Unique solution techniques for bisimilarity

Adrien Durier

With Daniel Hirschkoff (ENS Lyon), Davide Sangiorgi (Università di Bologna)

Rencontres GéoCal-LAC, 28 novembre 2016
This talk

• About proof techniques for coinductive equivalences

• **Bisimilarity** comes with bisimulation
  → Bisimulation enhancements (up-to techniques)

• Proof techniques based on equations and unique solutions
  → General idea: **Guardedness** guarantees unique solution
  → Historical **syntactic** criteria
  → **Here:** (general) non-syntactic criteria for unique solutions
Unique solutions of equations (as a proof technique)

- $\equiv$: equivalence between programs
- $x$: ranges over programs
- $f$: function over program, program context

**Equation:** $x = f[x]$
Unique solutions of equations (as a proof technique)

- \( \equiv \): equivalence between programs
- \( x \): ranges over programs
- \( f \): function over program, program context

Equation: \( x = f[x] \)

\( f \) has a **unique solution** (for \( = \)):
\[
\begin{align*}
x &= f[x] \\
y &= f[y]
\end{align*}
\]

Then \( x = y \)
Calculus of Communicating Systems

channels: a, b, c . . .

\[ P, Q := 0 | \mu P | P | Q | K | \nu a P \]

Milner, *Communication and concurrency*, 1989

Only models *synchronizations*
Calculus of Communicating Systems

channels: a, b, c...

\[ P, Q \ := \ 0 \ | \ \mu P \ | \ P \ | \ Q \ | \ K \ | \ \nu a P \]

\[ \mu P \ \xrightarrow{\mu} \ P \]

\[ \mu \ := \]

- a: Receives on channel a
- \( \bar{a} \): Emits on channel a
- \( \tau \): Internal action (invisible)

Example: \( \bar{a} \cdot 0 \ \xrightarrow{\bar{a}} \ 0 \)
Calculus of Communicating Systems

channels: \( a, b, c \ldots \)

\[
P, Q \; := \; 0 \mid \mu.P \mid P \mid Q \mid K \mid \nu a \; P
\]

\[
\mu.P \xrightarrow{\mu} P
\]

Example: \( a.0 \mid b.0 \)

\[
a \xrightarrow{0} b.0
\]

\[
b \xrightarrow{a.0 \mid 0}
\]
Calculus of Communicating Systems

channels: \( a, b, c \ldots \)

\[
P, Q ::= 0 \mid \mu P \mid P \mid Q \mid K \mid \nu a P
\]

\[
\mu P \xrightarrow{\mu} P
\]

\[
P \xrightarrow{a} P' \quad Q \xrightarrow{\overline{a}} Q'
\]

\[
P \mid Q \xrightarrow{\tau} P' \mid Q'
\]

Example: \( a \cdot 0 \mid \overline{a} \cdot b \cdot 0 \)

\[
0 \mid b \cdot 0 \quad a \cdot 0 \mid b \cdot 0
\]

\[
0 \mid \overline{a} \cdot b \cdot 0
\]
Calculus of Communicating Systems

*channels*: $a, b, c \ldots$

$$P, Q ::= 0 \mid \mu P \mid P \mid Q \mid K \mid \nu a P$$

*Constants*: $K ::= P$

For example, $K_a ::= a.K_a$

$$K_a \xrightarrow{a} K_a$$
Calculus of Communicating Systems

channels: a, b, c . . .

\[ P, Q := 0 \mid \mu.P \mid P \mid Q \mid K \mid \nu a P \]

\[ \nu a P \not\rightarrow \]

Example: \[ \nu a ( \bar{a} \mid a ) \rightarrow 0 \]
Bisimulations (weak)

\[
P \xrightarrow{\mu} P' \\
\overrightarrow{\mu} \\
R \\
\overrightarrow{\mu} \\
Q \xrightarrow{\hat{\mu}} Q'
\]

\[
\hat{\mu} := \begin{cases} 
\tau \xrightarrow{*} \mu \xrightarrow{*} \tau \xrightarrow{*} & \text{if } \mu \neq \tau \\
\tau \xrightarrow{*} & \text{if } \mu = \tau
\end{cases}
\]

weak transitions: \(\tau\) is invisible
Bisimulations (weak)

\[
\begin{array}{ccc}
P & & Q \\
\Downarrow & \mathcal{R} & \Downarrow \\
\hat{\mu} & & \mu \\
P' & & Q' \\
\end{array}
\]

\[
\hat{\mu} := \begin{cases} 
\tau \rightarrow^* \mu \rightarrow^* \tau & \text{if } \mu \neq \tau \\
\tau \rightarrow^* & \text{if } \mu = \tau 
\end{cases}
\]

weak transitions: \( \tau \) is invisible
Bisimulations (weak)

\[ P \approx Q \]

\[ P' \approx Q' \]

\[ \approx = \bigcup \mathcal{R} \]

\[ \approx: \text{bisimilarity} \]
Bisimulations (weak)

Examples

\[ X \approx \tau.X \]

\[ \forall P, \quad P \approx \tau.P \]

(not a constant: \( K_\tau \ ::= \tau. K_\tau \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\tau} \ldots \))
<table>
<thead>
<tr>
<th>Background</th>
<th>Equations</th>
<th>Unique solutions and divergences</th>
<th>Generalization</th>
</tr>
</thead>
</table>

Equations and unique solutions
Equations and unique solutions

\[ X \approx E[X] \]

Unique solutions:

If \( P \approx E[P] \) and \( Q \approx E[Q] \),

Then \( P \approx Q \)
Equations and unique solutions

\[ X \approx E[X] \]

Example

\[ X \approx a \tau X \]

Solutions \( \approx a.a.a.a.a \ldots \)
Equations and unique solutions

\[ X \approx E[X] \]

**Unique solutions:**

If \( P \approx E[P] \) and \( Q \approx E[Q] \)

Then \( P \approx Q \)

**Solutions:**

- Consider the constant \( K_E := E[K_E] \)
- \( K_E = E[E[E[E[\ldots]]]] \) is always solution

\( E^\infty: \) syntactic solution
Equations do not always have a unique solution

\[ X \approx X \text{ or } X \approx \tau.X \] do not have unique solutions:

\[ \forall P, \; P \approx \tau.P \]
Equations do not always have a unique solution

\[ X \approx X \text{ or } X \approx \tau.X \] do not have unique solutions:

\[ \forall P, P \approx \tau.P \]

1. **No prefix** to constrain behavior
2. **Weak prefix** (\(\tau\)) does not constrain behavior

\[ X \approx a\overline{b}.X \]

**Unique solution**: \(a\overline{b}.a\overline{b}.a\ldots\)
Equations do not always have a unique solution

\[ X \approx X \text{ or } X \approx \tau.X \] do not have unique solutions:

\[ \forall P, P \approx \tau.P \]

1. **No prefix** to constrain behavior
2. **Weak prefix** (\(\tau\)) does not constrain behavior

\[ X \approx a.b.X \]

**Unique solution:** \(a.b.a.b.a\ldots\)

Is this enough?
Failure of unique solutions

\[ X = b. \nu b ( \bar{b} \mid X ) \]

\( b. P \) is a solution for any \( P \) (st \( b \not\in \text{fn}(P) \))
Failure of unique solutions

\[ X = b. \nu b ( \overline{b} \mid X ) \]

\( b.P \) is a solution for any \( P \) (st \( b \not\in \text{fn}(P) \))

\[
\begin{align*}
\downarrow b & \quad \approx & \quad \downarrow b \\
\downarrow P & \quad \approx & \quad \nu b ( \overline{b} \mid b. P )
\end{align*}
\]
Failure of unique solutions

\[ X = b. \nu b (\bar{b} \mid X) \]

\( b. P \) is a solution for any \( P \) \((\text{st } b \not\in \text{fn}(P))\)

\[
\begin{array}{ccc}
b. P & \approx & b. \nu b (\bar{b} \mid b. P) \\
b \downarrow & & \downarrow b \\
P & \approx & \nu b (\bar{b} \mid b. P) \\
\equiv & \tau. P & \approx P
\end{array}
\]
Milner’s unique solutions

Theorem (Milner, ’89 CCS book)

A system of equations that is **strongly guarded** and **sequential** has a **unique solution** for $\approx$.

- **Strongly guarded** if each variable underneath a *visible* prefix
  - reasonable hypothesis
- **Sequential** if variables not underneath parallel compositions
  - way too constraining

Examples:
- $X \approx \tau.X$ is sequential, but not strongly guarded
- $X \approx (a.X) \mid \overline{b}$ and $X \approx a.(\overline{b} \mid X)$ are strongly guarded, but not sequential

Unique solution techniques for bisimilarity
### Milner’s unique solutions

**Theorem (Milner, ’89 CCS book)**

A system of equations that is *strongly guarded* and *sequential* has a *unique solution* for $\approx$.

- **Strongly guarded** if each variable underneath a *visible* prefix
  - reasonable hypothesis
- **Sequential** if variables not underneath parallel compositions
  - way too constraining

**Examples:**

- $X \approx \tau.\overline{X}$ is *sequential*, but not *strongly guarded*
- $X \approx (a.X) | \overline{b}$ and $X \approx a.(\overline{b} | X)$ are *strongly guarded*, but not *sequential*
A uniqueness result for divergence-free equations
Divergences and unique solutions

\[ X \approx \tau \cdot X \]

- \[ E^\infty = \tau \cdot \tau \cdot \tau \cdot \tau \ldots \]
Divergences and unique solutions

$$X \approx \bar{b} \mid b.X$$

- Solutions: $$\forall P, \boldsymbol{P} \mid \bar{b} (\mid b.\bar{b})^\omega$$
- $$\mathbf{E}^\infty = \bar{b} \mid b.(\bar{b} \mid b.(\bar{b} \mid b \ldots )) \xrightarrow{T} \xrightarrow{T} \xrightarrow{T} \ldots$$
Divergences and unique solutions

\[ X \approx \overline{b} \mid b.X \]

- Solutions: \( \forall P, P \mid \overline{b} \mid b.(\overline{b} \mid b.\overline{b})^\omega \)
- \( E^\infty = \overline{b} \mid b.(\overline{b} \mid b.\overline{b} \mid b \ldots)) \overrightarrow{T} \overrightarrow{T} \overrightarrow{T} \overrightarrow{T} \ldots \)
- **Divergence**: infinite sequence of \( \overrightarrow{T} \) transitions
Unique solutions for divergence free equations

**Theorem (Unique solutions for divergence free equations)**

If $E^\infty$ has no divergences, then guarded equation $X \approx E[X]$ has a unique solution.

- $P$ has a divergence: $P \xrightarrow{\mu_1} \xrightarrow{\mu_2} \ldots \xrightarrow{\mu_n} \xrightarrow{T} \xrightarrow{T} \ldots \xrightarrow{T} \ldots$

- **Syntactic solution** $E^\infty := E[E[E[\ldots ]]]$
Unique solution and context transitions

\[ P \approx E[P] \quad E[Q] \approx Q \]

\textbf{P} are \textbf{Q} solutions of \( X \approx E[X] \).

We show unique solution:

\[ P \approx Q \]
Unique solution and context transitions

\[ P \approx E[P] \approx E[Q] \approx Q \]

Challenges of \( P \)

Unique solution techniques for bisimilarity

Adrien Durier
Unique solution and context transitions

\[ P \approx E \left[ P \right] \approx E \left[ Q \right] \approx Q \]
Unique solution and context transitions

This transition is a context transition of $E$:
Unique solution and context transitions

This transition is a context transition of $E$: $E[Q]$ can match it;
Unique solution and context transitions

This transition is a context transition of $E$: $E[Q]$ can match it; $Q$ too.
Unique solution and context transitions

\[ C[P] \approx C[E[P]] \approx C'[P] \]
\[ C[Q] \approx C'[Q] \]

We keep playing the game, so we need to close by contexts...
Unique solution and context transitions

Context transitions

- Transitions **that are independent from the process inside:**
  \[ C[\cdot] \xrightarrow{\mu} C'[\cdot] \text{ if } \forall P, \; C[P] \xrightarrow{\mu} C'[P] \]

- General notion, independent of the language

- Related to **guardedness** in CCS
  (guarded context \(\Rightarrow\) context transition)
Unique solution and context transitions

\[
P \approx E^n[P] \quad \Downarrow \hat{\mu} \approx C'[P]
\]
\[
E^n[Q] \approx Q \quad \Downarrow \hat{\mu} \approx C'[Q]
\]

P is also solution of \( X \approx E^n[X] \)
Unique solution and context transitions

\[
C[P] \cong C[E^n[P]] \quad C[E^n[Q]] \cong C[Q]
\]

\[
\hat{\mu} \quad \hat{\mu} \quad \hat{\mu} \quad \hat{\mu}
\]

\[
\cong \quad \cong \quad \cong
\]

Unique solution if any transition of \( C[P] \) can be matched by a \( C[E^n[\cdot]] \):

\('
E[\cdot] \) protects its solutions’
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \]

Idea: \( E_n \cdot E \) cannot always catch up to \( P \); the transition eventually only depends on \( E_n \cdot E \) is guarded. Therefore we can reproduce this transition in the context \( E_n \).

And we start again.
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \]

\( E[\cdot] \) is guarded
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \approx C[E^2[P]] \]

\[ P' \approx T_1 \]
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \approx C[E^2[P]] \]

We complete by bisimilarity
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \approx C[E^2[P]] \]

And we start again…
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \approx C[E^2[P]] \approx C[E^3[P]] \]

And we start again…
A divergence-free equation protects its solutions

\[ C[P] \approx C[E[P]] \approx C[E^2[P]] \approx C[E^3[P]] \approx \ldots \]
A divergence-free equation protects its solutions

\[
C[P] \approx C[E[P]] \approx C[E^2[P]] \approx C[E^3[P]] \approx \ldots \approx C[E^n[P]]
\]

Idea:

\[E^n[\cdot] \text{ cannot always catch up to } P; \text{ the transition eventually only depends on } E^n[\cdot] \]

Therefore we can reproduce this transition in the context \(E^2[\cdot]\)

We complete by bisimilarity

And we start again.

Unique solution techniques for bisimilarity

Adrien Durier
Limit

If the construction never stops:

⇒ divergence of $E^\infty$

\[
C[E[\cdot]] \quad C[E^2[\cdot]] \quad \ldots \quad C[E^n[\cdot]] \quad \ldots \\
C[E^\infty]
\]

Unique solution techniques for bisimilarity

Adrien Durier
A theorem for unique solutions

- Divergence-free equation $\rightarrow$ build context transitions
- With context transitions $\rightarrow$ $P \approx Q$ (Unique solution)

**Theorem**

\[
\text{If } X \approx E[X] \text{ is guarded and } E^\infty \text{ has no divergences, then } X \approx E[X] \text{ has a unique solution for } \approx.
\]
Generalization
Generalization

- **Guardedness** and **non-divergence** guarantee a **unique solution**

- **What we need:**
  - **Context transitions**
    \[ c \xrightarrow{\mu} c' \iff \forall x, c(x) \xrightarrow{\mu} c'(x) \]
  - **Guarded contexts**
    \[ c(x) \xrightarrow{\mu} y \Rightarrow \exists c', c \xrightarrow{\mu} c' \text{ and } y = c'(x) \]
  - Contexts are **congruences**
    \[ x \approx y \Rightarrow c(x) \approx c(y) \]
  - Contexts **compose**, and composition respects guardedness

- Hence, works with any **1st order LTS**, asynchronous \(\pi\)-calculus, trace equivalence, behavioral preorders...
Generalization

- **Guardedness** and non-divergence guarantee a unique solution

- What we need:
  - Context transitions
    \[ c \xrightarrow{\mu} c' \iff \forall x, c(x) \xrightarrow{\mu} c'(x) \]
  - Guarded contexts
    \[ c(x) \xrightarrow{\mu} y \Rightarrow \exists c', c \xrightarrow{\mu} c' \text{ and } y = c'(x) \]
  - Contexts are congruences
    \[ x \approx y \Rightarrow c(x) \approx c(y) \]
  - Contexts compose, and composition respects guardedness

- Hence, works with any 1st order LTS, asynchronous \( \pi \)-calculus, trace equivalence, behavioral preorders...
Correspondence with up-to techniques

- **Up-to techniques**: widely studied bisimulation enhancements

- 'Up to context techniques and unique solutions are the same’ [Sangiorgi15]

- This theorem is inspired by a theorem for CSP due to Roscoe (fixpoints in CSP), but is still essentially an up-to technique