



HAL
open science

Name-passing calculi: from fusions to preorders and types, Appendix

Daniel Hirschhoff, Jean-Marie Madiot, Davide Sangiorgi

► **To cite this version:**

Daniel Hirschhoff, Jean-Marie Madiot, Davide Sangiorgi. Name-passing calculi: from fusions to preorders and types, Appendix. 2013. hal-00818068v1

HAL Id: hal-00818068

<https://inria.hal.science/hal-00818068v1>

Preprint submitted on 26 Apr 2013 (v1), last revised 11 May 2013 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Name-passing calculi: from fusions to preorders and types (Appendix)

Daniel Hirschhoff, Jean-Marie Madiot

ENS Lyon, U. de Lyon, CNRS, INRIA, UCBL
{daniel.hirschhoff, jeanmarie.madiot}@ens-lyon.fr

Davide Sangiorgi

University of Bologna and INRIA
davide.sangiorgi@cs.unibo.it

This is the appendix of the paper “Name-passing calculi: from fusions to preorders and types” (D Hirschhoff, JM. Madiot, D. Sangiorgi), to appear in LICS’2013.

APPENDIX

A. Reduction-closed barbed congruence

Definition 1 (Reduction-closed barbed congruence). *Let \mathcal{L} be a process calculus, in which a reduction relation $\longrightarrow_{\mathcal{L}}$ and barb predicates $\downarrow_a^{\mathcal{L}}$, for each a in a given set of names, have been defined.*

A relation \mathcal{R} on the processes of \mathcal{L} is context-closed if PRQ implies $C[P]RC[Q]$, for each context C of \mathcal{L} ; the relation is barb-preserving if for any name a , $P \downarrow_a^{\mathcal{L}}$ implies $Q \downarrow_a^{\mathcal{L}}$; it is reduction-closed if whenever $P \longrightarrow_{\mathcal{L}} P'$, there is Q' s.t. $Q \longrightarrow_{\mathcal{L}} Q'$ and $P'RQ'$.

Then reduction-closed barbed congruence in \mathcal{L} , written $\simeq_{\mathcal{L}}$, is the largest symmetric relation on the processes of \mathcal{L} that is context-closed, reduction-closed, and barb-preserving.

B. Proofs of impossibility results

Statement of Theorem ??: *A typed calculus with fusions that is plain and supports narrowing has trivial subtyping.*

Proof Sketch: We define the following active context:

$$E \triangleq (\nu cb)(\bar{u}b \mid uc \mid \bar{v}a \mid vc \mid [\cdot]) .$$

Note that in E we only use b as an output object. The intention is that, given some process P , and u, v, c some fresh names, $E[P]$ should reduce to $P\{a/b\}$. Indeed, by applying hypothesis (??) twice, we have

$$E[P] = (\nu bc)(\bar{u}b \mid \bar{v}a \mid uc \mid vc \mid P) \quad (1)$$

$$\implies (\nu b)(\bar{v}a \mid vb \mid P\{b/c\}) \quad (2)$$

$$= (\nu b)(\bar{v}a \mid vb \mid P) \quad (3)$$

$$\implies P\{a/b\} . \quad (4)$$

Suppose $U \leq T$, we show $\Gamma, a : T \vdash P$ iff $\Gamma, a : U \vdash P$. The implication from left to right is narrowing. To prove the right to left implication, suppose $\Gamma, a : U \vdash P$, and prove $\Gamma, a : T \vdash P$. By injective name substitution we have $\Gamma, b : U \vdash P\{b/a\}$ for some fresh b .

In the typing environment $\Gamma, b:U, u:\sharp T, v:\sharp T, c:T, a:T$ the process $\bar{u}b$ is well-typed thanks to narrowing and weakening, hence so is $(\bar{u}b \mid uc \mid \bar{v}a \mid vc \mid P\{b/a\})$. By the restriction rule we get $\Gamma, a:T, u:\sharp T, v:\sharp T \vdash E[P\{b/a\}]$, the latter reducing to $P\{b/a\}\{a/b\}$ by (4). Since b has been taken fresh, $P\{b/a\}\{a/b\} = P$. Hence, by Subject Reduction, $\Gamma, a:T, u:\sharp T, v:\sharp T \vdash P$. We finally deduce $\Gamma, a : T \vdash P$ by Strengthening. \blacksquare

Statement of Theorem ??: *Suppose a typed calculus with fusions is plain and there is at least one prefix α with object b , different from the subject, and there are two types S and T such that $S \leq T$ and one of the following forms of narrowing holds for all Γ :*

- 1) *whenever $\Gamma, b : T \vdash \alpha. \mathbf{0}$, we also have $\Gamma, b : S \vdash \alpha. \mathbf{0}$;*
- 2) *whenever $\Gamma, b : S \vdash \alpha. \mathbf{0}$, we also have $\Gamma, b : T \vdash \alpha. \mathbf{0}$.*

Then S and T are interchangeable in all typing judgements.

Proof Sketch: For all Δ we prove that $\Delta, x : T \vdash P$ iff $\Delta, x : S \vdash P$. Let x_1, x_2, a_1 and a_2 be fresh names.

$$\Delta_i \stackrel{\text{def}}{=} \Delta, x_i : T, x_{3-i} : S$$

We will prove that $\Delta_i \vdash P\{x_1/x\}$ implies $\Delta_i \vdash P\{x_2/x\}$ for all $i \in \{1, 2\}$. From there it is enough to conclude using weakening, strengthening and injective substitutions. We use $D = \bar{a}_1x_1 \mid \bar{a}_2x_2 \mid a_1y \mid a_2y$ to simulate a substitution:

$$(\nu x_1y)(D \mid P\{x_1/x\}) \Rightarrow P\{x_2/x\}$$

We have to prove that $\Delta' = \Delta_i, a_1 : T_{a_1}, a_2 : T_{a_2}, y : T_y \vdash D$ for some types T_{a_1}, T_{a_2}, T_y . We note a the subject of α . Using the plainness of the subtyping, we can suppose that a is any of a_1 or a_2 and that b is any of x_1, x_2 or y , so to apply the hypothesis on different cases. There are eight subcases, along the cases from the hypothesis, i , and the form of α .

- (1), $i = 1$, $\alpha = \bar{a}_2x_2$: $T_{a_1} = T_{a_2} = \sharp T, T_y = T$;
- (1), $i = 1$, $\alpha = a_1y$: $T_{a_1} = \sharp T, T_{a_2} = \sharp S, T_y = S$;
- (2), $i = 1$, $\alpha = \bar{a}_1x_1$: $T_{a_1} = T_{a_2} = \sharp S, T_y = S$;
- (2), $i = 1$, $\alpha = a_2y$: $T_{a_1} = \sharp T, T_{a_2} = \sharp S, T_y = T$;
- (1), $i = 2$, $\alpha = \bar{a}_2x_2$: $T_{a_1} = T_{a_2} = \sharp T, T_y = T$;
- (1), $i = 2$, $\alpha = a_2y$: $T_{a_1} = \sharp S, T_{a_2} = \sharp T, T_y = S$;
- (2), $i = 2$, $\alpha = \bar{a}_1x_1$: $T_{a_1} = T_{a_2} = \sharp S, T_y = S$;

- (2), $i = 2$, $\alpha = a_1y$: $T_{a_1} = \sharp S$, $T_{a_2} = \sharp T$, $T_y = T$.

In all these cases we prove that $\Delta' \vdash D$ using plainness and the hypothesis on α . Plainness also give us $\Delta' \vdash P\{x_1/x\}$. We use rules from (??) and Subject Reduction to get that $\Delta' \vdash P\{x_2/x\}$ from which strengthening is enough to conclude. ■

C. Structural congruence in πP

Definition 2 (Structural congruence). *Structural congruence on πP , written \equiv , is the smallest congruence containing the associativity and commutativity of $|$ and the following rules:*

$$P \mid \mathbf{0} \equiv P \quad \nu a \mathbf{0} \equiv \mathbf{0} \quad \nu a \nu b P \equiv \nu b \nu a P$$

$$\nu a(P \mid Q) \equiv (\nu a P) \mid Q \text{ if } a \notin \text{fn}(Q)$$

D. Alternative definition of Υ

Given an active context E , the set of *captured names* of E , $\text{cn}(E)$, is defined as follows: $c \in \text{cn}(E)$ iff the hole occurs in the scope of a restriction on c in E ($\text{cn}(E)$ is included in the set of names that are bound in E , but might be distinct from it).

Definition 3 (Reachability / Joinability of names). *We introduce $\varphi ::= a \leq b \mid a \Upsilon b$ in which $a \leq b$ is read “ b is reachable from a ”, and $a \Upsilon b$ is read “ a and b are joinable”. In both cases, we have $\text{n}(\varphi) = \{a, b\}$. We first define a judgement $\varphi_1, \varphi_2 \vdash \varphi$, as follows:*

$$\frac{}{a \leq b, b \leq c \vdash a \leq c} \quad \frac{}{a \leq c, b \leq c \vdash a \Upsilon b}$$

$$\frac{}{a \Upsilon b, c \leq a \vdash c \Upsilon b} \quad \frac{}{a \Upsilon b, c \leq b \vdash a \Upsilon c} \quad \frac{\varphi_1, \varphi_2 \vdash \varphi}{\varphi_2, \varphi_1 \vdash \varphi}$$

We exploit this judgement to define how $a \leq b$ and $a \Upsilon b$ can be derived according to a process, or to an active context (we use $A ::= P \mid E$):

$$\frac{\text{REFL}}{A \triangleright a \leq a} \quad \frac{\text{DEDUCT}}{A \triangleright \varphi_1 \quad A \triangleright \varphi_2 \quad \varphi_1, \varphi_2 \vdash \varphi}{A \triangleright \varphi}$$

Then we define \triangleright for processes:

$$\frac{}{b/a \triangleright a \leq b} \quad \frac{P \triangleright \varphi}{P \mid R \triangleright \varphi} \quad \frac{P \triangleright \varphi}{R \mid P \triangleright \varphi}$$

$$\frac{P \triangleright \varphi \quad a \notin \text{n}(\varphi)}{(\nu a)P \triangleright \varphi}$$

and for contexts (symmetrically for $E \mid P$):

$$\frac{P \triangleright \varphi \quad \text{n}(\varphi) \cap \text{cn}(E) = \emptyset}{P \mid E \triangleright \varphi} \quad \frac{E \triangleright \varphi}{P \mid E \triangleright \varphi} \quad \frac{E \triangleright \varphi}{(\nu a)E \triangleright \varphi}$$

Lemma 4. *If P is a πP process, the relation \leq_P defined by $\{(a, b) \mid P \triangleright a \leq b\}$ is a preorder.*

Proof: Thanks to the rule REFL, \leq_P is reflexive and thanks to the rule DEDUCT and the fact that $a \leq b, b \leq c \vdash a \leq c$, \leq_P is transitive, hence it is a preorder. ■

E. Coincidence of eager and by-need equivalences in $\pi P1$

Statement of Theorem ??: $\approx_{\pi P1bn} = \approx_{\pi P1ea}$.

Proof Sketch: The result follows from reflexivity of a relation we define below, between processes in the eager semantics and processes in the by-need semantics.

Lemma 5. *For $P \in \pi P1$, we write $Eq(P)$ for the relation between names defined by $Eq(P)(a, b)$ iff $P \triangleright a \Upsilon b$.*

Then $Eq(P)$ is an equivalence relation.

Let \mathcal{R} be the relation such that $P \mathcal{R} Q$ iff

$$P, Q \in \pi P1 \wedge Eq(P) = Eq(Q) = \varphi \wedge P =_{\varphi} Q$$

where $P =_{\varphi} Q$ iff P is obtained from Q by replacing some subjects in active prefixes with names related by $Eq(P)$.

We prove that $P \mathcal{R} Q$ entails the following:

- 1) if $C[P], C[Q] \in \pi P1$ then $C[P] \mathcal{R} C[Q]$,
- 2) $P \Downarrow_a^{\text{ea}}$ iff $Q \Downarrow_a^{\text{bn}}$,
- 3) if $P \Longrightarrow_{\text{ea}} P'$ then $Q \Longrightarrow_{\text{bn}} Q'$ with $P' \mathcal{R} Q'$,
- 4) if $Q \Longrightarrow_{\text{bn}} Q'$ then $P \Longrightarrow_{\text{ea}} P'$ with $P' \mathcal{R} Q'$.

We call the union of relations satisfying these properties the *eager/by-need weak reduction-closed barbed congruence* for $\pi P1$, written $\overset{\text{ea}}{\underset{1}{\approx}} \overset{\text{bn}}{\underset{1}{\approx}}$.

- 1) \mathcal{R} is clearly context-closed in $\pi P1$.
- 2) $P \Downarrow_a^{\text{bn}}$ implies $P \Downarrow_a^{\text{ea}}$ as each arc involved in the joinability condition generates a $\longrightarrow_{\text{ea}}$ reduction, and $P \Downarrow_a^{\text{ea}}$ implies $P \Downarrow_a^{\text{bn}}$, as $P \longrightarrow_{\text{ea}} P'$ implies $P \longrightarrow_{\text{bn}} P'$.
- 3) By induction we suppose $P \longrightarrow_{\text{ea}} P'$. If this is a renaming then $P =_{\varphi} P'$. If this is a communication then the corresponding subjects are equated by φ in Q , which means they are joinable i.e. the by need reduction is possible.
- 4) Again we suppose $Q \longrightarrow_{\text{bn}} Q'$, with a communication on a and b with $a \Upsilon b$. The corresponding names a', b' in P are such that $a' \Upsilon a \Upsilon b \Upsilon b'$ i.e. $a' \Upsilon b'$ so a' and b' can be rewritten into a common name, letting the communication happen.

Since $\mathcal{R} \subseteq \overset{\text{ea}}{\underset{1}{\approx}} \overset{\text{bn}}{\underset{1}{\approx}}$, for all $P \in \pi P1$ we have $P \overset{\text{ea}}{\underset{1}{\approx}} \overset{\text{bn}}{\underset{1}{\approx}} P$ which implies that $P \approx_{\pi P1bn} Q$ iff $P \approx_{\pi P1ea} Q$. ■

F. The Fusion calculus

Definition 6. *The syntax of the polyadic Fusion calculus [6] without matching and choice is the following. Structural congruence is defined as usual (Definition 2).*

$$P ::= \mathbf{0} \mid P \mid P \mid \tilde{a}\tilde{x}.P \mid a\tilde{x}.P \mid \nu a P$$

We follow the reduction semantics of the Fusion calculus, from [22]. The side conditions for (5) are that \tilde{x} and \tilde{y} are of the same arity, that $\text{dom}(\sigma) = \tilde{z}$ and that $\sigma(x_i) = \sigma(y_i)$. Note that (??), from Section ??, holds.

$$\frac{P \equiv P_1 \quad P_1 \rightarrow_F Q_1 \quad Q_1 \equiv Q}{P \rightarrow_F Q} \quad \frac{P \rightarrow_F Q}{E[P] \rightarrow_F E[Q]}$$

$$(\nu \tilde{z})(R \mid a\tilde{x}.P \mid \tilde{a}\tilde{y}.Q) \rightarrow_F (R \mid P \mid Q)\sigma \quad (5)$$

G. Auxiliary results

a) Results involving name preorders:

Lemma 7. *If $P \triangleright a \curlywedge b$ and $\{a, b\} \subseteq \text{fn}(P)$, then $P \equiv P'$ implies $P' \triangleright a \curlywedge b$.*

Proof: The predicate $P \triangleright \varphi$ only depends on the occurrences of arcs in P ; those occurrences are trivially preserved by structural congruence, except that to keep track of alpha-conversion one must consider that P 's binders also bind φ 's names. Hence the statement only holds for free names. ■

Lemma 8. *If $P \simeq_{\text{bn}} Q$ and $P \triangleright a \curlywedge b$. Then $Q \triangleright a \curlywedge b$.*

Proof: We characterise joinability using the context $E = (- \mid \bar{a}.f \mid b.g)$ where f and g are fresh: we easily prove that $R \triangleright a \curlywedge b$ iff $E[R] \longrightarrow_{\text{bn}} R_1$ where $R_1 \downarrow_f^{\text{bn}}$ and $R_1 \downarrow_g^{\text{bn}}$. By definition of \simeq_{bn} we know that $E[P] \simeq_{\text{bn}} E[Q]$ and we conclude playing the bisimulation game of \simeq_{bn} . ■

Lemma 9. *If $P \mathcal{R} Q$ and \mathcal{R} preserves \curlywedge and parallel composition of arcs (in particular if \mathcal{R} is a \sim_{bn} -relation), then $P \triangleright a \leq b$ iff $Q \triangleright a \leq b$.*

Proof: Let P and Q be processes and f be a fresh name. Then $P \triangleright a \leq b$ iff $(P \mid f/b) \triangleright a \curlywedge f$ and similarly for Q . Thanks to the second hypothesis on \mathcal{R} we have $(P \mid f/b) \mathcal{R} (Q \mid f/b)$ and we conclude with the second one. ■

b) Basic tools: Prefixes delimit the action of structural congruence.

Lemma 10. *Suppose π_1, π_2 are prefixes.*

- 1) *If $E[\pi_1.P_1] \equiv P'$ then there exist E' and P'_1 such that $P_1 \equiv P'_1$, $P' = E'[\pi_1.P'_1]$ and $E \triangleright a \curlywedge b$ iff $E' \triangleright a \curlywedge b$. Moreover for all Q_1 such that all names of $\text{fn}(Q_1)$ are either in $\text{fn}(P_1)$ or not captured by E then the latter are not captured by E' and $E[Q_1] \equiv E'[Q_1]$.*
- 2) *If $G[\pi_1.P_1][\pi_2.P_2] \equiv P'$ then there exist G', P'_1 and P'_2 such that $P_1 \equiv P'_1$, $P_2 \equiv P'_2$ and $P' = G'[\pi_1.P_1][\pi_2.P_2]$ or $P' = G'[\pi_2.P_2][\pi_1.P_1]$ and $G \triangleright a \curlywedge b$ iff $G' \triangleright a \curlywedge b$.*

Proof: Structural congruence can act under prefixes only using the fact that \equiv is a congruence, i.e. using the rule “if $P \equiv P'$ then $C[P] \equiv C[P']$ ” for some arbitrary context C containing a prefix. For this rule we work an induction on C to get the same cutting as $E[\pi_1.P_1]$; all the other rules deriving \equiv are handled by the corresponding case analysis on the context E . Note that the statement also holds when E is an arbitrary context. ■

Lemma 11. *If $P \equiv Q$ then $P \sim_{\text{bn}} Q$.*

Proof: We show that \equiv is a \sim_{bn} -bisimulation. (The proof is not by induction over the derivation of $P \equiv Q$ because the fact that \equiv is a congruence is not easy to handle.) The clauses 1), 2), 4) are easy – respectively handled by the fact that \equiv is a congruence, Lemma 7 and the fact that \equiv is symmetric – as is the clause 3) when $\mu = \tau$ – since $\xrightarrow{\tau}_{\text{bn}} = \longrightarrow_{\text{bn}}$ is stable by \equiv . For the remaining labels we examine the case where $\mu = \hat{b}d$,

the other case being similar. We know that $P = E[ac.P_1]$ with $E \triangleright a \curlywedge b$ and $P' = E[d/c \mid P_1]$. We use Lemma 10 to get $Q = E'[ac.P_1]$ which implies $Q \xrightarrow{\hat{b}d} E'[d/c \mid P_1] \equiv P'$. ■

c) Proof techniques:

Definition 12 (By-need bisimulation up to \sim_{bn} and restriction). *A relation \mathcal{R} is a by-need bisimulation up to \sim_{bn} and restriction if $P \mathcal{R} Q$ implies:*

- 1) $P \mid a/b \mathcal{R} Q \mid a/b$, for all names a, b ;
- 2) if a and b appear free in P , then $P \triangleright a \curlywedge b$ implies $Q \triangleright a \curlywedge b$;
- 3) if $P \xrightarrow{\mu}_{\text{bn}} P'$ (where the object part of μ is fresh, whenever $\mu \neq \tau$), then $Q \xrightarrow{\mu}_{\text{bn}} Q'$ and there are P'', Q'', \tilde{x} s.t. $P' \sim_{\text{bn}} \nu \tilde{x} P''$, $Q' \sim_{\text{bn}} \nu \tilde{x} Q''$, and $P'' \mathcal{R} Q''$,
- 4) the converse of clauses (2) and (3).

Lemma 13. *If \mathcal{R} is a by-need bisimulation up to \sim_{bn} and restriction then $\mathcal{R} \subseteq \sim_{\text{bn}}$.*

H. Soundness of \sim_{bn}

We now move to the proof that \sim_{bn} is a congruence. What is missing is closure by parallel composition, which is rather delicate. This is because we defined the semantics of τ -actions with a reduction semantics. (The standard schema is to define a pure SOS semantics, show that it coincides with the reduction semantics, and then work with the SOS.)

For the proof of congruence we introduce *communication contexts*. These are, intuitively, the composition of two active contexts, one used for an input, the other for an output; such input and output may produce a τ -action. Communication contexts, ranged over by G , have two holes, each occurring exactly once.

$$G ::= P \mid G \mid G \mid P \mid \nu a G \mid E_1 \mid E_2 .$$

By convention the leftmost hole is the first one, the other is the second one. We write $P = G[ac.Q][\bar{b}d.R]$ if P is obtained from G with $ac.Q$, and the second hole with $\bar{b}d.R$.

Communication contexts can be used to decompose a $\xrightarrow{\tau}_{\text{bn}}$ transition:

Lemma 14. *Suppose $P \xrightarrow{\tau}_{\text{bn}} P'$ (that is, $P \longrightarrow_{\text{bn}} P'$). Then one of the following statements holds:*

- $P = G[\bar{a}b.Q][cd.R]$ and $P' \sim_{\text{bn}} \nu f (G[b/f \mid Q][f/d \mid R])$,
- $P = G[cd.R][\bar{a}b.Q]$ and $P' \sim_{\text{bn}} \nu f (G[f/d \mid R][b/f \mid Q])$,

where $P \triangleright a \curlywedge c$ and f is fresh.

Proof: The two cases are similar, the main difficulty is to keep track of the structural congruence operations. If $P \longrightarrow_{\text{bn}} P'$ it means that, $P \equiv E[\bar{a}b.Q_1 \mid ac.R_1]$ and $P' \equiv E[b/c \mid Q_1 \mid R_1]$. From the first relation we can get G such that $P = G[\bar{a}b.Q][cd.R]$ (with $G \triangleright a \curlywedge c$, $Q \equiv Q_1$ and $R \equiv R_1$), ignoring the symmetric case for which the output is the left argument of G . We extract the potential restrictions $\nu \hat{b}$ and $\nu \hat{d}$ ($\hat{b} = \emptyset$ if b is not bound and $\hat{b} = \{b\}$ if is captured by G) from G , yielding the much alike context G' (and $G \equiv (\nu \hat{b} \hat{d})G'$).

The interesting part is that we can write the reduction with the arc at the top, then use Lemma 17 and then structural congruence to put back b and d inside G .

$$\begin{aligned}
P &\equiv (\nu \hat{b} \hat{d}) G'[\bar{a}b. Q][cd. R] \\
&\longrightarrow_{\text{bn}} (\nu \hat{b} \hat{d})(b/d \mid G'[Q][R]) \\
&\sim_{\text{bn}} (\nu \hat{b} \hat{d})((\nu f)(b/f \mid f/d) \mid G'[Q][R]) \\
&\equiv (\nu f)(\nu \hat{b} \hat{d})(G'[b/f \mid Q][f/d \mid R]) \\
&\equiv (\nu f)G[b/f \mid Q][f/d \mid R] .
\end{aligned}$$

To conclude we need to relate this last process to P' which is done by proving that $E[b/d \mid Q_1 \mid R_1] \equiv (\nu \hat{b} \hat{d})(b/d \mid G'[Q][R])$, which is done by keeping tracks of the derivation of $E[\bar{a}b. Q_1 \mid cd. R_1] \equiv P$. ■

Lemma 15. *Suppose $Q \xrightarrow{bf}_{\text{bn}} Q'$ and suppose b is not captured by E . Then $Q \mid E[\bar{b}d. R_1] \xrightarrow{\tau}_{\text{bn}} \sim_{\text{bn}} \nu f(E[d/f \mid R_1])$.*

Lemma 16 (Congruence for restriction). *If $P \sim_{\text{bn}} Q$ then for all c , $\nu cP \sim_{\text{bn}} \nu cQ$.*

Proof: Given a relation \mathcal{R} , we define

$$(\mathcal{R})^{\text{Sub}} = \{(P \mid \sigma, Q \mid \sigma). PRQ \text{ and } \sigma \text{ is a parallel composition of arcs}\} .$$

We show that $(\{\nu cP, \nu cQ, P \sim_{\text{bn}} Q\})^{\text{Sub}}$ is a bisimulation up to \equiv . This is a consequence of the following observations:

- For any u, v, c, P such that $\{u, v\} \subseteq \text{fn}(P)$ and $c \notin \{u, v\}$, we have $P \triangleright u \Upsilon v$ iff $\nu cP \triangleright u \Upsilon v$.
- The visible transitions of our labelled transition system do not involve name extrusion, and we have that $P \xrightarrow{\alpha}_{\text{bn}} P'$ iff $\nu cP \xrightarrow{\alpha}_{\text{bn}} \nu cP'$ for $c \notin \text{n}(\alpha)$.
- Suppose now $\nu cP \xrightarrow{\tau}_{\text{bn}} P'$. This means $P \xrightarrow{\tau}_{\text{bn}} P_0$ for some P_0 s.t. $P' \equiv \nu cP_0$. But then $Q \xrightarrow{\tau}_{\text{bn}} Q_0$, $P_0 \sim_{\text{bn}} Q_0$ and $\nu cQ \xrightarrow{\tau}_{\text{bn}} \nu cQ_0$. ■

Lemma 17 (Transitivity of arcs). *For all active context E we have: $E[a/c] \sim_{\text{bn}} E[\nu b(a/b \mid b/c)]$.*

Proof: Let \mathcal{R} be the corresponding relation. We show that \mathcal{R} is a \sim_{bn} -bisimulation up to \equiv . Of course the relation is stable by parallel composition of arcs, since E can be an arbitrary active context. Concerning the Υ condition, the left-to-right implication is rather clear. From right to left, we must prove that we cannot get more from $\nu b(a/b \mid b/c)$ than from a/c which is achieved by the restriction νb . Now concerning the transitions we know from the Υ condition that the same names will be joinable through the preorder, independently of \equiv or the context. The resulting processes will still stay in \mathcal{R} , up to \equiv . ■

Lemma 18 (Congruence for parallel composition). *If $P \sim_{\text{bn}} Q$ then also $P \mid R \sim_{\text{bn}} Q \mid R$.*

Proof (Sketch): **Special case:** we first suppose that all arcs in R occur under at least one prefix. We show that

$\{(P \mid R, Q \mid R), P \sim_{\text{bn}} Q \text{ and } R \text{ does not contain active arcs}\}$ by contexts. ■

is a bisimulation up to restriction and up to bisimilarity.

Suppose then $P \mid R \xrightarrow{\tau}_{\text{bn}} U$, in which both P and R contribute (the other possibilities are easier).

Suppose P makes the input (the case of output is symmetric). In this case we have, using Lemma 14:

$$P = E[ac. P_1] \quad R = F[\bar{b}d. R_1]$$

where $E \triangleright a \Upsilon b$ (since R has no arc) and with $P' = E[f/c \mid P_1]$ and $R' = F[d/f \mid R_1]$:

$$U \sim_{\text{bn}} \nu f(P' \mid R') .$$

Using rule EN-INP, we also have $P \xrightarrow{bf}_{\text{bn}} P'$. Hence, since $P \sim_{\text{bn}} Q$, $Q \xrightarrow{bf}_{\text{bn}} Q'$ and $P' \sim_{\text{bn}} Q'$ for some Q' , which gives $Q' = E'[a'c'. Q_1]$ for some a' s.t. $E' \triangleright a' \Upsilon b$, and $Q' = E'[f/c' \mid Q_1]$. From this, Lemma 15 gives us directly:

$$Q \mid R \xrightarrow{\tau}_{\text{bn}} \sim_{\text{bn}} \nu f(Q' \mid R')$$

We can now extract the arc from R' :

$$R' \equiv \nu \tilde{n}(R'' \mid \sigma) ,$$

where σ is a parallel composition of arcs and R'' contains no active arc. We then have

$$P' \mid R' \equiv (\nu \tilde{n})(P' \mid \sigma \mid R'') ,$$

and similarly for $Q' \mid R'$. We can conclude by remarking that $P' \sim_{\text{bn}} Q'$ entails $P' \mid \sigma \sim_{\text{bn}} Q' \mid \sigma$, and using up to restriction to remove the topmost restrictions.

General case: Consider now the case where R is an arbitrary process. We reason by induction on R , to show that $P \sim_{\text{bn}} Q$ implies $P \mid R \sim_{\text{bn}} Q \mid R$. The cases where R is a prefixed process or $R = \mathbf{0}$ are treated by the result above.

The case where $R = u/v$ holds by definition of \sim_{bn} : $P \sim_{\text{bn}} Q$ implies $P \mid u/v \sim_{\text{bn}} Q \mid u/v$.

If $R = R_1 \mid R_2$, then by induction $P \mid R_1 \sim_{\text{bn}} Q \mid R_1$, which gives, by induction again, $(P \mid R_1) \mid R_2 \sim_{\text{bn}} (Q \mid R_1) \mid R_2$, hence the result by associativity of \mid .

Suppose now $R = \nu cR'$. We can suppose w.l.o.g. $c \notin \text{fn}(P) \cup \text{fn}(Q)$. Then by induction $P \mid R' \sim_{\text{bn}} Q \mid R'$, which gives, by Lemma 16, $(\nu c)(P \mid R') \sim_{\text{bn}} (\nu c)(Q \mid R')$. Lemma 11 gives $(\nu c)(P \mid R') \sim_{\text{bn}} P \mid \nu cR'$, and similarly for Q , hence $P \mid R \sim_{\text{bn}} Q \mid R$. This concludes the proof. ■

Statement of Theorem ??: *Bisimilarity is a congruence.*

Proof: Follows from Lemmas 16 and 18, closure by prefixes being immediate. ■

Theorem 19 (Soundness). *If $P \sim_{\text{bn}} Q$ then $P \simeq_{\text{bn}} Q$.*

Proof: Preservation of fresh barbs: when f does not appear in any arc, $P \downarrow_f^{\text{bn}}$ is equivalent to $P \xrightarrow{\alpha}$ where α is an input or output label with subject f .

Preservation of general barbs: $P \downarrow_a^{\text{bn}}$ is equivalent to $(P \mid \alpha. f) \xrightarrow{\tau}_{\text{bn}} \downarrow_f^{\text{bn}}$ for some α whose subject is a .

Closure under reduction holds trivially since $\longrightarrow_{\text{bn}}$ coincides with $\xrightarrow{\tau}_{\text{bn}}$ and finally, Theorem ?? guarantees closure

by contexts. ■

I. Completeness of \sim_{bn}

For a prefix α we write $\bar{\alpha}$ for the dual prefix, i.e. $\bar{\bar{a}b} = ab$ and $\bar{\bar{a}b} = \bar{a}b$. Any prefix α can be also seen as a label.

Lemma 20. *Let P and P' be processes and f a name fresh w.r.t. P and such that $P' \not\downarrow_f^{\text{bn}}$. Then $P \xrightarrow{\alpha}_{\text{bn}} \equiv P'$ if and only if there exists a process P_1 such that $P_1 \downarrow_f^{\text{bn}}$ and*

$$P \mid \bar{\alpha}.(\bar{f} \mid f) \xrightarrow{\text{bn}} P_1 \xrightarrow{\text{bn}} P' .$$

Proof: Let us consider the case where α is an input prefix bd , the output case being similar.

Left to right: since $\xrightarrow{\text{bn}}$ is stable by \equiv we directly suppose that $P \xrightarrow{\alpha}_{\text{bn}} P'$. Then $P = E[ac.Q]$ with $E \triangleright a \gamma b$ and $P' = E[d/c \mid Q]$. Then

$$\begin{aligned} P_\alpha &\stackrel{\text{def}}{=} P \mid \bar{\alpha}.(\bar{f} \mid f) \\ &\equiv E[ac.Q \mid \bar{b}d.(\bar{f} \mid f)] \\ &\xrightarrow{\text{bn}} E[d/c \mid Q \mid \bar{f} \mid f] \stackrel{\text{def}}{=} P_1 \\ &\xrightarrow{\text{bn}} E[d/c \mid Q] = P' . \end{aligned}$$

Right to left: since P_1 and f is fresh in P we know that $\bar{\alpha}$ has been triggered, that is, $P_\alpha \equiv E[ac.Q \mid \bar{b}d.(\bar{f} \mid f)]$ and $P' \equiv E[d/c \mid Q]$ since P' has no f barb. This means that P is of the form $P \equiv E[ac.Q]$. Hence $P \xrightarrow{\alpha}_{\text{bn}} \equiv P'$. ■

Theorem 21 (Completeness). *If $P \simeq_{\text{bn}} Q$ then $P \sim_{\text{bn}} Q$.*

Proof: We show that \simeq_{bn} is a \sim_{bn} -bisimulation up to \equiv . The clause for preservation of γ is treated with Lemma 8. The one about parallel composition of arcs is trivial, as well as the symmetry and the clause for the τ -transition. We are left with the case for an input or output transition α .

Suppose $P \xrightarrow{\alpha}_{\text{bn}} P'$ and let f be a name fresh wrt to P , P' and Q . Lemma 20 provides us P_1 such that $P_1 \downarrow_f^{\text{bn}}$ and a reduction scheme that we can transport to Q :

$$Q \mid \bar{\alpha}.(\bar{f} \mid f) \xrightarrow{\text{bn}} Q_1 \xrightarrow{\text{bn}} Q_2 .$$

We know that $P_1 \simeq_{\text{bn}} Q_1$ and $P' \simeq_{\text{bn}} Q_2$, hence $Q_1 \downarrow_f^{\text{bn}}$ and $Q_2 \not\downarrow_f^{\text{bn}}$ (since f is fresh for P'). Another application of Lemma 20 directly gives us $Q \xrightarrow{\alpha}_{\text{bn}} \equiv Q_2$. ■

Statement of Theorem ??: *In $\pi\mathcal{P}$, relations \sim_{bn} and \simeq_{bn} coincide.*

Proof: Consequence of Theorems 21 and 19. ■

J. Encoding $A\pi$ in $\pi\mathcal{P}$

1) *Operational correspondence results:* We say that $P \in \pi\mathcal{P}$ is *asynchronous* if the continuation of all outputs in P is $\mathbf{0}$. We can remark that the encoding of a process in $A\pi$ is an asynchronous $\pi\mathcal{P}$ process.

We use the following properties of the encoding, where $\xrightarrow{\pi}$ is the reduction in the π -calculus. Barbs in the π -calculus are defined in the standard way: $P \downarrow_a$ iff $P \equiv (\nu\tilde{c})(\alpha.P \mid R)$ where α is a prefix whose subject is a . (It is equivalent to $P = E[\alpha.P_1]$ for some active context E .)

Lemma 22. *Let P be any π -calculus process.*

- 1) *If $P \equiv Q$ then $\llbracket P \rrbracket \equiv \llbracket Q \rrbracket$;*
- 2) *if $\llbracket P \rrbracket \equiv \llbracket Q \rrbracket$ then $P \equiv Q$;*
- 3) *if $\llbracket P \rrbracket \equiv E_1[\bar{a}b.Q_1 \mid ax.R_1]$ then $Q_1 \equiv \llbracket Q \rrbracket$, $R_1 \equiv \llbracket R \rrbracket$ and $P \equiv E[\bar{a}b.Q \mid a(x).R]$ with $\llbracket E \rrbracket[\nu x[\cdot]] \equiv E_1[\cdot]$.*
- 4) *if $P \xrightarrow{\pi} P'$ then $\llbracket P \rrbracket \xrightarrow{\text{bn}} \simeq_{\text{bn}} \llbracket P' \rrbracket$;*
- 5) *conversely, if $\llbracket P \rrbracket \xrightarrow{\text{bn}} P_1$ then there is P' such that $P \xrightarrow{\pi} P'$ and $P_1 \simeq_{\text{bn}} \llbracket P' \rrbracket$;*
- 6) *$P \downarrow_a$ iff $\llbracket P \rrbracket \downarrow_a$.*

Proof:

- 1) Straightforward.
- 2) We prove tediously but straightforwardly the following refined statement: if $\llbracket P \rrbracket \equiv R_1$ then there exist R such that $P \equiv R$ and we can obtain R_1 from $\llbracket R \rrbracket$ such that $R_1 \equiv \llbracket R \rrbracket$ but only by moving restrictions of input objects. In the case where $R_1 = \llbracket Q \rrbracket$ we prove that R is necessarily Q (the restrictions of input objects have only one possible position).
- 3) We combine techniques used in the previous item to get back the fact Q_1 and R_1 are structurally congruent to encoding of processes, and techniques from the proof of Lemma 10 to separate the transformations of \equiv in the subterms Q_1 , R_1 guarded by the prefixes $\bar{a}b$, ax from those in the rest of the term.
- 4) The reduction $\xrightarrow{\pi}$ is quotiented by structural congruence, so in the induction proof there is a case handling the rule “if $P \equiv P_1 \xrightarrow{\pi} P'_1 \equiv P'$ then $P \xrightarrow{\pi} P'$ ”. Since $\llbracket P \rrbracket \equiv \llbracket P_1 \rrbracket$ and $\llbracket P'_1 \rrbracket \equiv \llbracket P' \rrbracket$ we only need to know that $\llbracket P_1 \rrbracket \xrightarrow{\text{bn}} \simeq_{\text{bn}} \llbracket P'_1 \rrbracket$ by induction. We also need to know that $(\equiv \xrightarrow{\text{bn}} \simeq_{\text{bn}} \equiv) \subseteq (\xrightarrow{\text{bn}} \simeq_{\text{bn}})$ which is true by definition of $\xrightarrow{\text{bn}}$ and \simeq_{bn} . Similarly since the reduction in π is also quotiented by active contexts we also remark that the encoding is compositional, and the encoding of an active context is still active. Also we have to prove that if $P \xrightarrow{\text{bn}} \simeq_{\text{bn}} Q$ then $P \xrightarrow{\text{bn}} \simeq_{\text{bn}} Q$ which is true by definition of $\xrightarrow{\text{bn}}$ and because \simeq_{bn} is a congruence.
- 5) We now focus on the simple case of $\bar{a}b.P \mid a(x).Q \xrightarrow{\pi} P \mid Q\{b/x\}$. The encoding of the left-hand side reduces into $\nu x(\llbracket P \rrbracket \mid b/x \mid \llbracket Q \rrbracket)$ and we know that x has no negative occurrence in $\llbracket Q \rrbracket$ so by Lemma ?? this process is equivalent to $\llbracket P \rrbracket \mid \llbracket Q \rrbracket\{b/x\}$ which is of the expected shape.
- 6) The implication from left to right is straightforward by induction, but one has to remark that to test the input barb, one needs a synchronous tester $\bar{a}b.\omega$. (Note that input barbs are not tested in the *asynchronous* version of

behavioural equivalences.) The other implication follows from the fact that there is no arc in $\llbracket P \rrbracket$ so $\llbracket P \rrbracket \downarrow_a$ if and only if $\llbracket P \rrbracket$ contains a prefix whose subject is a (which is equivalent to the fact P does, too).

Lemma 23 (Label-syntax correspondence). *If P is only contains trivial arcs (of the form $e|e$) and α is a prefix ac or $\bar{a}c$ then $P \xrightarrow{\alpha}_{\text{bn}} \equiv P'$ iff $P \equiv E[\alpha.P_1]$ and $P' \equiv E[c|c | P_1]$, with E binding neither a nor c (and P' has only trivial arcs).*

Moreover $P \downarrow_a^{\text{bn}}$ iff $P \xrightarrow{\alpha}_{\text{bn}}$ iff $P \equiv E[\alpha.P_1]$.

In addition if $\sigma \triangleright a \gamma b$ then $P \xrightarrow{ac}_{\text{bn}} P'$ implies $P | \sigma \xrightarrow{bc}_{\text{bn}} P' | \sigma$ (resp. $\bar{a}c, \bar{b}c$).

Lemma 24 (Label correspondences). *Let P be any π process and f a fresh name.*

- 1) If $P \xrightarrow{\bar{a}c}_{\pi} P'$ then $\llbracket P \rrbracket \xrightarrow{\bar{a}f}_{\text{bn}} \equiv c|f | \llbracket P' \rrbracket$.
- 2) If $P \xrightarrow{\bar{a}(c)}_{\pi} P'$ then $\llbracket P \rrbracket \xrightarrow{\bar{a}f}_{\text{bn}} \equiv \nu c(c|f | \llbracket P' \rrbracket)$.
- 3) If $P \xrightarrow{a(x)}_{\pi} P'$ then $\llbracket P \rrbracket \xrightarrow{af}_{\text{bn}} \equiv \nu x(f/x | \llbracket P' \rrbracket)$.
- 4) If $\llbracket P \rrbracket \xrightarrow{\bar{a}f}_{\text{bn}} P_1$ then
 - a) either $P \xrightarrow{\bar{a}c}_{\pi} P'$ with $P_1 \equiv c|f | \llbracket P' \rrbracket$,
 - b) or $P \xrightarrow{\bar{a}(c)}_{\pi} P'$ with $P_1 \equiv \nu c(c|f | \llbracket P' \rrbracket)$
- 5) If $\llbracket P \rrbracket \xrightarrow{af}_{\text{bn}} P_1$ then
$$P \xrightarrow{a(x)}_{\pi} P' \text{ with } P_1 \equiv \nu x.(f/x | \llbracket P' \rrbracket)$$

Lemma 25 (Decomposition of transitions, asynchronous $\pi\mathcal{P}$). *Let P be an asynchronous $\pi\mathcal{P}$ term without visible arc, σ a parallel composition of arcs, and f, g some fresh names.*

- 1) If $P | \sigma \xrightarrow{\tau}_{\text{bn}} P_t$ then $P \xrightarrow{\bar{a}f}_{\text{bn}} P_1 \xrightarrow{bg}_{\text{bn}} P_2$ with $P_t \sim_{\text{bn}} (\nu fg)(P_2 | f/g) | \sigma$ and $\sigma \triangleright a \gamma b$.
- 2) Suppose $P \xrightarrow{\bar{a}f}_{\text{bn}} P_1 \xrightarrow{ag}_{\text{bn}} P_2$ and $\sigma \triangleright a \gamma b$. Then $P | \sigma \xrightarrow{\tau}_{\text{bn}} \sim_{\text{bn}} (\nu fg)(P_2 | f/g) | \sigma$.

This result is directly a consequence of the syntax of asynchronous $\pi\mathcal{P}$ as for similar results in $A\pi$. We use \sim_{bn} for renaming and concatenating fresh names using Lemma 17.

2) *Full abstraction for the encoding of $A\pi$:* One inclusion in the full abstraction result actually holds for the whole π -calculus:

Lemma 26. *Let P and Q be π terms. Then $\llbracket P \rrbracket \simeq_{\text{bn}} \llbracket Q \rrbracket$ implies $P \simeq_{\pi} Q$.*

Proof: The relation $\{(P, Q) \mid \llbracket P \rrbracket \simeq_{\text{bn}} \llbracket Q \rrbracket\}$ is reduction-closed (consequence of Lemma 22), barb-preserving (consequence of Lemma 22), and context-closed: if C is a π context then there exists a $\pi\mathcal{P}$ context C_1 such that $\llbracket C[P] \rrbracket = C_1[\llbracket P \rrbracket]$, similarly for Q ; hence $\llbracket P \rrbracket \simeq_{\text{bn}} \llbracket Q \rrbracket$ implies $\llbracket C[P] \rrbracket \simeq_{\text{bn}} \llbracket C[Q] \rrbracket$. ■

Lemma 27. *Let P and Q be asynchronous π -terms. Then $P \simeq_{\pi} Q$ implies $\llbracket P \rrbracket \simeq_{\text{bn}} \llbracket Q \rrbracket$.*

Proof: Thanks to Theorem 19 and to the characterisation of barbed congruence by ground bisimilarity in the asynchronous π -calculus [5], we only have to prove that $P \sim_{\text{g}} Q$

implies $\llbracket P \rrbracket \sim_{\text{bn}} \llbracket Q \rrbracket$. We do so by showing that the following relation is a \sim_{bn} -bisimulation up to restriction and \sim_{bn} :

$$\mathcal{R} \stackrel{\text{def}}{=} (\sim_{\text{g}})^{\text{Sub}} \stackrel{\text{def}}{=} \{(\llbracket P \rrbracket \mid \sigma, \llbracket Q \rrbracket \mid \sigma) \mid P \sim_{\text{g}} Q\}$$

where σ stands for any parallel composition of arcs. In order to do that, we rely on Lemma 24 ($\llbracket P \rrbracket$ is arc-free) to relate non- τ transitions in π and $\pi\mathcal{P}$, as well as on Lemma 25 to decompose τ -transitions into visible transitions.

We analyse all possible transitions from $\llbracket P \rrbracket \mid \sigma$. We omit intermediate steps to focus on the relevant details.

- 1) $\llbracket P \rrbracket \mid \sigma \xrightarrow{af}_{\text{bn}} \sim_{\text{bn}} \nu x(f/x | \llbracket P' \rrbracket \mid \sigma)$ with $P \xrightarrow{b(x)}_{\pi} P'$ for some b such that $\sigma \triangleright a \gamma b$. Drawing the \sim_{g} -diagram yields eventually $\llbracket Q \rrbracket \xrightarrow{bf}_{\text{bn}} \sim_{\text{bn}} \nu x(f/x | \llbracket Q' \rrbracket)$. We add σ to derive a transition along the original label af , and relate in \mathcal{R} the resulting processes.
- 2) $\llbracket P \rrbracket \mid \sigma \xrightarrow{\bar{a}f}_{\text{bn}} \sim_{\text{bn}} \nu \hat{c}(c|f | \llbracket P' \rrbracket)$ with $P \xrightarrow{\nu \hat{c}bc}_{\pi} P'$ with $\hat{c} \in \{\emptyset, \{c\}\}$ and $\sigma \triangleright a \gamma b$. The reasoning is similar to the previous case.
- 3) $\llbracket P \rrbracket \mid \sigma \xrightarrow{\tau}_{\text{bn}} P_t \mid \sigma$ with

$$\begin{aligned} \llbracket P \rrbracket \xrightarrow{\bar{a}f}_{\text{bn}} \xrightarrow{bg}_{\text{bn}} \nu \hat{c}x(c|f | g/x | \llbracket P'' \rrbracket) &\stackrel{\text{def}}{=} P_2 \\ P \xrightarrow{\nu \hat{c}ac}_{\pi} \xrightarrow{b(x)}_{\pi} P'' & \end{aligned}$$

such that $\sigma \triangleright a \gamma b$ and $P_t \sim_{\text{bn}} \nu fg(P_2 | f/g)$. We can again play the ground bisimilarity game and use Lemma 25 to get the same relations on the Q side, to finally get $P \sim_{\text{g}} Q$ and thus:

$$(\llbracket P'' \rrbracket \mid \sigma') \mathcal{R} (\llbracket Q'' \rrbracket \mid \sigma')$$

with $\sigma' = \sigma | c|f | f/g | g/x$. We use the up to restriction technique on f, g, x , and \hat{c} .

The relation \mathcal{R} is symmetric, and clearly satisfies the clause about joinability and the clause about the addition of arcs. Thus \mathcal{R} is a \sim_{bn} -bisimulation up to restriction and \sim_{bn} . ■

Theorem 28 (Full abstraction). *Suppose P, Q are processes from the asynchronous π -calculus, $A\pi$. Then $P \simeq_{A\pi} Q$ iff $\llbracket P \rrbracket \simeq_{\text{bn}} \llbracket Q \rrbracket$.*

K. Encoding of Explicit Fusions

Definition 29. *Let $P \triangleright a = b$ be the judgement conjunction of $P \triangleright a \leq b$ and $P \triangleright b \leq a$.*

In the following we note φ_P the relation $\{(a, b) \mid P \triangleright a \varphi b\}$, e.g. $a \gamma_P b$ for the joinability $a \leq_P b$ for the reachability or $a =_P b$ for the equality. We will note $P =_{a,b} Q$ iff $P\{b/a\} = Q\{b/a\}$ i.e. if the only difference between P and Q is the exchange of some a and b . We will also write $a = b$ for $[a = b]$ which is $a/b \mid b/a$.

Lemma 30. *If $P =_{a,b} Q$ then $\varphi_{P|a=b} = \varphi_{Q|a=b}$.*

Proof: By symmetry we only consider inclusion. We use induction on the derivation of $(P | a = b) \triangleright \varphi$ along Definition 3. Only the base case is interesting, when P and Q are arcs and φ is of the form $d \leq e$. Then if $n(\varphi) \subseteq \{a, b\}$

then $(a = b) \triangleright \varphi$; if $P \neq Q$ then (P, Q) can only be of the form $(a_1/c, a_2/c)$ (or, resp., $(c/a_1, c/a_2)$) where $a_i \in \{a, b\}$. In this last case φ must be $c \leq a_i$ (resp. $a_i \leq c$) which is easily achieved by $(a_2/c \mid a = b)$ (resp. $(a_2/c \mid a = b)$). ■

We extend the definition of $=_{a,b}$ to predicates: $\varphi =_{a,b} \psi$ iff φ and ψ differ only by a, b swaps. Lemma 30 can be slightly generalised:

Lemma 31. *If $P =_{a,b} Q$, $\varphi =_{a,b} \psi$ then $\varphi_{P|a=b} = \psi_{Q|a=b}$.*

Proof: By Lemma 30 we only have to prove that if $R = S \mid a = b$ then $R \triangleright \varphi$ implies $R \triangleright \psi$, which is easy, since for each case there is a rule of Definition 3 that uses either a/b or b/a to replace one a with a b or vice versa. ■

Lemma 32. *If $P =_{a,b} Q$ then $(P \mid a = b) \sim_{\text{bn}} (Q \mid a = b)$.*

Proof: Let \mathcal{R} be the corresponding relation, quantifying over every P and Q . We prove that \mathcal{R} is a \sim_{bn} -bisimulation:

- 1) invariance under arcs is trivial;
- 2) is implied by Lemma 30;
- 3) we use Lemma 31 to ensure the communication is possible (when $\mu = \tau$) or that the subject of μ can be related to the subject of the prefix (when $\mu \neq \tau$). The resulting processes are still related through $=_{a,b}$ since this relation commutes with \equiv and contexts.

We conclude by symmetry of $=_{a,b}$. ■

Lemma 33. *If P and Q are prefix-free, and if their preorders coincide on free names, then $P \sim_{\text{bn}} Q$.*

Proof: The corresponding relation is a \sim_{bn} -bisimulation: all condition checks are straightforward, even when we add arcs since Definition 3 is compositional: $\text{preor}(P \mid Q)$ only depends on $\text{preor}(P)$ and $\text{preor}(Q)$. ■

Lemma 34. *For every fusion process P if $\llbracket P \rrbracket \triangleright a \leq b$ or $\llbracket P \rrbracket \triangleright a \vee b$ then $\llbracket P \rrbracket \triangleright a = b$ and $P \equiv P \mid a = b$ (i.e. a and b are related through P 's fusions).*

Proof: First we prove that $\llbracket P \rrbracket \triangleright a \leq b$ implies $\llbracket P \rrbracket \triangleright b \leq a$ by induction on the derivation of the first judgement. The only interesting case is when we use an arc b/a : then we know that there is the other arc a/b next to b/a , so this is enough. We also know that this is coming from $a = b$ in the original process. Now if the hypothesis is about $a \vee b$ we know that there is a name u such that $a \leq u$ and $b \leq u$ and we use the first part of the proof to prove $u \leq a$ and $u \leq b$ which you can compose to get $a \leq b$ and $b \leq a$. ■

Statement of Theorem ??: *Suppose P and Q are processes of the fusion calculus.*

- 1) *If $P \equiv Q$ then $\llbracket P \rrbracket \approx_{\text{bn}} \llbracket Q \rrbracket$;*
- 2) *if $P \rightarrow_{\text{EF}} P'$ then $\llbracket P \rrbracket \rightarrow_{\text{bn}} \approx_{\text{bn}} \llbracket P' \rrbracket$;*
- 3) *conversely, if $\llbracket P \rrbracket \rightarrow_{\text{bn}} Q$, then $Q \approx_{\text{bn}} \llbracket P' \rrbracket$ for some P' such that $P \rightarrow_{\text{EF}} P'$.*

Proof: 1) Thanks to Theorem ??, it is enough to prove $\llbracket P \rrbracket \sim_{\text{bn}} \llbracket Q \rrbracket$, which we do by induction on the derivation of $P \equiv Q$. The standard base cases like associativity are translated directly into structural congruent processes that are

therefore related through \sim_{bn} . The other base cases that those dedicated to fusions:

- $\llbracket a = b \mid P \rrbracket \sim_{\text{bn}} \llbracket a = b \mid P\{a/b\} \rrbracket$ by Lemma 32,
- $\llbracket a = b \mid b = c \rrbracket \sim_{\text{bn}} \llbracket a = c \mid b = c \rrbracket$ by Lemma 32,
- $\llbracket a = b \rrbracket \equiv \llbracket b = a \rrbracket$ by commutativity of \mid ,
- $\llbracket a = a \rrbracket \sim_{\text{bn}} \llbracket 0 \rrbracket$ by Lemma 33,
- $\llbracket (\nu a)a = b \rrbracket \sim_{\text{bn}} \llbracket 0 \rrbracket$ by Lemma 33.

We conclude thanks to the fact that \sim_{bn} is a congruence and an equivalence relation.

2) Thanks to 1) and the fact \rightarrow_{bn} is stable by active contexts we only consider the base case of the reduction relation: $R \stackrel{\text{def}}{=} \bar{a}b.P \mid ac.Q \rightarrow_{\text{EF}} b = c \mid P \mid Q \stackrel{\text{def}}{=} R'$. Since \approx_{bn} is stable by \equiv and active contexts, we just have to consider the following: $\llbracket R \rrbracket \rightarrow_{\text{bn}} (\nu wy)(b/c \mid w/y \mid wb. \llbracket P \rrbracket \mid \bar{y}(c). \llbracket Q \rrbracket)$ which has only one deterministic reduction to $\llbracket R' \rrbracket \mid (\nu wy)(w/y)$ which is strongly bisimilar to $\llbracket R' \rrbracket$ by Lemma 33.

3) In $\llbracket R \rrbracket$ the only visible prefixes $\pi.P$ are the form $\llbracket \pi'. P' \rrbracket$. Suppose that $\llbracket R \rrbracket \rightarrow_{\text{bn}} S$ comes from the communication between $\pi_1.P$ and $\pi_2.Q$ of subjects a and b . We know that $\llbracket R \rrbracket \triangleright a \vee b$ which means thanks to Lemma 34 that the communication is possible between $\pi'_1.P'$ and $\pi'_2.Q'$: for some $R', R \rightarrow_{\text{EF}} R'$. The process S is then one step away to create the next step and free arcs (corresponding to the encoding of the fusion just created) the continuations $\llbracket P' \rrbracket$ and $\llbracket Q' \rrbracket$ which places us into a situation similar to 2). ■

REFERENCES

- [1] B. Pierce and D. Sangiorgi, "Typing and subtyping for mobile processes," *Math. Str. in Comp. Sci.*, vol. 6, no. 5, pp. 409–453, 1996.
- [2] N. Kobayashi, "Type systems for concurrent programs," in *10th Anniversary Colloquium of UNU/IIST*, ser. LNCS, vol. 2757. Springer, 2003, pp. 439–453.
- [3] —, "A new type system for deadlock-free processes," in *CONCUR*, ser. LNCS, vol. 4137. Springer, 2006, pp. 233–247.
- [4] K. Honda, V. T. Vasconcelos, and M. Kubo, "Language primitives and type discipline for structured communication-based programming," in *ESOP*, ser. LNCS, vol. 1381. Springer, 1998, pp. 122–138.
- [5] D. Sangiorgi and D. Walker, *The Pi-Calculus: a theory of mobile processes*. Cambridge University Press, 2001.
- [6] J. Parrow and B. Victor, "The fusion calculus: expressiveness and symmetry in mobile processes," in *LICS*. IEEE, 1998, pp. 176–185.
- [7] —, "The update calculus (extended abstract)," in *AMAST*, ser. LNCS, vol. 1349. Springer, 1997, pp. 409–423.
- [8] L. Wischik and P. Gardner, "Explicit fusions," *Theor. Comput. Sci.*, vol. 340, no. 3, pp. 606–630, 2005.
- [9] Y. Fu, "The χ -calculus," in *APDC*. IEEE Comp. Soc., 1997, pp. 74–81.
- [10] C. Laneve and B. Victor, "Solos in concert," *Math. Str. in Comp. Sci.*, vol. 13, no. 5, pp. 657–683, 2003.
- [11] P. Gardner and L. Wischik, "Explicit fusions," in *MFCS*, ser. LNCS, vol. 1893. Springer, 2000, pp. 373–382.
- [12] J. Parrow and B. Victor, "The tau-laws of fusion," in *CONCUR*, ser. LNCS, vol. 1466. Springer, 1998, pp. 99–114.
- [13] G. L. Ferrari, U. Montanari, E. Tuosto, B. Victor, and K. Yemane, "Modelling Fusion Calculus using HD-Automata," in *CALCO*, ser. LNCS, vol. 3629. Springer, 2005, pp. 142–156.
- [14] F. Bonchi, M. G. Buscemi, V. Ciancia, and F. Gadducci, "A presheaf environment for the explicit fusion calculus," *J. Autom. Reasoning*, vol. 49, no. 2, pp. 161–183, 2012.
- [15] M. Boreale, M. G. Buscemi, and U. Montanari, "A general name binding mechanism," in *TGC*, ser. LNCS, vol. 3705. Springer, 2005, pp. 61–74.
- [16] N. Kobayashi, B. Pierce, and D. Turner, "Linearity and the pi-calculus," *TOPLAS*, vol. 21, no. 5, pp. 914–947, 1999.
- [17] K. Honda and N. Yoshida, "On reduction-based process semantics," *Theor. Comp. Sci.*, vol. 152, no. 2, pp. 437–486, 1995.

- [18] R. De Nicola and M. Hennessy, "Testing equivalences for processes," *Theor. Comput. Sci.*, vol. 34, pp. 83–133, 1984.
- [19] D. Sangiorgi, "Pi-calculus, internal mobility, and agent-passing calculi," *Theor. Comput. Sci.*, vol. 167, no. 1&2, pp. 235–274, 1996.
- [20] M. Merro, "Locality in the pi-calculus and applications to distributed objects," Ph.D. dissertation, École des Mines, France, 2000.
- [21] J. Bengtson, M. Johansson, J. Parrow, and B. Victor, "Psi-calculi: Mobile processes, nominal data, and logic," in *LICS*. IEEE, 2009, pp. 39–48.
- [22] B. Victor, "The fusion calculus : Expressiveness and symmetry in mobile processes," Ph.D. thesis, Uppsala University, 1998.
- [23] Web appendix to this paper, available at <http://hal.inria.fr/hal-00818068>, 2013.
- [24] H. Hüttel, "Typed ψ -calculi," in *CONCUR*, ser. LNCS, vol. 6901. Springer, 2011, pp. 265–279.