# Extensionality of Spatial Observations in Distributed Systems

Luís Caires and Hugo Torres Vieira
CITI / DI / FCT / UNL
Portugal

CIC'06 – 11/10/06 – Braga, Portugal

# Motivation

- Modeling concurrency
  - Communication is the central focus.
- Modeling distribution
  - Is communicating in space transparent?
    - In practice distributed systems indirectly give away their structure since interactions may depend on it:
      - resources may be available at some locations only;
      - access policies may constrain communications;
      - communications may take longer;
      - failures may take place…

# Spatial logics

- Introduced to specify distributed behavior.

  @ UNL:
  - [Caires PhD Thesis 1999]
  - [Caires, Cardelli 2003,2004]
  - [Caires, Lozes 2003]
  - [Monteiro 2004]
  - [Tuosto, Vieira 2006]
  - [Caires, Vieira 2006] ← This work (CONCUR/EXPRESS'06)

- Have been used with several models:
  - Mobile Ambients [Cardelli, Gordon 2000]
  - Pi-calculus [Caires, Cardelli 2003]
  - Bigraphs [Conforti, Macedonio, Sassone 2005]
  - Types for service oriented computing [Caires 2006 (to appear)]

# Expressiveness for distribution

- Spatial logics express properties that talk about the structure of systems, *e.g.*:
  - Has exactly one site;
  - Holds a unique resource at a site;
  - All sites are listening on a given channel;
  - Part of the system is liable to fail;
  - …

# Intensionality vs. extensionality

- Graded intensional since:
  - *they "can separate terms on the basis of their internal structure, even though their behaviors are the same"* [Sangiorgi 2001].
  - their discriminating power often coincides with structural congruence.
- What if structure can be observed?
  - Spatial observations that precisely capture the structural features that are observable by means of interactions must be seen as extensional.

# Main goal

- Extensionality claim:
  - We show that spatial observations, as the ones used by spatial logics, can be seen as extensional in natural models of distribution.

# Modeling distribution

- Essential distributed systems features:
  - Computation scattered in space;
  - Local synchronous communication;
  - Remote asynchronous communication;
  - Partial failures;
  - …
- Our toy model, in spite of it's simplicity, takes into consideration all these features.

# Failures

- Failures are a good example of distributed system features that give away structural information.
- Fail-stop fashion:
  - Simplicity: *e.g.* handle delays as failures.
- Any (non empty) network can fail:
  - Generality: *e.g.* covers network partition.

# Outline

- A simple distributed calculus
- Abstract semantics (strong case)
  - Reference observational equivalence
  - Alternative characterizations
- Weak case
  - Minimality results

# A simple distributed calculus

(*Actions*)

$\alpha ::= a$

$\bar{a}$

$\tau$

(*Processes*)

$P,Q ::= P \mid Q$

**nil**

$\alpha.P$

**go**$.P$

(*Networks*)

$N,M ::= N \mid M$

$0$

$[P]$

# Operational semantics

*Structural congruence* $\equiv$

($\mathcal{P}$, **nil**, $|$) and ($\mathcal{N}$, **0**, $|$) are comm. monoids and $P \equiv Q \Rightarrow [P] \equiv [Q]$

*Reduction* $\rightarrow$ (...)

$[\bar{a}.P \mid a.Q \mid R] \rightarrow [P \mid Q \mid R]$ (Red Comm)

$[\tau.P \mid Q] \rightarrow [P \mid Q]$ (Red Tau)

$[\mathbf{go}.P \mid Q] \mid [R] \rightarrow [Q] \mid [P \mid R]$ (Red Go)

$[P] \mid N \rightarrow \mathbf{0}$ (Red Fail)

# Reduction illustrated

$N \triangleq$ [**go**.**go**.$\bar{a}$.**nil** | **go**.$\bar{a}$.**nil**] | [**nil**] | [$\tau$.$a$.**nil**]

[**go**.**go**.$\bar{a}$.**nil** | **go**.$\bar{a}$.**nil**] | [**nil**] | [$\tau$.$a$.**nil**]
$\longrightarrow$ [**go**.$\bar{a}$.**nil**] | [**go**.$\bar{a}$.**nil** | **nil**] | [$\tau$.$a$.**nil**]
$\longrightarrow$ [**go**.$\bar{a}$.**nil**] | 0 | [$\tau$.$a$.**nil**]
$\longrightarrow$ [**nil**] | [$\bar{a}$.**nil** | $\tau$.$a$.**nil**]
$\longrightarrow$ [**nil**] | [$\bar{a}$.**nil** | $a$.**nil**]
$\longrightarrow$ [**nil**] | [**nil**]

# Abstract semantics

- Characterize systems from an external observer viewpoint:
  - Observe barbs that hint on what is going on;
  - Consider systems evolutions;
  - Place systems in a context.
- Standard reduction barbed congruence is our reference observational equivalence.

# Observational equivalence

*Barbs* $N\downarrow_a \triangleq \exists P,Q,M.\ N \equiv [a.P \mid Q] \mid M$

*Contexts* $C[\bullet] ::= N \mid \bullet$

*Strong reduction barbed congruence* $\simeq$

Largest symmetric relation $\mathcal{R}$ such that for all $(N,M) \in \mathcal{R}$:

$\forall a.\ N\downarrow_a \Rightarrow M\downarrow_a$

$N \rightarrow N' \Rightarrow \exists M'.\ M \rightarrow M' \wedge (N',M') \in \mathcal{R}$

$\forall C[\bullet].\ (C[N], C[M]) \in \mathcal{R}$

# Structure & equivalence

$N \triangleq [\mathbf{nil}] \mid [\mathbf{nil}]$ $M \triangleq [\mathbf{nil}]$

Are $N$ and $M$ equivalent? **NO!**

$C[\bullet] \triangleq [\mathbf{go}.(a_1.\mathbf{nil} \mid \bar{a}_2.f.\mathbf{nil})$

$\mid \mathbf{go}.(a_2.\mathbf{nil} \mid \bar{a}_1.f.\mathbf{nil})] \mid \bullet$

$C[N] \rightarrow^2 [a_1.\mathbf{nil} \mid \bar{a}_2.f.\mathbf{nil}] \mid [a_2.\mathbf{nil} \mid \bar{a}_1.f.\mathbf{nil}] \ldots \downarrow_f$

$C[M] \rightarrow^2 [a_1.\mathbf{nil} \mid \bar{a}_2.f.\mathbf{nil} \mid a_2.\mathbf{nil} \mid \bar{a}_1.f.\mathbf{nil}]$

$\rightarrow^2 [f.\mathbf{nil} \mid f.\mathbf{nil}] \downarrow_f$

$[P_1] \mid \ldots \mid [P_k] \simeq M \Rightarrow M \equiv [Q_1] \mid \ldots \mid [Q_k]$ (...)

# Counting

- The observer's ability to count sites is due solely to the combination in the model of mobility and local synchronization, not relying on failures.
- Counting has an extensional character.
  - While usually the spatial logics ability to count and express arithmetic constraints is related to the intensional character…

# Alternative coinductive characterization of equivalence

- Quantifying over all contexts is hard to manage:
  - Bisimulations abstract context interaction using labeled transition systems that infer the possible behaviors from the structure.
  - In our case we must abstract process migrations from the context and process migrations to the context.
- We aim to precisely characterize reduction barbed congruence (full abstraction).
  - This implies that our bisimulation must also take into account the internal structure of the systems…

# Commitment

$Commitment \xrightarrow{\lambda} (\ldots)$

$[\bar{a}.P \mid a.Q \mid R] \xrightarrow{\tau} [P \mid Q \mid R]$ (Comm)

$[\tau.P \mid Q] \xrightarrow{\tau} [P \mid Q]$ (Tau)

$[\mathbf{go}.P \mid Q] \mid [R] \xrightarrow{\tau} [Q] \mid [P \mid R]$ (Go)

$[P] \mid N \xrightarrow{\tau} \mathbf{0}$ (Fail)

$[\bar{a}.P \mid Q] \xrightarrow{\bar{a}} [P \mid Q]$ (Out)

$[a.P \mid Q] \xrightarrow{a} [P \mid Q]$ (In)

$N \xrightarrow{[a]} N \mid [a.\mathbf{nil}]$ (Grow)

# Context interaction (going in)

$$[\bar{a}.P \mid Q] \xrightarrow{\bar{a}} [P \mid Q] \qquad \text{(Out)}$$

$$[a.P \mid Q] \xrightarrow{a} [P \mid Q] \qquad \text{(In)}$$

Process migration from the context:

(Out) and (In) transitions abstract the migration of foreign processes into the system that then communicate on a determined channel.

# Context interaction (going out)

$N \xrightarrow{[a]} N \mid [a.\mathbf{nil}]$ (Grow)

Process migration to the context:

(Grow) transitions allow for the internalization of the migration of processes to the outer context, by importing a minimal representation of a foreign migration target.

# Grow and separate

$N_1 \triangleq [\mathbf{go}.\bar{a}.\mathbf{nil}]$ $N_2 \triangleq [\mathbf{nil}]$

$N_1$ and $N_2$ act the same in isolation but:

$[\mathbf{go}.\bar{a}.\mathbf{nil}] \xrightarrow{[b]} [\mathbf{go}.\bar{a}.\mathbf{nil}] \mid [b.\mathbf{nil}] \xrightarrow{\tau} (\ldots)$

Is commitment enough?

$M_1 \triangleq [\tau.\mathbf{nil}]$ $M_2 \triangleq [\mathbf{nil}] \mid [\mathbf{nil}]$

Networks $M_1$ and $M_2$ have the same commitment graph…

# Strong bisimulation (candidate)

*Strong bisimulation*

Symmetric relation $\mathcal{B}$ such that whenever $(N,M) \in \mathcal{B}$:

$$N \xrightarrow{\lambda} N' \quad \Rightarrow \exists M'.\ M \xrightarrow{\lambda} M' \wedge (N',M') \in \mathcal{B}$$

# Strong bisimulation

*Strong bisimulation*

Symmetric relation $\mathcal{B}$ such that whenever $(N,M) \in \mathcal{B}$:

$$N \xrightarrow{\lambda} N' \quad \Rightarrow \exists M'.\ M \xrightarrow{\lambda} M' \wedge (N',M') \in \mathcal{B}$$

$$N \equiv N' \mid N'' \Rightarrow \exists M', M''.\ M \equiv M' \mid M''$$
$$\wedge\ (N',M') \in \mathcal{B} \wedge (N'',M'') \in \mathcal{B}$$

$$N \equiv \mathbf{0} \quad \Rightarrow M \equiv \mathbf{0}$$

*Strong bisimilarity* $\sim$ Largest strong bisimulation.

# Grow and separate revisited

$N_1 \triangleq [\mathbf{go}.\bar{a}.\mathbf{nil}]$ $N_2 \triangleq [\mathbf{nil}]$ $N_1 \not\sim N_2$

$[\mathbf{go}.\bar{a}.\mathbf{nil}] \xrightarrow{[b]} [\mathbf{go}.\bar{a}.\mathbf{nil}] \mid [b.\mathbf{nil}]$ $(\ldots) \xrightarrow{\bar{a}}$

$[\mathbf{nil}] \xrightarrow{[b]} [\mathbf{nil}] \mid [b.\mathbf{nil}]$ $(\ldots) \not\xrightarrow{\bar{a}}$

$M_1 \triangleq [\tau.\mathbf{nil}]$ $M_2 \triangleq [\mathbf{nil}] \mid [\mathbf{nil}]$ $M_1 \not\sim M_2$

$M_2 \equiv [\mathbf{nil}] \mid [\mathbf{nil}]$

$\nexists M', M''.\ M_1 \equiv M' \mid M''$

$\wedge\ M' \sim [\mathbf{nil}] \wedge M'' \sim [\mathbf{nil}]$

# Full abstraction

We have $\sim = \simeq$.

– Key compositionality principle to prove $\sim \subseteq \simeq$:
Let $P^i$ and $Q^i$ ($i$ in $I$) be collections of processes such that $[P^i] \sim [Q^i]$ for $i$ in $I$. Then for $k,m,n, \ldots$ in $I$ we have:
$[P^k | P^m | \ldots] | [P^n | \ldots] | \ldots \sim [Q^k | Q^m | \ldots] | [Q^n | \ldots] | \ldots$ .

– Key property to prove $\simeq \subseteq \sim$:
Let $P_1,\ldots,P_k$ be a collection of processes and $M$ a network. If $[P_1] | \ldots | [P_k] \simeq M$ then there exist $Q_1,\ldots,Q_k$ such that $M \equiv [Q_1] | \ldots | [Q_k]$ and for all $i$ in $\{1,\ldots,k\}$ it is the case that $[P_i] \simeq [Q_i]$.

# Compositionality principle

- Proof by coinduction:
  - Take the relation of pairs of networks that are built out of bisimilar bits and show that this relation is closed by bisimulation operators.
- The tricky part is handling mobility:
  - Use the grow transition to isolate migrating processes to ensure mobile bits are bisimilar.

# Logical characterization of equivalence

- We aim at characterizing the equivalence with a spatial logic: extensionality claim.

- We take HML and add spatial connectives.

  Logical equivalence identifies systems that are indistinguishable with respect to a logic, i.e., systems that satisfy exactly the same formulas.

  – $N =_{\mathcal{L}_S} M \triangleq \forall A.\ N \vDash A \Leftrightarrow M \vDash A$

# Spatial logic $\mathcal{L}s$

$A,B ::=$ (*Formulas*)

| | |
|---|---|
| $\mathbf{T}$ | $N \models \mathbf{T}$ always |
| $\neg A$ | $N \models \neg A$ if $N \not\models A$ |
| $A \wedge B$ | $N \models A \wedge B$ if $N \models A$ and $N \models B$ |
| $\mathbf{0}$ | $N \models \mathbf{0}$ if $N \equiv \mathbf{0}$ |
| $A \mid B$ | $N \models A \mid B$ if $\exists N', N''.\ N \equiv N' \mid N''$ and $N' \models A$ and $N'' \models B$ |
| $\langle \lambda \rangle A$ | $N \models \langle \lambda \rangle A$ if $\exists N'.\ N \xrightarrow{\lambda} N'$ and $N' \models A$ |

# Logical characterization

We have $\sim = =_{\mathcal{L}s}$.

- We prove $\sim \subseteq =_{\mathcal{L}s}$ by a standard induction on the structure of the formulas.
  Exploiting the fact that our bisimulation is already equipped with spatial clauses…
- We prove $=_{\mathcal{L}s} \subseteq \sim$ by coinduction on the definition of bisimulation.
  Using the finiteness of transition image sets and separation sets, up to structural congruence, we can build formulas that address properties of all possible transitions and decompositions…

As an immediate corollary we have $\simeq = =_{\mathcal{L}s}$.

# Weak equivalences

- Weak equivalences abstract systems internal actions and focus mainly on the possible interactions with the context.

- Are strong equivalences, in some sense, intensional?

  In our model the ability to count internal actions even informs on the structure of the system: only empty systems have no internal actions due to failures.

# Weak observational equivalence

*Weak reduction* $\Rightarrow$ ref. tr. closure of $\rightarrow$

*Weak barbs* $N \Downarrow_a \triangleq \exists N'.\ N \Rightarrow N'$ and $N' \downarrow_a$

*Weak reduction barbed congruence* $\approx$

Largest symmetric relation $\mathcal{R}$ such that for all $(N,M) \in \mathcal{R}$:

$\forall a.\ N \downarrow_a \Rightarrow M \Downarrow_a$

$N \rightarrow N' \Rightarrow \exists M'.\ M \Rightarrow M' \wedge (N',M') \in \mathcal{R}$

$\forall C[\bullet].\ (C[N], C[M]) \in \mathcal{R}$

# Weak bisimulation

*Weak commitment* $N \stackrel{\lambda}{\Rightarrow} N'$

$N \stackrel{\tau}{\longrightarrow}{}^* M' \stackrel{\lambda}{\longrightarrow} M'' \stackrel{\tau}{\longrightarrow}{}^* N'$ $(\lambda \neq \tau)$ or $N \stackrel{\tau}{\longrightarrow}{}^* N'$

*Weak bisimulation*

Symmetric relation $\mathcal{B}$ such that whenever $(N,M) \in \mathcal{B}$:

$N \stackrel{\lambda}{\longrightarrow} N' \quad \Rightarrow \exists M'.\ M \stackrel{\lambda}{\Rightarrow} M' \wedge (N',M') \in \mathcal{B}$

$N \equiv N' \mid N'' \Rightarrow \exists M', M''.\ M \Rightarrow M' \mid M''$

$\wedge\ (N',M') \in \mathcal{B} \wedge (N'',M'') \in \mathcal{B}$

$N \equiv \mathbf{0} \quad \Rightarrow M \equiv \mathbf{0}$

*Weak bisimilarity* $\approx$ Largest weak bisimulation.

# Spatial logic $\mathcal{L}$w

$A,B ::=$ (*Formulas*)

| | |
|---|---|
| $\mathbf{T}$ | $N \models \mathbf{T}$ always |
| $\neg A$ | $N \models \neg A$ if $N \not\models A$ |
| $A \wedge B$ | $N \models A \wedge B$ if $N \models A$ and $N \models B$ |
| $\mathbf{0}$ | $N \models \mathbf{0}$ if $N \equiv \mathbf{0}$ |
| $A \upharpoonright B$ | $N \models A \upharpoonright B$ if $\exists N', N''.\ N \Rightarrow N' \mid N''$ and $N' \models A$ and $N'' \models B$ |
| $\langle\langle\lambda\rangle\rangle A$ | $N \models \langle\langle\lambda\rangle\rangle A$ if $\exists N'.\ N \stackrel{\lambda}{\Rightarrow} N'$ and $N' \models A$ |

# Summary of results

$$
\begin{array}{ccccc}
 & & \equiv & & \\
 & & \subsetneq & & \\
\cong & = & \sim & = & =_{\mathcal{L}\mathrm{s}} \\
 & & \subsetneq & & \\
\cong\!\!\cong & = & \approx & = & =_{\mathcal{L}\mathrm{w}}
\end{array}
$$

# Minimality

- We have shown a spatial logic that supports the precise characterization of a standard observational equivalence.

- But is it, in some sense, minimal?

  Are all connectives essential for it's expressiveness and for characterizing the equivalence?

# Minimality results

The $(\mathbf{T},\langle\langle\tau\rangle\rangle\,\mathrm{A})$-free fragment of $\mathcal{L}\mathrm{w}$ is minimal:

$\neg$-free fragment equates **[nil]** | **[nil]** and **[nil]**

$\wedge$-free fragment does not express property $1^{(*)}$

$\mathbf{0}$-free fragment equates **[nil]** and $0$

$\restriction\!\uparrow$-free fragment equates **[nil]** | **[nil]** and **[nil]**

$\langle\langle\alpha\rangle\rangle$-free fragment equates $[\alpha.$**nil**$]$ and **[nil]**

$\langle\langle[b]\rangle\rangle$-free fragment equates **[go.**$\bar{a}.$**nil]** and **[nil]**

$^{(*)}\ 1 \triangleq \{\, N \mid \exists P.\ N \equiv [P] \}$

# Concluding remarks

- We developed a model considering a standard observational equivalence and constructed alternative characterizations based on spatial observations:
  - thus spatial observations can have an extensional role as they are essential to characterize standard observational equivalences in distributed settings.
- We are studying these issues considering richer models, starting with name restriction.
- What are, in general, the relevant spatial observables of distributed systems?