LTSs, revisited

Francesco Zappa Nardelli[1]

francesco.zappa_nardelli@inria.fr

1. INRIA Rocquencourt, MOSCOVA research team.

Plan

Objective:

understand what lies behind the equivalences for process languages.

Plan:

1. A *natural contextual equivalence*:

   motivations, definition, relationships with bisimilarity in CCS, what an LTS *is*;

2. from CCS to pi-calculus:

   congruence of bisimulation, full bisimulation.

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. But...

...lifting CCS techniques was not so smooth

The original paper on pi-calculus defines *two* LTSs:

Early LTS

$$\overline{x}v.P \xrightarrow{\overline{x}v} P$$

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

$$\frac{P \xrightarrow{\overline{x}v} P' \qquad Q \xrightarrow{x(v)} Q'}{P \,||\, Q \xrightarrow{\tau} P' \,||\, Q'}$$

Late LTS

$$\overline{x}v.P \xrightarrow{\overline{x}v} P$$

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

$$\frac{P \xrightarrow{\overline{x}v} P' \qquad Q \xrightarrow{x(y)} Q'}{P \,||\, Q \xrightarrow{\tau} P' \,||\{^{v}/_{y}\}Q'}$$

These LTSs define the same τ-transitions. But the bisimilarity built on top of them observe *all* the labels: do the resulting bisimilarities coincide? No...

Question: which is the *right* one?

A step backward: defining a language

Recipe:

1. define the *syntax* of the language (that is, specify what a program is);

2. define its *reduction semantics* (that is, specify how programs are executed);

3. define when *two terms are equivalent* (that is, hum...?!).

Share and enjoy the new language...

Equivalent?

Suppose that P and Q are equivalent (in symbols: $P \simeq Q$).

Which properties do we expect?

Preservation under contexts For all contexts $C[-]$, we have $C[P] \simeq C[Q]$;

Same observations If $P \downarrow n$ then $Q \downarrow n$, where $P \downarrow n$ means that we can *observe* n at P (or P *can do* n);

Preservation of reductions P and Q must mimic their reduction steps (that is, they realise the same nondeterministic choices).

What if we apply this recipe to (a subset of) CCS?

Syntax:

$$P \quad ::= \quad \mathbf{0} \quad \Big| \quad a.P \quad \Big| \quad \overline{a}.P \quad \Big| \quad P \,\Big|\Big|\, P \quad \Big| \quad (\boldsymbol{\nu} a)P$$

Reduction semantics:

$$a.P \,||\, \overline{a}.Q \;\rightharpoonup\; P \,||\, Q \qquad\qquad \frac{P \equiv P' \rightharpoonup Q' \equiv Q}{P \rightharpoonup Q}$$

where $\equiv$ is defined as:

$$P \,||\, Q \equiv Q \,||\, P \qquad\qquad (P \,||\, Q) \,||\, R \equiv P \,||\, (Q \,||\, R)$$

$$(\boldsymbol{\nu} a)P \,||\, Q \equiv (\boldsymbol{\nu} a)(P \,||\, Q) \text{ if } a \notin \mathrm{fn}(Q)$$

The recipe, formally

A relation $\mathcal{R}$ between processes is

preserved by contexts: if $P \mathrel{\mathcal{R}} Q$ implies $C[P] \mathrel{\mathcal{R}} C[Q]$ for all contexts $C[-]$.

barb preserving: if $P \mathrel{\mathcal{R}} Q$ and $P \downarrow_n$ imply $Q \Downarrow_n$, where $P \Downarrow n$ holds if there exists P' such that $P \rightarrow^* P'$ and $P' \downarrow n$, while

$$P \downarrow n \quad \text{holds if} \quad P \equiv (\boldsymbol{\nu}\tilde{a})(n.P' \,\|\, P'') \text{ with } n \notin \{\tilde{a}\} \ .$$

reduction closed: if $P \mathrel{\mathcal{R}} Q$ and $P \rightarrow P'$, imply that there is a Q' such that $Q \rightarrow^* Q'$ and $P' \mathrel{\mathcal{R}} Q'$ ($\rightarrow^*$ is the reflexive and transitive closure of $\rightarrow$).

The recipe, formally (ctd.)

Definition *Reduction barbed congruence*, denoted $\simeq$, is the largest symmetric relation over processes which is reduction closed, barb preserving, and preserved by contexts.

Claim: reduction barbed congruence is a *natural*, *intuitive*, contextual equivalence.

Pro and contra of reduction barbed congruence

Reduction barbed congruence is *simple* (even a programmer will understand it), "*natural*", and can be defined over any (process) language: just pick up a reasonable observation $P \downarrow n$ and you are done. Great!

Great? Hum, the definition of reduction barbed congruence tells you *nothing* about the language. In particular you have *no hints about which terms are equivalent*.

And proving that $P \simeq Q$ holds is *difficult*, because of the *universal quantification over all contexts*.

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!).

Background: LTS and weak bisimilarity for CCS

$$a.P \xrightarrow{a} P \qquad \overline{a}.P \xrightarrow{\overline{a}} P \qquad \frac{P \xrightarrow{a} P' \quad Q \xrightarrow{\overline{a}} Q'}{P \,\|\, Q \xrightarrow{\tau} P' \,\|\, Q'}$$

$$\frac{P \xrightarrow{\ell} P'}{P \,\|\, Q \xrightarrow{\ell} P' \,\|\, Q} \qquad \frac{P \xrightarrow{\ell} P' \quad a \notin \mathrm{fn}(\ell)}{(\boldsymbol{\nu} a)P \xrightarrow{\ell} (\boldsymbol{\nu} a)P'}$$

symmetric rules omitted.

Let $\stackrel{\hat{\ell}}{\Longrightarrow}$ 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 $Q \stackrel{\hat{\ell}}{\Longrightarrow} Q'$ 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. (Omitted).

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

Suppose that $P \approx Q$ and $P \rightharpoonup P'$. 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 $Q \rightharpoonup^{*} Q'$. 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

$$\begin{array}{rclrcl} C_a[-] & = & - \,\|\, \overline{a}.d & \quad Flip & = & \overline{d}.(o \oplus f) \\ C_{\overline{a}}[-] & = & - \,\|\, a.d & \quad -_1 \oplus -_2 & = & (\boldsymbol{\nu} z)(z.\, -_1 \,\|\, z.\, -_2 \,\|\, \overline{z}) \end{array}$$

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

Lemma 1. $C_a[P] \rightarrow^* P' \,\|\, d$ if and only if $P \stackrel{a}{\Longrightarrow} P'$. Similarly for $C_{\overline{a}}[-]$.

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

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 $C_a[Q] \,||\, Flip \rightarrow^* Q_1$ 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 $Q_1 \equiv Q' \,||\, o \,||(\boldsymbol{\nu} z)z.f$, and by Lemma 1. we also have $Q \stackrel{a}{\Longrightarrow} Q'$.

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

Lemma 3. $(\boldsymbol{\nu} z)z.P \simeq \mathbf{0}$.

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

$$P' \equiv P' \Big|\Big| (\boldsymbol{\nu} o)o \Big|\Big| (\boldsymbol{\nu} z)z.f \;\equiv\; (\boldsymbol{\nu} o)P_1 \;\simeq\; (\boldsymbol{\nu} o)Q_1 \;\equiv\; Q' \Big|\Big| (\boldsymbol{\nu} o)o \Big|\Big| (\boldsymbol{\nu} z)z.f \simeq Q' \;.$$

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

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

Back to pi-calculus: weak bisimilairity

Both weak labels and weak bisimilarity can be built as done in CCS.

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

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

Reduction barbed congruence and pi-calculus

First, define barbs:

$$P \downarrow x \quad \text{iff} \quad P \equiv (\boldsymbol{\nu}\tilde{n})(x(y).P' \,\Big|\Big|\, P'') \text{ with } x \notin \tilde{n} \ .$$

Let reduction barbed congruence $\simeq$ be the largest symmetric relation over pi-calculus processes that is *preserved by all contexts*, barb preserving, and reduction closed.

Exercise: prove that defining $P \downarrow x$ as $P \equiv (\boldsymbol{\nu}\tilde{n})(\overline{x}y.P \,||\, P'')$ with $x \notin \tilde{n}$ yields the same equivalence.

Reduction barbed congruence and pi-calculus, ctd.

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

$$\begin{aligned} P &= \overline{x}v \,\|\, y(z) \\ Q &= \overline{x}v.y(z) + y(z).\overline{x}v \end{aligned}$$

1. Prove that $P \approx Q$.
2. Does $P \simeq Q$?[1][2]

[1] Hint: define a context that *equates* the names x and y.

[2] Hint: 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.

Conclusion: 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 $C[-] = - || \overline{a}$, yielding P'.

More interestingly, in pi-calculus (early LTS), $P \xrightarrow{x(v)} P'$ denotes that P can interact with the context $C[-] = - || \overline{x}v$, yielding P'.

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