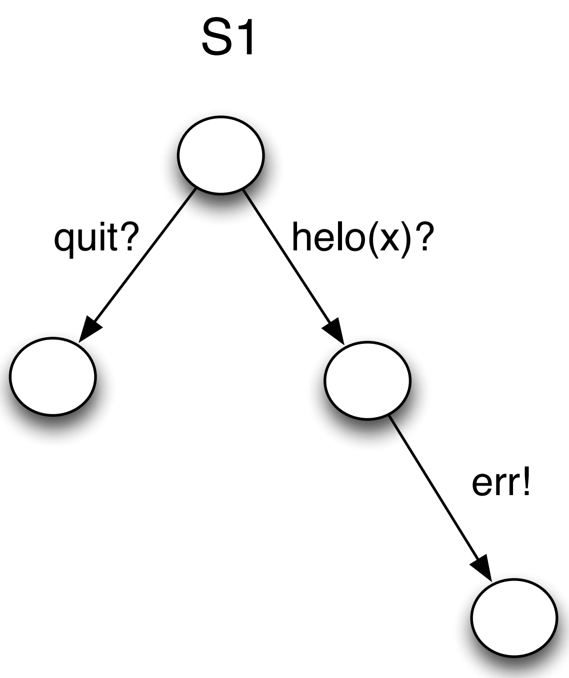
- These notions have been discussed in scenarios where choices in both choreographies and realisations are *non-deterministic*
- Open issue: defining completeness for deterministic realisations

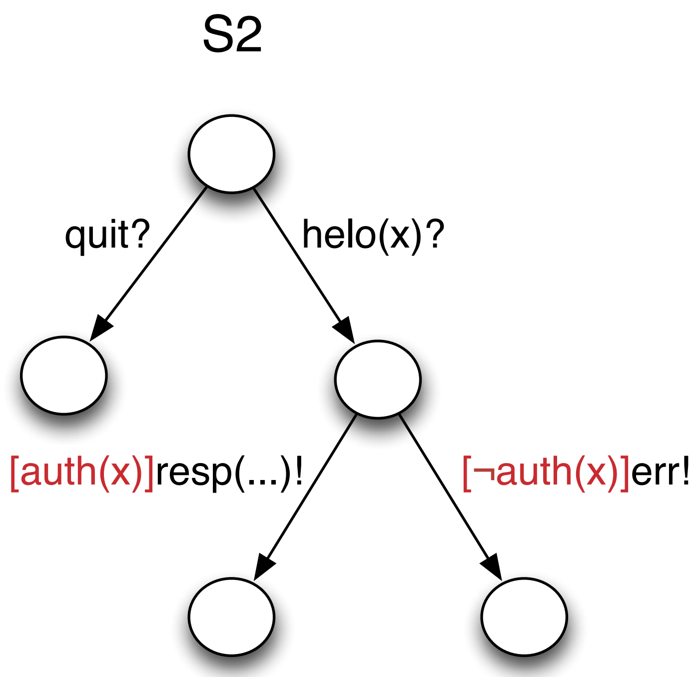


Choreography as a constraint	Choreography as an obligation
partial realisation	***complete realisation***
✓	✗

Two Partial Realisations

Let us focus on one single participant at a time:





Systematically precludes a choice

The choice depends on the partner

We want a definition of complete implementation that

- Expresses the "obligation" perspective of choreographies
- Discards S1 and accepts S2

Whole-spectrum implementation

The implementation P of a participant in a choreography G is whole-spectrum when for each internal choice in G and for each option of this choice, there exists a context for P for which this choice is met and this option is taken

- Choreographies are modeled as ***global types***
- Implementations are modeled as (session-pi-like) ***processes***
- The semantics of choreographies and implementations is given as **runs** (i.e., sets of traces with *mandatory* and *optional* actions)
- *Whole-spectrum implementation (WSI)* is given in terms of a partial order between runs

Choreographies as Global Types

Global Type

$$\mathtt{G} \;::=\; \mathtt{p} \to \mathtt{q} : y\langle \mathtt{U} \rangle \;\mid\; \mathtt{G} + \mathtt{G} \;\mid\; \mathtt{G} \mid \mathtt{G} \;\mid\; \mathtt{G};\mathtt{G} \;\mid\; \mathtt{G}^* \;\mid\; \mathtt{end}$$

Example [Post Office Protocol (POP2)]

$$\mathtt{G}_{\mathtt{POP}} = \mathtt{C} \to \mathtt{S} : \mathtt{QUIT}\,\langle\rangle; \mathtt{G}_{\mathtt{EXIT}} + \mathtt{C} \to \mathtt{S} : \mathtt{HELO}\,\langle \mathtt{String} \rangle; \mathtt{G}_{\mathtt{MBOX}}$$

$$\mathtt{G}_{\mathtt{MBOX}} = \mathtt{S} \to \mathtt{C} : \mathtt{R}\,\langle \mathtt{Int} \rangle; \mathtt{G}_{\mathtt{NMBR}} + \mathtt{S} \to \mathtt{C} : \mathtt{E}\,\langle\rangle; \mathtt{G}_{\mathtt{EXIT}}$$

Runs (by example)

$$\mathcal{R}(\mathtt{G}_{\mathtt{POP}}) \qquad r_1 = \langle \mathtt{C}, \overline{\mathtt{QUIT}}\ \_\rangle \langle \mathtt{S}, \mathtt{QUIT}\ \_\rangle \ldots$$

$$r_2 = \langle \mathtt{C}, \overline{\mathtt{HELO\ String}}\rangle \langle \mathtt{S}, \mathtt{HELO\ String}\rangle \langle \mathtt{S}, \overline{\mathtt{R}}\ \mathtt{Int}\rangle \langle \mathtt{C}, \mathtt{R\ Int}\rangle \ldots$$

$$r_3 = \langle \mathtt{C}, \overline{\mathtt{HELO\ String}}\rangle \langle \mathtt{S}, \mathtt{HELO\ String}\rangle \langle \mathtt{S}, \overline{\mathtt{E}}\ \rangle \langle \mathtt{C}, \mathtt{E}\ \rangle \ldots$$

$$\mathcal{R}(\mathtt{G}^*_{\mathtt{POP}}) \qquad r \in \mathcal{R}(\mathtt{G}_{\mathtt{POP}}), r' \in \mathcal{R}(\mathtt{G}^*_{\mathtt{POP}}) \;\Rightarrow\; [r']r \in \mathcal{R}(\mathtt{G}^*_{\mathtt{POP}})$$

$$[r_1]r_1 \;\; [r_1 r_1]r_1 \ldots [r_1 r_2]r_3 \;\; \ldots$$

Implementations as Processes

$$P, Q ::= u_i(\mathbf{y}).P \mid \overline{u}^n(\mathbf{y}).P \mid \sum_{i \in I} y_i(x_i); P_i \mid \overline{s}e \mid \texttt{if } e:\ P \texttt{ else } Q \mid P; P \mid \texttt{for } x \texttt{ in } \ell\texttt{:}\ P \mid \texttt{do } N \texttt{ until } b$$

Example [Post Office Protocol (POP2) – role S]

$$\begin{array}{lcl}
P_{\texttt{INIT}} & = & u_{\texttt{S}}(\mathbf{y}).P_{\texttt{S}} \\
P_{\texttt{S}} & = & y_{\texttt{QUIT}}; P_{\texttt{EXIT}} + y_{\texttt{HELO}}\ x; P_{\texttt{MBOX}} \\
P_{\texttt{MBOX}} & = & \texttt{if } \texttt{auth}(x)\ :\ \overline{y}_{\texttt{R}}\texttt{fn}(inbox); P_{\texttt{NMBR}} \texttt{ else } \overline{y}_{\texttt{E}}; P_{\texttt{EXIT}}
\end{array}$$

Candidate implementations of G

$$\boxed{\iota : \mathcal{P}(\texttt{G}) \mapsto \mathbb{P}}$$

$$\mathcal{I}^{\iota}_{\texttt{G}} \equiv \iota(\mathtt{p}_1) \mid \ldots \mid \iota(\mathtt{p}_n) \qquad \texttt{ch}(\texttt{G}) \cap \texttt{fc}(\iota(\mathtt{p}_i)) = \emptyset$$

Whole-Spectrum Implementation

- $\mathcal{R}_2$ *covers* $\mathcal{R}_1$ if $r \in \mathcal{R}_1$ implies $\exists r' \in \mathcal{R}_2$ s.t. $r \lessdot r'$

$$[r] \lessdot \epsilon \qquad r \lessdot r'r \qquad \frac{r \lessdot r'}{[r] \lessdot r'} \qquad \frac{r \lessdot r'}{[r] \lessdot [r']} \qquad \frac{r_1 \lessdot r'_1 \quad r_2 \lessdot r'_2}{r_1 r_2 \lessdot r'_1 r'_2}$$

E.g., $[r_1 r_2] r_3 \lessdot r_3$

- A process P is a *whole-spectrum implementation* of $\mathtt{p}_i \in \mathtt{G}$ when there exists a set $\mathbb{I}$ of implementations that covers $\mathtt{G}$ s.t. $\mathcal{I}^{\iota}_{\mathtt{G}} \in \mathbb{I}$ implies $\mathcal{I}^{\iota}_{\mathtt{G}} = \iota(\mathtt{p}_1) \mid \ldots \mid \iota(\mathtt{p}_n)$ and $\iota(\mathtt{p}_i) = P$

Typing Whole-Spectrum Implementations

$$\mathcal{C} \mathbin{\llcorner\!\lrcorner} \Gamma \vdash P \triangleright \Delta \divideontimes \Gamma'$$

Example [Post Office Protocol (POP2) – typing]

$$\mathtt{G}_{\mathtt{MBOX}} = \mathtt{S} \to \mathtt{C} : y_{\mathrm{R}} \langle \mathtt{Int} \rangle ; \mathtt{G}_{\mathtt{NMBR}} + \mathtt{S} \to \mathtt{C} : y_{\mathrm{E}} \langle \rangle ; \mathtt{G}_{\mathtt{EXIT}}$$

$$\mathtt{G}_{\mathtt{MBOX}} \upharpoonright \mathtt{S} = y_{\mathrm{R}} ! \mathtt{Int} ; \mathtt{T}_{\mathtt{NMBR}} \oplus y_{\mathrm{E}} ! ; \mathtt{T}_{\mathtt{EXIT}}$$

$$\mathtt{true} \mathbin{\llcorner\!\lrcorner} \Gamma \vdash \mathtt{if}\ \mathtt{auth}(x) : \overline{y}_{\mathrm{R}} \mathtt{fn}(inbox) ; P_{\mathtt{NMBR}}\ \mathtt{else}\ \overline{y}_{\mathrm{E}} ; P_{\mathtt{EXIT}} \triangleright$$

$$\mathbf{y} : y_{\mathrm{R}} ! \mathtt{Int} ; \mathtt{T}_{\mathtt{NMBR}} \oplus y_{\mathrm{E}} ! ; \mathtt{T}_{\mathtt{EXIT}} \divideontimes \Gamma'$$

$$\frac{\Gamma(e) = \mathtt{bool} \qquad \begin{array}{ll} \mathcal{C} \wedge e \nvDash \bot & \mathcal{C} \wedge e \mathbin{\llcorner\!\lrcorner} \Gamma \vdash P \triangleright \Delta_1 \divideontimes \Gamma_1 \\ \mathcal{C} \wedge \neg e \nvDash \bot & \mathcal{C} \wedge \neg e \mathbin{\llcorner\!\lrcorner} \Gamma \vdash Q \triangleright \Delta_2 \divideontimes \Gamma_2 \end{array}}{\mathcal{C} \mathbin{\llcorner\!\lrcorner} \Gamma \vdash \mathtt{if}\ e : P\ \mathtt{else}\ Q \triangleright \Delta_1 \bowtie \Delta_2 \divideontimes \Gamma_1 \cap \Gamma_2}$$

Properties

Corollary (Soundness). If $\mathcal{C} \,\llcorner\, \Gamma \vdash P \triangleright \Delta \divideontimes \Gamma'$ then

$$P \lesssim \Gamma,\ \Delta$$

Theorem (Covering projections). For any global type $\mathtt{G}$ s.t. $\mathtt{ch}(\mathtt{G}) = \mathbf{s}$,

$$\mathcal{R}_{\mathbf{s}}(\{\mathbf{s} : (\mathtt{G} \restriction \mathtt{p})@\mathtt{p}\}_{\mathtt{p} \in \mathtt{G}})\ \textit{covers}\ \mathcal{R}(\mathtt{G})$$

Theorem (WSI). Let $\mathtt{G}$ be a global type s.t. $\mathtt{ch}(\mathtt{G}) = \mathbf{s}$, for $\mathtt{p} \in \mathtt{G}$ consider

$$\mathbb{I}^{\mathtt{p}}_{P} = \{\mathcal{I}^{\iota}_{\mathtt{G}} \mid \iota(\mathtt{p}) = P,\ \forall \mathtt{q} \in \mathtt{G}\ :\ \mathtt{true} \,\llcorner\, \Gamma, u : \mathtt{G} \vdash \iota(\mathtt{q}) \triangleright \Delta, \mathbf{s} : \mathtt{G} \restriction \mathtt{q} \divideontimes \Gamma'\}$$

Then,

$$\mathcal{R}_{\mathbf{u}}(\mathbb{I}^{\mathtt{p}}_{P})\ \ \textit{covers}\ \ \mathcal{R}_{\mathbf{s}}(\{\mathbf{s} : (\mathtt{G} \restriction \mathtt{p})@\mathtt{p}\}_{\mathtt{p} \in \mathtt{G}})$$

Conclusion

Summary

- WSI based on the relation between the traces of a global type and the traces of its candidate implementations
- The set of projections of a global type covers that global type
- Proof system guarantees safety and that all the traces of a local type can be mimicked by a well-typed implementation
- It works also with interleaved sessions

Future work

- Subtyping
- Completeness
- Practical application: may and must choices

Questions?

http://mrg.doc.ic.ac.uk/publications.html