The Applied Pi Calculus... with Proofs

Bruno Blanchet

INRIA Paris-Rocquencourt

joint work with Martín Abadi and Cédric Fournet

April 2015
The applied pi calculus

- Designed by Abadi and Fournet (*Mobile Values, New Names, and Secure Communication*, POPL’01).
- Extension of the **pi calculus** with **terms** instead of names for messages.
- Language for modeling security protocols:
  - Terms represent protocol messages.
  - Function symbols represent cryptographic primitives.
  - The properties of these primitives are modeled by equations.
  - The input language of ProVerif is a dialect of the applied pi calculus.
- The applied pi calculus and ProVerif are widely used.
  - Interesting to make them converge, with a solid theoretical foundation.
Our contribution

- Minor changes to the language
  - Closer to ProVerif
- Detailed proofs of all results
  - Minor fixes; some side-conditions were not explicit
  - 74 pages of proofs...
- Revised examples
  - New example on indifferentiability
Related work

- Avik Chaudhuri (private communication, 2007)
  - found a counter-example to “observational equivalence equals labelled bisimilarity”, due to a missing side-condition.

- Bengtson et al, LICS’09
  - mentioned a similar counter-example;
  - proposed a framework for defining various extensions of the pi calculus (psi-calculi), with machine-checked proofs.

- Jia Liu (http://lcs.ios.ac.cn/~jliu/papers/LiuJia0608.pdf)
  - made the missing side-condition explicit, and gave a proof of “observational equivalence equals labelled bisimilarity”;
  - closer to the original applied pi calculus paper;
  - extension to a stateful variant (POST’14, with Arapinis, Ritter, and Ryan).
Syntax: processes

\[ L, M, N, T, U, V ::= \]
\[ a, b, c, \ldots, k, \ldots, m, n, \ldots, s \]
\[ x, y, z \]
\[ f(M_1, \ldots, M_l) \]

\[ P, Q, R ::= \]
\[ 0 \]
\[ P | Q \]
\[ !P \]
\[ \nu n. P \]
\[ if \ M = N \ then \ P \ else \ Q \]
\[ u(x).P \]
\[ \overline{u}(M).P \]
Syntax: processes

\[ L, M, N, T, U, V ::= \]
\[ a, b, c, \ldots, k, \ldots, m, n, \ldots, s \]
\[ x, y, z \]
\[ f(M_1, \ldots, M_l) \]

\[ P, Q, R ::= \]
\[ 0 \]
\[ P \mid Q \]
\[ !P \]
\[ \nu n.P \]
\[ if \ M = N \ then \ P \ else \ Q \]
\[ N(x).P \]
\[ \overline{N}\langle M\rangle.P \]
Syntax: extended processes

\[ A, B, C ::= \]
- \( P \) extended processes
- \( A | B \) plain process
- \( \nu n.A \) parallel composition
- \( \nu x.A \) name restriction
- \( \{^M/x\} \) variable restriction
- \( \{^M/x\} \) active substitution

- Active substitutions model the knowledge of the adversary.
- \( \{^M_1/x_1, \ldots, ^M_l/x_l\} \) for \( \{^M_1/x_1\} | \ldots | \{^M_l/x_l\} \).
- Substitutions are cycle-free.
- At most one substitution for each variable.
- Exactly one when the variable is restricted.
Sorts

Variables, names, and functions come with sorts:

- $u : \tau$ means that $u$ has sort $\tau$.
  - Examples of sorts: Integer, Key, Data, …
  - There are infinite numbers of variables and names of each sort.
- $f : \tau_1 \times \cdots \times \tau_l \to \tau$ means that $f$ has arguments of sorts $\tau_1, \ldots, \tau_l$ and a result of sort $\tau$. 
Sorts

Special sort Channel\(\langle \tau \rangle\) for channels.
Special sort **Channel** for channels.

- The unsorted applied pi is a particular case of the sorted applied pi, using the single sort Channel.

The sort system enforces that:

- Functional applications are well-sorted.
- $M$ and $N$ are of the same sort in the conditional expression.
- $N$ has sort Channel in the input and output expressions.
  
  - The sort system can enforce that channels are names or variables: choose types of functions so that no function returns sort Channel.

- Active substitutions preserve sorts.
Semantics: equations

The signature $\Sigma$ is equipped with an **equational theory**
  - closed under substitutions of terms for variables and names;
    - intuitively, defined from equations that do not contain names;
  - respects the sort system;
  - **non-trivial**, that is, there exist two different terms in each sort.

**Example**

\[
\begin{align*}
\text{fst}((x, y)) & = x \\
\text{snd}((x, y)) & = y \\
\text{dec}(\text{enc}(x, y), y) & = x \\
\text{check}(x, \text{sign}(x, \text{sk}(y)), \text{pk}(y)) & = \text{ok}
\end{align*}
\]

Equality modulo the equational theory: $\Sigma \vdash M = N$. 
Processes are considered equal modulo renaming of bound names and variables.

- Needed to define $P\{M/x\}$.

A context is a (possibly extended) process with a hole. An evaluation context is a context whose hole is not under a replication, a conditional, an input, or an output.

$$E ::=$$

- evaluation context
  - hole
  - parallel composition
  - parallel composition
  - name restriction
  - variable restriction

Bruno Blanchet (INRIA)  
Applied pi calculus  
April 2015
Semantics: structural equivalence

Structural equivalence ≡

- equivalence relation
- closed by application of evaluation contexts

\[
\begin{align*}
\text{Par-0} & \quad A ≡ A \mid 0 \\
\text{Par-A} & \quad A \mid (B \mid C) ≡ (A \mid B) \mid C \\
\text{Par-C} & \quad A \mid B ≡ B \mid A \\
\text{Repl} & \quad !P ≡ P \mid !P \\
\text{New-0} & \quad \nu n.0 ≡ 0 \\
\text{New-C} & \quad \nu u.\nu v.A ≡ \nu v.\nu u.A \\
\text{New-Par} & \quad A \mid \nu u.B ≡ \nu u.(A \mid B) \\
\text{Alias} & \quad \nu x.\{^M/x\} ≡ 0 \\
\text{Subst} & \quad \{^M/x\} \mid A ≡ \{^M/x\} \mid A\{^M/x\} \\
\text{Rewrite} & \quad \{^M/x\} ≡ \{^N/x\} \quad \text{when } \Sigma ⊢ M = N
\end{align*}
\]
Semantics: internal reduction

Internal reduction →

- closed by structural equivalence
- closed by application of evaluation contexts

\[
\text{COMM} \quad \overline{N}\langle x \rangle . P | N(x).Q \rightarrow P | Q
\]

\[
\text{THEN} \quad if \ M = M \ then \ P \ else \ Q \rightarrow P
\]

\[
\text{ELSE} \quad if \ M = N \ then \ P \ else \ Q \rightarrow Q
\]

for any ground terms \( M \) and \( N \) such that \( \Sigma \not\vdash M = N \)

Using structural equivalence:

\[
\overline{N}\langle M \rangle . P | N(x).Q \equiv \nu x. (\{M/x\} | \overline{N}\langle x \rangle . P | N(x).Q)
\]

\[
\rightarrow \nu x. (\{M/x\} | P | Q) \quad \text{by COMM}
\]

\[
\equiv P | Q\{M/x\}
\]
Preliminary definitions

- $\text{dom}(A)$: domain, set of variables that $A$ exports.
- $\text{fv}(A)$: free variables
- $A$ is closed when its free variables are all defined by an active substitution, that is, $\text{dom}(A) = \text{fv}(A)$.
- $E[\_]$ closes $A$ when $E[A]$ is closed.
- $A \downarrow \alpha$ when $A \rightarrow^* \equiv E[\alpha \langle M \rangle. P]$ for some evaluation context $E[\_]$ that does not bind $\alpha$.
  - $A$ can send a message on channel $\alpha$. 

Bruno Blanchet (INRIA)  
Applied pi calculus  
April 2015
Observational equivalence

Definition

An observational bisimulation is a symmetric relation $\mathcal{R}$ between closed extended processes with the same domain such that $A \mathcal{R} B$ implies:

1. if $A \Downarrow a$, then $B \Downarrow a$;
2. if $A \rightarrow^* A'$ and $A'$ is closed, then $B \rightarrow^* B'$ and $A' \mathcal{R} B'$ for some $B'$;

Observational equivalence ($\approx$) is the largest such relation.

- Intuitively, $A \approx B$ when an adversary (evaluation context) cannot distinguish $A$ from $B$.
- Hard to prove because of the universal quantification over all contexts.
  - Use a labeled bisimulation.
A frame \( \varphi \) is an extended process built up from 0 and active substitutions \( \{M/x\} \) by parallel composition and restriction.

The frame of \( A \), \( \varphi(A) \), is obtained replacing every plain process in \( A \) with 0.

**Definition**

Two terms \( M \) and \( N \) are equal in the frame \( \varphi \), written \( (M = N)\varphi \), if and only if

- \( \text{fv}(M) \cup \text{fv}(N) \subseteq \text{dom}(\varphi) \),
- \( \varphi \equiv \nu \tilde{n}.\sigma, M\sigma = N\sigma, \text{ and } \{\tilde{n}\} \cap (\text{fn}(M) \cup \text{fn}(N)) = \emptyset \)

for some names \( \tilde{n} \) and substitution \( \sigma \).

Independent of the representative \( \nu \tilde{n}.\sigma \).
Static equivalence

Definition

Two closed frames $\varphi$ and $\psi$ are statically equivalent, written $\varphi \approx_s \psi$, when

1. $\text{dom}(\varphi) = \text{dom}(\psi)$ and
2. for all terms $M$ and $N$, $(M = N)\varphi$ if and only if $(M = N)\psi$.

Two closed extended processes are statically equivalent, written $A \approx_s B$, when their frames are statically equivalent.

- Static equivalence $\varphi \approx_s \psi$ expresses that the frames cannot be distinguished by performing equality tests.
- $A \approx_s B$ expresses that the current knowledge of the adversary in the processes $A$ and $B$ does not allow it to distinguish $A$ from $B$. The dynamic behavior of $A$ and $B$ is ignored.
The labelled semantics defines $A \xrightarrow{\alpha} A'$ where $\alpha$ is a label:

- $N(M)$: input of $M$ on channel $N$;
- $\nu x. N\langle x \rangle$: output of $x$ on channel $N$.
  $x$ must not occur in $N$.

\[
\begin{align*}
    bv(N(M)) & \overset{\text{def}}{=} \emptyset \quad \text{and} \quad bv(\nu x. N\langle x \rangle) \overset{\text{def}}{=} \{x\}. \\
    fv(N(M)) & \overset{\text{def}}{=} fv(N) \cup fv(M) \quad \text{and} \quad fv(\nu x. N\langle x \rangle) \overset{\text{def}}{=} fv(N).
\end{align*}
\]

The conference paper has labels $\bar{a}\langle u \rangle$ and $\nu u. \bar{a}\langle u \rangle$ for outputs.

- We simplify the semantics by having a single output label.
- One always needs to create a fresh variable for the output message.
- A refined semantics allows $\nu \tilde{u}. N\langle M \rangle$ as label.
Labeled semantics

\[ N(x).P \xrightarrow{N(M)} P\{M/x\} \]

\[ \text{OUT-VAR} \quad x \notin \text{fv}(\bar{N}\langle M \rangle . P) \]

\[ \bar{N}\langle M \rangle . P \xrightarrow{\nu x.\bar{N}\langle x \rangle} P \{M/x\} \]

\[ \text{SCOPE} \quad A \xrightarrow{\alpha} A' \quad u \text{ does not occur in } \alpha \]

\[ \nu u.A \xrightarrow{\alpha} \nu u.A' \]

\[ \text{PAR} \quad A \xrightarrow{\alpha} A' \quad \text{bv}(\alpha) \cap \text{fv}(B) = \emptyset \]

\[ A \parallel B \xrightarrow{\alpha} A' \parallel B \]

\[ \text{STRUCT} \quad A \equiv B \]

\[ B \xrightarrow{\alpha} B' \]

\[ B' \equiv A' \]

\[ A \xrightarrow{\alpha} A' \]
A labelled bisimulation is a symmetric relation $\mathcal{R}$ on closed extended processes such that $A \mathcal{R} B$ implies:

1. $A \approx_s B$;
2. if $A \rightarrow A'$ and $A'$ is closed, then $B \rightarrow^* B'$ and $A' \mathcal{R} B'$ for some $B'$;
3. if $A \overset{\alpha}{\rightarrow} A'$, $A'$ is closed, and $fv(\alpha) \subseteq dom(A)$, then $B \rightarrow^* \overset{\alpha}{\rightarrow} \rightarrow^* B'$ and $A' \mathcal{R} B'$ for some $B'$.

Labelled bisimilarity ($\approx_1$) is the largest such relation.

- Item 1 guarantees that the adversary cannot distinguish $A$ from $B$ using its current knowledge.
- Items 2 and 3 guarantee that this property is preserved by reduction.
Observational equivalence is labelled bisimilarity: $\approx = \approx_1$. 
Bengtson et al’s counter example

\[ A = \nu a. (\{^a/x\} \mid x(y). b\langle M\rangle.0) \quad B = \nu a. (\{^a/x\} \mid 0) \]

- \( A \) and \( B \) are not observationally equivalent
  - The context \( x\langle N\rangle \) distinguishes them.
- According to the POPL’01 paper:
  - \( A \) and \( B \) have the same frame and no transitions,
  - so they are labelled bisimilar.
- A possible fix is to require that exported variables must not be of channel type.
- In our semantics,
  - \( A \) has a labelled transition \( x(N) \),
  - so \( A \) and \( B \) are not labelled bisimilar.
Motivation

- Structural equivalence complicates the analysis of possible reductions in a process.
- In a process $A | B$,
  - substitutions in $A$ may influence the possible reductions in $B$,
  - and conversely, substitutions in $B$ may influence reductions in $A$. 
Partial normal forms

Partial formal form of an extended process $A$:

$$\text{pnf}(A) = \nu \tilde{n}.(\{\tilde{M}/\tilde{x}\} \mid P)$$

with $(fv(P) \cup fv(\tilde{M})) \cap \{\tilde{x}\} = \emptyset$.

Formally defined by induction on $A$.

Lemma

$A \equiv \text{pnf}(A)$. 
Structural equivalence \(\equiv\) on plain processes

- equivalence relation
- closed by application of evaluation contexts

\[
\begin{align*}
\text{Par-0'} & \quad P \parallel 0 \equiv P \\
\text{Par-A'} & \quad P \parallel (Q \parallel R) \equiv (P \parallel Q) \parallel R \\
\text{Par-C'} & \quad P \parallel Q \equiv Q \parallel P \\
\text{Repl'} & \quad !P \equiv P \parallel !P \\
\text{New-0'} & \quad \nu n.0 \equiv 0 \\
\text{New-C'} & \quad \nu n.\nu n'.P \equiv \nu n'.\nu n.P \\
\text{New-Par'} & \quad P \parallel \nu n.Q \equiv \nu n.(P \parallel Q) \quad \text{when } n \not\in fn(P) \\
\text{Rewrite'} & \quad P\{M/x\} \equiv P\{N/x\} \quad \text{when } \Sigma \vdash M = N
\end{align*}
\]
Structural equivalence on partial normal forms

Structural equivalence \( \overset{\circ}{\equiv} \) on extended processes in partial normal form

- equivalence relation

\[
P \overset{\circ}{\equiv} P' \quad (\text{fv}(P) \cup \text{fv}(P')) \cap \text{dom}(\sigma) = \emptyset
\]

\[
\nu \tilde{n}.(\sigma \mid P) \overset{\circ}{\equiv} \nu \tilde{n}.(\sigma \mid P')
\]

\( \tilde{n}' \) is a reordering of \( \tilde{n} \)

\[
\nu \tilde{n}.(\sigma \mid P) \overset{\circ}{\equiv} \nu \tilde{n}'.(\sigma \mid P)
\]

\( n' \notin \text{fn}(\sigma) \)

\[
\nu \tilde{n}.(\sigma \mid \nu n'.P) \overset{\circ}{\equiv} \nu \tilde{n}, n'.(\sigma \mid P)
\]

\[
\text{dom}(\sigma) = \text{dom}(\sigma') \quad \Sigma \vdash x\sigma = x\sigma' \text{ for all } x \in \text{dom}(\sigma)
\]

\[
(\text{fv}(x\sigma) \cup \text{fv}(x\sigma')) \cap \text{dom}(\sigma) = \emptyset \text{ for all } x \in \text{dom}(\sigma)
\]

\[
\nu \tilde{n}.(\sigma \mid P) \overset{\circ}{\equiv} \nu \tilde{n}.(\sigma' \mid P)
\]
Links between structural equivalences

Lemma

- If \( A \equiv B \), then \( \text{pnf}(A) \circ \equiv \text{pnf}(B) \).
- If \( P \hat{\cdot} Q \), then \( P \equiv Q \).
- If \( A \hat{\circ} B \), then \( A \equiv B \).

By induction on the derivations.
Internal reduction

Internal reduction $\rightarrow_{\diamond}$ on plain processes

- closed by $\equiv$

- closed by application of evaluation contexts
  \[
  \text{COMM' } \quad \overline{N}(M).P \mid N(x).Q \rightarrow_{\diamond} P \mid Q\{M/x\}
  \]
  \[
  \text{THEN' } \quad \text{if } M = M \text{ then } P \text{ else } Q \rightarrow_{\diamond} P
  \]
  \[
  \text{ELSE' } \quad \text{if } M = N \text{ then } P \text{ else } Q \rightarrow_{\diamond} Q
  \]
  
  for any ground terms $M$ and $N$

  such that $\Sigma \not\vdash M = N$

Internal reduction $\rightarrow_{\circ}$ on extended processes in partial normal form

- closed by $\equiv$

- $P \rightarrow_{\circ} P'$

- $\nu\tilde{n}.(\sigma \mid P) \rightarrow_{\circ} \nu\tilde{n}.(\sigma \mid P')$
Link between internal reductions

Lemma

- If $A \rightarrow B$, then $\text{pnf}(A) \rightarrow \circ \text{pnf}(B)$.
- If $P \rightarrow \circ Q$, then $P \rightarrow Q$.
- If $A \rightarrow \circ B$, then $A \rightarrow B$.

By induction on the derivations.
Labelled reduction on plain processes

Labelled reduction $P \xrightarrow{\alpha} A$ on plain processes

**I**n

$$N(x).P \xrightarrow{N(M)} P\{M/x\}$$

**O**ut-**V**ar

$$\begin{align*}
N(M).P & \xrightarrow{\nu x.\overline{N}⟨x⟩} P\{M/x\} \\
x & \notin \text{fv}(\overline{N}⟨M⟩.P)
\end{align*}$$

**S**cope

$$\begin{align*}
P & \xrightarrow{\alpha} A \\
n & \text{does not occur in } \alpha
\end{align*}$$

**Par**

$$\begin{align*}
P & \xrightarrow{\alpha} A \\
\text{bv}(\alpha) \cap \text{fv}(Q) & = \emptyset
\end{align*}$$

**S**truct

$$\begin{align*}
P & \equiv Q \\
Q & \xrightarrow{\alpha} B \\
B & \equiv A
\end{align*}$$

Bruno Blanchet (INRIA) 
Applied pi calculus 
April 2015
Labelled reduction $A \overset{\alpha}{\to} B$, where

- $A$ is an extended process in partial normal form and
- $B$ is an extended process

$$A \equiv \nu \tilde{n}.(\sigma | P) \quad P \overset{\alpha'}{\to} B' \quad B \equiv \nu \tilde{n}.(\sigma | B')$$

$$fv(\sigma) \cap bv(\alpha') = \emptyset \quad \Sigma \vdash \alpha \sigma = \alpha'$$

the elements of $\tilde{n}$ do not occur in $\alpha$

$$A \overset{\alpha}{\to} B$$
Links between labelled reductions

**Lemma (Characterization of labelled reductions)**

\[ P \overset{\alpha}{\rightarrow} \diamond A \text{ if and only if for some } \tilde{n}, P_1, P_2, A_1, N, M, P', x, \]

\[ P \equiv \nu\tilde{n}.(P_1 \mid P_2), A \equiv \nu\tilde{n}.(A_1 \mid P_2), \{\tilde{n}\} \cap \text{fn}(\alpha) = \emptyset, \]

\[ \text{bv}(\alpha) \cap \text{fv}(P_1 \mid P_2) = \emptyset, \text{ and one of the following two cases holds:} \]

1. \( \alpha = N(M), P_1 = N(x).P', \text{ and } A_1 = P'\{M/x\}; \) or

2. \( \alpha = \nu x.N\langle x \rangle, P_1 = N\langle M \rangle. P', \text{ and } A_1 = P'\mid\{M/x\}. \)

**Lemma**

- If \( A \overset{\alpha}{\rightarrow} B, \text{ then } \text{pnf}(A) \overset{\alpha}{\rightarrow} \diamond B. \)
- If \( P \overset{\alpha}{\rightarrow} \diamond A, \text{ then } P \overset{\alpha}{\rightarrow} A. \)
- If \( A \overset{\alpha}{\rightarrow} \diamond B, \text{ then } A \overset{\alpha}{\rightarrow} B. \)
Lemma

Suppose that $P_0$ is closed, $\alpha$ is $\nu x.\overline{N}'\langle x \rangle$ or $N'(M')$ for some ground term $N'$, and $P_0 \xrightarrow{\alpha} A$. Then one of the following cases holds:

1. $P_0 = P \mid Q$ and either $P \xrightarrow{\alpha} A'$ and $A \equiv A' \mid Q$, or $Q \xrightarrow{\alpha} A'$ and $A \equiv P \mid A'$, for some $P$, $Q$, and $A'$;

2. $P_0 = \nu n.P$, $P \xrightarrow{\alpha} A'$, and $A \equiv \nu n.A'$ for some $P$, $A'$, and $n$ that does not occur in $\alpha$;

3. $P_0 = !P$, $P \xrightarrow{\alpha} A'$, and $A \equiv A' \mid !P$ for some $P$ and $A'$;

4. $P_0 = N(x).P$, $\alpha = N'(M')$, $\Sigma \vdash N \equiv N'$, and $A \equiv P\{M'/x\}$ for some $N$, $x$, $P$, $N'$, and $M'$;

5. $P_0 = \overline{N}\langle M \rangle.P$, $\alpha = \nu x.\overline{N}'\langle x \rangle$, $\Sigma \vdash N \equiv N'$, $x \notin \text{fv}(P_0)$, and $A \equiv P\{M'/x\}$ for some $N$, $M$, $P$, $x$, and $N'$. 
Lemma

If

- $\nu\tilde{n}.(\sigma \mid P)$ is a closed extended process in partial normal form,
- $\nu\tilde{n}.(\sigma \mid P) \xrightarrow{\alpha} A$,
- $fv(\alpha) \subseteq dom(\sigma)$, and
- the elements of $\tilde{n}$ do not occur in $\alpha$,

then $P \xrightarrow{\alpha\sigma} A'$, $A \equiv \nu\tilde{n}.(\sigma \mid A')$, and $bv(\alpha) \cap dom(\sigma) = \emptyset$ for some $A'$. 
Composition of labelled reductions

Lemma

If

• \( P \) and \( Q \) are closed processes, \( N \) is a ground term,
• \( P \xrightarrow{N(x)} A \), and
• \( Q \xrightarrow{\nu x.\overline{N(x)}} B \),

then \( P | Q \xrightarrow{\circ} R \) and \( R \equiv \nu x.(A \mid B) \) for some \( R \).
Suppose that $P_0$ is a closed process and $P_0 \rightarrow_R$. Then one of the following cases holds:

1. $P_0 = P \mid Q$ for some $P$ and $Q$, and one of the following cases holds:
   1. $P \rightarrow_R P'$ and $R \equiv P' \mid Q$ for some closed process $P'$,
   2. $P \xrightarrow{N(x)} A$, $Q \xrightarrow{\nu x.N(x)} B$, and $R \equiv \nu x.(A \mid B)$ for some $A$, $B$, $x$, and ground term $N$,

   and two symmetric cases obtained by swapping $P$ and $Q$;

2. $P_0 = \nu n.P$, $P \rightarrow_R Q'$, and $R \equiv \nu n.Q'$ for some $n$ and some closed processes $P$ and $Q'$;

3. $P_0 = !P$, $P \mid P \rightarrow_R Q'$, and $R \equiv Q' \mid !P$ for some closed processes $P$ and $Q'$.

4. $P_0 = \text{if } M = N \text{ then } P \text{ else } Q$ and either $\Sigma \vdash M = N$ and $R \equiv P$, or $\Sigma \vdash M \neq N$ and $R \equiv Q$, for some $M$, $N$, $P$, and $Q$. 

Decomposition of internal reductions: partial normal forms

Lemma

If

- $\nu \tilde{n}.\left(\sigma \mid P\right)$ is a closed extended process in partial normal form and
- $\nu \tilde{n}.\left(\sigma \mid P\right) \rightarrow_{} A$,

then $P \rightarrow_{} P'$ and $A \equiv \nu \tilde{n}.\left(\sigma \mid P'\right)$ for some closed process $P'$. 

Bruno Blanchet (INRIA)
Applied pi calculus
April 2015 36 / 47
Proof technique

- Induction on the derivations.
- Strengthen the inductive invariant, to be able to apply the current lemma to a derivation built as a result of applying the inductive hypothesis.
Static equivalence

Lemma

*Static equivalence is*
- invariant by structural equivalence and reduction, and
- closed by application of closing evaluation contexts.

For the second point,
- show that we can restrict ourselves to contexts $E = \nu \tilde{u}.(\_ | C)$ such that all subcontexts of $E$ are closing.
- proceed by structural induction on $E$. 
Context closure

Lemma

\( \approx_1 \) is closed by application of closing evaluation contexts.

- Restrict attention to contexts of the form \( \nu\tilde{u}.(\_ | C) \).
- To every relation \( \mathcal{R} \) on closed extended processes, we associate \( \mathcal{R}' = \{(\nu\tilde{u}.(A | C), \nu\tilde{u}.(B | C)) | A \mathcal{R} B, \nu\tilde{u}.(\_ | C) \text{ closing for } A \text{ and } B \}\).
- We prove that, if \( \mathcal{R} \) is a labelled bisimulation, then \( \mathcal{R}' \) is a labelled bisimulation up to \( \equiv \), hence \( \mathcal{R} \subseteq \mathcal{R}' \subseteq \approx_1 \).
- For \( \mathcal{R} = \approx_1 \), this property entails that \( \approx_1 \) is closed by application of evaluation contexts \( \nu\tilde{u}.(\_ | C) \).
Context closure

- To every relation $\mathcal{R}$ on closed extended processes, we associate $\mathcal{R}' = \{(\nu \tilde{u}.(A \mid C), \nu \tilde{u}.(B \mid C)) \mid A \mathcal{R} B, \nu \tilde{u}.(\_ \mid C)$ closing for $A$ and $B\}$.
- We prove that, if $\mathcal{R}$ is a labelled bisimulation, then $\mathcal{R}'$ is a labelled bisimulation up to $\equiv$.

**Definition**

A relation $\mathcal{R}$ on closed extended processes is a labelled bisimulation up to $\equiv$ if and only if $\mathcal{R}$ is symmetric and $A \mathcal{R} B$ implies:

1. $A \approx_s B$;
2. if $A \rightarrow A'$ and $A'$ is closed, then $B \rightarrow^* B'$ and $A' \equiv \mathcal{R} \equiv B'$ for some closed $B'$;
3. if $A \overset{\alpha}{\rightarrow} A'$, $A'$ is closed, and $fv(\alpha) \subseteq \text{dom}(A)$, then $B \rightarrow^* \overset{\alpha}{\rightarrow} \rightarrow^* B'$ and $A' \equiv \mathcal{R} \equiv B'$ for some closed $B'$. 
Context closure

To every relation $\mathcal{R}$ on closed extended processes, we associate $\mathcal{R}' = \{(\nu\tilde{u}.(A \mid C), \nu\tilde{u}.(B \mid C)) \mid A \mathcal{R} B, \nu\tilde{u}.(\_ \mid C) \text{ closing for } A \text{ and } B\}$.

We prove that, if $\mathcal{R}$ is a labelled bisimulation, then $\mathcal{R}'$ is a labelled bisimulation up to $\equiv$.

Assume $S \mathcal{R}' T$, with $S = \nu\tilde{u}.(A \mid C)$, $T = \nu\tilde{u}.(B \mid C)$, and $A \mathcal{R} B$.

- $S \approx_s T$ follows from $A \approx_s B$ by a previous lemma.
- For reductions, consider the partial normal forms of $A$, $B$, $C$:
  \[
  \text{pnf}(A) = \nu\tilde{n}.(\sigma \mid P), \quad \text{pnf}(B) = \nu\tilde{n}'.(\sigma' \mid P'), \quad \text{pnf}(C) = \nu\tilde{n}''.(\sigma'' \mid P'').
  \]

A reduction on $S = \nu\tilde{u}.(A \mid C)$ implies a reduction on $P \mid P''\sigma$, so a reduction on $P$ and/or $P''\sigma$ (by the decomposition lemmas).

A reduction on $P$ implies a reduction $A$, so the same reduction on $B$ since $\mathcal{R}$ is a labelled bisimulation, so a reduction on $P'$.

A reduction on $P''\sigma$ implies a reduction on $P''\sigma'$ by static equivalence $A \approx_s B$.

Hence we obtain a reduction on $P' \mid P''\sigma'$, hence on $T = \nu\tilde{u}.(B \mid C)$.
Characterizing barbs

**Lemma**

Let $A$ be a closed extended process.

$A \Downarrow a$ if and only if $A \rightarrow^* \nu x.a\langle x\rangle \Rightarrow A'$ for some fresh variable $x$ and some $A'$.

$A \equiv E[a\langle M\rangle.P]$ for some evaluation context $E[\_]$ that does not bind $a$ if and only if

$A \nu x.a\langle x\rangle \Rightarrow A'$ for some fresh variable $x$ and some $A'$. 
Lemma

\[ \approx_l \subseteq \approx. \]

\( \approx_l \) satisfies the three properties of observational bisimulations:

1. \( \approx_l \) preserves barbs, by characterization of barbs and Properties 2 and 3 of a labelled bisimulation.

2. Suppose that \( A \approx_l B, A \rightarrow^* A' \), and \( A' \) is closed. Close all intermediate processes in \( A \rightarrow^* A' \), then conclude that \( B \rightarrow^* B' \) and \( A' \approx_l B' \) for some \( B' \) by Property 2 of a labelled bisimulation.

3. \( \approx_l \) is closed by application of closing evaluation contexts, as shown previously.

Moreover, \( \approx_l \) is symmetric. Since \( \approx \) is the largest observational bisimulation, we obtain \( \approx_l \subseteq \approx \).
Observational equivalence implies static equivalence

Lemma

≈ ⊆ ≈ₜ.

If $A$ and $B$ are observationally equivalent, then $A \mid C$ and $B \mid C$ have the same barb $\Downarrow a$ for every $C = \text{if } M = N \text{ then } \overline{a}\langle s \rangle$, where $a$ does not occur in $A$ or $B$ and $\text{fv}(M) \cup \text{fv}(N) \subseteq \text{dom}(A)$.

Assuming that $A$ is closed, $\text{fv}(M) \cup \text{fv}(N) \subseteq \text{dom}(A)$, and $a$ does not occur in $A$, we have

$(M = N)\varphi(A)$ if and only if $A \mid \text{if } M = N \text{ then } \overline{a}\langle s \rangle \Downarrow a$.

(Shown using partial normal forms.)
Let $T^p_{N(M)} \overset{\text{def}}{=} \overline{p}(p) \mid \overline{N}(M).p(x)$. 

**Lemma**

Let $A$ be a closed extended process. Let $N$ and $M$ be terms such that $\text{fv}(\overline{N}(M)) \subseteq \text{dom}(A)$ and $p$ does not occur in $A$, $M$, and $N$.

- If $A \xrightarrow{N(M)} A'$ and $p$ does not occur in $A'$, then $A \mid T^p_{N(M)} \rightarrow A'$ and $A' \not\Downarrow p$.

- If $A \mid T^p_{N(M)} \rightarrow^* A'$ and $A' \not\Downarrow p$, then $A \rightarrow^* N(M) \rightarrow^* A'$. 

Shown using partial normal forms.
Characterizing outputs

Let \( T_{\nu x.N\langle x\rangle}^{p,q} \overset{\text{def}}{=} p\langle p\rangle | N(x).p(y).q\langle x\rangle \).  

Lemma

Let \( A \) be a closed extended process and \( N \) such that \( \text{fv}(N) \subseteq \text{dom}(A) \).

- If \( A \xrightarrow{\nu x.N\langle x\rangle} A' \) and \( p \) and \( q \) do not occur in \( A, A', \) and \( N \), then \( A | T_{\nu x.N\langle x\rangle}^{p,q} \rightarrow \nu x.(A' | q\langle x\rangle), \nu x.(A' | q\langle x\rangle) \not\Downarrow p, \) and \( x \notin \text{dom}(A) \).
- If \( A | T_{\nu x.N\langle x\rangle}^{p,q} \rightarrow^* A'' \), \( A'' \not\Downarrow p, x \notin \text{dom}(A), \) and \( p \) and \( q \) do not occur in \( A \) and \( N \), then \( A \rightarrow^* \nu x.N\langle x\rangle \rightarrow^* A' \) and \( A'' \equiv \nu x.(A' | q\langle x\rangle) \) for some \( A' \).

Shown using partial normal forms.
Lemma (Extrusion)

Let $A$ and $B$ two closed extended processes with a same domain that contains $\tilde{x}$. Let $E_{\tilde{x}}[-] \overset{\text{def}}{=} \nu \tilde{x}. (\prod_{x \in \tilde{x}} n_x(x) | -)$ using names $n_x$ that do not occur in $A$ or $B$. If $E_{\tilde{x}}[A] \approx E_{\tilde{x}}[B]$, then $A \approx B$.

If $A$ is a closed extended process with $\{\tilde{x}\} \subseteq \text{dom}(A)$ and $E_{\tilde{x}}[A] \rightarrow C'$, then $A \rightarrow A'$ and $C' \equiv E_{\tilde{x}}[A']$ for some closed extended process $A'$.

(Proved using partial normal forms.)

Let $A R B$ if and only if $\{\tilde{x}\} \subseteq \text{dom}(A) = \text{dom}(B)$ and $E_{\tilde{x}}[A] \approx E_{\tilde{x}}[B]$, for some $\tilde{x}$ and some names $\tilde{n}_x$ that do not occur in $A$ or $B$.

We show that $R$ is an observational bisimulation.
Observational equivalence implies labelled bisimilarity

The relation $\approx$ is symmetric. It satisfies the three properties of labelled bisimulations:

1. If $A \approx B$, then $A \approx_s B$, shown previously.
2. If $A \approx B$, $A \xrightarrow{\alpha} A'$, and $A'$ is closed, then $B \xrightarrow{\ast} B'$ and $A' \approx B'$ for some $B'$, by Property 2 of the definition of observational bisimulation.
3. If $A \approx B$, $A \overset{\alpha}{\xrightarrow{\ast}} A'$, $A'$ is closed, and $\text{fv}(\alpha) \subseteq \text{dom}(A)$, then $B \overset{\ast}{\xrightarrow{\alpha}} B'$ and $A' \approx B'$ for some $B'$. To prove this property, we rely on characteristic parallel contexts $T_\alpha$, shown in previous lemmas. In the output case, we obtain a pair $\nu x.(A' \mid \overline{q}\langle x \rangle) \approx \nu x.(B' \mid \overline{q}\langle x \rangle)$, and conclude by the extrusion lemma.

Hence $\approx$ is a labelled bisimulation, and $\approx \subseteq \approx_\ell$, since $\approx_\ell$ is the largest labelled bisimulation.
Conclusion

- Importance of **detailed proofs**.
  - Could be interesting to formalize in a theorem prover, e.g. Coq.
- **Partial normal forms** are likely to be useful for proving many other results about the applied pi calculus.
- With the minor changes we made, one should be able to show that
  - The plain processes of the applied pi calculus are a subset of the ProVerif input language.
  - The semantics and the notions of observational equivalence match.
- Does anybody want to read the draft?