Howe's Method for Contextual Semantics

Sergueï Lenglet, Alan Schmitt

Howe's Method for Contextual Semantics

Sergueï Lenglet, Alan Schmitt

RESEARCH REPORT
N° 8750
June 2015
Project-Team Celtique

ISSN 0249-6399   ISRN INRIA/RR--8750--FR+ENG

Howe's Method for Contextual Semantics

Sergueï Lenglet*, Alan Schmitt†

Project-Team Celtique

Research Report n° 8750 — June 2015 — 31 pages

Abstract: We show how to use Howe's method to prove that context bisimilarity is a congruence for process calculi equipped with their usual semantics. We apply the method to two extensions of HOπ, with passivation and with join patterns, illustrating different proof techniques.

Key-words: Bisimulations, process calculi, Howe's Method

* Université de Lorraine
† Inria

RESEARCH CENTRE
RENNES – BRETAGNE ATLANTIQUE

Campus universitaire de Beaulieu
35042 Rennes Cedex

Méthode de Howe pour la sémantique contextuelle

Résumé : Nous montrons comment utiliser la méthode de Howe pour prouver que la bissimilarité contextuelle d'un calcul de processus muni de sa sémantique habituelle est une congruence. Nous appliquons cette méthode à deux extensions de HOπ, l'une avec passivation, l'autre avec des motifs à jointure, pour mettre en évidence des techniques de preuve différentes.

Mots-clés : Bissimilarité contextuelle, calculs de processus, méthode de Howe

1 Introduction

Process equivalence relates processes whose behavior may not be distinguished, even when inserted in arbitrary contexts. Equivalent processes may thus be used interchangeably in any larger system, with no observable difference. This property is quite strong, and to prove it directly, one has to consider every possible context. Much effort has thus been applied to techniques that simplify the proofs of process equivalence. Such techniques often involve the definition of a relation between processes that is easier to establish. The relation, typically a form of *bisimilarity*, is then shown to characterize process equivalence. This characterization has two parts: bisimilarity is *sound*—bisimilar processes are equivalent—and *complete*—equivalent processes are bisimilar.

As process equivalence is generally intended to be preserved by every context, it is often a congruence. Hence a sound and complete bisimilarity also has to be a congruence. Even when considering sound (but not complete) bisimilarities, it is very convenient that they be congruences. Indeed, to prove that two processes are equivalent, one can then simply show they have the same external structure (context) with bisimilar processes inside. Proving congruence is thus a crucial step when working with process equivalence.

Howe's method [7] is a powerful approach to show that a bisimilarity is a congruence. In a nutshell, it reverses the problem: first define a relation, called "Howe's closure", that includes the bisimilarity of interest and is a congruence by definition. Second, show it is a bisimulation. As bisimilarity contains every bisimulations, Howe's closure is thus included in bisimilarity. Third, conclude that the bisimilarity and its Howe's closure coincide, thus the former is a congruence.

This approach works well in a functional setting. Until now, its application to higher-order process calculi has required significant adjustments, either yielding a sound but not complete bisimilarity [5], or requiring the definition of a new semantics [10]. We present a direct application of Howe's method for the higher-order π calculus (HOπ) with its usual semantics, and state the central *pseudo-simulation* property that enables the application of the method (Section 2). We then detail two approaches to prove this lemma for two extensions of HOπ: one with *passivation* (Section 3), the other with *join-patterns* (Section 4).

2 Howe's Method in HOπ with Contextual Semantics

2.1 Syntax and Contextual Semantics

We recall the syntax and contextual semantics of (the process-passing fragment of) HOπ [13] in Figure 1, omitting the symmetric rules for Par and HO. We use a, b, c to range over channel names, $\overline{a}$, $\overline{b}$, $\overline{c}$ to range over conames, γ to range over names and conames, and X, Y to range over process variables. We define $\overline{\overline{a}}$ as a. Multisets $\{x_1 \dots x_n\}$ (where x ranges over some entities) are written $\widetilde{x}$.

Finally, we write $\uplus$ for multiset union.

An input $a(X)P$ binds X in P, and a restriction $\nu a.P$ binds a in P. We write $\mathrm{fv}(P)$ for the free variables of a process P and $\mathrm{fn}(P)$ for its free names. A *closed process* has no free variable. We identify processes up to α-conversion of names and variables: processes and agents are always chosen such that their bound names and variables are pairwise distinct, and distinct from their free names and variables. We write $P\{Q/X\}$ for the capture-free substitution of X by Q in P. *Structural congruence* $\equiv$ equates processes up to reorganization of their sub-processes and their name restrictions; it is the smallest congruence verifying the rules of Figure 1. Because the ordering of restrictions does not matter, we abbreviate $\nu a_1 \ldots . \nu a_n.P$ as $\nu\widetilde{a}.P$; since bound names are pairwise distinct, $\widetilde{a}$ is a set.

We define a labeled transition system (LTS), where agents transition to processes, *abstractions* F of the form $(X)Q$, or *concretions* C of the form $\nu\widetilde{b}.\langle R\rangle S$. Like for processes, the ordering of restrictions does not matter for a concretion, therefore we write them using a set of names $\widetilde{b}$; in particular, we write $\langle R\rangle S$ if $\widetilde{b} = \emptyset$. Labels of the LTS are ranged over by α. Transitions are either an *internal action* $P \xrightarrow{\tau} P'$, a *message input* $P \xrightarrow{a} F$, or a *message output* $P \xrightarrow{\overline{a}} C$. The transition $P \xrightarrow{a} (X)Q$ means that P may receive a process R on a to continue as $Q\{R/X\}$. The transition $P \xrightarrow{\overline{a}} \nu\widetilde{b}.\langle R\rangle S$ means that P may send the process R on a and then continue as S, and the scope of the names $\widetilde{b}$ has to be expanded to encompass the recipient of R. A higher-order communication takes place when a concretion interacts with an abstraction (rule HO).

2.2 Behavioral Equivalences

Barbed congruence relates processes based on their observable actions, or *barbs*. The observable actions γ of a process P, written $P \downarrow_\gamma$, are unrestricted names or conames on which a communication may immediately occur ($P \xrightarrow{\gamma} A$, for some A). A context $\mathbb{C}$ is a term with a single hole $\square$, that may be filled with a process P, written $\mathbb{C}\{P\}$; the free names or free variables of P may be captured by $\mathbb{C}$. An equivalence relation $\mathcal{R}$ is a *congruence* if $P \mathrel{\mathcal{R}} Q$ implies $\mathbb{C}\{P\} \mathrel{\mathcal{R}} \mathbb{C}\{Q\}$ for all contexts $\mathbb{C}$.

Definition 1. A symmetric relation $\mathcal{R}$ on closed processes is a strong barbed bisimulation if $P \mathrel{\mathcal{R}} Q$ implies:

- $P \downarrow_\gamma$ implies $Q \downarrow_\gamma$;
- if $P \xrightarrow{\tau} P'$, then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{R}} Q'$.

Two processes P, Q are strong barbed congruent, written $P \sim_b Q$, if for all context $\mathbb{C}$, there exists a strong barbed bisimulation $\mathcal{R}$ such that $\mathbb{C}\{P\} \mathrel{\mathcal{R}} \mathbb{C}\{Q\}$.

A relation $\mathcal{R}$ is *sound* with respect to $\sim_b$ if $\mathcal{R} \subseteq \sim_b$; $\mathcal{R}$ is *complete* with respect to $\sim_b$ if $\sim_b \subseteq \mathcal{R}$. In [13], barbed congruence is characterized by a (strong) *context bisimilarity*, defined as follows.

Syntax: $P ::= \mathbf{0} \mid X \mid P \,|\, P \mid a(X)P \mid \overline{a}\langle P\rangle P \mid \nu a.P$

Agents: $A, B ::= P \mid F \mid C$

Abstractions $F, G ::= (X)P$ Concretions $C, D ::= \langle P\rangle Q \mid \nu a.C$

Extension of operators to abstractions and concretions

$$
\begin{aligned}
(X)Q \,|\, P &\triangleq (X)(Q \,|\, P) \text{ if } X \notin \mathrm{fv}(P) \\
P \,|\, (X)Q &\triangleq (X)(P \,|\, Q) \text{ if } X \notin \mathrm{fv}(P) \\
\nu a.(X)P &\triangleq (X)\nu a.P \\
(\nu\widetilde{b}.\langle Q\rangle R) \,|\, P &\triangleq \nu\widetilde{b}.\langle Q\rangle(R \,|\, P) \text{ if } \widetilde{b} \cap \mathrm{fn}(P) = \emptyset \\
P \,|\, (\nu\widetilde{b}.\langle Q\rangle R) &\triangleq \nu\widetilde{b}.\langle Q\rangle(P \,|\, R) \text{ if } \widetilde{b} \cap \mathrm{fn}(P) = \emptyset \\
\nu a.(\nu\widetilde{b}.\langle Q\rangle R) &\triangleq \nu a, \widetilde{b}.\langle Q\rangle R \text{ if } a \in \mathrm{fn}(\nu\widetilde{b}.Q) \\
\nu a.(\nu\widetilde{b}.\langle Q\rangle R) &\triangleq \nu\widetilde{b}.\langle Q\rangle \nu a.R \text{ if } a \notin \mathrm{fn}(\nu\widetilde{b}.Q)
\end{aligned}
$$

Pseudo-application and process application

$$(X)P \bullet \nu\widetilde{b}.\langle R\rangle Q \triangleq \nu\widetilde{b}.(P\{R/X\} \,|\, Q) \text{ if } \widetilde{b} \cap \mathrm{fn}(P) = \emptyset \qquad (X)P \circ Q \triangleq P\{Q/X\}$$

Structural congruence

$$(P \,|\, Q) \,|\, R \equiv P \,|\, (Q \,|\, R) \qquad P \,|\, Q \equiv Q \,|\, P \qquad P \,|\, \mathbf{0} \equiv P \qquad \nu a.\nu b.P \equiv \nu b.\nu a.P$$

$$P \,|\, \nu a.Q \equiv \nu a.(P \,|\, Q) \text{ if } a \notin \mathrm{fn}(P) \qquad \nu a.P \equiv P \text{ if } a \notin \mathrm{fn}(P)$$

LTS rules: $\alpha ::= \tau \mid a \mid \overline{a}$

$$a(X)P \xrightarrow{a} (X)P \;\; \textsc{In} \qquad \overline{a}\langle Q\rangle P \xrightarrow{\overline{a}} \langle Q\rangle P \;\; \textsc{Out} \qquad \frac{P \xrightarrow{\alpha} A}{P \,|\, Q \xrightarrow{\alpha} A \,|\, Q} \;\; \textsc{Par}$$

$$\frac{P \xrightarrow{\alpha} A \qquad \alpha \notin \{a, \overline{a}\}}{\nu a.P \xrightarrow{\alpha} \nu a.A} \;\; \textsc{Restr} \qquad \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \,|\, Q \xrightarrow{\tau} F \bullet C} \;\; \text{HO}$$

Figure 1: Contextual LTS for HOπ

Definition 2. A relation $\mathcal{R}$ on closed processes is a context simulation if $P \mathrel{\mathcal{R}} Q$ implies:

- for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{R}} Q'$;
- for all $P \xrightarrow{a} F$, for all C, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C \mathrel{\mathcal{R}} F' \bullet C$;
- for all $P \xrightarrow{\overline{a}} C$, for all F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $F \bullet C \mathrel{\mathcal{R}} F \bullet C'$.

A relation $\mathcal{R}$ is a context bisimulation if $\mathcal{R}$ and $\mathcal{R}^{-1}$ are context simulations. Context bisimilarity, written $\sim$, is the largest context bisimulation.

The definition is written in the *early* style, because the answer $Q \xrightarrow{a} F'$ depends on the particular C considered in the input case, and $Q \xrightarrow{\overline{a}} C'$ depends on F in the output case. In the *late* style, this dependency is broken by moving the universal quantification on C or F after the existential one on F' or C'.

We extend the equivalences to open terms by defining the *open extension* of a relation $\mathcal{R}$.

Definition 3. For two open processes P and Q, $P \mathrel{\mathcal{R}^\circ} Q$ holds if $P\sigma \mathrel{\mathcal{R}} Q\sigma$ holds for all process substitutions σ that close P and Q.

Conversely, we write $\mathcal{R}_c$ for the relation $\mathcal{R}$ restricted to closed processes.

In the following, we use (bi)simulation up to structural congruence, a (bi)simulation proof technique which allows to use $\equiv$ when relating processes.

Definition 4. A relation $\mathcal{R}$ is a context simulation up to $\equiv$ if $P \mathrel{\mathcal{R}} Q$ implies the clauses of Definition 2, where $\mathcal{R}$ is changed into $\equiv\mathcal{R}\equiv$.

Since $\equiv$ is a context bisimulation, the resulting proof technique is sound.

Lemma 5. *If $\mathcal{R}$ is a context bisimulation up to $\equiv$, then $\mathcal{R} \subseteq \sim$.*

Context bisimilarity is sound and complete. The congruence proof of [13] does not apply, however, to certain process calculi, such as the ones with passivation [10]. For this reason, other congruence proof techniques, such as Howe's method [7], have been considered.

2.3 Howe's Method

We sketch the principles behind Howe's method and recall why its application to (early) context bisimilarity has been deemed problematic.

Howe's method [7, 6] is a systematic proof technique to show that a bisimilarity $\mathcal{B}$ (and its open extension $\mathcal{B}^\circ$) is a congruence. The method can be divided in three steps: first, prove some basic properties on the *Howe's closure* $\mathcal{B}^\bullet$ of the relation. By construction, $\mathcal{B}^\bullet$ contains $\mathcal{B}^\circ$ and is a congruence. Second, prove a simulation-like property for $\mathcal{B}^\bullet$. Finally, prove that $\mathcal{B}$ and $\mathcal{B}^\bullet$ coincide on closed processes. Since $\mathcal{B}^\bullet$ is a congruence, then so is $\mathcal{B}$.

Given a relation $\mathcal{R}$, Howe's closure is inductively defined as the smallest congruence which contains $\mathcal{R}^\circ$ and is closed under right composition with $\mathcal{R}^\circ$.

Definition 6. Howe's closure $\mathcal{R}^\bullet$ of a relation $\mathcal{R}$ is defined inductively by the following rules, where op ranges over the operators of the language.

$$\frac{P\ \mathcal{R}^\circ\ Q}{P\ \mathcal{R}^\bullet\ Q} \qquad \frac{P\ \mathcal{R}^\bullet\ P' \qquad P'\ \mathcal{R}^\circ\ Q}{P\ \mathcal{R}^\bullet\ Q} \qquad \frac{\widetilde{P}\ \mathcal{R}^\bullet\ \widetilde{Q}}{\mathsf{op}(\widetilde{P})\ \mathcal{R}^\bullet\ \mathsf{op}(\widetilde{Q})}$$

Instantiating $\mathcal{R}$ as $\mathcal{B}$, $\mathcal{B}^\bullet$ is a congruence by definition. The composition with $\mathcal{B}^\circ$ enables some transitivity and additional properties. In particular, we can prove that $\mathcal{B}^\bullet$ is *substitutive*: if $P\ \mathcal{B}^\bullet\ Q$ and $R\ \mathcal{B}^\bullet\ S$, then $P\{R/X\}\ \mathcal{B}^\bullet\ Q\{S/X\}$. By definition, we have $\mathcal{B}^\circ \subseteq \mathcal{B}^\bullet$; for the reverse inclusion to hold, we prove that $\mathcal{B}^\bullet$ is a bisimulation, hence it is included in the bisimilarity. To this end, we first prove that $\mathcal{B}^\bullet$ (restricted to closed terms) is a simulation, using a pseudo-simulation lemma (second step of the method, discussed below). We then use the following result on the reflexive and transitive closure $(\mathcal{B}^\bullet)^*$ of $\mathcal{B}^\bullet$.

Lemma 7. *Let $\mathcal{R}$ be an equivalence. Then $(\mathcal{R}^\bullet)^*$ is symmetric.*

If $\mathcal{B}^\bullet$ is a simulation, then $(\mathcal{B}^\bullet)^*$ (restricted to closed terms) is also a simulation. By Lemma 7, $(\mathcal{B}^\bullet)^*$ is in fact a bisimulation. Consequently, we have $\mathcal{B} \subseteq \mathcal{B}^\bullet \subseteq (\mathcal{B}^\bullet)^* \subseteq \mathcal{B}$ on closed terms, and we conclude that $\mathcal{B}$ is a congruence.

The main challenge is stating and proving a simulation-like property for the Howe's closure $\mathcal{B}^\bullet$ of a bisimilarity $\mathcal{B}$. The labels λ of a LTS $\xrightarrow{\lambda}$ of a higher-order language usually contain or depend on terms (e.g., in the λ-calculus, λ-abstractions are labels), so the technique generally extends $\mathcal{B}^\bullet$ to labels. The simulation-like property then follows the pattern below, similar to a higher-order bisimilarity clause as in Plain CHOCS [17].

If $P\ \mathcal{B}^\bullet\ Q$ and $P \xrightarrow{\lambda} A$, then for all $\lambda\ \mathcal{B}^\bullet\ \lambda'$, there exists B such that $Q \xrightarrow{\lambda'} B$ and $A\ \mathcal{B}^\bullet\ B$.

Stating and proving such a result for a Howe's closure built from an early context bisimilarity $\sim$, where inputs and outputs depend on respectively concretions and abstractions, is problematic. Indeed, we would like to prove that $P \sim^\bullet Q$ implies:

- for all $P \xrightarrow{a} F$, for all $C \sim^\bullet C'$, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C \sim^\bullet F' \bullet C'$;
- for all $P \xrightarrow{\overline{a}} C$, for all $F \sim^\bullet F'$ there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $F \bullet C \sim^\bullet F' \bullet C'$.

These clauses raise several issues. First, we have to find extensions of Howe's closure to abstractions and concretions which fit an early style. Even assuming such extensions, we cannot use this result to show $\sim^\bullet$ is a simulation. Indeed, suppose we are in the higher-order communication case: the processes are a parallel composition ($P = P_1 \mid P_2$, $Q = Q_1 \mid Q_2$, $P_1 \sim^\bullet Q_1$, and $P_2 \sim^\bullet Q_2$) and the transition is a higher-order communication ($P \xrightarrow{\tau} F \bullet C$, $P_1 \xrightarrow{a} F$, and $P_2 \xrightarrow{\overline{a}} C$). We thus need to find F' and C' such that $Q \xrightarrow{\tau} F' \bullet C'$, and

$F \bullet C \sim^\bullet F' \bullet C'$. However, we cannot apply the input clause with $P_1 \sim^\bullet Q_1$: to have a F' such that $Q_1 \xrightarrow{a} F'$, we have to find first a concretion C' such that $C \sim^\bullet C'$. We cannot use the output clause with P_2 and Q_2 either: to have a C' such that $Q_2 \xrightarrow{\overline{a}} C'$, we have to find first an abstraction F' such that $F \sim^\bullet F'$. Taking $C \sim^\bullet C$ to obtain F' such that $F \bullet C \sim^\bullet F' \bullet C$, then $F' \sim^\bullet F'$ to yield C' and $F' \bullet C \sim^\bullet F' \bullet C'$ would not work either: to conclude we would need to show that $\sim^\bullet$ is transitive. Transitivity is the reason usual congruence proof techniques fail with weak bisimulations, and the very motivation to turn to Howe's method [10, Section 3.1]. As we cannot bypass this mutual dependency nor this transitivity requirement, the proof fails in the communication case.

In [5], the authors break the mutual dependency by partially dropping the early style: they write the output clause in the late style. The resulting *input-early* bisimilarity is complete in the strong case, but not in the weak case. In [10], we propose to make the output clause a little less early: instead of first requiring the abstraction to provide a matching output, we only require the process that does the reception—that reduces to the abstraction. This small change is sufficient to break the mutual dependency. Indeed, the concretion C' from Q_2 matching the $P_2 \xrightarrow{\overline{a}} C$ step depends only on P_1, which is known, and not on some unknown abstraction. We can then obtain the abstraction F' from Q_2 that matches the $P_1 \xrightarrow{a} F$ step. This abstraction depends fully on C', in the usual early style.

Unfortunately, we do not directly use abstractions and concretions in [10], we define instead a *complementary* LTS, and its bisimilarity. Such a LTS implements the change above as follows: when P sends a message to Q, this becomes a transition from P *using* Q *as a label.* As a result, in the corresponding bisimilarity, an output action depends on a process that performs the input instead of the input itself. The LTS we obtain is serialized compared to the contextual one: in a communication, we do not have two parallel derivation trees for the output and the input, as with rule HO, but a single one, where we first look for the output, and then look for the input. But creating such a complementary LTS can be difficult, especially to handle scope extrusion properly, as we observed with passivation [10]. In the next section, we show that we can in fact apply Howe's method with the regular LTS.

2.4 Congruence Proof Using Howe's Method

As explained in Section 2.3, the main challenge to apply Howe's method is stating and proving a pseudo-simulation lemma for the Howe's closure $\sim^\bullet$. With contextual semantics, the challenge is to avoid mutual dependencies between the input and output clauses. Following the main idea behind the complementary semantics, we propose to keep the usual LTS but change the definition of the pseudo-simulation property to make the output depend on a process performing an input, and not the input itself. Conversely, the input now depends on a process performing an output, and not the output itself. Formally, if $P_1 \sim^\bullet Q_1$, then

- for all $P_1 \xrightarrow{a} F_1$, for all $P_2 \sim^\bullet Q_2$ such that $P_2 \xrightarrow{\overline{a}} C_1$, there exist F_2, C_2, such that $Q_1 \xrightarrow{a} F_2$, $Q_2 \xrightarrow{\overline{a}} C_2$, and $F_1 \bullet C_1 \sim^\bullet F_2 \bullet C_2$;
- for all $P_1 \xrightarrow{\overline{a}} C_1$, for all $P_2 \sim^\bullet Q_2$ such that $P_2 \xrightarrow{a} F_1$, there exist F_2, C_2, such that $Q_1 \xrightarrow{\overline{a}} C_2$, $Q_2 \xrightarrow{a} F_2$, and $F_1 \bullet C_1 \sim^\bullet F_2 \bullet C_2$.

This definition offers two advantages. First, we do not have to define an extension of $\sim^\bullet$ to abstractions and concretions as we relate only processes. Second, the clauses for the input and the output are identical, exchanging only the roles of P_1 and P_2, and of Q_1 and Q_2. Therefore, we can capture the input and output clause as a single symmetric clause. This gives us the up-to $\equiv$ pseudo-simulation lemma we will prove for $\sim^\bullet_c$ (the restriction of $\sim^\bullet$ to closed processes).

Lemma 8 (Pseudo-Simulation Lemma)**.** *Let $P_1 \sim^\bullet_c Q_1$ and $P_2 \sim^\bullet_c Q_2$. If $P_1 \xrightarrow{\overline{a}} C_1$ and $P_2 \xrightarrow{a} F_1$, then there exist C_2, F_2 such that $Q_1 \xrightarrow{\overline{a}} C_2$, $Q_2 \xrightarrow{a} F_2$, and $F_1 \bullet C_1 \equiv\sim^\bullet_c\equiv F_2 \bullet C_2$.*

With this formulation of the pseudo-simulation lemma, we easily dispatch the communication case. Suppose $P = P_1 \,|\, P_2$ and $Q = Q_1 \,|\, Q_2$ with $P_1 \sim^\bullet_c Q_1$ and $P_2 \sim^\bullet_c Q_2$. If $P \xrightarrow{\tau} F \bullet C$, with $P_1 \xrightarrow{a} F_1$ and $P_2 \xrightarrow{\overline{a}} C_1$, then we immediately have F_2, C_2 such that $Q \xrightarrow{\tau} F_2 \bullet C_2$ and $F_1 \bullet C_1 \equiv\sim^\bullet_c\equiv F_2 \bullet C_2$.

Lemma 8 can be proved in several ways, using either serialized inductions, or a simultaneous induction on $P_1 \sim^\bullet_c Q_1$ and $P_2 \sim^\bullet_c Q_2$. We discuss here the former, with proofs detailed in Appendix A. We then adapt this approach to a calculus with passivation (Section 3). The simultaneous induction approach is presented in Section 4 for a calculus with join patterns.

Using serialized inductions, we can start with $P_1 \sim^\bullet_c Q_1$ or with $P_2 \sim^\bullet_c Q_2$. Suppose we start with an induction on the sending processes $P_1 \sim^\bullet_c Q_1$. Most cases consist in using the induction hypothesis, followed by congruence properties of $\sim^\bullet_c$. There are two exceptions: (1) the base case $P_1 \sim Q_1$, and (2) the case $P_1 = \overline{a}\langle P_1^1\rangle P_1^2$, $Q_1 = \overline{a}\langle Q_1^1\rangle Q_1^2$, with $P_1^1 \sim^\bullet_c Q_1^1$ and $P_1^2 \sim^\bullet_c Q_1^2$. In these cases, we know which concretion C_2 the process Q_1 reduces to (either using $\sim$ in case (1), or by construction of P_1 and Q_1 in case (2)), but we have to find the abstraction F_2 the process Q_2 reduces to. To do so, we prove the following.

Lemma 9. *Let $P_1^1 \sim^\bullet_c Q_1^1$ and $P_2 \sim^\bullet_c Q_2$ such that $P_2 \xrightarrow{a} F_1$. There exists F_2 such that $Q_2 \xrightarrow{a} F_2$, and $F_1 \circ P_1^1 \sim^\bullet_c F_2 \circ Q_1^1$.*

The proof of this lemma is by induction on the derivation of $P_2 \sim^\bullet_c Q_2$. Lemma 9 deals with case (2) directly (just add the continuations P_1^2 and Q_1^2 using congruence), but it also handles case (1) ($P_1 \sim Q_1$). Indeed, if R is the message of C_1, applying Lemma 9 with $P_1^1 = Q_1^1 = R$ gives $F_1 \circ R \sim^\bullet_c F_2 \circ R$, which implies $F_1 \bullet C_1 \sim^\bullet_c F_2 \bullet C_1$ by congruence of $\sim^\bullet_c$. Since $P_1 \sim Q_1$, there exists C_2 such that $Q_1 \xrightarrow{\overline{a}} C_2$, and $F_2 \bullet C_1 \sim F_2 \bullet C_2$. We therefore have $F_1 \bullet C_1 \sim^\bullet_c\sim F_2 \bullet C_2$, which implies $F_1 \bullet C_1 \sim^\bullet_c F_2 \bullet C_2$ by right transitivity with $\sim$.

Alternatively, we can prove Lemma 8 by starting with the induction on the receiving processes $P_2 \sim_c^\bullet Q_2$. To handle the two cases (3) $P_2 \sim Q_2$ and (4) $P_2 = a(X)P$, $Q_2 = a(X)Q$, $P \sim^\bullet Q$, we need the following result.

Lemma 10. *Let $P \sim^\bullet Q$ such that $fv(P) \cup fv(Q) \subseteq \{X\}$, and $P_1 \sim_c^\bullet Q_1$ such that $P_1 \xrightarrow{\overline{a}} C_1$. There exists C_2 such that $Q_1 \xrightarrow{\overline{a}} C_2$ and $(X)P \bullet C_1 \equiv\sim_c^\bullet\equiv (X)Q \bullet C_2$.*

Remark. Lemmas 8 and 10 are defined up to $\equiv$ while Lemma 9 is not. Structural congruence is needed to move name restriction: suppose we have $P_1 \sim_c^\bullet Q_1$, $\nu b.P_2 \sim_c^\bullet \nu b.Q_2$, with $P_2 \sim_c^\bullet Q_2$, $P_1 \xrightarrow{a} F_1$, and $\nu b.P_2 \xrightarrow{\overline{a}} \nu b.C_2$ (which comes from $P_2 \xrightarrow{\overline{a}} C_2$). Using the induction with P_1, Q_1, P_2, and Q_2, there exist F_2 and C_2 such that $Q_1 \xrightarrow{a} F_2$, $Q_2 \xrightarrow{\overline{a}} C_2$, and $F_1 \bullet C_1 \sim_c^\bullet F_2 \bullet C_2$. We also have $\nu b.Q_2 \xrightarrow{\overline{a}} \nu b.C_2$. Note that, by our convention on bound names, b is neither in F_1 nor in F_2.

We want to prove $F_1 \bullet (\nu b.C_1) \sim_c^\bullet F_2 \bullet (\nu b.C_2)$, but from $F_1 \bullet C_1 \sim_c^\bullet F_2 \bullet C_2$, we can deduce $\nu b.(F_1 \bullet C_1) \sim_c^\bullet \nu b.(F_2 \bullet C_2)$ by congruence of $\sim_c^\bullet$. Depending on whether the scope of b has to be extended or not, it is not the same as $F_1 \bullet (\nu b.C_1) \sim_c^\bullet F_2 \bullet (\nu b.C_2)$; at best, we have $F_1 \bullet (\nu b.C_1) \equiv \nu b.(F_1 \bullet C_1) \sim_c^\bullet \nu b.(F_2 \bullet C_2) \equiv F_2 \bullet (\nu b.C_2)$, hence the need for $\equiv$. We do not have this issue in Lemma 9, since only messages, and not concretions, are involved.

For $\sim_c^\bullet$ to be a simulation, we have to prove the following result on τ-actions (by induction on the derivation of $P \sim_c^\bullet Q$), using Lemma 8 in the communication case.

Lemma 11. *If $P \sim_c^\bullet Q$ and $P \xrightarrow{\tau} P'$, then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \equiv\sim_c^\bullet\equiv Q'$.*

We can then prove $\sim_c^\bullet$ is a simulation up to $\equiv$. Suppose $P \sim_c^\bullet Q$. If $P \xrightarrow{a} F$, then for all $C = \nu\widetilde{b}.\langle R\rangle S$, we apply Lemma 8 with $P_2 = P$, $Q_2 = Q$, and $P_1 = Q_1 = \nu\widetilde{b}.\overline{a}\langle R\rangle S$. This yields an F' such that $Q \xrightarrow{a} F'$ and $F \bullet C \equiv\sim_c^\bullet\equiv F' \bullet C$. Similarly, if $P \xrightarrow{\overline{a}} C$, then for all $F = (X)R$, we apply Lemma 8 with $P_1 = P$, $Q_1 = Q$, and $P_2 = Q_2 = a(X)R$. We can then deduce that $(\equiv\sim_c^\bullet\equiv)^*$ is a bisimulation, and finally conclude $\sim = \equiv\sim_c^\bullet\equiv$, as explained in Section 2.3. Since $\equiv\sim_c^\bullet\equiv$ is a congruence, then $\sim$ is a congruence.

3 Application to a Calculus with Passivation

3.1 The HOπP Calculus

HOπP [10] extends HOπ with passivation, an operation that may stop a running process and capture its state. The granularity of passivation is the *locality* $a[P]$, a new construct added to the syntax of HOπ. The semantics of $a[P]$ is as follows: P can freely reduce and communicate with any other process; it may also be captured at any time by a process $a(X)R$, substituting its contents P for X

in R. Formally, we extend the locality construct to all agents, and we add the rules Loc and Passiv to the LTS of Figure 1.

$$a[(X)P] \triangleq (X)a[P] \qquad a[\nu\widetilde{b}.\langle P\rangle Q] \triangleq \nu\widetilde{b}.\langle P\rangle a[Q] \text{ if } a \notin \widetilde{b}$$

$$a[P] \xrightarrow{\overline{a}} \langle P\rangle 0 \text{ Passiv} \qquad \frac{P \xrightarrow{\alpha} A}{a[P] \xrightarrow{\alpha} a[A]} \text{ Loc}$$

The rule Loc and the definition of $a[C]$ imply that the scope of restricted names may cross locality boundaries, but structural congruence is left unchanged. In particular, $\nu b.a[P]$ is not congruent to $a[\nu b.P]$. Indeed, the combination of lazy scope extrusion and passivation may generate two distinct behaviors from these terms. See [10, Section 2.3] for more details.

3.2 Context Bisimilarity

The definition of context bisimulation is more complex in HOπP than in HOπ because of the discriminating power added by passivation. We briefly explain the differences; more details and examples can be found in [10, Section 2.4]. First, we can distinguish between processes with different free names using passivation and lazy scope extrusion [2]. Indeed, suppose a is free in P but not in Q, and consider the context $b[\nu a.\overline{c}\langle\Box\rangle R]$. Then a communication on c extends the scope of a outside b for P but not for Q, which gives us processes of the form $\nu a.(b[R] \mid P')$ and $b[\nu a.R] \mid Q'$ for some P' and Q'. If we then capture the locality b and duplicate its content, we obtain $\nu a.(R \mid R \mid P')$ in one case, and $(\nu a.R) \mid (\nu a.R) \mid Q'$ in the other: for the first process, a is shared, but not for the second one, and by choosing R accordingly, we obtain different behavior. Therefore, two processes P and Q are equivalent only if $\mathrm{fn}(P) = \mathrm{fn}(Q)$.

Next, when a message is sent outside a locality, the continuation stays in the locality (by definition of $a[C]$). The continuation can then be put into a completely different context using passivation. As a result, the message and its continuation may end up in different contexts, but still share a common information (the extruded names). To be able to express this situation specific to calculi with passivation, we introduce *bisimulation contexts* $\mathbb{E}$, i.e., evaluation contexts used for observational purposes.

$$\mathbb{E} ::= \Box \mid \nu a.\mathbb{E} \mid \mathbb{E} \mid P \mid P \mid \mathbb{E} \mid a[\mathbb{E}]$$

Instead of comparing $F \bullet C$ with $F \bullet C'$ in the output case, we now compare $F \bullet \mathbb{E}\{C\}$ with $F \bullet \mathbb{E}\{C'\}$. The extra context $\mathbb{E}$ represents the potential passivation of the continuations of C and C'. The definition of context bisimulation for HOπP is then as follows.

Definition 12. A relation $\mathcal{R}$ on closed processes is a context simulation if $P \mathrel{\mathcal{R}} Q$ implies $\mathrm{fn}(P) = \mathrm{fn}(Q)$ and:

- for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{R}} Q'$;

- for all $P \xrightarrow{a} F$, for all C, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C \mathcal{R} F' \bullet C$;
- for all $P \xrightarrow{\overline{a}} C$, for all F, $\mathbb{E}$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $F \bullet \mathbb{E}\{C\} \mathcal{R} F \bullet \mathbb{E}\{C'\}$.

A relation $\mathcal{R}$ is a context bisimulation if $\mathcal{R}$ and $\mathcal{R}^{-1}$ are context simulations. Context bisimilarity, written $\sim$, is the largest context bisimulation.

The usual approach to prove soundness of $\sim$ consists in proving that its transitive and congruence closure is a context bisimulation. This proof technique does not carry to the weak case. In [10], we prove soundness of a weak complementary bisimilarity, which coincides with a weak variant of $\sim$, by defining a weak complementary LTS for HOπP, with elaborate labels and subtle side-conditions in the LTS rules to handle lazy scope extrusion. The resulting LTS has almost twice as many rules as the contextual one.

We show here how to directly apply Howe's method with the contextual semantics, as in HOπ. We give these results for the strong bisimilarity $\sim$ to ease the presentation; the proofs for the weak case are in Appendix B. As usual when adapting Howe's method to calculi with passivation [5, 10], we have to extend Howe's closure to bisimulation contexts. We define $\mathbb{E}_1 \sim^\bullet \mathbb{E}_2$ as the smallest congruence satisfying the following rules.

$$\frac{\mathbb{E}_1 \sim^\bullet \mathbb{E}_2 \qquad P_1 \sim^\bullet P_2}{\mathbb{E}_1 \,|\, P_1 \sim^\bullet \mathbb{E}_2 \,|\, P_2} \qquad\qquad \frac{P_1 \sim^\bullet P_2 \qquad \mathbb{E}_1 \sim^\bullet \mathbb{E}_2}{P_1 \,|\, \mathbb{E}_1 \sim^\bullet P_2 \,|\, \mathbb{E}_2}$$

We can then write a pseudo-simulation lemma similar to Lemma 8, as follows.

Lemma 13 (Pseudo-Simulation Lemma)**.** *Let $P_1 \sim_c^\bullet Q_1$ and $P_2 \sim_c^\bullet Q_2$. If $P_1 \xrightarrow{\overline{a}} C_1$ and $P_2 \xrightarrow{a} F_1$, then for all $\mathbb{E}_1 \sim_c^\bullet \mathbb{E}_2$, there exist C_2, F_2 such that $Q_1 \xrightarrow{\overline{a}} C_2$, $P_2 \xrightarrow{a} F_2$, and $F_1 \bullet \mathbb{E}_1\{C_1\} \sim_c^\bullet F_2 \bullet \mathbb{E}_2\{C_2\}$.*

Unlike the case with HOπ, we do not have a choice in the induction strategy for the proof of Lemma 13: we cannot prove it by doing first the induction on the derivation for the receiving processes $P_2 \sim_c^\bullet Q_2$. Indeed, suppose $F_1 \bullet \mathbb{E}_1\{C_1\} \sim_c^\bullet F_2 \bullet \mathbb{E}_2\{C_2\}$ holds for all $\mathbb{E}_1 \sim_c^\bullet \mathbb{E}_2$, and we want to prove $b[F_1] \bullet \mathbb{E}_1\{C_1\} \sim_c^\bullet b[F_2] \bullet \mathbb{E}_2\{C_2\}$. With congruence of $\sim_c^\bullet$, we can only deduce $b[F_1 \bullet \mathbb{E}_1\{C_1\}] \sim_c^\bullet b[F_2 \bullet \mathbb{E}_2\{C_2\}]$, and we cannot move the boundaries of b with $\equiv$. Therefore, when reasoning by induction on the receiving processes $P_2 \sim_c^\bullet Q_2$, we cannot apply the resulting abstractions F_1, F_2 to concretions. However, we can apply them to messages, as in the following lemma, identical to Lemma 9.

Lemma 14. *Let $P_1^1 \sim_c^\bullet Q_1^1$ and $P_2 \sim_c^\bullet Q_2$ such that $P_2 \xrightarrow{a} F_1$. There exists F_2 such that $Q_2 \xrightarrow{a} F_2$, and $F_1 \circ P_1^1 \sim_c^\bullet F_2 \circ Q_1^1$.*

Indeed, if $F_1 \circ P_1^1 \sim_c^\bullet F_2 \circ Q_1^1$, then $b[F_1 \circ P_1^1] \sim_c^\bullet b[F_2 \circ Q_1^1]$ by congruence of $\sim_c^\bullet$. We then prove Lemma 13 by induction on the derivation for the sending processes $P_1 \sim_c^\bullet Q_1$. We do not have problems with localities when doing the induction on the derivation of $P_1 \sim_c^\bullet Q_1$, thanks to the bisimulation contexts: if $F_1 \bullet \mathbb{E}_1\{C_1\} \sim_c^\bullet F_2 \bullet \mathbb{E}_2\{C_2\}$ holds for all $\mathbb{E}_1 \sim_c^\bullet \mathbb{E}_2$, then it also holds for $\mathbb{E}_1\{b[\square]\} \sim_c^\bullet \mathbb{E}_2\{b[\square]\}$, and we have $F_1 \bullet \mathbb{E}_1\{b[C_1]\} \sim_c^\bullet F_2 \bullet \mathbb{E}_2\{b[C_2]\}$, as wished. Note that it also implies $F_1 \bullet \mathbb{E}_1\{\nu b.C_1\} \sim_c^\bullet F_2 \bullet \mathbb{E}_2\{\nu b.C_2\}$ by taking $\mathbb{E}_1\{\nu b.\square\} \sim_c^\bullet \mathbb{E}_2\{\nu b.\square\}$, therefore restriction poses no problem, and Lemma 13 is formulated without structural congruence, unlike Lemma 8. In addition to Lemma 13, we also prove a lemma similar to Lemma 11 for τ-actions, and then deduce that $\sim_c^\bullet$ is a simulation. We conclude as for HOπ.

Completeness. The strong and weak variants of the context bisimilarity $\sim$ coincide with respectively the strong and weak complementary bisimilarities of [10], which are themselves complete (see [10, Section 5.2]). Consequently, the strong and weak context bisimilarities are also complete.

4 Application to a Calculus with Join Patterns

4.1 Syntax and Semantics

Join patterns allow several messages to be received at once by the same process. The syntax of HOπJ is given in Figure 2. We replace the receiving process $a(X)P$ of HOπ by a process $\pi \triangleright P$, where π is a join pattern $a_1(X_1) \mid \ldots \mid a_n(X_n)$. A higher-order communication takes place when messages are available simultaneously on the names $a_1 \ldots a_n$. We write $\prod_{i\in\{1..n\}} x_i$ or $\prod \widetilde{x}$ (where x ranges over some entity) for the parallel composition $x_1 \mid \ldots \mid x_n$ if $n > 1$, or for simply x_1 if $n = 1$. We also abbreviate $\pi = a_1(X_1) \mid \ldots \mid a_n(X_n)$ as $\prod \widetilde{a(X)}$. The syntax of abstractions is changed accordingly ($F \triangleq (\pi)P$), and concretions now accumulate the messages of several emitting processes in parallel. A concretion is of the form $\nu\widetilde{b}.\langle a_1, P_1\rangle \ldots \langle a_n, P_n\rangle Q$, meaning that each process P_i is sent on the name a_i, and the scope of the names $\widetilde{b}$ has to be extended to encompass the recipient of the messages. We abbreviate $\nu\widetilde{b}.\langle a_1, P_1\rangle \ldots \langle a_n, P_n\rangle Q$ as $\nu\widetilde{b}.\widetilde{\langle a, P\rangle}Q$.

The semantics of HOπJ is given by the LTS rules of Figure 2, where the symmetric of rules Par, HO, and Part-HO are omitted. An input $P \xrightarrow{\widetilde{a}} F$ is labelled with the multiset $\widetilde{a}$ of names on which messages are expected, and an output $P \xrightarrow{\widetilde{\overline{a}}} C$ is labelled by the multiset $\widetilde{\overline{a}}$ of conames on which messages are sent. Operators are extended to all agents as in HOπ, with the addition of parallel composition of concretions, to deal with the case where two processes P and Q in parallel reduce to C_1 and C_2. The parallel composition of C_1 and C_2 is defined as a concretion C which merges the messages and extruded names of C_1 and C_2, and composes in parallel their continuations (Figure 2, rule Par-Out).

A process P, receiving on names $\widetilde{a}$ (i.e., such that $P \xrightarrow{\widetilde{a}} (\pi)P'$), may communicate with a process Q emitting on names $\widetilde{b}$ (i.e., such that $Q \xrightarrow{\widetilde{\overline{b}}} C$) if $\widetilde{b} \subseteq \widetilde{a}$. We have two possible outcomes: either $\widetilde{b} = \widetilde{a}$ and the resulting agent is a process (rule HO), or $\widetilde{b} \subsetneq \widetilde{a}$—some inputs of the join patterns are not

Syntax: $P ::= \mathbf{0} \mid X \mid P|P \mid \nu a.P \mid \overline{a}\langle P\rangle P \mid \pi \triangleright P \qquad \pi ::= \pi|\pi \mid a(X)$

Agents: $F ::= (\pi)P \qquad C ::= D \mid \nu a.D \qquad D ::= \langle a, P\rangle Q \mid \langle a, P\rangle D$

Parallel composition of concretions

$$\nu\widetilde{b}.\langle\widetilde{a,R}\rangle P \,|\, \nu\widetilde{b'}.\langle\widetilde{a',R'}\rangle Q \triangleq \nu\widetilde{b}\cup\widetilde{b'}.\langle\widetilde{a,R}\uplus\widetilde{a',R'}\rangle(P\,|\,Q)$$
$$\text{if } \widetilde{b}\cap \mathrm{fn}(Q) = \widetilde{b'}\cap\mathrm{fn}(P) = \widetilde{b}\cap\widetilde{b'} = \emptyset$$

Structural congruence for join patterns

$$\pi_1\,|\,\pi_2 \equiv \pi_2\,|\,\pi_1 \qquad\qquad \pi_1\,|\,(\pi_2\,|\,\pi_3) \equiv (\pi_1\,|\,\pi_2)\,|\,\pi_3$$

Pseudo-application

$$(\textstyle\prod \widetilde{a(X)})P \bullet \nu\widetilde{b}.\langle\widetilde{a,R}\rangle Q \vdash \nu\widetilde{b}.(P\{\widetilde{R}/\widetilde{X}\}\,|\,Q) \text{ if } \widetilde{b}\cap\mathrm{fn}(P)=\emptyset$$
$$(\textstyle\prod \widetilde{a(X)}\,|\,\pi)P \bullet \nu\widetilde{b}.\langle\widetilde{a,R}\rangle Q \vdash (\pi)\nu\widetilde{b}.(P\{\widetilde{R}/\widetilde{X}\}\,|\,Q) \text{ if } \widetilde{b}\cap\mathrm{fn}(P)=\emptyset$$

LTS rules: $\alpha_{\mathrm{j}} ::= \tau \mid \widetilde{a} \mid \widetilde{\overline{a}}$

$$\pi \triangleright P \xrightarrow{\widetilde{a}} (\pi)P \;\; \textsc{In} \qquad \overline{a}\langle Q\rangle P \xrightarrow{\overline{a}} \langle a, Q\rangle P \;\; \textsc{Out} \qquad \frac{P \xrightarrow{\alpha_{\mathrm{j}}} A}{P\,|\,Q \xrightarrow{\alpha_{\mathrm{j}}} A\,|\,Q} \;\; \textsc{Par}$$

$$\frac{P \xrightarrow{\widetilde{\overline{a}}} C_1 \qquad Q \xrightarrow{\widetilde{\overline{b}}} C_2}{P\,|\,Q \xrightarrow{\widetilde{\overline{a}}\uplus\widetilde{\overline{b}}} C_1\,|\,C_2} \;\; \textsc{Par-Out} \qquad \frac{P \xrightarrow{\widetilde{a}} F \qquad Q \xrightarrow{\widetilde{\overline{a}}} C \qquad F \bullet C \vdash P'}{P\,|\,Q \xrightarrow{\tau} P'} \;\; \text{HO}$$

$$\frac{P \xrightarrow{\alpha_{\mathrm{j}}} A \qquad a \notin \alpha_{\mathrm{j}}}{\nu a.P \xrightarrow{\alpha_{\mathrm{j}}} \nu a.A} \;\; \textsc{Restr}$$

$$\frac{P \xrightarrow{\widetilde{a}\uplus\widetilde{b}} F \qquad Q \xrightarrow{\widetilde{\overline{b}}} C \qquad \widetilde{a} \neq \emptyset \qquad F \bullet C \vdash F'}{P\,|\,Q \xrightarrow{\widetilde{a}} F'} \;\; \textsc{Part-HO}$$

Figure 2: Syntax and operational semantics of HOπJ

filled with Q—and we obtain an abstraction (rule Part-HO). For instance, we have $\overline{a}\langle R\rangle\mathbf{0} \mid (a(X) \mid b(Y)) \triangleright P \xrightarrow{b} (b(Y))P\{R/X\}$. The definition of $\bullet$ in Figure 2 takes into account these two cases. Besides, the pseudo-application of an abstraction to a concretion may generate several results, depending on how the matching between the outputs and the input is done. For instance, $\overline{a}\langle R_1\rangle\mathbf{0} \mid \overline{a}\langle R_2\rangle\mathbf{0} \mid (a(X) \mid a(Y)) \triangleright P$ can reduce to either $P\{R_1/X\}\{R_2/Y\}$, or $P\{R_2/X\}\{R_1/Y\}$ (assuming R_1 and R_2 closed). Consequently, we write $\bullet$ as a predicate $F \bullet C \vdash P$ (respectively $F \bullet C \vdash F'$), meaning that P (respectively F') can be obtained as a result of the pseudo-application of F to C.

4.2 Context Bisimilarity

The definition of context bisimilarity for HOπJ is the same as for HOπ, adapted to the fact that $\bullet$ may generate several results for a given F and C.

Definition 15. A relation $\mathcal{R}$ on closed processes is a context simulation if $P \mathrel{\mathcal{R}} Q$ implies:

- for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \mathrel{\mathcal{R}} Q'$;
- for all $P \xrightarrow{\widetilde{a}} F$, for all C, for all P' such that $F \bullet C \vdash P'$, there exist F', Q' such that $Q \xrightarrow{\widetilde{a}} F'$, $F' \bullet C \vdash Q'$, and $P' \mathrel{\mathcal{R}} Q'$;
- for all $P \xrightarrow{\widetilde{\overline{a}}} C$, for all F, for all P' such that $F \bullet C \vdash P'$, there exist C', Q' such that $Q \xrightarrow{\widetilde{\overline{a}}} C'$, $F \bullet C' \vdash Q'$, and $P' \mathrel{\mathcal{R}} Q'$.

A relation $\mathcal{R}$ is a context bisimulation if $\mathcal{R}$ and $\mathcal{R}^{-1}$ are context simulations. Context bisimilarity, written $\sim$, is the largest context bisimulation.

A similar context bisimulation has been defined for Kell [16], a higher-order calculus with passivation and join patterns. It is sound and complete in the strong case; the soundness proof of [16] does not rely on Howe's method, but instead shows that the reflexive, transitive, and congruence closure of the bisimilarity is itself a bisimulation. This direct method unfortunately does not scale to the weak case, as explained in [10]. Here, we prove that $\sim$ is a congruence using Howe's method. As in the previous section, even though we present the results in the strong case for simplicity, the complete proofs in Appendix C are for the weak case. To our knowledge, it is the first proof of soundness of a weak bisimilarity for a higher-order calculus with join patterns.

Bisimulation up to $\equiv$ is defined as in HOπ, by replacing $\mathcal{R}$ by $\equiv\mathcal{R}\equiv$ in the clauses. To prove that $\sim$ is sound with Howe's method, we use the following pseudo-simulation lemma.

Lemma 16 (Pseudo-Simulation Lemma)**.** *Let $P \sim_c^\bullet Q$ and $\widetilde{R} \sim_c^\bullet \widetilde{R'}$ such that $P \xrightarrow{\widetilde{a}} F$, $R_i \xrightarrow{\widetilde{\overline{a}}_i} C_i$ for all i, $\widetilde{a} = \biguplus_i \widetilde{a}_i$, and let P' such that $F \bullet \prod_i C_i \vdash P'$. Then there exist F', $\widetilde{C'}$, and Q' such that we have $Q \xrightarrow{\widetilde{a}} F'$, $R'_i \xrightarrow{\widetilde{\overline{a}}_i} C'_i$ for all i, $F' \bullet \prod_i C'_i \vdash Q'$, and $P' \equiv\sim_c^\bullet\equiv Q'$.*

We extend relations to multisets of same size in a pointwise way: $\widetilde{R} \sim_c^\bullet \widetilde{R'}$ means the two multisets are of the same size, and $R_i \sim_c^\bullet R'_i$ holds for every i. Note that Lemma 16 is a direct extension of Lemma 8 to multisets of sending processes; indeed, if we replace $\widetilde{R}$ and $\widetilde{R'}$ with single processes, we obtain the same formulation as Lemma 8 (with the exception that $\bullet$ is a predicate).

The proofs by serialization of Lemma 8, where we proceed by induction on the derivations for the the sender and then on the receiver (or conversely), do not apply to a calculus with join patterns, where a receiver communicates with several emitters—we cannot focus on a sender in particular, we have to consider them together. As a result, we consider another proof method, where we reason by induction on the derivations of $P \sim_c^\bullet Q$ and all the $\widetilde{R} \sim_c^\bullet \widetilde{R'}$ simultaneously. We distinguish two kinds of cases, depending on whether we need the induction hypothesis (detailed proofs are in Appendix C). Using the same definitions as in Lemmas 8 and 9, the cases where we do not need induction are those where each $R_i \sim_c^\bullet R'_i$ verifies either (1) or (2) (bisimilar, or congruent outputs), and $P \sim_c^\bullet Q$ verifies either (3) or (4) (bisimilar, or congruent inputs). In these cases, we can conclude using substitutivity of $\sim_c^\bullet$ and the definition of $\sim$. The remaining cases are dealt with by using the induction hypothesis, and then congruence of $\sim_c^\bullet$ and $\equiv$. Again, we rely on structural congruence to change the scope of names when needed (we have the same issue as described in Remark 2.4).

Using Lemma 16, we can prove that $\sim_c^\bullet$ is a simulation up to $\equiv$, and then conclude that $\equiv\sim_c^\bullet\equiv = \sim$ as in HOπ.

Completeness In Appendix D, we prove that a weak variant of $\sim$ is complete, using the usual technique of [15]. We can prove completeness in the strong case with a similar proof.

Remark. Proving Lemma 8 in HOπ is possible by reasoning simultaneously on $P_1 \sim_c^\bullet Q_1$ and $P_2 \sim_c^\bullet Q_2$, as described above. However, this method does not work for HOπP (Lemma 13) as pseudo-application and locality contexts do not commute (even up to structural congruence). One way to make the simultaneous induction works in calculi with passivation would be to add bisimulation contexts in the input clause, as follows:

- for all $P \xrightarrow{a} F$, for all C, there exists F' such that $Q \xrightarrow{a} F'$ and for all $\mathbb{E}$, we have $\mathbb{E}\{F\} \bullet C \mathcal{R} \mathbb{E}\{F'\} \bullet C$.

With such a definition, we can prove soundness of the resulting bisimilarity in a calculus with passivation and join patterns (such as Kell) with the simultaneous induction. However, this extra use of bisimulation context adds complexity to the bisimulation. We conjecture they are not necessary in the input case.

5 Related Work

Howe's method in process calculi. Howe's method has been originally used to prove congruence in a lazy functional programming language [7]. Baldamus and Frauenstein [1] are the first to adapt the method to process calculi for variants of Plain CHOCS [17], and prove in particular the soundness of a weak late delay context bisimilarity. Hildebrandt and Godskesen [5] then adapt Howe's method for their calculus Homer, to prove the congruence of a (delay) input-early context bisimilarity (see Section 2.3). In [10], we use Howe's method to prove congruence of strong and weak complementary bisimilarities in HOπ and HOπP. The Howe's proof of [10] is somewhat similar to the serialized proof of Sections 2 and 3, except for the symmetric formulation of the pseudo-simulation lemma. However, there is no equivalent to the simultaneous induction proof of Section 4 in [10].

Bisimilarities in calculi with passivation. In addition to the context (or complementary) bisimilarities already discussed for Kell [16], Homer [5], and HOπP [10], *environmental bisimilarities* [14] have also been defined by Piérard and Sumii for calculi with passivation [11, 12]. Such relations compare P and Q using an environment $\mathcal{E}$, which represents the knowledge that an observer has about these processes, like the messages they have sent. The observer then uses $\mathcal{E}$ to challenge P and Q. For instance, the observer is able to compare inputs from P and Q with any messages built from the processes inside $\mathcal{E}$. In [11], the authors propose a sound weak environmental bisimilarity for HOπP. Their approach is not complete, seemingly because of the interplay between "by need" scope extrusion and passivation. In [12], they consider a variant of HOπP with name creation instead of name restriction, for which they define a sound and complete weak environmental bisimilarity. With name creation, a name generated in a given locality becomes automatically known from the whole system. Name creation is therefore less expressive than name restriction with lazy scope extrusion, where we can control more finely the scope of generated names. In particular, it is not possible to implement internal choice or recursion using name creation, as shown in [8]. Finally, Koutavas and Hennessy recently developed a correct and complete symbolic bisimulation for a higher-order process calculus with passivation [8]. Their approach avoids the quantification over contexts at the cost of a more complex calculus, with local ports to recover the expressivity lost by using name creation.

Bisimilarities in calculi with join patterns. In [4], Fournet and Laneve define bisimilarities for the Join-Calculus, a first-order process calculus with join patterns. They define a weak bisimilarity which is sound w.r.t. the weak barbed congruence defined in [3], and also complete if name matching is added to the calculus. To our knowledge, only Kell [16] combines higher-order communication with join patterns. In [9], we define a weak complementary bisimilarity for Kell, which tests inputs by passing them messages one by one. This strategy requires processes to choose which input to perform without having all the necessary information (i.e., all the messages they are going to receive), and the resulting bisimilarity is therefore too discriminating (i.e., not complete).

6 Conclusion

In this paper, we showed how to directly use Howe's method to prove congruence properties of a context bisimilarity, without relying on an auxiliary relation such as complementary bisimilarity. We proposed a symmetric formulation of the pseudo-simulation lemma, which we can prove either with a serialized or with a simultaneous induction on the derivations for the emitting and receiving processes. The latter seems necessary in calculi with join patterns, while the former seems more appropriate for calculi with passivation. The resulting soundness proofs are much simpler than in complementary semantics [10], and they scale better to calculi with join patterns. Indeed, we compare receiving patterns by passing them several messages at once, and not only one by one as in the complementary case [9]. Finally, the bisimilarities of this paper are also complete in the weak case, unlike the input-early bisimilarity of [5], or the bisimilarity of [9] for join patterns. The use of Howe's method remains an open problem for calculi with both passivation and join patterns, such as Kell, if we do not want to make the definition of the bisimilarity more complex by using bisimulation contexts in the input case (see the remark at the end of Section 4).

References

[1] Michael Baldamus and Thomas Frauenstein. Congruence proofs for weak bisimulation equivalences on higher–order process calculi. Technical report, Berlin University of Technology, 1995.

[2] Giuseppe Castagna, Jan Vitek, and Francesco Zappa Nardelli. The Seal Calculus. *Information and Computation*, 201(1):1–54, 2005.

[3] Cédric Fournet and Georges Gonthier. The reflexive cham and the join-calculus. In *POPL '96*, pages 372–385. ACM Press, 1996.

[4] Cédric Fournet and Cosimo Laneve. Bisimulations in the join-calculus. *Theorectical Computer Science*, 266(1-2):569–603, 2001.

[5] Jens C. Godskesen and Thomas Hildebrandt. Extending howe's method to early bisimulations for typed mobile embedded resources with local names. In *FSTTCS '05*, volume 3821 of *LNCS*, pages 140–151. Springer, 2005.

[6] Andrew D. Gordon. Bisimilarity as a theory of functional programming. *Electronic Notes in Theoretical Computer Science*, 1:232–252, 1995.

[7] Douglas J. Howe. Proving congruence of bisimulation in functional programming languages. *Information and Computation*, 124(2):103–112, 1996.

[8] Vasileios Koutavas and Matthew Hennessy. Symbolic bisimulation for a higher-order distributed language with passivation. In *CONCUR '13*, pages 167–181. Springer-Verlag, 2013.

[9] Sergueï Lenglet. *Bisimulations dans les calculs avec passivation.* PhD thesis, Université de Grenoble, 2010.

[10] Sergueï Lenglet, Alan Schmitt, and Jean-Bernard Stefani. Characterizing contextual equivalence in calculi with passivation. *Information and Computation*, 209(11):1390–1433, 2011.

[11] Adrien Piérard and Eijiro Sumii. Sound bisimulations for higher-order distributed process calculus. In *FOSSACS '11*, volume 6604 of *LNCS*, pages 123–137. Springer, 2011.

[12] Adrien Piérard and Eijiro Sumii. A higher-order distributed calculus with name creation. In *LICS '12*, pages 531–540. IEEE, 2012.

[13] Davide Sangiorgi. Bisimulation for higher-order process calculi. *Information and Computation*, 131(2):141–178, 1996.

[14] Davide Sangiorgi, Naoki Kobayashi, and Eijiro Sumii. Environmental bisimulations for higher-order languages. *ACM Transactions on Programming Languages and Systems*, 33(1), 2011.

[15] Davide Sangiorgi and David Walker. *The Pi-Calculus: A Theory of Mobile Processes*. Cambridge University Press, 2001.

[16] Alan Schmitt and Jean-Bernard Stefani. The Kell Calculus: A Family of Higher-Order Distributed Process Calculi. In *Global Computing 2004 workshop*, volume 3267 of *LNCS*, 2004.

[17] Bent Thomsen. Plain chocs: A second generation calculus for higher order processes. *Acta Informatica*, 30(1):1–59, 1993.

A Congruence proof in HOπ

We prove the pseudo-simulation lemma by induction on the receiving processes.

Lemma 17. *For any relation $\mathcal{R}$, if $P \mathcal{R}^\bullet Q$, then there exists a substitution σ which closes P and Q such that $P\sigma \mathcal{R}^\bullet_c Q\sigma$, and the size of the derivation of $P\sigma \mathcal{R}^\bullet_c Q\sigma$ is equal to the size of the derivation of $P \mathcal{R}^\bullet Q$.*

Proof. Immediate induction on $P \mathcal{R}^\bullet Q$. □

Lemma 18. *Let $P \sim^\bullet Q$ such that $fv(P, Q) \subseteq \{X\}$. Then*

- *for all C, we have $(X)P \bullet C \sim^\bullet_c (X)Q \bullet C$;*
- *for all $P^1 \sim^\bullet_c Q^1$ and $P^2 \sim^\bullet_c Q^2$, we have $(X)P \bullet \langle P^1\rangle P^2 \sim^\bullet_c (X)Q \bullet \langle Q^1\rangle Q^2$.*

Proof. Immediate by substitutivity (Lemma 7) and congruence of $\sim^\bullet$. □

Lemma 19. *Let $P^1_1 \sim^\bullet_c Q^1_1$ and $P_2 \sim^\bullet_c Q_2$ such that $P_2 \xrightarrow{a} F$. There exists F_2 such that $Q_2 \xrightarrow{a} F_2$, and $F_1 \circ P^1_1 \sim^\bullet_c F_2 \circ Q^1_1$.*

Proof. By induction on the size of $P_2 \sim^\bullet_c Q_2$.

If $P_2 \sim Q_2$, then there exists F_2 such that $Q_2 \xrightarrow{a} F_2$ and $F_1 \bullet \langle Q^1_1\rangle \mathbf{0} \sim F_2 \bullet \langle Q^1_1\rangle \mathbf{0}$. By congruence of $\sim^\bullet_c$, we have $F_1 \bullet \langle P^1_1\rangle \mathbf{0} \sim^\bullet_c F_1 \bullet \langle Q^1_1\rangle \mathbf{0}$. Consequently, we have $F_1 \circ P^1_1 \sim^\bullet_c\sim F_2 \circ Q^1_1$, i.e., $F_1 \circ P^1_1 \sim^\bullet_c F_2 \circ Q^1_1$, as required.

If $P_2 \sim^\bullet R \sim^\circ Q_2$, then by Lemma 17, there exists σ closing R such that $P_2 \sim^\bullet_c R\sigma \sim Q_2$, with the derivation of $P_2 \sim^\bullet_c R\sigma$ of the same size as $P_2 \sim^\bullet R$. The result then follows by the induction hypothesis and the definitions of $\sim$ and $\sim^\bullet_c$.

If $P_2 = \mathsf{op}(\widetilde{P^i})$ and $Q_2 = \mathsf{op}(\widetilde{Q^i})$, then we proceed by case analysis on op.

Suppose $P_2 = a(X)P$, $Q_2 = a(X)Q$ with $P \sim^\bullet Q$. We have $Q_2 \xrightarrow{a} (X)Q$, and by Lemma 18, we have $(X)P \circ P^1_1 \sim^\bullet_c (X)Q \circ Q^1_1$, hence the result holds.

Suppose $P_2 = P^1 \,|\, P^2$, $Q_2 = Q^1 \,|\, Q^2$ with $P^1 \sim^\bullet_c Q^1$ and $P^2 \sim^\bullet_c Q^2$. Assume $P^1 \xrightarrow{a} F$, so that $F_1 = F \,|\, P^2$ (the case $P^2 \xrightarrow{a} F$ is similar). By induction, there exists F' such that $Q^1 \xrightarrow{a} F'$, and $F \circ P^1_1 \sim^\bullet_c F' \circ Q^1_1$. We then have $Q_2 \xrightarrow{a} F' \,|\, Q^2 \triangleq F_2$, and also $F_1 \circ P^1_1 = F \circ P^1_1 \,|\, P^2 \sim^\bullet_c F' \circ Q^1_1 \,|\, Q^2 = F_2 \circ Q^1_1$ (by congruence of $\sim^\bullet_c$). We therefore have $F_1 \circ P^1_1 \sim^\bullet_c F_2 \circ Q^1_1$, as required. The case $P_2 = \nu b.P$, $Q_2 = \nu b.Q$ with $P \sim^\bullet_c Q$ is similar. □

Lemma 20. *Let $P_1 \sim Q_1$, $P_2 \sim^\bullet_c Q_2$ such that $P_1 \xrightarrow{\overline{a}} C_1$ and $P_2 \xrightarrow{a} F$. There exist C_2, F_2 such that $Q_1 \xrightarrow{\overline{a}} C_2$, $Q_2 \xrightarrow{a} F_2$, and $F_1 \bullet C_1 \sim^\bullet_c F_2 \bullet C_2$.*

Proof. Suppose $C_1 = \nu\widetilde{b}.\langle R\rangle S$. By Lemma 19 (taking $P^1_1 = Q^1_1 = R$), there exists F_2 such that $Q_2 \xrightarrow{a} F_2$ and $F_1 \circ R \sim^\bullet_c F_2 \circ R$. By congruence of $\sim^\bullet_c$, we have $F_1 \bullet C_1 \sim^\bullet_c F_2 \bullet C_1$. From $P_1 \sim Q_1$, there exists C_2 such that $Q_1 \xrightarrow{\overline{a}} C_2$

and $F_2 \bullet C_1 \sim F_2 \bullet C_2$. We therefore have $F_1 \bullet C_1 \sim_c^\bullet \sim F_2 \bullet C_2$, i.e., $F_1 \bullet C_1 \sim_c^\bullet F_2 \bullet C_2$, as wished.

□

Lemma 21. *Let $P_1^1 \sim_c^\bullet Q_1^1$, $P_1^2 \sim_c^\bullet Q_1^2$, and $P_2 \sim_c^\bullet Q_2$ such that $P_2 \xrightarrow{a} F_1$. There exists F_2 such that $Q_2 \xrightarrow{a} F_2$ and $F_1 \bullet \langle P_1^1 \rangle P_1^2 \sim_c^\bullet F_2 \bullet \langle Q_1^1 \rangle Q_1^2$.*

Proof. Direct consequence of Lemma 19 and of congruence of $\sim_c^\bullet$. □

Lemma 22 (Simulation Lemma)**.** *Let $P_1 \sim_c^\bullet Q_1$ and $P_2 \sim_c^\bullet Q_2$.*

- *If $P_1 \xrightarrow{\tau} P'$, then there exists Q' such that $Q_1 \xrightarrow{\tau} Q'$ and $P' \equiv\sim_c^\bullet\equiv Q'$.*
- *If $P_1 \xrightarrow{\overline{a}} C_1$ and $P_2 \xrightarrow{a} F_1$, there exist C_2, F_2 such that $Q_1 \xrightarrow{\overline{a}} C'$, $P_2 \xrightarrow{a} F_2$, and $F_1 \bullet C_1 \equiv\sim_c^\bullet\equiv F_2 \bullet C_2$.*

Proof. By induction on the size of $P_1 \sim_c^\bullet Q_1$.

If $P_1 \sim Q_1$, then the first item is straightforward. The second item follows by Lemma 20.

If $P_1 \sim^\bullet R \sim^\circ Q_1$, then by Lemma 17, there exists σ closing R such that $P_1 \sim_c^\bullet R\sigma \sim Q_1$, with the derivation of $P_1 \sim_c^\bullet R\sigma$ of the same size as $P_1 \sim^\bullet R$. The result then follows easily using the induction hypothesis and the definition of $\sim$ (respectively Lemma 20) for the first (respectively second) item.

If $P_1 = \mathsf{op}(\widetilde{P^i})$ and $Q_1 = \mathsf{op}(\widetilde{Q^i})$, then we proceed by case analysis on op.

Suppose $P_1 = \overline{a}\langle P_1^1 \rangle P_1^2$, $Q_1 = \overline{a}\langle Q_1^1 \rangle Q_1^2$ with $P_1^1 \sim_c^\bullet Q_1^1$ and $P_1^2 \sim_c^\bullet Q_1^2$. The required result follows by Lemma 21.

Suppose $P_1 = P^1 \mid P^2$, $Q_1 = Q^1 \mid Q^2$ with $P^1 \sim_c^\bullet Q^1$ and $P^2 \sim_c^\bullet Q^2$. We distinguish several cases.

- Suppose $P^1 \xrightarrow{a} F$, $P^2 \xrightarrow{\overline{a}} C$, and $P \xrightarrow{\tau} F \bullet C$. By induction, there exist C', F' such that $Q^2 \xrightarrow{\overline{a}} C'$, $Q^1 \xrightarrow{a} F'$, and $F \bullet C \equiv\sim_c^\bullet\equiv F' \bullet C'$. We also have $Q \xrightarrow{\tau} F' \bullet C'$, hence the result holds.
- Suppose $P^1 \xrightarrow{\overline{a}} C$, and $P_1 \xrightarrow{\overline{a}} C \mid P_2 \triangleq C_1$ (the case $P^2 \xrightarrow{\overline{a}} C$ is similar). By induction, there exist C', F_2 such that $Q^1 \xrightarrow{\overline{a}} C'$, $Q_2 \xrightarrow{a} F_2$, and $F_1 \bullet C \equiv\sim_c^\bullet\equiv F_2 \bullet C'$. We have $Q_1 \xrightarrow{\overline{a}} C' \mid Q^2 \triangleq C_2$. By congruence of $\equiv$ and $\sim_c^\bullet$, we have $F_1 \bullet C_1 \equiv F_1 \bullet C \mid P^2 \equiv\sim_c^\bullet\equiv F_2 \bullet C' \mid Q^2$, i.e., $F_1 \bullet C_1 \equiv\sim_c^\bullet\equiv F_2 \bullet C_2$, as required.
- The cases $P^1 \xrightarrow{\tau} P^1$ and its symmetric $P^2 \xrightarrow{\tau} P^2$ are straightforward by induction.

Suppose $P_1 = \nu b.P$, $Q_1 = \nu b.Q$, $P \sim_c^\bullet Q$, and $P \xrightarrow{\overline{a}} C$ with $a \neq b$; then $P_1 \xrightarrow{\overline{a}} \nu b.C \triangleq C_1$. By induction, there exist C', F_2 such that $Q \xrightarrow{\overline{a}} C'$, $Q_2 \xrightarrow{a} F_2$, and $F_1 \bullet C \equiv\sim_c^\bullet\equiv F_2 \bullet C'$. We have $Q_1 \xrightarrow{\overline{a}} \nu b.C' \triangleq C_2$. By congruence of $\equiv$ and $\sim_c^\bullet$, we have $F_1 \bullet C_1 \equiv \nu b.(F_1 \bullet C) \equiv\sim_c^\bullet\equiv \nu b.(F_2 \bullet C') \equiv F_2 \bullet C_2$, i.e.,

$F_1 \bullet C_1 \equiv \sim^\bullet_c \equiv F_2 \bullet C_2$, as required. The case $P \xrightarrow{\tau} P'$ is straightforward by induction.

□

Lemma 23. *The relation $\sim^\bullet_c$ is a simulation up to $\equiv$.*

Proof. Consequence of Lemma 22. □

Corollary 24. *The relation $(\sim^\bullet_c)^*$ is a bisimulation up to $\equiv$.*

Proof. Consequence of Lemmas 23 and 7. □

Theorem 25. *The relation $\sim$ is a congruence.*

Proof. We have $\sim \subseteq \sim^\bullet_c \subseteq (\sim^\bullet_c)^* \subseteq \sim$, hence $\sim = \sim^\bullet_c$, and $\sim^\bullet_c$ is a congruence. □

B Congruence proof in HOπP

Lemma 26. *Let $P^1_1 \approx^\bullet_c Q^1_1$, and $P_2 \approx^\bullet_c Q_2$ such that $P_2 \xrightarrow{a} F_1$. There exists F_2, Q' such that $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_2 \circ Q^1_1 \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \circ P^1_1 \approx^\bullet_c Q'$.*

Proof. By induction on the size of $P_2 \approx^\bullet_c Q_2$.

If $P_2 \approx Q_2$, then there exist F_2, Q' such that $Q_2 \stackrel{a}{\Rightarrow} F_2$ and $F_2 \bullet \langle Q^1_1 \rangle \mathbf{0} \stackrel{\tau}{\Rightarrow} Q'$ and $F_1 \bullet \langle Q^1_1 \rangle \mathbf{0} \approx Q'$. By congruence of $\approx^\bullet_c$, we have $F_1 \circ P^1_1 \approx^\bullet_c F_1 \circ Q^1_1$. Consequently, we have $F_1 \circ P^1_1 \approx^\bullet_c \approx Q'$, i.e., $F_1 \circ P^1_1 \approx^\bullet_c Q'$, as required.

If $P_2 \approx^\bullet R \approx^\circ Q_2$, then by Lemma 17, there exists σ closing R such that $P_2 \approx^\bullet_c R\sigma \approx Q_2$, with the derivation of $P_2 \approx^\bullet_c R\sigma$ of the same size as $P_2 \approx^\bullet R$. The result then follows by the induction hypothesis and the definitions of $\approx$ and $\approx^\bullet_c$.

If $P_2 = \mathsf{op}(\widetilde{P^i})$ and $Q_2 = \mathsf{op}(\widetilde{Q^i})$, then we proceed by case analysis on op.

Suppose $P_2 = a(X)P$, $Q_2 = a(X)Q$ with $P \approx^\bullet Q$. We have $Q_2 \xrightarrow{a} (X)Q$, and by Lemma 18, we have $(X)P \circ P^1_1 \approx^\bullet_c (X)Q \circ Q^1_1$, hence the result holds.

Suppose $P_2 = P^1 \,|\, P^2$, $Q_2 = Q^1 \,|\, Q^2$ with $P^1 \approx^\bullet_c Q^1$ and $P^2 \approx^\bullet_c Q^2$. Assume $P^1 \xrightarrow{a} F$, so that $F_1 = F \,|\, P^2$ (the case $P^2 \xrightarrow{a} F$ is similar). By induction, there exists F', Q' such that $Q^1 \stackrel{a}{\Rightarrow} F'$, $F' \circ Q^1_1 \stackrel{\tau}{\Rightarrow} Q'$, and $F \circ P^1_1 \approx^\bullet_c Q'$. By congruence, we have $F \circ P^1_1 \,|\, P^2 \approx^\bullet_c Q' \,|\, P^2$, i.e., $F_1 \circ P^1_1 \approx^\bullet_c Q' \,|\, P^2$. We also have $Q_2 \stackrel{a}{\Rightarrow} F' \,|\, Q^2 \stackrel{\Delta}{=} F_2$, and $F_2 \circ Q^1_1 \stackrel{\tau}{\Rightarrow} Q' \,|\, P^2$, hence the result holds.

Suppose $P_2 = \nu b.P$, $Q_2 = \nu b.Q$ with $P \approx^\bullet_c Q$. The transition $P_2 \xrightarrow{a} F_1$ comes from $P \xrightarrow{a} F$ with $F_1 = \nu b.F$ and $a \neq b$. By induction, there exists F', Q' such that $Q^1 \stackrel{a}{\Rightarrow} F'$, $F' \circ Q^1_1 \stackrel{\tau}{\Rightarrow} Q'$, and $F \circ P^1_1 \approx^\bullet_c Q'$. By congruence, we have $\nu b.(F \circ P^1_1) \approx^\bullet_c \nu b.Q'$, i.e., $F_1 \circ P^1_1 \approx^\bullet_c \nu b.Q'$. We also have $Q_2 \stackrel{a}{\Rightarrow} \nu b.F' \stackrel{\Delta}{=} F_2$, and $F_2 \circ Q^1_1 \stackrel{\tau}{\Rightarrow} \nu b.Q'$, hence the result holds.

Suppose $P_2 = b[P]$, $Q_2 = b[Q]$ with $P \approx^\bullet_c Q$. The transition $P_2 \xrightarrow{a} F_1$ comes from $P \xrightarrow{a} F$ with $F_1 = b[F]$. By induction, there exists F', Q' such that $Q^1 \stackrel{a}{\Rightarrow} F'$, $F' \circ Q^1_1 \stackrel{\tau}{\Rightarrow} Q'$, and $F \circ P^1_1 \approx^\bullet_c Q'$. By congruence, we have

$b[F \circ P_1^1] \approx_c^\bullet b[Q']$, i.e., $F_1 \circ P_1^1 \approx_c^\bullet b[Q']$. We also have $Q_2 \stackrel{a}{\Rightarrow} b[F'] \triangleq F_2$, and $F_2 \circ Q_1^1 \stackrel{\tau}{\Rightarrow} b[Q']$, hence the result holds.

□

Lemma 27. *Let $P_1 \approx Q_1$, $P_2 \approx_c^\bullet Q_2$ such that $P_1 \xrightarrow{\overline{a}} C_1$ and $P_2 \xrightarrow{a} F_1$. Let $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$. There exist C_2, F_2, Q' such that $Q_1 \stackrel{\overline{a}}{\Rightarrow} C_2$, $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_2 \bullet \mathbb{E}_2\{C_2\} \stackrel{\tau}{\Rightarrow} Q'$ and $F_1 \bullet \mathbb{E}_1\{C_1\} \approx_c^\bullet Q'$.*

Proof. Suppose $C_1 = \nu\widetilde{b}.\langle R\rangle S$, and let $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$. Then by Lemma 26 (taking $P_1^1 = Q_1^1 = R$) , there exist F_2, Q'', such that $F_2 \circ R \stackrel{\tau}{\Rightarrow} Q''$, and $F_1 \circ R \approx_c^\bullet Q''$. We have $F_2 \bullet \mathbb{E}_2\{C_1\} \stackrel{\tau}{\Rightarrow} \nu\widetilde{b},\widetilde{c}.(Q'' \mid {\mathbb{E}'}_2\{C_1\}) \triangleq Q^{(3)}$ (where $\widetilde{c}$ are the names of R captured by $\mathbb{E}_2$, and $\mathbb{E}'_2$ is the context obtained from $\mathbb{E}_2$ by removing the restrictions on $\widetilde{c}$), and we have $F_1 \bullet \mathbb{E}_1\{C_1\} \approx_c^\bullet Q^{(3)}$ (by congruence of $\approx_c^\bullet$). By definition of $\approx$, there exists C_2, $Q^{(4)}$ such that $Q_1 \xrightarrow{\overline{a}} C_2$, $F_2 \bullet \mathbb{E}_2\{C_2\} \stackrel{\tau}{\Rightarrow} Q^{(4)}$, and $F_2 \bullet \mathbb{E}_2\{C_1\} \approx Q^{(4)}$. Because $F_2 \bullet \mathbb{E}_2\{C_1\} \stackrel{\tau}{\Rightarrow} Q^{(3)}$, there exists Q' such that $Q^{(4)} \stackrel{\tau}{\Rightarrow} Q'$ and $Q^{(3)} \approx Q'$. We therefore have $F_2 \bullet \mathbb{E}_2\{C_2\} \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \bullet \mathbb{E}_1\{C_1\} \approx_c^\bullet\approx Q'$, i.e., $F_1 \bullet \mathbb{E}_1\{C_1\} \approx_c^\bullet Q'$, hence the result holds. □

Lemma 28. *Let $P_1^1 \approx_c^\bullet Q_1^1$, $P_1^2 \approx_c^\bullet Q_1^2$, and $P_2 \approx_c^\bullet Q_2$ such that $P_2 \xrightarrow{a} F_1$. Let $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$. There exist F_2, Q' such that $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_2 \bullet \mathbb{E}_2\{\langle Q_1^1\rangle Q_1^2\} \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \bullet \mathbb{E}_1\{\langle P_1^1\rangle P_1^2\} \approx_c^\bullet Q'$.*

Proof. By Lemma 28, there exists F_2, Q' such that $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_2 \circ Q_1^1 \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \circ P_1^1 \approx_c^\bullet Q''$. By congruence of $\approx_c^\bullet$, we have $F_1 \bullet \mathbb{E}_1\{\langle P_1^1\rangle P_1^2\} \approx_c^\bullet \nu\widetilde{b}.(Q'' \mid {\mathbb{E}'}_2\{Q_1^2\})$ (where $\widetilde{b}$ are the names that need to be extruded, and $\mathbb{E}'_2$ can be obtained from $\mathbb{E}_2$ by removing the binders for $\widetilde{b}$), and we have $F_2 \bullet \mathbb{E}_2\{\langle Q_1^1\rangle Q_1^2\} = \nu\widetilde{b}.(F_2 \circ Q_1^1 \mid {\mathbb{E}'}_2\{Q_1^2\}) \stackrel{\tau}{\Rightarrow} \nu\widetilde{b}.(Q'' \mid {\mathbb{E}'}_2\{Q_1^2\})$, hence the result holds. □

Lemma 29 (Simulation Lemma)**.** *Let $P_1 \approx_c^\bullet Q_1$ and $P_2 \approx_c^\bullet Q_2$.*

- *If $P_1 \xrightarrow{\tau} P'$, then there exists Q' such that $Q_1 \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx_c^\bullet Q'$.*
- *If $P_1 \xrightarrow{\overline{a}} C_1$ and $P_2 \xrightarrow{a} F_1$, for all $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$, there exist C_2, F_2, Q' such that $Q_1 \stackrel{\overline{a}}{\Rightarrow} C_2$, $P_2 \stackrel{a}{\Rightarrow} F_2$, $F_2 \bullet \mathbb{E}_2\{C_2\} \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \bullet \mathbb{E}_1\{C_1\} \approx_c^\bullet Q'$.*

Proof. By induction on the size of $P_1 \approx_c^\bullet Q_1$.

If $P_1 \approx Q_1$, then the first item is straightforward. The second item follows by Lemma 27.

If $P_1 \approx^\bullet R \approx^\circ Q_1$, then by Lemma 17, there exists σ closing R such that $P \approx_c^\bullet R\sigma \approx Q$, with the derivation of $P \approx_c^\bullet R\sigma$ of the same size as $P \approx^\bullet R$. The result then follows easily using the induction hypothesis and the definition of $\approx$ (respectively Lemma 27) for the first (respectively second) item.

If $P_1 = \mathsf{op}(\widetilde{P^i})$ and $Q_1 = \mathsf{op}(\widetilde{Q^i})$, then we proceed by case analysis on op.

Suppose $P_1 = \overline{a}\langle P_1^1\rangle P_1^2$, $Q_1 = \overline{a}\langle Q_1^1\rangle Q_1^2$ with $P_1^1 \approx_c^\bullet Q_1^1$ and $P_1^2 \approx_c^\bullet Q_1^2$. The required result follows by Lemma 28.

Suppose $P_1 = P^1 \mid P^2$, $Q_1 = Q^1 \mid Q^2$ with $P^1 \approx_c^\bullet Q^1$ and $P^2 \approx_c^\bullet Q^2$. We distinguish several cases.

- Suppose $P^1 \xrightarrow{a} F$, $P^2 \xrightarrow{\overline{a}} C$, and $P \xrightarrow{\tau} F \bullet C$. By induction, there exist C', F', and Q' such that $Q^2 \stackrel{\overline{a}}{\Rightarrow} C'$, $Q^1 \stackrel{a}{\Rightarrow} F'$, $F' \bullet C' \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet C \approx_c^\bullet Q'$. We also have $Q \stackrel{\tau}{\Rightarrow} F' \bullet C'$, hence the result holds.

- Suppose $P^1 \xrightarrow{\overline{a}} C$, and $P_1 \xrightarrow{\overline{a}} C \mid P_2 \stackrel{\Delta}{=} C_1$ (the case $P^2 \xrightarrow{\overline{a}} C$ is similar). Let $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$. By induction, there exist C', F_2, Q' such that $Q^1 \stackrel{\overline{a}}{\Rightarrow} C'$, $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_1 \bullet \mathbb{E}_2\{C' \mid Q^2\} \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \bullet \mathbb{E}_1\{C \mid P^1\} \approx_c^\bullet Q'$ (using the fact that $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$ and $P^2 \approx_c^\bullet Q^2$ imply $\mathbb{E}_1\{\Box \mid P^1\} \approx_c^\bullet \mathbb{E}_2\{\Box \mid P^2\}$). We have $Q_1 \stackrel{\overline{a}}{\Rightarrow} C' \mid Q^2 \stackrel{\Delta}{=} C_2$, hence the result holds.

- The cases $P^1 \xrightarrow{\tau} P'^1$ and its symmetric $P^2 \xrightarrow{\tau} P'^2$ are straightforward by induction.

Suppose $P_1 = \nu b.P$, $Q_1 = \nu b.Q$, $P \approx_c^\bullet Q$, and $P \xrightarrow{\overline{a}} C$ with $a \neq b$; then $P_1 \xrightarrow{\overline{a}} \nu b.C \stackrel{\Delta}{=} C_1$. Let $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$. By induction, there exist C', F_2, Q' such that $Q^1 \stackrel{\overline{a}}{\Rightarrow} C'$, $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_1 \bullet \mathbb{E}_2\{\nu b.C'\} \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \bullet \mathbb{E}_1\{\nu b.C\} \approx_c^\bullet Q'$ (using the fact that $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$ implies $\mathbb{E}_1\{\nu b.\Box\} \approx_c^\bullet \mathbb{E}_2\{\nu b.\Box\}$). We have $Q_1 \stackrel{\overline{a}}{\Rightarrow} \nu b.C' \stackrel{\Delta}{=} C_2$, hence the result holds. The case $P \xrightarrow{\tau} P'$ is straightforward by induction.

Suppose $P_1 = b[P]$, $Q_1 = b[Q]$ with $P \approx_c^\bullet Q$. The case $P \xrightarrow{\tau} P'$ is straightforward by induction. The case $b[P] \xrightarrow{\overline{b}} \langle P \rangle \mathbf{0}$ follows from Lemma 28. Suppose $P \xrightarrow{\overline{a}} C$; then $P_1 \xrightarrow{\overline{a}} b[C] \stackrel{\Delta}{=} C_1$. Let $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$. By induction, there exist C', F_2, Q' such that $Q^1 \stackrel{\overline{a}}{\Rightarrow} C'$, $Q_2 \stackrel{a}{\Rightarrow} F_2$, $F_1 \bullet \mathbb{E}_2\{b[C']\} \stackrel{\tau}{\Rightarrow} Q'$, and $F_1 \bullet \mathbb{E}_1\{b[C]\} \approx_c^\bullet Q'$ (using the fact that $\mathbb{E}_1 \approx_c^\bullet \mathbb{E}_2$ implies $\mathbb{E}_1\{b[\Box]\} \approx_c^\bullet \mathbb{E}_2\{b[\Box]\}$). We have $Q_1 \stackrel{\overline{a}}{\Rightarrow} \nu b.C' \stackrel{\Delta}{=} C_2$, hence the result holds.

□

C Congruence Proof in HOπJ

We write $\stackrel{\tau}{\Rightarrow}$ for the reflexive and transitive closure of $\xrightarrow{\tau}$ and we write $\stackrel{\alpha_\mathrm{j}}{\Rightarrow}$ for the weak delay transition $\stackrel{\tau}{\Rightarrow}\xrightarrow{\alpha_\mathrm{j}}$ if $\alpha_\mathrm{j} \neq \tau$. Finally, we write $F \bullet C \vdash\stackrel{\tau}{\Rightarrow} P$ if there exists P' such that $F \bullet C \vdash P'$ and $P' \stackrel{\tau}{\Rightarrow} P$. We define weak context bisimilarity as follows.

Definition 30. A relation $\mathcal{R}$ on closed processes is a weak context simulation if $P \mathcal{R} Q$ implies:

- for all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \mathcal{R} Q'$;

- for all $P \xrightarrow{\widetilde{a}} F$, for all C, for all P' such that $F \bullet C \vdash P'$, there exist F', Q' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet C \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \mathcal{R} Q'$;

- for all $P \xrightarrow{\widetilde{\widetilde{a}}} C$, for all F, for all P' such that $F \bullet C \vdash P'$, there exist C', Q' such that $Q \stackrel{\widetilde{\widetilde{a}}}{\Rightarrow} C'$, $F \bullet C' \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \mathcal{R} Q'$.

A relation $\mathcal{R}$ is a weak context bisimulation if $\mathcal{R}$ and $\mathcal{R}^{-1}$ are weak context simulations. Weak context bisimilarity, written $\approx$, is the largest weak context bisimulation.

Note that we can use weak transitions for the moves of P.

Lemma 31. *If $P \approx Q$ then*

- *for all $P \stackrel{\tau}{\Rightarrow} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx Q'$;*
- *for all $P \stackrel{\widetilde{a}}{\Rightarrow} F$, for all C, for all P' such that $F \bullet C \vdash\stackrel{\tau}{\Rightarrow} P'$, there exist F', Q' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet C \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \approx Q'$;*
- *for all $P \stackrel{\widetilde{\widetilde{a}}}{\Rightarrow} C$, for all F, for all P' such that $F \bullet C \vdash\stackrel{\tau}{\Rightarrow} P'$, there exist C', Q' such that $Q \stackrel{\widetilde{\widetilde{a}}}{\Rightarrow} C'$, $F \bullet C' \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \approx Q'$.*

Proof. The result for τ-actions is proved by induction on the number of steps in $P \stackrel{\tau}{\Rightarrow} P'$. We then deduce the result for inputs and outputs. □

Lemma 32. *Let $P \approx_c^\bullet Q$ and $\widetilde{R} \approx_c^\bullet \widetilde{R'}$ such that $P \xrightarrow{\widetilde{a}} F$ and $R_i \xrightarrow{\widetilde{\widetilde{a}}_i} C_i$, with $\widetilde{a} = \bigcup_i \widetilde{\widetilde{a}}_i$, and P' such that $F \bullet \prod_i C_i \vdash P'$. There exist F', C_i', and Q' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $R_i' \stackrel{\widetilde{\widetilde{a}}_i}{\Rightarrow} C_i'$, $F' \bullet \prod_i C_i' \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \equiv\approx_c^\bullet\equiv Q'$.*

Proof. By induction on the sum of the sizes of $P \approx_c^\bullet Q$ and $\widetilde{R} \approx_c^\bullet \widetilde{R'}$. We distinguish several cases, depending on whether we need the induction hypothesis or not.

Case $P \approx_c^\bullet Q$ and $\widetilde{R} \approx_c^\bullet \widetilde{R'}$ not using induction on $\approx_c^\bullet$. This covers the cases where each of the R and R' are directly related by $\sim$ or they are message output whose sub-processes are related by $\approx_c^\bullet$, and either P and Q are directly related by $\approx$, or P and Q are message input whose sub-processes are related by $\approx_c^\bullet$.

We start by focusing on the R and R' processes. For each R and R' in $\widetilde{R} \approx_c^\bullet \widetilde{R'}$, assume we either have $R \approx R'$ (recall that they are closed), or $R = \overline{a_j}\langle T_j^1\rangle T_j^2$ and $R' = \overline{a_j}\langle {T'}_j^1\rangle {T'}_j^2$ with the sub-processes related by $\approx_c^\bullet$. We write S for processes of the first kind, and T for processes of the second kind. We have $\widetilde{R} = \widetilde{S} \uplus \widetilde{T}$, $\widetilde{R'} = \widetilde{S'} \uplus \widetilde{T'}$ and we let i range over $\widetilde{R}$ or $\widetilde{R'}$, k range over $\widetilde{S}$ or $\widetilde{S'}$, and j range over $\widetilde{T}$ and $\widetilde{T'}$. We thus have $S_k \approx S_k'$, $T_j = \overline{a_j}\langle T_j^1\rangle T_j^2$, $T_j' = \overline{a_j}\langle {T'}_j^1\rangle {T'}_j^2$, $T_j^l \approx_c^\bullet {T'}_j^l$ ($l \in \{1,2\}$). Finally, if $R_i = S_k$, then $S_k \xrightarrow{\widetilde{\widetilde{b}}_k} C_k = \nu\widetilde{c}_k.\langle\widetilde{d_k, U_k}\rangle V_k$ with $C_k = C_i$ and $\widetilde{\widetilde{b}}_k = \widetilde{\widetilde{a}}_i$. Similarly, if $R_i = T_j$, then $C_i = \langle a_j, T_j^1\rangle T_j^2$ and $\widetilde{\widetilde{a}}_i = a_j$.

We next derive a more general result that will allow us to proceed for the two ways by which P and Q may be related. Let F^a and F^b be two arbitrary abstractions such that $F^a \circ (\widetilde{\widetilde{d_k, U_k}}, \widetilde{a_j, T^1_j}) \vdash P'$ and $F^b \circ (\widetilde{\widetilde{d_k, U_k}}, \widetilde{a_j, T'^1_j}) \vdash P''$ implies $P' \approx^\bullet_c P''$ (these abstractions are applied to arbitrary but identical processes, and to the related messages from the T and T' processes). We now show that we can apply these abstractions to the concretions obtained from $\widetilde{R}$ and $\widetilde{R'}$, and keep the results (weakly) related. The first step consist of adding the continuations of the T and T' processes, and instantiate the arbitrary U processes with the concretions derived from of the S processes. By congruence of $\approx^\bullet_c$ and the definition of F^a and F^b, for any P' and P'' such that $F^a \bullet \prod_i C_i \vdash P'$ and $F^b \bullet (\prod_k C_k, \prod_j \langle a_j, T'^1_j \rangle T'^2_j) \vdash P''$, we have $P' \approx^\bullet_c P''$. Let P' and P'' be as such. We now show that we can change each C_k into C'_k and remain in the relation. Let k_0 be one of the k. We have $S_{k_0} \approx S'_{k_0}$, so by bisimilarity (taking the abstraction $F_0 = F^b \bullet (\prod_{k \neq k_0} C_k, \prod_j \langle a_j, T'^1_j \rangle T'^2_j))$, there exist C'_{k_0}, $P^{k_0}_0$, P^{k_0} such that $S'_{k_0} \stackrel{\widetilde{\widetilde{b}}_{k_0}}{\Longrightarrow} C'_{k_0}$, $F^b \bullet (\prod_{k \neq k_0} C_k, \prod_j \langle a_j, T'^1_j \rangle T'^2_j, C'_{k_0}) \vdash P^{k_0}_0$, $P^{k_0}_0 \stackrel{\tau}{\Rightarrow} P^{k_0}$ and $P'' \approx P^{k_0}$. We also define C'_{i_0} as C'_{k_0} for the index i_0 such that $S_{k_0} = R_{i_0}$. Note that the resulting processes are in the $\approx$ relation, and that by our notation conventions, we have the reduction $R'_{i_0} \stackrel{\widetilde{\widetilde{a}}_{i_0}}{\Longrightarrow} C'_{i_0}$. Consider now k_1 one of the k distinct from k_1. We have $S_{k_1} \approx S'_{k_1}$, so by bisimilarity (taking the abstraction $F_1 = F^b \bullet (\prod_{k \neq k_0, k_1} C_k, \prod_j \langle a_j, T'^1_j \rangle T'^2_j, C'_{k_0}))$, there exist C'_{k_1}, $P^{k_0}_0$, such that $S'_{k_1} \stackrel{\widetilde{\widetilde{b}}_{k_1}}{\Longrightarrow} C'_{k_1}$, $F^b \bullet (\prod_{k \neq k_0, k_1} C_k, \prod_j \langle a_j, T'^1_j \rangle T'^2_j, C'_{k_0}, C'_{k_1}) \vdash\stackrel{\tau}{\Rightarrow} P^{k_1}_0$, and $P^{k_0}_0 \approx P^{k_1}_0$. Because $P^{k_0}_0 \stackrel{\tau}{\Rightarrow} P^{k_0}$, there exists P^{k_1} such that $P^{k_1}_0 \stackrel{\tau}{\Rightarrow} P^{k_1}$ and $P^{k_0} \approx P^{k_1}$. As before, we define C'_{i_1} as C'_{k_1} for the index i_1 such that $S_{k_1} = R_{i_1}$. Repeating the process for the remaining k, we obtain $S'_k \stackrel{\widetilde{\widetilde{b}}_k}{\Longrightarrow} C'_k$, $F^b \bullet (\prod_k C'_k, \prod_j \langle a_j, T'^1_j \rangle T'^2_j) = F^b \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q'$ for some Q', and $P'' \approx Q'$ by transitivity of $\approx$. We conclude by right transitivity of $\approx^\bullet_c$ and $\approx$ that $P' \approx^\bullet_c Q'$.

We now turn to P and Q and consider the two cases for $P \approx^\bullet_c Q$ where induction is not needed: either $P \approx^\circ Q$, or $P = \pi \triangleright P'$, $Q = \pi \triangleright Q'$, with $P' \approx^\bullet_c Q'$. First, if $P \approx^\circ Q$, we then have $P \approx Q$ as they are closed. By congruence of $\approx^\bullet_c$, for all P', P'' such that $F \circ (\widetilde{\widetilde{d_k, U_k}}, \widetilde{a_j, T^1_j}) \vdash P'$ and $F \circ (\widetilde{\widetilde{d_k, U_k}}, \widetilde{a_j, T'^1_j}) \vdash P''$, we have $P' \approx^\bullet_c P''$; thus by taking $F^a = F^b = F$ and P' such that $F \bullet \prod_i C_i \vdash P'$, there exist $Q^{(3)}$, Q'' such that $F \bullet \prod_i C'_i \vdash Q^{(3)}$, $Q^{(3)} \stackrel{\tau}{\Rightarrow} Q''$ and $P' \approx^\bullet_c Q''$. From $P \stackrel{\widetilde{a}}{\rightarrow} F$, we deduce there exist F', $Q^{(4)}$ such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q^{(4)}$, and $Q^{(3)} \approx Q^{(4)}$. Because $Q^{(3)} \stackrel{\tau}{\Rightarrow} Q''$, there exists Q' such that $Q^{(4)} \stackrel{\tau}{\Rightarrow} Q'$ and $Q'' \approx Q'$. As a result, we have $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q'$, and by right transitivity of $\approx^\bullet_c$ and $\approx$, $P' \approx^\bullet_c Q'$, as required.

For the second case, suppose $P = \pi \triangleright P^0$, $Q = \pi \triangleright Q^0$, with $P^0 \approx^\bullet_c Q^0$. By substitutivity, for all P'', Q'' such that $(\pi)P^0 \circ (\widetilde{\widetilde{d_k, U_k}}, \widetilde{a_j, T^1_j}) \vdash P''$,

$(\pi)Q^0 \circ (\widetilde{\widetilde{d_k, U_k}}, \widetilde{a_j, T'^1_j}) \vdash Q''$, we have $P'' \approx^\bullet_c Q''$. Taking $F^a = (\pi)P^0$, $F^b = (\pi)Q^0$, and P' such that $(\pi)P^0 \bullet \prod_i C_i \vdash P'$, there exists Q' such that $(\pi)Q^0 \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx^\bullet_c Q'$, as wished.

Inductive cases. The remaining cases are those where either $P \approx^\bullet_c Q$ is not derived through $\approx$ or through congruence of input, or where one of the $R \approx^\bullet_c R'$ is not derived through $\approx$ or through congruence of output. For these cases we proceed using the induction hypothesis.

Suppose $P \approx^\bullet_c P^0 \approx Q$ and $\widetilde{R} \approx^\bullet_c \widetilde{R'}$ (as usual, we can close P^0 with Lemma 17). Let P' such that $F \bullet \prod_i C_i \vdash P'$. By induction, there exist F'', C'_i, and P'' such that $P^0 \stackrel{\widetilde{a}}{\Rightarrow} F''$, $R_i \stackrel{\widetilde{\widetilde{a}}_i}{\Rightarrow} C'_i$, $F'' \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} P''$, and $P' \equiv\approx^\bullet_c\equiv P''$. By Lemma 31, there exist F', Q' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P'' \approx Q'$. We conclude by using the fact that $\equiv \subseteq \approx$, and the definition of $\approx^\bullet_c$.

Suppose $P \approx^\bullet_c Q$ and $R_i \approx^\bullet_c R'_i$ for $i \neq i_0$, and $R_{i_0} \approx^\bullet_c R''_{i_0} \approx R'_{i_0}$ (as usual, we can close R''_{i_0}). Let P' such that $F \bullet \prod_i C_i \vdash P'$. By induction, there exist F', C'_i, C''_{i_0}, Q'' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $R_i \stackrel{\widetilde{\widetilde{a}}_i}{\Rightarrow} C'_i$, $R''_{i_0} \stackrel{\widetilde{\widetilde{a}}_{i_0}}{\Longrightarrow} C''_{i_0}$, $F' \bullet (\prod_{i\neq i_0} C'_i, C''_{i_0}) \vdash\stackrel{\tau}{\Rightarrow} Q''$, and $P' \equiv\approx^\bullet_c\equiv Q''$. By Lemma 31, there exist C'_{i_0}, Q' such that $R'_{i_0} \stackrel{\widetilde{a}}{\Rightarrow} C'_{i_0}$, $F' \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $Q'' \approx Q'$. We conclude by using the fact that $\equiv \subseteq \approx$, and the definition of $\approx^\bullet_c$.

Suppose $P = P^1 \mid P^2$, $Q = Q^1 \mid Q^2$, with $P^1 \approx^\bullet_c Q^1$, and $P^2 \approx^\bullet_c Q^2$, and $\widetilde{R} \approx^\bullet_c \widetilde{R'}$. We have several possibilities.

- $P^1 \stackrel{\widetilde{a}}{\rightarrow} F^1$, $F = F^1 \mid P^2$. Let P' such that $F \bullet \prod_i C_i \vdash P'$; there exists P'' such that $F^1 \bullet \prod_i C_i \vdash P''$ and $P' \equiv P'' \mid P^2$. By induction with $P^1 \approx^\bullet_c Q^1$ and the same $\widetilde{R}, \widetilde{R'}$, there exist F'^1, C'_1, and Q'' such that $Q^1 \stackrel{\widetilde{a}}{\Rightarrow} F'^1$, $R'_i \stackrel{\widetilde{\widetilde{a}}_i}{\Rightarrow} C'_i$, $F'_1 \bullet \prod_i C'_i \vdash\stackrel{\tau}{\Rightarrow} Q''$, and $P'' \equiv\approx^\bullet_c\equiv Q''$. We therefore have $Q \stackrel{\widetilde{a}}{\Rightarrow} F'^1 \mid Q^2 \stackrel{\Delta}{=} F'$, and $F' \bullet \prod_i C'_i \equiv F'_1 \bullet \prod_i C'_i \mid Q^2 \vdash\stackrel{\tau}{\Rightarrow} Q'' \mid Q^2 \stackrel{\Delta}{=} Q'$. From $P'' \equiv\approx^\bullet_c\equiv Q''$ and $P^2 \approx^\bullet_c Q^2$, we deduce $P'' \mid P^2 \equiv\approx^\bullet_c\equiv Q'' \mid Q^2$, i.e., $P' \equiv\approx^\bullet_c\equiv Q'$, as wished. The case $P^2 \stackrel{\widetilde{a}}{\rightarrow} F^2$, $F = P^1 \mid F^2$ is similar.

- $P^1 \xrightarrow{\widetilde{a}\uplus\widetilde{b}} F^1$, $P^2 \stackrel{\widetilde{\widetilde{b}}}{\rightarrow} C^2$, and $F = F^1 \bullet C^2$. We obtain the required result by applying the induction hypothesis on $P^1 \approx^\bullet_c Q^1$ and $P^2 \approx^\bullet_c Q^2, \widetilde{R} \approx^\bullet_c \widetilde{R'}$. The case $P^2 \xrightarrow{\widetilde{a}\uplus\widetilde{b}} F^1$, $P^1 \stackrel{\widetilde{\widetilde{b}}}{\rightarrow} C^2$, and $F = F^1 \bullet C^2$ is similar.

Suppose $P \approx^\bullet_c Q$, $R_i \approx^\bullet_c R'_i$ for $i \neq i_o$, $R_{i_0} = R^1_{i_0} \mid R^2_{i_0}$, $R'_{i_0} = R'^1_{i_0} \mid R'^2_{i_0}$, $R^1_{i_0} \approx^\bullet_c R'^1_{i_0}$, and $R^2_{i_0} \approx^\bullet_c R'^2_{i_0}$. We have several possibilities.

- $R^1_{i_0} \xrightarrow{\widetilde{\widetilde{a}}_{i_0}} C$, $C_{i_0} = C \mid R^2_{i_0}$. Let P' such that $F \bullet (\prod_i C_i) \vdash P'$; there exists P'' such that $F \bullet (\prod_{i\neq i_0} C_i, C^1_{i_0}) \vdash P''$ and $P' \equiv P'' \mid R^2_{i_0}$. By induction with $R^1_{i_0}$ instead of R_i, there exist F', C'_i, $C'^1_{i_0}$, and Q'' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $R'_i \stackrel{\widetilde{\widetilde{a}}_i}{\Rightarrow} C'_i$, ${R'}^1_{i_0} \stackrel{\widetilde{\widetilde{a}}_{i_0}}{\Longrightarrow} {C'}^1_{i_0}$, $F' \bullet (\prod_i C'_i, {C'}^1_{i_0}) \vdash\stackrel{\tau}{\Rightarrow} Q''$, and $P'' \equiv\approx^\bullet_c\equiv Q''$. We therefore have $R'_{i_0} \stackrel{\widetilde{a}_{i_0}}{\Longrightarrow} {C'}^1_{i_0} \,|\, {R'}^2_{i_0} \stackrel{\Delta}{=} {C'}_{i_0}$, with $F' \bullet \prod_i C'_i \equiv F' \bullet \prod_{i \neq i_0} C'_i, {C'}^1_{i_0} \,|\, {R'}^2_{i_0} \vdash\stackrel{\tau}{\Rightarrow} Q'' \,|\, {R'}^2_{i_0} \stackrel{\Delta}{=} Q'$. From $P'' \equiv\approx^\bullet_c\equiv Q''$ and $R^2_{i_0} \approx^\bullet_c {R'}^2_{i_0}$, we deduce $P'' \,|\, R^2_{i_0} \equiv\approx^\bullet_c\equiv Q'' \,|\, {R'}^2_{i_0}$, i.e., $P' \equiv\approx^\bullet_c\equiv Q'$, as wished. The case $R^2_{i_0} \xrightarrow{\widetilde{a}_{i_0}} C$, $C_{i_0} = R^1_{i_0} \,|\, C$ is similar.

- $R^1_{i_0} \xrightarrow{\widetilde{a}^1_{i_0}} C^1_{i_0}$, $R^2_{i_0} \xrightarrow{\widetilde{a}^2_{i_0}} C^2_{i_0}$, $C_{i_0} = C^1_{i_0} \,|\, C^2_{i_0}$. We obtain the required result by applying the induction hypothesis on $P \approx^\bullet_c Q$, $R_i \approx^\bullet_c R'_i$ for $i \neq i_0$, and $R^l_{i_0} \approx^\bullet_c {R'}^l_{i_0}$ $(l \in \{1, 2\})$.

Suppose $P = \nu b.P'$, $Q = \nu b.Q'$, with $P' \approx^\bullet_c Q'$, and $\widetilde{R} \approx^\bullet_c \widetilde{R'}$. The transition $P \xrightarrow{\widetilde{a}} F$ comes from $P' \xrightarrow{\widetilde{a}} F_1$ and $F = \nu b.F_1$. We can apply the induction hypothesis with P', Q' instead of P, Q, and then conclude with congruence (we need up to $\equiv$ to move the νb around).

Suppose $P \approx^\bullet_c Q$, $R_i \approx^\bullet_c R'_i$ for $i \neq i_o$, $R_{i_0} = \nu b.R^1_{i_0}$, $R'_{i_0} = \nu b.{R'}^1_{i_0}$, and $R^j_{i_0} \approx^\bullet_c {R'}^j_{i_0}$, and $\widetilde{R} \approx^\bullet_c \widetilde{R'}$. Same as the case above.

□

Lemma 33. *$\approx^\bullet_c$ is a simulation up to $\equiv$.*

Proof. Let $P \approx^\bullet_c Q$. Suppose $P \xrightarrow{\widetilde{a}} F$, let C be a concretion, and let P' such that $F \bullet C \vdash P'$. By Lemma 32 (taking $R = \widetilde{\overline{a}}.C$ and since $\approx^\bullet_c$ is reflexive), there exist F', Q' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet C \vdash\stackrel{\tau}{\Rightarrow} Q'$ and $P' \equiv\approx^\bullet_c\equiv Q'$ (since R can only reduce to C). The case $P \xrightarrow{\widetilde{\overline{a}}} C$ is similar.

If $P \xrightarrow{\tau} P'$, we proceed by induction on $P \approx^\bullet_c Q$. All the cases are straightforward, except for HO communication, where we can use Lemma 32.

□

D Completeness in HOπJ

In this section, we prove completeness of weak context bisimilarity w.r.t. barbed congruence in HOπJ. We define reduction $\longrightarrow$ as $\equiv\xrightarrow{\tau}\equiv$ and weak reduction $\Longrightarrow$ as the reflexive and transitive closure of $\longrightarrow$. The observable actions of a process P are either sets of names on which a reception can be done (if $P \xrightarrow{\widetilde{a}} F$, then $P \downarrow_{\widetilde{a}}$), or names on which an emission may occur (if $P \xrightarrow{\overline{a}} C$, then $P \downarrow_{\overline{a}}$). We write $P \Longrightarrow\downarrow_\gamma$ if there exists P' such that $P \Longrightarrow P'$ and $P' \downarrow_\gamma$ We let γ range over conames and sets of names. The definition of weak barbed congruence is then as follows.

Definition 34. A symmetric relation on closed processes $\mathcal{R}$ is a weak barbed bisimulation iff $P \mathrel{\mathcal{R}} Q$ implies:

- for all $P \downarrow_\gamma$, we have $Q \Longrightarrow\downarrow_\gamma$;
- for all $P \longrightarrow P'$, there exists Q' such that $Q \Longrightarrow Q'$ and $P' \mathcal{R}\, Q'$.

Two processes P, Q are *weak barbed congruent*, written $P \approx_b Q$, if for all $\mathbb{C}$ there exists a weak barbed bisimulation $\mathcal{R}$ such that $\mathbb{C}\{P\} \mathcal{R}\, \mathbb{C}\{Q\}$.

We prove completeness on image-finite processes only, a usual restriction when proving completeness in process calculi [15]. We define image-finite processes as follows.

Definition 35. A process P is image finite iff

- the set $\{P' \mid P \stackrel{\tau}{\Rightarrow} P'\}$ is finite;
- for all $\widetilde{a}$, C, the set $\{P' \mid \exists F, P \stackrel{\widetilde{a}}{\Rightarrow} F \wedge (F \bullet C) \vdash\stackrel{\tau}{\Rightarrow} P'\}$ is finite;
- for all $\widetilde{\widetilde{a}}$, C, the set $\{P' \mid \exists C, P \stackrel{\widetilde{\widetilde{a}}}{\Rightarrow} C \wedge (F \bullet C) \vdash\stackrel{\tau}{\Rightarrow} P'\}$ is finite.

We now prove the completeness of $\approx$ on image-finite processes. The method is standard [15] and relies on a decomposition of $\approx$ into a family of relations $(\approx^k)_{k \geq 0}$.

Definition 36. We define $(\approx^k)_{k\geq 0}$ as:

- we have $P \approx^0 Q$ for all P, Q;
- we have $P \approx^{k+1} Q$ if
  - for all $P \stackrel{\tau}{\rightarrow} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx^k Q'$;
  - for all $P \stackrel{\widetilde{a}}{\rightarrow} F$, for all C, for all P' such that $F \bullet C \vdash P'$, there exist F', Q' such that $Q \stackrel{\widetilde{a}}{\Rightarrow} F'$, $F' \bullet C \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \approx^k Q'$;
  - for all $P \stackrel{\widetilde{\widetilde{a}}}{\rightarrow} C$, for all F, for all P' such that $F \bullet C \vdash P'$, there exist C', Q' such that $Q \stackrel{\widetilde{\widetilde{a}}}{\Rightarrow} C'$, $F \bullet C' \vdash\stackrel{\tau}{\Rightarrow} Q'$, and $P' \approx^k Q'$;
  - the symmetric cases with the transitions from Q.

The relation $\approx^\omega$ is defined as $\approx^\omega \triangleq \bigcap_{k \in \mathcal{N}} \approx^k$.

Roughly, we have $P \approx^k Q$ iff P and Q can mimic each others on k transition steps. Note that for all k, we have $\approx_{k+1} \subseteq \approx_k$ by definition.

In the following, we write $a.P$ for $a(X) \triangleright P$ with $X \notin \mathrm{fv}(P)$ and $\overline{a}.P$ for $\overline{a}\langle \mathbf{0} \rangle P$. We often omit the trailing $\mathbf{0}$; in particular, we write a for $a.\mathbf{0}$. We define an operator $\oplus$ as:

$$\bigoplus_{j=1}^{n} P_j \quad \triangleq \quad \nu a.(\overline{a}\langle P_1 \rangle \mathbf{0} \,|\, \ldots \,|\, \overline{a}\langle P_n \rangle \mathbf{0} \,|\, a(X)X)$$

The operator $\oplus$ is a choice operator, with the following properties:

- $P \oplus a \Longrightarrow\downarrow_a$;
- for all $i \in \{1 \dots n\}$, we have $\bigoplus_{j=1}^{n} P_j \stackrel{\tau}{\Rightarrow}\sim P_i$.

We are now ready to prove the main result for completeness.

Lemma 37. *If P, Q are image finite and $P \not\approx^k Q$, then there exists R such that for all fresh name a, one of the following holds:*

1. $P' \,|\, (R \oplus a) \not\approx_b Q \,|\, (R \oplus a)$ *for all P' such that $P \Longrightarrow P'$;*
2. $P \,|\, (R \oplus a) \not\approx_b Q' \,|\, (R \oplus a)$ *for all Q' such that $Q \Longrightarrow Q'$.*

Proof. By induction on k. There is nothing to prove for $k = 0$. Let $k > 0$. Either a transition from P is not matched by Q or the opposite holds (a transition of Q is not matched by P). We put ourselves in the former case, and we prove (2) holds; in the latter case, one would prove (1). We distinguish several cases.

Assume a transition $P \xrightarrow{\tau} P'$ is not matched by Q. For all $Q \stackrel{\tau}{\Rightarrow} Q'$, we have $P' \not\approx^{k-1} Q'$. Since Q is image-finite, the set $\{Q_i \mid Q \stackrel{\tau}{\Rightarrow} Q_i\}$ is finite, and by induction, there exist (R_i) verifying the lemma for each P', Q_i. Given some fresh names (b_i), we define $R \triangleq \bigoplus_i (R_i \oplus b_i)$. Let Q' such that $Q \Longrightarrow Q'$, and let a be a fresh name. Suppose, for a contradiction, that $P \mid (R \oplus a) \approx_b Q' \mid (R \oplus a)$. The transition $P \mid (R \oplus a) \longrightarrow P' \mid (R \oplus a) \triangleq P_2$ can only be matched by $Q' \,|\, (R \oplus a) \Longrightarrow Q_j \,|\, (R \oplus a) \triangleq Q_2$ for some j, because $P_2 \Longrightarrow\downarrow_a$. We have $P_2 \approx_b Q_2$, and either (1) or (2) holds for P', Q_j, and R_j. If (2) holds, then $P_2 (\longrightarrow)^2 \sim P' \mid (R_j \oplus b_j) \triangleq P_3$ can only be matched by $Q_2 \Longrightarrow\sim Q'_j \mid (R_j \oplus b_j) \triangleq Q_3$ for some $Q_j \Longrightarrow Q'_j$, because $P_3 \Longrightarrow\downarrow_{b_j}$. We have $P_3 \not\approx_b Q_3$ by the induction hypothesis, hence a contradiction. If (1) holds, the reasoning is the same by matching the transition $Q_2 (\longrightarrow)^2 \sim Q_j \,|\, (R_j \oplus b_j)$.

Assume a transition $P \xrightarrow{\widetilde{a}} F$ is not matched by Q. Let C be a concretion, and P' such that $F \bullet C \vdash P'$. For all $Q \stackrel{\widetilde{a}}{\Rightarrow} F$, $F \bullet C \vdash\stackrel{\tau}{\Rightarrow} Q'$, we have $P' \not\approx^{k-1} Q'$. Since Q is image-finite, the set $\{Q_i \mid Q \stackrel{\widetilde{a}}{\Rightarrow} F, F \bullet C \vdash\stackrel{\tau}{\Rightarrow} Q_i\}$ is finite, and by induction, there exist (R_i) verifying the lemma for each P', Q_i. Suppose $C = \nu\widetilde{d}.\langle a_0, S_0\rangle \dots \langle a_n, S_n\rangle T$. Given some fresh names (b_i), (c_j), we define

$$R \triangleq \nu\widetilde{d}.(\overline{a_0}\langle S_0\rangle(T \,|\, c_1.c_2.\dots.c_n.\bigoplus_i (R_i \oplus b_i)) \,|\, \prod_{j>0} \overline{a_j}\langle S_j\rangle\overline{c_j}).$$

Let Q' such that $Q \Longrightarrow Q'$, and let a be a fresh name. Suppose, for a contradiction, that $P \,|\, (R \oplus a) \approx_b Q' \,|\, (R \oplus a)$. The transition

$$P \,|\, (R \oplus a)(\longrightarrow)^2 \sim P' \,|\, c_1.c_2.\dots.c_n.\bigoplus_i (R_i \oplus b_i) \,|\, \prod_{j>0} \overline{c_j} \triangleq P_2$$

can only be matched by

$$Q' \,|\, (R \oplus a) \Longrightarrow\sim Q_l \,|\, c_1.c_2.\dots.c_n.\bigoplus_i (R_i \oplus b_i) \,|\, \prod_{j>0} \overline{c_j} \triangleq Q_2$$

for some l, because $P_2 \Longrightarrow\downarrow_{\overline{c_j}}$ for all $j > 0$ and $P_2 \Longrightarrow\downarrow_{c_1}$. We have $P_2 \approx_b Q_2$, and $P_2 \longrightarrow^n P' \mid \bigoplus_i (R_i \oplus b_i) \triangleq P_3$, which can only be matched by $Q_2 \Longrightarrow Q_j \mid \bigoplus_i (R_i \oplus b_i) \triangleq Q_3$ for some j. We have $P_3 \approx_b Q_3$, and either (1) or (2) holds for P', Q_j, and R_j. If (2) holds, then $P_3 (\longrightarrow)^2 \sim P' \mid (R_j \oplus b_j) \triangleq P_4$ can only be matched by $Q_3 \Longrightarrow\sim Q'_j \mid (R_j \oplus b_j) \triangleq Q_4$ for some $Q_j \Longrightarrow Q'_j$, because $P_4 \Longrightarrow\downarrow_{b_j}$. We have $P_4 \not\approx_b Q_4$ by the induction hypothesis, hence a contradiction. If (1) holds, the reasoning is the same by trying to match the transition $Q_3 (\longrightarrow)^2 \sim Q_j \mid (R_j \oplus b_j)$.

Assume a transition $P \xrightarrow{\tilde{\tilde{a}}} C$ **is not matched by** Q**.** Let F be an abstraction, and P' such that $F \bullet C \vdash P'$. For all $Q \overset{\tilde{\tilde{a}}}{\Rightarrow} C$, $F \bullet C \vdash\overset{\tau}{\Rightarrow} Q'$, we have $P' \not\approx^{k-1} Q'$. Since Q is image-finite, the set $\{Q_i \mid Q \overset{\tilde{\tilde{a}}}{\Rightarrow} C, F \bullet C \vdash\overset{\tau}{\Rightarrow} Q_i\}$ is finite, and by induction, there exist (R_i) verifying the lemma for each P', Q_i. Suppose $F = \pi \triangleright S$. Given some fresh name (b_i), we define $R \triangleq \pi \triangleright (S \mid \bigoplus_i (R_i \oplus b_i))$. Let Q' such that $Q \Longrightarrow Q'$, and let a be a fresh name. Suppose, for a contradiction, that $P \mid (R \oplus a) \approx_b Q' \mid (R \oplus a)$. The transition $P \mid (R \oplus a) (\longrightarrow)^2 \sim P' \mid \bigoplus_i (R_i \oplus b_i) \triangleq P_2$ can only be matched by $Q' \mid (R \oplus a) \Longrightarrow\sim Q_j \mid \bigoplus_i (R_i \oplus b_i) \triangleq Q_2$ for some j, because $P_2 \Longrightarrow\downarrow_{\overline{b_i}}$ for all i. We have $P_2 \approx_b Q_2$, and either (1) or (2) holds for P', Q_j, and R_j. If (2) holds, then $P_2 (\longrightarrow)^2 \sim P' \mid (R_j \oplus b_j) \triangleq P_3$ can only be matched by $Q_2 \Longrightarrow\sim Q'_j \mid (R_j \oplus b_j) \triangleq Q_3$ for some $Q_j \Longrightarrow Q'_j$, because $P_3 \Longrightarrow\downarrow_{b_j}$. We have $P_3 \not\approx_b Q_3$ by the induction hypothesis, hence a contradiction. If (1) holds, the reasoning is the same by trying to match the transition $Q_2 (\longrightarrow)^2 \sim Q_j \mid (R_j \oplus b_j)$.

□

RESEARCH CENTRE
RENNES – BRETAGNE ATLANTIQUE

Campus universitaire de Beaulieu
35042 Rennes Cedex

Publisher
Inria
Domaine de Voluceau - Rocquencourt
BP 105 - 78153 Le Chesnay Cedex
inria.fr

ISSN 0249-6399