MPRI Concurrency (course number 2-3) 2004-2005: π-calculus

2 December 2004

http://pauillac.inria.fr/~leifer/teaching/mpri-concurrency-2004/

James J. Leifer
INRIA Rocquencourt

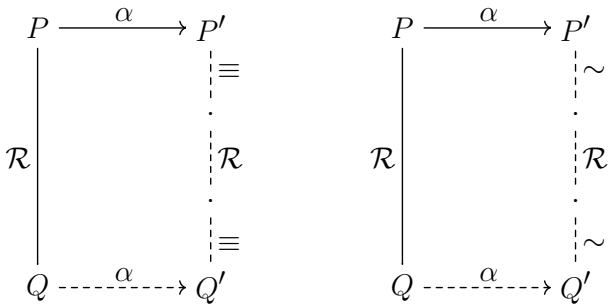
James.Leifer@inria.fr

Today's plan

- exercises from last week
- strong bisimulation "up to"
- strong bisimilarity is not a congruence
- full strong bisimilarity
- the design of operational equivalences
- strong barbed bisimulation
- comparison between strong bisimilarity and strong barbed bisimilarity

Strong bisimulation up to $\equiv$ and $\sim$

Suppose for all $(P, Q) \in \mathcal{R}$ and $P \xrightarrow{\alpha} P'$, where $\mathsf{bn}(\alpha) \cap \mathsf{fn}(Q) = \varnothing$, there exists Q' such that $Q \xrightarrow{\alpha} Q'$ and $(P', Q') \in \equiv\mathcal{R}\equiv$, and symmetrically.



Then $\equiv\mathcal{R}\equiv$ is a strong bisimulation. Likewise for $\sim$ in place of $\equiv$. Is $\mathcal{R}$ also a strong bisimulation?

Evaluation contexts

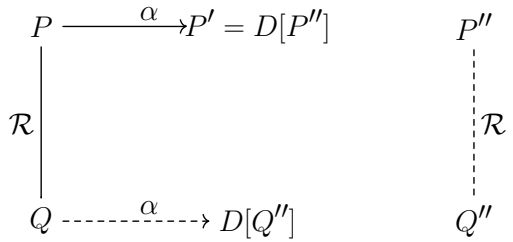
Let $\mathcal{E}$ be the set of evaluation contexts; these are generated by the grammar:

$$\begin{aligned} D \in \mathcal{E} ::= {} & - \\ & D \mid P \\ & P \mid D \\ & \boldsymbol{\nu} x.D \end{aligned}$$

What isn't an evaluation context?

Strong bisimulation up to contexts

Suppose for all $(P, Q) \in \mathcal{R}$ and $P \xrightarrow{\alpha} P'$, where $\mathsf{bn}(\alpha) \cap \mathsf{fn}(Q) = \varnothing$, there exists $D \in \mathcal{E}$, P'', and Q'' such that $P' = D[P'']$ and $Q \xrightarrow{\alpha} D[Q'']$ and $(P'', Q'') \in \mathcal{R}$, and symmetrically.



Then $\{(D[P], D[Q]) \;/\; (P, Q) \in \mathcal{R}, D \in \mathcal{E}\}$ is a strong bisimulation.

Example: $!!P \sim !P$.

Easier reduction rules for replication

To prove this example, we use easier reduction rules for replication:

$$\frac{P \xrightarrow{\alpha} P'}{!P \xrightarrow{\alpha} P' \mid !P} \text{if } \mathsf{bn}(\alpha) \cap \mathsf{fn}(P) = \varnothing \quad \text{(lab-bang-simple)}$$

$$\frac{P \xrightarrow{\overline{x}y} P' \qquad P \xrightarrow{xy} P''}{!P \xrightarrow{\tau} (P' \mid P'') \mid !P} \quad \text{(lab-bang-comm)}$$

$$\frac{P \xrightarrow{\overline{x}(y)} P' \qquad P \xrightarrow{xy} P''}{!P \xrightarrow{\tau} \boldsymbol{\nu} y.(P' \mid P'') \mid !P} \text{if } y \notin \mathsf{fn}(P) \quad \text{(lab-bang-close)}$$

Congruence?

A relation $\mathcal{R}$ is a congruence if for all $(P, Q) \in \mathcal{R}$ and all contexts C, we have $(C[P], C[Q]) \in \mathcal{R}$.

Theorem: Strong bisimilarity, $\sim$, is a congruence with respect to all non input-prefixing contexts, i.e. $P \sim Q$ implies $C[P] \sim C[Q]$ where

$$\begin{aligned} C ::= {} & - \\ & C \mid S \\ & S \mid C \\ & \boldsymbol{\nu} x.C \\ & !C \\ & \overline{x}y.C \end{aligned}$$

But is it a congruence?

Congruences and substitution preservation

A relation $\mathcal{R}$ is preserved by substitution if for all $(P, Q) \in \mathcal{R}$ and any substitution σ, we have $(\sigma P, \sigma Q) \in \mathcal{R}$.

Claim: If $\mathcal{R}$ is a strong bisimulation and a congruence then it is preserved by substitution.

To see why, consider the input-prefixing context $C = z(y).- \mid \overline{z}x$. Suppose $(P, Q) \in \mathcal{R}$. Since $\mathcal{R}$ is a congruence, $(C[P], C[Q]) \in \mathcal{R}$.

Since $C[P] \xrightarrow{\tau} \{x/y\}P$ and $\mathcal{R}$ is a bisimulation, $C[Q]$ must be able to match this τ transition with the only one it is capable of, namely $C[Q] \xrightarrow{\tau} \{x/y\}Q$, and $(\{x/y\}P, \{x/y\}Q) \in \mathcal{R}$, as desired.

Strong bisimilarity is not a congruence

By the contrapositive, if $\sim$ is not preserved by substitution, then it is not a congruence.

- Counter example with sum: $\overline{x} \mid y \sim \overline{x}.y + y.\overline{x}$
- Counter example with sum: $\boldsymbol{\nu} w.(\overline{x}.\overline{w} \mid y.w.\overline{a}) \sim \overline{x}.y.\tau.\overline{a} + y.\overline{x}.\tau.\overline{a}$
- Counter example without sum:

$$\begin{array}{ll} & !(\boldsymbol{\nu} w.(\overline{x}.\overline{w} \mid y.w.\overline{a})) \\ \sim & !(\overline{x}.y.\tau.\overline{a} + y.\overline{x}.\tau.\overline{a}) \qquad \text{by the previous exercise and (1)} \\ \sim & !(\overline{x}.y.\tau.\overline{a}) \mid !(y.\overline{x}.\tau.\overline{a}) \qquad \text{by (2)} \end{array}$$

where we know that $\sim$ is a congruence with respect to replication

$$P \sim Q \text{ implies } !P \sim !Q \tag{1}$$

and that replication "distributes" through sum:

$$!(\overline{x}u.P + y(v).Q) \sim !\overline{x}u.P \mid !y(v).Q \tag{2}$$

Strong bisimilarity and full strong bisimilarity

As we've just seen, $\sim$ isn't a congruence with respect to input prefixing.

Definition (full strong bisimilarity): The relation $\sim^{\mathsf{c}}$ is defined as follows. For all P and Q, we have that $P \sim^{\mathsf{c}} Q$ iff for all substitutions σ, $\sigma P \sim \sigma Q$.

Theorem: $\sim^{\mathsf{c}}$ is a congruence.

Proof sketch: The most interesting case is that of input prefixing. Suppose $P \sim^{\mathsf{c}} Q$. We want to show that $x(y).P \sim^{\mathsf{c}} x(y).Q$, i.e. for all σ we have $\sigma(x(y).P) \sim \sigma(x(y).Q)$. Assuming y is fresh, we can push the substitution in: $(\sigma x)(y).(\sigma P) \sim (\sigma x)(y).(\sigma Q)$. The LHS's only labelled transition $(\sigma x)(y).(\sigma P) \xrightarrow{(\sigma x)z} \{z/y\}\sigma P$ is matched by a similar one on the RHS to $\{z/y\}\sigma Q$. Finally, the hypothesis $P \sim^{\mathsf{c}} Q$ implies $\{z/y\}\sigma P \sim \{z/y\}\sigma Q$, as desired.

Operational equivalences and process calculi: from automata to compositional languages

1956: E. F. Moore. "Gedanken-experiments on sequential machines".
"finite automata from the experimental point of view" — trace refinement and trace equivalence of automata

1980: R. Milner. *A Calculus of Communicating Systems*.
a compositional syntax, namely CCS; operational equivalences based on bisimulation; congruence results for compositional reasoning.

1981: D. Park. "Concurrency and automata on infinite sequences".
bisimulation: an operational equivalence that is sensitive to nondeterminism.

1989: R. Milner, J. Parrow, and D. Walker. "A calculus of mobile processes, parts I and II".
π-calculus without structural congruence or reductions

Operational equivalences and process calculi: from labelled transitions to reductions

1990: G. Berry and G. Boudol. "The chemical abstract machine"
structural congruence and reduction rules

1990: R. Milner. "Functions as processes".
(written while visiting INRIA Sophia) structural congruence and reduction rules to π-calculus

1992: R. Milner and D. Sangiorgi. "Barbed bisimulation".
equivalence based on reduction and observations of "barbs", not labelled transitions.

... followed by a wealth of new reduction-based process calculi, e.g.

1998: L. Cardelli and A. D. Gordon. "Mobile ambients".

$$n[\mathsf{in}\, m.P \mid Q] \mid m[R] \longrightarrow m[n[P \mid Q] \mid R]$$

...

2003: M. Merro and F. Zappa Nardelli. "Bisimulation proof methods for Mobile Ambients".
first LTS for ambients that recovers barbed bisimilarity

Operational equivalences based on reduction

- For all $(P, Q) \in \mathcal{R}$ and $P \longrightarrow P'$, there exists Q' such that $Q \longrightarrow Q'$ and $(P', Q') \in \mathcal{R}$, and vice versa.

  Problem: this definition equates $\overline{x}y$ and $\mathbf{0}$.

- For all $(P, Q) \in \mathcal{R}$ and $P \longrightarrow P'$, there exists Q' such that $Q \longrightarrow Q'$ and $(P', Q') \in \mathcal{R}$, and vice versa; moreover, for all x, we have $P \downarrow x$ iff $Q \downarrow x$.

  We say that P has a strong barb x, written $P \downarrow x$ iff there exists P_0, P_1, and $\vec{y}$ such that $P \equiv \boldsymbol{\nu}\vec{y}.(\overline{x}u.P_0 \mid P_1)$ and $x \notin \vec{y}$.

  Strong barbed bisimilarity is the largest such $\mathcal{R}$ and is written $\dot{\sim}$.

  Problem: $\dot{\sim}$ equates $\overline{x}y$ and $\overline{x}z$, thus it is not a congruence since it distinguishes between $C[\overline{x}y]$ and $C[\overline{x}z]$ where $C = - \mid x(u).\overline{u}w$.

- Strong barbed congruence $\dot{\sim}^{\mathsf{c}}$ is the context closure of $\dot{\sim}$, i.e. $P \dot{\sim}^{\mathsf{c}} Q$ iff for all contexts C we have $C[P] \dot{\sim} C[Q]$

Barbs can be simple!

Why no input barbs? How do we check that a process P is capable of inputting on x, i.e. that there exists P_0, P_1, and $\vec{y}$ such that $P \equiv \boldsymbol{\nu}\vec{y}.(x(u).P_0 \mid P_1)$ and $x \notin \vec{y}$?
Easy! Just use the context $- \mid \overline{x}v.\overline{k}w$ for k fresh and check for a barb on k.

Are a variety of output barbs even necessary? No. All we need is just one (or sometimes two) distinguished observables. Let us add a new construct $\mathbf{beep}$:

$$P ::= \ldots \mid \mathbf{beep}$$

We can observe that a process beeps, written $P \downarrow \mathbf{beep}$, if there exists $D \in \mathcal{E}$, an evaluation context, such that $P \equiv D[\mathbf{beep}]$.
Then P has an output barb x, i.e. $P \downarrow x$, iff $C[P] \longrightarrow\downarrow \mathbf{beep}$ where $C = - \mid x(u).\mathbf{beep}$.

Advantages and disadvantages of barbed congruence

Advantages: even for complex process calculi, it's easy to work with barbs: they're just "beeps" or "print statements". Compare this to the difficulty of modifying the π-calculus's labelled transitions to cope with polyadic communication, code mobility, etc.

Disadvantages: the quantification over all contexts is heavy.

Exercises for next lecture

1. You might have noticed that the "up to" technique we used in the proof of $!!P \sim !P$ was different from those justified by the theorems. In particular, we combined "up to contexts" and "up to structural congruence" without justification. The goal of this exercise is to show some general criteria for composing "up to" techniques.

   Let us say that a relation $\mathcal{R}$ strongly progresses to a relation $\mathcal{T}$, written $\mathcal{R} \rightsquigarrow \mathcal{T}$, if for all $(P, Q) \in \mathcal{R}$ and $P \xrightarrow{\alpha} P'$, where $\mathsf{bn}(\alpha) \cap \mathsf{fn}(Q) = \varnothing$, there exists Q' such that $Q \xrightarrow{\alpha} Q'$ and $(P', Q') \in \mathcal{T}$, and symmetrically.

   $$\begin{array}{ccc} P & \xrightarrow{\alpha} & P' \\ \mathcal{R} \big| & & \big| \mathcal{T} \\ Q & \dashrightarrow^{\alpha} & Q' \end{array}$$

   Next, say that a function $\mathcal{F}$ on relations is strongly safe if $\mathcal{R} \subseteq \mathcal{T}$ and $\mathcal{R} \rightsquigarrow \mathcal{T}$ implies $\mathcal{F}(\mathcal{R}) \subseteq \mathcal{F}(\mathcal{T})$ and $\mathcal{F}(\mathcal{R}) \rightsquigarrow \mathcal{F}(\mathcal{T})$.

(a) Prove that if $\mathcal{R} \subseteq \mathcal{R}' \rightsquigarrow \mathcal{T}' \subseteq \mathcal{T}$ then $\mathcal{R} \rightsquigarrow \mathcal{T}$.

(b) Consider two families of relations $\{\mathcal{R}_i \ / \ i \in I\}$ and $\{\mathcal{T}_j \ / \ j \in J\}$. Suppose that for all $i \in I$ there exists $j \in J$ such that $\mathcal{R}_i \rightsquigarrow \mathcal{T}_j$. Prove that $\bigcup_{i \in I} \mathcal{R}_i \rightsquigarrow \bigcup_{j \in J} \mathcal{T}_j$.

(c) Principle of "up to": Prove that if $\mathcal{F}$ is strongly safe and $\mathcal{R} \rightsquigarrow \mathcal{F}(\mathcal{R})$ then $\mathcal{R}$ and $\mathcal{F}(\mathcal{R})$ are included in $\sim$.
Hint: Let $\mathcal{R}_i = \mathcal{R}$ and $\mathcal{R}_{i+1} = \mathcal{R}_i \cup \mathcal{F}(\mathcal{R}_i)$. Let $\mathcal{R}_* = \bigcup_{i \in \mathbb{N}} \mathcal{R}_i$. Show that $\mathcal{R}_*$ is a bisimulation.

(d) Example: structural congruence: Let $\mathcal{F}_{\equiv}(\mathcal{R}) = \equiv\mathcal{R}\equiv$. Show that $\mathcal{F}_{\equiv}$ is strongly safe.

(e) Example: Evaluation contexts: Let $\mathcal{F}_{\mathcal{E}}(\mathcal{R}) = \{(D[P], D[Q]) \ / \ (P, Q) \in \mathcal{R} \text{ and } D \in \mathcal{E}\}$. Show that $\mathcal{F}_{\mathcal{E}}$ is strongly safe.

(f) Composition: Suppose that $\mathcal{F}$ and $\mathcal{F}'$ are strongly safe. Show that their composition, $\mathcal{F} \circ \mathcal{F}'$ is too, where $(\mathcal{F} \circ \mathcal{F}')(\mathcal{R}) = \mathcal{F}(\mathcal{F}'(\mathcal{R}))$.

(g) The initial motivation for all this work(!): Deduce that $\mathcal{F}_{\equiv} \circ \mathcal{F}_{\mathcal{E}}$ is strongly safe and give the inferred "up to" principle explicitly.

2. Prove $!P \mid !P \sim !P$ using the easier derivation rules for replication and the "up to" techniques. (I gave this exercise last week, but now you have all the necessary knowledge to do it.)

3. When arguing that bisimilarity isn't preserved by substitution, we relied on the following result: $!(\overline{x}u.P + y(v).Q) \sim !\overline{x}u.P \mid !y(v).Q$. Prove it using "up to" techniques.