A completeness proof for bisimulation in the π-calculus using Isabelle

Jesper Bengtson Joachim Parrow

Department of Information Technology
University of Uppsala, Sweden

7th December 2007

Our previous work

Our formalisation of the π-calculus includes the following results for both late and early semantics.

- Strong bisimulation is preserved by all operators except input-prefix.
- Strong equivalence is a congruence
- Weak bisimulation is preserved by all operators except $+$ and input-prefix.
- Weak congruence is a congruence
- All structurally congruent terms are also bisimilar
- The Hennessy lemma.

Motivation

Our motivation for doing this work was twofold.

- We wanted to try our wings – how easy would it be to add these results building on our formalisation.
- These results have never been proven inside a theorem prover.

The finite π-calculus

Prefixes

$$\begin{aligned} \pi_p &= a(x) \\ &\mid \bar{a}b \\ &\mid \tau \end{aligned}$$

Processes

$$\begin{aligned} \pi &= 0 \\ &\mid \pi_p.\pi \\ &\mid [a = b]\pi \\ &\mid [a \neq b]\pi \\ &\mid \pi + \pi \\ &\mid \pi \mid \pi \\ &\mid (\nu x)\pi \end{aligned}$$

Strong late bisimulation

Simulation

$$P \rightsquigarrow_{\mathcal{R}} Q \equiv \quad \forall Q'\ \alpha.\ \mathsf{bn}(\alpha) \cap \mathsf{fn}(P) = \emptyset \wedge Q \xrightarrow{\alpha} Q' \longrightarrow \exists P'.P \xrightarrow{\alpha} P' \wedge D(P',\ Q',\ \alpha,\ \mathcal{R})$$

The requirements of the derivatives depend on the action used.

D

$$D(P', Q', \alpha, \mathcal{R}) \equiv \quad \begin{array}{lll} \text{case } \alpha \text{ of } a(x) & \rightarrow & \forall u.P'\{u/x\}\ \mathcal{R}\ Q'\{u/x\} \\ \mid \_ & \rightarrow & P'\ \mathcal{R}\ Q' \end{array}$$

$P \rightsquigarrow_{\mathcal{R}} Q$ can be read "P simulates Q preserving $\mathcal{R}$"

Bisimulation

$$P \sim Q \equiv P \rightsquigarrow_{\sim} Q \wedge Q \rightsquigarrow_{\sim} P$$

Proof outline

We will prove soundness and completeness of strong bisimulation in three phases.

- A core calculus using only prefix, match, mismatch and sum.
- Add restriction
- Add parallelism

The axioms for strong late bisimulation

The axioms for strong late bisimulation excluding restriction and the parallel operator are the following:

str1 $P + \mathbf{0} \equiv P$

str2 $P + Q \equiv Q + P$

str3 $P + (Q + R) \equiv (P + Q) + R$

congr1 If $P \equiv Q$ then $\bar{a}u.P \equiv \bar{a}u.Q$, $\tau.P \equiv \tau.Q$, $P + R \equiv Q + R$

congr2 If $P\{y/x\} \equiv Q\{y/x\}$ for all $y \in (P, Q, x)$ then $a(x).P \equiv a(x).Q$

The axioms for strong late bisimulation cont.

idemp	$P + P$	$\equiv$	P	
m1	$[x = x]P$	$\equiv$	P	
m2	$[x = y]P$	$\equiv$	$\mathbf{0}$	if $x \neq y$
mm1	$[x \neq x]P$	$\equiv$	$\mathbf{0}$	
mm2	$[x \neq y]P$	$\equiv$	P	if $x \neq y$

Soundness

In order to prove soundness we need to prove the following:

str1	$P + \mathbf{0} \sim P$	
str2	$P + Q \sim Q + P$	
str3	$P + (Q + R) \sim (P + Q) + R$	
congr1	If $P \sim Q$ then	$\bar{a}u.P \sim \bar{a}u.Q$
		$\tau.P \sim \tau.Q$
		$P + R \sim Q + R$
congr2	If $P\{y/x\} \sim Q\{y/x\}$ for all $y \in (P, Q, x)$ then	
	$a(x).P \sim a(x).Q$	

We proved all of these in previous work except for **congr2**.

Soundness cont.

The remaining lemmas for the soundness proofs were:

idemp	$P + P$	$\sim$	P	
m1	$[x = x]P$	$\sim$	P	
m2	$[x = y]P$	$\sim$	$\mathbf{0}$	if $x \neq y$
mm1	$[x \neq x]P$	$\sim$	$\mathbf{0}$	
mm2	$[x \neq y]P$	$\sim$	P	if $x \neq y$

None of these were difficult for Isabelle to prove.

Completeness

At the core of the completeness proof lies the concept of the head normal form.

Head normal form (hnf)

$$
\begin{aligned}
\texttt{hnf}(\mathbf{0}) &= \texttt{True} \\
\texttt{hnf}(\alpha.P) &= \texttt{True} \\
\texttt{hnf}(P + Q) &= \texttt{hnf}(P) \wedge \texttt{hnf}(Q) \wedge P \neq \mathbf{0} \wedge Q \neq \mathbf{0} \\
\texttt{hnf}\ \_ &= \texttt{False}
\end{aligned}
$$

Completeness

At the core of the completeness proof lies the concept of the head normal form.

Head normal form (hnf)

$$
\begin{aligned}
\texttt{hnf}(\mathbf{0}) &= \texttt{True} \\
\texttt{hnf}(\alpha.P) &= \texttt{True} \\
\texttt{hnf}(P + Q) &= \texttt{hnf}(P) \wedge \texttt{hnf}(Q) \wedge P \neq \mathbf{0} \wedge Q \neq \mathbf{0} \\
\texttt{hnf}\ \_ &= \texttt{False}
\end{aligned}
$$

Terms on `hnf`	*Terms not on* `hnf`
$\mathbf{0}$	$\mathbf{0} + a(x).P$
$a(x).P$	$P \mid Q$
$a(x).P + \bar{b}c.Q + \tau.R$	$a(x).P + \mathbf{0} + \tau.R$

Summands

We will reason about hnfs using their summands. Intuitively the summand of a term is the set of it's prefixed sub terms which are composed by the $+$-operator.

Summand

$$
\begin{aligned}
\texttt{summands}(\alpha.P) &= \{\alpha.P\} \\
\texttt{summands}(P+Q) &= \texttt{summands}(P) \cup \texttt{summands}(Q) \\
\texttt{summands}\ \_ &= \{\}
\end{aligned}
$$

Summands

We will reason about hnfs using their summands. Intuitively the summand of a term is the set of it's prefixed sub terms which are composed by the $+$-operator.

Summand

$$
\begin{aligned}
\texttt{summands}(\alpha.P) &= \{\alpha.P\} \\
\texttt{summands}(P+Q) &= \texttt{summands}(P) \cup \texttt{summands}(Q) \\
\texttt{summands}\ \_ &= \{\}
\end{aligned}
$$

$$
\begin{aligned}
\texttt{summands}\ \mathbf{0} &= \{\} \\
\texttt{summands}\ a(x).P &= \{a(x).P\} \\
\texttt{summands}\ a(x).P + \bar{b}c.Q + \tau.R &= \{a(x).P,\ \bar{b}c.Q,\ \tau R\}
\end{aligned}
$$

Induction over summands

Isabelle's inductive rule for finite sets.

$$\frac{\begin{array}{c}\texttt{finite}\ \mathcal{F} \\ \mathcal{P}\ \{\} \\ \forall x\ \mathcal{F}.\ \texttt{finite}\ \mathcal{F} \wedge x \notin \mathcal{F} \wedge \mathcal{P}\ \mathcal{F} \longrightarrow \mathcal{P}\ (\texttt{insert}\ x\ \mathcal{F})\end{array}}{\mathcal{P}\ \mathcal{F}}$$

The inductive step is problematic as our proofs are working up to provable equivalence by the axioms and not syntactic equivalence. If we remove a term from a set a provably equal one can still remain.

A stronger head normal form

Unique head normal form (uhnf)

$\texttt{uhnf}\ P = \texttt{hnf}\ P \wedge \forall R\ R' \in \texttt{summands}\ P.\ R \neq R' \longrightarrow R \not\equiv R'$

A stronger head normal form

Unique head normal form (uhnf)

$\texttt{uhnf}\ P = \texttt{hnf}\ P \wedge \forall R\ R' \in \texttt{summands}\ P.\ R \neq R' \longrightarrow R \not\equiv R'$

Terms on uhnf	*Terms not on* uhnf
$\mathbf{0}$	$\mathbf{0} + a(x).P$
$a(x).P$	$P \mid Q$
$a(x).P + \bar{b}c.Q + \tau.R$	$a(x).P + \bar{b}c.Q + a(x).P$

Making uhnfs behave like sets

Lemma

If $P \in \texttt{summands}\ Q$ *and* $\texttt{uhnf}\ Q$ *then there exists a* Q' *s.t.* $P + Q' \equiv Q$, $\texttt{summands}\ Q' = \texttt{summands}\ Q - \{P\}$ *and* $\texttt{uhnf}\ Q'$.

Making uhnfs behave like sets

Lemma

If $P \in \texttt{summands}\ Q$ *and* $\texttt{uhnf}\ Q$ *then there exists a* Q' *s.t.* $P + Q' \equiv Q$, $\texttt{summands}\ Q' = \texttt{summands}\ Q - \{P\}$ *and* $\texttt{uhnf}\ Q'$.

For instance, if we have: $Q = a(x).P + \bar{b}c.Q + \tau.R + b(y).T$ then $\tau.R \in \texttt{summands}\ Q$ and $\texttt{uhnf}\ Q$.

We can pick a $Q' = a(x).P + \bar{b}c.Q + b(y).T$ and we have that: $\tau.R + Q' \equiv Q$, $\texttt{summands}\ Q' = \texttt{summands}\ Q - \{\tau.R\}$ and $\texttt{uhnf}\ Q'$.

Connecting provable equivalence to summands

Lemma

$$\frac{\begin{array}{c}\texttt{uhnf}\ P \\ \texttt{uhnf}\ Q \\ \forall P' \in \texttt{summands}\ P.\ \exists Q' \in \texttt{summands}\ Q.\ P' \equiv Q' \\ \forall Q' \in \texttt{summands}\ Q.\ \exists P' \in \texttt{summands}\ P.\ Q' \equiv P'\end{array}}{P \equiv Q}$$

Proof.

By induction over $\texttt{summands}\ P$. □

Connecting summands to transitions

Lemma

If $\texttt{hnf}\ P$ *then* $P \xrightarrow{\alpha} P'$ *iff* $\alpha.P' \in \texttt{summands}\ P$

Proof.

By induction over P. □

Depth

Our main proof will be done by induction over the maximum number of steps that the bisimulating processes can perform.

Depth

$$
\begin{aligned}
\mathtt{depth}(\mathbf{0}) &= 0 \\
\mathtt{depth}(\alpha.P) &= 1 + \mathtt{depth}(P) \\
\mathtt{depth}([a = b]P) &= \mathtt{depth}([a \neq b]P) = \mathtt{depth}(P) \\
\mathtt{depth}(P + Q) &= \mathtt{max}(\mathtt{depth}(P),\ \mathtt{depth}(\mathtt{Q}))
\end{aligned}
$$

Depth

Our main proof will be done by induction over the maximum number of steps that the bisimulating processes can perform.

Depth

$$
\begin{aligned}
\mathtt{depth}(\mathbf{0}) &= 0 \\
\mathtt{depth}(\alpha.P) &= 1 + \mathtt{depth}(P) \\
\mathtt{depth}([a = b]P) &= \mathtt{depth}([a \neq b]P) = \mathtt{depth}(P) \\
\mathtt{depth}(P + Q) &= \mathtt{max}(\mathtt{depth}(P),\ \mathtt{depth}(\mathtt{Q}))
\end{aligned}
$$

$$
\begin{aligned}
\mathtt{depth}\ \mathbf{0} &= 0 \\
\mathtt{depth}\ a(x).\mathbf{0} &= 1 \\
\mathtt{depth}\ a(x).\mathbf{0} + \bar{b}c.\tau.\tau.\mathbf{0} &= 3
\end{aligned}
$$

Depth decreases

In order to use depth in induction we much prove that it decreases over transitions.

Lemma

If $P \xrightarrow{\alpha} P'$ *then* $\texttt{depth}(P') < \texttt{depth}(P)$

Proof.

By induction over $P \xrightarrow{\alpha} P'$. □

All processes have a provably equal *uhnf*

A key idea of the completion proof is that it only works on processes which are on *uhnf*. As such, all processes must be translated to *uhnf* before starting the proof.

Lemma

For every P, *there exists a* Q *s.t.* $\texttt{uhnf}(Q)$, $P \equiv Q$ *and* $\texttt{depth}(Q) \leq \texttt{depth}(P)$

We will need the following auxiliary lemma

Lemma

If $\texttt{uhnf}(P)$ *and* $\texttt{uhnf}(Q)$ *then there exists an* R *such that* $\texttt{uhnf}(R)$, $P + Q \equiv R$ *and* $\texttt{depth}(R) \leq \texttt{depth}(P + Q)$

The axiomatisation is complete

Lemma

If $P \sim Q$, $\texttt{uhnf}\ P$, $\texttt{uhnf}\ Q$ *and* $\texttt{depth}\ P + \texttt{depth}\ Q < n$ *then* $P \equiv Q$.

Proof.

By induction on n. □

The axiomatisation is complete

Lemma

If $P \sim Q$, $\texttt{uhnf}\ P$, $\texttt{uhnf}\ Q$ *and* $\texttt{depth}\ P + \texttt{depth}\ Q < n$ *then* $P \equiv Q$.

Proof.

By induction on n. □

We can now prove our main theorem.

Lemma

If $P \sim Q$ *then* $P \equiv Q$

Proof.

Pick an n larger than $\texttt{depth}\ P + \texttt{depth}\ Q$, convert P and Q to $\texttt{uhnfs}\ P'$ and Q' and apply the auxiliary lemma. Since the axiomatisation is sound, $P \sim Q$. □

The restriction axioms

The following axioms need to be added to handle restriction.

str4	$(\nu x)(\nu y)P \equiv (\nu y)(\nu x)P$	
str5	$(\nu x)P \equiv P$	$x \notin \mathtt{fn}(P)$
congr1	If $P \equiv Q$ then $(\nu x)P \equiv (\nu x)Q$	
r1	$(\nu x)\alpha.P \equiv \alpha.(\nu x)P$	if $x \notin \alpha$
r2	$(\nu x)\alpha.P \equiv \mathbf{0}$	if x is the subject of α
r3	$(\nu x)(P+Q) \equiv (\nu x)P + (\nu x)Q$	

Soundness

In order to prove soundness we need to prove the following:

str4	$(\nu x)(\nu y)P \sim (\nu y)(\nu x)P$	
str5	$(\nu x)P \sim P$	$x \notin \mathtt{fn}(P)$
congr1	If $P \sim Q$ then $(\nu x)P \sim (\nu x)Q$	
r1	$(\nu x)\alpha.P \sim \alpha.(\nu x)P$	if $x \notin \alpha$
r2	$(\nu x)\alpha.P \sim \mathbf{0}$	if x is the subject of α
r3	$(\nu x)(P+Q) \sim (\nu x)P + (\nu x)Q$	

We proved all of these in previous work except for **r1**, **r2** and **r3**

Completeness

We need to extend our functions to handle restriction.

hnf

$\texttt{hnf}\ (\nu x)P = \exists a\ P'.\ a \neq x \wedge P = \bar{a}x.P'$

Summands

$$\texttt{summands}\ (\nu x)P = \texttt{if}\ \exists a\ P'.\ a \neq x \wedge P = \bar{a}x.P'\ \texttt{then}\ \{(\nu x)P\}\ \texttt{else}\ \{\}$$

Depth

$\texttt{depth}\ (\nu x)P = \texttt{depth}\ P$

Completeness cont.

We need the following lemma to prove that processes with restrictions can be rewritten to uhnf.

Lemma

If $\texttt{uhnf}(P)$ *then there exists an* Q *such that* $\texttt{uhnf}(Q)$, $(\nu x)P \equiv Q$ *and* $\texttt{depth}(Q) \leq \texttt{depth}((\nu x)P)$

Adding parallelism

We can explode two processes running in parallel to a sequence of choices.

The expansion law

$$
\begin{aligned}
&\texttt{expand}(\texttt{P},\ \texttt{Q}) = \\
&\{\alpha.(P' \mid Q) \mid\ \alpha.P' \in \texttt{summands}(P) \wedge \texttt{bn}\ \alpha \cap \texttt{fn}\ Q = \emptyset\} \cup \\
&\{\tau.(P'\{b/x\} \mid Q') \mid a(x).P' \in \texttt{summands}(P) \wedge \\
&\qquad\qquad \bar{a}b.Q' \in \texttt{summands}(Q)\} \cup \\
&\{\tau.(\nu y)(P'\{y/x\} \mid Q') \mid a(x).P' \in \texttt{summands}(P) \wedge y \notin \texttt{fn}\ P \wedge \\
&\qquad\qquad (\nu y)\bar{a}y.Q' \in \texttt{summands}(Q)\}
\end{aligned}
$$

Adding parallelism

We can explode two processes running in parallel to a sequence of choices.

The expansion law

$$\begin{aligned}
&\texttt{expand}(\texttt{P},\ \texttt{Q}) = \\
&\{\alpha.(P' \mid Q) \mid\ \alpha.P' \in \texttt{summands}(P) \wedge \texttt{bn}\ \alpha \cap \texttt{fn}\ Q = \emptyset\} \cup \\
&\{\tau.(P'\{b/x\} \mid Q') \mid a(x).P' \in \texttt{summands}(P) \wedge \\
&\qquad\qquad \bar{a}b.Q' \in \texttt{summands}(Q)\} \cup \\
&\{\tau.(\nu y)(P'\{y/x\} \mid Q') \mid a(x).P' \in \texttt{summands}(P) \wedge y \notin \texttt{fn}\ P \wedge \\
&\qquad\qquad (\nu y)\bar{a}y.Q' \in \texttt{summands}(Q)\}
\end{aligned}$$

$$\begin{aligned}
\texttt{expand}(a(x).P,\ \bar{a}b.Q) = \{&a(x).(P \mid \bar{a}b.Q),\ \bar{a}b.(a(x).P \mid Q), \\
&\tau.(P\{b/x\},\ Q)\}
\end{aligned}$$

Compacting a set

The relation $\mathcal{S}$

$(\mathbf{0},\ \{\}) \in \mathcal{S}$
$(P,\ \{P\}) \in \mathcal{S}$
$Q \in F \wedge (P,\ F - \{Q\}) \in \mathcal{S} \Longrightarrow (P + Q,\ F) \in \mathcal{S}$

Axioms for the parallel operator

par if $(R,\ \texttt{expand}(P,\ Q)) \in \mathcal{S}$ then $P \mid Q \equiv R$

Soundness

Two prove soundness we need the following lemma:

Lemma

If $(R,\ \mathit{expand}(P,\ Q)) \in \mathcal{S}$, $\mathtt{hnf}(P)$ *and* $\mathtt{hnf}(Q)$ *then* $P \mid Q \xrightarrow{\alpha} P'$ *iff* $R \xrightarrow{\alpha} P'$.

Proving soundness then becomes easy.

par if $(R,\ \mathtt{expand}(P,\ Q)) \in \mathcal{S}$ then $P \mid Q \sim R$

Completeness

The only function we need to update for parallelism is the depth function.

Depth of two parallel processes

$$\texttt{depth}(P \mid Q) = \texttt{depth}(P) + \texttt{depth}(Q)$$

Completeness

The only function we need to update for parallelism is the depth function.

Depth of two parallel processes

$$\texttt{depth}(P \mid Q) = \texttt{depth}(P) + \texttt{depth}(Q)$$

$$\begin{aligned} \texttt{depth}\ \mathbf{0} &= 0 \\ \texttt{depth}\ a(x).\mathbf{0} &= 1 \\ \texttt{depth}\ a(x).\mathbf{0} \mid \bar{b}c.\tau.\tau.\mathbf{0} &= 4 \end{aligned}$$

Completeness cont.

To finalise our completeness proof, we need the following lemma:

Lemma

If $\texttt{uhnf}(P)$ *and* $\texttt{uhnf}(Q)$ *then there exists an* R *s.t.*
$(R,\ \texttt{expand}(P,\ Q) \in \mathcal{S}$, $\texttt{uhnf}(R)$ *and* $\texttt{depth}(R) \leq \texttt{depth}(P \mid Q)$

Conclusions

- Most of the soundness proofs were already done from our earlier formalisations.
- Human intuition and hand waving regarding hnfs required us to strengthen the concept to get it through a theorem prover.
- Proofs resemble their pen-and-paper counterparts very closely.
- About three weeks work.
- About 3800 lines of code, apart from our previous formalisation.

Thank you for your attention