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

Daniel Hirschkoff, Jean-Marie Madiot, Davide Sangiorgi

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

Daniel Hirschkoff, Jean-Marie Madiot

ENS Lyon, U. de Lyon, CNRS, INRIA, UCBL
{daniel.hirschkoff, 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 Hirschkoff, 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 $P\mathcal{R}Q$ implies $C[P]\mathcal{R}C[Q]$, 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 $P'\mathcal{R}Q'$.*

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:

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

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

$$\begin{aligned} E[P] &= (\boldsymbol{\nu} bc)(\overline{u}b \mid \overline{v}a \mid uc \mid vc \mid P) && (1)\\ &\Longrightarrow (\boldsymbol{\nu} b)(\overline{v}a \mid vb \mid P\{b/c\}) && (2)\\ &= (\boldsymbol{\nu} b)(\overline{v}a \mid vb \mid P) && (3)\\ &\Longrightarrow P\{a/b\}\ . && (4)\end{aligned}$$

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 $\overline{u}b$ is well-typed thanks to narrowing and weakening, hence so is $(\overline{u}b \mid uc \mid \overline{v}a \mid vc \mid P\{b/a\})$. 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. ∎

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 $D = \overline{a_1}x_1 \mid \overline{a_2}x_2 \mid a_1 y \mid a_2 y$ to simulate a substitution:

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

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), $i = 1$, $\alpha = \overline{a_2}x_2$: $T_{a_1} = T_{a_2} = \sharp\, T$, $T_y = T$;
- (1), $i = 1$, $\alpha = a_1 y$: $T_{a_1} = \sharp\, T$, $T_{a_2} = \sharp\, S$, $T_y = S$;
- (2), $i = 1$, $\alpha = \overline{a_1}x_1$: $T_{a_1} = T_{a_2} = \sharp\, S$, $T_y = S$;
- (2), $i = 1$, $\alpha = a_2 y$: $T_{a_1} = \sharp\, T$, $T_{a_2} = \sharp\, S$, $T_y = T$;
- (1), $i = 2$, $\alpha = \overline{a_2}x_2$: $T_{a_1} = T_{a_2} = \sharp\, T$, $T_y = T$;
- (1), $i = 2$, $\alpha = a_2 y$: $T_{a_1} = \sharp\, S$, $T_{a_2} = \sharp\, T$, $T_y = S$;
- (2), $i = 2$, $\alpha = \overline{a_1}x_1$: $T_{a_1} = T_{a_2} = \sharp\, S$, $T_y = S$;

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

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 $\pi\mathtt{P}$

Definition 2 (Structural congruence)**.** *Structural congruence on $\pi\mathtt{P}$, written $\equiv$, is the smallest congruence containing the associativity and commutativity of $\mid$ and the following rules:*

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

$$\boldsymbol{\nu} a(P \mid Q) \equiv (\boldsymbol{\nu} a P) \mid Q \quad \textit{if } a \notin \mathrm{fn}(Q)$$

D. Alternative definition of $\curlyvee$

Given an active context E, the set of *captured names* of E, $\mathrm{cn}(E)$, is defined as follows: $c \in \mathrm{cn}(E)$ iff the hole occurs in the scope of a restriction on c in E ($\mathrm{cn}(E)$ 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 $\varphi ::= a \leqslant b \mid a \curlyvee b$ in which $a \leqslant b$ is read "b is reachable from a", and $a \curlyvee b$ is read "a and b are joinable". In both cases, we have $\mathrm{n}(\varphi) = \{a, b\}$. We first define a judgement $\varphi_1, \varphi_2 \vdash \varphi$, as follows:*

$$\frac{}{a \leqslant b, b \leqslant c \vdash a \leqslant c} \qquad \frac{}{a \leqslant c, b \leqslant c \vdash a \curlyvee b}$$

$$\frac{}{a \curlyvee b, c \leqslant a \vdash c \curlyvee b} \qquad \frac{}{a \curlyvee b, c \leqslant b \vdash a \curlyvee c} \qquad \frac{\varphi_1, \varphi_2 \vdash \varphi}{\varphi_2, \varphi_1 \vdash \varphi}$$

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

$$\textsc{Refl}\ \frac{}{A \rhd a \leqslant a} \qquad \textsc{Deduct}\ \frac{A \rhd \varphi_1 \qquad A \rhd \varphi_2 \qquad \varphi_1, \varphi_2 \vdash \varphi}{A \rhd \varphi}\ .$$

Then we define $\rhd$ for processes:

$$\frac{}{b/a \rhd a \leqslant b} \qquad \frac{P \rhd \varphi}{P \mid R \rhd \varphi} \qquad \frac{P \rhd \varphi}{R \mid P \rhd \varphi}$$

$$\frac{P \rhd \varphi \qquad a \notin \mathrm{n}(\varphi)}{(\boldsymbol{\nu} a) P \rhd \varphi}$$

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

$$\frac{P \rhd \varphi \qquad \mathrm{n}(\varphi) \cap \mathrm{cn}(E) = \emptyset}{P \mid E \rhd \varphi} \qquad \frac{E \rhd \varphi}{P \mid E \rhd \varphi} \qquad \frac{E \rhd \varphi}{(\boldsymbol{\nu} a) E \rhd \varphi}$$

Lemma 4. *If P is a $\pi\mathtt{P}$ process, the relation $\leqslant_P$ defined by $\{(a, b) \mid P \rhd a \leqslant b\}$ is a preorder.*

Proof: Thanks to the rule Refl, $\leqslant_P$ is reflexive and thanks to the rule Deduct and the fact that $a \leqslant b, b \leqslant c \vdash a \leqslant c$, $\leqslant_P$ is transitive, hence it is a preorder. ■

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

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

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 $P \in \pi\mathtt{P1}$, we write $Eq(P)$ for the relation between names defined by $Eq(P)(a, b)$ iff $P \rhd a \curlyvee b$.*

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

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

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

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

We call the union of relations satisfying these properties the *eager/by-need weak reduction-closed barbed congruence* for $\pi\mathtt{P1}$, written ${}^{\mathrm{ea}}_{1}\!\approxeq^{\mathrm{bn}}_{1}$.

1) $\mathcal{R}$ is clearly context-closed in $\pi\mathtt{P1}$.
2) $P \downarrow_a^{\mathrm{bn}}$ implies $P \Downarrow_a^{\mathrm{ea}}$ as each arc involved in the joinability condition generates a $\longrightarrow_{\mathrm{ea}}$ reduction, and $P \downarrow_a^{\mathrm{ea}}$ implies $P \downarrow_a^{\mathrm{bn}}$, as $P \longrightarrow_{\mathrm{ea}} P'$ implies $P \longrightarrow_{\mathrm{bn}} P'$.
3) By induction we suppose $P \longrightarrow_{\mathrm{ea}} P'$. 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 $Q \longrightarrow_{\mathrm{bn}} Q'$, with a communication on a and b with $a \curlyvee b$. The corresponding names a', b' in P are such that $a' \curlyvee a \curlyvee b \curlyvee b'$ i.e. $a' \curlyvee b'$ so a' and b' can be rewritten into a common name, letting the communication happen.

Since $\mathcal{R} \subseteq {}^{\mathrm{ea}}_{1}\!\approxeq^{\mathrm{bn}}_{1}$, for all $P \in \pi\mathtt{P1}$ we have $P\ {}^{\mathrm{ea}}_{1}\!\approxeq^{\mathrm{bn}}_{1}\ P$ which implies that $P \approxeq_{\pi\mathtt{P1bn}} Q$ iff $P \approxeq_{\pi\mathtt{P1ea}} Q$. ■

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).*

$$P ::= \ \mathbf{0} \ \Big|\ P \mid P \ \Big|\ \overline{a}\widetilde{x}.\, P \ \Big|\ a\widetilde{x}.\, P \ \Big|\ \boldsymbol{\nu} a P\ .$$

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

$$\frac{P \equiv P_1 \qquad P_1 \to_F Q_1 \qquad Q_1 \equiv Q}{P \to_F Q} \qquad \frac{P \to_F Q}{E[P] \to_F E[Q]}$$

$$(\boldsymbol{\nu} \widetilde{z})(R \mid a\widetilde{x}.\, P \mid \overline{a}\widetilde{y}.\, Q) \to_F (R \mid P \mid Q)\sigma \qquad (5)$$

G. Auxiliary results

a) Results involving name preorders:

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

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 $P \simeq_{\mathrm{bn}} Q$ and $P \triangleright a \curlyvee b$. Then $Q \triangleright a \curlyvee b$.*

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

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

Proof: Let P and Q be processes and f be a fresh name. Then $P \triangleright a \leqslant b$ iff $(P \mid f/b) \triangleright a \curlyvee f$ 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 $E \triangleright a \curlyvee b$ iff $E' \triangleright a \curlyvee b$. Moreover for all Q_1 such that all names of $\mathrm{fn}(Q_1)$ are either in $\mathrm{fn}(P_1)$ 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 $G \triangleright a \curlyvee b$ iff $G' \triangleright a \curlyvee b$.*

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 $P \sim_{\mathrm{bn}} Q$.*

Proof: We show that $\equiv$ is a $\sim_{\mathrm{bn}}$-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 $\xrightarrow{\tau}_{\mathrm{bn}} = \longrightarrow_{\mathrm{bn}}$ is stable by $\equiv$. For the remaining labels we examine the case where $\mu = bd$, the other case being similar. We know that $P = E[ac.\, P_1]$ with $E \triangleright a \curlyvee b$ and $P' = E[d/c \mid P_1]$. We use Lemma 10 to get $Q = E'[ac.\, P_1]$ which implies $Q \xrightarrow{bd} E'[d/c \mid P_1] \equiv P'$. ∎

c) Proof techniques:

Definition 12 (By-need bisimulation up to $\sim_{\mathrm{bn}}$ and restriction)**.** *A relation $\mathcal{R}$ is a* by-need bisimulation up to $\sim_{\mathrm{bn}}$ 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 $P \triangleright a \curlyvee b$ implies $Q \triangleright a \curlyvee b$;*
3) *if $P \xrightarrow{\mu}_{\mathrm{bn}} P'$ (where the object part of μ is fresh, whenever $\mu \neq \tau$), then $Q \xrightarrow{\mu}_{\mathrm{bn}} Q'$ and there are $P'', Q'', \widetilde{x}$ s.t. $P' \sim_{\mathrm{bn}} \boldsymbol{\nu}\widetilde{x}\, P''$, $Q' \sim_{\mathrm{bn}} \boldsymbol{\nu}\widetilde{x}\, Q''$, 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 $\sim_{\mathrm{bn}}$ and restriction then $\mathcal{R} \subseteq \sim_{\mathrm{bn}}$.*

H. Soundness of $\sim_{\mathrm{bn}}$

We now move to the proof that $\sim_{\mathrm{bn}}$ 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.

$$G ::= P \mid G \;\Big|\; G \mid P \;\Big|\; \boldsymbol{\nu} a\, G \;\Big|\; E_1 \mid E_2 \;\; .$$

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

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

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

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

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

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

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.

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

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

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

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

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

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

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

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

∎

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

Proof: Let $\mathcal{R}$ be the corresponding relation. We show that $\mathcal{R}$ is a $\sim_{\mathrm{bn}}$-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 $\curlyvee$ condition, the left-to-right implication is rather clear. From right to left, we must prove that we cannot get more from $\boldsymbol{\nu}b(a/b \mid b/c)$ than from a/c which is achieved by the restriction $\boldsymbol{\nu}b$. Now concerning the transitions we know from the $\curlyvee$ 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 $P \sim_{\mathrm{bn}} Q$ then also $P \mid R \sim_{\mathrm{bn}} Q \mid R$.*

Proof (Sketch): **Special case:** we first suppose that all arcs in R occur under at least one prefix. We show that $\{(P \mid R,\, Q \mid R),\ P \sim_{\mathrm{bn}} Q$ and R does not contain active arcs$\}$ is a bisimulation up to restriction and up to bisimilarity.

Suppose then $P \mid R \xrightarrow{\tau}_{\mathrm{bn}} U$, 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:

$$P = E[ac.\,P_1] \qquad R = F[\overline{b}d.\,R_1]$$

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

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

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

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

We can now extract the arc from R':

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

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

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

and similarly for $Q' \mid R'$. We can conclude by remarking that $P' \sim_{\mathrm{bn}} Q'$ entails $P' \mid \sigma \ \sim_{\mathrm{bn}}\ Q' \mid \sigma$, 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 $P \sim_{\mathrm{bn}} Q$ implies $P \mid R \sim_{\mathrm{bn}} Q \mid R$. 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 $\sim_{\mathrm{bn}}$: $P \sim_{\mathrm{bn}} Q$ implies $P \mid u/v \ \sim_{\mathrm{bn}}\ Q \mid u/v$.

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

Suppose now $R = \boldsymbol{\nu}cR'$. We can suppose w.l.o.g. $c \notin \mathrm{fn}(P) \cup \mathrm{fn}(Q)$. Then by induction $P \mid R' \ \sim_{\mathrm{bn}}\ Q \mid R'$, which gives, by Lemma 16, $(\boldsymbol{\nu}c)(P \mid R') \ \sim_{\mathrm{bn}}\ (\boldsymbol{\nu}c)(Q \mid R')$. Lemma 11 gives $(\boldsymbol{\nu}c)(P \mid R') \ \sim_{\mathrm{bn}}\ P \mid \boldsymbol{\nu}cR'$, and similarly for Q, hence $P \mid R \ \sim_{\mathrm{bn}}\ Q \mid R$. 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 $P \sim_{\mathrm{bn}} Q$ then $P \simeq_{\mathrm{bn}} Q$.*

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

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

Closure under reduction holds trivially since $\longrightarrow_{\mathrm{bn}}$ coincides with $\xrightarrow{\tau}_{\mathrm{bn}}$ and finally, Theorem **??** guarantees closure by contexts. ∎

I. Completeness of $\sim_{\mathrm{bn}}$

For a prefix α we write $\overline{\alpha}$ for the dual prefix, i.e. $\overline{\overline{a}b} = ab$ and $\overline{ab} = \overline{a}b$. 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 $P' \not\downarrow_f^{\mathrm{bn}}$. Then $P \xrightarrow{\alpha}_{\mathrm{bn}} \equiv P'$ if and only if there exists a process P_1 such that $P_1 \downarrow_f^{\mathrm{bn}}$ and*

$$P \mid \overline{\alpha}.\,(\overline{f} \mid f) \longrightarrow_{\mathrm{bn}} P_1 \longrightarrow_{\mathrm{bn}} P' \ .$$

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

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

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

Right to left: since P_1 and f is fresh in P we know that $\overline{\alpha}$ has been triggered, that is, $P_\alpha \equiv E[ac.\,Q \mid \overline{b}d.\,(\overline{f} \mid f)]$ 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 $P \xrightarrow{\alpha}_{\mathrm{bn}} \equiv P'$. ∎

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

Proof: We show that $\simeq_{\mathrm{bn}}$ is a $\sim_{\mathrm{bn}}$-bisimulation up to $\equiv$. The clause for preservation of $\curlyvee$ 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 $P \xrightarrow{\alpha}_{\mathrm{bn}} P'$ and let f be a name fresh wrt to P, P' and Q. Lemma 20 provides us P_1 such that $P_1 \downarrow_f^{\mathrm{bn}}$ and a reduction scheme that we can transport to Q:

$$Q \mid \overline{\alpha}.\,(\overline{f} \mid f) \longrightarrow_{\mathrm{bn}} Q_1 \longrightarrow_{\mathrm{bn}} Q_2 \ .$$

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

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

Proof: Consequence of Theorems 21 and 19. ∎

J. Encoding $\mathrm{A}\pi$ *in* $\pi\mathtt{P}$

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

We use the following properties of the encoding, where $\longrightarrow_\pi$ is the reduction in the π-calculus. Barbs in the π-calculus are defined in the standard way: $P \downarrow_a$ iff $P \equiv (\boldsymbol{\nu}\widetilde{c})(\alpha.\,P \mid R)$ 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 $[\![P]\!] \equiv [\![Q]\!]$;*
2) *if $[\![P]\!] \equiv [\![Q]\!]$ then $P \equiv Q$;*
3) *if $[\![P]\!] \equiv E_1[\overline{a}b.\,Q_1 \mid ax.\,R_1]$ then $Q_1 \equiv [\![Q]\!]$, $R_1 \equiv [\![R]\!]$ and $P \equiv E[\overline{a}b.\,Q \mid a(x).\,R]$ with $[\![E]\!][\boldsymbol{\nu}x[\cdot]] \equiv E_1[\cdot]$.*
4) *if $P \longrightarrow_\pi P'$ then $[\![P]\!] \longrightarrow_{\mathrm{bn}} \simeq_{\mathrm{bn}} [\![P']\!]$;*
5) *conversely, if $[\![P]\!] \longrightarrow_{\mathrm{bn}} P_1$ then there is P' such that $P \longrightarrow_\pi P'$ and $P_1 \simeq_{\mathrm{bn}} [\![P']\!]$;*
6) *$P \downarrow_a$ iff $[\![P]\!] \downarrow_a$.*

Proof:

1) Straightforward.
2) We prove tediously but straightforwardly the following refined statement: if $[\![P]\!] \equiv R_1$ then there exist R such that $P \equiv R$ and we can obtain R_1 from $[\![R]\!]$ such that $R_1 \equiv [\![R]\!]$ but only by moving restrictions of input objects. In the case where $R_1 = [\![Q]\!]$ 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 $\overline{a}b$, ax from those in the rest of the term.
4) The reduction $\longrightarrow_\pi$ is quotiented by structural congruence, so in the induction proof there is a case handling the rule "if $P \equiv P_1 \longrightarrow_\pi P_1' \equiv P'$ then $P \longrightarrow_\pi \equiv P'$". Since $[\![P]\!] \equiv [\![P_1]\!]$ and $[\![P_1']\!] \equiv [\![P']\!]$ we only need to know that $[\![P_1]\!] \longrightarrow_{\mathrm{bn}} \simeq_{\mathrm{bn}} [\![P_1']\!]$ by induction. We also need to know that $(\equiv \longrightarrow_{\mathrm{bn}} \simeq_{\mathrm{bn}} \equiv) \subseteq (\longrightarrow_{\mathrm{bn}} \simeq_{\mathrm{bn}})$ which is true by definition of $\longrightarrow_{\mathrm{bn}}$ and $\simeq_{\mathrm{bn}}$.
   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 $P \longrightarrow_{\mathrm{bn}} \simeq_{\mathrm{bn}} Q$ then $P \longrightarrow_{\mathrm{bn}} \simeq_{\mathrm{bn}} Q$ which is true by definition of $\longrightarrow_{\mathrm{bn}}$ and because $\simeq_{\mathrm{bn}}$ is a congruence.
   We now focus on the simple case of $\overline{a}b.\,P \mid a(x).\,Q \longrightarrow_\pi P \mid Q\{b/x\}$. The encoding of the left-hand side reduces into $\boldsymbol{\nu}x([\![P]\!] \mid b/\!\!/x \mid [\![Q]\!])$ and we know that x has no negative occurrence in $[\![Q]\!]$ so by Lemma **??** this process is equivalent to $[\![P]\!] \mid [\![Q]\!]\{b/x\}$ which is of the expected shape.
5) If $[\![P]\!] \longrightarrow_{\mathrm{bn}} Q$, since $[\![P]\!]$ does not have any arc, the reduction comes from a communication between two prefixes on the same name a: $[\![P]\!] \equiv E_1[\overline{a}b.\,[\![Q]\!] \mid ax.\,[\![R]\!]]$ with E binding x, and then keeping track of all actions operated by $\equiv$ we know that P_1 is of the form $P_1 \equiv E_1[[\![Q]\!] \mid b/\!\!/x \mid [\![R]\!]]$. We can recover $P \equiv E[\overline{a}b.\,Q \mid a(x).\,R] \longrightarrow_\pi E[Q \mid R\{b/x\}] \stackrel{\text{def}}{=} P'$. Then $[\![P']\!] = [\![E]\!][[\![Q]\!] \mid [\![R]\!]\{b/x\}] \equiv E_1[[\![Q]\!] \mid [\![R]\!]\{b/x\}] \simeq_{\mathrm{bn}} P_1$.
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 $\overline{a}b.\,\omega$. (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 $[\![P]\!]$ so $[\![P]\!] \downarrow_a$ if and only if $[\![P]\!]$ 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 $\overline{a}c$ then $P \xrightarrow{\alpha}_{\mathrm{bn}} \equiv P'$ iff $P \equiv E[\alpha.P_1]$ and $P' \equiv E[c/c \mid P_1]$, with E binding neither a nor c (and P' has only trivial arcs).*

Moreover $P \downarrow^{\mathrm{bn}}_a$ iff $P \xrightarrow{\alpha}_{\mathrm{bn}}$ iff $P \equiv E[\alpha.P_1]$.

In addition if $\sigma \triangleright a \curlyvee b$ then $P \xrightarrow{ac}_{\mathrm{bn}} P'$ implies $P \mid \sigma \xrightarrow{bc}_{\mathrm{bn}} P' \mid \sigma$ (resp. $\overline{a}c$, $\overline{b}c$).

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

1) *If $P \xrightarrow{\overline{a}c}_\pi P'$ then $[\![P]\!] \xrightarrow{\overline{a}f}_{\mathrm{bn}} \equiv c/f \mid [\![P']\!]$.*
2) *If $P \xrightarrow{\overline{a}(c)}_\pi P'$ then $[\![P]\!] \xrightarrow{\overline{a}f}_{\mathrm{bn}} \equiv \boldsymbol{\nu} c(c/f \mid [\![P']\!])$.*
3) *If $P \xrightarrow{a(x)}_\pi P'$ then $[\![P]\!] \xrightarrow{af}_{\mathrm{bn}} \equiv \boldsymbol{\nu} x(f/x \mid [\![P']\!])$.*
4) *If $[\![P]\!] \xrightarrow{\overline{a}f}_{\mathrm{bn}} P_1$ then*
   a) *either $P \xrightarrow{\overline{a}c}_\pi P'$ with $P_1 \equiv c/f \mid [\![P']\!]$,*
   b) *or $P \xrightarrow{\overline{a}(c)}_\pi P'$ with $P_1 \equiv \boldsymbol{\nu} c(c/f \mid [\![P']\!])$*
5) *If $[\![P]\!] \xrightarrow{af}_{\mathrm{bn}} P_1$ then*
   $P \xrightarrow{a(x)}_\pi P'$ with $P_1 \equiv \boldsymbol{\nu} x.\,(f/x \mid [\![P']\!])$

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

1) *If $P \mid \sigma \xrightarrow{\tau}_{\mathrm{bn}} P_t$ then $P \xrightarrow{\overline{a}f}_{\mathrm{bn}} P_1 \xrightarrow{bg}_{\mathrm{bn}} P_2$ with $P_t \sim_{\mathrm{bn}} (\boldsymbol{\nu} fg)(P_2 \mid f/g) \mid \sigma$ and $\sigma \triangleright a \curlyvee b$.*
2) *Suppose $P \xrightarrow{\overline{a}f}_{\mathrm{bn}} P_1 \xrightarrow{ag}_{\mathrm{bn}} P_2$ and $\sigma \triangleright a \curlyvee b$. Then $P \mid \sigma \xrightarrow{\tau}_{\mathrm{bn}} \sim_{\mathrm{bn}} (\boldsymbol{\nu} fg)(P_2 \mid f/g) \mid \sigma$.*

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

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

Lemma 26. *Let P and Q be π terms. Then $[\![P]\!] \simeq_{\mathrm{bn}} [\![Q]\!]$ implies $P \simeq_\pi Q$.*

Proof: The relation $\{(P, Q) \mid [\![P]\!] \simeq_{\mathrm{bn}} [\![Q]\!]\}$ 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 $\pi\mathtt{P}$ context C_1 such that $[\![C[P]]\!] = C_1[[\![P]\!]]$, similarly for Q; hence $[\![P]\!] \simeq_{\mathrm{bn}} [\![Q]\!]$ implies $[\![C[P]]\!] \simeq_{\mathrm{bn}} [\![C[Q]]\!]$. ■

Lemma 27. *Let P and Q be asynchronous π-terms. Then $P \simeq_\pi Q$ implies $[\![P]\!] \simeq_{\mathrm{bn}} [\![Q]\!]$.*

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 $P \sim_{\mathrm{g}} Q$ implies $[\![P]\!] \sim_{\mathrm{bn}} [\![Q]\!]$. We do so by showing that the following relation is a $\sim_{\mathrm{bn}}$-bisimulation up to restriction and $\sim_{\mathrm{bn}}$:

$$\mathcal{R} \stackrel{\text{def}}{=} (\sim_{\mathrm{g}})^{\mathrm{Sub}} \stackrel{\text{def}}{=} \{([\![P]\!] \mid \sigma, [\![Q]\!] \mid \sigma) \;\big|\; P \sim_{\mathrm{g}} Q\}$$

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

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

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

$$[\![P]\!] \xrightarrow{\overline{a}f}_{\mathrm{bn}} \xrightarrow{bg}_{\mathrm{bn}} \boldsymbol{\nu} \hat{c}x(c/f \mid g/x \mid [\![P'']\!]) \stackrel{\text{def}}{=} P_2$$

$$P \xrightarrow{\boldsymbol{\nu}\hat{c}ac}_\pi \xrightarrow{b(x)}_\pi P''$$

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

$$([\![P'']\!] \mid \sigma') \;\mathcal{R}\; ([\![Q'']\!] \mid \sigma')$$

with $\sigma' = \sigma \mid c/f \mid f/g \mid g/x$. 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 $\sim_{\mathrm{bn}}$-bisimulation up to restriction and $\sim_{\mathrm{bn}}$. ■

Theorem 28 (Full abstraction)**.** *Suppose P, Q are processes from the asynchronous π-calculus,* Aπ*. Then $P \simeq_{\mathrm{A}\pi} Q$ iff $[\![P]\!] \simeq_{\mathrm{bn}} [\![Q]\!]$.*

K. Encoding of Explicit Fusions

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

In the following we note φ_P the relation $\{(a, b) \mid P \triangleright a \varphi b\}$, e.g. $a \curlyvee_P b$ for the joinability $a \leqslant_P b$ 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 $\varphi_{P \mid a=b} = \varphi_{Q \mid a=b}$.*

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

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 $c \leqslant a_i$ (resp. $a_i \leqslant c$) 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 $(P \mid a = b) \sim_{\mathrm{bn}} (Q \mid a = b)$.*

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

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

Lemma 34. *For every fusion process P if $[\![P]\!] \triangleright a \leqslant b$ or $[\![P]\!] \triangleright a \curlyvee b$ then $[\![P]\!] \triangleright a = b$ and $P \equiv P \mid a = b$ (i.e. a and b are related through P's fusions).*

Proof: First we prove that $[\![P]\!] \triangleright a \leqslant b$ implies $[\![P]\!] \triangleright b \leqslant a$ 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 $a \curlyvee b$ we know that there is a name u such that $a \leqslant u$ and $b \leqslant u$ and we use the first part of the proof to prove $u \leqslant a$ and $u \leqslant b$ which you can compose to get $a \leqslant b$ and $b \leqslant a$. ∎

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

1) *If $P \equiv Q$ then $[\![P]\!] \simeq_{\mathrm{bn}} [\![Q]\!]$;*
2) *if $P \longrightarrow_{\mathrm{EF}} P'$ then $[\![P]\!] \longrightarrow_{\mathrm{bn}} \approx_{\mathrm{bn}} [\![P']\!]$;*
3) *conversely, if $[\![P]\!] \longrightarrow_{\mathrm{bn}} Q$, then $Q \approx_{\mathrm{bn}} [\![P']\!]$ for some P' such that $P \longrightarrow_{\mathrm{EF}} P'$.*

Proof: 1) Thanks to Theorem **??**, it is enough to prove $[\![P]\!] \sim_{\mathrm{bn}} [\![Q]\!]$, 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 $\sim_{\mathrm{bn}}$. The other base cases that those dedicated to fusions:

- $[\![a = b \mid P]\!] \sim_{\mathrm{bn}} [\![a = b \mid P\{a/b\}]\!]$ by Lemma 32,
- $[\![a = b \mid b = c]\!] \sim_{\mathrm{bn}} [\![a = c \mid b = c]\!]$ by Lemma 32,
- $[\![a = b]\!] \equiv [\![b = a]\!]$ by commutativity of $|$,
- $[\![a = a]\!] \sim_{\mathrm{bn}} [\![0]\!]$ by Lemma 33,
- $[\![(\boldsymbol{\nu} a) a = b]\!] \sim_{\mathrm{bn}} [\![0]\!]$ by Lemma 33.

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

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

3) In $[\![R]\!]$ the only visible prefixes $\pi. P$ are the form $[\![\pi'. P']\!]$. Suppose that $[\![R]\!] \longrightarrow_{\mathrm{bn}} S$ comes from the communication between $\pi_1. P$ and $\pi_2. Q$ of subjects a and b. We know that $[\![R]\!] \triangleright a \curlyvee b$ which means thanks to Lemma 34 that the communication is possible between $\pi_1'. P'$ and $\pi_2'. Q'$: for some R', $R \longrightarrow_{\mathrm{EF}} R'$. 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 $[\![P']\!]$ and $[\![Q']\!]$ 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.