Structural Rewriting in the π-Calculus

David Sabel

Goethe-University, Frankfurt, Germany

WPTE'14, Vienna, Austria

Introduction

- the π-**calculus** (R. Milner, J. Parrow & D. Walker, 1992) is a core language for **mobile concurrent processes**
- it is a minimalistic model for **concurrent programming languages**
- lot of applications and variants exist:
  - Spi-calculus (cryptographic protocols)
  - modelling of business processes,
  - stochastic pi-calculus (biochemical processes),
  - join-calculus (distributed programming)
  - ...
- all these applications need reasoning tools for **process equivalence**
- lot of process equivalence notions are based on the **operational semantics** of π-processes

Evaluation of π-processes: **Reduction semantics**

- reduction relation on processes for interaction of processes
- closure by **structural congruence** used **implicitly**

Structural congruence

- "natural" conversions, e.g. $P_1 \mid (P_2 \mid P_3) \equiv (P_2 \mid P_1) \mid P_3$
- hard to **automatize**
- more freedom than necessary
- **high complexity**, decidability is **unknown**, at least EXPSPACE-hard

A **new reduction strategy** for the π-calculus:

- make structural congruence **explicit** by reduction rules
- only **necessary** rules are included

Correctness:

- same equational semantics of processes
- coarsest sensible semantics: **barbed may- and should-testing**

Advantages:

- new strategy is **easier to automatize**, since all transformations are explicit
- may be used in deduction system for proving **correctness of process transformations**
  (Rau, PhD-thesis, in progress)

Syntax of the Synchronous π-Calculus

$$
\begin{array}{rcll}
\text{Processes: } P & ::= & \pi.P & \text{(action)} \\
 & \mid & P_1 \mid P_2 & \text{(parallel composition)} \\
 & \mid & !\,P & \text{(replication)} \\
 & \mid & \mathbf{0} & \text{(silent process)} \\
 & \mid & \nu x.P & \text{(name restriction)} \\
\text{Action prefixes: } \pi & ::= & x(y) & \text{input} \\
 & \mid & \overline{x}\langle y \rangle & \text{output}
\end{array}
$$

where x, y are names

Contexts: $C \in \mathcal{C} ::= [\cdot] \mid \pi.C \mid C \mid P \mid P \mid C \mid !\,C \mid \nu x.C$.

Reduction Semantics (Classic Definition)

Reduction rule for **interaction**:

$$x(y).P \mid \overline{x}\langle v\rangle.Q \xrightarrow{ia} P[v/y] \mid Q$$

Reduction contexts: $\mathbf{D} \in \mathcal{D} ::= [\cdot] \mid \mathbf{D} \mid P \mid P \mid \mathbf{D} \mid \nu x.\mathbf{D}$

$$\frac{P \xrightarrow{ia} Q}{\mathbf{D}[P] \xrightarrow{\mathcal{D},ia} \mathbf{D}[Q]}\ \mathbf{D} \in \mathcal{D} \qquad \frac{P \equiv P' \wedge P' \xrightarrow{\mathcal{D},ia} Q' \wedge Q' \equiv Q}{P \xrightarrow{sr} Q}$$

Closure w.r.t. reduction contexts — Standard reduction

$\equiv$ is structural congruence (next slide)

Structural Congruence $\equiv$

Smallest congruence on processes satisfying the following axioms

$$
\begin{array}{rcl}
P & \equiv & Q, \text{ if } P =_\alpha Q \\
P_1 \mid (P_2 \mid P_3) & \equiv & (P_1 \mid P_2) \mid P_3 \\
P_1 \mid P_2 & \equiv & P_2 \mid P_1 \\
P \mid \mathbf{0} & \equiv & P \\
\nu z.\nu w.P & \equiv & \nu w.\nu z.P \\
\nu z.\mathbf{0} & \equiv & \mathbf{0} \\
\nu z.(P_1 \mid P_2) & \equiv & P_1 \mid \nu z.P_2, \text{ if } z \notin \mathsf{fn}(P_1) \\
!\,P & \equiv & P \mid !\,P
\end{array}
$$

Remark (see Engelfriet & Gelsema 2004, 2007, Khomenko & Meyer 2009, Schmidt-Schauß,S. & Rau 2013)

The decision problem whether for two π-processes $P \equiv Q$ holds is **EXPSPACE**-hard. Its decidability is still **unknown**.

Structural Congruence as Reduction

$$
\begin{array}{lrl}
(assocl) & P_1 \mid (P_2 \mid P_3) & \xrightarrow{sca} (P_1 \mid P_2) \mid P_3 \\
(assocr) & (P_1 \mid P_2) \mid P_3 & \xrightarrow{sca} P_1 \mid (P_2 \mid P_3) \\
(commute) & P_1 \mid P_2 & \xrightarrow{sca} P_2 \mid P_1 \\
(replunfold) & !\,P & \xrightarrow{sca} P \mid !\,P \\
(nuup) & \mathbf{D}[\nu z.P] & \xrightarrow{sca} \nu z.\mathbf{D}[P],\ \text{if } z \notin \mathsf{fn}(\mathbf{D}),\ [\cdot] \neq \mathbf{D} \in \mathcal{D} \\
(nudown) & \nu z.\mathbf{D}[P] & \xrightarrow{sca} \mathbf{D}[\nu z.P],\ \text{if } z \notin \mathsf{fn}(\mathbf{D}),\ [\cdot] \neq \mathbf{D} \in \mathcal{D} \\
(nuintro) & P & \xrightarrow{sca} \nu z.P\ \ \text{if } z \notin \mathsf{fn}(P) \\
(nurem) & \nu z.P & \xrightarrow{sca} P\ \ \text{if } z \notin \mathsf{fn}(P) \\
(replfold) & P \mid !\,P & \xrightarrow{sca} !\,P \\
(intro0l) & P & \xrightarrow{sca} \mathbf{0} \mid P \\
(intro0r) & P & \xrightarrow{sca} P \mid \mathbf{0} \\
(rem0r) & P \mid \mathbf{0} & \xrightarrow{sca} P
\end{array}
$$

$$
\frac{P \xrightarrow{sca} Q}{C[P] \xrightarrow{\mathcal{C},sca} C[Q]} \quad \text{where } C \in \mathcal{C}
$$

Lemma

$$
\xrightarrow{\mathcal{C},sca,*} \;=\; \equiv
$$

New Definition: Structural Reduction instead of Congruence

Restricted structural reduction: $\xrightarrow{sc} \;\subset\; \xrightarrow{sca}$

$$
\begin{array}{ll}
(assocl) & P_1 \mid (P_2 \mid P_3) \xrightarrow{sc} (P_1 \mid P_2) \mid P_3 \\
(assocr) & (P_1 \mid P_2) \mid P_3 \xrightarrow{sc} P_1 \mid (P_2 \mid P_3) \\
(commute) & P_1 \mid P_2 \xrightarrow{sc} P_2 \mid P_1 \\
(replunfold) & !\,P \xrightarrow{sc} P \mid !\,P \\
(nuup) & \mathbf{D}[\nu z.P] \xrightarrow{sc} \nu z.\mathbf{D}[P],\ \text{if } z \notin \mathsf{fn}(\mathbf{D}),\ [\cdot] \neq \mathbf{D} \in \mathcal{D}
\end{array}
$$

$$
\frac{P \xrightarrow{sc} Q}{\mathbf{D}[P] \xrightarrow{\mathcal{D},sc} \mathbf{D}[Q]}\ \mathbf{D} \in \mathcal{D}
$$

Structural standard reduction

$$
\frac{P \xrightarrow{\mathcal{D},sc,*} P' \wedge P' \xrightarrow{\mathcal{D},ia} Q' \wedge Q' \xrightarrow{\mathcal{D},sc,*} Q}{P \xrightarrow{dsr} Q}
$$

$\mathcal{D}$-Standard Reduction

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Restricted structural reduction: $\xrightarrow{sc} \;\subset\; \xrightarrow{sca}$

$$
\begin{array}{lrcl}
(assocl) & P_1 \mid (P_2 \mid P_3) & \xrightarrow{sc} & (P_1 \mid P_2) \mid P_3 \\
(assocr) & (P_1 \mid P_2) \mid P_3 & \xrightarrow{sc} & P_1 \mid (P_2 \mid P_3) \\
(commute) & P_1 \mid P_2 & \xrightarrow{sc} & P_2 \mid P_1 \\
(replunfold) & !\,P & \xrightarrow{sc} & P \mid !\,P \\
(nuup) & \mathbf{D}[\nu z.P] & \xrightarrow{sc} & \nu z.\mathbf{D}[P],\ \text{if } z \notin \mathsf{fn}(\mathbf{D}),\ [\cdot] \neq \mathbf{D} \in \mathcal{D}
\end{array}
$$

$$
\frac{P \xrightarrow{sc} Q}{\mathbf{D}[P] \xrightarrow{\mathcal{D},sc} \mathbf{D}[Q]}\ \mathbf{D} \in \mathcal{D}
$$

Structural standard reduction

$$
\frac{P \xrightarrow{\mathcal{D},sc,*} P' \wedge P' \xrightarrow{\mathcal{D},ia} Q' \wedge Q' \xrightarrow{\mathcal{D},sc,*} Q}{P \xrightarrow{dsr} Q}
$$

$\mathcal{D}$-Standard Reduction

Goal: Show that $\xrightarrow{dsr}$ induces the same semantics as $\xrightarrow{sr}$

A Hierarchy of Process Equivalences

(see Fournet & Gonthier 2005)

fine ↑

full strong labelled bisimilarity

$\cap$

full (weak) labelled bisimilarity

$|\cap$

barbed congruence

$\cap$

barbed may- and should-testing

$\cap$

barbed may-testing

↓ coarse

A Hierarchy of Process Equivalences

(see Fournet & Gonthier 2005)

fine

full strong labelled bisimilarity

$\cap$

full (weak) labelled bisimilarity

$\subsetneq$

barbed congruence

$\cap$

barbed may- and should-testing

$\cap$

barbed may-testing

coarse

very fine, e.g.
choice P_1 (*choice* P_2 P_3)
$\not\sim$ *choice* (*choice* P_1 P_2) P_3

A Hierarchy of Process Equivalences

(see Fournet & Gonthier 2005)

full strong labelled bisimilarity

$\cap$

full (weak) labelled bisimilarity

$\subsetneq$

barbed congruence

$\cap$

barbed may- and should-testing

$\cap$

barbed may-testing

fine ↕ coarse

very fine, e.g.
choice P_1 (*choice* P_2 P_3)
$\not\sim$ *choice* (*choice* P_1 P_2) P_3

too coarse, e.g.
choice P $\mathbf{0}$ $\sim$ P

A Hierarchy of Process Equivalences

(see Fournet & Gonthier 2005)

fine

full strong labelled bisimilarity

$\cap$

full (weak) labelled bisimilarity

$\cap\!\!\!\mid$

very fine, e.g.
choice P_1 (*choice* P_2 P_3)
$\not\sim$ *choice* (*choice* P_1 P_2) P_3

barbed congruence

$\cap$

barbed may- and should-testing

$\cap$

too coarse, e.g.
choice P $\mathbf{0}$ $\sim$ P

barbed may-testing

coarse

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Process P **has a barb** on x:

- $P{\upharpoonright^{x}}$: P has an open input on x $\quad (P = \nu\mathcal{X}.(x(y).P' \mid P''),\ x \notin \mathcal{X})$
- $P{\upharpoonright^{\overline{x}}}$: P has an open output on x $\quad (P = \nu\mathcal{X}.(\overline{x}\langle y\rangle.P' \mid P''),\ x \notin \mathcal{X})$

Process P **has a barb** on x:

- $P\!\upharpoonright^{x}$: P has an open input on x $\quad(P = \nu\mathcal{X}.(x(y).P' \mid P''),\ x \notin \mathcal{X})$
- $P\!\upharpoonright^{\overline{x}}$: P has an open output on x $\quad(P = \nu\mathcal{X}.(\overline{x}\langle y\rangle.P' \mid P''),\ x \notin \mathcal{X})$

May-barb and **Should-barb**: For $\mu \in \{x, \overline{x}\}$,

- P may have a barb on μ: $P{\downarrow_\mu}$ iff $\exists Q : P \xrightarrow{sr,*} Q \ \wedge\ Q \equiv Q' \ \wedge\ Q'\!\upharpoonright^{\mu}$
- P should have a barb on μ: $P{\Downarrow_\mu}$ iff $\forall Q : P \xrightarrow{sr,*} Q \implies Q{\downarrow_\mu}$.

Process P **has a barb** on x:

- $P{\upharpoonright^{x}}$: P has an open input on x $\quad (P = \nu\mathcal{X}.(x(y).P' \mid P''),\ x \notin \mathcal{X})$
- $P{\upharpoonright^{\overline{x}}}$: P has an open output on x $\quad (P = \nu\mathcal{X}.(\overline{x}\langle y\rangle.P' \mid P''),\ x \notin \mathcal{X})$

May-barb and **Should-barb**: For $\mu \in \{x, \overline{x}\}$,

- P may have a barb on μ: $P{\downarrow_\mu}$ iff $\exists Q : P \xrightarrow{sr,*} Q \ \wedge\ Q \equiv Q' \ \wedge\ Q'{\upharpoonright^{\mu}}$
- P should have a barb on μ: $P{\Downarrow_\mu}$ iff $\forall Q : P \xrightarrow{sr,*} Q \implies Q{\downarrow_\mu}$.

Barbed May- and Should-Testing Equivalence

$P \sim Q$ iff $P \precsim Q$ and $Q \precsim P$ where

$P \precsim Q$ iff $P \precsim_{\mathrm{may}} Q$ and $P \precsim_{\mathrm{should}} Q$

$P \precsim_{\mathrm{may}} Q$ iff $\forall x \in \mathcal{N},\ \mu \in \{x, \overline{x}\}, C \in \mathcal{C}$: $C[P]{\downarrow_\mu} \implies C[Q]{\downarrow_\mu}$

$P \precsim_{\mathrm{should}} Q$ iff $\forall x \in \mathcal{N},\ \mu \in \{x, \overline{x}\}, C \in \mathcal{C}$: $C[P]{\Downarrow_\mu} \implies C[Q]{\Downarrow_\mu}$

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Barbed May- and Should-Testing Equivalence w.r.t. $\xrightarrow{dsr}$

$$P \sim_{\mathcal{D}} Q \text{ iff } P \precsim_{\mathcal{D}} Q \text{ and } Q \precsim_{\mathcal{D}} P \text{ where}$$

$P \precsim_{\mathcal{D}} Q$ iff $P \precsim_{\mathcal{D},\mathrm{may}} Q$ and $P \precsim_{\mathcal{D},\mathrm{should}} Q$

$P \precsim_{\mathcal{D},\mathrm{may}} Q$ iff $\forall x \in \mathcal{N},\ \mu \in \{x, \overline{x}\}, C \in \mathcal{C}$: $C[P]{\downarrow_{\mathcal{D},\mu}} \implies C[Q]{\downarrow_{\mathcal{D},\mu}}$

$P \precsim_{\mathcal{D},\mathrm{should}} Q$ iff $\forall x \in \mathcal{N},\ \mu \in \{x, \overline{x}\}, C \in \mathcal{C}$: $C[P]{\Downarrow_{\mathcal{D},\mu}} \implies C[Q]{\Downarrow_{\mathcal{D},\mu}}$

May-barb and Should-barb w.r.t. $\xrightarrow{dsr}$: For $\mu \in \{x, \overline{x}\}$,

- May: $P{\downarrow_{\mathcal{D},\mu}}$ iff $\exists Q : P \xrightarrow{dsr,*} Q \ \wedge\ Q \xrightarrow{\mathcal{D},sc,*} Q' \ \wedge\ Q' \upharpoonright^{\mu}$
- Should: $P{\Downarrow_{\mathcal{D},\mu}}$ iff $\forall Q : P \xrightarrow{dsr,*} Q \implies Q{\downarrow_{\mathcal{D},\mu}}$.

Main Result

Theorem

$$\sim \; = \; \sim_{\mathcal{D}}$$

Proof:

- It suffices to show $\downarrow_\mu \; = \; \downarrow_{\mathcal{D},\mu}$ and $\Downarrow_\mu \; = \; \Downarrow_{\mathcal{D},\mu}$.
- We only consider may-observation $\downarrow_\mu \; = \; \downarrow_{\mathcal{D},\mu}$ (should-observation works analogously)
- Trivial case: $\downarrow_{\mathcal{D},\mu} \; \subseteq \; \downarrow_\mu$
- Remaining case: $\downarrow_\mu \; \subseteq \; \downarrow_{\mathcal{D},\mu}$

Proof Sketch for $\downarrow_{\mu} \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \upharpoonright^{\mu}$

Proof Sketch for $\downarrow_\mu \ \subseteq \ \downarrow_{\mathcal{D},\mu}$

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \upharpoonright^{\mu}$

1) make $\equiv$ explicit:

$$P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q \text{ and } Q \upharpoonright^{\mu}$$

Proof Sketch for $\downarrow_\mu \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \upharpoonright^{\mu}$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q \upharpoonright^{\mu}$$

Proof Sketch for $\downarrow_\mu \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \Gamma^\mu$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q \Gamma^\mu$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions
(internal conversions $\xrightarrow{isca} := \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q \Gamma^\mu$$

Proof Sketch for $\downarrow_\mu \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q{\upharpoonright}^{\mu}$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q{\upharpoonright}^{\mu}$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions
(internal conversions $\xrightarrow{isca} \; := \; \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q{\upharpoonright}^{\mu}$$

Proof Sketch for $\downarrow_\mu \ \subseteq \ \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q\!\upharpoonright^{\mu}$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q\!\upharpoonright^{\mu}$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions
(internal conversions $\xrightarrow{isca} \ := \ \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q\!\upharpoonright^{\mu}$$

3) shift internal conversions to the right:

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q\!\upharpoonright^{\mu}$$

Proof Sketch for $\downarrow_{\mu} \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q{\Rsh}^{\mu}$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q{\Rsh}^{\mu}$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions

(internal conversions $\xrightarrow{isca} \; := \; \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q{\Rsh}^{\mu}$$

3) shift internal conversions to the right:

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \dots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{isca,*} Q \text{ and } Q{\Rsh}^{\mu}$$

Proof Sketch for $\downarrow_\mu \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \Gamma^{\mu}$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q \Gamma^{\mu}$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions

(internal conversions $\xrightarrow{isca} \ := \ \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q \Gamma^{\mu}$$

3) shift internal conversions to the right:

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \xrightarrow{isca,*} Q \text{ and } Q \Gamma^{\mu}$$

Proof Sketch for $\downarrow_\mu \subseteq \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \Gamma^\mu$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q \Gamma^\mu$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions
(internal conversions $\xrightarrow{isca} := \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q \Gamma^\mu$$

3) shift internal conversions to the right:

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \xrightarrow{isca,*} Q \text{ and } Q \Gamma^\mu$$

4) apply base case lemma: $Q' \equiv Q \wedge Q \Gamma^\mu$ iff $Q' \xrightarrow{\mathcal{D},sc,*} Q'' \wedge Q'' \Gamma^\mu$.

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \xrightarrow{isca,*} Q \text{ and } Q \Gamma^\mu$$

Proof Sketch for $\downarrow_\mu \;\subseteq\; \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q\!\upharpoonright^\mu$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q\!\upharpoonright^\mu$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions
(internal conversions $\xrightarrow{isca} \;:=\; \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q\!\upharpoonright^\mu$$

3) shift internal conversions to the right:

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \xrightarrow{isca,*} Q \text{ and } Q\!\upharpoonright^\mu$$

4) apply base case lemma: $Q' \equiv Q \wedge Q\!\upharpoonright^\mu$ iff $Q' \xrightarrow{\mathcal{D},sc,*} Q'' \wedge Q''\!\upharpoonright^\mu$.

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \equiv Q \text{ and } Q\!\upharpoonright^\mu$$

Proof Sketch for $\downarrow_\mu \;\subseteq\; \downarrow_{\mathcal{D},\mu}$

Given reduction sequence: $P \equiv \xrightarrow{\mathcal{D},ia} \equiv \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \equiv Q$ and $Q \upharpoonright^\mu$

1) make $\equiv$ explicit:

$$P \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{C},sca,*} Q \text{ and } Q \upharpoonright^\mu$$

2) split $\xrightarrow{\mathcal{C},sca}$ into internal conversions $\xrightarrow{isca}$ and $\xrightarrow{\mathcal{D},sc}$ conversions

(internal conversions $\xrightarrow{isca} \;:=\; \xrightarrow{\mathcal{C},sca} \setminus \xrightarrow{\mathcal{D},sc}$)

$$P \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{isca \vee \mathcal{D},sc,*} Q \text{ and } Q \upharpoonright^\mu$$

3) shift internal conversions to the right:

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \xrightarrow{isca,*} Q \text{ and } Q \upharpoonright^\mu$$

4) apply base case lemma: $Q' \equiv Q \wedge Q \upharpoonright^\mu$ iff $Q' \xrightarrow{\mathcal{D},sc,*} Q'' \wedge Q'' \upharpoonright^\mu$.

$$P \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} \xrightarrow{\mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},ia} \xrightarrow{\mathcal{D},sc,*} Q' \xrightarrow{\mathcal{D},sc,*} Q'' \text{ and } Q'' \upharpoonright^\mu$$

Main Lemma (Shift internal conversions to the end)

If $P_1 \xrightarrow{\mathcal{C},sca \vee \mathcal{D},ia} P_2 \xrightarrow{\mathcal{C},sca \vee \mathcal{D},ia} \ldots \xrightarrow{\mathcal{C},sca \vee \mathcal{D},ia} P_n$
then $P_1 \xrightarrow{\mathcal{D},sc \vee \mathcal{D},ia} Q_1 \xrightarrow{\mathcal{D},sc \vee \mathcal{D},ia} \ldots \xrightarrow{\mathcal{D},sc \vee \mathcal{D},ia} Q_m \xrightarrow{isca,*} P_n$

Proof: Induction on the given sequence, and inspection of overlappings of the forms:

- $P \xrightarrow{isca} P' \xrightarrow{\mathcal{D},sc} P''$
- $P \xrightarrow{isca} P' \xrightarrow{\mathcal{D},ia} P''$

All possible cases:

$$\xrightarrow{isca} . \xrightarrow{\mathcal{D},sc\vee ia} \ \rightsquigarrow\ \xrightarrow{\mathcal{D},sc\vee ia} . \xrightarrow{isca} . \xrightarrow{isca} \tag{1}$$

$$\xrightarrow{isca} . \xrightarrow{\mathcal{D},sc\vee ia} \ \rightsquigarrow\ \xrightarrow{\mathcal{D},sc\vee ia,n} . \xrightarrow{isca} \text{ for any } n \geq 1 \tag{2}$$

$$\xrightarrow{isca} . \xrightarrow{\mathcal{D},sc\vee ia} \ \rightsquigarrow\ \varepsilon \text{ (where } \varepsilon \text{ represents the empty string)} \tag{3}$$

$$\xrightarrow{isca} . \xrightarrow{\mathcal{D},sc\vee ia} \ \rightsquigarrow\ \xrightarrow{isca} \tag{4}$$

$$\xrightarrow{isca} . \xrightarrow{\mathcal{D},sc\vee ia} \ \rightsquigarrow\ \xrightarrow{\mathcal{D},sc\vee ia} \tag{5}$$

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

All possible cases:

$$\xrightarrow{isca\langle k\rangle} . \xrightarrow{\mathcal{D},sc\vee ia} \;\rightsquigarrow\; \xrightarrow{\mathcal{D},sc\vee ia} . \xrightarrow{isca\langle k-1\rangle} . \xrightarrow{isca\langle k\rangle} \text{ for } k \geq 1 \tag{1}$$

$$\xrightarrow{isca\langle k\rangle} . \xrightarrow{\mathcal{D},sc\vee ia} \;\rightsquigarrow\; \xrightarrow{\mathcal{D},sc\vee ia,n} . \xrightarrow{isca\langle k\rangle} \text{ for } k \geq 0 \text{ and any } n \geq 1 \tag{2}$$

$$\xrightarrow{isca\langle 0\rangle} . \xrightarrow{\mathcal{D},sc\vee ia} \;\rightsquigarrow\; \varepsilon \text{ (where } \varepsilon \text{ represents the empty string)} \tag{3}$$

$$\xrightarrow{isca\langle 0\rangle} . \xrightarrow{\mathcal{D},sc\vee ia} \;\rightsquigarrow\; \xrightarrow{isca\langle 0\rangle} \tag{4}$$

$$\xrightarrow{isca\langle 0\rangle} . \xrightarrow{\mathcal{D},sc\vee ia} \;\rightsquigarrow\; \xrightarrow{\mathcal{D},sc\vee ia} \tag{5}$$

where $\xrightarrow{isca\langle k\rangle} = \xrightarrow{isca}$-transformation at replication depth k

Automatic Proof

Encode the shifting as a term rewriting system:

$$
\begin{aligned}
isca(S(\mathsf{K}), dscdia(\mathsf{X})) &\to dscdia(isca(\mathsf{K}, isca(S(\mathsf{K}), \mathsf{X}))) && (1)\\
isca(\mathsf{K}, dscdia(\mathsf{X})) &\to gen(S(\mathsf{N}), isca(\mathsf{K}, \mathsf{X})) && (2)\\
gen(S(\mathsf{N}), \mathsf{X}) &\to dscdia(gen(\mathsf{N}, \mathsf{X})) && (2')\\
gen(Z, \mathsf{X}) &\to \mathsf{X} && (2'')\\
isca(Z, dscdia(\mathsf{X})) &\to \mathsf{X} && (3)\\
isca(Z, dscdia(\mathsf{X})) &\to isca(Z, \mathsf{X}) && (4)\\
isca(Z, dscdia(\mathsf{X})) &\to dscdia(Z, \mathsf{X}) && (5)
\end{aligned}
$$

- Numbers are encoded by Peano-numbers $S(\cdot)$,Z.
- TRS with free variables on the right hand side
- AProVE shows innermost-termination, CeTA verifies the proof
- Termination proof implies that an **induction measure exists**
- Extends the encoding approach for automating correctness proofs for program transformations in Rau, S., Schmidt-Schauß, 2012

Conclusion

- **new rewriting semantics** for the π-calculus
- conversion w.r.t. structural congruence are explicit by rewriting
- restricted set of conversions is sufficient
- without any semantic difference w.r.t. barbed may- and should-testing

Further work

- use the new strategy for automated correctness proofs of process transformations
- extensions and variants of the π-calculus
- look for other notions of process equivalence