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)

- $=$: equivalence between programs
- $\mathbf{x}$: ranges over programs
- f: function over program, program context

Equation: $\mathbf{x} = f[\mathbf{x}]$

Unique solutions of equations (as a proof technique)

- $=$: equivalence between programs
- $\mathbf{x}$: ranges over programs
- f: function over program, program context

Equation: $\mathbf{x} = f[\mathbf{x}]$

f has **a unique solution** (for $=$):

$\mathbf{x} = f[\mathbf{x}]$ $\qquad$ $\mathbf{y} = f[\mathbf{y}]$

Then $\mathbf{x} = \mathbf{y}$

Calculus of Communicating Systems

channels: $\mathtt{a}, \mathtt{b}, \mathtt{c} \ldots$

$$\mathbf{P}, \mathbf{Q} \;:=\; \mathbf{0} \;\;|\;\; \mu.\mathbf{P} \;\;|\;\; \mathbf{P} \,|\, \mathbf{Q} \;\;|\;\; \mathbf{K} \;\;|\;\; \nu a\, \mathbf{P}$$

Milner, *Communication and concurrency*, 1989

Only models **synchronizations**

Calculus of Communicating Systems

channels: $\mathtt{a}, \mathtt{b}, \mathtt{c} \ldots$

$$\mathbf{P}, \mathbf{Q} \; := \; \mathbf{0} \;\mid\; \mu.\mathbf{P} \;\mid\; \mathbf{P} \mid \mathbf{Q} \;\mid\; \mathbf{K} \;\mid\; \nu a\, \mathbf{P}$$

$$\mu.\mathbf{P} \xrightarrow{\mu} \mathbf{P}$$

$\mu \; :=$

- a: Receives on channel a
- $\overline{\mathsf{a}}$: Emits on channel a
- τ: Internal action (invisible)

Example: $\overline{\mathsf{a}}.\mathbf{0} \xrightarrow{\overline{\mathsf{a}}} \mathbf{0}$

Calculus of Communicating Systems

channels: $\mathtt{a}, \mathtt{b}, \mathtt{c} \dots$

$$\mathbf{P}, \mathbf{Q} \;:=\; \mathbf{0} \;\mid\; \mu.\mathbf{P} \;\mid\; \mathbf{P} \mid \mathbf{Q} \;\mid\; \mathbf{K} \;\mid\; \nu a\, \mathbf{P}$$

$$\mu.\mathbf{P} \xrightarrow{\mu} \mathbf{P}$$

$$\frac{\mathbf{P} \xrightarrow{\mu} \mathbf{P'}}{\mathbf{P} \mid \mathbf{Q} \xrightarrow{\mu} \mathbf{P'} \mid \mathbf{Q}} \qquad \frac{\mathbf{Q} \xrightarrow{\mu} \mathbf{Q'}}{\mathbf{P} \mid \mathbf{Q} \xrightarrow{\mu} \mathbf{P} \mid \mathbf{Q'}}$$

Example: $\mathtt{a}.\mathbf{0} \mid \mathtt{b}.\mathbf{0} \xrightarrow{\mathtt{a}} \mathbf{0} \mid \mathtt{b}.\mathbf{0}$

$\mathtt{a}.\mathbf{0} \mid \mathtt{b}.\mathbf{0} \xrightarrow{\mathtt{b}} \mathtt{a}.\mathbf{0} \mid \mathbf{0}$

Calculus of Communicating Systems

channels: a, b, c . . .

$$\mathbf{P}, \mathbf{Q} \; := \; \mathbf{0} \;\mid\; \mu.\mathbf{P} \;\mid\; \mathbf{P} \mid \mathbf{Q} \;\mid\; \mathbf{K} \;\mid\; \nu a\, \mathbf{P}$$

$$\mu.\mathbf{P} \xrightarrow{\mu} \mathbf{P}$$

$$\frac{\mathbf{P} \xrightarrow{a} \mathbf{P}' \qquad \mathbf{Q} \xrightarrow{\overline{a}} \mathbf{Q}'}{\mathbf{P} \mid \mathbf{Q} \xrightarrow{\tau} \mathbf{P}' \mid \mathbf{Q}'}$$

Example: $a.\mathbf{0} \mid \overline{a}.b.\mathbf{0} \xrightarrow{\tau} \mathbf{0} \mid b.\mathbf{0}$

$a.\mathbf{0} \mid \overline{a}.b.\mathbf{0} \xrightarrow{\overline{a}} a.\mathbf{0} \mid b.\mathbf{0}$

$a.\mathbf{0} \mid \overline{a}.b.\mathbf{0} \xrightarrow{a} \mathbf{0} \mid \overline{a}.b.\mathbf{0}$

Calculus of Communicating Systems

channels: $\mathtt{a}, \mathtt{b}, \mathtt{c} \ldots$

$$\mathbf{P}, \mathbf{Q} \;:=\; \mathbf{0} \;\;|\;\; \mu.\mathbf{P} \;\;|\;\; \mathbf{P} \mid \mathbf{Q} \;\;|\;\; \mathbf{K} \;\;|\;\; \boldsymbol{\nu} a\, \mathbf{P}$$

Constants: $\mathbf{K} \;:=\; \mathbf{P}$

For example, $\mathbf{K}_{\mathtt{a}} \;:=\; \mathtt{a}.\mathbf{K}_{\mathtt{a}}$

$$\mathbf{K}_{\mathtt{a}} \xrightarrow{a} \mathbf{K}_{\mathtt{a}}$$

Calculus of Communicating Systems

channels: $\mathtt{a}, \mathtt{b}, \mathtt{c} \ldots$

$$\mathbf{P}, \mathbf{Q} \ := \ \mathbf{0} \ \mid \ \mu.\mathbf{P} \ \mid \ \mathbf{P} \mid \mathbf{Q} \ \mid \ \mathbf{K} \ \mid \ \nu a \ \mathbf{P}$$

$$\nu a \ \mathbf{P} \stackrel{\mathtt{a}}{\not\rightarrow}$$

Example: $\nu \mathtt{a} \ (\ \overline{\mathtt{a}} \mid \mathtt{a} \ ) \xrightarrow{\tau} \mathbf{0}$

Bisimulations (weak)

$$
\begin{tikzcd}
\mathbf{P} \arrow[d, "\mu"'] & \mathcal{R} & \mathbf{Q} \arrow[d, Rightarrow, "\hat{\mu}"'] \\
\mathbf{P'} & \mathcal{R} & \mathbf{Q'}
\end{tikzcd}
$$

$$
\overset{\hat{\mu}}{\Longrightarrow} := \begin{cases} \xrightarrow{\tau}{}^{*} \xrightarrow{\mu} \xrightarrow{\tau}{}^{*} & \text{if } \mu \neq \tau \\ \xrightarrow{\tau}{}^{*} & \text{if } \mu = \tau \end{cases}
$$

weak transitions: τ is **invisible**

Bisimulations (weak)

$$
\begin{tikzcd}
\mathbf{P} \arrow[d, Rightarrow, "\hat{\mu}"'] & \mathcal{R} & \mathbf{Q} \arrow[d, "\mu"'] \\
\mathbf{P'} & \mathcal{R} & \mathbf{Q'}
\end{tikzcd}
$$

$$
\stackrel{\hat{\mu}}{\Longrightarrow} := \left\{ \begin{array}{ll} \xrightarrow{\tau}^{*} \xrightarrow{\mu} \xrightarrow{\tau}^{*} & \text{if } \mu \neq \tau \\ \xrightarrow{\tau}^{*} & \text{if } \mu = \tau \end{array} \right\}
$$

weak transitions: τ is **invisible**

Bisimulations (weak)

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

$$\approx \; = \; \cup \mathcal{R}$$

$\approx$: bisimilarity

Bisimulations (weak)

Examples

$$X \approx \tau.X$$

$$\forall \mathbf{P},\ \mathbf{P} \approx \tau.\mathbf{P}$$

(not a constant: $\mathbf{K}_\tau := \tau.\mathbf{K}_\tau \xrightarrow{\tau}\xrightarrow{\tau}\xrightarrow{\tau} \ldots$)

Equations and unique solutions

Equations and unique solutions

$$X \approx \mathbf{E}[X]$$

Unique solutions:

If $\mathbf{P} \approx \mathbf{E}[\mathbf{P}]$ **and** $\mathbf{Q} \approx \mathbf{E}[\mathbf{Q}]$

Then $\mathbf{P} \approx \mathbf{Q}$

Equations and unique solutions

$$X \approx \mathbf{E}[X]$$

Example

$$X \approx a.\tau.X$$

Solutions $\approx a.a.a.a.a\ldots$

Equations and unique solutions

$$X \approx \mathbf{E}[X]$$

Unique solutions:

$$\textbf{If} \quad \mathbf{P} \approx \mathbf{E}[\mathbf{P}] \quad \textbf{and} \quad \mathbf{Q} \approx \mathbf{E}[\mathbf{Q}]$$

$$\textbf{Then } \mathbf{P} \approx \mathbf{Q}$$

Solutions:

- Consider the constant $\mathbf{K_E} \ := \ \mathbf{E}[\mathbf{K_E}]$
- $\mathbf{K_E} = \underbrace{\mathbf{E}[\mathbf{E}[\mathbf{E}[\mathbf{E}[\ldots]]]]}_{\mathbf{E}^{\infty}:\ \text{syntactic solution}}$ is always solution

Equations do not always have a unique solution

$\mathrm{X} \approx \mathrm{X}$ or $\mathrm{X} \approx \tau.\mathrm{X}$ do not have unique solutions:

$$\forall \mathbf{P}, \mathbf{P} \approx \tau.\mathbf{P}$$

Equations do not always have a unique solution

$\mathrm{X} \approx \mathrm{X}$ or $\mathrm{X} \approx \tau.\mathrm{X}$ do not have unique solutions:

$$\forall \mathbf{P}, \mathbf{P} \approx \tau.\mathbf{P}$$

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

$$\mathrm{X} \approx \mathrm{a}.\overline{\mathrm{b}}.\mathrm{X}$$

Unique solution: $\mathrm{a}.\overline{\mathrm{b}}.\mathrm{a}.\overline{\mathrm{b}}.\mathrm{a}\ldots$

Equations do not always have a unique solution

$X \approx X$ or $X \approx \tau.X$ do not have unique solutions:

$$\forall \mathbf{P}, \mathbf{P} \approx \tau.\mathbf{P}$$

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

$$X \approx a.\overline{b}.X$$

Unique solution: $a.\overline{b}.a.\overline{b}.a\ldots$

Is this enough?

Failure of unique solutions

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

$b.\mathbf{P}$ is a solution for any $\mathbf{P}$ (st $b \notin \mathrm{fn}(\mathbf{P})$)

Failure of unique solutions

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

$b.\mathbf{P}$ is a solution for any $\mathbf{P}$ (st $b \notin \mathrm{fn}(\mathbf{P})$)

$$\begin{array}{ccc}
b.\,\mathbf{P} & \approx & b.\, \boldsymbol{\nu} b\, (\, \overline{b} \mid b.\,\mathbf{P}\,) \\
\Big\downarrow{\scriptstyle b} & & \Big\downarrow{\scriptstyle b} \\
\mathbf{P} & \approx & \boldsymbol{\nu} b\, (\, \overline{b} \mid b.\,\mathbf{P}\,)
\end{array}$$

Failure of unique solutions

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

$b.\mathbf{P}$ is a solution for any $\mathbf{P}$ (st $b \notin \mathrm{fn}(\mathbf{P})$)

$$\begin{array}{ccccc}
b.\,\mathbf{P} & \approx & b.\, \nu b\, (\, \overline{b} \mid b.\,\mathbf{P}\,) & & \\
\big\downarrow{\scriptstyle b} & & \big\downarrow{\scriptstyle b} & & \\
\mathbf{P} & \approx & \nu b\, (\, \overline{b} \mid b.\,\mathbf{P}\,) & \equiv & \tau.\,\mathbf{P} \approx \mathbf{P}
\end{array}$$

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

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

A uniqueness result for divergence-free equations

Divergences and unique solutions

$$X \approx \tau.\ X$$

- $\mathbf{E}^{\infty} = \tau.\tau.\tau.\tau \ldots$

Divergences and unique solutions

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

- Solutions: $\forall \mathbf{P},\ \mathbf{P} \mid \overline{b}\ (\mid b.\overline{b})^{\omega}$
- $\mathbf{E}^{\infty} = \overline{b} \mid b.(\overline{b} \mid b.(\overline{b} \mid b \ldots)) \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\tau} \ldots$

Divergences and unique solutions

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

- Solutions: $\forall \mathbf{P}$, $\mathbf{P} \mid \overline{b}\ (\mid b.\overline{b})^{\omega}$
- $\mathbf{E}^{\infty} = \overline{b} \mid b.(\overline{b} \mid b.(\overline{b} \mid b \ldots)) \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\tau} \xrightarrow{\tau} \ldots$
- **Divergence:** infinite sequence of $\xrightarrow{\tau}$ transitions

Unique solutions for divergence free equations

Theorem (Unique solutions for divergence free equations)

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

- P has a divergence: $P \xrightarrow{\mu_1}\xrightarrow{\mu_2} \dots \xrightarrow{\mu_n} \xrightarrow{\tau}\xrightarrow{\tau} \dots \xrightarrow{\tau} \dots$
- **Syntactic solution** $E^\infty := E[E[E[\dots]]]$

Unique solution and context transitions

$$\mathbf{P} \quad \approx \quad \mathbf{E}\,[\mathbf{P}] \qquad\qquad \mathbf{E}\,[\mathbf{Q}] \quad \approx \quad \mathbf{Q}$$

$\mathbf{P}$ are $\mathbf{Q}$ solutions of $X \approx \mathbf{E}[X]$.
We show unique solution:

$$\mathbf{P} \approx \mathbf{Q}$$

Unique solution and context transitions

$$\begin{array}{ccccccc} \mathbf{P} & \approx & \mathbf{E}\,[\mathbf{P}] & \approx & \mathbf{E}\,[\mathbf{Q}] & \approx & \mathbf{Q} \\ \big\downarrow \mu & & & & & & \big\Downarrow \hat{\mu} \\ & & & \approx & & & \end{array}$$

Challenges of **P**

Unique solution and context transitions

$$\begin{tikzcd}
\mathbf{P} \arrow[d, "\mu"'] & \approx & \mathbf{E}\ [\mathbf{P}] \arrow[d, Rightarrow, "\hat{\mu}"'] & & \mathbf{E}\ [\mathbf{Q}] & \approx & \mathbf{Q} \\
{} & \approx & {} & & & &
\end{tikzcd}$$

Unique solution and context transitions

$$\begin{array}{ccccccccc} \mathbf{P} & \approx & \mathbf{E}\,[\mathbf{P}] & & & & \mathbf{E}\,[\mathbf{Q}] & \approx & \mathbf{Q} \\ \downarrow{\scriptstyle \mu} & & \Downarrow{\scriptstyle \hat{\mu}} & & & & & & \end{array}$$

This transition is a context transition of E:

Unique solution and context transitions

$$
\begin{tikzcd}
\mathbf{P} \arrow[d, "\mu"'] & \approx & E\,[\mathbf{P}] \arrow[d, Rightarrow, "\hat{\mu}"'] & & E\,[\mathbf{Q}] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & \mathbf{Q} \\
{} & & C'[\mathbf{P}] & & C'[\mathbf{Q}] & &
\end{tikzcd}
$$

This transition is a context transition of E:

$E[\mathbf{Q}]$ can match it;

Unique solution and context transitions

$$\begin{tikzcd} \mathbf{P} \arrow[d, "\mu"'] & \approx & \mathbf{E}\,[\mathbf{P}] \arrow[d, Rightarrow, "\hat{\mu}"'] & & \mathbf{E}\,[\mathbf{Q}] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & \mathbf{Q} \arrow[d, Rightarrow, "\hat{\mu}"'] \\ {} & \approx & C'[\mathbf{P}] & & C'[\mathbf{Q}] & \approx & {} \end{tikzcd}$$

This transition is a context transition of E:

$\mathbf{E}[\mathbf{Q}]$ can match it;

$\mathbf{Q}$ too.

Unique solution and context transitions

$$
\begin{tikzcd}
C[\mathbf{P}] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & C[\mathbf{E}\ [\mathbf{P}]] \arrow[d, Rightarrow, "\hat{\mu}"'] & & C[\mathbf{E}\ [\mathbf{Q}]] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & C[\mathbf{Q}] \arrow[d, Rightarrow, "\hat{\mu}"'] \\
 & \approx & C'[\mathbf{P}] & & C'[\mathbf{Q}] & \approx &
\end{tikzcd}
$$

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:**
$$C[\cdot] \xrightarrow{\mu} C'[\cdot] \text{ if } \forall \mathbf{P},\ C[\mathbf{P}] \xrightarrow{\mu} C'[\mathbf{P}]$$
- General notion, independent of the language
- Related to guardedness in CCS
(guarded context $\Rightarrow$ context transition)

Unique solution and context transitions

$$
\begin{tikzcd}
\mathbf{P} \arrow[d, "\mu"'] & \approx & \mathbf{E}^{n}[\mathbf{P}] \arrow[d, Rightarrow, "\hat{\mu}"'] & & \mathbf{E}^{n}[\mathbf{Q}] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & \mathbf{Q} \arrow[d, Rightarrow, "\hat{\mu}"'] \\
{} & \approx & C'[\mathbf{P}] & & C'[\mathbf{Q}] & \approx & {}
\end{tikzcd}
$$

$\mathbf{P}$ is also solution of $\mathrm{X} \approx \mathbf{E}^{n}[\mathrm{X}]$

Unique solution and context transitions

$$
\begin{tikzcd}
C[\mathbf{P}] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & C[\mathbf{E}^n[\mathbf{P}]] \arrow[d, Rightarrow, "\hat{\mu}"'] & & C[\mathbf{E}^n[\mathbf{Q}]] \arrow[d, Rightarrow, "\hat{\mu}"'] & \approx & C[\mathbf{Q}] \arrow[d, Rightarrow, "\hat{\mu}"'] \\
 & \approx & C'[\mathbf{P}] & & C'[\mathbf{Q}] & \approx &
\end{tikzcd}
$$

Unique solution if any transition of $C[\mathbf{P}]$ can be matched by a $C[\mathbf{E}^n[\cdot]]$:

'$\mathbf{E}[\cdot]$ protects its solutions'

A divergence-free equation protects its solutions

$$
\begin{tikzcd}
C[\mathbf{P}] \arrow[d, Rightarrow, "\mathtt{a}"'] \arrow[r, phantom, "\approx"] & C[\mathbf{E}[\mathbf{P}]] \arrow[d, Rightarrow, "\mathtt{a}"'] \\
\mathbf{P}' \arrow[r, phantom, "\approx"] & \mathbf{T}_1
\end{tikzcd}
$$

A divergence-free equation protects its solutions

$$\begin{tikzcd} C[\mathbf{P}] \arrow[r, phantom, "\approx"] \arrow[d, Rightarrow, "a"'] & C[\mathbf{E}[\mathbf{P}]] \arrow[d, Rightarrow, "a"'] \\ \mathbf{P}' \arrow[r, phantom, "\approx"] & \mathbf{T}_1 \end{tikzcd}$$

$\mathbf{E}[\cdot]$ is guarded

A divergence-free equation protects its solutions

$$\begin{tikzcd} C[\mathbf{P}] \arrow[d, Rightarrow, "\mathtt{a}"'] & \approx & C[\mathbf{E}[\mathbf{P}]] \arrow[d, Rightarrow, "\mathtt{a}"'] & \approx & C[\mathbf{E}^2[\mathbf{P}]] \\ \mathbf{P}' & \approx & \mathbf{T}_1 & & \end{tikzcd}$$

A divergence-free equation protects its solutions

$$\begin{tikzcd}
C[\mathbf{P}] \arrow[d, Rightarrow, "\mathtt{a}"'] & \approx & C[\mathbf{E}[\mathbf{P}]] \arrow[d, Rightarrow, "\mathtt{a}"'] & \approx & C[\mathbf{E}^2[\mathbf{P}]] \arrow[d, Rightarrow, "\mathtt{a}"'] \\
\mathbf{P}' & \approx & \mathbf{T}_1 & \approx & \mathbf{T}_2
\end{tikzcd}$$

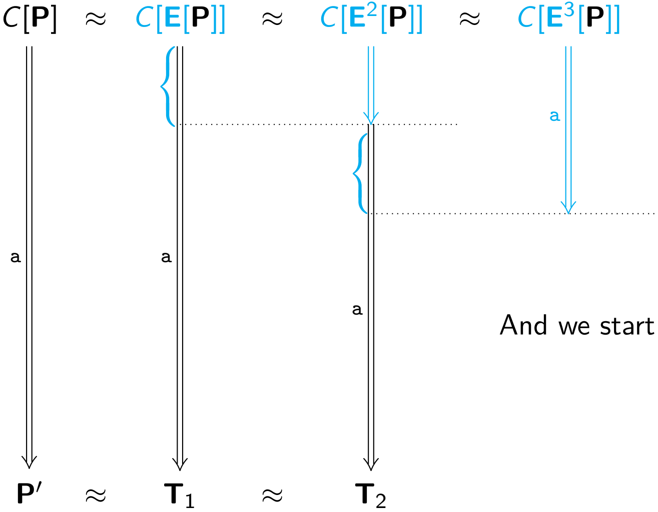
We complete by bisimilarity

A divergence-free equation protects its solutions

$$\begin{array}{ccccc} C[\mathbf{P}] & \approx & C[\mathbf{E}[\mathbf{P}]] & \approx & C[\mathbf{E}^2[\mathbf{P}]] \\ \Big\Downarrow \mathtt{a} & & \Big\Downarrow \mathtt{a} & & \Big\Downarrow \mathtt{a} \\ \mathbf{P}' & \approx & \mathbf{T}_1 & \approx & \mathbf{T}_2 \end{array}$$

And we start again. . .

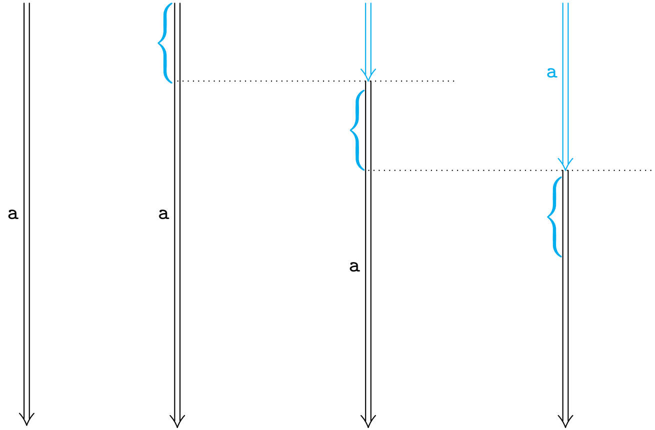
A divergence-free equation protects its solutions



And we start again. . .

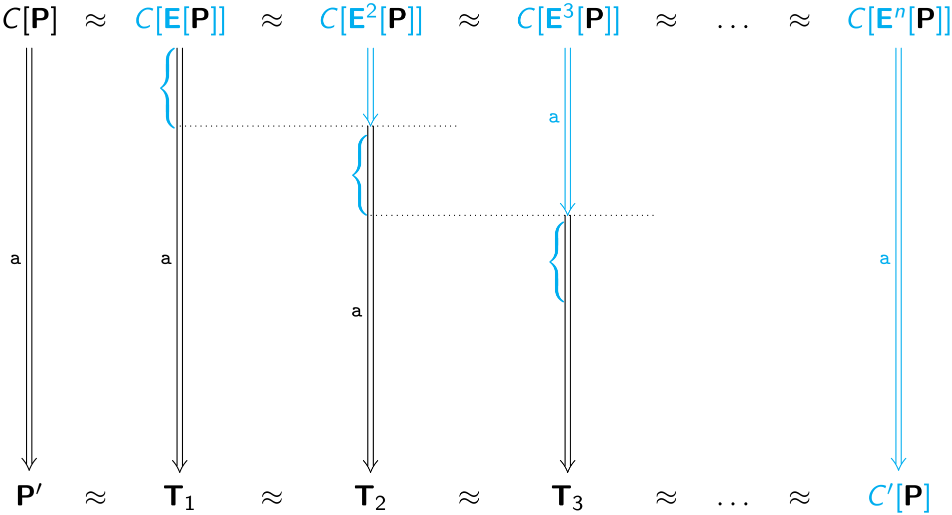
A divergence-free equation protects its solutions

$$C[\mathbf{P}] \quad \approx \quad C[\mathbf{E}[\mathbf{P}]] \quad \approx \quad C[\mathbf{E}^2[\mathbf{P}]] \quad \approx \quad C[\mathbf{E}^3[\mathbf{P}]] \quad \approx \quad \ldots$$



$$\mathbf{P}' \quad \approx \quad \mathbf{T}_1 \quad \approx \quad \mathbf{T}_2 \quad \approx \quad \mathbf{T}_3 \quad \approx \quad \ldots$$

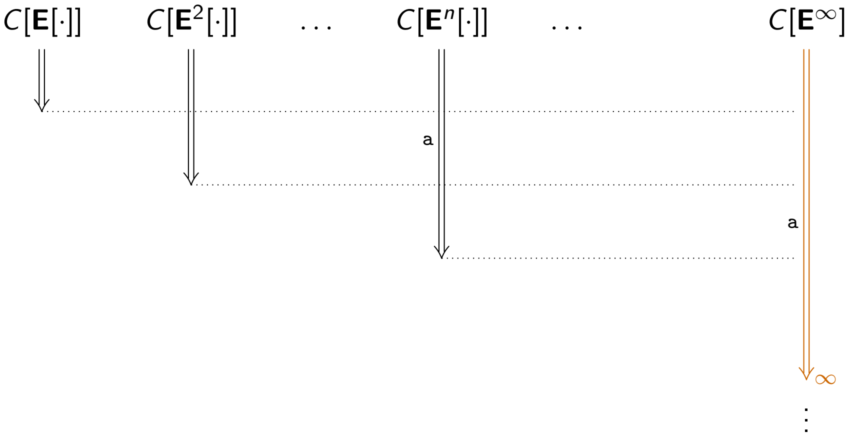
A divergence-free equation protects its solutions



Limit

If the construction never stops:

$\Rightarrow$ **divergence of $\mathbf{E}^\infty$**



A theorem for unique solutions

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

Theorem

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

Generalization

Generalization

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

- What we need:
  - **Context transitions**
    $$c \xrightarrow{\mu} c' \Leftrightarrow \forall x, c(x) \xrightarrow{\mu} c'(x)$$
  - **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 π-calculus, trace equivalence, behavioral preorders...

Generalization

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

- What we need:
  - **Context transitions**
    $$c \xrightarrow{\mu} c' \Leftrightarrow \forall x, c(x) \xrightarrow{\mu} c'(x)$$
  - **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 π-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