Compositional and Nameless Formalization of HOcore

Final Bachelor Talk

Lukas Convent

Advisor: Tobias Tebbi

Supervisor: Prof. Dr. Gert Smolka

SAARLAND UNIVERSITY

COMPUTER SCIENCE

Programming Systems

July 29, 2016

Overview

1. HOcore process calculus
2. Compositional properties
3. How to prove them
4. Application to HOcore

5. Contributions & Conclusions

HOcore: Processes and Transitions

Processes

$$P, Q \quad ::= \quad \overline{a}\langle P \rangle \quad | \quad a.P \quad | \quad n \in \mathbb{N} \quad | \quad P \parallel Q \quad | \quad \emptyset$$

$$\textsc{Out} \quad \frac{}{\overline{a}\langle P \rangle \xrightarrow{\overline{a}\langle P \rangle} \emptyset}$$

$$\textsc{ParOutL} \quad \frac{P \xrightarrow{\overline{a}\langle R \rangle} P'}{P \parallel Q \xrightarrow{\overline{a}\langle R \rangle} P' \parallel Q}$$

$$\textsc{In} \quad \frac{}{a.P \xrightarrow{a} P}$$

$$\textsc{ParInL} \quad \frac{P \xrightarrow{a} P'}{P \parallel Q \xrightarrow{a} P' \parallel Q[\uparrow]}$$

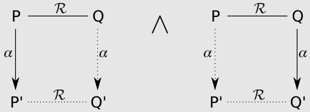
$$\textsc{SynL} \quad \frac{P \xrightarrow{\overline{a}\langle R \rangle} P' \qquad Q \xrightarrow{a} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'[R :: id]}$$

$$\textsc{ParTauL} \quad \frac{P \xrightarrow{\tau} P}{P \parallel Q \xrightarrow{\tau} P' \parallel Q}$$

Bisimilarity

Bisimulation

Bisimulation $\mathcal{R}$ $:\Leftrightarrow$



Bisimilarity

$P \sim Q :\Leftrightarrow$

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

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

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

$$b(\mathcal{R}) = \{(P, Q) \mid \begin{array}{c}\forall P'.P \longrightarrow P' \Rightarrow \\ \exists Q'.Q \longrightarrow Q' \wedge P'\ \mathcal{R}\ Q'\end{array} \bigwedge \begin{array}{c}\forall Q'.Q \longrightarrow Q' \Rightarrow \\ \exists P'.P \longrightarrow P' \wedge P'\ \mathcal{R}\ Q'\end{array}\}$$

Bisimulation as a Post-Fixed-Point

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

Bisimilarity as the Greatest Fixed-Point

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

From Simulation to Bisimulation

- **Simulation** functional:

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

$$s(\mathcal{R}) = \{(P, Q) \mid \begin{array}{l} \forall P'.P \longrightarrow P' \Rightarrow \\ \exists Q'.Q \longrightarrow Q' \wedge P' \; \mathcal{R} \; Q' \end{array}\}$$

- Notation:

$$\textit{Transposition:} \qquad \overline{s}(\mathcal{R}) := \overline{s(\overline{\mathcal{R}})}$$

$$\textit{Symmetrization:} \qquad \overleftrightarrow{s}(\mathcal{R}) := s(\mathcal{R}) \cap \overline{s}(\mathcal{R})$$

- **Compositional bisimulation** functional:

$$\overleftrightarrow{s} := \overleftrightarrow{s_1 \cap s_2 \cap s_3}$$

$$= s_1 \cap s_2 \cap s_3 \cap \overline{s_1} \cap \overline{s_2} \cap \overline{s_3}$$

Previous work

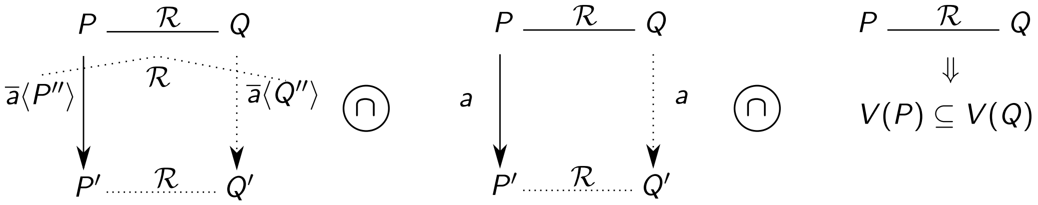
- Lanese, Pérez, Sangiorgi, Schmitt: **On the Expressiveness and Decidability of Higher-Order Process Calculi**.
  LICS 2008
- Maksimovic, Schmitt: **HOCore in Coq**.
  Interactive Theorem Proving, Vol. 9236, 2015

Underlying framework:

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

IO Bisimilarity

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



HO output sim.

s_{ho_out}

HO input sim.

s_{ho_in}

Variable multiset sim.

s_{var_multi}

Unguarded Variable

A variable occurrence is **unguarded** in a process if it is not prefixed and not contained in an output process. $V(P) :=$ *multiset of unguarded variable occurrences*

Proofs about Bisimilarity

Correctness of **up-to techniques**

- A monotone function f is an s-correct up-to technique if $\nu(s \circ f) \subseteq \nu s$
- Instead of $\mathcal{R} \subseteq s(\mathcal{R})$
  ... prove $\mathcal{R} \subseteq s(f(\mathcal{R}))$

Closure properties

- Many properties are closure properties: Substitutivity, congruence, ...: $f(\nu s) \subseteq \nu s$

Problem: These properties are not composable:

- For a functional $s = s_1 \cap s_2$,

$$\begin{array}{l} \nu(s_1 \circ f) \subseteq \nu s_1 \\ \nu(s_2 \circ f) \subseteq \nu s_2 \end{array} \not\Rightarrow \nu(s \circ f) \subseteq \nu s$$

- **Solution**: *Compatibility* criterion

- For a functional $s = s_1 \cap s_2$,

$$\begin{array}{l} f(\nu s_1) \subseteq \nu s_1 \\ f(\nu s_2) \subseteq \nu s_2 \end{array} \not\Rightarrow f(\nu s) \subseteq \nu s$$

- **Solution**: *Closedness* criterion

Compatible Up-to Techniques

Definition

A monotone function f is **s-compatible** if $\dfrac{\mathcal{R} \subseteq s(\mathcal{S})}{f(\mathcal{R}) \subseteq s(f(\mathcal{S}))}$ $(\Leftrightarrow \quad f \circ s \subseteq s \circ f)$

Lemma

f is s-compatible $\quad \Rightarrow \quad f$ is s-correct, i.e. $\nu(s \circ f) \subseteq \nu s$

$$\frac{f \ s\text{-compatible} \quad g \ s\text{-compatible}}{(f \circ g) \ s\text{-compatible}}$$

$$\frac{f_1 \ s\text{-compatible} \quad f_2 \ s\text{-compatible}}{(f_1 \cup f_2) \ s\text{-compatible}} \qquad \frac{f \ s_1\text{-compatible} \quad f \ s_2\text{-compatible}}{f \ (s_1 \cap s_2)\text{-compatible}}$$

$$\frac{f \ s\text{-compatible}}{\overline{f} \ \overline{s}\text{-compatible}} \qquad \frac{f \ \text{symmetric} \quad f \ s\text{-compatible}}{f \ \overleftrightarrow{s}\text{-compatible}}$$

Closure properties of Bisimilarity

Definition

A monotone function f is **s-compatible** if $\dfrac{\mathcal{R} \subseteq s(\mathcal{S})}{f(\mathcal{R}) \subseteq s(f(\mathcal{S}))}$

- Given a function f, we want to show $f(\nu s) \subseteq \nu s$
- E.g., $f_{subst}(\mathcal{R}) := \{(A[\sigma], B[\sigma]) \mid (A, B) \in \mathcal{R},\ \sigma \text{ substitution}\}$

Lemma

$$f \text{ is } s\text{-compatible} \quad \Rightarrow \quad f(\nu s) \subseteq \nu s$$

- But we cannot show f_{subst} s_{ho_out}-compatible
- Closedness only if νs is at **least** *reflexive* and at **most** a *variable context sim.*

Explanation comes in a minute!

Conditional Closedness (1)

Based on compatibility, we introduce a new criterion for showing closedness:

Conditional Closedness

A functional s is conditionally f-closed **above g_1** and **below g_2** (f-closed$^{g_2}_{g_1}$) if

$$\frac{g_1(\mathcal{R}) \subseteq \mathcal{R} \qquad g_2(\mathcal{R}) \supseteq \mathcal{R} \qquad \mathcal{R} \subseteq s(\mathcal{R})}{f(\mathcal{R}) \subseteq s(f(\mathcal{R}))}$$

Lemma

$$\begin{array}{l} s \text{ is } f\text{-closed}^{g_2}_{g_1} \\ g_1(\nu s) \subseteq \nu s \\ g_2(\nu s) \supseteq \nu s \end{array} \quad \Rightarrow \quad f(\nu s) \subseteq \nu s$$

Conditional Closedness (2)

Based on compatibility, we introduce a new criterion for showing closedness:

Conditional Closedness

A functional s is conditionally f-closed **above g_1** and **below g_2** (f-closed$_{g_1}^{g_2}$) if

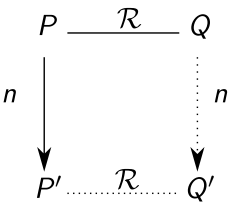
$$\frac{g_1(\mathcal{R}) \subseteq \mathcal{R} \qquad g_2(\mathcal{R}) \supseteq \mathcal{R} \qquad \mathcal{R} \subseteq s(\mathcal{R})}{f(\mathcal{R}) \subseteq s(f(\mathcal{R}))}$$

Has very similar closure properties: $$\frac{s_1 \ f\text{-closed}_{g_1}^{g_2} \qquad s_2 \ f\text{-closed}_{g_1}^{g_2}}{(s_1 \cap s_2) \ \text{f-closed}_{g_1}^{g_2}}$$ [...]

Dealing with Unguarded Variables

Different approaches on how to require that P and Q have same unguarded variables:

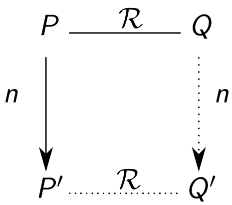
[Maksimovic et al., 2015]



$$\textsc{Rem}\ \frac{}{n \xrightarrow{n} \emptyset}$$

$$\textsc{RemL}\ \frac{P \xrightarrow{n} P'}{P \parallel Q \xrightarrow{n} P' \parallel Q}$$

Producing contexts $\mathbf{s_{var\_cxt}}$



$$\textsc{Cxt}\ \frac{}{n \xrightarrow{n} 0}$$

$$\textsc{CxtL}\ \frac{P \xrightarrow{n} P'}{P \parallel Q \xrightarrow{n} P' \parallel Q[\uparrow]}$$

$\nu s_{io} \subseteq s_{var\_cxt}(\nu s_{io})$

Multiset incl. $\mathbf{s_{var\_multi}}$

$$P \ \mathcal{R}\ Q$$

$$\Downarrow$$

$$V(P) \subseteq V(Q)$$

$V(P) :=$ multiset of unguarded variable occurrences

Part of s_{io}

Substituted processes

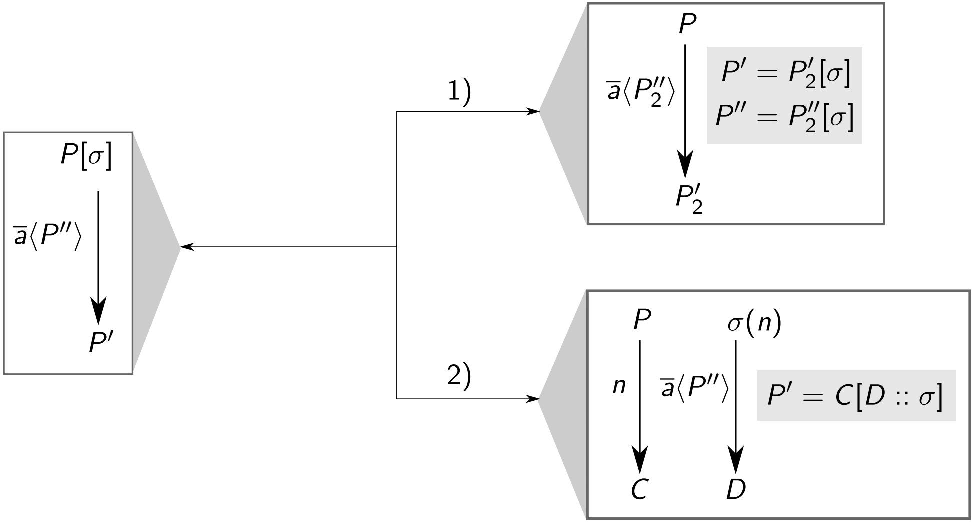
Lemma

Transitions are **substitutive**:
$$\frac{P \xrightarrow{\overline{a}\langle Q\rangle} P'}{P[\sigma] \xrightarrow{\overline{a}\langle Q[\sigma]\rangle} P'[\sigma]}$$

Lemma

Transitions **propagate** through substitutions:
$$\frac{P \xrightarrow{n} C \qquad \sigma(n) \xrightarrow{\overline{a}\langle Q\rangle} D}{P[\sigma] \xrightarrow{\overline{a}\langle Q\rangle} C[D :: \sigma]}$$

Substituted Processes: Analysis Lemma



Using Contexts: Proving Substitutivity

Conditional Closedness

A functional s is f-closed$^{g_2}_{g_1}$ if

$$\frac{g_1(\mathcal{R}) \subseteq \mathcal{R} \qquad g_2(\mathcal{R}) \supseteq \mathcal{R} \qquad \mathcal{R} \subseteq s(\mathcal{R})}{f(\mathcal{R}) \subseteq s(f(\mathcal{R}))}$$

- $f_{subst}(\mathcal{R}) := \{(A[\sigma], B[\sigma]) \mid (A, B) \in \mathcal{R},\ \sigma \text{ substitution}\}$

We prove:

- s_{ho_out} is f_{subst}-closed$^{sVarCxt}_{f_{refl}}$
- s_{ho_in} is f_{subst}-closed^{sVarCxt}
- s_{ho_out} is f_{subst}-closed

Congruence of IO Bisimilarity (1)

Congruence of IO Bisimilarity

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

1. $\overline{a}\langle P \rangle \sim_{io} \overline{a}\langle Q \rangle$
2. $a.P \sim_{io} a.Q$
3. $P \parallel R \sim_{io} Q \parallel R$

- For each operator, we define a corresponding closure:

$$
\begin{aligned}
f_{send}(\mathcal{R}) &:= \{(\overline{a}\langle P \rangle, \overline{a}\langle Q \rangle) &&\mid (P, Q) \in \mathcal{R}\} \\
f_{receive}(\mathcal{R}) &:= \{(a.P, a.Q) &&\mid (P, Q) \in \mathcal{R}\} \\
f_{par}(\mathcal{R}) &:= \{(P \parallel R, Q \parallel R) &&\mid (P, Q) \in \mathcal{R}\}
\end{aligned}
$$

Congruence of IO Bisimilarity (2)

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

It suffices to show $\quad \mathring{f}(\sim_{io}) \subseteq \sim_{io} \quad$ with $\mathring{f} := f \cup id$

$$\frac{\begin{array}{ll}\mathring{f}_{send} & s_{ho\_out}\text{-}compat_{f_{refl}} \\ \mathring{f}_{send} & s_{ho\_in}\text{-}compat \\ \mathring{f}_{send} & s_{var\_multi}\text{-}compat\end{array}}{\mathring{f}_{send}(\nu b_{io}) \subseteq \nu b_{io}} \qquad \frac{\begin{array}{ll}\mathring{f}_{receive} & s_{ho\_out}\text{-}compat \\ \mathring{f}_{receive} & s_{ho\_in}\text{-}compat \\ \mathring{f}_{receive} & s_{var\_multi}\text{-}compat\end{array}}{\mathring{f}_{receive}(\nu b_{io}) \subseteq \nu b_{io}} \qquad \frac{\begin{array}{ll}\mathring{f}_{par} & s_{ho\_out}\text{-}compat \\ \mathring{f}_{par} & s_{ho\_in}\text{-}compat_{f_{subst}} \\ \mathring{f}_{par} & s_{var\_multi}\text{-}compat_{f_{subst}}\end{array}}{\mathring{f}_{par}(\nu b_{io}) \subseteq \nu b_{io}}$$

Contributions

- Conditional closedness as a compositional criterion
- Variable context simulations
- Application of complete lattice theory (Pous) to HOcore (Lanese et al.)

Conclusion

- Bisimilarity for HOcore is defined compositionally
- Can be used for compositional proofs of up-to techniques:
  - *Advantage*: Small separate proofs
  - *Disadvantage*: Only if components are independent
- Conditional closedness can be used for dependent components
  - *Advantage*: Small separate proofs, clear dependencies
  - *Disadvantage*: Only for closure properties, not for up-to techniques
- All presented results formalized in Coq

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*
- Maksimovic, 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