

Compositional Proofs about HOcore

Second Bachelor Seminar Talk

Lukas Convent

Advisor: Tobias Tebbi

Supervisor: Prof. Dr. Gert Smolka



May 13, 2016

HOcore: Processes and Transitions

Processes

$$P, Q ::= \bar{a}\langle P \rangle \mid a.P \mid n \in \mathbb{N} \mid P \parallel Q \mid \emptyset$$

$$\text{OUT} \quad \frac{}{\bar{a}\langle P \rangle \xrightarrow{\bar{a}\langle P \rangle} \emptyset}$$

$$\text{PAROUTL} \quad \frac{P \xrightarrow{\bar{a}\langle R \rangle} P'}{P \parallel Q \xrightarrow{\bar{a}\langle R \rangle} P' \parallel Q}$$

$$\text{IN} \quad \frac{}{a.P \xrightarrow{a} P}$$

$$\text{PARINL} \quad \frac{P \xrightarrow{a} P'}{P \parallel Q \xrightarrow{a} P' \parallel Q[\uparrow]}$$

$$\text{SYNL} \quad \frac{P \xrightarrow{\bar{a}\langle R \rangle} P' \quad Q \xrightarrow{a} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'[R :: id]}$$

$$\text{PARTAUL} \quad \frac{P \xrightarrow{\tau} P}{P \parallel Q \xrightarrow{\tau} P' \parallel Q}$$

$$\text{REM} \quad \frac{}{n \xrightarrow{n} \emptyset}$$

$$\text{PARREML} \quad \frac{P \xrightarrow{n} P'}{P \parallel Q \xrightarrow{n} P' \parallel Q}$$

Bisimilarity

Bisimulation

Bisimulation $\mathcal{R} : \Leftrightarrow$



Bisimilarity

$P \sim Q : \Leftrightarrow$

$\exists \text{ Bisimulation } \mathcal{R}. (P, Q) \in \mathcal{R}$

Bisimilarity is a co-inductive notion. We can characterize it by a monotone functional:

$$b \in (Pr \times Pr)^2$$

$$b(\mathcal{R}) = \{(P, Q) \mid \forall Q'. Q \rightarrow Q' \wedge P' \mathcal{R} Q' \wedge \exists P'. P \rightarrow P' \wedge P' \mathcal{R} Q'\}$$



Bisimulation as a Post-Fixed-Point

Bisimulation $\mathcal{R} : \Leftrightarrow \mathcal{R} \subseteq b(\mathcal{R})$

Bisimilarity as the Greatest Fixed-Point

$\sim := \nu(b) \stackrel{\text{Tarski}}{=} \bigcup \{\mathcal{R} \mid \text{Bisimulation } \mathcal{R}\}$

Previous work

-  Lanese, Pérez, Sangiorgi, Schmitt: **On the Expressiveness and Decidability of Higher-Order Process Calculi.**
LICS 2008
-  Maksimovi, Schmitt: **HOCore in Coq.**
Interactive Theorem Proving, Vol. 9236, 2015

Underlying framework:

-  Pous: **Complete Lattices and Up-To Techniques.**
LICS, Vol. 4807, 2007

From Simulation to Bisimulation

- Define **bisimulation** in terms of **simulation**:

$$s \in (Pr \times Pr)^2$$

$$s(\mathcal{R}) = \{(P, Q) \mid \exists Q'. Q \xrightarrow{\forall P'. P \rightarrow P' \Rightarrow} Q' \wedge P' \mathcal{R} Q'\}$$

- Notation:

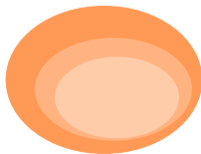
$$\text{Transposition:} \quad \bar{s}(\mathcal{R}) := \overline{s(\overline{\mathcal{R}})}$$

$$\text{Symmetrization:} \quad \overleftrightarrow{s}(\mathcal{R}) := s(\mathcal{R}) \cap \bar{s}(\mathcal{R})$$

- \mathcal{R} is 2-simulation $\Leftrightarrow \mathcal{R} \subseteq s(\mathcal{R}) \wedge \mathcal{R} \subseteq \bar{s}(\mathcal{R})$

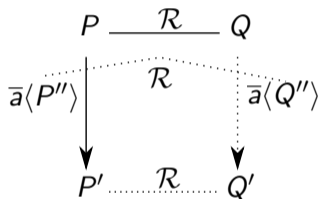
- \mathcal{R} is bisimulation $\Leftrightarrow \mathcal{R} \subseteq \overleftrightarrow{s}(\mathcal{R})$

- \mathcal{R} is sym. bisimulation $\Leftrightarrow \mathcal{R}$ symmetric $\wedge \mathcal{R} \subseteq s(\mathcal{R})$



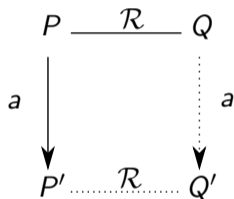
IO Bisimilarity

\mathcal{R} is an **IO Bisimulation** if the following properties (+ their transpositions) hold:



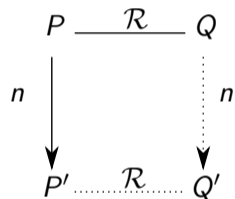
HO **Output** Simulation

S_{ho_out}



HO **Input** Simulation

S_{ho_in}



Variable Simulation

S_{var}

Compositional Proofs

We **define** IO bisimilarity through a **compositional** functional:

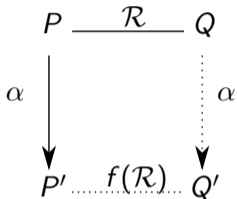
$$\begin{aligned} \overleftrightarrow{S}_{io} &= \overleftarrow{S_{ho_out}} \cap S_{ho_in} \cap \overrightarrow{S_{var}} \\ &= S_{ho_out} \cap S_{ho_in} \cap S_{var} \cap \overline{S_{ho_out}} \cap \overline{S_{ho_in}} \cap \overline{S_{var}} \quad \Rightarrow \quad \sim_{io} = \nu(\overleftrightarrow{S}_{io}) \end{aligned}$$

We want to **reason** about such a bisimilarity by **using its compositional structure**:

- Bisimulation-up-to-bisimilarity technique is correct (Revisited with new framework)
- Congruence of IO bisimilarity

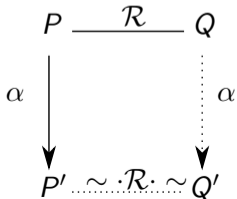
Up-to Relations (1)

\mathcal{R} is a **simulation-up-to-f** if:



$$\Leftrightarrow \mathcal{R} \subseteq s(f(\mathcal{R})) \Leftrightarrow \mathcal{R} \text{ is a Post-Fixed-Point of } s \circ f$$

We have seen the notion of **simulation-up-to-bisimilarity**:



$$\Leftrightarrow \mathcal{R} \subseteq s(\sim \cdot \mathcal{R} \cdot \sim)$$

Here, f is instantiated like this: $f(\mathcal{A}) := \sim \cdot \mathcal{A} \cdot \sim$

Up-to Relations (2)

s-correct functions:

$$\nu(s \circ f) = \nu(s)$$

s-compatible functions:

$$f \circ s \subseteq s \circ f$$

We have seen:

up-to-bisimilarity: $f(\mathcal{A}) = \sim \cdot \mathcal{A} \cdot \sim$

Compatible Functions

Compatibility implies Correctness

Let f be s -compatible: $f \circ s \subseteq s \circ f$ Then f is s -correct: $\nu(s \circ f) \subseteq \nu(s)$.

Compatible functions enjoy nice closure properties. They are closed under

- **Funct. comp.:** If f_1 and f_2 are both s -compatible, then $f_1 \circ f_2$ is s -compatible
- **Intersection:** If f is both s_1 - and s_2 -compatible, then f is $s_1 \cap s_2$ -compatible
- **Union, Transposition**

Congruence of IO Bisimilarity (1)

Congruence of IO Bisimilarity

If $P \sim_{io} Q$, then also

$$1. \bar{a}\langle P \rangle \sim_{io} \bar{a}\langle Q \rangle$$

$$2. a.P \sim_{io} a.Q$$

$$3. P \parallel R \sim_{io} Q \parallel R$$

- Establish congruence in a modular way
- For each operator, we define a corresponding closure:

$$C_{send}(\mathcal{R}) := \{(\bar{a}\langle P \rangle, \bar{a}\langle Q \rangle) \mid (P, Q) \in \mathcal{R}\} \sqcup id$$

$$C_{receive}(\mathcal{R}) := \{(a.P, a.Q) \mid (P, Q) \in \mathcal{R}\}$$

$$C_{par}(\mathcal{R}) := \{(P \parallel R, Q \parallel R) \mid (P, Q) \in \mathcal{R}\} \sqcup id$$

To show: \sim_{io} is closed under each C : $C(\sim_{io}) \subseteq \sim_{io}$

Congruence of IO Bisimilarity (2)

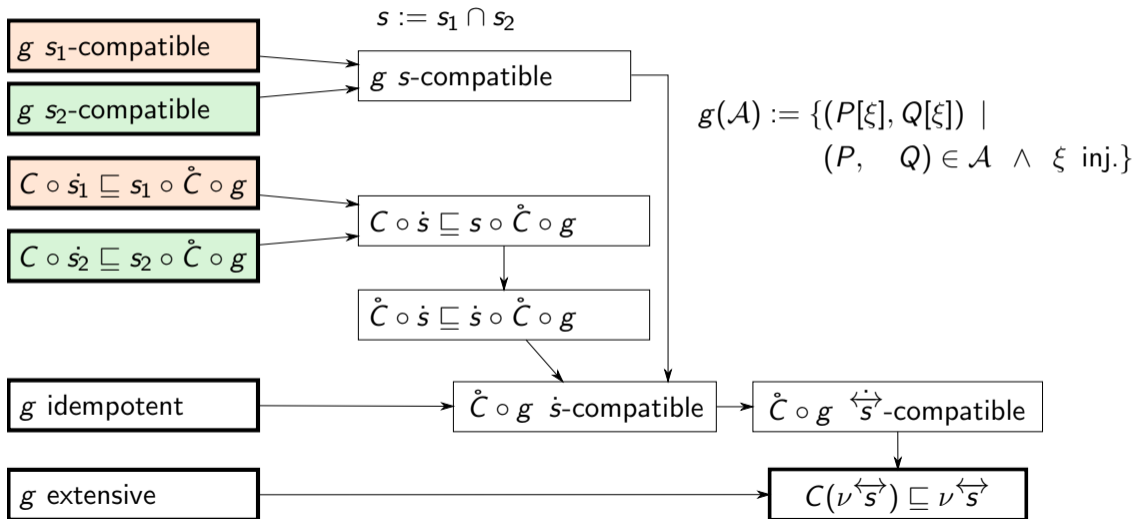
To show: \sim_{io} is closed under each C : $C(\sim_{io}) \subseteq \sim_{io}$

Compatibility implies Congruence

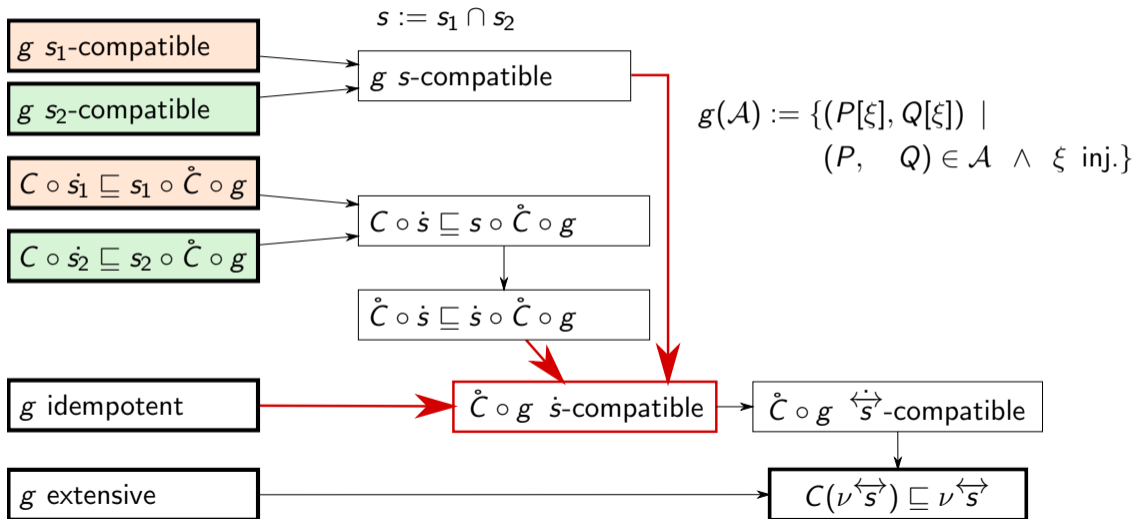
If C is s -compatible, then $C(\nu s) \subseteq \nu s$

- It would suffice to show that each C is $\overset{\leftarrow}{s}_{io}\overset{\rightarrow}{}$ -compatible:
 \Rightarrow Show for each C , each s_x : $C \circ s_x \subseteq s_x \circ C$
- Because of $[\uparrow]$ in PARIN transition, this **condition is too strong**
- Instead, we show **weaker condition**, using *closure under injective renamings* (g):
 $C \circ \dot{s} \subseteq s \circ \dot{C} \circ g$
- Notation: $\dot{f}(x) := f(x) \sqcap x$ $\mathring{f}(x) := f(x) \sqcup x$

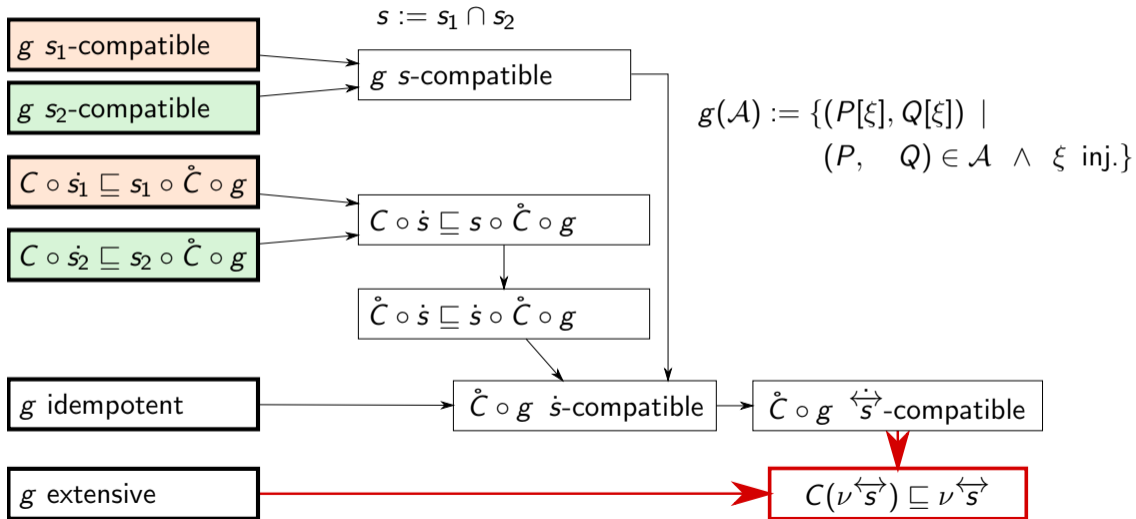
Congruence of IO Bisimilarity (3)



Congruence of IO Bisimilarity (3)



Congruence of IO Bisimilarity (3)








Conclusion & Outlook

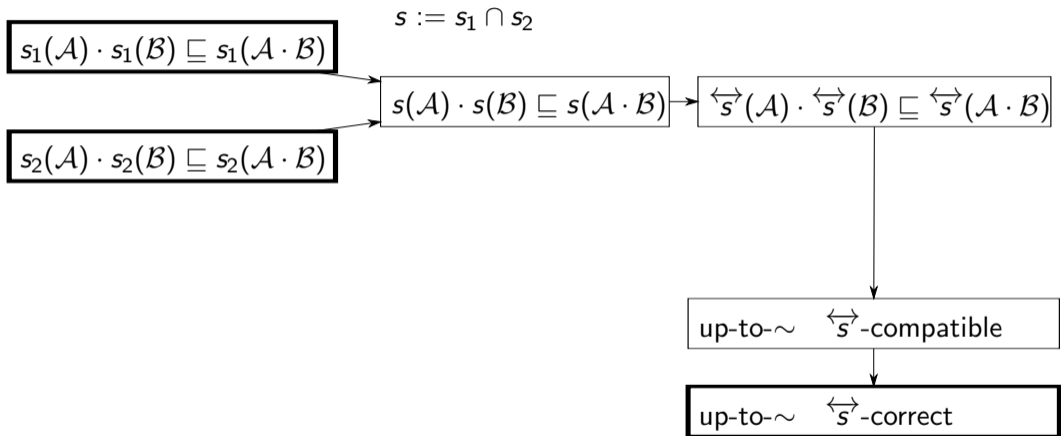
- Bisimilarity for HOcore is stated compositionally
- This can be used for compositional proofs:
 - Advantage: Small proofs for single components
 - Disadvantage: Possibly overly generalized machinery
- Next steps:
 - Substitutivity for \sim_{io} : $P \sim_{io} Q \Rightarrow P[\sigma] \sim_{io} Q[\sigma]$
 - $\sim_{\tau} \subseteq \sim_{io}$

Thank you!

References

-  Lanese, Pérez, Sangiorgi, Schmitt: **On the Expressiveness and Decidability of Higher-Order Process Calculi.**
LICS 2008
-  Pérez: <http://www.cs.unibo.it/~perez/talks/coplas.pdf>
-  Maksimovi, Schmitt: **HOCore in Coq.**
Interactive Theorem Proving, Vol. 9236, 2015
-  Sangiorgi: Presentation on **Bisimulation and Coinduction:**
<http://www.fing.edu.uy/inco/eventos/SEFM2011/cursos/Davide.pdf>
-  Pous: **Complete Lattices and Up-To Techniques.**
LICS, Vol. 4807, 2007

Bisimulation-up-to-Bisimilarity (1)



Bisimulation-up-to-Bisimilarity (2)

$$\overleftarrow{s}(\mathcal{A}) \cdot \overleftarrow{s}(\mathcal{B}) \sqsubseteq \overleftarrow{s}(\mathcal{A} \cdot \mathcal{B})$$

- \overleftarrow{s} -compatibility is closed under relation composition
 $f_1, f_2 \overleftarrow{s}$ -compatible $\Rightarrow f(\mathcal{A}) = f_1(\mathcal{A}) \cdot f_2(\mathcal{A}) \overleftarrow{s}$ -compatible
- $\lambda \mathcal{R}. \mathcal{R} \overleftarrow{s}$ -compatible
- For any post-fixed-point \mathcal{A} of \overleftarrow{s} ,
 $\lambda \mathcal{R}. \mathcal{A} \overleftarrow{s}$ -compatible
- \sim is a post-fixed-point of \overleftarrow{s}

up-to- $\sim \overleftarrow{s}$ -compatible

up-to- $\sim(\mathcal{R}) := \sim \cdot \mathcal{R} \cdot \sim$