

Pi-calculus

LTSs, bisimilarity

Francesco Zappa Nardelli

INRIA Rocquencourt, MOSCOVA research team

`francesco.zappa_nardelli@inria.fr`

MPRI Concurrency course with:

Pierre-Louis Curien (PPS), Roberto Amadio (PPS), Catuscia Palamidessi (INRIA Futurs)

A historical perspective

CCS Milner defined the operational semantics of CCS in term of a *labelled transition system* and associated *bisimilarity*;

...several attempts to handle mobility algebraically led to...

pi-calculus Milner, Parrow and Walker introduced the pi-calculus. They defined its semantics along the lines of research on CCS, that is, before defining the reduction semantics, they defined an LTS...

...at the blackboard

Lifting CCS techniques to name-passing is not straightforward

Actually, the original paper on pi-calculus defines *two* LTSs (excerpts):

Early LTS

$$\bar{x}\langle v \rangle . P \xrightarrow{\bar{x}\langle v \rangle} P$$

$$x(y) . P \xrightarrow{x(v)} \{v/y\}P$$

$$\frac{P \xrightarrow{\bar{x}\langle v \rangle} P' \quad Q \xrightarrow{x(v)} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'}$$

$$P \parallel Q \xrightarrow{\tau} P' \parallel Q'$$

Late LTS

$$\bar{x}\langle v \rangle . P \xrightarrow{\bar{x}\langle v \rangle} P$$

$$x(y) . P \xrightarrow{x(y)} P$$

$$\frac{P \xrightarrow{\bar{x}\langle v \rangle} P' \quad Q \xrightarrow{x(y)} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel \{v/y\}Q'}$$

$$P \parallel Q \xrightarrow{\tau} P' \parallel \{v/y\}Q'$$

These LTSs define the **same τ -transitions**, where is the problem?

Problem

Definition: Weak bisimilarity, denoted \approx , is the largest symmetric relation such that whenever $P \approx Q$ and $P \xrightarrow{\ell} P'$ there exists Q' such that $Q \xRightarrow{\hat{\ell}} Q'$ and $P' \approx Q'$.

But the bisimilarity built on top of them observe **all the labels**: do the resulting bisimilarities coincide? No!

Which is the **right** one? Which is the role of the LTS?

Back to CCS – reductions

Syntax:

$$P ::= \mathbf{0} \mid a.P \mid \bar{a}.P \mid P \parallel P \mid (\nu a)P$$

Reduction semantics:

$$a.P \parallel \bar{a}.Q \rightarrow P \parallel Q \quad \frac{P \rightarrow P'}{(\nu a)P \rightarrow (\nu a)P'} \quad \frac{P \equiv P' \rightarrow Q' \equiv Q}{P \rightarrow Q}$$

where \equiv is defined as:

$$P \parallel \mathbf{0} \equiv P \quad P \parallel Q \equiv Q \parallel P \quad (P \parallel Q) \parallel R \equiv P \parallel (Q \parallel R) \\ (\nu a)P \parallel Q \equiv (\nu a)(P \parallel Q) \text{ if } a \notin \text{fn}(Q)$$

Back to CCS – observational equivalence

Let **reduction barbed congruence**, denoted \simeq , be the largest symmetric relation over processes that is

preserved by contexts: if $P \simeq Q$ then $C[P] \simeq C[Q]$ for all contexts $C[-]$.

barb preserving: if $P \simeq Q$ and $P \downarrow_n$, then $Q \downarrow_n$.

Remark:

$P \downarrow n$ holds if $P \equiv (\nu \tilde{a})(n.P' \parallel P'')$ with $n \notin \{\tilde{a}\}$

and $P \Downarrow n$ holds if there exists P' such that $P \rightarrow^* P'$ and $P' \downarrow n$.

reduction closed: if $P \simeq Q$ and $P \rightarrow P'$, then there is a Q' such that $Q \rightarrow^* Q'$ and $P' \simeq Q'$ (\rightarrow^* is the reflexive and transitive closure of \rightarrow).

The role of bisimilarity

Observation: the definition of bisimilarity does not involve a universal quantification over all contexts!

Question: is there any relationship between (weak) bisimilarity and reduction barbed congruence?

Theorem:

1. $P \approx Q$ implies $P \simeq Q$ (soundness of bisimilarity);
2. $P \simeq Q$ implies $P \approx Q$ (completeness of bisimilarity).

Point 2. does not hold in general (it does for the subset of CCS we consider).

Point 1. ought to hold (otherwise your LTS/bisimilarity is very odd!).

Back to CCS: LTS and weak bisimilarity

$$a.P \xrightarrow{a} P$$

$$\bar{a}.P \xrightarrow{\bar{a}} P$$

$$\frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\bar{a}} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'}$$

$$\frac{P \xrightarrow{\ell} P'}{P \parallel Q \xrightarrow{\ell} P' \parallel Q}$$

$$\frac{P \xrightarrow{\ell} P' \quad a \notin \text{fn}(\ell)}{(\nu a)P \xrightarrow{\ell} (\nu a)P'}$$

symmetric rules omitted.

Let $\hat{\ell}$ be $\xrightarrow{\tau}^* \xrightarrow{\ell} \xrightarrow{\tau}^*$ if $\ell \neq \tau$, and $\xrightarrow{\tau}^*$ otherwise.

Definition: Weak bisimilarity, denoted \approx , is the largest symmetric relation such that whenever $P \approx Q$ and $P \xrightarrow{\ell} P'$ there exists Q' such that $Q \xrightarrow{\hat{\ell}} Q'$ and $P' \approx Q'$.

Soundness of weak bisimilarity: $P \approx Q$ implies $P \simeq Q$.

Proof We show that \approx is contextual, barb preserving, and reduction closed.

Contextuality of \approx can be shown by induction on the structure of the contexts, and by case analysis of the possible interactions between the processes and the contexts. (Done by Curien).

Suppose that $P \approx Q$ and $P \downarrow a$. Then $P \equiv (\nu \tilde{n})(a.P_1 \parallel P_2)$, with $a \notin \tilde{n}$. We derive $P \xrightarrow{a} (\nu \tilde{n})(P_1 \parallel P_2)$. Since $P \approx Q$, there exists Q' such that $Q \xrightarrow{a} Q'$, that is $Q \xrightarrow{\tau}^* Q'' \xrightarrow{a} \dots$. But Q'' must be of the form $(\nu \tilde{m})(a.Q_1 \parallel Q_2)$ with $a \notin \tilde{m}$. This implies that $Q'' \downarrow a$, and in turn $Q \Downarrow a$, as required.

Suppose that $P \approx Q$ and $P \rightarrow P'$. We have that $P \xrightarrow{\tau} P'' \equiv P'$. Since $P \approx Q$, there exists Q' such that $Q \xrightarrow{\tau}^* Q'$ and $P' \equiv P'' \approx Q'$. Since $Q \xrightarrow{\tau}^* Q'$ it holds that $Q \rightarrow^* Q'$. Since $P' \equiv P''$ implies $P' \approx P''$, by transitivity of \approx we conclude $P' \approx Q'$, as required. \square

Completeness of weak bisimilarity: $P \simeq Q$ implies $P \approx Q$.

Proof We show that \simeq is a bisimulation.

Suppose that $P \simeq Q$ and $P \xrightarrow{a} P'$ (the case $P \simeq Q$ and $P \xrightarrow{\tau} P'$ is easy). Let

$$\begin{aligned} C_a[-] &= - \parallel \bar{a}.d & Flip &= \bar{d}.(o \oplus f) \\ C_{\bar{a}}[-] &= - \parallel a.d & -_1 \oplus -_2 &= (\nu z)(z. -_1 \parallel z. -_2 \parallel \bar{z}) \end{aligned}$$

where the names z, o, f, d are *fresh* for P and Q .

Lemma 1. $C_a[P] \rightarrow^* P' \parallel d$ if and only if $P \xrightarrow{a} P'$. Similarly for $C_{\bar{a}}[-]$.

Since \simeq is contextual, we have $C_a[P] \parallel Flip \simeq C_a[Q] \parallel Flip$. By Lemma 1. we have $C_a[P] \parallel Flip \rightarrow^* P_1 \equiv P' \parallel o \parallel (\nu z)z.f$.

Lemma 2. If $P \simeq Q$ and $P \rightarrow^* P'$ then there exists Q' such that $Q \rightarrow^* Q'$ and $P' \simeq Q'$.

By Lemma 2. there exists Q_1 such that $C_a[Q] \parallel \text{Flip} \rightarrow^* Q_1$ and $P_1 \simeq Q_1$. Now, $P_1 \downarrow o$ and $P_1 \not\downarrow f$. Since \simeq is barb preserving, we have $Q_1 \downarrow o$ and $Q_1 \not\downarrow f$. The absence of the barb f implies that the \oplus operator reduced, and in turn that the d action has been consumed: this can only occur if Q realised the a action. Thus we can conclude $Q_1 \equiv Q' \parallel o \parallel (\nu z)z.f$, and by Lemma 1. we also have $Q \xrightarrow{a} Q'$.

It remains to show that $P' \simeq Q'$.

Lemma 3. $(\nu z)z.P \simeq 0$.

Since $P_1 \simeq Q_1$ and \simeq is contextual, we have $(\nu o)P_1 \simeq (\nu o)Q_1$. By Lemma 3., we have

$$P' \simeq P' \parallel (\nu o)o \parallel (\nu z)z.f \equiv (\nu o)P_1 \simeq (\nu o)Q_1 \equiv Q' \parallel (\nu o)o \parallel (\nu z)z.f \simeq Q' .$$

The equivalence $P' \simeq Q'$ follows because $\equiv \subseteq \simeq$ and \simeq is transitive. □

Exercise: explain the role of the *Flip* process.

LTSs revisited

Reduction barbed congruence involves a universal quantification over all contexts. Weak bisimilarity does not, yet bisimilarity *is a sound proof technique* for reduction barbed congruence. How is this possible?

An LTS captures all the interactions that a term can have with an arbitrary context. In particular, each label correspond to a minimal context.

For instance, in CCS, $P \xrightarrow{a} P'$ denotes the fact that P can interact with the context $C[-] = - \parallel \bar{a}$, yielding P' .

And τ transitions characterises all the interactions with an *empty context*.

Pi-calculus: labels

Given a process P , which are the contexts¹ that yield a reduction?

- if $P \equiv (\nu \tilde{n})(\bar{x}\langle v \rangle.P_1 \parallel P_2)$ with $x, v \notin \tilde{n}$, then P interacts with the context

$$C[-] = - \parallel x(y).Q$$

yielding:

$$C[P] \rightarrow \underbrace{(\nu \tilde{n})(P_1 \parallel P_2)}_{P'} \parallel Q\{v/y\}$$

We record this interaction with the label $\bar{x}\langle v \rangle$: $P \xrightarrow{\bar{x}\langle v \rangle} P'$.

¹to simplify the notations, we will not write the most general contexts.

-
- if $P \equiv (\nu \tilde{n})(x(y).P_1 \parallel P_2)$ with $x \notin \tilde{n}$, then P interacts with the context

$$C[-] = - \parallel \bar{x}\langle v \rangle.Q \quad \text{for } v \notin \tilde{n}, \text{ yielding:}$$

$$C[P] \rightarrow \underbrace{(\nu \tilde{n})(P_1\{v/y\} \parallel P_2)}_{P'} \parallel Q$$

We record this interaction with the label $x(v)$: $P \xrightarrow{x(v)} P'$

- If $P \rightarrow P'$, then P reduces without interacting with a context $C[-] = - \parallel Q$:

$$C[P] \rightarrow P' \parallel Q$$

We record this interaction with the label τ : $P \xrightarrow{\tau} P'$.

Intermezzo

What if we define a labelled bisimilarity using the previous labels?

Consider the processes:

$$P = (\nu v)\bar{x}\langle v \rangle \quad \text{and} \quad Q = \mathbf{0}$$

Obviously, $P \not\approx Q$ because $P \downarrow x$ while $Q \not\Downarrow x$.

But both P and Q realise no labels: they are equated by the bisimilarity.

The bisimilarity is not *sound*!

Maybe we forgot a label...

The missing interaction

- if $P \equiv (\nu \tilde{n})(\bar{x}\langle v \rangle.P_1 \parallel P_2)$ with $x \notin \tilde{n}$ and $v \in \tilde{n}$, then P interacts with the context

$$C[-] = - \parallel x(y).Q$$

yielding:

$$C[P] \rightarrow (\nu v) \underbrace{((\nu \tilde{n} \setminus v)(P_1 \parallel P_2))}_{P'} \parallel Q\{v/y\}$$

We record this interaction with the label $(\nu v)\bar{x}\langle v \rangle$: $P \xrightarrow{(\nu v)\bar{x}\langle v \rangle} P'$.

Intuition: in P' the scope of v has been **opened**.

Summary of actions

ℓ	kind	$\text{fn}(\ell)$	$\text{bn}(\ell)$	$\text{n}(\ell)$
$\bar{x}\langle y \rangle$	free output	$\{x, y\}$	\emptyset	$\{x, y\}$
$(\nu y)\bar{x}\langle y \rangle$	bound output	$\{x\}$	$\{y\}$	$\{x, y\}$
$x(y)$	input	$\{x, y\}$	\emptyset	$\{x, y\}$
τ	internal	\emptyset	\emptyset	\emptyset

Pi-calculus: LTS

$$\bar{x}\langle v \rangle . P \xrightarrow{\bar{x}\langle v \rangle} P \quad x(y) . P \xrightarrow{x(v)} \{v/y\}P \quad \frac{P \xrightarrow{\bar{x}\langle v \rangle} P' \quad Q \xrightarrow{x(v)} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'}$$

$$\frac{P \xrightarrow{\ell} P' \quad \text{bn}(\ell) \cap \text{fn}(Q) = \emptyset}{P \parallel Q \xrightarrow{\ell} P \parallel Q} \quad \frac{P \xrightarrow{\ell} P' \quad v \notin \text{n}(\ell)}{(\nu v)P \xrightarrow{\ell} (\nu v)P'} \quad \frac{P \parallel !P \xrightarrow{\ell} P'}{!P \xrightarrow{\ell} P'}$$

$$\frac{P \xrightarrow{\bar{x}\langle v \rangle} P' \quad x \neq v}{(\nu v)P \xrightarrow{(\nu v)\bar{x}\langle v \rangle} P'} \quad \frac{P \xrightarrow{(\nu v)\bar{x}\langle v \rangle} P' \quad Q \xrightarrow{x(v)} Q' \quad v \notin \text{fn}(Q)}{P \parallel Q \xrightarrow{\tau} (\nu v)(P' \parallel Q')}$$

Pi-calculus: bisimilarity

We can define bisimilarity for pi-calculus in the standard way.

Let $\xRightarrow{\hat{\ell}}$ be $\xrightarrow{\tau}^* \xrightarrow{\ell} \xrightarrow{\tau}^*$ if $\ell \neq \tau$, and $\xrightarrow{\tau}^*$ otherwise.

Definition: Weak bisimilarity, denoted \approx , is the largest symmetric relation such that whenever $P \approx Q$ and $P \xrightarrow{\ell} P'$ there exists Q' such that $Q \xRightarrow{\hat{\ell}} Q'$ and $P' \approx Q'$.

Last week examples

1. $\bar{x}\langle y \rangle \not\approx \mathbf{0}$: trivial because $\bar{x}\langle y \rangle \xrightarrow{\bar{x}\langle y \rangle}$ and $\mathbf{0} \not\xrightarrow{\bar{x}\langle y \rangle}$.
2. $(\nu x)\bar{x}\langle \rangle.R \approx \mathbf{0}$: the relation $\mathcal{R} = \{((\nu x)\bar{x}\langle \rangle.R, \mathbf{0})\}^=$ is a bisimulation.
3. $(\nu x)(\bar{x}\langle y \rangle.R_1 \parallel x(z).R_2) \approx (\nu x)(R_1 \parallel R_2\{y/z\})$

The relation

$$\mathcal{R} = \{((\nu x)(\bar{x}\langle y \rangle.R_1 \parallel x(z).R_2), (\nu x)(R_1 \parallel R_2\{y/z\}))\}^= \cup \mathcal{I}$$

is a bisimulation.

\mathcal{I} is the identity relation over processes, and $\mathcal{R}^=$ denotes the symmetric closure of \mathcal{R} .

Reduction barbed congruence and pi-calculus

Exercise: Consider the terms (in a pi-calculus with sums):

$$P = \bar{x}\langle v \rangle \parallel y(z)$$

$$Q = \bar{x}\langle v \rangle.y(z) \oplus y(z).\bar{x}\langle v \rangle$$

where $-_1 \oplus -_2 = (\nu w)(\bar{w}\langle \rangle \parallel w(). -_1 \parallel w(). -_2)$.

1. Prove that $P \approx Q$.

2. Does $P \simeq Q$?²³

²Hint: define a context that *equates* the names x and y .

³Hint: use input prefix.

Bisimilarity is not a congruence

In pi-calculus, bisimilarity (both strong and weak) is not preserved by input prefixes, that is contexts of the form $C[-] = x(y).-$.

Question: how to recover the soundness of the bisimilarity with respect to the reduction barbed congruence? Two solutions:

1. close the reduction barbed congruence under *all non input prefix contexts*;
2. close the bisimilarity under substitution: let $P \approx^c Q$ (P is *fully bisimilar* with Q) if $P\sigma \approx Q\sigma$ for all substitutions σ .

Exercise: Show that $P \not\approx^c Q$, where P and Q are defined in the previous slide.

And completeness?

Completeness of bisimulation with respect to barbed congruence⁴ (closed under non-input prefixes, denoted \simeq^-) holds in the strong case. In the weak case, we have that for

$$P = \bar{a}\langle x \rangle \parallel E_{xy} \quad Q = \bar{a}\langle y \rangle \parallel E_{xy}$$

where

$$E_{xy} = !x(z).\bar{y}\langle z \rangle \parallel !y(z).\bar{x}\langle z \rangle$$

it holds that $P \not\approx Q$ but $P \simeq^- Q$ for each context $C[-]$.

Completeness (for image-finite processes) holds if a name-matching operator is added to the language.

⁴barbed congruence is a variant of reduction-closed barbed congruence in which closure under context is allowed only at the beginning of the bisimulation game (formally introduced in the next lecture).

Summary

- Define **intuitive** equivalencies between processes;
- labelled bisimilarities are useful proof methods to show equivalence of processes because...
- ...they capture all the interactions a process may have with a context in a concise way (the LTS).

In the next lecture we will enrich our proof methods with powerful techniques and we will show non-trivial equivalence laws.

Exercises

1. Propose an encoding for lists of integers (done last week). Implement a process $\text{copy } l \ m$ that copies the list found at l in m . Prove that for all lists L

$$(\nu l).(L[l] \parallel \text{copy}[l, m]) \approx L[m] .$$

2. Prove that pi-calculus weak bisimilarity is a congruence with respect to parallel composition, that is prove that whenever $P \approx Q$ then $P \parallel R \approx Q \parallel R$ for all processes R .

Detail at least the cases where context and processes interact, eg, when $P \xrightarrow{x(y)}$ and $R \xrightarrow{(\nu v)\bar{x}\langle v \rangle}$.