Equations, contractions, and unique solutions

(work in progress)

Davide Sangiorgi

Focus Team,
University of Bologna (Italy)/INRIA (France)

`Email: Davide.Sangiorgi@cs.unibo.it`
`http://www.cs.unibo.it/~sangio/`

Bertinoro, June 2014

This talk

Bisimulation proof method and coinductive operational techniques

– enhancements such as ’up-to context’

Contractions

Some new proof techniques for behavioural equivalence, eg unique solutions of contractions

– unique solutions of equations for bisimilarity [Milner ’89]

– comparable in strength to ‘up-to context’ bisimulation enhancements

– transport to inductive equivalences

The buzzwords (and some motivations)

Behavioural equivalence (processes or other objects)

P and Q behaviourally equal: no difference between them is observable

Weak equivalences (wrt internal moves)

Some standard notations (Milner's CCS book) :

μ	(action)
$\tau, \quad \ell$	(internal action, visible action $a, b \ldots$)
$P \xrightarrow{\mu} P'$	(one action)
$P \longrightarrow P'$	(one internal step, also $P \xrightarrow{\tau} P'$)
$P \Longrightarrow P'$	(reflexive and transitive closure of $\longrightarrow$)
$P \xrightarrow{\wedge} P'$	($P \longrightarrow P'$ or $P = P'$)
$P \stackrel{\mu}{\Longrightarrow} P'$	($P \Longrightarrow \xrightarrow{\mu} \Longrightarrow P'$)
$P \xrightarrow{\widehat{\mu}} P'$	($P \xrightarrow{\mu} P'$ or ($\mu = \tau$ and $P = P'$))
$P \stackrel{\widehat{\mu}}{\Longrightarrow} P'$	($P \stackrel{\mu}{\Longrightarrow} P'$ or ($\mu = \tau$ and $P = P'$))

Bisimilarity and the bisimulation proof method

Bisimulation:

A relation $\mathcal{R}$ s.t.

$$\begin{array}{ccc} P & \mathcal{R} & Q \\ \mu \downarrow & & \Downarrow \widehat{\mu} \\ P' & \mathcal{R} & Q' \end{array} \qquad\qquad \begin{array}{ccc} P & \mathcal{R} & Q \\ \widehat{\mu} \Downarrow & & \downarrow \mu \\ P' & \mathcal{R} & Q' \end{array}$$

Bisimilarity ($\approx$) :

$$\bigcup \; \{\mathcal{R} \; : \; \mathcal{R} \text{ is a bisimulation } \}$$

Hence:

$$\frac{x \,\mathcal{R}\, y \qquad \mathcal{R} \text{ is a bisimulation}}{x \approx y}$$

(bisimulation proof method)

Today by far the most popular proof technique for $\approx$
(coupled with enhancements)

Enhancements of the bisimulation proof method

Bisimulation up-to contexts:

$$\begin{array}{ccccccc}
P & & & \mathcal{R} & & & Q \\
\mu \downarrow & & & & & & \Downarrow \widehat{\mu} \\
P' & = & \cancel{C}\,[P''] & \mathcal{R} & \cancel{C}\,[Q''] & = & Q'
\end{array}$$

Identity ($=$) too strong, ideally we would like $\approx$
(eg applying some algebraic laws)

'up-to $\approx$' is unsound:

$$\begin{array}{ccccccc}
\tau.a & & & \mathcal{R} & & & 0 \\
\tau \downarrow & & & & & & \Downarrow \\
a & \approx & \tau.a & \mathcal{R} & 0 & \approx & 0
\end{array}$$

Enhancements of the bisimulation proof method (cont.)

Expansion ($\sqsupseteq$):

$$
\begin{array}{ccc}
P & \sqsupseteq & Q \\
\mu \big\downarrow & & \big\downarrow \widehat{\mu} \\
P' & \sqsupseteq & Q'
\end{array}
\qquad\qquad
\begin{array}{ccc}
P & \sqsupseteq & Q \\
\mu \Big\Downarrow & & \big\downarrow \mu \\
P' & \sqsupseteq & Q'
\end{array}
$$

Example: $\quad a + \tau . a \;\substack{\sqsupseteq \\ \not\sqsubseteq}\; a$

Bisimulation up-to expansion and contexts:

$$
\begin{array}{ccccccccc}
P & & & & \mathcal{R} & & & & Q \\
\mu \big\downarrow & & & & & & & & \Big\Downarrow \widehat{\mu} \\
P' & \sqsupseteq & \cancel{C}\,[P''] & & \mathcal{R} & & \cancel{C}\,[Q''\,] & \approx & Q'
\end{array}
$$

- Sound in CCS, π, ...
- Very effective in higher-order languages, including π
- used also on automata [Bonchi, Bonsangue, Pous, Rot, Rutten, ...]

Open problem: soundness proof of up-to context in higher-order languages

Equations and unique solutions

Unique solutions of equations

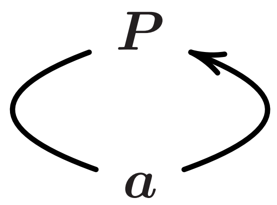
A landmark for bisimulation: **Milner's book on CCS, 1989**

One of the proof techniques proposed: unique solutions of equations

Example: $X = a.\, X$

unique solution for bisimilarity (modulo $\approx$) is P with

$$[\ P \approx a.\, P\ ]$$

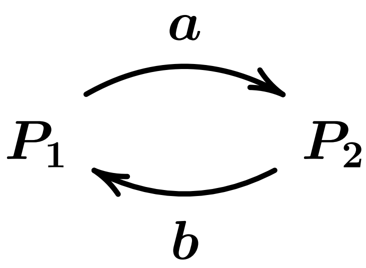


Hence: if $Q \approx a.\, Q$ then $Q \approx P$

Another example of unique solution: $X_1 = a.\, X_2,$
$X_2 = b.\, X_1$

unique solution for bisimilarity (modulo $\approx$) is (P_1, P_2) with

$$\left[\ \begin{array}{l} P_1 \approx a.\, P_2 \\ P_2 \approx b.\, P_1 \end{array}\ \right]$$



Systems of equations (in CCS)

$$\{X_i = E_i\}_{i \in I} \qquad (E_i \text{ may contain the variables } \widetilde{X})$$

Notations: $\widetilde{X} = \widetilde{E}$ as an abbreviation

$E[\widetilde{P}]$: replace (syntactically) each X_i with P_i

– **a solution for $\approx$:**

$\widetilde{P}$ with $P_i \approx E_i[\widetilde{P}]$ for each i

– **the system has unique solution for $\approx$:**

$\widetilde{P}$ and $\widetilde{Q}$ solutions imply $\widetilde{P} \approx \widetilde{Q}$.

Another example: $X = a.\,(X \mid b)$

Non examples: $X = X$ and $X = \tau.\,X$

Milner's theorem

A system of equations is

- **guarded** if each variable underneath a visible prefix
- **sequential** if each variable only underneath prefixes and sums

Examples:

- $X = \tau. X + \alpha. 0$ is sequential but not guarded
- $X = a. X \mid P$ is guarded but not sequential
- $X = a. X + \tau. b. X + \tau$ is both guarded and sequential.

Theorem [Milner, '89 CCS book] A system of equations that is guarded and sequential has unique solutions of equation for $\approx$.

Other versions of the theorem?

The sequentiality condition

... cannot be removed from the theorem. Example [Mil89] :

$$X = \nu a\, (a.\, X \mid \overline{a}) \qquad \text{(the same as } X = \tau.\, X)$$

A wrong attempt at relaxing it:

require each expression to be **sequentially guarded**
(i.e., of the form $X_i = \ell.\, E_i$)

Counterexample:

$$X = a.\, \nu b\, (\nu a\, (\overline{a}.\, !a.\, \overline{b} \mid X) \mid !b.\, a)$$

Some solutions: $a.\, 0$, $a.\, a.\, 0$, a^ω

Incompleteness

There is no system of guarded and sequential equations in which one of the solutions is the process K:

$$K \triangleq \tau.\,(a \mid K) + \tau.\,0$$

The behaviour of K can be expressed via the following process definitions (for i natural number):

$$H_i \triangleq \tau.\,H_{i+1} + a.\,H_{i-1} + \tau.\,a^i s$$

Remarks on unique solutions of equations

- The technique incorporates the **flavour of up-to context**: an equations $\widetilde{X} = \widetilde{E}$ describes the behaviour of each X_i in term of a structure (E_i)
- However: the **sequentiality condition** makes the up-to context useless (when X in E is reached, there is no "context" left)
- The same definitions, examples, counterexamples apply to **other behavioural equivalences** (eg., contextual equivalence)

  Has it been used with other equivalences?

The proposal in this talk

A new technique, refinement of unique solutions of equations

Contractions in place of equations

Pros:

- no constraints on sequentiality
- complete
- **up-to context**
- can be transported onto contextual/inductive equivalences
  (more generally any equivalence with finitary observables)
- bisimulations up-to contraction and context
- language independent

Cons:

- later ....

Contractions

The contraction $\underset{\frown}{\succ}$ of a behavioural equivalence $\asymp$

$P \underset{\frown}{\succ} Q \triangleq P \asymp Q$ and, in addition, Q has the **possibility** of being as efficient as P (however Q may also have slower paths)

Example: the **bisimilarity contraction** $\succapprox$

$$\begin{tikzcd} P \arrow[d, "\mu"'] \arrow[r, phantom, "\succapprox"] & Q \arrow[d, "\widehat{\mu}"] \\ P' \arrow[r, phantom, "\succapprox"] & Q' \end{tikzcd} \qquad\qquad \begin{tikzcd} P \arrow[d, Rightarrow, "\widehat{\mu}"'] \arrow[r, phantom, "\succapprox"] & Q \arrow[d, "\mu"] \\ P' \arrow[r, phantom, "\approx"] & Q' \end{tikzcd}$$

(same as for expansion) (same as for bisimulation)

- Examples: $a + \tau. a \succapprox a, \quad a \succapprox a + \tau. a, \quad a \not\succapprox \tau. a$
- Coarser than expansion
- (Pre)-congruence properties: as those of bisimilarity and expansion

Systems of contractions

$\{X_i \succeq E_i\}_{i \in I}$ (E_i may contain the variables $\widetilde{X}$)

- **a solution for $\succsim$:**
  $\widetilde{P}$ with $P_i \succsim E_i[\widetilde{P}]$ for each i
- **the system has unique solution for $\approx$:**
  whenever $\widetilde{P}$ and $\widetilde{Q}$ are solutions for $\succsim$, then $\widetilde{P} \approx \widetilde{Q}$.

Some simple facts:

- unique solutions for $\widetilde{X} = \widetilde{E}$ implies unique solutions for $\widetilde{X} \succeq \widetilde{E}$ (because there is at least one solution for strong bisimilarity)
- converse false, for $X \succeq \tau. X$ (unique solution for $\approx$ is τ^ω)
- still no unique solutions for $X \succeq X$

Conditions for unique solutions

A system of contractions $\{X_i \succeq E_i\}_{i \in I}$ is **weakly guarded** if each variable underneath a prefix (possibly τ)

Theorem A weakly-guarded system of contractions has unique solutions for $\approx$.

NB: ‘guarded and sequential’ replaced by ‘weakly guarded’

Examples:

- $X \succeq \tau.\, X$
- $X \succeq a.\, \nu b\, (\nu a\, (\overline{a}.\, !a.\, \overline{b} \mid X) \mid !b.\, a)$ (a solution is $a.\, \tau^{\omega}$)

Completeness (in CCS)

Theorem Any process bisimilarity can be proved using a system of weakly guarded contractions

Also computationally complete:

Theorem Suppose $\mathcal{R}$ is a bisimulation. Then there is a system of weakly guarded contractions, of the same size, of which the projections of $\mathcal{R}$ are solutions for $\approx$.

The result also holds wrt bisimulation enhancements, such as ‘bisimulation up-to expansion and context’.

(The contraction technique is equivalent to ‘bisimulation up-to contraction and context’)

Proofs: the definition of contraction is crucial

Applications to non-coinductive equivalences

Contextual equivalence

$P \Downarrow \triangleq P \Longrightarrow\xrightarrow{\ell}$, for $\ell \neq \tau$ (ie, barb/convergence)

Definition [contextual equivalence] $P \smile Q$ if for all C:
$C[\,P\,] \Downarrow$ iff $C[\,Q\,] \Downarrow$.

$P \Downarrow^n \triangleq P(\xrightarrow{\tau})^n \xrightarrow{\ell}$. Similarly for $P \Downarrow^{\leq n}$

Definition [contextual equivalence contraction] $P \succsim Q$ if for all C:

1. $C[\,P\,] \Downarrow^n$ implies $C[\,Q\,] \Downarrow^{\leq n}$;
2. $C[\,Q\,] \Downarrow$ implies $C[\,P\,] \Downarrow$.

unique solution of $\widetilde{X} \succeq \widetilde{E}$ for $\smile$: if $\widetilde{P} \succsim \widetilde{E}[\widetilde{P}]$ and $\widetilde{Q} \succsim \widetilde{E}[\widetilde{Q}]$ then $\widetilde{P} \smile \widetilde{Q}$

Theorem **A system of weakly guarded contractions has unique solution for $\smile$.**

Proof (sketch): Suppose $\widetilde{P}$ and $\widetilde{Q}$ are solutions.

Show that $C[\ \widetilde{P}\ ] \Downarrow$ implies $C[\ \widetilde{Q}\ ] \Downarrow$.

Induction on n s.t. $C[\ \widetilde{P}\ ] \Downarrow^{n}$. Case $n = 0$ easy.

Case $n > 0$.

$C[\ \widetilde{P}\ ] \Downarrow^{n}$ and $\widetilde{P} \succeq \widetilde{E}[\widetilde{P}]$ imply $C[\ \widetilde{E}[\widetilde{P}]\ ] \Downarrow^{\leq n}$.

Since $\widetilde{E}$ is weakly guarded, either $C[\ \widetilde{E}[\widetilde{P}]\ ] \Downarrow^{0}$, or
$C[\ \widetilde{E}[\widetilde{P}]\ ] \longrightarrow C'[\widetilde{P}] \Downarrow^{\leq n-1}$

Latter case: also $C[\ \widetilde{E}[\widetilde{Q}]\ ] \longrightarrow C'[\widetilde{Q}]$ (since $\widetilde{E}$ is weakly guarded)

By induction and $C'[\widetilde{P}] \Downarrow^{\leq n-1}$ infer $C'[\widetilde{Q}] \Downarrow$.

Hence $C[\ \widetilde{E}[\widetilde{Q}]\ ] \Downarrow$.

From $\widetilde{Q} \succeq \widetilde{E}[\widetilde{Q}]$, deduce $C[\ \widetilde{Q}\ ] \Downarrow$. $\square$

Theorem **A system of weakly guarded contractions has unique solution for $\smile$.**

- Only hypothesis on the calculus: a weakly guarded term does not contribute to the first reduction.

- A more general condition than ‘weakly guarded’:

E is **autonomous** if for all processes $\widetilde{P}$ and context C:

- if $C[\,\widetilde{E}[\widetilde{P}]\,] \longrightarrow R$, then there is a context C' such that $R = C'[\widetilde{P}]$, and for all $\widetilde{Q}$, also $C[\,\widetilde{E}[\widetilde{Q}]\,] \longrightarrow C'[\widetilde{Q}]$;

- if $C[\,\widetilde{E}[\widetilde{P}]\,] \Downarrow^0$ then for all $\widetilde{Q}$, also $C[\,\widetilde{E}[\widetilde{Q}]\,] \Downarrow^0$.

Theorem **A system of autonomous contractions has unique solution for $\smile$.**

Similar theorems for other equivalences, eg trace equivalence, ready-trace equivalence, barbed congruence.

Example: an eager and a lazy server

Spec: a server when contacted by a client at c, starts a certain interaction protocol with the client after consulting an auxiliary server A at a.

Two implementations:
- an **eager** server E anticipates the consultation to A
- a **lazy** server L consults A after a client request

$$\boxed{\begin{array}{rcl} E & \triangleq & a(x).\,c(z).\,(E \mid R\langle c,x,z\rangle) \\ L & \triangleq & c(z).\,a(x).\,(L \mid R\langle c,x,z\rangle) \\ A\langle n\rangle & \triangleq & \overline{a}\langle n\rangle.\,A\langle n+1\rangle \end{array}}$$

$R\langle c,x,z\rangle$ = interaction protocol with the client

(possibly involving c, x, z)

NB: A is deterministic

We compare the systems:

$$\begin{array}{rcl} SE\langle n\rangle & \triangleq & \nu a\,(A\langle n\rangle \mid E) \\ SL\langle n\rangle & \triangleq & \nu a\,(A\langle n\rangle \mid L) \end{array}$$

We wish to prove $SE\langle n\rangle \approx SL\langle n\rangle$

They are both solutions, for the bisimulation contraction, to the system

$$\{X_n \succeq c(z).\,(X_{n+1} \mid R\langle c,n,z\rangle)\}_n$$

The proof uses some simple agebraic proof, e.g.,

$$\begin{array}{rcll} \nu a\ (a(\widetilde{x}).\, P \mid \overline{a}\langle\widetilde{v}\rangle.\, Q) & \gtrapprox & \nu a\ (P\{\widetilde{v}/\widetilde{x}\} \mid Q) & \\ Q \mid \nu a\, P & \sim & \nu a\ (P \mid Q) & a \text{ not free in } Q \end{array}$$

Thus:

$$\begin{array}{rcl} SE\langle n\rangle & \sim & \nu a\ (\tau.\, (A\langle n+1\rangle \mid c(z).\, (E \mid R\langle c,n,z\rangle))) \\ & \sim & \tau.\, c(z).\, (\nu a\ (A\langle n+1\rangle \mid E) \mid R\langle c,n,z\rangle) \\ & \gtrapprox & c(z).\, (\nu a\ (A\langle n+1\rangle \mid E) \mid R\langle c,n,z\rangle) \\ & = & c(z).\, (SE\langle n+1\rangle \mid R\langle c,n,z\rangle) \end{array}$$

$$\begin{array}{rcl} SE\langle n\rangle & \triangleq & \nu a\ (A\langle n\rangle \mid E) \\ SL\langle n\rangle & \triangleq & \nu a\ (A\langle n\rangle \mid L) \end{array}$$

$$\begin{array}{rcl} E & \triangleq & a(x).\, c(z).\, (E \mid R\langle c,x,z\rangle) \\ L & \triangleq & c(z).\, a(x).\, (L \mid R\langle c,x,z\rangle) \\ A\langle n\rangle & \triangleq & \overline{a}\langle n\rangle.\, A\langle n+1\rangle \end{array}$$

Another pair of an eager and a lazy server

Now the auxiliary server A is nondeterministic

$$
\begin{array}{lcl}
E & \triangleq & a(x).\, c(z).\, (E \mid R\langle c, x, z\rangle) \\
L & \triangleq & c(z).\, a(x).\, (L \mid R\langle c, x, z\rangle) \\
A & \triangleq & \Sigma_{n \in N}\ \overline{a}\langle n\rangle.\, A
\end{array}
$$

We compare the systems:

$$
\begin{array}{lcl}
SE & \triangleq & \nu a\, (A \mid E) \\
SL & \triangleq & \nu a\, (A \mid L)
\end{array}
$$

- They are not bisimilar
  Not even simulation equivalent

We wish to prove SE and SL contextually equivalent.

They are both solutions, for the contextual equivalence contraction, of

$$X \succeq c(z).\, \Sigma_n (X \mid R\langle c, n, z\rangle)$$

Proof: similar algebraic laws as for the previous servers, plus the law

$$\alpha.\, \Sigma_i P_i \succsim \Sigma_i \alpha.\, P_i$$

We derive:

$$\begin{array}{rcl} SE & \succsim & c(z).\, \Sigma_n (SE \mid R\langle c, n, z\rangle) \\ SL & \succsim & c(z).\, \Sigma_n (SL \mid R\langle c, n, z\rangle) \end{array}$$

Hence: $SE \smile SL$

Non-applicability of the technique of unique solution of contractions

Notation: $\asymp$ for infinitary trace equivalence
(ie, same traces, including the infinite ones)
$\overset{\succ}{\frown}$ for its contraction

Let $P \triangleq \Sigma_n a^n$ and $Q \triangleq P + a^\omega$

We have $P \not\asymp Q$

However they both are solutions for $\overset{\succ}{\frown}$ to the (guarded and sequential) contraction

$$X \succeq a + a.\, X$$

Must equivalence ? fair must?

... back to the bisimulation game

Injecting contractions into the the ‘bisimulation up-to’ game

Bisimulation up-to bisimilarity contraction ($\underset{\approx}{\succ}$) and contexts:

$$\begin{array}{ccccccc} P & & & \mathcal{R} & & & Q \\ \mu\big\downarrow & & & & & & \Big\Downarrow\mu \\ P' & \underset{\approx}{\succ} & \cancel{C}[P''] & \mathcal{R} & \cancel{C}[Q''] & \approx & Q' \end{array}$$

Bisimulation up-to contextual contraction ($\underset{\smile}{\succ}$) and contexts:

$$\begin{array}{ccccccc} P & & & \mathcal{R} & & & Q \\ \mu\big\downarrow & & & & & & \Big\Downarrow\mu \\ P' & \underset{\smile}{\succ} & \cancel{C}[P''] & \mathcal{R} & \cancel{C}[Q''] & \smile & Q' \end{array}$$

This technique is (in CCS):

- sound for contextual equivalence ($\smile$)
- can be used to handle the server examples

Final remarks

Some conclusions on contractions

Pros:

– no constraints on sequentiality

– the power of up-to context and up-to expansion (at least)

– can be transported onto contextual equivalences
(more generally any equivalence with inductive weak observables)

– bisimulations up-to contraction and context

– language independent

– in the λ-calculus and higher-order concurrency:
it allows us to derive new forms of up-to context for bisimilarity

Cons:

– (wrt equations) solutions not invariant wrt the chosen behavioural equivalence: eg, $\widetilde{P} \succeq\!\!\!\approx \widetilde{E}[\widetilde{P}]$ and $\widetilde{P} \approx \widetilde{Q}$ does not imply $\widetilde{Q} \succeq\!\!\!\approx \widetilde{E}[\widetilde{Q}]$

Other issues for unique-solution of contractions

- what makes the technique applicable to a certain equivalence?
- calculi with binders
  - Example: contractions of the form $X \succeq a(z).\,Y + \ldots$ are limiting
    (a single equations for each instantiation of y)
  - ok in the π-calculus, using the match and mismatch operators,
  - non-ok in the λ-calculus, though still useful
    (the resulting up-to context looks still more powerful than the existing ones)
- axiomatisation of contraction
- comparison with the theory of bisimulation enhancements
- contractions in metric spaces