Deadlock Avoidance in SCC
based on the AMAST 2008 paper
“Types and deadlock freedom in a calculus of services, sessions and pipelines”

Roberto Bruni\textsuperscript{1}  Leonardo Gaetano Mezzina\textsuperscript{2}

\textsuperscript{1}Dipartimento di Informatica
Università di Pisa

\textsuperscript{2}IMT Lucca
Instute for Advanced Studies

SENSORIA Workshop on Calculi for Service Oriented Computing
IMT Alti Studi, Lucca, Italy
17–18 September 2008
Outline

1. Introduction & Motivation
2. SCC in a Nutshell
3. A Type System for SCC
4. Concluding Remarks
Outline

1. Introduction & Motivation
2. SCC in a Nutshell
3. A Type System for SCC
4. Concluding Remarks
Service Oriented Computing (SOC)

Services

SOC is an emerging paradigm where services are understood as:

- autonomous
- platform-independent

computational entities that can be:

- described
- published
- discovered
- dynamically assembled

for developing massively distributed, interoperable, evolvable systems.

e-Expectations

Big companies put many efforts for service delivery on a variety of computing platforms. Tomorrow, there will be a plethora of new services for e-health, e-forensics, e-government, e-* within the rapidly evolving Information Society.

Semantic foundations?

Industrial consortia are developing orchestration and choreography languages, targeting the standardization of Web Services and XML-centric technologies for which neat semantic foundations are necessary.
Service Oriented Computing (SOC)

**Services**

SOC is an emerging paradigm where *services* are understood as:
- autonomous
- platform-independent

Computational entities that can be:
- described
- published
- discovered
- dynamically assembled

For developing massively distributed, interoperable, evolvable systems.

**e-Expectations**

Big companies put many efforts for service delivery on a variety of computing platforms.

Tomorrow, there will be a plethora of new services for e-health, e-forensics, e-government, e-* within the rapidly evolving Information Society.

**Semantic foundations?**

Industrial consortia are developing orchestration and choreography languages, targeting the standardization of Web Services and XML-centric technologies for which *neat semantic foundations are necessary.*
Aim

Developing a novel, comprehensive approach to the engineering of software systems for service-oriented overlay computers.

Strategy

Integration of foundational theories, techniques, methods and tools in a pragmatic software engineering approach.
The role of process calculi

Coordinating and combining services
A crucial role in the project is played by formalisms for service description that can lay the mathematical basis for analysing and experimenting with components interactions, and for combining services.

Sensoria Work Packages 2 and 5
We experiment with a small set of primitives, concepts and features that might serve as a basis for formalizing, programming and disciplining service oriented applications over global computers.

Sensoria core calculi
- *Signal Calculus*: middleware level
- *SOCK, COWS*: service level, correlation-based
- *SCC-family* (*SCC, SSCC, CC, CaSPiS*): service level, session-based
- *cc-pi, lambda-req*: SLA contract level
Main Contribution

Goal
Define a type system for SCC to guarantee sound interaction.

AMAST 2008 Proceedings
- Syntax + LTS semantics (see Section 2)
- Type system + subject reduction (see Section 3)
- **Initial processes do not deadlock**: We define a class of processes, called *initial*, for which we can guarantee that a normal form is reached with no pending session protocols unless infinitely many services are invoked provoking divergence (see Theorem 2).
- Simple examples

Talk
- Sketches of syntax and semantics
- Intuitive idea and flashes of typing rules
- Simple examples
Related Work

- Honda, Vasconcelos, Kubo + Gay, Hole + Kobayashi: starting point
- Acciai, Boreale (Ugo Montanari’s Festschrift): CaSPiS\(^{-}\), asymmetric notion of progress
- Dezani et al. (TGC’07): progress, no recursion
- Lanese et al. (SEFM’07): SSCC orchestration is via streams instead of pipelines
- Bonelli, Compagnoni + Honda, Yoshida, Carbone: multiparty asynchronous sessions
- Bruni et al. (PLACES’08, ongoing): \(\mu\)se, dynamic multiparty sessions
- Caires, Vieira (ongoing): conversation calculus, dynamic multiparty sessions
- ...
- given the audience, please name your own
Outline

1. Introduction & Motivation

2. SCC in a Nutshell

3. A Type System for SCC

4. Concluding Remarks
SCC Genesis [see WS-FM 2006]

Sources of inspiration

- $\pi$ (names, communication): $a(y).P, \bar{a}k.P, (\nu k)P$
- $\pi I$, structured communication (session types): $a(k).P, \bar{a}(k).P$
  - roughly, think of $\bar{a}(k).P$ as $(\nu k)\bar{a}k.P$
- Orc (pipelining and pruning of activities):
  $$(EAPLS\langle 2008 \rangle | EATCS\langle 2008 \rangle) > x_{cfp} > Email\langle rb@gmail.it, x_{cfp} \rangle$$
  $$Email\langle rb@gmail.it, x_{cfp} \rangle \textbf{where } x_{cfp} \in (EAPLS\langle 2008 \rangle | EATCS\langle 2008 \rangle)$$

To keep in mind

We are dealing with conceptual abstractions: the syntax does not necessarily expose implementation details. For example:

- a session is a logical entity that can be implemented by an additional $sid$ parameter carried by all related messaging
- all service instances (serving different requests) can be handled by one service port
## Sources of inspiration

- **\( \pi \)** (names, communication): \( a(y).P, \bar{a}k.P, (\nu k)P \)
- **\( \pi I \)**, structured communication (session types): \( a(k).P, \bar{a}(k).P \)
  
  Roughly, think of \( \bar{a}(k).P \) as \( (\nu k)\bar{a}.P \)

- **Orc** (pipelining and pruning of activities):
  
  \[
  (EAPLS\langle2008\rangle | EATCS\langle2008\rangle) > x_{\text{cfp}} > Email\langle rb@\text{gmail.it}, x_{\text{cfp}} \rangle
  \]

  \[
  Email\langle rb@\text{gmail.it}, x_{\text{cfp}} \rangle \text{ where } x_{\text{cfp}} : \in (EAPLS\langle2008\rangle | EATCS\langle2008\rangle)
  \]

## To keep in mind

We are dealing with conceptual abstractions: the syntax does not necessarily expose implementation details. For example:

- A session is a logical entity that can be implemented by an additional \( sid \) parameter carried by all related messaging.
- All service instances (serving different requests) can be handled by one service port.
Sources of inspiration

- \(\pi\) (names, communication): \(a(y).P, \bar{a}k.P, (\nu k)P\)
- \(\pi I\), structured communication (session types): \(a(k).P, \bar{a}(k).P\)
  roughly, think of \(\bar{a}(k).P\) as \((\nu k)\bar{a}k.P\)
- Orc (pipelining and pruning of activities):
  \((EAPLS\langle2008\rangle | EATCS\langle2008\rangle) > x_{cfp} > Email\langle rb@gmail.it, x_{cfp}\rangle\)
  \(Email\langle rb@gmail.it, x_{cfp}\rangle\ where\ x_{cfp} :\in (EAPLS\langle2008\rangle | EATCS\langle2008\rangle)\)

To keep in mind

We are dealing with conceptual abstractions: the syntax does not necessarily expose implementation details. For example:

- a session is a logical entity that can be implemented by an additional \(sid\) parameter carried by all related messaging
- all service instances (serving different requests) can be handled by one service port
SCC Genesis [see WS-FM 2006]

Sources of inspiration

- \(\pi\) (names, communication): \(a(y).P, \overline{a}k.P, (\nu k)P\)
- \(\pi I\), structured communication (session types): \(a(k).P, \overline{a}(k).P\)
  roughly, think of \(\overline{a}(k).P\) as \((\nu k)\overline{a}k.P\)
- Orc (pipelining and pruning of activities):
  \((EAPLS\langle 2008\rangle | EATCS\langle 2008\rangle) > x_{cfp} > Email\langle rb@gmail.it, x_{cfp}\rangle\)
  \(Email\langle rb@gmail.it, x_{cfp}\rangle\) \textbf{where} \(x_{cfp} \in (EAPLS\langle 2008\rangle | EATCS\langle 2008\rangle)\)

To keep in mind

We are dealing with conceptual abstractions: the syntax does not necessarily expose implementation details. For example:

- a session is a logical entity that can be implemented by an additional \(sid\) parameter carried by all related messaging
- all service instances (serving different requests) can be handled by one service port
### Service definitions: $s.P$
- services expose their protocols
- (persistent) services can handle multiple requests separately

### Service invocations: $\tilde{s}.Q$
- service invocations expose their protocols
- sequential composition via pipelining (à la Orc)

### Sessions: $r^+ \triangleright P \mid r^- \triangleright Q$
- to be read as run-time syntax
- service invocation spawns fresh session parties (locally to each partner)
- sessions are: two-party (service-side + client-side) + private
- interaction between session protocols: bi-directional
- nested sessions: values can be returned outside sessions (one level up)
### Service definitions: \( s.P \)
- Services expose their protocols.
- (Persistent) services can handle multiple requests separately.

### Service invocations: \( s.Q \)
- Service invocations expose their protocols.
- Sequential composition via pipelining (à la Orc).

### Sessions: \( r^+ \triangleright P \mid r^- \triangleright Q \)
- To be read as run-time syntax.
- Service invocation spawns fresh session parties (locally to each partner).
- Sessions are: two-party (service-side + client-side) + private.
- Interaction between session protocols: bi-directional.
- Nested sessions: values can be returned outside sessions (one level up).
SCC: General Principles

**Service definitions: $s.P$**
- Services expose their protocols.
- (Persistent) services can handle multiple requests separately.

**Service invocations: $\overline{s}.Q$**
- Service invocations expose their protocols.
- Sequential composition via pipelining (à la Orc).

**Sessions: $r^+ \triangleright P \mid r^- \triangleright Q$**
- To be read as run-time syntax.
- Service invocation spawns fresh session parties (locally to each partner).
- Sessions are: two-party (service-side + client-side) + private.
- Interaction between session protocols: bi-directional.
- Nested sessions: values can be returned outside sessions (one level up).
Sketch of Multiple Sessions

- Service def

- Service call

- Service call

- Service call

Powered by yFiles
Sketch of Multiple Sessions

 Powered by yFiles
Sketch of Multiple Sessions

 Powered by yFiles
Sketch of Multiple Sessions

Powered by yFiles
Sketch of Conversations

1. in.out.in
2. in.out.in
3. in.out.in

r1
r2
r3

out.in.out
out | in | out
out | in.out

Powered by yFiles
Sketch of Nested Sessions

Powered by yFiles
Sketch of Nested Sessions
Sketch of Nested Sessions

[Diagram of nested sessions with rectangles and labels]

Powered by yFiles
Sketch of Nested Sessions

 Powered by yFiles
Sketch of Return

Deadlock Avoidance in SCC
Sensoria Wk on CSOC (2008)
SCC Raw Syntax

Names, Values, Polarities

\[ m ::= s \mid r \quad \text{(name)} \]
\[ v ::= b \mid s \mid x \mid f(\tilde{v}) \quad \text{(value)} \]
\[ p, q ::= - \mid + \quad \text{(polarity)} \]

Processes

\[ P, Q ::= 0 \quad \text{(nil)} \]
\[ s.P \quad \text{(service definition / invoke)} \]
\[ \langle \tilde{v} \rangle . P \quad \text{values output / tuple input} \]
\[ \langle l \rangle . P \quad \text{(label selection / branching)} \]
\[ \Sigma_{i=1}^{n}(l_i).P_i \quad \text{(return)} \]
\[ \text{return } \tilde{v}.P \]
\[ \text{if } v = v' \text{ then } P \text{ else } Q \quad \text{(if-then-else)} \]
\[ (\nu m)P \quad \text{(restriction)} \]
\[ r^P \triangleright P \quad \text{(polarized session)} \]
\[ P > \tilde{x} > Q \quad \text{(pipe)} \]
\[ P | Q \quad \text{(parallel)} \]
### SCC Raw Syntax

#### Names, Values, Polarities

\[
m ::= \text{s} \mid \text{r} \\
v ::= \text{b} \mid \text{s} \mid \text{x} \mid f(\tilde{v}) \\
p, q ::= - \mid +
\]

(name)

(value)

(polarity)

#### Processes

\[
P, Q ::= 0 \\
s.P \\
\langle \tilde{v} \rangle . P \\
\langle \ell \rangle . P \\
\nu. Q \\
(\tilde{x}). Q \\
\Sigma_{i=1}^n (l_i). P_i \\
\text{return } \tilde{v}. P \\
\text{if } v = v' \text{ then } P \text{ else } Q \\
(\nu m) P \\
r^p \triangleright P \\
P > \tilde{x} > Q \\
P | Q
\]

(nil)

(service definition / invoke)

(values output / tuple input)

(label selection / branching)

(return)

(if-then-else)

(restriction)

(polarized session)

(pipe)

(parallel)
SCC Structural Congruence

Axioms

- alpha-conversion
- parallel composition
- name restriction
- garbage collection of terminated sessions
SCC Structural Congruence

Standard axioms (assume $m, y \notin \text{fn}(Q)$ and $r \neq m$)

\[
(\nu m')Q \equiv (\nu m)(Q[m/m']) \\
(\tilde{x}).Q \equiv (\tilde{y}).Q[\gamma/x]
\]

\[
P > \tilde{x} > Q \equiv P > \tilde{y} > (Q[\gamma/x])
\]

\[
P\mid \mathbf{0} \equiv P \\
P\mid Q \equiv Q\mid P \\
(P\mid Q)\mid R \equiv P\mid (Q\mid R)
\]

\[
Q\mid ((\nu m)P) \equiv (\nu m)(Q\mid P) \\
(\nu m)(\nu m')P \equiv (\nu m')(\nu m)P
\]

\[
r^P \triangleright (\nu m)P \equiv (\nu m)(r^P \triangleright P) \\
((\nu m)P) > \tilde{x} > Q \equiv (\nu m)(P > \tilde{x} > Q)
\]

Axioms for garbage collection of terminated sessions

\[
\mathbf{0} > \tilde{x} > P \equiv \mathbf{0} \\
(P\mid Q) > \tilde{x} > R \equiv (P > \tilde{x} > R)(Q > \tilde{x} > R)
\]

\[
(r^P \triangleright \mathbf{0}) > \tilde{x} > R \equiv r^P \triangleright \mathbf{0} \\
(r_1^P \triangleright (Q\mid r_2^g \triangleright \mathbf{0}) \equiv r_1^P \triangleright Q\mid r_2^g \triangleright \mathbf{0}
\]

\[
(\nu r)(r^+ \triangleright \mathbf{0}\mid r^- \triangleright \mathbf{0}) \equiv \mathbf{0}
\]
Main assumptions

Services are

- **persistent** (not consumed after invocations)
- **top-level** (not nested, not dynamically installed)
- **stateless** (no top-level return on service side)

Sessions are

- not interruptable (**close-free** fragment)
- with **non recursive** communication protocols
Example 1: Factorial

Service definition

\[
fatt.(n) . \text{if } (n = 0) \text{ then } \langle 1 \rangle \text{ else } (fatt.(n-1).(x).return x) > x > \langle n \cdot x \rangle
\]

A \textit{fatt} instance waits for a natural number \( n \): if equal to zero then sends back 1 to the client, otherwise issues a (nested) invocation to a fresh instance of \textit{fatt} with argument \( n - 1 \), waits for the response and passes the result \( x \) to a pipe that sends back \( n \cdot x \) to the client.

Service invocation

\[
fatt.(3).(x) \mid fatt.(5).(x).return x
\]

The first client passes the argument 3 to the service instance, then waits for the response; the second client passes a different argument and returns the computed result to the parent session. The protocols of the two clients will run in fresh, separated sessions and will not interfere.
Example 1: Factorial

Service definition

\[
\text{fatt}.(n).\text{if } (n = 0) \text{ then } \langle 1 \rangle \text{ else } (\text{fatt}.\langle n - 1 \rangle.(x).\text{return } x) > x > \langle n \cdot x \rangle
\]

A \textit{fatt} instance waits for a natural number \( n \): if equal to zero then sends back 1 to the client, otherwise issues a \textit{(nested) invocation} to a fresh instance of \textit{fatt} with argument \( n - 1 \), waits for the response and passes the result \( x \) to a pipe that sends back \( n \cdot x \) to the client.

Service invocation

\[
\text{fatt}.\langle 3 \rangle.(x) \mid \text{fatt}.\langle 5 \rangle.(x).\text{return } x
\]

The first client passes the argument 3 to the service instance, then waits for the response; the second client passes a different argument and returns the computed result to the parent session. The protocols of the two clients will run in fresh, separated sessions and will not interfere.
Example 2: Room reservation

Service definition (with branching)

\[
\text{reserve.} \left( \begin{array}{c}
\text{(single).}(x).\langle \text{code}(x,"\"\"\rangle \\
+ \text{(double).}(x, y).\langle \text{code}(x, y)\rangle \\
\end{array} \right)
\]

(where \text{code} : \text{str} \times \text{str} \rightarrow \text{int} is a function only available on service side)

Service invocations (with selection)

\[
\begin{align*}
\text{reserve.(single).} & \langle "\text{Bob}\rangle .(x).\text{return } x \\
\text{reserve.(double).} & \langle "\text{Bob","Leo}\rangle .(y).\text{return } y \\
\text{reserve.if } & (\ldots) \\
\text{then } & \langle \text{single}\rangle .\langle "\text{Bob}\rangle .(x).\text{return } x \\
\text{else } & \langle \text{double}\rangle .\langle "\text{Bob","Leo}\rangle .(y).\text{return } y
\end{align*}
\]
Example 2: Room reservation

Service definition (with branching)

\[ reserve.\left(\text{(single).}(x).\langle\text{code}(x,"")\rangle + \text{(double).}(x,y).\langle\text{code}(x,y)\rangle\right) \]

(where \(\text{code} : \text{str} \times \text{str} \rightarrow \text{int}\) is a function only available on service side)

Service invocations (with selection)

\[
\begin{align*}
\overline{\text{reserve}.\langle\text{single}\rangle.\langle"\text{Bob}\rangle.(x).\text{return } x} \\
\overline{\text{reserve}.\langle\text{double}\rangle.\langle"\text{Bob","Leo}\rangle.(y).\text{return } y} \\
\overline{\text{reserve}.\text{if } (\ldots)} \\
\text{then } \langle\text{single}\rangle.\langle"\text{Bob}\rangle.(x).\text{return } x \\
\text{else } \langle\text{double}\rangle.\langle"\text{Bob","Leo}\rangle.(y).\text{return } y
\end{align*}
\]
Example 3: Proxy service for load balancing

Service definition (with name passing and extrusion)

\[(\nu a, b)(a. P \mid b. P \mid loadbalance. if (\text{choose}(a, b) = 1) \text{ then } \langle a \rangle \text{ else } \langle b \rangle )\]

Service invocation

\[(loadbalance.(z).return z) > x > \bar{z}.Q\]
Example 3: Proxy service for load balancing

Service definition (with name passing and extrusion)

\[(\nu a, b)(a.P \mid b.P \mid loadbalance.if(choose(a,b)=1) then \langle a \rangle else \langle b \rangle)\]

Service invocation

\[(\overline{loadbalance}(z).return z) > x > \overline{z}.Q\]
1. Introduction & Motivation

2. SCC in a Nutshell

3. A Type System for SCC

4. Concluding Remarks
Type judgements

Overall idea

- Type values: $\Gamma \vdash v : S$
- Type a process as if part of a current session:

  $$\Gamma \vdash P : U[T]$$

  separating intra-session interaction $T$ from upward interaction $U$
- The type $T$ of the protocol on one side of a session should be dual w.r.t. the type $T'$ of its partner's protocol ($T = T'$)
- In case of nested sessions, the $U$ typed upward interaction will contribute to the type of its "father" session
Sketch of Typing

Some issues and limitations

- Some flexibility required w.r.t. branching and selection
- Some care needed in parallel composition of protocols
- Some care needed in dealing with the replication due to pipelines
- Recursive invocation of services is possible
- No form of delegation allowed
- Mobility of service names
### Syntax of types

\[
S ::=  [T] \quad \text{(session)} \\
| B \quad \text{(basic data types)} \\
T ::= \text{end} \quad \text{(no action)} \\
| ?(S_1, \ldots, S_n).T \quad \text{(input of a tuple)} \\
| !(S_1, \ldots, S_n).T \quad \text{(output of a tuple)} \\
| \&\{l_1 : T_1, \ldots, l_n : T_n\} \quad \text{(external choice)} \\
| \oplus\{l_1 : T_1, \ldots, l_n : T_n\} \quad \text{(internal choice)} \\
U ::= !(\tilde{S})^k\cdot\text{end} \quad \text{(upward interaction)}
\]

### Dual types

\[
\overline{\text{end}} = \text{end} \quad \overline{?(\tilde{S}).T} = !(\tilde{S}).\overline{T} \quad \overline{\&\{l_i : T_i\}_i} = \oplus\{l_i : \overline{T_i}\}_i \\
\overline{!(\tilde{S}).T'} = ?(\tilde{S}).\overline{T'} \quad \overline{\oplus\{l_i : T_i\}_i} = \&\{l_i : \overline{T_i}\}_i
\]
**Services**

\[(\text{SERVICE})\]
\[
\Gamma, s : S \vdash s : S
\]

\[(\text{TDEF})\]
\[
\begin{align*}
\Gamma \vdash P : \text{end}[T] & & \Gamma \vdash s : [T] \\
\Gamma \vdash s. P : \text{end}[\text{end}] 
\end{align*}
\]

\[(\text{TINV})\]
\[
\begin{align*}
\Gamma \vdash Q : U[\overline{T}] & & \Gamma \vdash s : [T] \\
\Gamma \vdash \overline{s}. Q : \text{end}[U] 
\end{align*}
\]

**Sessions**

\[(\text{TSES})\]
\[
\begin{align*}
\Gamma \vdash P : U[T] \\
\Gamma, r : [T] \vdash r^+ \triangleright P : \text{end}[U] 
\end{align*}
\]

\[(\text{TSESI})\]
\[
\begin{align*}
\Gamma \vdash Q : U[\overline{T}] \\
\Gamma, r : [T] \vdash r^- \triangleright Q : \text{end}[U] 
\end{align*}
\]
Type System Highlights: Services and Sessions

**Services**

(Student)
\[ \Gamma, s : S \vdash s : S \]

(Tdef)
\[ \frac{\Gamma \vdash P : \text{end}[T]}{\Gamma \vdash s \cdot P : \text{end}[\text{end}]} \]

(Tinv)
\[ \frac{\Gamma \vdash Q : U[T]}{\Gamma \vdash \overline{s} \cdot Q : \text{end}[U]} \]

**Sessions**

(Tses)
\[ \frac{\Gamma \vdash P : U[T]}{\Gamma, r : [T] \vdash r^+ \triangleright P : \text{end}[U]} \]

(TsesI)
\[ \frac{\Gamma \vdash Q : U[T]}{\Gamma, r : [T] \vdash r^- \triangleright Q : \text{end}[U]} \]
Type System Highlights: Protocols

Input, output, and return

\[
\begin{align*}
(T_{\text{IN}}) & \quad \Gamma, \tilde{x} : \tilde{S} \vdash P : U[T] \\
& \quad \Gamma \vdash (\tilde{x}).P : U[?(\tilde{S}).T] \\
(T_{\text{TOUT}}) & \quad \Gamma \vdash P : U[T] \quad \Gamma \vdash \tilde{v} : \tilde{S} \\
& \quad \Gamma \vdash \langle \tilde{v} \rangle.P : U[!(\tilde{S}).T] \\
(T_{\text{TRET}}) & \quad \Gamma \vdash P : U[T] \quad \Gamma \vdash \tilde{v} : \tilde{S} \\
& \quad \Gamma \vdash \text{return } \tilde{v}.P : !?(\tilde{S}).U[T]
\end{align*}
\]

Branching and Selection

\[
\begin{align*}
(T_{\text{BRANCH}}) & \quad I \subseteq \{1, \ldots, n\} \quad \forall i \in I. \Gamma \vdash P_i : U[T_i] \\
& \quad \Gamma \vdash \sum_{i=0}^{n} (l_i).P_i : U[\&\{l_i : T_i\}]_{i \in I} \\
(T_{\text{CHOICE}}) & \quad k \in I \quad \Gamma \vdash P : U[T_k] \\
& \quad \Gamma \vdash \langle l_k \rangle.P : U[\oplus\{l_i : T_i\}_{i \in I}]
\end{align*}
\]
Type System Highlights: Protocols

Input, output, and return

(TIN) \[ \Gamma, \bar{x} : \tilde{S} \vdash P : U[T] \]
\[ \Gamma \vdash (\bar{x}).P : U[?(\tilde{S}).T] \]

(TOUT) \[ \Gamma \vdash P : U[T] \quad \Gamma \vdash \bar{v} : \tilde{S} \]
\[ \Gamma \vdash \langle \bar{v} \rangle.P : U[!(\tilde{S}).T] \]

(TRET) \[ \Gamma \vdash P : U[T] \quad \Gamma \vdash \bar{v} : \tilde{S} \]
\[ \Gamma \vdash \text{return} \; \bar{v}.P : !(\tilde{S}).U[T] \]

Branching and Selection

(TBRANCH) \[ I \subseteq \{1, \ldots, n\} \quad \forall i \in I. \Gamma \vdash P_i : U[T_i] \]
\[ \Gamma \vdash \sum_{i=0}^{n} (I_i).P_i : U[\&\{I_i : T_i\}]_{i \in I} \]

(TCHOICE) \[ k \in I \quad \Gamma \vdash P : U[T_k] \]
\[ \Gamma \vdash \langle I_k \rangle.P : U[\oplus\{I_i : T_i\}]_{i \in I} \]
Type System Highlights: Protocols

**Parallel**

$$\begin{align*}
(T_{PRL}) \\
\Gamma \vdash P : !(\tilde{S})^n\text{end}[T] & \quad \Gamma \vdash Q : !(\tilde{S})^m\text{end}[\text{end}] \\
\Gamma \vdash P \mid Q : !(\tilde{S})^{n+m}\text{end}[T]
\end{align*}$$

**Conditional**

$$\begin{align*}
(T_{IF}) \\
\Gamma \vdash v_1 : S & \quad \Gamma \vdash v_2 : S & \quad \Gamma \vdash P : U[T] & \quad \Gamma \vdash Q : U[T] \\
\Gamma \vdash \text{if } v_1 = v_2 \text{ then } P \text{ else } Q : U[T]
\end{align*}$$
Type System Highlights: Protocols

Parallel

\[(\text{TPARL})\]

\[
\Gamma \vdash P : !(\tilde{S})^n.\text{end}[T] \quad \Gamma \vdash Q : !(\tilde{S})^m.\text{end}[\text{end}]
\]

\[
\Gamma \vdash P|Q : !(\tilde{S})^{n+m}.\text{end}[T]
\]

Conditional

\[(\text{TIF})\]

\[
\Gamma \vdash v_1 : S \quad \Gamma \vdash v_2 : S \quad \Gamma \vdash P : U[T] \quad \Gamma \vdash Q : U[T]
\]

\[
\Gamma \vdash \text{if } v_1 = v_2 \text{ then } P \text{ else } Q : U[T]
\]
Main properties

Subject Congruence

If $\Gamma \vdash P : U[T]$ and $P \equiv Q$ then $\Gamma \vdash Q : U[T]$

Subject reduction

- If $\Gamma, r : S \vdash P : U[T]$ and $P \overset{rT}{\rightarrow} Q$ then $\Gamma, r : S' \vdash Q : U[T]$
- If $\Gamma \vdash P : U[T]$ and $P \overset{T}{\rightarrow} Q$ then $\Gamma \vdash Q : U[T]$

$P \overset{rT}{\rightarrow} Q$ means that $Q$ is reached by $P$ after a communication or a selection within session $r$, with $r$ a free name in $P$

$P \overset{T}{\rightarrow} Q$ means that $Q$ is reached by $P$ after interaction in a restricted session or after a service invocation
Main result

Initial processes

- $\emptyset \vdash P : \text{end[end]}$
- $P$ does not contain session constructs
- all service definitions are at the top level

Normal form

$P \equiv (\nu s_1) \cdots (\nu s_n)(s_1.Q_1 | \cdots | s_n.Q_n)$

Deadlock free processes

$P$ such that whenever $P \xrightarrow{\omega}^* Q$ either $Q \xrightarrow{\tau}$ or $Q$ is in normal form.

As a technicality, we modify the LTS so to remove all $(\nu r)$ produced by service invocations, introduce the label $r\iota$ to observe that a service invocation takes place inside session $r$ and let $\omega$ be any sequence of $\tau$, $r\tau$ and $r\iota$ steps.

Deadlock avoidance

If $P$ is an initial process, then it is deadlock free.
Main result

Initial processes

- $\emptyset \vdash P : \text{end[\text{end}]}$
- $P$ does not contain session constructs
- all service definitions are at the top level

Normal form

$$P \equiv (\nu s_1) \ldots (\nu s_n)(s_1.Q_1 | \ldots | s_n.Q_n)$$

Deadlock free processes

$P$ such that whenever $P \xrightarrow{\omega}^* Q$ either $Q \xrightarrow{\tau}$ or $Q$ is in normal form.

As a technicality, we modify the LTS so to remove all $(\nu r)$ produced by service invocations, introduce the label $r\iota$ to observe that a service invocation takes place inside session $r$ and let $\omega$ be any sequence of $\tau$, $r\tau$ and $r\iota$ steps.

Deadlock avoidance

If $P$ is an initial process, then it is deadlock free.
Main result

**Initial processes**
- $\emptyset \vdash P : \text{end[end]}$
- $P$ does not contain session constructs
- all service definitions are at the top level

**Normal form**

$P \equiv (\nu s_1) \cdots (\nu s_n)(s_1.Q_1 | \cdots | s_n.Q_n)$

**Deadlock free processes**

$P$ such that whenever $P \xrightarrow{\omega}^* Q$ either $Q \xrightarrow{\tau}$ or $Q$ is in normal form.

As a technicality, we modify the LTS so to remove all $(\nu r)$ produced by service invocations, introduce the label $r.\iota$ to observe that a service invocation takes place inside session $r$ and let $\omega$ be any sequence of $\tau$, $r.\tau$ and $r.\iota$ steps.

**Deadlock avoidance**

If $P$ is an initial process, then it is deadlock free.
Example: Factorial

Processes

\[
F \equiv \text{fatt.}(n).\text{if } (n = 0)
\text{ then } \langle 1 \rangle
\text{ else } (\text{fatt.}(n - 1).(x).\text{return } x) > x > \langle n \cdot x \rangle
\]

\[
P \equiv \text{fatt.}(3).(x) \mid \text{fatt.}(5).(x).\text{return } x
\]

\[
Q \equiv P > z > \text{fatt.}(z).(x)
\]

Types

\[
\Gamma = \text{fatt} : [(\text{int}).!(\text{int})], \_ : \text{int} \times \text{int} \to \text{int}, \cdot : \text{int} \times \text{int} \to \text{int}
\]

\[
\Gamma \vdash F : \text{end[end]}
\]

\[
\Gamma \vdash P : \text{end}[!(\text{int}).\text{end}]
\]

\[
\Gamma \vdash Q : \text{end[end]}
\]

\[
\emptyset \vdash (\nu \text{fatt})(F|Q) : \text{end[end]}
\]
Example: Factorial

Processes

\[ F \equiv \text{fatt}(n).\text{if } (n = 0) \]
\[ \quad \text{then } \langle 1 \rangle \]
\[ \quad \text{else } (\text{fatt} \langle n - 1 \rangle.(x).\text{return } x) > x > \langle n \cdot x \rangle \]

\[ P \equiv \overline{\text{fatt}}.\langle 3 \rangle.(x) \mid \overline{\text{fatt}}.\langle 5 \rangle.(x).\text{return } x \]

\[ Q \equiv P > z > \overline{\text{fatt}}.\langle z \rangle.(x) \]

Types

\[ \Gamma = \text{fatt} : [?(int).(!(int))], - : \text{int} \times \text{int} \to \text{int}, \cdot : \text{int} \times \text{int} \to \text{int} \]
\[ \Gamma \vdash F : \text{end[end]} \]
\[ \Gamma \vdash P : \text{end[!}(int).\text{end]} \]
\[ \Gamma \vdash Q : \text{end[end]} \]
\[ \emptyset \vdash (\nu \text{fatt})(F \mid Q) : \text{end[end]} \]
1. Introduction & Motivation

2. SCC in a Nutshell

3. A Type System for SCC

4. Concluding Remarks
Conclusion and Future Work

SCC
- Original mix of several ingredients
- Flexible and expressive

Type system
- Strong result over a (reasonable) fragment of SCC
- Difficult to obtain by encoding SCC in other typed calculi

Ongoing work (submitted 2008)
- Subtyping
- Recursive protocols and regular session types
- Type inference (don’t miss Leonardo Mezzina’s talk)

THANKS FOR THE ATTENTION!

Bruni, Mezzina  (DIPISA, IMT LUCCA)  Deadlock Avoidance in SCC  Sensoria Wk on CSOC (2008)
Conclusion and Future Work

**SCC**
- Original mix of several ingredients
- Flexible and expressive

**Type system**
- Strong result over a (reasonable) fragment of SCC
- Difficult to obtain by encoding SCC in other typed calculi

**Ongoing work (submitted 2008)**
- Subtyping
- Recursive protocols and regular session types
- Type inference (*don’t miss Leonardo Mezzina’s talk*)

THANKS FOR THE ATTENTION!