Semantic Subtyping for Session Types

Luca Padovani

Dipartimento di Informatica, Università di Torino

BTW'11

Semantic subtyping in a nutshell

- Frisch, Castagna, Benzaken, **Semantic Subtyping**, 2008

$$t \leqslant s \stackrel{\text{def}}{\iff} [\![t]\!] \subseteq [\![s]\!]$$

+ Intuition

$$[\![t \wedge s]\!] = [\![t]\!] \cap [\![s]\!] \qquad [\![t \vee s]\!] = [\![t]\!] \cup [\![s]\!]$$

+ Expressiveness

$$[\![\neg t]\!] = \mathcal{V} \setminus [\![t]\!]$$

+ Precision

$$t \not\leqslant s \quad \text{implies} \quad v \in [\![t]\!] \setminus [\![s]\!]$$

Subtyping for session types

- Gay, Hole, **Subtyping for session types in the pi calculus**, 2005

$$\mathsf{end} \leqslant_{\mathsf{U}} \mathsf{end}$$

$$\frac{T_i \leqslant_{\mathsf{U}} S_i \ ^{(i \in I)}}{\sum_{i \in I} ?a_i.T_i \leqslant_{\mathsf{U}} \sum_{i \in I \cup J} ?a_i.S_i} \qquad \frac{T_i \leqslant_{\mathsf{U}} S_i \ ^{(i \in I)}}{\bigoplus_{i \in I \cup J} !a_i.T_i \leqslant_{\mathsf{U}} \bigoplus_{i \in I} !a_i.S_i}$$

$T \leqslant_{\mathsf{U}} S$ means...

- it is safe to use a channel of type T where a channel of type S is expected, or...
- it is safe to use a process that behaves as S where a process that behaves as T is expected

Subtyping for session types

- Gay, Hole, **Subtyping for session types in the pi calculus**, 2005

$$\mathsf{end} \leqslant_{\mathsf{U}} \mathsf{end}$$

$$\frac{T_i \leqslant_{\mathsf{U}} S_i \ ^{(i \in I)}}{\sum_{i \in I} \mathtt{p}?a_i.T_i \leqslant_{\mathsf{U}} \sum_{i \in I \cup J} \mathtt{p}?a_i.S_i} \qquad \frac{T_i \leqslant_{\mathsf{U}} S_i \ ^{(i \in I)}}{\bigoplus_{i \in I \cup J} \mathtt{p}!a_i.T_i \leqslant_{\mathsf{U}} \bigoplus_{i \in I} \mathtt{p}!a_i.S_i}$$

$T \leqslant_{\mathsf{U}} S$ means...

- it is safe to use a channel of type T where a channel of type S is expected, or...
- it is safe to use a process that behaves as S where a process that behaves as T is expected

Example: multi-party session

$$\begin{tikzcd} \oplus \arrow[loop above, "\mathtt{q}!a"] \arrow[r, "\mathtt{q}!b"'] & \oplus \arrow[r, "\mathtt{r}!c"'] & \text{end} \end{tikzcd} \qquad \begin{tikzcd} + \arrow[loop above, "\mathtt{p}?a"] \arrow[r, "\mathtt{p}?b"'] & \text{end} \end{tikzcd} \qquad \begin{tikzcd} + \arrow[r, "\mathtt{p}?c"'] & \text{end} \end{tikzcd}$$

- $\mathtt{p} : T = \mathtt{q}!a.T \oplus \mathtt{q}!b.\mathtt{r}!a.\text{end}$
- $\mathtt{q} : S = \mathtt{p}?a.S + \mathtt{p}?b.\text{end}$
- $\mathtt{r} : \mathtt{p}?c.\text{end}$

Is this session "**OK**"?

Example: multi-party session

$$
\begin{tikzcd}
\oplus \arrow[loop above, "\mathtt{q}!a"] \arrow[r, "\mathtt{q}!b"'] & \oplus \arrow[r, "\mathtt{r}!c"'] & \mathsf{end}
\end{tikzcd}
\qquad
\begin{tikzcd}
+ \arrow[loop above, "\mathtt{p}?a"] \arrow[r, "\mathtt{p}?b"'] & \mathsf{end}
\end{tikzcd}
\qquad
\begin{tikzcd}
+ \arrow[r, "\mathtt{p}?c"'] & \mathsf{end}
\end{tikzcd}
$$

- $\mathtt{p} : T = \mathtt{q}!a.T \oplus \mathtt{q}!b.\mathtt{r}!a.\mathsf{end}$
- $\mathtt{q} : S = \mathtt{p}?a.S + \mathtt{p}?b.\mathsf{end}$
- $\mathtt{r} : \mathtt{p}?c.\mathsf{end}$

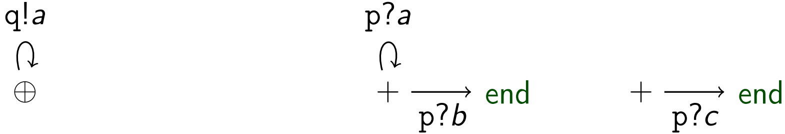
Is this session "**OK**"? Yes, under a fairness assumption

Example: multi-party session (and subtyping)

$$\begin{tikzcd} \oplus \arrow[loop above, "\mathtt{q}!a"] \arrow[r, "\mathtt{q}!b"'] & \oplus \arrow[r, "\mathtt{r}!c"'] & \mathsf{end} \end{tikzcd} \qquad \begin{tikzcd} + \arrow[loop above, "\mathtt{p}?a"] \arrow[r, "\mathtt{p}?b"'] & \mathsf{end} \end{tikzcd} \qquad \begin{tikzcd} + \arrow[r, "\mathtt{p}?c"'] & \mathsf{end} \end{tikzcd}$$

- $\mathtt{p} : T = \mathtt{q}!a.T \oplus \mathtt{q}!b.\mathtt{r}!a.\mathsf{end}$
- $\mathtt{q} : S = \mathtt{p}?a.S + \mathtt{p}?b.\mathsf{end}$
- $\mathtt{r} : \mathtt{p}?c.\mathsf{end}$

Example: multi-party session (and subtyping)



- $\mathtt{p} : T = \mathtt{q}!a.T$
- $\mathtt{q} : S = \mathtt{p}?a.S + \mathtt{p}?b.\mathsf{end}$
- $\mathtt{r} : \mathtt{p}?c.\mathsf{end}$

Is this session is "**OK**"?

How to fix subtyping

Definition (OK session)

- $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n$ OK if
  $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n \Longrightarrow \mathrm{p}_1 : T'_1 \mid \cdots \mid \mathrm{p}_n : T'_n$ implies
  $\mathrm{p}_1 : T'_1 \mid \cdots \mid \mathrm{p}_n : T'_n \Longrightarrow \mathrm{p}_1 : \mathsf{end} \mid \cdots \mid \mathrm{p}_n : \mathsf{end}$

Definition (semantic subtyping)

- $[\![T]\!] = \{M \quad \mid \quad (\mathrm{p} : T \mid M) \text{ is OK}\}$
- $T \leqslant S \quad \text{iff} \quad [\![T]\!] \subseteq [\![S]\!]$

How to fix subtyping

Definition (OK session)

- $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n$ OK if
  $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n \Longrightarrow \mathrm{p}_1 : T'_1 \mid \cdots \mid \mathrm{p}_n : T'_n$ implies
  $\mathrm{p}_1 : T'_1 \mid \cdots \mid \mathrm{p}_n : T'_n \Longrightarrow \mathrm{p}_1 : \mathsf{end} \mid \cdots \mid \mathrm{p}_n : \mathsf{end}$

Definition (semantic subtyping)

- $[\![T]\!] = \{M \quad \mid \quad (\mathrm{p} : T \mid M) \text{ is OK}\}$
- $T \leqslant S \quad \text{iff} \quad [\![T]\!] \subseteq [\![S]\!]$

How to fix subtyping

Definition (OK session)

- $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n$ OK if
  $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n \Longrightarrow \mathrm{p}_1 : T_1' \mid \cdots \mid \mathrm{p}_n : T_n'$ implies
  $\mathrm{p}_1 : T_1' \mid \cdots \mid \mathrm{p}_n : T_n' \Longrightarrow \mathrm{p}_1 : \mathsf{end} \mid \cdots \mid \mathrm{p}_n : \mathsf{end}$

Definition (semantic subtyping)

- $[\![T]\!] = \{M \mid (\mathrm{p} : T \mid M) \text{ is OK}\}$
- $T \leqslant S \quad \text{iff} \quad [\![T]\!] \subseteq [\![S]\!]$

How to fix subtyping

Definition (OK session)

- $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n$ **OK** if
  $\mathrm{p}_1 : T_1 \mid \cdots \mid \mathrm{p}_n : T_n \Longrightarrow \mathrm{p}_1 : T_1' \mid \cdots \mid \mathrm{p}_n : T_n'$ implies
  $\mathrm{p}_1 : T_1' \mid \cdots \mid \mathrm{p}_n : T_n' \Longrightarrow \mathrm{p}_1 : \mathsf{end} \mid \cdots \mid \mathrm{p}_n : \mathsf{end}$

Definition (semantic subtyping)

- $[\![T]\!] = \{M \quad | \quad (\mathrm{p} : T \mid M) \text{ is } \mathbf{OK}\}$
- $T \leqslant S \quad \text{iff} \quad [\![T]\!] \subseteq [\![S]\!]$

Dilemma

$$\leqslant_{\mathsf{U}} \quad \text{versus} \quad \leqslant$$

- $\leqslant_{\mathsf{U}}$ is intuitive but unsound
- $\leqslant$ is sound but obscure

(Fair) subtyping = (fair) testing preorder

- P passes test T
- $P \sqsubseteq Q$ iff P passes test T implies Q passes test T

"Unfair" testing

- De Nicola, Hennessy, **Testing equivalences for processes**, 1983
- ...

Fair testing

- Cleaveland, Natarajan, **Divergence and fair testing**, 1995
- Rensink, Vogler, **Fair testing**, 2007

$\leqslant_{\mathsf{U}}$ and $\leqslant$ are incomparable

$$
\begin{array}{rcl}
T & = & \mathtt{p}!a.T \\
S & = & \mathtt{q}?b.S
\end{array}
\qquad
\begin{array}{rcl}
T & \leqslant & S \\
S & \leqslant & T
\end{array}
\qquad
\begin{array}{rcl}
T & \not\leqslant_{\mathsf{U}} & S \\
S & \not\leqslant_{\mathsf{U}} & T
\end{array}
$$

$\leqslant_{\mathsf{U}}$ and $\leqslant$ are incomparable

$$
\begin{array}{rcl@{\qquad\qquad}rcl@{\qquad\qquad}rcl}
T & = & \mathtt{p}!a.T & T & \leqslant & S & T & \not\leqslant_{\mathsf{U}} & S \\
S & = & \mathtt{q}?b.S & S & \leqslant & T & S & \not\leqslant_{\mathsf{U}} & T
\end{array}
$$

not viable

$\mathsf{fail} \lesseqgtr T \lesseqgtr S \lesseqgtr \cdots$

$\leqslant \subseteq \leqslant_{\mathsf{U}}$

viable

A normal form for session types

T is in normal form if either

- $T = \mathsf{fail}$, or
- $\mathsf{end} \in \mathsf{trees}(S)$ for every $S \in \mathsf{trees}(T)$

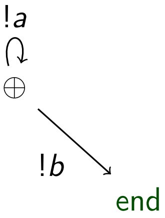
Proposition

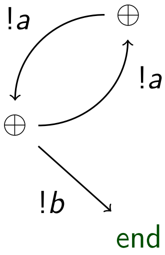
For every T there exists $S \leqslant T$ in nf

Theorem

Let $T, S \neq \mathsf{fail}$ be in nf. Then $T \leqslant S$ implies $T \leqslant_{\mathsf{U}} S$

Experiment 1





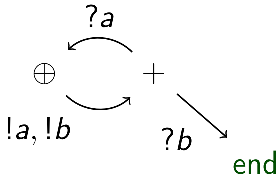
$T = !a.T \oplus !b.\mathsf{end}$ $\qquad$ $S = !a.!a.S \oplus !b.\mathsf{end}$

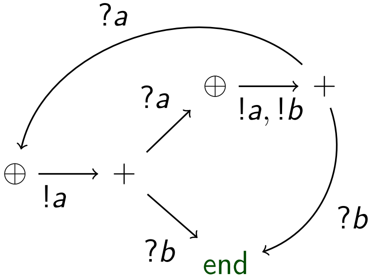
Is there a context R such that

- $R \mid T$ is **OK**
- $R \mid S \not\Longrightarrow \mathsf{end} \mid \mathsf{end}$

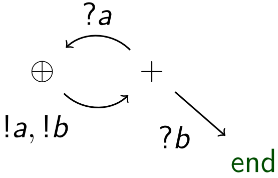
?

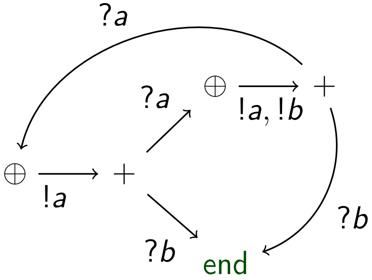
Experiment 2

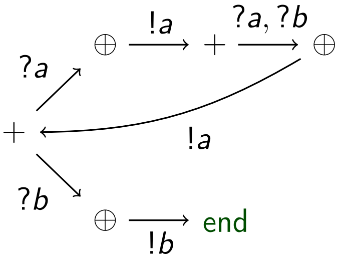




Experiment 2







Rule of thumb

If

- $!a.T$ does not occur in a loop

or

- $!a.T$ occurs in a loop ℓ of p, and
- there exists an exit path in ℓ that starts from a $\oplus$ node,

then

- $!a.T$ can be safely pruned

Rationale

- no context can rely on the eventual observation of $!a$ from p because p can autonomously exit ℓ

Behavioral difference

Theorem

Let T, S be in nf and $T \leqslant_{\mathsf{U}} S$.
*Then $T - S$ viable iff $R \mid T$ **OK** and $R \mid S \not\Longrightarrow \mathsf{end} \mid \mathsf{end}$ for some R*

$$\mathsf{end} - \mathsf{end} = \mathsf{fail}$$

$$\sum_{i \in I} \mathtt{p?}a_i.T_i - \sum_{i \in I \cup J} \mathtt{p?}a_i.S_i = \sum_{i \in I} \mathtt{p?}a_i.(T_i - S_i)$$

$$\bigoplus_{i \in I \cup J} \mathtt{p!}a_i.T_i - \bigoplus_{i \in I} \mathtt{p!}a_i.S_i = \bigoplus_{i \in I} \mathtt{p!}a_i.(T_i - S_i) \oplus \bigoplus_{j \in J} \mathtt{p!}a_j.T_j$$

Fair subtyping, at last

$$\mathsf{fail} \leqslant_{\mathsf{A}} T \qquad \mathsf{end} \leqslant_{\mathsf{A}} \mathsf{end}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)}}{\sum_{i \in I} \mathtt{p}?a_i.T_i \leqslant_{\mathsf{A}} \sum_{i \in I \cup J} \mathtt{p}?a_i.S_i}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)} \qquad \mathsf{nf}(T - S) = \mathsf{fail}}{T = \bigoplus_{i \in I \cup J} \mathtt{p}!a_i.T_i \leqslant_{\mathsf{A}} \bigoplus_{i \in I} \mathtt{p}!a_i.S_i = S}$$

Theorem

$T \leqslant S$ *iff* $\mathsf{nf}(T) \leqslant_{\mathsf{A}} \mathsf{nf}(S)$

Fair subtyping, at last

$$\mathsf{fail} \leqslant_{\mathsf{A}} T \qquad \mathsf{end} \leqslant_{\mathsf{A}} \mathsf{end}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)}}{\sum_{i \in I} \mathtt{p}?a_i.T_i \leqslant_{\mathsf{A}} \sum_{i \in I \cup J} \mathtt{p}?a_i.S_i}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)} \qquad \mathsf{nf}(T - S) = \mathsf{fail}}{T = \bigoplus_{i \in I \cup J} \mathtt{p}!a_i.T_i \leqslant_{\mathsf{A}} \bigoplus_{i \in I} \mathtt{p}!a_i.S_i = S}$$

Theorem

$T \leqslant S$ *iff* $\mathsf{nf}(T) \leqslant_{\mathsf{A}} \mathsf{nf}(S)$

Fair subtyping, at last

$$\text{fail} \leqslant_{\mathsf{A}} T \qquad \text{end} \leqslant_{\mathsf{A}} \text{end}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)}}{\sum_{i \in I} \mathtt{p}?a_i.T_i \leqslant_{\mathsf{A}} \sum_{i \in I \cup J} \mathtt{p}?a_i.S_i}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)} \qquad \mathrm{nf}(T - S) = \text{fail}}{T = \bigoplus_{i \in I \cup J} \mathtt{p}!a_i.T_i \leqslant_{\mathsf{A}} \bigoplus_{i \in I} \mathtt{p}!a_i.S_i = S}$$

Theorem

$T \leqslant S$ *iff* $\mathrm{nf}(T) \leqslant_{\mathsf{A}} \mathrm{nf}(S)$

Fair subtyping, at last

$$\mathsf{fail} \leqslant_{\mathsf{A}} T \qquad \mathsf{end} \leqslant_{\mathsf{A}} \mathsf{end}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)}}{\sum_{i \in I} \mathtt{p}?a_i.T_i \leqslant_{\mathsf{A}} \sum_{i \in I \cup J} \mathtt{p}?a_i.S_i}$$

$$\frac{T_i \leqslant_{\mathsf{A}} S_i \ ^{(i \in I)} \qquad \mathsf{nf}(T - S) = \mathsf{fail}}{T = \bigoplus_{i \in I \cup J} \mathtt{p}!a_i.T_i \leqslant_{\mathsf{A}} \bigoplus_{i \in I} \mathtt{p}!a_i.S_i = S}$$

Theorem

$T \leqslant S$ *iff* $\mathsf{nf}(T) \leqslant_{\mathsf{A}} \mathsf{nf}(S)$

Fair testing vs fair subtyping

Fair testing

- Cleaveland, Natarajan, **Divergence and fair testing**, 1995
- Rensink, Vogler, **Fair testing**, 2007

– denotational (= obscure) characterization

– no complete deduction system

– exponential

Fair subtyping

\+ operational (= hopefully less obscure) characterization
(and maybe it can be further simplified)

\+ complete deduction system

\+ polynomial

More on semantic subtyping

- Padovani, **Session Types = Intersection Types + Union Types**, ITRS 2010

$$
\begin{array}{rcl}
!a.T \oplus !b.S & \iff & !a.T \wedge !b.S \\
?a.T + ?b.S & \iff & ?a.T \vee ?b.S
\end{array}
$$

$$?a.T \vee ?a.S \lesseqgtr ?a.(T \vee S)$$

More on fair subtyping

- Padovani, **Fair Subtyping for Multi-Party Session Types**, COORDINATION 2011

+ formal definitions and proofs
+ algorithms (viability, normal form, subtyping)

Future work: fair type checking

$$T = \,!a.T \oplus \,!b.\mathsf{end} \qquad\qquad P = u!a.P$$

$$\dfrac{\dfrac{u : T \vdash P}{u : \,!a.T \vdash u!a.P}\,(\text{T-Output}) \qquad T \leqslant \,!a.T}{u : T \vdash P}\,(\text{T-Narrow})$$

thank you