A Fully Abstract Model for Higher-Order Mobile Ambients

joint paper with Mariangiola Dezani-Ciancaglini

Mikado meeting, February 19, 2002

”Filter” Models

- Filter models are designed via type systems.
- The interpretation of a term is the set of its possible typings.
- Types as properties of terms. Each type represent a *finite* piece of information.
- To have a model we usually need strong undecidable type systems. The next step is to define decidable and effective restriction.

Motivations of this paper

- Define a denotational (compositional) model of a (higher order) Calculus for Mobility (the Ambient Calculus), provided with the "observational" preorder $\sqsubseteq$)

- We want a model M which is Adequate with respect to $\sqsubseteq$ (what is true in the model is true w.r.t. $\sqsubseteq$). Adequate models can be safely used to check properties of the underlying systems.

- As a reference property we want here that the model is also Complete with respect to $\sqsubseteq$ (what is true w.r.t. $\sqsubseteq$ is true in the model). In this case M is said to be Fully Abstract with respect to $\sqsubseteq$.

- A key problem: to find a natural semantic counterpart of the notions of *location* and *mobility*.

The ”Logical” Semantics

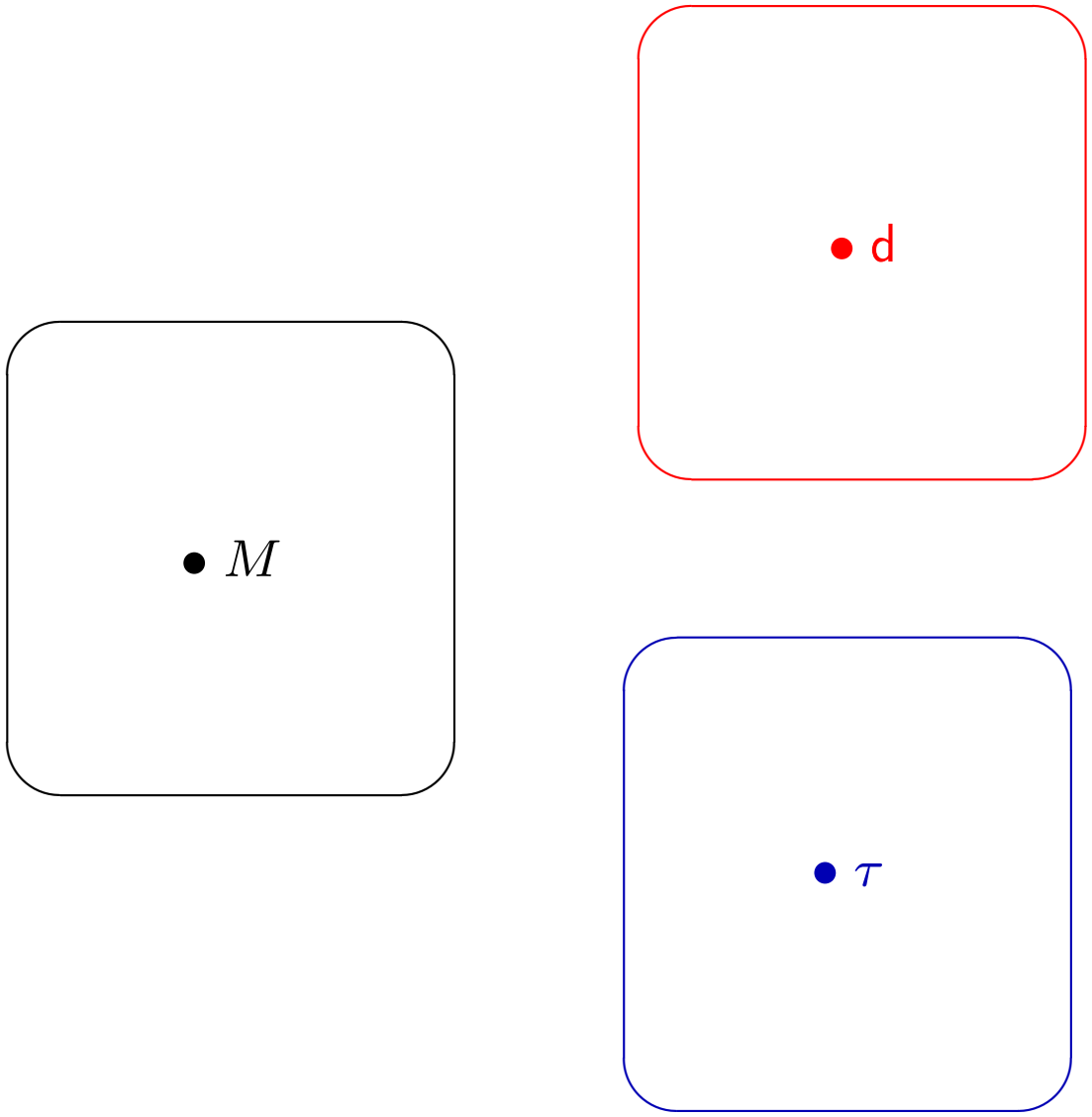
Domains are described by abstract filters of logical formulas (types) expressing properties of the terms of the calculus.

Some basic refernces

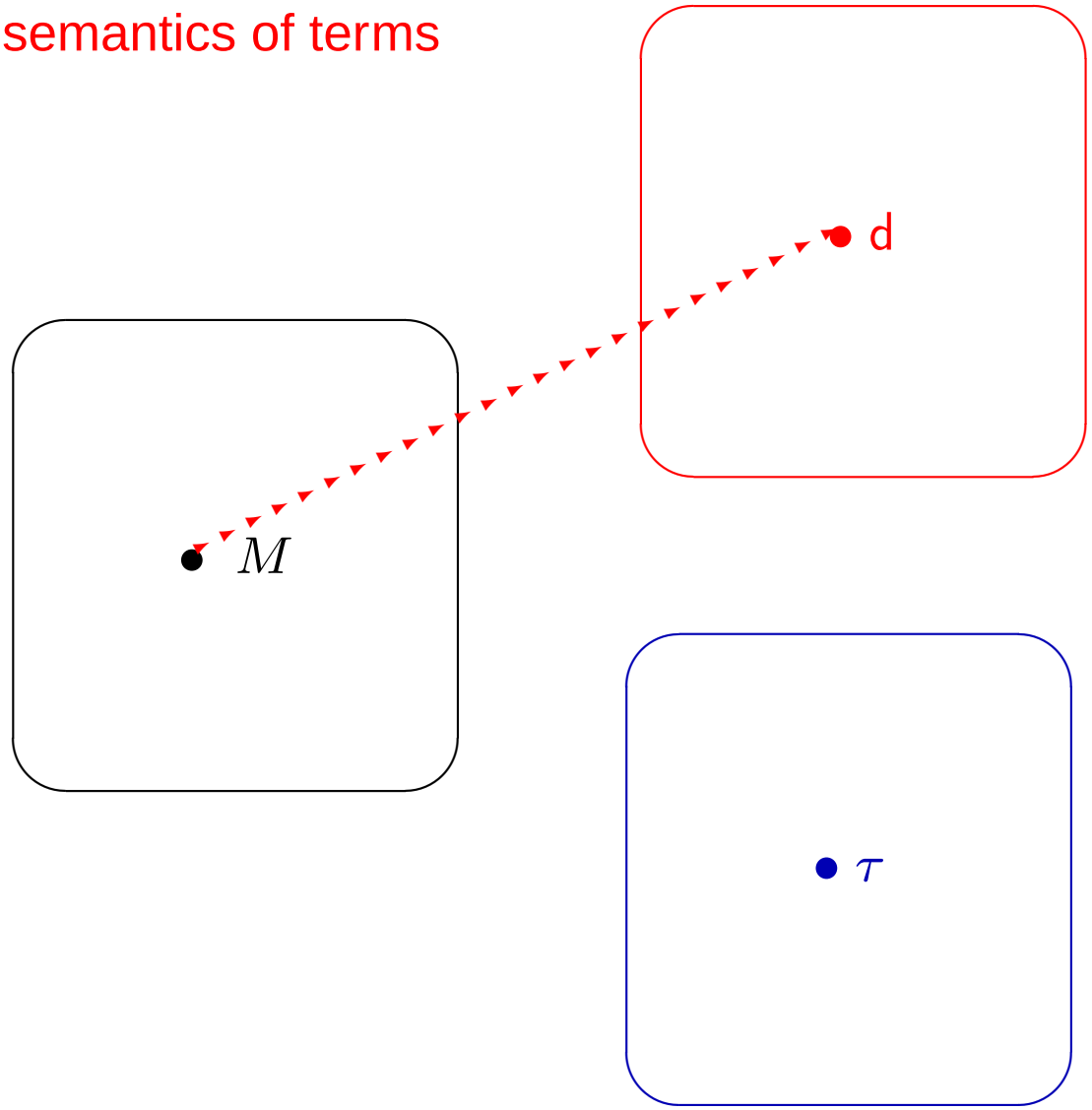
- Scott(1982)
- Barendregt-Coppo-Dezani (1983)
- Abramsky (1991)
- Buodol (1994)
- Hennessy (1994)

Other work has been done on this subject, in particular Damiani-Dezani-Giannini(1999), Coppo-Dezani(2000).

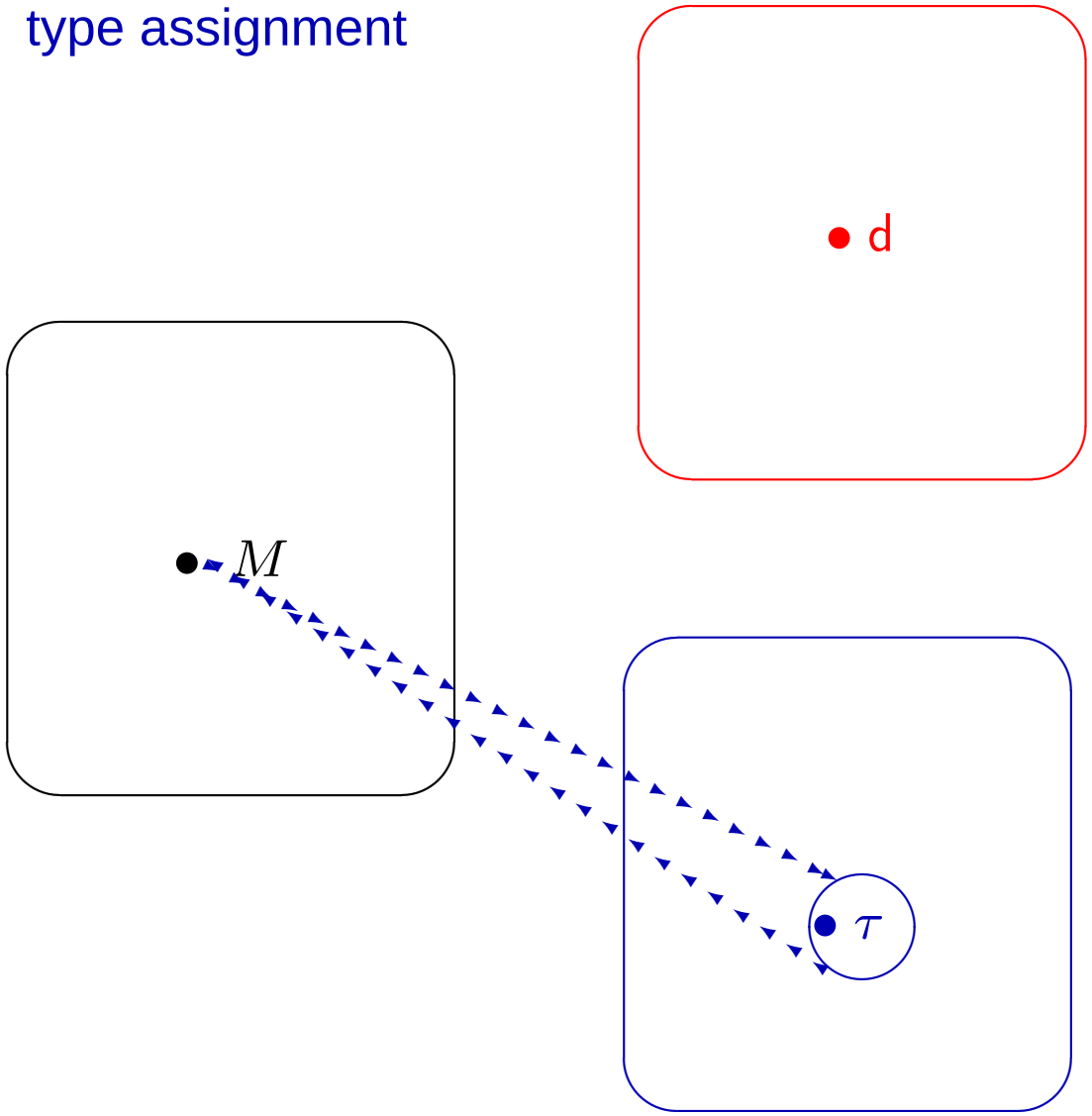
With this approach one can get a model starting from a (suitable) set of logical properties (types) of the language.


d
M
τ

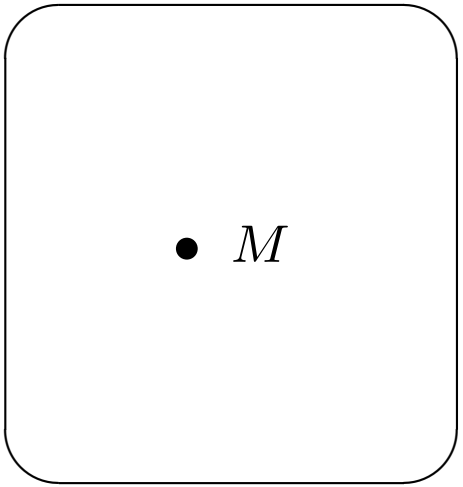
semantics of terms

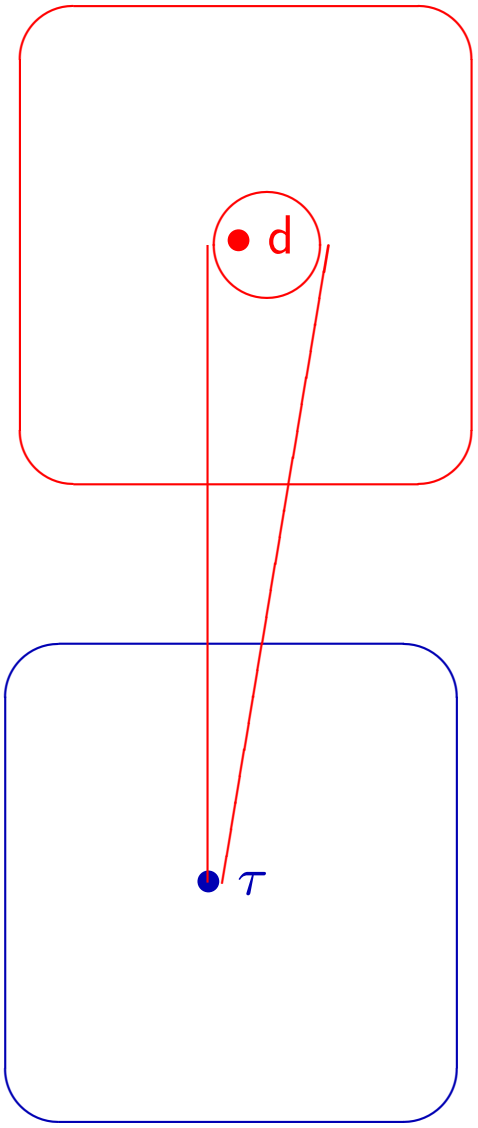


type assignment



semantics of types

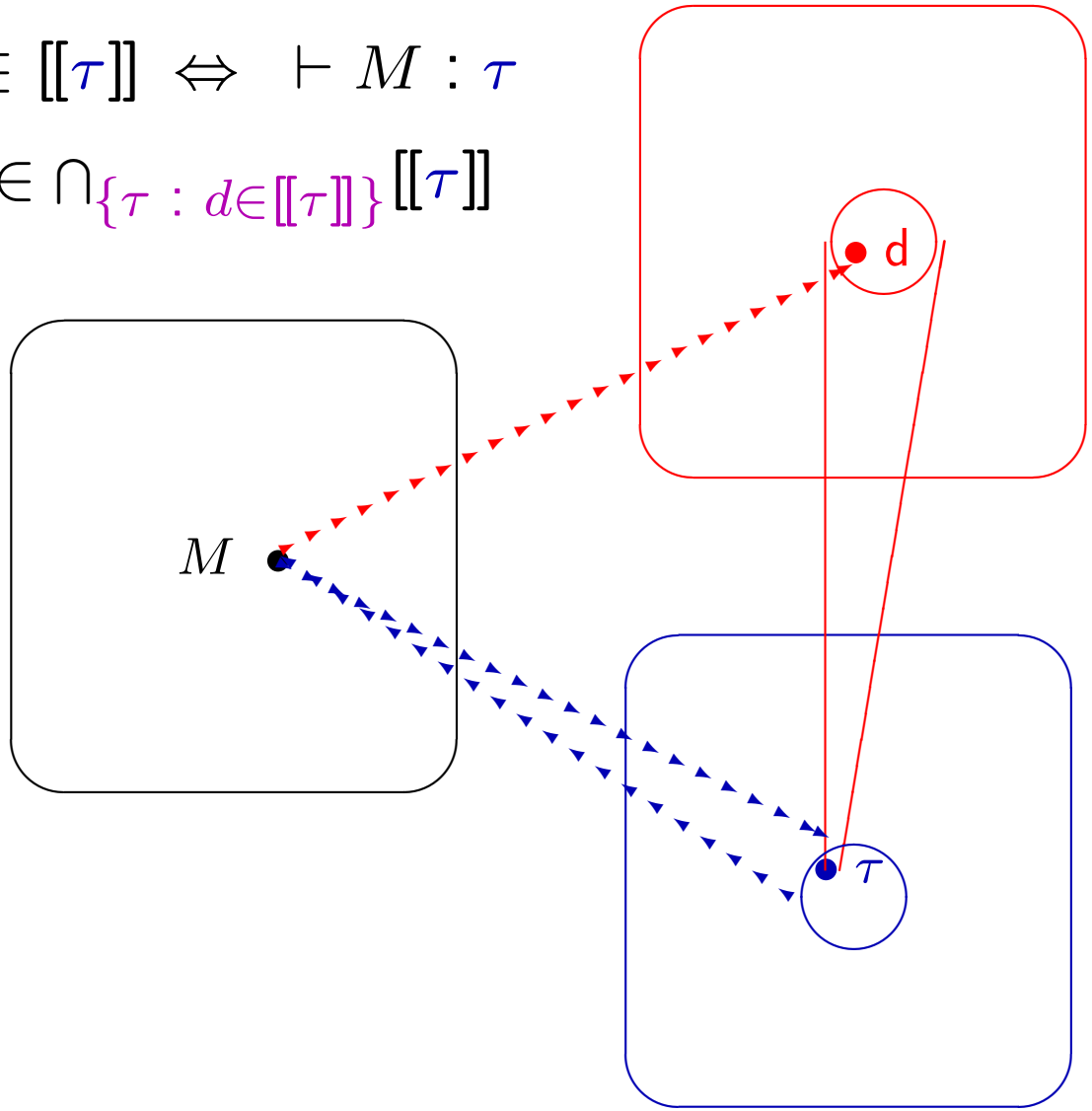




$\mathsf{d} = [\![M]\!]$

$\mathsf{d} \in [\![\tau]\!] \Leftrightarrow \vdash M : \tau$

$\mathsf{d} \in \bigcap_{\{\tau \,:\, d \in [\![\tau]\!]\}} [\![\tau]\!]$



The set $\{\tau \mid d \in [\![\tau]\!]\}$ is a *filter*. The set of all filters of types defines a domain.

A Higher Order Ambient Calculus

$$
\begin{array}{rcl}
\mathcal{P} & ::= & \mathbf{0} \mid X \\
& & in\, a.\mathcal{P} \mid out\, a.\mathcal{P} \mid open\, a.\mathcal{P} \mid (X).\mathcal{P} \mid \langle \mathcal{P} \rangle.\mathcal{P} \\
& & a[\mathcal{P}] \\
& & \mathcal{P} \mid \mathcal{P} \\
& & !\mathcal{P}.
\end{array}
$$

where a represent an Ambient Names and X a Process Variable.

Note: the pure λ-calculus can be easily represented:

- $trans(\lambda X.M) = (X).trans(M)$
- $trans(MN) = trans(M) \mid \langle trans(N) \rangle$

Operational Semantics

$$
\begin{array}{lll}
(red\ in) & a[in\, b.P \mid Q] \mid b[R] & \rightarrow \quad b[a[P \mid Q] \mid R] \\
(red\ out) & a[b[out\, a.P \mid Q] \mid R] & \rightarrow \quad a[R] \mid b[P \mid Q] \\
(red\ open) & open\, a.P \mid a[Q] & \rightarrow \quad P \mid Q \\
(comm) & (X).P \mid \langle Q \rangle.R & \rightarrow \quad P[X := Q] \mid R \\
(R - par) & P \rightarrow Q & \Rightarrow \quad P \mid R \rightarrow Q \mid R \\
(R - amb) & P \rightarrow Q & \Rightarrow \quad a[P] \rightarrow a[Q] \\
(R- \equiv) & P' \equiv P' \quad P \rightarrow Q \quad Q \equiv Q' & \Rightarrow \quad P' \rightarrow Q'
\end{array}
$$

where $\equiv$ is the minimal congruence which:

- satisfies $!P \equiv P \mid !P$ and α-conversion.
- makes $\mid$ commutative, associative with **0** as neutral element.

Observational Equivalence

- Define $P \Downarrow a$ if $P \rightarrow^* a[Q] \mid R$ for some processes Q, R.
- $P \sqsubseteq Q$ if for all context $\mathcal{C}[\ ]$ and ambients a: $\mathcal{C}[P] \Downarrow a \Rightarrow \mathcal{C}[Q] \Downarrow a$.
- $P \cong Q$ if $P \sqsubseteq Q$ and $Q \sqsubseteq P$.

Note. $P \rightarrow Q \Rightarrow Q \sqsubseteq P$. But in general $P \not\cong Q$.

Example:

$$P_1 = open\, a \mid a[b[\mathbf{0}]] \rightarrow b[\mathbf{0}] = P_2$$

But $P_1 \not\cong P_2$ (take $\mathcal{C}[\ ]$ as $[-]$).

remark

Take rule

$$(red\ in)\quad a[in\, b.P \mid Q] \mid b[R] \quad \rightarrow \quad b[a[P \mid Q] \mid R]$$

Note that, if $P \equiv out\, b.in\, b.P'$

$$\begin{aligned} a[in\, b.out\, b.in\, b.P' \mid Q] \mid b[R] &\rightarrow b[a[out\, b.in\, b.P' \mid Q] \mid R] \\ &\rightarrow a[out\, b.in\, b.P'] \mid b[Q] \mid R \\ &\rightarrow b[a[P' \mid Q] \mid R] \end{aligned}$$

i.e. $\boxed{in\, b.P \sqsubseteq in\, b.out\, b.in\, b.P}$

The Set of Types

$$
\begin{array}{rcl}
\mathcal{T} & ::= & \omega \\
 & & in\, a.\mathcal{T} \quad | \quad out\, a.\mathcal{T} \quad | \quad open\, a.\mathcal{T} \\
 & & \langle \mathcal{T}^{-} \rangle.\mathcal{T} \quad | \quad (\mathcal{T}^{-}).\mathcal{T} \\
 & & a[\mathcal{T}] \\
 & & \mathcal{T} \mid \mathcal{T} \\
 & & \mathcal{T} \wedge \mathcal{T}
\end{array}
$$

where where $a \in \mathcal{L}$ and $\mathcal{T}^{-}$ is the set of simple types, not containing $\wedge$.

Partial Order Relation ($\leq$) over types: axioms and rules

- Commutativity and distributivity of $|$ . . . .
- Axioms for ω: $(\omega 1)\quad \alpha \leq \omega \qquad (\omega 2)\quad \alpha \simeq \alpha \,|\, \omega$
- Distributivity of $\wedge$ (example)

$$([\,]\wedge)\quad a[\alpha \wedge \beta] \simeq a[\alpha] \wedge a[\beta]\quad \ldots$$

- Sequentialization. Let m denote a mobility or in-out action $\{in\, a, \ldots, (X), \langle P\rangle\}$

$(.\,|_1)$ $\mathsf{m}.\alpha \,|\, \beta \leq \mathsf{m}.(\alpha \,|\, \beta)$

$(.\,|_2)$ $\mathsf{m}.\alpha \,|\, \mathsf{n}.\beta \simeq \mathsf{m}.(\alpha \,|\, \mathsf{n}.\beta) \wedge \mathsf{n}.(\mathsf{m}.\alpha \,|\, \beta)$ if m does not match n

$(comm)$ $(\sigma).\beta \,|\, \langle\tau\rangle.\gamma \simeq \underbrace{\beta \,|\, \gamma}_{sync.} \wedge \underbrace{(\sigma).(\beta \,|\, \langle\tau\rangle.\gamma)}_{input\ first} \wedge \underbrace{\langle\tau\rangle.((\alpha).\beta \,|\, \gamma)}_{output\ first}$ if $\tau \leq \sigma$

(continue)

- Reduction

$$(in) \quad a[in\, b.\alpha \mid \beta] \mid b[\gamma] \leq b[a[\alpha \mid \beta] \mid \gamma]$$

$$(out) \quad a[b[out\, a.\alpha \mid \beta] \mid \gamma] \leq a[\gamma] \mid b[\alpha \mid \beta]$$

$$(open) \quad open\, a.\alpha \mid a[\beta] \leq \alpha \mid \beta$$

$$(out-in) \quad in\, a.out\, a.in\, a.\alpha \leq in\, a.\alpha$$

$$(in-out) \quad out\, a.in\, a.out\, a.\alpha \leq out\, a.\alpha$$

(continue)

- Congruence (example)

$$(cg - [\,]) \quad \frac{\alpha \leq \beta}{a[\alpha] \leq a[\beta]} \quad \ldots$$

- Transitivity . . .

- Logical (for $\wedge$) . . .

Note: $\alpha \,|\, \beta \leq \alpha \qquad \alpha \,|\, \beta \leq \alpha$

$\alpha \,|\, \beta \leq \alpha \wedge \beta$

Type Assignment Rules

$$(\omega) \qquad \Gamma \vdash P : \omega$$

$$(\mathsf{m}^{\updownarrow}) \qquad \frac{\Gamma \vdash P : \alpha \quad (\mathsf{m} \in \mathcal{M}^{\updownarrow}}{\Gamma \vdash \mathsf{m}.P : \mathsf{m}.\alpha}$$

$$(input) \qquad \frac{\Gamma, X : \sigma \vdash P : \alpha}{\Gamma \vdash (X).P : (\sigma).\alpha}$$

$$(output) \qquad \frac{\Gamma \vdash P : \sigma \quad \Gamma \vdash Q : \alpha}{\Gamma \vdash \langle P \rangle.Q : \langle \sigma \rangle.\alpha}$$

$$(amb) \qquad \frac{\Gamma \vdash P : \alpha}{\Gamma \vdash a[P] : a[\alpha]}$$

$$(\,|\,) \qquad \frac{\Gamma \vdash P : \alpha \quad \Gamma \vdash Q : \beta}{\Gamma \vdash P \,|\, Q : \alpha \,|\, \beta}$$

$$(!) \qquad \frac{\Gamma \vdash P : \alpha \quad \Gamma \vdash !P : \beta}{\Gamma \vdash !P : \alpha \,|\, \beta}$$

$$(\leq) \qquad \frac{\Gamma \vdash P : \alpha \quad \alpha \leq \beta}{\Gamma \vdash P : \beta}$$

where $\mathcal{M}^{\updownarrow} = \{in\, a,\ out\, a.\ open\, a\}$ for all $a \in \mathcal{L}$.

EXAMPLE

A derivable typing:

$$\vdash !((X).b[in\, a.X]) \mid a[!(open\, b) \mid P] \mid \langle open\, c.\, Q \mid R \rangle : a[open\, c.\omega]$$

Basic Properties

Subject Congruence. $P \equiv Q$ and $\vdash Q : \alpha \quad \Rightarrow \quad \vdash P : \alpha.$

Subject Expansion $P \rightarrow^* Q$ and $\vdash Q : \alpha \quad \Rightarrow \quad \vdash P : \alpha.$

Admissibility of $(\wedge I)$**.** Rule

$$(\wedge I) \qquad \frac{\vdash P : \alpha \quad \vdash P : \beta}{\vdash P : \alpha \wedge \beta}$$

is admissible.

The Filter Model

Let $\langle D; \sqsubseteq \rangle$ be a preorder.

A subset L of D is a filter if:

- L is a non-empty upper set ($l \in L$ and $l \sqsubseteq l'$ imply $l' \in L$)
- and every finite subset of L has a greatest lower bound in L

Fact. $\langle \mathcal{T}, \leq \rangle$ is a preorder in which $\wedge$ represent *glb*.

Let $\mathcal{F}(\mathcal{T})$ be the set of filters over $\mathcal{T}$.

Then $\mathcal{F}(\mathcal{T})$ is a consistently complete ω-algebraic c.p.o..

Operators

$\widetilde{in}, \widetilde{out}, \widetilde{open}, \widetilde{amb} : \mathcal{L} \times \mathcal{F}(\mathcal{T}) \to \mathcal{F}(\mathcal{T})$ are defined by:

- $\widetilde{in}\,(a, F) \;=\; \uparrow \{in\, a.\alpha \mid \alpha \in F\}$

- $\widetilde{out}\,,\ \widetilde{open}$ are similar

- $\widetilde{amb}(a, F) \;=\; \uparrow \{a[\alpha] \mid \alpha \in F\}$

$\widetilde{par} : \mathcal{F}(\mathcal{T}) \times \mathcal{F}(\mathcal{T}) \to \mathcal{F}(\mathcal{T})$ are defined by:

- $\widetilde{par}(F, G) \;=\; \uparrow \{\alpha \,|\, \beta \mid \alpha \in F$ and $\beta \in G\}$

Interpretation in $\mathcal{F}(\mathcal{T})$

Let $\rho : \mathcal{V} \to \mathcal{F}(\mathcal{T})$:

- $[[\mathbf{0}]]_\rho \;=\; \uparrow\{\omega\}$

- $[[in\, a.P]]_\rho \;=\; \widetilde{in}\,(a, [[P]]_\rho)$

- ($[[out\, a.P]]_\rho$, $[[open\, a.P]]_\rho$, $[[a[P]]]_\rho$ are similar)

- $[[(X).P]]_\rho \;=\; \uparrow\{(\alpha).\beta \mid \beta \in [[P]]_{\rho[X:=\uparrow\{\alpha\}]}\}$

- $[[\langle P\rangle.Q]]_\rho \;=\; \uparrow\{\langle\alpha\rangle.\beta \mid \alpha \in [[P]]_\rho \;and\; \beta \in [[Q]]_\rho\}$

Interpretation in $\mathcal{F}(\mathcal{T})$ (continue)

- $[[P \mid Q]] \;=\; \widetilde{par}([[P]], [[Q]])$.

- $[[!P]] \;=\; fix(\lambda X \in \mathcal{F}(\mathcal{T}).\, \widetilde{par}([[P]], X))$.

Fact. $[[P]]_\rho = \{\alpha \in \mathcal{T} \mid \Gamma_\rho \vdash P : \alpha\}$.

Note: $[[(X).P \mid \langle Q \rangle.R]]$ contains:

$$\{\alpha \mid \beta \;\mid\; \beta \in [[R]]_\rho \; and \; \exists\, \gamma \in [[Q]]_\rho.\; \alpha \in [[P]]_{\rho[X:=\uparrow\{\gamma\}]}\}$$

Adeguacy of $\mathcal{F}(\mathcal{T})$

Define $P \sqsubseteq_F Q$ if $[[P]] \subseteq [[Q]]$.

Theorem [Adeguacy] $P \sqsubseteq_F Q \Rightarrow P \sqsubseteq Q$.

About the proof: the proof is done by a double induction on types and terms, via a ”realizability” interpretation of types.

Completeness fails

Take

$$P_1 = a[b[out\, c]]$$

$$P_2 = a[b[open\, d]] \mid d[in\, b.out\, c]$$

$P_1 \not\sqsubseteq_F P_2$, but $P_1 \sqsubseteq P_2$

In fact

- both exhibit a at top level and b inside a.
- to show the difference we must allow $open\, c$ to act.
- If we open a we cannot prevent d to jump into b, be opened and unlash $out\, c$.

The "selfopen" action

Add a new primitive "$so\, a$" for all $a \in \mathcal{L}$ with reduction rule

$$a[so\, a.P \mid Q] \quad \rightarrow \quad P \mid Q$$

Note. The "so" action cannot be internally represented in the ambient calculus.

The $so\, a$ action is similar to action *acid* (Cardelli and Gordon) whose reduction is:

$$a[acid.P \mid Q] \rightarrow P \mid Q$$

This makes objective moves internally representable. For example

$$a[b[\,]] \mid c[in\, a.so\, c.out\, a] \rightarrow^* a[\,] \mid \; b[\,]$$

The "selfopening" Ambient Calculus

The "selfopening" Ambinet Calculus is obtained by

- Adding the $so\,a$ action and the corresponding reduction rule as in the previous slide.
- adding to the definition of types the clause $so\,a.\alpha \in \mathcal{T}_{so}$ for all $a \in \mathcal{L}$
- Adding to the rules for $\leq$ the rule

$$(selfopen) \quad a[so\,a.\,\alpha \mid \beta] \leq \alpha \mid \beta$$

- modifying the type inference rules and the definition of the model in the obvious way. Let $\mathcal{F}(\mathcal{T}_{so})$ be the resulting filter model and $\sqsubseteq_{\mathcal{F}_{so}}$ the induced partial order on terms.

Full Abstraction

Theorem [Full Abstraction] In the ”selfopening” Ambient Calculus $P \sqsubseteq Q$ if and only if $P \sqsubseteq_{\mathcal{F}_{so}} Q$.

Corollary $\mathcal{F}(\mathcal{T}_{so})$ is adequate (i.e. $P \sqsubseteq_{\mathcal{F}_{so}} Q \Rightarrow P \sqsubseteq Q$) also with respect to the standard Ambient Calculus (*without* so).
But in this case obviously it is *not* complete

About the proof: the proof of completeness relies on the definition of *test processes*.

Future work

- Find weaker primitives to get a fully abstract model, or find a stronger notion of type inclusion.

- Specialize the type system for more practical analyses.

- Develop a type systems to control the so operation.