Controlling communication

Hanne Riis Nielson & Flemming Nielson

Informatics & Mathematical Modelling
Technical University of Denmark

Overview

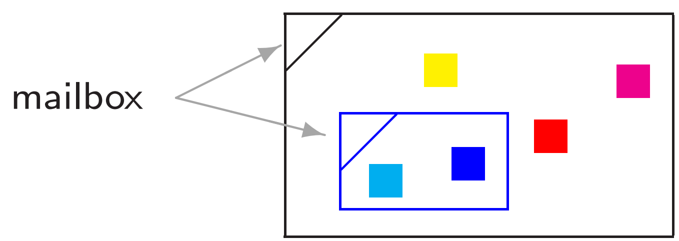
- Local communication
  - mailboxes
  - extending the analysis
- Communication in context
  - boxed ambients
  - extending the analysis
  - variations

Local communication

Cardelli & Gordon

Communication happens via the mailboxes of the ambients

- all communication is local between the top-level processes of an ambient
- long distance communication is a combination of local communication and movement within the ambient hierarchi
- ambient names as well as sequences of capabilities can be exchanged



Syntax:

$\langle msg \rangle$	output the message msg (asynchronously) to the mailbox
$(x).P$	input a message from the mailbox, bind it to x and continue as P

Example: communicating the destination

$\mathsf{A}[\,\mathsf{p}[(x).\,\mathsf{out}\;\mathsf{A}.\,\mathsf{in}\;x \mid \mathsf{open}\;\mathsf{C}\,] \mid \mathsf{C}[\mathsf{in}\;\mathsf{p}.\,\langle \mathsf{B}\rangle]\,] \mid \mathsf{B}[\,\mathsf{open}\;\mathsf{p}\,]$

$\longrightarrow \mathsf{A}[\,\mathsf{p}[(x).\,\mathsf{out}\;\mathsf{A}.\,\mathsf{in}\;x \mid \mathsf{open}\;\mathsf{C} \mid \mathsf{C}[\langle \mathsf{B}\rangle]\,]\,] \mid \mathsf{B}[\,\mathsf{open}\;\mathsf{p}\,]$ C enters p

$\longrightarrow \mathsf{A}[\,\mathsf{p}[(x).\,\mathsf{out}\;\mathsf{A}.\,\mathsf{in}\;x \mid \langle \mathsf{B}\rangle\,]\,] \mid \mathsf{B}[\,\mathsf{open}\;\mathsf{p}\,]$ C is opened

$\longrightarrow \mathsf{A}[\,\mathsf{p}[\,\mathsf{out}\;\mathsf{A}.\,\mathsf{in}\;\mathsf{B}\,]] \mid \mathsf{B}[\,\mathsf{open}\;\mathsf{p}\,]$ the name B is exchanged

$\longrightarrow \mathsf{A}[\;] \mid \mathsf{p}[\,\mathsf{in}\;\mathsf{B}\,] \mid \mathsf{B}[\,\mathsf{open}\;\mathsf{p}\,]$

$\longrightarrow \mathsf{A}[\;] \mid \mathsf{B}[\,\mathsf{p}[\;] \mid \mathsf{open}\;\mathsf{p}\,]$

$\longrightarrow \mathsf{A}[\;] \mid \mathsf{B}[\;]$

Example: communicating the route

$\mathsf{A}[\,\mathsf{p}[(\mathsf{x}).\,\mathsf{x} \mid \mathsf{open}\ \mathsf{C}\,] \mid \mathsf{C}[\mathsf{in}\ \mathsf{p}.\ \langle \mathsf{out}\ \mathsf{A}.\ \mathsf{in}\ \mathsf{B}\rangle]\,] \mid \mathsf{B}[\,\mathsf{open}\ \mathsf{p}\,]$

$\longrightarrow\ \mathsf{A}[\,\mathsf{p}[(\mathsf{x}).\,\mathsf{x} \mid \mathsf{open}\ \mathsf{C} \mid \mathsf{C}[\langle \mathsf{out}\ \mathsf{A}.\ \mathsf{in}\ \mathsf{B}\rangle]\,]]\, \mid \mathsf{B}[\,\mathsf{open}\ \mathsf{p}\,]$ C enters p

$\longrightarrow\ \mathsf{A}[\,\mathsf{p}[(\mathsf{x}).\,\mathsf{x} \mid \langle \mathsf{out}\ \mathsf{A}.\ \mathsf{in}\ \mathsf{B}\rangle\,]] \mid \mathsf{B}[\,\mathsf{open}\ \mathsf{p}\,]$ C is opened

$\longrightarrow\ \mathsf{A}[\,\mathsf{p}[\,\mathsf{out}\ \mathsf{A}.\ \mathsf{in}\ \mathsf{B}\,]] \mid \mathsf{B}[\,\mathsf{open}\ \mathsf{p}\,]$ the capability out A. in B is exchanged

$\longrightarrow\ \mathsf{A}[\ ] \mid \mathsf{p}[\,\mathsf{in}\ \mathsf{B}\,] \mid \mathsf{B}[\,\mathsf{open}\ \mathsf{p}\,]$

$\longrightarrow\ \mathsf{A}[\ ] \mid \mathsf{B}[\,\mathsf{p}[\ ] \mid \mathsf{open}\ \mathsf{p}\,]$

$\longrightarrow\ \mathsf{A}[\ ] \mid \mathsf{B}[\ ]$

Syntax

$$\begin{array}{rcl} P & ::= & \cdots \mid \langle M_1, \cdots, M_k \rangle \mid (x_1, \cdots, x_k).\, P \\ M & ::= & \text{in } N \mid \text{out } N \mid \text{open } N \mid N \mid M.M' \mid \epsilon \\ N & ::= & n \mid x \end{array}$$

Obs: elements of the syntactic categories M and N may denote ambient names as well as sequences of capabilities — they must be used consistently in the syntax.

This can e.g. be expressed by a simple type system distinguishing between ambient names and capabilities.

Semantics

Extensions to the transition relation:

$$\langle M_1, \cdots, M_k \rangle \mid (x_1, \cdots, x_k).\, P \;\rightarrow\; P\{x_1 \leftarrow M_1, \cdots, x_k \leftarrow M_k\}$$

Extensions to the structural congruence relation:

$$P \equiv Q \;\Rightarrow\; (x_1, \cdots, x_k).\, P \equiv (x_1, \cdots, x_k).\, Q$$

$$\epsilon.P \equiv P$$

$$(M.M').P \equiv M.(M'.P)$$

Example: Encryption and decryption

- Encryption of plaintext msg with key key (assuming $\mathsf{key} \notin \underline{\mathsf{fn}}(\mathsf{msg})$):

$$\mathsf{key}\,[\langle \mathsf{msg} \rangle]$$

- Decryption of ciphertext C encrypted with key key:

$$\mathsf{C} \mid \mathsf{open}\ \mathsf{key}.(\mathsf{x}).\mathsf{x}$$

as in

$$\begin{aligned} \mathsf{key}\,[\langle \mathsf{msg} \rangle] \mid \mathsf{open}\ \mathsf{key}.(x).x \quad &\longrightarrow \quad \langle \mathsf{msg} \rangle \mid (\mathsf{x}).\mathsf{x} \\ &\longrightarrow \quad \mathsf{msg} \end{aligned}$$

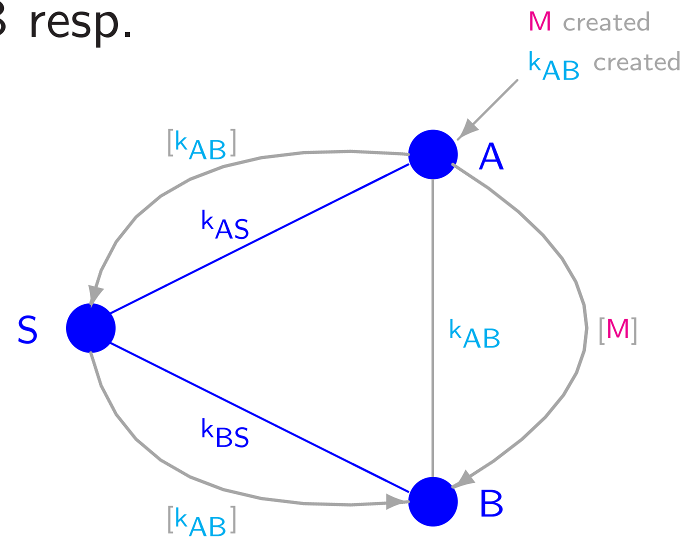
"As usual": perfect cryptology assumed

Wide Mouthed Frog protocol

Given: Agents A, S and B

Keys k_{AS}, k_{BS} between S and A and B resp.

$$
\begin{array}{l}
A\,[(\nu\, M : \mathsf{Msg})(\nu\, k_{AB} : \mathsf{Key}) \\
\quad k_{AS}\,[\,\mathsf{out}\ A.\ \mathsf{in}\ S.\ \langle k_{AB}\rangle\,]\ \mid \\
\quad k_{AB}\,[\,\mathsf{out}\ A.\ \mathsf{in}\ B.\ \langle M\rangle\,]\,] \\
\mid \\
S\,[\,\mathsf{open}\ k_{AS}.\ (x).\ k_{BS}\,[\,\mathsf{out}\ S.\ \mathsf{in}\ B.\ \langle x\rangle\,]\,] \\
\mid \\
B\,[\,\mathsf{open}\ k_{BS}.\ (y).\ \mathsf{open}\ y.\ (z).\ z\,]
\end{array}
$$



Adapting the analysis

We must keep track of

- the contents of the mailboxes of the groups:

$$\mathcal{C} : \mathbf{Group} \to \mathcal{P}(\mathbf{Group} \cup \mathbf{Cap})$$

- the values bound to the variables:

$$\mathcal{R} : \mathbf{Var} \to \mathcal{P}(\mathbf{Group} \cup \mathbf{Cap})$$

- who is inside whom (as before):

$$\mathcal{I} : \mathbf{Group} \to \mathcal{P}(\mathbf{Group} \cup \mathbf{Cap})$$

Judgements:

$$\boxed{(\mathcal{I}, \mathcal{C}, \mathcal{R}) \models^{\mu}_{\Gamma} P}$$

Example: Encryption and decryption

$$(\mathcal{I}, \mathcal{C}, \mathcal{R}) \models^{\star}_{\Gamma} \mathsf{key}\,[\,\langle \mathsf{msg} \rangle\,] \mid \mathsf{open}\ \mathsf{key}.\ (\mathsf{x}).\ \mathsf{x}$$

will hold for

Γ	
key	$\mathbb{K}$
msg	$\mathbb{M}$

$\mathcal{I}$	
$\star$	$\mathbb{K}$, open $\mathbb{K}$, $\mathbb{M}$
$\mathbb{K}$	
$\mathbb{M}$	

$\mathcal{C}$	
$\star$	$\mathbb{M}$
$\mathbb{K}$	$\mathbb{M}$
$\mathbb{M}$	

$\mathcal{R}$	
x	$\mathbb{M}$

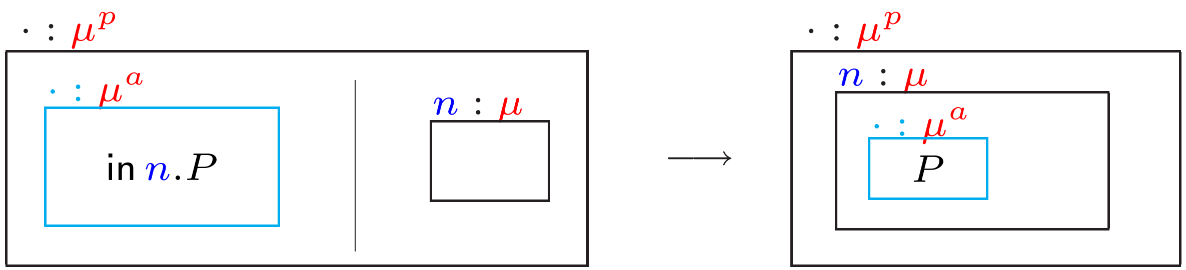
Recall: $\mathcal{C}$: the potential contents of the mailboxes

$\mathcal{R}$: the potential values bound to the variables

Analysis of in-capability (as before)

$$
\begin{aligned}
(\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} \mathsf{in}\, n.\ P \ \underline{\text{iff}} \quad & \mathsf{in}\ \mu \in \mathcal{I}(\star)\ \wedge\ (\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} P\ \wedge \\
& \forall\, \mu^a, \mu^p :\ \mathsf{in}\ \mu \in \mathcal{I}(\mu^a)\ \wedge \\
& \qquad\qquad\quad \mu^a \in \mathcal{I}(\mu^p)\ \wedge \\
& \qquad\qquad\quad \mu \in \mathcal{I}(\mu^p) \\
& \qquad\quad\ \Rightarrow\ \mu^a \in \mathcal{I}(\mu) \\
& \text{where } \mu = \Gamma(n)
\end{aligned}
$$

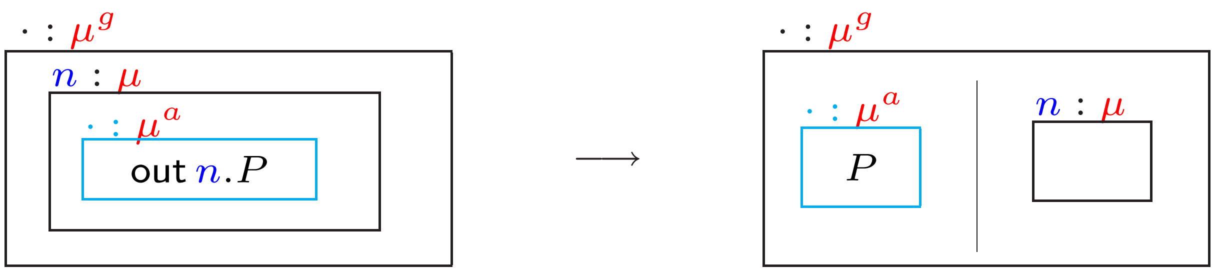
Mimicking the semantics:



Analysis of out-capability (as before)

$$
\begin{aligned}
(\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} \text{out}\, n.\ P\ \underline{\text{iff}}\quad & \text{out}\ \mu \in \mathcal{I}(\star)\ \wedge\ (\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} P\ \wedge \\
& \forall\ \mu^a, \mu^g :\ \ \text{out}\ \mu \in \mathcal{I}(\mu^a) \wedge \\
& \qquad\qquad \mu^a \in \mathcal{I}(\mu)\ \wedge \\
& \qquad\qquad \mu \in \mathcal{I}(\mu^g) \\
& \qquad\ \ \Rightarrow\ \ \mu^a \in \mathcal{I}(\mu^g) \\
& \text{where } \mu = \Gamma(n)
\end{aligned}
$$

Mimicking the semantics:



Analysis of open-capability

$$(\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} \text{open}\, n.\ P \ \underline{\text{iff}} \quad \text{open}\ \mu \in \mathcal{I}(l) \ \wedge\ (\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} P \ \wedge$$

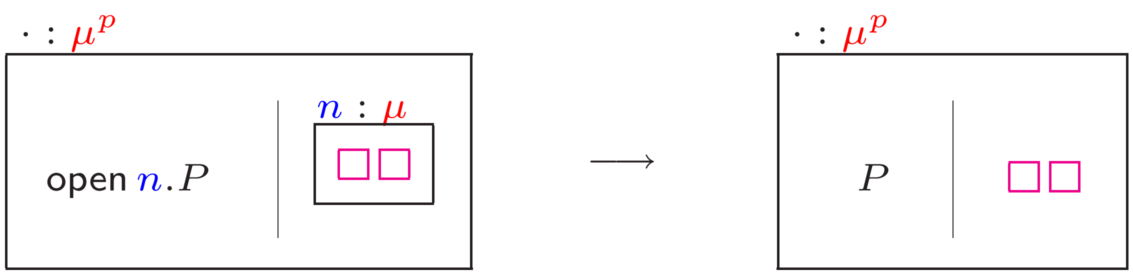
$$\forall\ \mu^p : \ \ \text{open}\ \mu \in \mathcal{I}(\mu^p) \ \wedge$$

$$\mu \in \mathcal{I}(\mu^p)$$

$$\Rightarrow\ \ \mathcal{I}(\mu) \subseteq \mathcal{I}(\mu^p) \ \wedge\ \ \mathcal{C}(\mu) \subseteq \mathcal{C}(\mu^p)$$

where $\mu = \Gamma(n)$

Mimicking the semantics:



Analysis of monadic input/output

$$(\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} \langle M \rangle \quad \underline{\text{iff}} \quad \mathcal{M}_{\Gamma,\mathcal{R}}(M) \subseteq \mathcal{C}(\star)$$

M is communicated inside $\star$

where

$$\begin{aligned}
\mathcal{M}_{\Gamma,\mathcal{R}}(\mathsf{in}\ N) &= \{\mathsf{in}\,\mu \mid \mu \in \mathcal{N}_{\Gamma,\mathcal{R}}(N)\} \\
\mathcal{M}_{\Gamma,\mathcal{R}}(\mathsf{out}\ N) &= \{\mathsf{out}\,\mu \mid \mu \in \mathcal{N}_{\Gamma,\mathcal{R}}(N)\} \\
\mathcal{M}_{\Gamma,\mathcal{R}}(\mathsf{open}\ N) &= \{\mathsf{open}\,\mu \mid \mu \in \mathcal{N}_{\Gamma,\mathcal{R}}(N)\} \\
\mathcal{M}_{\Gamma,\mathcal{R}}(N) &= \mathcal{N}_{\Gamma,\mathcal{R}}(N) \\
\mathcal{M}_{\Gamma,\mathcal{R}}(M.M') &= \mathcal{M}_{\Gamma,\mathcal{R}}(M) \cup \mathcal{M}_{\Gamma,\mathcal{R}}(M') \\
\mathcal{M}_{\Gamma,\mathcal{R}}(\epsilon) &= \emptyset \\
\mathcal{N}_{\Gamma,\mathcal{R}}(x) &= \mathcal{R}(x) \\
\mathcal{N}_{\Gamma,\mathcal{R}}(n) &= \{\mu\} \text{ where } \mu = \Gamma(n)
\end{aligned}$$

$$(\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} (x).\,P \quad \underline{\text{iff}} \quad \mathcal{C}(\star) \subseteq \mathcal{R}(x) \ \wedge \ (\mathcal{I},\mathcal{C},\mathcal{R}) \models^{\star}_{\Gamma} P$$

x is bound inside $\star$

Polyadic input/output

$$P \quad ::= \quad \cdots \mid (x_1, \cdots, x_k).\, P \mid \langle M_1, \cdots, M_k \rangle$$

- Relational method: record information about the individual tuples

$$\mathcal{C} : \mathbf{Group} \rightarrow \mathcal{P}((\mathbf{Group} \cup \mathbf{Cap})^*)$$

- Independent attribute method: record information about the individual components of the tuples

$$\mathcal{C} : \mathbf{Group} \rightarrow (\mathcal{P}(\mathbf{Group} \cup \mathbf{Cap}))^*$$

Exchange analysis

For mobile ambients extended with communication:

Property: What is the topic of conversation for the ambient n?

- no communication at all
- exchange of ambient names only
- exchange of capabilities only

In the analysis: Assume $(\mathcal{I}, \mathcal{C}, \mathcal{R}) \models^{\star}_{\Gamma} P$ and let $\mu = \Gamma(\mathsf{n})$

- no communication: $\mathcal{C}(\mu) = \emptyset$
- only names: $\mathcal{C}(\mu) \subseteq \mathbf{Group}$
- only capabilities: $\mathcal{C}(\mu) \subseteq \mathbf{Cap}$