Howe's Method for Early Bisimilarities

Sergueï Lenglet, Alan Schmitt, Jean-Bernard Stefani

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Howe's Method for Early Bisimilarities

Sergueï Lenglet — Alan Schmitt — Jean-Bernard Stefani

N° 6773

December 2008

Thème COM

ISSN 0249-6399 ISRN INRIA/RR--6773--FR+ENG

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

centre de recherche
GRENOBLE - RHÔNE-ALPES

Howe's Method for Early Bisimilarities

Sergueï Lenglet , Alan Schmitt , Jean-Bernard Stefani

Thème COM — Systèmes communicants
Équipes-Projets SARDES

Rapport de recherche n° 6773 — December 2008 — 70 pages

Abstract: This report shows how to apply Howe's method for the proof of congruence of early bisimilarities in higher-order process calculi. This involves the introduction of a new kind of transition system and a new kind of bisimilarity, collectively called complementary semantics. We show that complementary semantics is equivalent to contextual semantics, originally introduced by Sangiorgi, that relies on classical transition systems for higher-order calculi and context bisimilarity.

Key-words: Process calculus, bisimilarity, bisimulation, early bisimilarity, Howe's method, higher-order calculus, congruence proof

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

La méthode de Howe pour bisimilarités précoces

Résumé : Ce rapport montre comment appliquer la méthode de Howe pour la preuve de congruence de bisimilarités précoces dans des calculs de processus d'ordre supérieur. Pour cela, nous introduisons une nouvelle forme de système de transition et une nouvelle forme de bisimilarité, que nous appelons sémantique complémentaire. Nous montrons que la sémantique complémentaire est équivalente à la sémantique contextuelle, introduite par Sangiorgi, qui s'appuie sur des systèmes de transition classiques pour calculs d'ordre supérieur, et sur une bisimilarité contextuelle.

Mots-clés : Calcul de processus, bisimilarité, bisimulation, bisimilarité précoce, méthode de Howe, calcul d'ordre supérieur, preuve de congruence.

Contents

1 Introduction

Motivation A natural notion of behavioral equivalence for process calculi is *barbed congruence*. Informally, two processes are barbed-congruent if they behave in the same way (i.e., have the same reductions and the same observables) when placed in similar, but arbitrary, contexts. Due to this quantification on contexts, barbed congruence is unwieldy to use in proofs of equivalence, or to serve as a basis for automated verification tools. One is thus lead to study coinductive characterizations of barbed congruence, typically in the form of bisimilarity relations. For first-order process calculi, such as the π-calculus and its variants, the resulting behavioral theory is well developed, and one can in general readily define bisimilarity relations that characterize barbed congruence.

For higher-order process calculi, the situation is less satisfactory. Simple higher-order calculi, such as HOπ [14, 15], have a well-studied behavioral theory. For HOπ, Sangiorgi has defined *context* bisimilarity relations, which are *sound* with respect to barbed congruence (i.e. are included in barbed congruence) and sometimes *complete* (i.e. they contain barbed congruence), leading to a full characterization. To establish equivalence between processes, context bisimilarity tests all environments which may interact with these processes. For instance, when assessing the equivalence of two processes which consist only of the output of a message on a communication channel a, context bisimilarity needs to consider every interacting system that is capable of doing an input on channel a. Context bisimilarities characterize barbed congruence both in the strong case (where internal steps are observable), and in the weak case (where internal steps are not observable).

Context bisimilarities have also been defined for more expressive calculi such as ones with localities. However the results are generally less satisfactory than in HOπ, especially in the weak case. We have characterization of weak barbed congruence only in a few cases, such as in Mobile Ambients [4, 12] and its variant NBA [3]. In Seal [19, 6] and Homer [9, 7], sound weak bisimilarities have been defined in a *delay* style: silent actions are not allowed after an observable one. Because of this limitation, the relations are likely not complete. In the Kell calculus [17], Schmitt and Stefani propose sound and complete context bisimilarities in the strong case only.

The main difficulty with the above calculi is to prove the soundness (or congruence) of a suitable weak non delay bisimilarity, which can characterize weak barbed congruence. An effective technique for proving soundness of bisimilarity relations in higher-order calculi is Howe's method [10, 1, 8]. Howe's method is a proof scheme to show that a candidate bisimilarity $\mathcal{R}$ based on a labeled transition semantics $\xrightarrow{\lambda}$ is a congruence. The method consists in defining the *Howe's closure* of $\mathcal{R}$, written $\mathcal{R}^\bullet$, which is a congruence and very close to a bisimulation by construction. One then proves a simulation-like result for $\mathcal{R}^\bullet$. Additional properties of $\mathcal{R}^\bullet$ allows to conclude that $\mathcal{R}^\bullet$ and $\mathcal{R}$ coincide, and therefore that $\mathcal{R}$ is a congruence. Until now, Howe's method has been used in process calculi to prove soundness of strong or weak higher-order bisimilarities [2, 11] or weak delay context bisimilarities [9, 7] only.

Contributions In this paper, we show how to apply Howe's method to prove the soundness of a weak (standard, i.e. non-delay) bisimilarity equivalent to context bisimilarity. Using HOπ as the main vehicle, we first explain why Howe's method fails with early bisimilarities for higher-order calculi defined with contextual semantics (relying on classical transition systems using *abstractions* and *concretions*, and on (early) context bisimilarities). We then introduce a new kind of transition system and associated bisimilarities for HOπ, which we call *complementary* semantics, which we prove equivalent to the contextual one, but which allows us to use Howe's method as a congruence proof technique in the weak case.

To show the benefits of our method, we define a complementary semantics for a calculus called HOπP [11], which extends HOπ with a special operator called *passivation*. Process passivation allows a named process to be stopped and its state captured at any time during its execution. It has been introduced in higher-order calculus, such as the Kell calculus [17] and Homer [9] to model process failures, online process replacement, and strong process mobility. In [11] we extensively studied contextual semantics and behavioral equivalences of HOπP and showed that we faced the same difficulties in HOπP as in the Kell calculus and Homer: we were able to define a sound and complete (early) context bisimilarity in the strong case, but only a sound (early) weak delay context one in the weak case.

In this paper, we define complementary semantics and bisimilarities for HOπP in the strong and weak cases, and prove that they coincide with their contextual counterpart. We then use Howe's method to prove the soundness of the bisimilarities, and we prove a completeness result in the weak case. To our knowledge, this is the first time one obtains a coinductive characterization of barbed congruence in a higher-order calculus featuring passivation and restriction. We also define a complementary semantics for Seal calculus and we prove its soundness.

Summary In Section 2, we explain why higher-order communication makes the Howe's method fail with early context bisimilarities in HOπ. We use HOπ since it is the most simple calculus where the problem arises. To deal with this issue, we propose in Section 3 a new semantics for HOπ, called complementary semantics, which relies on a new kind of labelled transition system and a new kind of bisimilarities. We prove that both semantics are equivalent, i.e. that complementary bisimilarity coincides with early context bisimilarity, and we prove the congruence of complementary bisimilarity with Howe's method.

The second main contribution is in Section 4. We first recall syntax, contextual semantics, and bisimilarity results for HOπP. We then define strong and weak complementary semantics for HOπP, and prove soundness of weak complementary bisimilarity. We also prove a completeness result, and correspondences with contextual semantics and bisimilarity. In Section 5, we define complementary semantics and bisimilarity for Seal calculus. We discuss related work in Section 6, and Section 7 concludes the paper. Appendix A details proofs for HOπ, Appendix B details the ones for HOπP, and Appendix C gives proof sketches in the Seal calculus case.

Notations:

- X, Y, Z: process variables
- $a, b, \overline{a}, \overline{b}$: names

Syntax:

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

Figure 1: Syntax of the Higher-Order π

2 Contextual Semantics and Howe's Method

We use the calculus HOπ defined in [15] as an example to show why contextual semantics is not well suited to apply Howe's method. We first recall HOπ syntax and contextual semantics. We then recall the Howe's method proof scheme, and explain why we cannot use it with early context bisimilarities, which are the usual candidate relations for characterizing barbed congruence in calculi inheriting from the π-calculus.

2.1 HOπ Syntax and Contextual LTS

Syntax The calculus HOπ [15] extends the π-calculus with higher-order communication, which allows process as messages. The syntax of the calculus and some notations can be found in Figure 1.

In a synchronous higher-order communication $a(X)P \mid \overline{a}\langle Q\rangle R$, the left process $a(X)P$ is waiting for a process (here Q) on name a, and then continues as $P\{Q/X\}$ ($P\{Q/X\}$ is the capture-free substitution of X by Q in P). The right process $\overline{a}\langle Q\rangle R$ sends the process Q on a and then continues as R. In process $a(X)P$, the variable X is bound. We write $\mathrm{fv}(P)$ the free variables of a process P. In name restriction $\nu a.P$, the name a is made local (i.e. bound) to the process P. We write $\mathrm{bn}(P)$ (resp $\mathrm{fn}(P)$) the bound names (resp free names) of a process P.

Convention on free names and variables We identify processes up to α-conversion of names and variables: process and agents are representative of their α-equivalence class, and are always chosen such that their bound names and variables are distinct from free names and variables. When considering a collection of processes, we assumes that the bound names and bound variables of the processes are chosen to be different from their free names and their free variables. In any discussion or proof, we assume that bound names and bound variables of any process or actions under consideration are chosen to be different from the names and variables occurring free in any other entities under consideration. Note that with this convention, we have $\nu a.(P \mid Q) \equiv P \mid \nu a.Q$ without qualification on the free variables of P.

Structural congruence Structural congruence $\equiv$ is the smallest congruence verifying the following laws.

$$a(X)P \xrightarrow{a} (X)P \ \textsc{Context-Abstr} \qquad \overline{a}\langle Q\rangle P \xrightarrow{\overline{a}} \langle Q\rangle P \ \textsc{Context-Concr}$$

$$\frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} \ \textsc{Context-Par} \qquad \frac{P \xrightarrow{\alpha} A \qquad \alpha \notin \{a, \overline{a}\}}{\nu a.P \xrightarrow{\alpha} \nu a.A} \ \textsc{Context-Restr}$$

$$\frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \ \textsc{Context-HO}$$

Figure 2: Contextual labeled transition system for HOπ

$$P \mid (Q \mid R) \equiv (P \mid Q) \mid R \qquad P \mid Q \equiv Q \mid P \qquad P \mid \mathbf{0} \equiv P$$

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

Remark 1. *We do not include replication since it may be encoded with the other constructs. See [11] for further details.*

Contextual LTS We now recall the labeled transition system proposed for HOπ by Sangiorgi in [15]. We call it *contextual* since it is used to define *context* bisimilarities. In this LTS, we have three kind of possible evolutions for processes:

- Internal actions labeled by τ, where a process evolves toward a process.
- Message input on a channel a, where a process evolves toward an *abstraction* $(X)Q$. The transition $P \xrightarrow{a} (X)Q$ means that the process P may receive a process R on the name a to continue as $Q\{R/X\}$.
- Message output on a channel a, where a process evolves toward a *concretion* $\nu\widetilde{b}.\langle R\rangle Q$. The transition $P \xrightarrow{\overline{a}} \nu\widetilde{b}.\langle R\rangle Q$ means that the process P may send the process R on the name a and continue as Q, and the scope of names $\widetilde{b}$ has to be expanded to encompass the recipient of R. We write $\text{bn}(C) = \widetilde{b}$ the bound names of a concretion, and $o(C)$ the emitted message (here R) of a concretion.

A higher-order communication takes place when a concretion interacts with an abstraction. We define a pseudo-application operator $\bullet$ between an abstraction $F = (X)P$ and a concretion $C = \nu\widetilde{b}.\langle R\rangle Q$ by:

$$(X)P \bullet \nu\widetilde{b}.\langle R\rangle Q \triangleq \nu\widetilde{b}.(P\{R/X\} \mid Q)$$

The rule for higher-order communication on name a is:

$$\frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \ \textsc{Context-HO}$$

We also sometimes use a process application between an abstraction $(X)P$ and a process Q, defined as $(X)P \circ Q \triangleq P\{Q/X\}$.

Let the set of *agents*, noted A, be the set of processes, abstractions and concretions. A process always evolves towards an agent. Rules CONTEXT-PAR and CONTEXT-RESTR require the extension of the parallel composition and restriction operators to all agents, which we define below:

- Let $F = (X)Q$
  - $F \mid P$ stands for $(X)(Q \mid P)$ and $P \mid F$ stands for $(X)(P \mid Q)$.
  - $\nu a.F = (X)\nu a.P$.
- Let $C = \nu\widetilde{b}.\langle Q\rangle R$
  - $C \mid P$ stands for $\nu\widetilde{b}.\langle Q\rangle(R \mid P)$, and $P \mid C$ stands for $\nu\widetilde{b}.\langle Q\rangle(P \mid R)$.
  - If $a \in \text{fn}(Q)$, then $\nu a.C = \nu\widetilde{b}, a.\langle Q\rangle R$. Otherwise, we have $\nu a.C = \nu\widetilde{b}.\langle Q\rangle\nu a.R$.

The LTS rules are given in Figure 2, with the exception of the symmetric rules for CONTEXT-PAR and CONTEXT-HO. All the transition rules are straightforward. The transitions are labeled with the names on which the communications may happen, or by τ for an internal evolution. The meta-variable α ranges over all the labels.

2.2 Context Bisimulation

Sangiorgi proposes *context* bisimulation as a LTS-based behavioral equivalence. The definition of (early strong) context bisimilarity is:

Definition 1 (**Early strong context bisimilarity**). *A binary relation $\mathcal{R}$ on closed processes is an* early strong context simulation *iff $P\ \mathcal{R}\ Q$ implies*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions 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 closed abstractions F, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $F \bullet C\ \mathcal{R}\ F \bullet C'$.*

A relation $\mathcal{R}$ is an early strong context bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early strong context simulations. Two closed processes P and Q are* strongly early context bisimilar*, noted $P \sim Q$, iff there exists an early strong context bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.*

In the message sending and input cases, the context bisimulation introduces the surrounding environment which interacts with the processes P and Q. When sending a message (resp inputting a message), it considers all the abstractions F (resp concretions C) which may input (resp send) a message on the same channel a.

In the following we also use the late strong context bisimilarity.

Definition 2 (**Late strong context bisimilarity**). *A binary relation $\mathcal{R}$ on closed processes is a* late strong context simulation *iff $P\ \mathcal{R}\ Q$ implies*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and for all closed concretions C, we have $F \bullet C\ \mathcal{R}\ F' \bullet C$.*
- *For all $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all closed abstractions F, we have $F \bullet C\ \mathcal{R}\ F \bullet C'$.*

A relation $\mathcal{R}$ is a late strong context bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are late strong context simulations. Two closed processes P and Q are* strongly late context bisimilar*, noted $P \sim_l Q$, iff there exists a late strong context bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.*

We now give definitions for the weak case, where internal steps $\xrightarrow{\tau}$ are not observable. We write $\stackrel{\tau}{\Rightarrow}$ the reflexive and transitive closure of $\xrightarrow{\tau}$. For all higher-order name or coname a, we write $\stackrel{a}{\Rightarrow}$ for $\Rightarrow\!\xrightarrow{a}$ (as higher order steps result in concretions and abstractions, they may not reduce further; silent steps after this reduction are taken into account in the definition of weak simulation below). We define weak early context bisimilarity as:

Definition 3 (**Weak early context bisimilarity**). *A binary relation $\mathcal{R}$ on closed processes is an* early weak context simulation *iff $P\ \mathcal{R}\ Q$ implies*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions C, there exists F', Q' such that $Q \stackrel{a}{\Rightarrow} F'$, $F' \bullet C \stackrel{\tau}{\Rightarrow} Q'$, and $F \bullet C\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{\overline{a}} C$, for all closed abstractions F, there exists C', Q' such that $Q \stackrel{\overline{a}}{\Rightarrow} C'$, $F \bullet C' \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet C\ \mathcal{R}\ Q'$.*

A relation $\mathcal{R}$ is an early weak context bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early weak context simulations. Two closed processes P and Q are* early weak context bisimilar*, noted $P \approx Q$, iff there exists an early weak context bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.*

In the strong and weak cases, late and early context bisimilarities are *congruences*, i.e. if P and Q are context bisimilar, then $op(P)$ and $op(Q)$ are context bisimilar for all the operators op of the language. To prove this congruence result on context bisimilarities, one relies on a *substitution lemma*:

Lemma 1. *Let A be an agent and P, Q be processes; if P and Q are strong (resp weak) context bisimilar, then $A\{P/X\}$ and $A\{Q/X\}$ are strong (resp weak) context bisimilar.*

The scheme of [15] to prove this lemma can be summed up by:

- The result is proved for evaluation contexts (parallel composition and restriction).

- The result is proved for all processes, using the first step.

The distinction is useful since if A is an evaluation context, the reductions of $A\{P/X\}$ may come from A or P, whereas if A is not an evaluation context, P cannot be reduced.

This proof scheme for Lemma 1 cannot be extended for more expressive process calculi; for instance, it does not work for HOπP, the calculus we use in Section 4. In the next subsection, we detail another congruence proof method called Howe's method.

2.3 Howe's Method

Howe's method [10, 1, 8] is a systematic proof technique to show that a candidate relation $\mathcal{R}$ is a congruence. The method can be divided in three steps:

- Definition of the *Howe's closure* $\mathcal{R}^\bullet$ and proofs of its basic properties. Howe's closure $\mathcal{R}^\bullet$ contains $\mathcal{R}$ and is a congruence by construction.
- Proof of a simulation-like property for $\mathcal{R}^\bullet$.
- Conclusive step: proof that $\mathcal{R}$ and $\mathcal{R}^\bullet$ coincide on closed processes. Since $\mathcal{R}^\bullet$ is a congruence, we conclude that $\mathcal{R}$ is a congruence.

The definition of the Howe's closure relies on the open extension of $\mathcal{R}$, noted $\mathcal{R}^\circ$: it extends the definition of the relation $\mathcal{R}$ to open processes, i.e. to processes with free process variables X.

Definition 4 (**Open extension**). *Let P and Q be two open processes. We have $P\ \mathcal{R}^\circ\ Q$ iff $P\sigma\ \mathcal{R}\ Q\sigma$ for all substitutions σ that close P and Q.*

The Howe's closure is inductively defined as the smallest congruence which contains $\mathcal{R}^\circ$ and is closed by right relation composition by $\mathcal{R}^\circ$.

Definition 5 (**Howe closure**). *The Howe's closure $\mathcal{R}^\bullet$ of a relation $\mathcal{R}$ is the smallest relation verifying:*

- $\mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$.
- $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$.
- *For all operators op of the language, if $\widetilde{P}\ \mathcal{R}^\bullet\ \widetilde{Q}$, then $op(\widetilde{P})\ \mathcal{R}^\bullet\ op(\widetilde{Q})$.*

By definition the Howe's closure is a congruence, and the composition with $\mathcal{R}^\circ$ allows some transitivity and gives some additional properties to the relation.

Remark 2. *In the literature (e.g. [10, 8, 9]) Howe's closure is usually inductively defined by the following rule for all operators op in the language:*

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

Both definitions are equivalent (see [8] for the proof). We believe that Definition 5 is easier to understand and easier to work with in proofs.

To prove that Howe's closure is a simulation (second step of the method), we need the following property:

Lemma 2. *Let $\mathcal{R}$ be an equivalence. If $P\ \mathcal{R}^\bullet\ Q$ and $R\ \mathcal{R}^\bullet\ S$, then we have $P\{R/X\}\ \mathcal{R}^\bullet\ Q\{S/X\}$.*

We sketch the proof in order to give an idea on why the transitive item $\mathcal{R}^\bullet\mathcal{R}^\circ\subseteq\mathcal{R}^\bullet$ is needed in Definition 5. The proof is by induction on the derivation of $P\ \mathcal{R}^\bullet\ Q$. Suppose we have $P\ \mathcal{R}^\circ\ Q$. Since $R\ \mathcal{R}^\bullet\ S$ and $\mathcal{R}^\bullet$ is a congruence, we have $P\{R/X\}\ \mathcal{R}^\bullet\ P\{S/X\}$. Let σ be a substitution that closes P and Q except for X; by open extension definition, we have $P\{S/X\}\sigma\ \mathcal{R}\ Q\{S/X\}\sigma$, i.e. we have $P\{S/X\}\ \mathcal{R}^\circ\ Q\{S/X\}$. Finally we have $P\{R/X\}\ \mathcal{R}^\bullet\mathcal{R}^\circ\ Q\{S/X\}$, hence we have $P\{R/X\}\ \mathcal{R}^\bullet\ Q\{S/X\}$. The other cases are easy using induction hypothesis.

Remark 3. *One may define Howe's closure with $\mathcal{R}^\circ\mathcal{R}^\bullet\subseteq\mathcal{R}^\bullet$ as the transitive item instead of $\mathcal{R}^\bullet\mathcal{R}^\circ\subseteq\mathcal{R}^\bullet$. However left relation composition with $\mathcal{R}^\circ$ raises issues when proving weak simulation properties, while right relation composition works in the strong and weak cases.*

In our case, we want to prove that a bisimilarity $\mathcal{B}$ is a congruence. By definition, we have $\mathcal{B}^\circ\subseteq\mathcal{B}^\bullet$. To have the reverse inclusion, we prove that $\mathcal{B}^\bullet$ is a bisimulation. However we cannot prove directly that $\mathcal{B}^\bullet$ is symmetric; instead, we prove a simulation property (second step of the method), and we use the following property.

Lemma 3. *Let $\mathcal{R}$ be an equivalence. Then the reflexive and transitive closure $(\mathcal{R}^\bullet)^*$ of $\mathcal{R}^\bullet$ is symmetric.*

Proof. By proving that $P(\mathcal{R}^\bullet)^{-1}Q$ implies $P(\mathcal{R}^\bullet)^*Q$ for all P, Q. It is done by induction on $P(\mathcal{R}^\bullet)^{-1}Q$. □

Using the simulation result, we can prove that the restriction of $(\mathcal{B}^\bullet)^*$ to closed terms is 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 difficulty is to prove the simulation-like property for Howe's closure. In the following subsection, we explain why we cannot use directly Howe's method with early context bisimilarities (Definitions 9 and 10).

2.4 Communication Problem with Contextual Semantics

We want to prove that $\mathcal{B}^\bullet$ is a simulation. Proving that a congruence is a simulation may raise transitivity issues; see the Kell-calculus congruence proof [17, 11] for instance. The Howe's method deals with this issue by establishing a stronger simulation result which features some transitivity in its clauses. Given a bisimilarity $\mathcal{B}$ based on a LTS $P \xrightarrow{\lambda} A$, the simulation result follows the pattern below:

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

This is quite close to a higher-order bisimilarity clause, similar to the one for Plain CHOCS [18], for instance. It supposes that the Howe's closure can be extended to labels λ. For instance, suppose we want to apply Howe's method to strong late context bisimilarity $\sim_l$, which has first been done for Homer in [9]. We extend Howe's closure to abstractions: we have $F \sim_l^\bullet F'$ iff for all C, we have $F \bullet C \sim_l^\bullet F' \bullet C$. We have then:

Lemma 4. *If $P \sim_l^\bullet Q$, then:*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \sim_l^\bullet Q'$.*
- *For all $P \xrightarrow{a} F$, there exists F' such that $Q \xrightarrow{a} F'$ and $F \sim_l^\bullet F'$.*
- *For all $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all closed F, F' such that $F \sim_l^\bullet F'$ and $F \bullet C \sim_l^\bullet F' \bullet C'$.*

Notice that some transitivity is built in the output clause of this simulation-like property: F and C are directly related to F' and C'. Finding a suitable simulation-like property featuring transitivity is more difficult for early context bisimilarity. Sticking to the pattern given earlier, one may think of the following property:

Conjecture 1. *If $P \sim^\bullet Q$, then:*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \sim^\bullet Q'$.*
- *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 if we have found such extensions, we have problems to conduct an inductive proof of conjecture 1 with higher-order communication. Suppose we conduct a proof by induction on the derivation of $P \sim^\bullet Q$. Suppose we are in the parallel case, i.e. we have $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$, with $P_1 \sim^\bullet Q_1$ and $P_2 \sim^\bullet Q_2$. Suppose that we have $P \xrightarrow{\tau} P'$, and the transition comes from rule CONTEXT-HO: we have $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\overline{a}} C$ and $P' = F \bullet C$. We want to find Q' such that $Q \xrightarrow{\tau} Q'$ and $P' \sim^\bullet Q'$. We want to use the same rule CONTEXT-HO, hence we have to find F', C' such that $Q \xrightarrow{\tau} F' \bullet C'$. However we cannot use the input clause of the induction hypothesis with P_1, 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, 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 $F \sim^\bullet F'$. We cannot bypass this mutual dependency, therefore the inductive proof of conjecture 1 fails in the higher-order communication case.

Godskesen and Hildebrandt [7] deal with this issue in Homer by making the concretion clause independent from abstractions. The considered bisimilarity is therefore

no longer early, but *input-early*: the input clause is in an early style and the output clause is in a late one. Adapted to HOπ, the definition is:

Definition 6 (**Input-early strong context bisimilarity**). *A binary relation $\mathcal{R}$ on closed processes is an* input-early strong context simulation *iff $P\ \mathcal{R}\ Q$ implies:*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions C, there exists G such that $Q \xrightarrow{a} G$ and $F \bullet C\ \mathcal{R}\ G \bullet C$.*
- *For all $P \xrightarrow{\overline{a}} C$, there exists D such that $Q \xrightarrow{\overline{a}} D$ and for all closed abstractions F, we have $F \bullet C\ \mathcal{R}\ F \bullet D$.*

A relation $\mathcal{R}$ is an input-early strong context bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are input-early strong context simulations. Two closed processes P and Q, noted $P \sim_{ie} Q$, are* input-early strongly context bisimilar *iff there exists an input-early strong context bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.*

Open extension and Howe's closure of input-early bisimilarity are extended to concretions in the following way:

- We have $C \sim^{\circ}_{ie} C'$ iff for all F, $F \bullet C \sim^{\circ}_{ie} F \bullet C'$
- If $C \sim^{\circ}_{ie} C'$ then $C \sim^{\bullet}_{ie} C'$. If $C \sim^{\bullet}_{ie} \sim^{\circ}_{ie} C'$ then $C \sim^{\bullet}_{ie} C'$.
- If $R \sim^{\bullet}_{ie} R'$ and $S \sim^{\bullet}_{ie} S'$, then we have $\langle R \rangle S \sim^{\bullet}_{ie} \langle R' \rangle S'$.
- If $C \sim^{\bullet}_{ie} C'$, then we have $\nu a.C \sim^{\bullet}_{ie} \nu a.C'$.

The extension does not rely on abstractions, however it respects the output late clause of the bisimilarity:

Lemma 5. *If $C \sim^{\bullet}_{ie} C'$, then for all P, P' such that $fv(P) = fv(P') \subseteq \{X\}$ and $P \sim^{\bullet}_{ie} P'$, we have $(X)P \bullet C \sim^{\bullet}_{ie} (X)P' \bullet C'$.*

We give the simulation-like property for input-early Howe's closure:

Lemma 6. *Let $(\sim_{ie})^{\bullet}_{c}$ be the restriction of $\sim^{\bullet}_{ie}$ to closed terms. If $P\ (\sim_{ie})^{\bullet}_{c}\ Q$ then:*

- *If $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ (\sim_{ie})^{\bullet}_{c}\ Q'$.*
- *If $P \xrightarrow{a} F$, for all closed concretion $C\ (\sim_{ie})^{\bullet}_{c}\ C'$, there exists F' such that $Q \xrightarrow{a} F'$ and $F \bullet C\ (\sim_{ie})^{\bullet}_{c}\ F' \bullet C'$*
- *If $P \xrightarrow{\overline{a}} C$, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and $C\ (\sim_{ie})^{\bullet}_{c}\ C'$.*

The property features transitivity in the input clause, and Lemma 5 deals with the communication problem. A similar simulation-like lemma can be defined in the weak case.

Lemma 7. *Let $(\approx)^{\bullet}_{c}$ be the restriction of $\approx^{\bullet}$ to closed terms. If $P\ (\approx)^{\bullet}_{c}\ Q$ then:*

- *If* $P \xrightarrow{\tau} P'$*, there exists* Q' *such that* $Q \stackrel{\tau}{\Rightarrow} Q'$ *and* $P' \ (\approx)_c^\bullet \ Q'$.
- *If* $P \xrightarrow{a} F$*, for all closed concretion* $C \ (\sim_{ie})_c^\bullet \ C'$*, there exists* F' *such that* $Q \stackrel{a}{\Rightarrow} F'$ *and* $F \bullet C \ (\approx)_c^\bullet \ F' \bullet C'$
- *If* $P \xrightarrow{\overline{a}} C$*, there exists* C' *such that* $Q \stackrel{\overline{a}}{\Rightarrow} C'$ *and* $C \ (\approx)_c^\bullet \ C'$.

Notice that the clauses are written in the *delay* style; internal actions are not allowed after a visible action. This is necessary to keep the concretion clause independent from abstractions. The delay style is not satisfactory in the weak case since delay bisimilarities are generally not complete with respect to weak barbed congruence. Congruence proof for delay input-early bisimilarity can be found for Homer in [7].

In the following section, we propose a new LTS semantics and bisimilarities for HOπ which coincide with the contextual ones and which allow the use of Howe's method to prove congruence results with early strong and weak (standard, i.e. non-delay) bisimilarities.

3 Complementary Semantics for HOπ

Until now Howe's method has been successfully used only with late [9] or delay input-early bisimilarities [7]. The input-early delay style is a drawback of making the output clause of the simulation-like property completely independent from abstractions. In this section, we propose a new LTS and bisimilarity which make the message output clause "independent enough" (but not completely independent) from abstractions to avoid the communication problem and to make Howe's method work with early bisimulations.

3.1 Complementary LTS

We define a LTS $P \stackrel{\lambda}{\mapsto} P'$ where processes always evolve towards other processes. We have three kinds of transitions: internal actions $P \stackrel{\tau}{\mapsto} P'$, message input $P \stackrel{a,R}{\longmapsto} P'$, and message output $P \stackrel{\overline{a},Q}{\longmapsto} P'$. We call this new LTS *complementary* since in the output action, we put the context which complements P in the label λ of the transition (more details below). For higher-order labels $\lambda = a, R$ or $\lambda = \overline{a}, R$ we define $n(\lambda)$ as the name a on which the communication may happen. Rules of the LTS can be found in Figure 3, except the symmetric of rules HOπ-PAR and HOπ-HO. We first detail the form of transitions in the complementary LTS.

Internal action transitions $P \stackrel{\tau}{\mapsto} P'$ are the same as in the contextual LTS $P \xrightarrow{\tau} P'$. A message input transition $P \stackrel{a,R}{\longmapsto} P'$ means that process P may receive the process R as a message on channel a and become P'. In the contextual style, it means that there exists an abstraction $F = (X)P''$ such that $P \xrightarrow{a} (X)P''$ and $P' = P''\{R/X\}$. Complementary and contextual message input transitions are fundamentally the same, except that the complementary action is written in the early style.

$$a(X)P \overset{a,R}{\longmapsto} P\{R/X\} \quad \text{HO}\pi\text{-In} \qquad \frac{Q \overset{a,R}{\longmapsto} Q'}{\overline{a}\langle R\rangle S \overset{\overline{a},Q}{\longmapsto} Q' \mid S} \quad \text{HO}\pi\text{-Out}$$

$$\frac{P_1 \overset{\lambda}{\longmapsto} P_1'}{P_1 \mid P_2 \overset{\lambda}{\longmapsto} P_1' \mid P_2} \quad \text{HO}\pi\text{-Par} \qquad \frac{P \overset{\lambda}{\longmapsto} P' \qquad a \notin n(\lambda)}{\nu a.P \overset{\lambda}{\longmapsto} \nu a.P'} \quad \text{HO}\pi\text{-Restr}$$

$$\frac{P \overset{\overline{a},Q}{\longmapsto} P'}{P \mid Q \overset{\tau}{\longmapsto} P'} \quad \text{HO}\pi\text{-HO}$$

Figure 3: Complementary LTS for HOπ

The main difference lies with output action transitions. The transition $P \overset{\overline{a},Q}{\longmapsto} P'$ means that P may send a message on channel a, Q may receive on a, and the communication on a between P and Q results in P'. Note that it is not the same as writing a contextual transition in an early style $P \xrightarrow{\overline{a},F} F \bullet C$: instead of putting an abstraction F in the label, we put a process Q (without any free process variable). There is a tight correspondence with an output action contextual transition, though: the transition $P \overset{\overline{a},Q}{\longmapsto} P'$ means that there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, and $P' = F \bullet C$.

Rules of the LTS in Figure 3 are standard, except rules HOπ-HO and HOπ-Out. In rule HOπ-HO, the premise $P \overset{\overline{a},Q}{\longmapsto} P'$ means that P and Q can communicate on a name a and the result is P', i.e. $P \mid Q \xrightarrow{\tau} P'$ (by communication on a), which is exactly what we want in the conclusion of the rule. Rule HOπ-Out has a premise (unlike its equivalent rule Context-Concr) since in the conclusion we need the result Q' of the input of process R on channel a by Q.

Remark 4. *Notice that in a message output $P \overset{\overline{a},Q}{\longmapsto} P'$, the message itself does not appear in the label or cannot be directly deduced from the transition. It is unusual in higher-order LTS: for instance in the contextual semantics of HOπ [15], in the Kell [17] or Homer [9], emitted processes appear in concretions. In the Mobile Ambients [12], moving ambients also appear in concretions; in the Seal-calculus [5], moved seals appear in labels (seal freeze P_z or seal chained P^z). Hiding the message in the LTS makes the Howe's method easier to apply.*

The correspondence between the complementary LTS and the contextual LTS is exact, and it is established by the following lemma:

Lemma 8. *Let P be an HOπ process. We have:*

- $P \xrightarrow{\tau} P'$ *iff* $P \overset{\tau}{\longmapsto} \equiv P'$.

- *If $P \xrightarrow{a} F$, then for all R we have $P \overset{a,R}{\longmapsto} F \circ R$. Conversely, if $P \overset{a,R}{\longmapsto} P'$, then there exists F such that $P \xrightarrow{a} F$ and $P' = F \circ R$.*
- *If $P \xrightarrow{\overline{a}} C$, then for all Q such that $Q \xrightarrow{a} F$, we have $P \overset{\overline{a},Q}{\longmapsto} F \bullet C$. Conversely, if $P \overset{\overline{a},Q}{\longmapsto} P'$, then there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $P' \equiv F \bullet C$.*

The proof is done by induction on P and can be found in Appendix A. The correspondence between the two LTS is up to structural congruence because of scope extrusion: in Sangiorgi's contextual LTS, scope extrusion is performed iff the name belongs to the free names of the message, while in the complementary LTS, we do not have such a condition. For instance, if we consider $P = \nu b.\overline{a}\langle\mathbf{0}\rangle\overline{b}\langle\mathbf{0}\rangle\mathbf{0}$, then we have $P \xrightarrow{\overline{a}} C = \langle\mathbf{0}\rangle\nu b.\overline{b}\langle\mathbf{0}\rangle\mathbf{0}$ and for all $F = (X)Q'$, we have $F \bullet C = Q'\{\mathbf{0}/X\} \mid \nu b.\overline{b}\langle\mathbf{0}\rangle\mathbf{0} \triangleq P_1$. With the complementary LTS, for all Q such that $Q \xrightarrow{a} F$ we have $P \overset{\overline{a},Q}{\longmapsto} \nu b.(Q'\{\mathbf{0}/X\} \mid \overline{b}\langle\mathbf{0}\rangle\mathbf{0}) \triangleq P_2$. We have $P_1 \neq P_2$ but we have $P_1 \equiv P_2$.

3.2 Complementary Bisimilarities

We now define strong complementary bisimilarity and prove its soundness by proving it is a congruence using Howe's method. The result in itself, i.e. the definition of a sound bisimilarity in HOπ, is not new [14, 15]. However it allows us to explain why complementary semantics is well suited to apply Howe's method. In the HOπ case, strong complementary bisimilarity is simply the bisimilarity associated to the complementary LTS. Let λ range over complementary LTS labels, i.e. $\lambda = \tau$, $\lambda = a, R$ or $\lambda = \overline{a}, R$, where R is a process.

Definition 7 (**Strong complementary bisimilarity**). *A binary relation $\mathcal{R}$ on closed processes is a* strong complementary simulation *iff $P \mathcal{R} Q$ implies for all $P \overset{\lambda}{\longmapsto} P'$, there exists Q' such that $Q \overset{\lambda}{\longmapsto} Q'$ and $P' \mathcal{R} Q'$.*

A relation $\mathcal{R}$ is a strong complementary bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are strong complementary simulations. Two closed processes P and Q are* strong complementary bisimilar*, noted $P \sim_m Q$, iff there exists a strong complementary bisimulation $\mathcal{R}$ such that $P \mathcal{R} Q$.*

As in context bisimilarity, in the message output case $P \overset{\overline{a},R}{\longmapsto} P'$, the matching transition $Q \overset{\overline{a},R}{\longmapsto} Q'$ still depends on a receiving entity (here R). However, instead of considering a context which directly receives the message (an abstraction F), we consider a process R which evolves toward an abstraction. This small nuance allows us to use Howe's method to prove soundness of $\sim_m$. To this end we prove the following simulation-like property for $\sim_m^\bullet$, the Howe closure of $\sim_m$:

Lemma 9. *Let P, Q be closed processes. If $P \sim_m^\bullet Q$ then:*

- *If $P \overset{\tau}{\longmapsto} P'$, then there exists Q' such that $Q \overset{\tau}{\longmapsto} Q'$ and $P' \sim_m^\bullet Q'$.*
- *If $P \overset{a,R}{\longmapsto} P'$, then for all $R \sim_m^\bullet R'$, there exists Q' such that $Q \overset{a,R'}{\longmapsto} Q'$ and $P' \sim_m^\bullet Q'$.*

- *If* $P \stackrel{\overline{a},T}{\longmapsto} P'$*, then for all* $T \sim_m^\bullet T'$*, there exists* Q' *such that* $Q \stackrel{\overline{a},T'}{\longmapsto} Q'$ *and* $P' \sim_m^\bullet Q'$.

We do not have the same problem as in Section 2.4 with higher-order communication case. We remind that in this case, we have $P_1 \mid P_2 \sim_m^\bullet Q_1 \mid Q_2$ with $P_1 \sim_m^\bullet Q_1$, $P_2 \sim_m^\bullet Q_2$ and $P_1 \stackrel{\overline{a},P_2}{\longmapsto} P'$. We can apply directly the message output clause of the induction hypothesis: there exists Q' such that $Q_1 \stackrel{\overline{a},Q_2}{\longmapsto} Q'$ and $P' \sim_m^\bullet Q'$. We conclude that $Q_1 \mid Q_2 \stackrel{\tau}{\mapsto} Q'$ (by rule HOπ-HO) with $P' \sim_m^\bullet Q'$ as wished.

Theorem 1. $\sim_m$ *is a congruence.*

Proving Lemma 9 is the only difficult part of the proof of Theorem 1. The complete proofs can be found in Appendix A.

Following the correspondence result between the two LTS (Lemma 8), we now prove that the bisimilarities have the same discriminating power. The differences in the message output clauses are covered mainly with Lemma 8. The bisimilarities differ also in how they deal with input actions: complementary bisimilarity tests with a process while context bisimilarity tests with a concretion. Testing with all concretions includes tests with $\langle P \rangle \mathbf{0}$, which are the same as tests with P (up to $\equiv$). Consequently one inclusion is easy to establish:

Lemma 10. *We have* $\sim \subseteq \sim_m$.

The proof is done by showing that $\sim$ is a strong complementary bisimilarity (up to $\equiv$). The reverse inclusion requires the congruence result on $\sim_m$ (Theorem 1).

Lemma 11. *We have* $\sim_m \subseteq \sim$.

We prove the inclusion by showing that $\sim_m$ is an early strong context bisimulation (up to $\equiv$). In the message input case, we have roughly $P'\{R/X\} \sim_m Q'\{R/X\}$; by congruence it implies that $\nu\widetilde{b}.(P'\{R/X\} \mid S) \sim_m \nu\widetilde{b}.(Q'\{R/X\} \mid S)$, i.e. $(X)P' \bullet \nu\widetilde{b}.\langle R \rangle S \sim_m (X)Q' \bullet \nu\widetilde{b}.\langle R \rangle S$. With Theorem 1, tests with processes are as discriminatory as tests with concretions.

Correspondence also holds in the weak case. We write $\stackrel{\tau}{\Mapsto}$ the reflexive and transitive closure of $\stackrel{\tau}{\mapsto}$, and we define $\stackrel{a,R}{\Longmapsto} \stackrel{\Delta}{=} \stackrel{\tau}{\Mapsto} \stackrel{a,R}{\longmapsto} \stackrel{\tau}{\Mapsto}$. In the weak case, two processes P and Q may evolve independently before interacting with each other. Since a transition $P \stackrel{\overline{a},Q}{\longmapsto} P'$ includes a communication between P and Q, we have to authorize Q to perform τ-actions before interacting with P in the weak output transition. We define $P \stackrel{\overline{a},Q}{\Longmapsto} P'$ as $P \stackrel{\tau}{\Mapsto} \stackrel{\overline{a},Q'}{\longmapsto} \stackrel{\tau}{\Mapsto} P'$ with $Q \stackrel{\tau}{\Mapsto} Q'$. Weak complementary semantics mimics weak context semantics in the following way.

Lemma 12. *Let* P *be an HO*π *process.*

- *We have* $P \stackrel{\tau}{\Rightarrow} P'$ *iff* $P \stackrel{\tau}{\Mapsto} P'$.

- *Let R be a closed process. If $P \stackrel{a}{\Rightarrow} F$ and $F \circ R \stackrel{\tau}{\Rightarrow} P'$ then we have $P \stackrel{a,R}{\Longmapsto} F \circ R$. If $P \stackrel{a,R}{\Longmapsto} P'$, then there exists F such that $P \stackrel{a}{\Rightarrow} F$ and $F \circ R \stackrel{\tau}{\Rightarrow} P'$.*
- *If $P \stackrel{\overline{a}}{\Rightarrow} C$, then for all Q such that $Q \stackrel{a}{\Rightarrow} F$ and $F \bullet C \stackrel{\tau}{\Rightarrow} P'$, we have $P \stackrel{\overline{a},Q}{\Longmapsto} P'$. If $P \stackrel{\overline{a},Q}{\Longmapsto} P'$, then there exists F, C such that $P \stackrel{\overline{a}}{\Rightarrow} C$, $Q \stackrel{a}{\Rightarrow} F$, and $F \bullet C \stackrel{\tau}{\Rightarrow} P'$.*

We now give the definition of the weak bisimilarity associated to the complementary LTS.

Definition 8. *A relation $\mathcal{R}$ on closed processes is a weak (non delay) complementary simulation iff $P \mathcal{R} Q$ implies for all $P \stackrel{\lambda}{\longmapsto} P'$, there exists Q' such that $Q \stackrel{\lambda}{\Rightarrow} Q'$ and $P' \mathcal{R} Q'$.*

A relation $\mathcal{R}$ is a weak complementary bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are weak complementary simulations. Two closed processes P and Q are weak complementary bisimilar, noted $P \approx_m Q$, iff there exists an weak complementary bisimulation $\mathcal{R}$ such that $P \mathcal{R} Q$.

Using the same proof schemes as in the strong case, we have the following results.

Theorem 2. *The relation $\approx_m$ is a congruence.*

Lemma 13. *We have $\approx_m = \approx$.*

We do not detail proofs for weak relations since they are similar to the strong ones. However we give the complete proofs in HOπP, where, unlike HOπ, the congruence result for a weak (non delay) relation is new.

4 Application to HOπP

In this section, we define a complementary semantics for a more involved calculus called HOπP (HOπ with Passivation) [11]. HOπP extends HOπ with a passivation operator inspired from Homer [9] and the Kell calculus [17]. HOπP is simpler than its parent calculi, mainly because it does not feature any control on communication. However its behavioral theory presents similar difficulties as that of Homer and of the Kell calculus. In particular, up to now no characterization of weak barbed congruence had yet been found. Using complementary semantics and Howe's method, we are able to define a sound weak (non delay) bisimilarity for HOπP. We also prove its completeness with respect to weak barbed congruence on image-finite processes. To the best of our knowledge, this is the first time that weak barbed congruence in a process calculus featuring restriction and passivation is given a co-inductive characterization.

4.1 Syntax and Contextual Semantics of HOπP

HOπP extends HOπ constructs with localities $a[P]$, that are passivation units. We extensively studied HOπP syntax, contextual semantics, and behavioral equivalence in

[11]. We give here the definitions and results we need without many details; see [11] for additional explanations and proofs.

With the same notations as for HOπ, the HOπP syntax is:

$$P ::= \mathbf{0} \mid X \mid P \mid P \mid a(X)P \mid \overline{a}\langle P\rangle P \mid \nu a.P \mid a[P]$$

When passivation is not triggered, a locality $a[P]$ is a transparent evaluation context: process P may evolve by itself and communicate freely with processes outside of locality a. At any time, passivation may be triggered and the process $a[P]$ becomes a concretion on a $\langle P\rangle\mathbf{0}$. Since the execution of a process is impossible in a message, P is frozen, but it can be activated again by a process receiving it on channel a.

We extend localities to all agents: if $F = (X)P$, then $a[F] \triangleq (X)a[P]$; if $C = \nu\widetilde{b}.\langle Q\rangle R$, then $a[C] \triangleq \nu\widetilde{b}.\langle Q\rangle a[R]$. We also add the following rules to the LTS:

$$\frac{P \xrightarrow{\alpha} A}{a[P] \xrightarrow{\alpha} a[A]}\ \textsc{Context-Loc} \qquad a[P] \xrightarrow{\overline{a}} \langle P\rangle\mathbf{0}\ \textsc{Context-Passiv}$$

Remark 5. *Note that rule* CONTEXT-LOC *implies that the scope of restricted names may cross locality boundaries. Scope extrusion outside localities is performed "by need" when a communication takes place. However, structural congruence follows the same rules as in Section 2.1, and, as in all calculi with non linear mobility (such as Seal [19], Homer [9] and Kell [17]), does not allow the restriction and locality operators to commute freely.*

Because of passivation, bisimilarities in HOπP require more discriminating power than in HOπ. The definition of context bisimilarities requires additional contexts $\mathbb{E}$ called *evaluation contexts*

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

We write $\mathbb{E}\{P\}$ the result of replacing (possibly with name capture) the hole $\Box$ in a context $\mathbb{E}$ by a process P. An evaluation context allows transition at the hole position: if $P \xrightarrow{\alpha} A$ then $\mathbb{E}\{P\} \xrightarrow{\alpha} \mathbb{E}\{A\}$. We write $\mathrm{bn}(\mathbb{E})$ the names bound at the hole position by the context $\mathbb{E}$: a name $x \in \mathrm{bn}(\mathbb{E}) \cap \mathrm{fn}(P)$ is free in P and becomes bound in $\mathbb{E}\{P\}$.

Definition 9 (Early strong context bisimilarity). *A binary relation $\mathcal{R}$ on closed processes is an* early strong context simulation *iff $P\ \mathcal{R}\ Q$ implies $fn(P) = fn(Q)$ and:*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions C, there exists G such that $Q \xrightarrow{a} G$ and $F \bullet C\ \mathcal{R}\ G \bullet C$.*
- *For all $P \xrightarrow{\overline{a}} C$, for all closed abstractions F, there exists D such that $Q \xrightarrow{\overline{a}} D$ and for all closed evaluation contexts $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\}\ \mathcal{R}\ F \bullet \mathbb{E}\{D\}$.*

A relation $\mathcal{R}$ is an early strong context bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early strong context simulations. Two closed processes P and Q are* early strong context bisimilar*, noted $P \sim Q$, iff there exists an early strong context bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.*

Note the condition $\text{fn}(P) = \text{fn}(Q)$ in the definition of early strong context simulation. It has been added because of the lazy scope extrusion: two bisimilar processes with different free names may be distinguished because of this mechanism (see [11] for details). Notice also that contexts $\mathbb{E}$ in the message output clause may bind free names of the concretions, and scope extrusion may happen if a free name of the emitted process is bound by $\mathbb{E}$.

Using the same proof technique as in the Kell calculus [17], we have the following result.

Theorem 3. *$\sim$ is a congruence.*

Note that Sangiorgi's congruence proof scheme (given in Section 2.2) does not work with HOπP because of passivation. Proof of Theorem 3 consists in showing that the congruence closure of $\sim$ is an early strong context bisimulation (see [11] for details). Unfortunately this technique fails with weak relations.

Definition 10 (Early weak context bisimilarity). *A relation $\mathcal{R}$ on closed processes is an* early weak context simulation *iff $P\ \mathcal{R}\ Q$ implies $fn(P) = fn(Q)$ and:*

- *For all $P \xrightarrow{\tau} P'$, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{a} F$, for all closed concretions C, there exists G, Q' such that $Q \stackrel{a}{\Rightarrow} G$, $G \bullet C \stackrel{\tau}{\Rightarrow} Q'$, and $F \bullet C\ \mathcal{R}\ Q'$.*
- *For all $P \xrightarrow{\overline{a}} C$, for all closed abstractions F, there exists D such that $Q \stackrel{\overline{a}}{\Rightarrow} D$ and for all closed evaluation contexts $\mathbb{E}$, there exists Q' such that $F \bullet \mathbb{E}\{D\} \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet \mathbb{E}\{C\}\ \mathcal{R}\ Q'$.*

A relation $\mathcal{R}$ is an early weak context bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are early weak context simulations. Two closed processes P and Q are* early weak context bisimilar*, noted $P \approx Q$, iff there exists an early weak context bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.*

Early weak context bisimilarities have been defined similarly for Homer and the Kell calculus. The weak hoe bisimilarity defined for the Seal calculus can also be seen as a form of weeak context bisimilarity. Until now we know of no congruence proof for these kinds of weak early context bisimilarities. Following Godskesen et al. [7], we can prove congruence for a weak delay input-early bisimilarity with Howe's method. However delay bisimilarities are not satisfactory since they are likely not complete with respect to barbed congruence. In the following, we define a weak (non delay) complementary bisimilarity $\approx_m$ which coincides with early weak context bisimilarity $\approx$, and we prove that $\approx_m$ is a congruence (and hence sound with respect to weak barbed congruence) using Howe's method. We also prove that $\approx_m$ is complete on image-finite processes, yielding the first co-inductive characterization of weak-barbed congruence in a calculus featuring passivation and restriction.

4.2 Complementary LTS

As in Section 3 we define a complementary LTS which considers processes instead of abstractions in the message output case. However we have two additional issues with

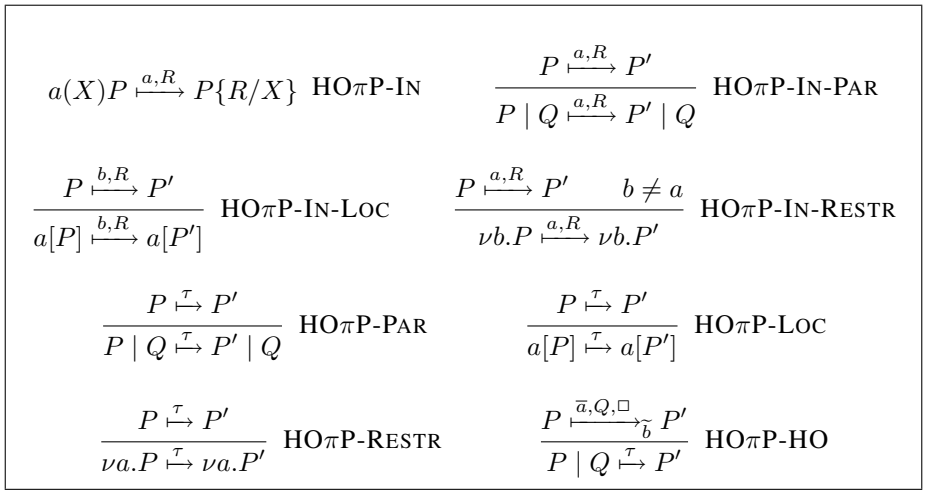

Figure 4: Complementary LTS for HOπP: internal and message input actions

HOπP. First, we have to include evaluation contexts $\mathbb{E}$ since they appear in bisimilarity definitions (Definitions 9 and 10). Second, handling scope extrusion is more involved than in HOπ, since the scope of restricted names may extend beyond locality boundaries by communication but not by structural congruence. We cannot always extrude names and still have an equivalent semantics (up to $\equiv$) as in HOπ.

Internal action transitions $P \overset{\tau}{\longmapsto} P'$ and input action transitions $P \overset{a,R}{\longmapsto} P'$ are similar to the corresponding HOπ complementary transitions. LTS rules dealing with these transitions can be found in Figure 4 except the symmetric counterpart of rules HOπP-PAR, HOπP-IN-PAR, and HOπP-HO. The rules are similar to those in HOπ, except that we have to add rules for localities. The rule HOπP-HO relies on message output transitions and is explained later.

In HOπP, context bisimilarities test a message output with an abstraction F and a bisimulation context $\mathbb{E}$. As in HOπ, complementary output actions $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ consider a receiving process Q instead of F. We have to add contexts $\mathbb{E}$ in our labels to keep the same discriminating power, and we also use a set of names $\widetilde{b}$ to deal with scope extrusion. Transition $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ means that P is put under context $\mathbb{E}$ and emits a message on a, which is received by Q, i.e. we have $\mathbb{E}\{P\} \mid Q \overset{\tau}{\longmapsto} P'$ by communication on a. In the contextual style, it means that there exists F, C such that $P \overset{\overline{a}}{\rightarrow} C$, $Q \overset{a}{\rightarrow} F$, and $P' = F \bullet \mathbb{E}\{C\}$. Output rules can be found in Figure 5, except for the symmetric of rule HOπP-OUT-PAR.

Scope extrusion may happen in the process under consideration (e.g. $P = \nu c.\overline{a}\langle R\rangle S$ with $c \in \text{fn}(R)$) or because of the bisimulation context $\mathbb{E}$ (e.g. $P = \overline{a}\langle R\rangle S$ and $\mathbb{E} = d[\nu c.(\Box \mid \overline{c}\langle \mathbf{0}\rangle \mathbf{0})]$ with $c \in \text{fn}(R)$). We first define auxiliary transitions $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto\!\!\!\!\!\!\cdot}_{\widetilde{b}} P'$, where we do not allow the latter kind of capture, and we then give rules for general output transitions.

Rule HOπP-OUT deals with message output $\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} \mathbb{E}\{S\} \mid Q'$. Premise $Q \xmapsto{a,R} Q'$ checks that Q may receive R on a, and the resulting process Q' is run in parallel with the continuation S under context $\mathbb{E}$. We check that that $\mathbb{E}$ does not capture free names of R with the side-condition $\text{bn}(\mathbb{E}) \cap \widetilde{b} = \emptyset$. We keep the free names $\widetilde{b}$ of R in the label for scope extrusion.

For instance, let $P = \overline{a}\langle R\rangle S$ and $c \in \text{fn}(R)$. Process $\nu c.P$ may emit R on a, but the scope of c has to be expanded to encompass the recipient of R. First premise of rule HOπP-OUT-EXTR checks that P may output a message; here we have $\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} \mathbb{E}\{S\} \mid Q'$ with $\widetilde{b} = \text{fn}(R)$. In conclusion, we have $\nu c.\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}\setminus c} \nu c.(\mathbb{E}\{S\} \mid Q')$. Scope of c includes the Q' as wished. We remove c from set $\widetilde{b}$ in the label for observational purposes. The set $\widetilde{b}$ consists of the names which may be extruded. For a concretion $C = \nu\widetilde{a}.\langle P_1\rangle P_2$, these names $\widetilde{b_C}$ are the free names of P_1 which are not already bound in $\widetilde{a}$, i.e. $\widetilde{b_C} = \text{fn}(P_1) \setminus \widetilde{a}$.

Suppose now that $P = \overline{a}\langle R\rangle S$ with $c \notin \text{fn}(R)$. Process $\nu c.P$ may emit a message, but the scope of c has to encompass the continuation S only: we want to obtain $\nu c.P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} \mathbb{E}\{\nu c.S\} \mid Q'$. To this end, we consider $P \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}_{\widetilde{b}} P'$ as a premise of rule HOπP-OUT-RESTR. In process P', the continuation is put under $\mathbb{E}\{\nu c.\Box\}$, hence we obtain $\overline{a}\langle R\rangle S \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}_{\widetilde{b}} \mathbb{E}\{\nu c.S\} \mid Q' = P'$. Process P' is exactly the resulting process we want for $\nu c.P$, hence the conclusion of the rule is simply $\nu c.P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$.

Rule for passivation HOπP-OUT-PASSIV is similar to rule HOπP-OUT, while rules HOπP-OUT-LOC, HOπP-OUT-PAR follow the same pattern as rule HOπP-OUT-RESTR. Rule HOπP-OUT-CAPTURE-FREE simply means that a transition with a capture-free context is a message output transition. We now explain how te deal with context capture with rule HOπP-OUT-CAPTURE. Suppose $P = \overline{a}\langle R\rangle S$ and $\mathbb{E}' = d[\nu c.(\Box \mid \overline{c}\langle \mathbf{0}\rangle \mathbf{0})]$ with $c \in \text{fn}(R)$; we want to obtain $P \xmapsto{\overline{a},Q,\mathbb{E}'}_{\widetilde{b}} \nu c.(d[S \mid \overline{c}\langle \mathbf{0}\rangle \mathbf{0}] \mid Q')$ (with the scope of c extended out of d). We first consider the transition $P \xmapsto{\overline{a},Q,\mathbb{E}\{\mathbb{F}\}}_{\widetilde{b}} P'$ without capture on c; in our case we have $P \xmapsto{\overline{a},Q,d[\Box]}_{\widetilde{b}} d[S \mid \overline{c}\langle \mathbf{0}\rangle \mathbf{0}] \mid Q' = P'$ with $\mathbb{E} = d[\Box]$ and $\mathbb{F} = \Box \mid \overline{c}\langle \mathbf{0}\rangle \mathbf{0}$. Using the rule we have $P \xmapsto{\overline{a},Q,\mathbb{E}\{\nu c.\mathbb{F}\}}_{\widetilde{b}} \nu c.P'$, i.e. $P \xmapsto{\overline{a},Q,\mathbb{E}'}_{\widetilde{b}} \nu c.(d[S \mid \overline{c}\langle \mathbf{0}\rangle \mathbf{0}] \mid Q')$. The scope of c is extended outside $\mathbb{E}$ and includes the recipient of the message as wished.

Premise $P \xmapsto{\overline{a},Q,\Box}_{\widetilde{b}} P'$ of rule HOπP-HO (Figure 4) means that process P sends a message on a to Q without any bisimulation context to surround P, and the result is P'. Consequently we have $P \mid Q \xmapsto{\tau} P'$ by communication on a, which is precisely the wished conclusion. Names $\widetilde{b}$ are no longer needed for scope extrusion, so we simply forget them.

We now establish the correspondence between the contextual LTS and the complementary LTS.

Lemma 14. *Let P be an HOπP process. We have:*

$$\frac{\mathrm{fn}(R) = \widetilde{b} \qquad Q \overset{a,R}{\longmapsto} Q' \qquad \mathrm{bn}(\mathbb{E}) \cap \widetilde{b} = \emptyset}{\overline{a}\langle R\rangle S \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} Q' \mid \mathbb{E}\{S\}}\ \text{HO}\pi\text{P-OUT}$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}\{b[\Box]\}}{\longrightarrow}_{\widetilde{b}} P'}{b[P] \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'}\ \text{HO}\pi\text{P-OUT-LOC}$$

$$\frac{\mathrm{fn}(P) = \widetilde{b} \qquad Q \overset{b,P}{\longmapsto} Q' \qquad \mathrm{bn}(\mathbb{E}) \cap \widetilde{b} = \emptyset}{b[P] \overset{\overline{b},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} Q' \mid \mathbb{E}\{\mathbf{0}\}}\ \text{HO}\pi\text{P-OUT-PASSIV}$$

$$\frac{P_1 \overset{\overline{a},Q,\mathbb{E}\{\Box \mid P_2\}}{\longrightarrow}_{\widetilde{b}} P'}{P_1 \mid P_2 \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'}\ \text{HO}\pi\text{P-OUT-PAR}$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P' \qquad c \neq a \qquad c \in \widetilde{b}}{\nu c.P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}\setminus c} \nu c.P'}\ \text{HO}\pi\text{P-OUT-EXTR}$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}{\longrightarrow}_{\widetilde{b}} P' \qquad c \neq a \qquad c \notin \widetilde{b}}{\nu c.P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'}\ \text{HO}\pi\text{P-OUT-RESTR}$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'}{P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'}\ \text{HO}\pi\text{P-OUT-CAPTURE-FREE}$$

$$\frac{P \overset{\overline{a},Q,\mathbb{E}\{\mathbb{F}\}}{\longmapsto}_{\widetilde{b}} P' \qquad c \in \widetilde{b}}{P \overset{\overline{a},Q,\mathbb{E}\{\nu c.\mathbb{F}\}}{\longmapsto}_{\widetilde{b}} \nu c.P'}\ \text{HO}\pi\text{P-OUT-CAPTURE}$$

Figure 5: Complementary LTS for HOπP: message output actions

- $P \xrightarrow{\tau} P'$ *iff* $P \overset{\tau}{\longmapsto} P'$.
- *If* $P \xrightarrow{a} F$, *then for all* R *we have* $P \overset{a,R}{\longmapsto} F \circ R$. *Conversely, if* $P \overset{a,R}{\longmapsto} P'$, *then there exists* F *such that* $P \xrightarrow{a} F$ *and* $P' = F \circ R$.
- *If* $P \xrightarrow{\overline{a}} C$, *then for all* Q *such that* $Q \xrightarrow{a} F$ *and for all* $\mathbb{E}$, *we have* $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$ *with* $\widetilde{b} = fn(o(C)) \setminus bn(C)$. *Conversely, if* $P \overset{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$, *then there exists* F, C *such that* $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = fn(o(C)) \setminus bn(C)$, *and* $P' = F \bullet \mathbb{E}\{C\}$.

The proof is done by induction on P and can be found in Appendix B.1.

4.3 Complementary Bisimilarities

Strong complementary bisimilarity is defined as follows.

Definition 11 (Strong complementary bisimilarity). *A relation* $\mathcal{R}$ *on closed processes is a* strong complementary simulation *iff* $P \mathcal{R} Q$ *implies* $fn(P) = fn(Q)$ *and for all* $P \overset{\lambda}{\longmapsto} P'$, *there exists* Q' *such that* $Q \overset{\lambda}{\longmapsto} Q'$ *and* $P' \mathcal{R} Q'$.

A relation $\mathcal{R}$ *is a* strong complementary bisimulation *iff* $\mathcal{R}$ *and* $\mathcal{R}^{-1}$ *are strong complementary simulations. Two closed processes* P *and* Q *are* strong complementary bisimilar, *noted* $P \sim_m Q$, *iff there exists a strong complementary bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$.

Notice that we still have the condition on free names $\text{fn}(P) = \text{fn}(Q)$. We now prove that $\sim_m$ is sound (by proving that it is a congruence) using Howe's method. We have to extend Howe's closure to evaluation contexts.

Definition 12 (Howe's closure for evaluation contexts). *We have* $\mathbb{E} \sim_m^\bullet \mathbb{F}$ *iff for all* P, *we have* $\mathbb{E}\{P\} \sim_m^\bullet \mathbb{F}\{P\}$.

We prove the following simulation-like property for $\sim_m^\bullet$.

Lemma 15. *Let* P, Q *be closed processes. If* $P \sim_m^\bullet Q$ *then:*

- *If* $P \overset{\tau}{\longmapsto} P'$, *then there exists* Q' *such that* $Q \overset{\tau}{\longmapsto} Q'$ *and* $P' \sim_m^\bullet Q'$.
- *If* $P \overset{a,R}{\longmapsto} P'$, *then for all* $R \sim_m^\bullet R'$, *there exists* Q' *such that* $Q \overset{a,R'}{\longmapsto} Q'$ *and* $P' \sim_m^\bullet Q'$.
- *If* $P \overset{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$, *then for all* $T \sim_m^\bullet T'$ *and all* $\mathbb{E} \sim_m^\bullet \mathbb{F}$, *there exists* Q' *such that* $Q \overset{\overline{a},T',\mathbb{F}}{\longmapsto}_{\widetilde{b}} Q'$ *and* $P' \sim_m^\bullet Q'$.

The proof is by induction on the derivation of $P \sim_m^\bullet Q$. We just detail the communication case: we have $P_1 \mid P_2 \sim_m^\bullet Q_1 \mid Q_2$ with $P_1 \sim_m^\bullet Q_1$, $P_2 \sim_m^\bullet Q_2$ and $P_1 \overset{\overline{a},P_2,\Box}{\longmapsto}_{\widetilde{b}} P'$. We can apply directly the message output clause of the induction hypothesis: there exists Q' such that $Q_1 \overset{\overline{a},Q_2,\Box}{\longmapsto}_{\widetilde{b}} Q'$ and $P' \sim_m^\bullet Q'$. We conclude that $Q_1 \mid Q_2 \overset{\tau}{\longmapsto} Q'$ (by rule HOπP-HO) with $P' \sim_m^\bullet Q'$ as wished.

Theorem 4. *$\sim_m$ is sound.*

The soundness proof for strong and weak complementary bisimilarities follow the same pattern, but the weak one is a little harder. Consequently we detail only the weak proof in Appendix B.2.

We may wonder if strong early context and complementary bisimilarities have the same discriminating power. The output clause of complementary bisimilarity requires that transition $P \overset{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ has to be matched by a transition $Q \overset{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} Q'$ with the same set of names $\widetilde{b}$ which may be extruded. At first glance, we do not have this requirement for the early strong context bisimilarity. Nevertheless, we prove that both relations coincide.

As explained in Section 3.2 for HOπ, soundness of $\sim_m$ gives us one inclusion easily.

Lemma 16. *We have $\sim_m \subseteq \sim$.*

For the reverse inclusion, we have to prove first the following result on concretion names:

Lemma 17. *Let $P \sim Q$. Let $P \xrightarrow{\overline{a}} C$, F an abstraction, and $Q \xrightarrow{\overline{a}} C'$ such that for all $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \sim F \bullet \mathbb{E}\{C'\}$. Then we have $fn(o(C)) \setminus bn(C) = fn(o(C')) \setminus bn(C')$.*

In the following proof, for a name a and a process P such that $X \notin \mathrm{fv}(P)$, we write $a.P$ for $a(X)P$, and we write $\overline{a}.P$ for $\overline{a}\langle \mathbf{0} \rangle P$. For a set of process (P_i), we write $(P_i)^i$ for $P_1 \mid \ldots \mid P_n$.

Proof. Let $P \sim Q$ such that $P \xrightarrow{\overline{a}} C$. Let F be an abstraction. By bisimilarity definition, there exists C' such that $Q \xrightarrow{\overline{a}} C'$ and for all $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \sim F \bullet \mathbb{E}\{C'\}$. Let $\{x_i\} = \mathrm{fn}(o(C)) \setminus \mathrm{bn}(C)$ and $y_i = \mathrm{fn}(o(C')) \setminus \mathrm{bn}(C')$. Given two sets $\widetilde{z_i}, \widetilde{d_i}$ of pairwise distinct names with the same number of element, we define $\mathbb{E}_{\widetilde{z_i},\widetilde{d_i}}$ as

$$\mathbb{E}_{\widetilde{z_i},\widetilde{d_i}} = \nu b.(b[\nu \widetilde{z_i}.(\Box \mid (z_i.\mathbf{0} \mid \overline{z_i}.\overline{z_i}.d_i.\mathbf{0})^i] \mid b(X)(X \mid X))$$

A name d_{i_0} becomes observable after passivation and duplication of hidden locality b iff two communications on the corresponding name z_{i_0} happen, which is possible iff z_{i_0} is extruded outside b.

Let $\widetilde{d_i}$ be a set of names with the same number of elements than $\widetilde{x_i}$, pairwise distinct, and which do not appear in P, Q, F. We have $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C\} \sim F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C'\}$. By definitions of $\widetilde{x_i}$, all the names $\widetilde{x_i}$ are extruded in $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C\}$, hence we have $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C\} \overset{\tau}{\Rightarrow} \xrightarrow{d_i}$ for all i. To match these transitions, the names $\widetilde{x_i}$ has to be extruded in $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C'\}$. However a name x is extruded in $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C'\}$ iff we have $x \in \widetilde{y_i}$, consequently we have $\widetilde{x_i} \subseteq \widetilde{y_i}$.

With the same reasoning on $F \bullet \mathbb{E}_{\widetilde{y_i},\widetilde{e_i}}\{C\} \sim F \bullet \mathbb{E}_{\widetilde{y_i},\widetilde{e_i}}\{C'\}$ (for some names $\widetilde{e_i}$) and using transitions from $F \bullet \mathbb{E}_{\widetilde{y_i},\widetilde{e_i}}\{C'\}$, we have $\widetilde{y_i} \subseteq \widetilde{x_i}$. Consequently we have $\widetilde{y_i} = \widetilde{x_i}$, i.e. $\mathrm{fn}(o(C)) \setminus \mathrm{bn}(C) = \mathrm{fn}(o(C')) \setminus \mathrm{bn}(C')$ as wished.

□

Using Lemma 17, we have the reverse inclusion:

Lemma 18. *We have* $\sim \subseteq \sim_m$.

The proof is done by showing that $\sim$ is a strong complementary bisimilarity.

We can also prove soundness and correspondence between bisimilarities in the weak case. As in HOPπ we write $\stackrel{\tau}{\Mapsto}$ the reflexive and transitive closure of $\stackrel{\tau}{\longmapsto}$. We define $\stackrel{a,R}{\Longmapsto} \triangleq \stackrel{\tau}{\Mapsto} \stackrel{a,R}{\longmapsto} \stackrel{\tau}{\Mapsto}$, and we define $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$ as $P \stackrel{\tau}{\Mapsto} \stackrel{\overline{a},Q',\mathbb{E}}{\longmapsto}_{\widetilde{b}} \stackrel{\tau}{\Mapsto} P'$ with $Q \stackrel{\tau}{\Mapsto} Q'$. Weak complementary bisimilarity is defined as follow:

Definition 13 (**Weak complementary bisimilarity**). *A relation $\mathcal{R}$ on closed processes is a* weak complementary simulation *iff $P \ \mathcal{R} \ Q$ implies $fn(P) = fn(Q)$ and for all $P \stackrel{\lambda}{\longmapsto} P'$, there exists Q' such that $Q \stackrel{\lambda}{\Mapsto} Q'$ and $P' \ \mathcal{R} \ Q'$.*

A relation $\mathcal{R}$ is a weak complementary bisimulation *iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are weak complementary simulations. Two closed processes P and Q are* weak complementary bisimilar*, noted $P \approx_m Q$, iff there exists an weak complementary bisimulation $\mathcal{R}$ such that $P \ \mathcal{R} \ Q$.*

As in the strong case, we have the following results:

Theorem 5. *The relation $\approx_m$ is a congruence.*

Lemma 19. *We have $\approx_m = \approx$.*

We use the same techniques as in the strong case. All correspondence proofs (between LTS and bisimilarities) and the soundness proof of $\approx_m$ can be found in Appendix B.

4.4 Completeness

In this section we give a completeness result with respect to weak barbed congruence, yielding the first co-inductive characterization of barbed congruence in a calculus featuring both passivation and restriction. It shows that weak complementary bisimilarity (and therefore weak early context bisimilarity since the two relations coincide) is a suitable behavioral equivalence.

We define reduction $\longrightarrow$ as $\equiv \stackrel{\tau}{\longmapsto} \equiv$ and weak reduction $\Longrightarrow$ as the reflexive and transitive closure of $\longrightarrow$. Observables $\mu = a \mid \overline{a}$ of a HOπP process P, written $P \downarrow_\mu$ are free names where a communication or passivation may happen. As usual, contexts $\mathbb{C}$ are HOπP terms with a hole $\Box$.

Definition 14 (**Weak barbed congruence**). *Two process P and Q are* weak barbed bisimilar *iff the following conditions hold:*

- *If $P \downarrow_\mu$, then we have $Q \Longrightarrow \downarrow_\mu$.*
- *If $P \longrightarrow P'$, then there exists Q' such that $Q \Longrightarrow Q'$ and P' and Q' are weak barbed bisimilar.*
- *The converse of the above conditions on Q.*

Two process P and Q are weak barbed congruent*, written $P \approx_b Q$, iff for all contexts $\mathbb{C}$, $\mathbb{C}\{P\}$ and $\mathbb{C}\{Q\}$ are weak barbed bisimilar.*

We now prove that weak complementary bisimilarity $\approx_m$ and weak barbed congruence coincide on *image-finite* processes. The limitation on image-finite processes is classical and can be found in π-calculus [16] for instance.

Definition 15 (**Image finite processes**). *A closed process P is image finite iff for all label λ, the set $\{P', P \stackrel{\lambda}{\Rightarrow} P'\}$ is finite.*

With Theorem 5, we already have the following inclusion.

Theorem 6. *We have $\approx_m \subseteq \approx_b$*

We now prove the reverse inclusion on image-finite processes.

Theorem 7. *Let P, Q be image-finite processes. If $P \approx_b Q$ then $P \approx_m Q$.*

The theorem is proved by contradiction. We define a family of relations $\approx_{m,k}$, with k an integer, which differentiate several levels of bisimulations by stating that processes have to be bisimilar only during the first k steps, and such that $\approx_m = \bigcap_k \approx_{m,k}$.

- We have $P \approx_{m,0} Q$ iff $\text{fn}(P) = \text{fn}(Q)$.
- We have $P \approx_{m,k+1} Q$ iff for $P \stackrel{\lambda}{\longmapsto} P'$, there exists Q' such that $Q \stackrel{\hat{\lambda}}{\Rightarrow} Q'$ and $P' \approx_{m,k} Q'$, and conversely for $Q \stackrel{\lambda}{\longmapsto} Q'$.

By induction we prove that if for some k we have $P \not\approx_{m,k} Q$, then there exists a context $\mathbb{C}_k$ such that $\mathbb{C}_k\{P\} \not\approx_b \mathbb{C}_k\{Q\}$. If $P \not\approx_m Q$, then there exists k such that $P \not\approx_{m,k} Q$, hence there exists a context $\mathbb{C}$ such that $\mathbb{C}\{P\} \not\approx_b \mathbb{C}\{Q\}$. Consequently P and Q are not weakly barbed congruent.

5 Application to the Seal calculus

In this section we define a complementary semantics for the Seal calculus [19, 6], a calculus with higher-order mobility. Until now only sound delay bisimilarities have been defined [6] for this calculus. We first quickly remind the syntax, semantics, and previous results on Seal-calculus bisimilarities.

5.1 Syntax and Semantics

The Seal-calculus [19] is a name-passing calculus with hierarchical localities (called *seals*) which may be duplicated, erased, or moved up and down in the seal hierarchy. Channel names are written $a, b, x, y, \ldots$. The syntax of the calculus is:

$$\begin{array}{lcl} P & ::= & \mathbf{0} \mid P \mid P \mid a[P] \mid \nu a.P \mid \overline{a}^{\eta}(\widetilde{b}).P \mid a^{\eta}(\widetilde{b}).P \mid \overline{a}^{\eta}\{b\}.P \mid a^{\eta}\{\widetilde{b}\}.P \\ \eta & ::= & * \mid \uparrow \mid a \end{array}$$

We work on the *Shared Seal* [6], where channels are shared between two communicating agents in parent-child relation. Locations η represents the partner the channel is shared with: $b^{\uparrow}$ means that channel b is shared with the parent seal, b^{a} means that channel b is shared with with the child a, and b^{*} means that b is local.

We give the Shared Seal operational semantics in terms of a structural congruence and of a reduction relation. The structural congruence $\equiv$ is the smallest congruence on Seal processes verifying the following rules:

$$P \mid (Q \mid R) \equiv (P \mid Q) \mid R \qquad P \mid Q \equiv Q \mid P \qquad P \mid \mathbf{0} \equiv P$$

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

Notice that as in Homer, Kell, and HOπP, we do not have $\nu a.b[P] \equiv b[\nu a.P]$ as a structural congruence axiom because of seal duplication [6].

The reduction relation $\longrightarrow$ is the smallest relation on Seal processes verifying the rules given in Figure 6. The first three rules deal with the first-order polyadic communications, while the three following rules deal with higher-order seal mobility. Seal mobility require interaction between three processes: the seal being moved $c[P]$, the emitting process $\overline{a}^{\eta}\{c\}.P$ which emits name c on channel a and continues as P, and the receiving process $a^{\eta}\{\widetilde{b}\}.Q$, which waits for a name c of a seal $c[P]$ on a, destroy seal $c[P]$, and run several seals $x_1[P] \ldots x_n[P]$ (where $x_1 \ldots x_n$ are the name specified in $\widetilde{b}$) in parallel with Q. Notice that scope extrusion outside seals is allowed for name passing but not for process mobility (because of premise $\text{fn}(R) \cap \widetilde{z} = \emptyset$).

Castagna and Zappa-Nardelli [6] define a LTS-based semantics and bisimilarity for Shared Seal. The interaction between three processes needed for seal mobility makes a LTS hard to define. In addition to the labels one may "naturally" think of (τ-action and the two kinds of emission and reception of names), Castagna and Zappa-Nardelli introduce four additional labels for seal mobility. First, they introduce a *freeze* label P_a which means that a seal a containing P may be moved. They also introduce three partial synchronizations between two processes, waiting for the third corresponding process to complete a seal move. For instance, a seal $c[P]$ in parallel with an emission $\overline{a}^{\eta}\{c\}.Q$ result in an action called *capsule*, which needs a seal reception on a to complete the seal move.

Castagna and Zappa-Nardelli define a weak delay context bisimilarity based on this LTS called *Hoe bisimilarity*, which performs tests on receiving contexts for the freeze and capsule actions (i.e. in the higher-order output cases). Hoe bisimilarity is sound but not complete with respect to barbed congruence because of its delay style. The authors also point out that it is probably not possible to find a context that distinguishes partial synchronization labels.

5.2 Complementary Semantics

We now give complementary semantics and bisimilarity for the Seal-calculus. The main issues are to deal with the three-parts seal mobility and with restrictions on com-

$$\overline{a}^*(\widetilde{v}).P \mid a^*(\widetilde{d}).Q \longrightarrow P \mid Q\{\widetilde{v}/\widetilde{d}\}$$

$$\frac{\widetilde{v} \cap \widetilde{z} = \emptyset \qquad a \notin \widetilde{z}}{\overline{a}^b(\widetilde{v}).P \mid b[\nu\widetilde{z}.(a^\uparrow(\widetilde{d}).Q_1 \mid Q_2)] \longrightarrow P \mid b[\nu\widetilde{z}.(Q_1\{\widetilde{v}/\widetilde{x}\} \mid Q_2)]}$$

$$\frac{a \notin \widetilde{z}}{a^b(\widetilde{d}).Q \mid b[\nu\widetilde{z}.(\overline{a}^\uparrow(\widetilde{v}).P_1 \mid P_2)] \longrightarrow \nu(\widetilde{z} \cap \widetilde{v}).(Q\{\widetilde{v}/\widetilde{d}\} \mid b[\nu(\widetilde{z} \setminus \widetilde{v}).(P_1 \mid P_2)])}$$

$$\overline{a}^*\{c\}.P \mid a^*\{\widetilde{d}\}.Q \mid c[R] \longrightarrow P \mid Q \mid x_1[R] \mid \ldots \mid x_n[R]$$

$$\frac{a \notin \widetilde{z} \qquad \mathrm{fn}(R) \cap \widetilde{z} = \emptyset}{\overline{a}^b\{c\}.P \mid c[R] \mid b[\nu\widetilde{z}.(a^\uparrow\{\widetilde{d}\}.Q_1 \mid Q_2)] \longrightarrow P \mid b[\nu\widetilde{z}.(Q_1 \mid Q_2 \mid x_1[R] \ldots x_n[R])]}$$

$$\frac{a \notin \widetilde{z} \qquad \mathrm{fn}(R) \cap \widetilde{z} = \emptyset}{a^b\{\widetilde{d}\}.Q \mid b[\nu\widetilde{z}.(c[R] \mid \overline{a}^\uparrow\{c\}.P_1 \mid P_2)] \longrightarrow Q \mid x_1[R] \ldots x_n[R] \mid b[\nu\widetilde{z}.(P_1 \mid P_2)]}$$

$$\frac{P \equiv P' \qquad P' \longrightarrow Q' \qquad Q' \equiv Q}{P \longrightarrow Q} \qquad \frac{P \longrightarrow P'}{P \mid Q \longrightarrow P' \mid Q} \qquad \frac{P \longrightarrow P'}{a[P] \longrightarrow a[P']}$$

$$\frac{P \longrightarrow P'}{\nu a.P \longrightarrow \nu a.P'}$$

Figure 6: Shared Seal reduction rules

munications.

We define location of an action $\gamma ::= * \mid a$ and $*[P] \triangleq P$. First-order input $P \overset{\gamma_1[a^{\eta_1}(\widetilde{v})]}{\longmapsto} P'$ means that process P may receive names $\widetilde{v}$ on shared channel a^{η_1} and continues as P'. Location γ_1 means that reception occurs at "top-level" if $\gamma_1 = *$ or inside a seal b if $\gamma_1 = b$. First-order output $Q \overset{(\nu\widetilde{z})\gamma_2[\overline{a}^{\eta_2}(\widetilde{v})]}{\longmapsto} Q'$ means that process Q may emits names $\widetilde{v}$ on shared channel a^{η_2} and continue as Q'. Scope of names $\widetilde{z}$ has to be expanded to encompass the recipient of names $\widetilde{v}$.

Labels $\gamma_1, \gamma_2, \eta_1$, and η_2 are used to check that communication may indeed happen between P and Q. We have synchronization between (γ_1, η_1) and (γ_2, η_2), written $(\gamma_1, \eta_1) \curlyvee (\gamma_2, \eta_2)$, iff $\gamma_1 = \eta_1 = \gamma_2 = \eta_2 = *$ or $\gamma_1 = b, \eta_1 = \uparrow, \gamma_2 = *, \eta_2 = b$ or $\gamma_1 = *, \eta_1 = b, \gamma_2 = b, \eta_2 = \uparrow$. Seal name output $P \overset{\overline{a}^{\eta}\{b\}}{\longmapsto} P'$ follows the same pattern as first-order output, except that location is not needed since a seal name b cannot cross a seal boundary without the moving seal b (see capsule rules for further explanation). Seal input $P \overset{\gamma[a^{\eta}\{Q\}]}{\longmapsto} P'$ means that process P may receive a seal name on a, and the body of the moving seal is Q.

We write μ for first-order labels, i.e. $\mu \in \{\tau, \gamma[a^{\eta}(\widetilde{v})], (\nu\widetilde{z})\gamma[\overline{a}^{\eta}(\widetilde{v})], \overline{a}^{\eta}\{b\}\}$. Rules for first-order communication, seal name output, seal input, and τ-actions can be found in 7, except the symmetric of communication and parallel rules. The rules are the same as Castagna and Zappa Nardelli's LTS, except the seal mobility synchronization rule which we explain later.

Rules for seal output are more difficult to write. To complement a seal $b[P]$, we need two processes: a sending process S and a receiving process R. Process S has to be within the same seal as $b[P]$ while process S may be in the parent seal or in a child seal. To take into account all the possible cases, we introduce a location label γ and evaluation contexts $\mathbb{E}, \mathbb{F}$. Syntax of seal evaluation context $\mathbb{E}$ is $\mathbb{E} ::= \Box \mid P \mid \mathbb{E} \mid \mathbb{E} \mid P \mid \nu a.\mathbb{E}$. Labels $\gamma, \mathbb{E}, \mathbb{F}$ mimic receiving contexts in Hoe bisimilarity definition [6]. The freeze action $P \overset{a,b,R,S,\gamma,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'$ means that P contains a seal b and we have $\gamma[\mathbb{F}\{\mathbb{E}\{P\} \mid S\}] \mid R \overset{\tau}{\longmapsto} P'$ by moving seal b (with $*[P] \triangleq P$ by convention). For instance we have the following rule

$$\frac{S \overset{\overline{a}^{*}\{b\}}{\longmapsto} S' \qquad R \overset{*[a^{*}\{P\}]}{\longmapsto} R' \qquad \text{fn}(P) = \widetilde{d}}{b[P] \overset{a,b,S,R,*,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} \mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid S'\} \mid R'}$$

Process S may emit locally a seal name b on a and process R may receive locally a seal body P on a. Synchronization may happen if both processes are in parallel with a seal $b[P]$. We keep free names of seal $\widetilde{d}$ in the label for scope extrusion. We may have to add a seal z like in the following rule:

$$\frac{S \overset{\overline{a}^{\uparrow}\{b\}}{\longmapsto} S' \qquad R \overset{*[a^{z}\{P\}]}{\longmapsto} R' \qquad \text{fn}(P) = \widetilde{d}}{b[P] \overset{a,b,S,R,z,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} z[\mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid S'\}] \mid R'}$$

Congruence

$$\frac{P \overset{\mu}{\longmapsto} P'}{P \mid Q \overset{\mu}{\longmapsto} P' \mid Q} \qquad \frac{P \overset{\mu}{\longmapsto} P' \qquad y \notin \mathrm{fn}(\mu) \qquad \mu \neq (\nu\widetilde{z})\gamma[\overline{a}^{\eta}(\widetilde{v})]}{\nu y.P \overset{\mu}{\longrightarrow} \nu y.P'}$$

$$\frac{P \overset{(\nu\widetilde{z})\gamma[\overline{a}^{\eta}(\widetilde{v})]}{\longmapsto} P' \qquad y \notin \{a, \gamma, \eta\} \qquad y \notin \widetilde{v}}{\nu y.P \overset{(\nu\widetilde{z})\gamma[\overline{a}^{\eta}(\widetilde{v})]}{\longmapsto} \nu y.P'}$$

$$\frac{P \overset{(\nu\widetilde{z})\gamma[\overline{a}^{\eta}(\widetilde{v})]}{\longmapsto} P' \qquad y \notin \{a, \gamma, \eta\} \qquad y \in \widetilde{v}}{\nu y.P \overset{(\nu\widetilde{z}\cup y)\gamma[\overline{a}^{\eta}(\widetilde{v})]}{\longmapsto} P'} \qquad \frac{P \overset{\tau}{\longmapsto} P'}{a[P] \overset{\tau}{\longmapsto} a[P']}$$

$$\frac{P \overset{*[\alpha]}{\longmapsto} P' \qquad \alpha \in \{a^{\uparrow}(\widetilde{v}), (\nu\widetilde{z})\overline{a}^{\uparrow}(\widetilde{v}), a^{\uparrow}\{Q\}\}}{b[P] \overset{b[\alpha]}{\longmapsto} b[P']} \qquad \frac{P_1 \overset{\gamma[a^{\eta}\{Q\}]}{\longmapsto} P_1'}{P_1 \mid P_2 \overset{\gamma[a^{\eta}\{Q\}]}{\longmapsto} P_1' \mid P_2}$$

First-order communication

$$a^{\eta}(\widetilde{d}).P \overset{*[a^{\eta}(\widetilde{v})]}{\longmapsto} P\{\widetilde{v}/\widetilde{d}\} \qquad \overline{a}^{\eta}(\widetilde{v}).P \overset{(\nu\ )*[\overline{a}^{\eta}(\widetilde{v})]}{\longmapsto} P$$

Seal name output and seal input

$$a^{\eta}\{\widetilde{d}\}.P \overset{*[a^{\eta}\{Q\}]}{\longmapsto} P \mid x_1[Q] \mid \ldots \mid x_n[Q] \qquad \overline{a}^{\eta}\{b\}.P \overset{\overline{a}^{\eta}\{b\}}{\longmapsto} P$$

Synchronization

$$\frac{P \overset{\gamma_1[x^{\eta_1}(\widetilde{v})]}{\longmapsto} P' \qquad Q \overset{(\nu\widetilde{z})\gamma_2[\overline{x}^{\eta_2}(\widetilde{v})]}{\longmapsto} Q' \qquad (\gamma_1, \eta_1) \curlyvee (\gamma_2, \eta_2)}{P \mid Q \overset{\tau}{\longmapsto} \nu\widetilde{z}.(P' \mid Q')}$$

$$\frac{P \overset{a,b,R,*,\square}{\longmapsto}_{\widetilde{d}} P'}{P \mid R \overset{\tau}{\longmapsto} P'}$$

Figure 7: Rules for first-order and seal input actions

Process R is waiting a seal from a child named z and process S may send a seal name to its parent seal. Synchronization may happen when we put seal $b[P]$ and S in a seal z, and we put R in parallel with z. All freeze rules can be found in Figure 8, except the symmetric rule for parallel. Congruence rules follows the same idea as in HOπP. We do not have a congruence rule for seal extrusion since a seal b is not allowed to cross a seal boundary "alone", i.e. without a process sending name b.

A seal partially synchronized with a sending process may perform an action (crossing a seal border) which cannot be performed by a seal alone. Consequently we add a transition $P \overset{a,b,R,\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'$, which corresponds to the "capsule" partial synchronization in the Castagna and Zappa Nardelli LTS [6]. Transition $P \overset{a,b,R,\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'$ means that process P contains a seal b and process sending name b on channel a, and we have $\gamma[\mathbb{F}\{P\}] \mid R \overset{\tau}{\longmapsto} P'$ by mobility of seal b. A capsule transition is close to a freeze transition, and indeed capsule actions depend on freeze ones.

$$\frac{P \overset{a,b,S,R,\gamma,\square,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}{P \mid S \overset{a,b,R,\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}$$

The transition $P \overset{a,b,S,R,\gamma,\square,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'$ checks that P contains a seal b and that S may send b on a, consequently $P \mid S$ contains a seal b and may emit b on a. Unlike freeze actions, there exists a seal congruence rule for capsule actions.

$$\frac{P \overset{a,b,R,z,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}{z[P] \overset{a,b,R,*,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}$$

Complete rules can be found in Figure 8, except the symmetric of the parallel rule. We now explain the synchronization rule for seal mobility (Figure 7).

$$\frac{P \overset{a,b,R,*,\square}{\longmapsto}_{\widetilde{d}} P'}{P \mid R \overset{\tau}{\longmapsto} P'}$$

Premise $P \overset{a,b,R,*,\square}{\longmapsto}_{\widetilde{d}} P'$ means that process P contains a seal b partially synchronized with a sending process. Furthermore process R may receive the seal body, and we have $*[P] \mid R = P \mid R \overset{\tau}{\longmapsto} P'$, i.e. the wished conclusion.

5.3 Complementary Bisimilarity

We now define weak complementary bisimilarity and prove its soundness using Howe's method. We first define weak transitions, following the same pattern as in HOπ and HOπP. We write $\overset{\tau}{\Longmapsto}$ the reflexive and transitive closure of $\overset{\tau}{\longmapsto}$. For all labels λ except freeze and capsule ones, we define $\overset{\lambda}{\Longmapsto} \overset{\Delta}{=\!\Longmapsto} \overset{\tau}{\Longmapsto} \overset{\lambda}{\longrightarrow} \overset{\tau}{\Longmapsto}$. We define $\overset{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}{\Longmapsto}_{\widetilde{d}}$ as $\overset{\tau}{\Longmapsto} \overset{a,b,S',R',\gamma,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} \overset{\tau}{\Longmapsto}$ for some $R \overset{\tau}{\Longmapsto} R'$ and $S \overset{\tau}{\Longmapsto} S'$. We define $\overset{a,b,R,\gamma,\mathbb{F}}{\Longmapsto}_{\widetilde{d}}$ as $\overset{\tau}{\Longmapsto} \overset{a,b,R',\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} \overset{\tau}{\Longmapsto}$ for some $R \overset{\tau}{\Longmapsto} R'$.

Weak complementary bisimilarity is defined as in HOπP.

Freeze

$$\frac{S \overset{\overline{a}^*\{b\}}{\longmapsto} S' \qquad R \overset{*[a^*\{P\}]}{\longmapsto} R' \qquad \mathrm{fn}(P) = \widetilde{d}}{b[P] \overset{a,b,S,R,*,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} \mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid S'\} \mid R'}$$

$$\frac{S \overset{\overline{a}^z\{b\}}{\longmapsto} S' \qquad R \overset{z[a^\uparrow\{P\}]}{\longmapsto} R' \qquad \mathrm{fn}(P) = \widetilde{d}}{b[P] \overset{a,b,S,R,*,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} \mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid S'\} \mid R'}$$

$$\frac{S \overset{\overline{a}^\uparrow\{b\}}{\longmapsto} S' \qquad R \overset{*[a^z\{P\}]}{\longmapsto} R' \qquad \mathrm{fn}(P) = \widetilde{d}}{b[P] \overset{a,b,S,R,z,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} z[\mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid S'\}] \mid R'} \qquad \frac{P_1 \overset{a,b,S,R,\gamma,\mathbb{E}\{\Box \mid P_2\},\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}{P_1 \mid P_2 \overset{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}$$

$$\frac{P \overset{a,b,S,R,\gamma,\mathbb{E}\{\nu y.\Box\},\mathbb{F}}{\longmapsto}_{\widetilde{d}} P' \qquad y \neq b \qquad y \notin \widetilde{d}}{\nu y.P \overset{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}$$

Capsule

$$\frac{P \overset{a,b,S,R,\gamma,\Box,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}{P \mid S \overset{a,b,R,\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'} \qquad \frac{P \overset{a,b,R,z,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}{z[P] \overset{a,b,R,*,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'} \qquad \frac{P_1 \overset{a,b,R,\gamma,\mathbb{F}\{\Box \mid P_2\}}{\longmapsto}_{\widetilde{x}} P'}{P_1 \mid P_2 \overset{a,b,R,\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}$$

$$\frac{P \overset{a,b,R,\gamma,\mathbb{F}\{\nu y.\Box\}}{\longmapsto}_{\widetilde{d}} P' \qquad y \notin \{a,b\} \cup \widetilde{d}}{\nu y.P \overset{a,b,R,\gamma,\mathbb{F}}{\longmapsto}_{\widetilde{d}} P'}$$

Figure 8: Freeze and capsule rules

Definition 16. *A relation $\mathcal{R}$ on closed processes is a weak complementary simulation iff $P\ \mathcal{R}\ Q$ implies $fn(P) = fn(Q)$ and for all $P \stackrel{\lambda}{\mapsto} P'$, there exists Q' such that $Q \stackrel{\hat{\lambda}}{\Rightarrow} Q'$ and $P'\ \mathcal{R}\ Q'$.*

A relation $\mathcal{R}$ is a weak complementary bisimulation iff $\mathcal{R}$ and $\mathcal{R}^{-1}$ are weak complementary simulations. Two closed processes P and Q are weak complementary bisimilar, noted $P \approx_m Q$, iff there exists an weak complementary bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.

Using Howe's method, one can establish the following result.

Theorem 8. *Relation $\approx_m$ is sound.*

We do not detail the proof in depth since it is similar to the HOπP one. We give proof sketches in Appendix C.

Notice that we have the condition $\text{fn}(P) = \text{fn}(Q)$ while Hoe bisimilarity [6] does not have such requirement. However a seal context may distinguish two processes P, Q based on their free names. Suppose we have $a \in \text{fn}(P) \setminus \text{fn}(Q)$. We consider the following context:

$$\mathbb{C} = b[\nu a.(c[\Box] \mid \overline{d}^{\uparrow}\{c\}.\mathbf{0})] \mid d^{b}\{e\}.\mathbf{0}$$

where b, c, d, e do not occur in P, Q. Since $a \notin \text{fn}(Q)$, we have $\mathbb{C}\{Q\} \longrightarrow b[\mathbf{0}] \mid e[Q]$: a seal e becomes observable. This reduction cannot be matched by $\mathbb{C}\{P\}$, since restriction on a prevents seal c from being extruded.

There are two additional main differences between the two semantics. First, Hoe bisimilarity is only a weak delay relation while weak complementary bisimilarity is a standard weak relation. Furthermore, we have a label for only one partial synchronization (the capsule one) in complementary semantics. We conjecture that weak complementary semantics is complete with respect to weak barbed congruence on image-finite processes. However, before proving completeness, we have to establish a correspondence result between Shared Seal reduction semantics and complementary semantics; this correspondence proof is beyond the scope of the paper.

6 Related Work

Howe's method Howe's method has been originally used to prove congruence in a lazy functional programming language [10]. Baldamus and Frauenstein [2] are the first to adapt the method to process calculi for variants of Plain CHOCS [18]. They prove congruence of a late delay context bisimilarity in SOCS, a CHOCS-like calculus with static scope, where restricted names follow the emitted processes as in HOπ. They then use it for late and early delay higher-order bisimilarities in SOCD, a calculus with dynamic scoping, where emitted messages may escape the scope of their restricted names.

Hildebrandt and Godskesen adapt Howe's method for their calculus Homer [9]. Homer is a higher-order process calculi featuring hierarchical localities, local names and active process mobility (passivation). They first prove congruence for a late context

strong and delay bisimilarities [9], and then for an input-early context delay bisimilarity [7]. Strong input-early bisimilarity is complete with respect to strong barbed congruence, but as stated by the authors themselves, delay input-early bisimilarity is probably not complete with respect to weak barbed congruence because of the delay style. In [11], we use Howe's method to prove congruence of a weak non-delay higher-order bisimilarity for a calculus featuring passivation but without restriction.

Behavioral equivalences in higher-order calculi Very few higher-order calculi feature a coinductive characterization of weak barbed congruence. The calculus HOπ enjoys a nice behavioral theory: on top of the context bisimilarity (discussed in Section 2, Sangiorgi defines *normal* bisimilarity which characterizes weak barbed congruence with fewer tests than context bisimilarity. Instead of testing a set of abstractions (resp concretions) in the message output (resp message input) clause, normal bisimilarity tests only one particular abstraction (resp concretion).

Mobile Ambients [4] is a calculus with hierarchical localities and subjective linear process mobility in which a characterization of weak barbed congruence has been found. In Mobile Ambients, localities moved by themselves in the locality hierarchy without any acknowledgment from their environment, and they cannot be duplicated. Contextual characterizations of weak barbed congruence have been defined for Mobile Ambients [12] and its variant NBA [3]. Soundness proofs are done by proving that the smallest congruence which contains weak context bisimilarity is a bisimulation.

Difficulties arise in more expressive process calculi. The Seal calculus [19] [6] is a calculus with objective process mobility which allows more flexibility than Mobile Ambients: localities may be stopped, duplicated, and moved up and down in the locality hierarchy. However a process inside a locality cannot be dissociated from its locality boundary. Process mobility requires synchronisation between three processes (a process sending a name a, a receiving process, and a locality named a). The authors define a weak delay context bisimilarity in [5] called *Hoe bisimilarity* for the Seal calculus and prove its soundness. The authors point out that Hoe bisimilarity is not complete, not only because of the delay style, but also because of the labels introduced for partial synchronisation which are most likely not observable.

The Kell-calculus [17] and Homer [9] are two higher-order calculi featuring a more general process mobility called passivation or active mobility. The calculi differ in how they handle communication. In the Kell-calculus, communications may use join patterns and are only local: processes may communicate only if they are in the same locality or in direct parent-child localities. In Homer, a process may send a message to a nested sub-locality or it may passivate it, but the interactions are not allowed in the other way: a process in a sub-locality cannot send a message to a process in a parent one. Sound and complete contexts bisimilarities have been defined for both calculi in the strong case. As stated before, a weak delay input-early bisimilarity has been proved sound in Homer using Howe's method.

The calculus HOπP used in Section 4 is inspired from Kell-calculus and Homer. We study its contextual semantics in [11], which is similar to the Homer one. We also study a variant of HOπP without restriction, called HOP. We define sound and complete early higher-order and normal bisimilarities for HOP in the strong and weak

cases. We use Howe's method to prove soundness of an early weak (non delay) higher-order bisimilarity. We also show that with HOπP a large class of tests does not suffice to build a sound normal bisimulation. This casts some doubt as to whether a suitable notion of normal bisimilarity, that is with finite testing, can be found for HOπP, and therefore for Homer and the Kell calculus.

7 Conclusion and Future Work

Contextual LTS (based on abstractions and/or concretions) are widely used to define semantics of calculi with process mobility, like for instance HOπ [15], Mobile Ambients [12], Seal calculus [5], Homer [9] and Kell calculus [17]. As we explain in this paper, contextual semantics are not well suited to prove congruence with Howe's method. The method relies on a simulation-like property, which is hard to establish with early context bisimilarities. Message output clauses of context bisimilarities rely on abstractions and message input clauses rely on concretions: because of these mutual dependencies we are unable to prove the simulation-like property in the higher-order communication case.

In Homer [9, 7], Hildebrandt and Godskesen break the mutual dependencies by making the message output clause of the bisimilarity independent from abstractions. As a drawback, the definition of this input-early bisimilarity is a delay one in the weak case, which makes the relation likely not complete with respect to barbed congruence. We propose a principle to design a semantics which makes message output clause independent enough from message input, allowing the Howe's congruence proof method to work, but not completely independent, to make it work with early strong and weak (non delay) bisimilarities. We make the message output clause dependent in a process which may receive the message (i.e. a process which evolve towards an abstraction), instead of an abstraction which may directly receive the message. This subtle difference allows us to successfully use Howe's method with early bisimilarities.

We exploit this idea to define a new semantics, called complementary semantics, for a calculus called HOπP. HOπP extends HOπ with passivation, an operator found in Kell calculus and Homer. We studied HOπP contextual semantics in [11] where we showed that the HOπP behavioral theory is as difficult as Homer and Kell calculus ones. In Section 4, we define a weak non delay complementary bisimilarity and prove its soundness using Howe's method. We also prove that it coincide with weak barbed congruence on image-finite processes, yielding the first co-inductive characterization of barbed congruence in a calculus featuring both passivation and restriction.

An immediate future work would be to define a complementary semantics for process calculi without any characterization result, such as Homer and the Kell calculus. It should be easy for Homer since the HOπP semantics is close from the Homer one. It should be more difficult for Kell calculus because of join patterns: to complement an emitting process P, we need a receiving process Q, but also other emitting processes $\widetilde{R}$ to match the receiving pattern of Q. Another future work is to define a LTS rule format which guarantees that Howe's method works with the corresponding bisimilarity, possibly extending the Promoted or Higher-Order PANTH format for higher-order calculi proposed by Mousavi et al. [13].

References

[1] Michael Baldamus. *Semantics and Logic of Higher-Order Processes: Characterizing Late Context Bisimulation*. PhD thesis, Berlin University of Technology, 1998.

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

[3] Michele Bugliesi, Silvia Crafa, Massimo Merro, and Vladimiro Sassone. Communication and mobility control in boxed ambients. *Information and Computation*, 202, 2005.

[4] Luca Cardelli and Andrew D. Gordon. Mobile ambients. In *FoSSaCS '98*, volume 1378 of *LNCS*, pages 140–155. Springer, 1998.

[5] Giuseppe Castagna and Francesco Zappa Nardelli. The seal calculus revisited: Contextual equivalence and bisimilarity. In *FSTTCS '02*, volume 2556 of *LNCS*, pages 85–96. Springer, 2002.

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

[7] Jens Chr. 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.

[8] Andrew D. Gordon. Bisimilarity as a theory of functional programming. Minicourse. Notes Series NS-95-3, BRICS, University of Cambridge Computer Laboratory, July 1995. iv+59 pp.

[9] Thomas Hildebrandt, Jens Chr. Godskesen, and Mikkel Bundgaard. Bisimulation congruences for Homer — a calculus of higher order mobile embedded resources. Technical Report ITU-TR-2004-52, IT University of Copenhagen, 2004.

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

[11] S. Lenglet, A. Schmitt, and J.B.Stefani. Normal bisimulations in process calculi with passivation. Technical Report RR 6664, INRIA, 2008. Available at http://sardes.inrialpes.fr/papers/files/RR-6664.pdf.

[12] Massimo Merro and Francesco Zappa Nardelli. Behavioral theory for mobile ambients. *Journal of the ACM*, 52(6):961–1023, 2005.

[13] MohammadReza Mousavi, Murdoch J. Gabbay, and Michel A. Reniers. Sos for higher order processes (extended abstract). In *CONCUR'05*, volume 3653 of *LNCS*, pages 308–322. Springer, 2005.

[14] Davide Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis, Department of Computer Science, University of Edinburgh, 1992.

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

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

[17] 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*, January 2004.

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

[19] Jan Vitek and Giuseppe Castagna. Seal: A framework for secure mobile computations. In *ICCL'98: Workshop on Internet Programming Languages*, volume 1686 of *LNCS*, pages 47–77. Springer, 1999.

A Proofs for HOπ

A.1 Correspondence Lemmas

Lemma 20. *If $P \xrightarrow{a} F$, then for all R we have $P \xmapsto{a,R} F \circ R$. If $P \xmapsto{a,R} P'$, then there exists F such that $P \xrightarrow{a} F$ and $P' = F \circ R$.*

Proof. We proceed by structural induction on P.

- If $P = (X)P'$, then by rule CONTEXT-ABSTR we have $P \xrightarrow{a} F = (X)P'$, and by rule HO$\pi$-IN we have $P \xmapsto{a,R} P'\{R/X\} = F \circ R$ for all R, hence the result holds.
- Let $P = P_1 \mid P_2$. Suppose we have $P \xrightarrow{a} F$, which is possible only by rule CONTEXT-PAR. Consequently we have $P_1 \xrightarrow{a} F'$ and $F = F' \mid P_2$. By induction we have $P_1 \xmapsto{a,R} F' \circ R$ for all R, hence by rule HOπ-PAR we have $P \xmapsto{a,R} F' \circ R \mid P_2 = F \circ R$ as required. Suppose we have $P \xmapsto{a,R} P'$, which is possible only by rule HOπ-PAR. Consequently we have $P_1 \xmapsto{a,R} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists F such that $P_1 \xrightarrow{a} F$ and $P_1' = F \circ R$. Consequently by rule CONTEXT-PAR we have $P \xrightarrow{a} F \mid P_2$ with $P' = (F \mid P_2) \circ R$ as required.
- The restriction case is similar to the parallel case.

□

Lemma 21. *Let P be an HOπ process.*

- *We have $P \xrightarrow{\tau} P'$ iff $P \xmapsto{\tau} \equiv P'$.*
- *If $P \xrightarrow{\overline{a}} C$, then for all Q such that $Q \xrightarrow{a} F$, we have $P \xmapsto{\overline{a},Q} \equiv F \bullet C$ If $P \xmapsto{\overline{a},Q} P'$, then there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $P' \equiv F \bullet C$.*

Proof. We proceed by structural induction on P.

- Let $P = \overline{a}\langle P_1 \rangle P_2$. We have $P \xrightarrow{\overline{a}} \langle P_1 \rangle P_2 = C$. Let Q such that $Q \xrightarrow{a} F$. We have $F \bullet C = F \circ P_1 \mid \mathbb{E}\{P_2\}$. By Lemma 20, we have $Q \xmapsto{a,P_1} F \circ P_1$. By rule HO$\pi$-OUT, we have $P \xmapsto{\overline{a},Q} F \bullet C$ as wished.

  We now prove the reverse implication. We have $P \xmapsto{\overline{a},Q} Q' \mid P_2$ with $Q \xmapsto{a,P_1} Q'$. By Lemma 20, there exists F such that $Q \xrightarrow{a} F$ and $Q' = F \circ P_1$. Let $C = \langle P_1 \rangle P_2$. We have $P \xrightarrow{\overline{a}} C$, $P' = F \bullet C$ as required.
- Let $P = P_1 \mid P_2$. We first prove $P \xrightarrow{\tau} P'$ implies $P \xmapsto{\tau} P'$ by case analysis on the rule used to derive $P \xrightarrow{\tau} P'$.

– CONTEXT-PAR: in this case we have $P_1 \xrightarrow{\tau} P_1'$ and $P' = P_1' \mid P_2$. By induction we have $P_1 \overset{\tau}{\longmapsto} P_1'$, hence by rule HO$\pi$-PAR we have $P \overset{\tau}{\longmapsto} P'$ as required.

– CONTEXT-HO: in this case, we have $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\overline{a}} C$, and $P' = F \bullet C$. By induction we have $P_2 \overset{\overline{a},P_1}{\longmapsto} \equiv F \bullet C$, so by rule HO$\pi$-HO we have $P \overset{\tau}{\longmapsto} \equiv P'$ as required.

We now prove the reverse implication.

– HOπ-PAR: we have $P_1 \overset{\tau}{\longmapsto} P_1'$ and $P' = P_1' \mid P_2$. By induction we have $P_1 \xrightarrow{\tau} P_1'$, hence we have $P \xrightarrow{\tau} P_1' \mid P_2$ by rule CONTEXT-PAR.

– HOπ-HO: we have $P_1 \overset{\overline{a},P_2}{\longmapsto} P'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $P_2 \xrightarrow{a} F$ and $P' \equiv F \bullet C$. By rule CONTEXT-HO, we have $P \xrightarrow{\tau} F \bullet C$ as required.

We now prove the result on concretions. Suppose we have $P \xrightarrow{\overline{a}} C$, which is possible only by rule CONTEXT-PAR. Consequently we have $P_1 \xrightarrow{a} C'$ and $C = C' \mid P_2$. Let $Q \xrightarrow{a} F$. By induction we have $P_1 \overset{\overline{a},Q}{\longmapsto} \equiv F \bullet C'$. By rule HO$\pi$-PAR we have $P \overset{\overline{a},Q}{\longmapsto} \equiv F \bullet C' \mid P_2 \equiv F \bullet C$ as required.

Suppose we have $P \overset{\overline{a},Q}{\longmapsto} P'$, which is possible only by rule HOπ-PAR. Consequently we have $P_1 \overset{\overline{a},Q}{\longmapsto} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, and $P_1' \equiv F \bullet C$. Consequently by rule CONTEXT-PAR we have $P \xrightarrow{\overline{a}} C \mid P_2 = C'$ with $P' \equiv F \bullet C'$ as required.

- Let $P = \nu b.P_1$. Proof for τ action is the same as in the parallel case. We prove now the output correspondence. Suppose first we have $P \xrightarrow{\overline{a}} \nu \widetilde{c}.\langle R \rangle S$. By rule CONTEXT-RESTR we have $P_1 \xrightarrow{\overline{a}} C'$ and $C = \nu b.C'$. Let $Q \xrightarrow{a} F$. By induction we have $P_1 \overset{\overline{a},Q}{\longmapsto} P_1'$ with $P_1' \equiv F \bullet C'$. By rule HOπ-RESTR, we have $P \overset{\overline{a},Q}{\longmapsto} \equiv \nu b.(F \bullet C')$. If $b \in \mathrm{fn}(R)$, then we have $\nu b.(F \bullet C') = F \bullet \nu b.C'$, otherwise we have $\nu b.(F \bullet C') \equiv F \bullet \nu b.C'$, hence the result holds.

  Suppose now that $P \overset{\overline{a},Q}{\longmapsto} P'$ with $P_1 \overset{\overline{a},Q}{\longmapsto} P_1'$, $b \neq a$, and $P' = \nu b.P_1'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, and $P_1' \equiv F \bullet C$. By rule CONTEXT-RESTR we have $P \xrightarrow{\overline{a}} \nu b.C$. If $b \in \mathrm{fn}(R)$, then $F \bullet \nu b.C = \nu b.(F \bullet C) \equiv \nu b.P_1' = P'$. If $b \notin \mathrm{fn}(R)$, then $F \bullet \nu b.C \equiv \nu b.(F \bullet C) \equiv \nu b.P_1' = P'$. Consequently the result holds.

□

We now prove correspondence between $\sim$ and $\sim_m$.

Definition 17. *A relation $\mathcal{R}$ is a strong complementary bisimulation up to $\equiv$ iff for all $P \mathcal{R} Q$ and $P \overset{\lambda}{\longmapsto} P'$, there exists Q' such that $Q \overset{\lambda}{\longmapsto} Q'$ and $P' \equiv \mathcal{R} \equiv Q'$, and conversely for $Q \overset{\lambda}{\longmapsto} Q'$.*

Lemma 22. *If $\mathcal{R}$ is a strong complementary bisimulation up to $\equiv$ then $\mathcal{R} \subseteq \sim_m$.*

Proof. By showing that $\equiv\mathcal{R}\equiv$ is a strong complementary bisimulation. □

Lemma 23. *If $P \sim Q$ then $P \sim_m Q$.*

Proof. We prove that $\sim$ is a strong complementary bisimulation up to $\equiv$. Let $P \sim Q$.

- If $P \stackrel{\tau}{\mapsto} P'$ then by Lemma 21 we have $P \stackrel{\tau}{\rightarrow} P'$. By definition there exists Q' such that $Q \stackrel{\tau}{\rightarrow} Q'$ and $P' \sim Q'$. By Lemma 21 we have $Q \stackrel{\tau}{\mapsto} \equiv Q'$, and we have $P' \sim \equiv Q'$ as wished.
- If $P \stackrel{a,R}{\longmapsto} P'$, then by Lemma 20 there exists F such that $P \stackrel{a}{\rightarrow} F$ and $P' = F \circ R$. By definition there exists G such that $Q \stackrel{a}{\rightarrow} G$ and $G' \bullet \langle R \rangle \mathbf{0} \sim F \bullet \langle R \rangle \mathbf{0}$. We have $G \bullet \langle R \rangle \mathbf{0} \equiv G \circ R$ so by Lemma 20 we have $Q \stackrel{a,R}{\longmapsto} G \circ R$, and we have $P' \equiv F \bullet \langle R \rangle \mathbf{0} \sim G \bullet \langle R \rangle \mathbf{0} \equiv G \circ R$ as wished.
- If $P \stackrel{\overline{a},T}{\longmapsto} P'$, then by Lemma 21 there exists F, C such that $T \stackrel{a}{\rightarrow} F$, $P \stackrel{\overline{a}}{\rightarrow} C$, and $P' \equiv F \bullet C$. By definition there exists D such that $Q \stackrel{\overline{a}}{\rightarrow} D$ and $F \bullet C \sim F \bullet D$. By Lemma 21 we have $Q \stackrel{\overline{a},T}{\longmapsto} \equiv F \bullet D$, and we have $P' \equiv \sim \equiv F \bullet D$ as required.

□

The reverse inclusion requires the congruence of $\sim_m$, and is proved in the next section.

A.2 Congruence Proof

We recall the definitions of open extension and Howe's closure of strong complementary bisimilarity $\sim_m$.

Definition 18. *Let P and Q be two open processes. We have $P \sim_m^\circ Q$ iff $P\sigma \sim_m Q\sigma$ for all substitutions that close P and Q.*

Definition 19. *The Howe's closure $\sim_m^\bullet$ of strong complementary bisimilarity is the smallest relation verifying:*

- $\sim_m^\circ \subseteq \sim_m^\bullet$.
- $\sim_m^\bullet \sim_m^\circ \subseteq \sim_m^\bullet$.
- *For all operators op of the language, if $\widetilde{P} \sim_m^\bullet \widetilde{Q}$, then $op(\widetilde{P}) \sim_m^\bullet op(\widetilde{Q})$.*

Lemma 24. *$\sim_m^\bullet$ is reflexive.*

Proof. Because $\sim_m$ is reflexive. □

Lemma 25. *If $R \sim_m^\bullet R'$, then $P\{R/X\} \sim_m^\bullet P\{R'/X\}$.*

If $P \stackrel{a,R}{\longmapsto} P'$ and $R \sim_m^\bullet R'$, then there exists P'' such that $P \stackrel{a,R'}{\longmapsto} P''$ and $P' \sim_m^\bullet P''$.

Proof. The first item is done by structural induction on P:

- $P = \mathbf{0}$: $P\{R/X\} = \mathbf{0} = P\{R'/X\}$, hence the result holds.
- $P = X$: $P\{R/X\} = R \sim_m^\bullet R' = P\{R'/X\}$, hence the result holds.
- $P = Y \neq X$: then $P\{R/X\} = P = P\{R'/X\}$, hence the result holds.
- $P = P_1 \mid P_2$: by induction we have $P_1\{R/X\} \sim_m^\bullet P_1\{R'/X\}$ and we have $P_2\{R/X\} \sim_m^\bullet P_2\{R'/X\}$. Since $\sim_m^\bullet$ is a congruence we have $P\{R/X\} = P_1\{R/X\} \mid P_2\{R/X\} \sim_m^\bullet P_1\{R'/X\} \mid P_2\{R'/X\} = P\{R'/X\}$ as required.
- $P = \overline{a}\langle P_1\rangle P_2$: similar to the case above.
- $P = a(Y)P_1$: similar to the case above.
- $P = \nu a.P_1$: by induction we have $P_1\{R/X\} \sim_m^\bullet P_1\{R'/X\}$. Since $\sim_m^\bullet$ is a congruence, we have $P\{R/X\} = \nu a.(P_1\{R/X\}) \sim_m^\bullet \nu a.(P_1\{R'/X\}) = P\{R'/X\}$, as required.

The second item is proved by induction on the derivation of $P \overset{a,R}{\longmapsto} P'$:

- Rule HOπ-IN: we have $P = a(X)P_1 \overset{a,R}{\longmapsto} P_1\{R/X\}$. Using the first item proved above, we have $P_1\{R/X\} \sim_m^\bullet P_1\{R'/X\}$, and by rule HO$\pi$P-IN we have $P \overset{a,R'}{\longmapsto} P_1\{R'/X\}$, as required.
- Rule HOπ-PAR: we have $P = P_1 \mid P_2$ with $P_1 \overset{a,R}{\longmapsto} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists P_1'' such that $P_1 \overset{a,R'}{\longmapsto} P_1''$ and $P_1' \sim_m^\bullet P_1''$. By rule HO$\pi$-PAR, we have $P \overset{a,R'}{\longmapsto} P_1'' \mid P_2 = P''$, and since $\sim_m^\bullet$ is a congruence, we have $P' \sim_m^\bullet P''$, as required.
- Rule HOπP-IN-RESTR: we have $P = \nu b.P_1$ with $P_1 \overset{a,R}{\longmapsto} P_1'$, $b \neq a$, and $P' = \nu b.P_1'$. By induction there exists P_1'' such that $P_1 \overset{a,R'}{\longmapsto} P_1''$ and $P_1' \sim_m^\bullet P_1''$. By rule HO$\pi$-RESTR we have $P \overset{a,R}{\longmapsto} \nu b.P_1'' = P''$, and since $\sim_m^\bullet$ is a congruence we have $P' \sim_m^\bullet P''$, as required.

□

Lemma 26. *For all $P \sim_m^\bullet Q$ and all $R \sim_m^\bullet R'$, we have $P\{R/X\} \sim_m^\bullet Q\{R'/X\}$.*

Proof. By induction on the derivation of $P \sim_m^\bullet Q$.

- $P \sim_m^\circ Q$: by Lemma 25, we have $P\{R/X\} \sim_m^\bullet P\{R'/X\}$. Let σ be a substitution which closes P and Q except for X. By open extension definition we have $P\{R'/X\}\sigma \sim_m Q\{R'/X\}\sigma$, i.e. we have $P\{R'/X\} \sim_m^\circ Q\{R'/X\}$. Hence we have $P\{R/X\} \sim_m^\bullet \sim_m^\circ Q\{R'/X\}$, i.e. $P\{R/X\} \sim_m^\bullet Q\{R'/X\}$, as required.

- $P \sim_m^\bullet T \sim_m^\circ Q$: by induction we have $P\{R/X\} \sim_m^\bullet T\{R'/X\}$, and using the same technique as in the first case we have $T\{R'/X\} \sim_m^\circ Q\{R'/X\}$, hence we have $P\{R/X\} \sim_m^\bullet Q\{R'/X\}$, as required.

- $op(\widetilde{P'}) \sim_m^\bullet op(\widetilde{Q'})$ with $\widetilde{P'} \sim_m^\bullet \widetilde{Q'}$. By induction we have $\widetilde{P'\{R/X\}} \sim_m^\bullet \widetilde{Q'\{R'/X\}}$, hence we have $op(\widetilde{P'\{R/X\}}) \sim_m^\bullet op(\widetilde{Q'\{R'/X\}})$ since $\sim_m^\bullet$ is congruence. Consequently we have $P\{R/X\} \sim_m^\bullet Q\{R'/X\}$, as required.

□

Lemma 27. *Let $P \sim_m^\bullet Q$. For every substitution σ, we have $P\sigma \sim_m^\bullet Q\sigma$ using a derivation of the same size.*

Proof. By induction on $P \sim_m^\bullet Q$. Most cases are immediate by induction. The base case is $P \sim_m^\circ Q$. We show that $P\sigma \sim_m^\circ Q\sigma$. Let σ' a substitution that closes $P\sigma$ and $Q\sigma$, then $\sigma\sigma'$ closes P and Q, thus $P\sigma\sigma' \sim_m Q\sigma\sigma'$. □

We write $(\sim_m)_c^\bullet$ the restriction of $\sim_m^\bullet$ to closed processes.

Lemma 28. *Let $P\ (\sim_m)_c^\bullet\ Q$. If $P \overset{a,R}{\longmapsto} P'$, then for all R' such that $R\ (\sim_m)_c^\bullet\ R'$, there exists Q' such that $Q \overset{a,R'}{\longmapsto} Q'$ and $P'\ (\sim_m)_c^\bullet\ Q'$.*

Proof. By induction on the size of the derivation of $P\ (\sim_m)_c^\bullet\ Q$.

- $P \sim_m^\circ Q$. By Lemma 25 there exists P'' such that $P \overset{a,R'}{\longmapsto} P''$ and $P' \sim_m^\bullet P''$. Since P, Q are closed, we have $P \sim_m Q$; by bisimulation definition there exists Q' such that $Q \overset{a,R'}{\longmapsto} Q'$ and $P'' \sim_m Q'$. Since P, R' are closed, P'' is closed. Consequently, we have $P' \sim_m^\bullet \sim_m^\circ Q'$. Since P, R are closed, P' is closed. Processes P', Q' are closed, hence we have $P'\ (\sim_m)_c^\bullet\ Q'$, as required.

- $P \sim_m^\bullet T \sim_m^\circ Q$. Let σ be a substitution that closes T; since P is closed and by Lemma 27, we have $P \sim_m^\bullet T\sigma$. By induction there exists T' such that $T\sigma \overset{a,R'}{\longmapsto} T'$ and $P'\ (\sim_m)_c^\bullet\ T'$. By open extension definition and since Q is closed, we have $T\sigma \sim_m Q$. By definition of $\sim_m$ there exists Q' such that $Q \overset{a,R'}{\longmapsto} Q'$ and $T' \sim_m Q'$. Consequently we have $P' \sim_m^\bullet \sim_m^\circ Q'$, and since P, Q, R, R' are closed, P', Q' are closed too. Thus, we have $P'\ (\sim_m)_c^\bullet\ Q'$ as required.

- $op(\widetilde{P}) \sim_m^\bullet op(\widetilde{Q})$ with $\widetilde{P} \sim_m^\bullet \widetilde{Q}$. By case analysis on op.

  - $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$ with $P_1 \overset{a,R}{\longmapsto} P_1'$. By induction there exists Q_1' such that $Q_1 \overset{a,R'}{\longmapsto} Q_1'$ and $P_1' \sim_m^\bullet Q_1'$. Using rule HOπ-PAR, we have $Q \overset{a,R'}{\longmapsto} Q_1' \mid Q_2$. Since $\sim_m^\bullet$ is a congruence, we have $P_1' \mid P_2 \sim_m^\bullet Q_1' \mid Q_2$. Since P, Q, R, R' are closed, all the involved processes are closed and we have $P_1' \mid P_2\ (\sim_m)_c^\bullet\ Q_1' \mid Q_2$, as required.

– $P = a(X)P_1$, $Q = a(X)Q_1$ with $P \overset{a,R}{\longmapsto} P_1\{R/X\}$. By Lemma 26, we have $P_1\{R/X\} \sim_m^\bullet Q_1\{R'/X\}$. Using rule HO$\pi$-IN, we have $Q \overset{a,R'}{\longmapsto} Q_1\{R'/X\}$. We have $P_1\{R/X\}\ (\sim_m)_c^\bullet\ Q_1\{R/X\}$ since the involved processes are closed.

– $P = \nu a.P_1$ and $Q = \nu a.Q_1$. Similar to the parallel case.

□

Lemma 29. *Let $P \overset{\overline{a},T}{\longmapsto} P'$ and $T \sim_m^\bullet T'$. There exists P'' such that $P \overset{\overline{a},T'}{\longmapsto} P''$ and $P' \sim_m^\bullet P''$.*

Proof. By induction on the derivation of $P \overset{\overline{a},T}{\longmapsto} P'$.

- $P = \overline{a}\langle R\rangle S$ with $T \overset{a,R}{\longmapsto} Q$ and $P' = Q \mid S$. By Lemma 28 there exists Q' such that $T' \overset{a,R}{\longmapsto} Q'$ and $Q \sim_m^\bullet Q'$. By rule HOπ-OUT, we have $P \overset{\overline{a},T'}{\longmapsto} Q' \mid S = P''$. Since $\sim_m^\bullet$ is a congruence, we have $P' \sim_m^\bullet P''$, as required.

- $P = P_1 \mid P_2$ with $P_1 \overset{\overline{a},T}{\longmapsto} P'$. By induction there exists P'' such that $P_1 \overset{\overline{a},T'}{\longmapsto} P''$ and $P' \sim_m^\bullet P''$. By rule HOπ-PAR we have $P \overset{\overline{a},T'}{\longmapsto} P'' \mid P_2$, and since $\sim_m^\bullet$ is a congruence, we have $P' \mid P_2 \sim_m^\bullet P'' \mid P_2$, as required.

- $P = \nu b.P_1$ with $P_1 \overset{\overline{a},T}{\longmapsto} P_1'$, $b \neq a$. Similar to the case above.

□

Lemma 30. *Let $P\ (\sim_m)_c^\bullet\ Q$.*

- *If $P \overset{\tau}{\longmapsto} P'$ then there exists Q' such that $Q \overset{\tau}{\longmapsto} Q'$ and $P'\ (\sim_m)_c^\bullet\ Q'$.*

- *If $P \overset{\overline{a},T}{\longmapsto} P'$ and $T\ (\sim_m)_c^\bullet\ T'$, then there exists Q' such that $Q \overset{\overline{a},T'}{\longmapsto} Q'$ and $P'\ (\sim_m)_c^\bullet\ Q'$.*

Proof. We proceed by induction on the size of the derivation of $P\ (\sim_m)_c^\bullet\ Q$.

- Assume $P \sim_m^\circ Q$. Since P, Q are closed, we have $P \sim_m Q$. The first condition is true by definition. We now prove the second point. By lemma 29, there exists P'' such that $P \overset{\overline{a},T'}{\longmapsto} P''$ and $P' \sim_m^\bullet P''$. By bisimulation definition, there exists Q' such that $Q \overset{\overline{a},T'}{\longmapsto} Q'$ and $P'' \sim_m Q'$. Let σ be a substitution that closes P''. Since Q' is closed, we have $P''\sigma \sim_m Q'$ by Lemma 26. Consequently we have $P' \sim_m^\bullet \sim_m^\circ Q'$, and since the involved processes are closed, we have $P'\ (\sim_m)_c^\bullet\ Q'$ as required.

- Assume $P \sim_m^\bullet R \sim_m^\circ Q$. Let σ be a substitution that closes R. Since P is closed, we have $P \sim_m^\bullet R\sigma$ by Lemma 27. Since Q is closed, we have $R\sigma \sim_m Q$ by open extension definition. We prove the first point, the proof for the second point is similar. By induction, there exists R' such that $R \overset{\tau}{\longmapsto} R'$ and $P' \sim_m^\bullet R'$.

By bisimulation definition, there exists Q' such that $Q \stackrel{\tau}{\mapsto} Q'$ and $R' \sim_m Q'$. Since R', Q' are closed, we have $R' \sim_m^\circ Q'$, consequently we have $P' \sim_m^\bullet \sim_m^\circ Q'$. The involved processes are closed, hence we have $P' \ (\sim_m)_c^\bullet \ Q'$, as required.

- Assume $P = op(\widetilde{P})$ and $Q = op(\widetilde{Q})$ with $\widetilde{P} \ (\sim_m)_c^\bullet \ \widetilde{Q}$. We prove the first item.
  - $P = P_1 \mid P_2$ with $P_1 \stackrel{\tau}{\mapsto} P_1'$. By induction there exists Q_1' such that $Q_1 \stackrel{\tau}{\mapsto} Q_1'$ and $P_1' \ (\sim_m)_c^\bullet \ Q_1'$. Using rule HO$\pi$-PAR, we have $Q \stackrel{\tau}{\mapsto} Q_1' \mid Q_2$ and since $\sim_m^\bullet$ is a congruence and the involved processes are closed, we have $P_1' \mid P_2 \ (\sim_m)_c^\bullet \ Q_1' \mid Q_2$, as required.
  - Restriction: similar to the case above.
  - Communication: $P = P_1 \mid P_2$ with $P_1 \stackrel{\overline{a},P_2}{\longmapsto} P'$. Since $P_2 \ (\sim_m)_c^\bullet \ Q_2$, by induction (second item) there exists Q' such that $Q_1 \stackrel{\overline{a},Q_2}{\longmapsto} Q'$ and $P' \ (\sim_m)_c^\bullet \ Q'$. By rule HO$\pi$-HO, we have $Q \stackrel{\tau}{\mapsto} Q'$, as required.

  We now prove the second item.

  - $P = \overline{a}\langle P_1 \rangle P_2$ and $Q = \overline{a}\langle Q_1 \rangle Q_2$ with $T \stackrel{a,P_1}{\longmapsto} U$, and $P' = U \mid P_2$. By Lemma 28 there exists U' such that $T' \stackrel{a,Q_1}{\longmapsto} U'$ and $U \ (\sim_m)_c^\bullet \ U'$. By rule HO$\pi$-OUT we have $Q \stackrel{\overline{a},T'}{\longmapsto} U' \mid Q_2 = Q'$. Since $(\sim_{ie})_c^\bullet$ is a congruence and all the involved processes are closed we have $P' \ (\sim_m)_c^\bullet \ Q'$, as required.
  - $P = P_1 \mid P_2$ with $P_1 \stackrel{\overline{a},T}{\longmapsto} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists Q_1' such that $Q_1 \stackrel{\overline{a},T'}{\longmapsto} Q_1'$ and $P' \ (\sim_m)_c^\bullet \ Q_1'$. By rule HO$\pi$-PAR we have $Q \stackrel{\overline{a},T'}{\longmapsto} Q_1' \mid Q_2 = Q'$. Since $\sim_m^\bullet$ is a congruence and all the involved processes are closed we have $P' \ (\sim_m)_c^\bullet \ Q'$, as required.
  - Restriction: similar to the case above.

□

Together Lemmas 30 and 28 show that $(\sim_m)_c^\bullet$ is a strong complementary simulation.

Lemma 31. *Let $(\sim_m^\bullet)^*$ be the reflexive and transitive closure of $\sim_m^\bullet$.*

- *$(\sim_m^\bullet)^*$ is symmetric.*
- *$((\sim_m)_c^\bullet)^*$ is a strong complementary bisimulation.*

Proof. We prove that $(\sim_m^\bullet)^{-1} \subseteq (\sim_m^\bullet)^*$. First, we prove by induction on the derivation of $P(\sim_m^\bullet)^{-1}Q$ that $P(\sim_m^\bullet)^{-1}Q$ implies $P(\sim_m^\bullet)^*Q$.

- If we have $Q \sim_m^\circ P$, then we have $P \sim_m^\circ Q$, i.e. we have $P(\sim_m^\bullet)^*Q$, as required.
- If we have $Q \sim_m^\bullet T \sim_m^\circ P$, by induction we have $T(\sim_m^\bullet)^*Q$. We have $P \sim_m^\circ T$, i.e. we have $P \sim_m^\bullet T$, so by transitivity we have $P(\sim_m^\bullet)^*Q$, as required.

- If we have $Q = Q_1 \mid Q_2$, $P = P_1 \mid P_2$ with $Q_1 \sim_m^\bullet P_1$ and $Q_2 \sim_m^\bullet P_2$. By induction we have $P_1(\sim_m^\bullet)^* Q_1$ and $P_2(\sim_m^\bullet)^* Q_2$. Since $\sim_m^\bullet$ is a congruence, we have $P_1 \mid P_2(\sim_m^\bullet)^* Q_1 \mid P_2$ and $Q_1 \mid P_2(\sim_m^\bullet)^* Q_1 \mid Q_2$, consequently we have $P(\sim_m^\bullet)^* Q$ by transitivity.
- The cases for other operators are similar.

We now prove that $((\sim_m)_c^\bullet)^*$ is a strong complementary bisimulation. Since $(\sim_m^\bullet)^*$ is symmetric, it is enough to prove that $((\sim_m)_c^\bullet)^*$ is a strong complementary simulation. Let $P((\sim_m)_c^\bullet)^* Q$; there exists k such that $P((\sim_m)_c^\bullet)^k Q$. We proceed by induction on k to prove that the conditions of strong complementary simulation hold for any k. The result holds for $k = 0$, suppose it holds for $l \leq k$, we prove for $k+1$. Let $P((\sim_m)_c^\bullet)^k P_k \ (\sim_m)_c^\bullet Q$. If $P \stackrel{\lambda}{\mapsto} P'$, then by induction there exists P'_k such that $P_k \stackrel{\lambda}{\mapsto} P'_k$ and $P'((\sim_m)_c^\bullet)^* P'_k$. Since $(\sim_m)_c^\bullet$ is a strong complementary simulation, there exists Q' such that $Q \stackrel{\lambda}{\mapsto} Q'$ and $P'_k \ (\sim_m)_c^\bullet Q'$. The result then holds by transitivity. □

Theorem 9. *$\sim_m$ is a congruence.*

Proof. We have $\sim_m \subseteq ((\sim_m)_c^\bullet)^* \subseteq \sim_m$, hence $((\sim_m)_c^\bullet)^* = \sim_m$, and $((\sim_m)_c^\bullet)^*$ is a congruence. □

Using the congruence theorem, we can prove the following inclusion between $\sim$ and $\sim_m$:

Lemma 32. *If $P \sim_m Q$ then $P \sim Q$.*

Proof. We prove that $\sim_m$ is a strong early context bisimulation up to $\equiv$.

- If $P \stackrel{\tau}{\rightarrow} P'$, then by Lemma 21 we have $P \stackrel{\tau}{\mapsto} \equiv P'$. By definition there exists Q' such that $Q \stackrel{\tau}{\mapsto} Q'$ and $P' \equiv \sim_m Q'$. By Lemma 21 we have $Q \stackrel{\tau}{\rightarrow} Q'$, hence the result holds.
- Let $P \stackrel{a}{\rightarrow} F$ and $C = \nu\widetilde{b}.\langle R \rangle S$ be a closed concretion. By Lemma 20 we have $P \stackrel{a,R}{\longmapsto} F \circ R$. By definition there exists Q' such that $Q \stackrel{a,R}{\longmapsto} Q'$ and $F \circ R \sim_m Q'$. By Lemma 20 there exists G such that $Q \stackrel{a}{\rightarrow} G$ and $G \circ R = Q'$. Since $\sim_m$ is a congruence, we have $F \bullet C = \nu\widetilde{b}.(F \circ R \mid S) \sim_m \nu\widetilde{b}.(Q' \mid S) = G \bullet C$, hence the result holds.
- Let $P \stackrel{\overline{a}}{\rightarrow} C$ and F be a closed abstraction. By Lemma 21, for some T such that $T \stackrel{a}{\rightarrow} F$, we have $P \stackrel{\overline{a},T}{\longmapsto} \equiv F \bullet C = P'$. By definition there exists Q' such that $Q \stackrel{\overline{a},T}{\longmapsto} Q'$ and $P' \sim_m Q'$. By Lemma 21 there exists C' such that $Q \stackrel{\overline{a}}{\rightarrow} C'$ and $Q' \equiv F \bullet C'$. We have $F \bullet C \equiv \sim_m \equiv F \bullet C'$, as required.

□

B Proofs for HOπP

B.1 Correspondence Lemmas

Lemma 33. *If $P \xrightarrow{a} F$, then for all R we have $P \xmapsto{a,R} F \circ R$. If $P \xmapsto{a,R} P'$, then there exists F such that $P \xrightarrow{a} F$ and $P' = F \circ R$.*

Proof. We proceed by structural induction on P.

- If $P = a(X)P'$, then by rule CONTEXT-ABSTR we have $P \xrightarrow{a} F = (X)P'$, and by rule HO$\pi$P-IN we have $P \xmapsto{a,R} P'\{R/X\} = F \circ R$ for all R, hence the result holds.
- Let $P = P_1 \mid P_2$. Suppose we have $P \xrightarrow{a} F$, which is possible only by rule CONTEXT-PAR (and its symmetric, which is handled similarly). Consequently we have $P_1 \xrightarrow{a} F'$ and $F = F' \mid P_2$. By induction we have $P_1 \xmapsto{a,R} F' \circ R$ for all R, hence by rule HOπP-IN-PAR we have $P \xmapsto{a,R} F' \circ R \mid P_2 = F \circ R$, as required. Suppose we have $P \xmapsto{a,R} P'$, which is possible only by rule HOπP-IN-PAR (and its symmetric, which is handled similarly). Consequently we have $P_1 \xmapsto{a,R} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists F such that $P_1 \xrightarrow{a} F$ and $P_1' = F \circ R$. Consequently by rule CONTEXT-PAR we have $P \xrightarrow{a} F \mid P_2$ with $P' = (F \mid P_2) \circ R$, as required.
- The locality and restriction cases are similar to the parallel case.

□

Lemma 34. *Let P be an HOπP process.*

Suppose $P \xrightarrow{\overline{a}} C$. Let $\widetilde{b} = fn(o(C)) \setminus bn(C)$. For all Q such that $Q \xrightarrow{a} F$ and for all $\mathbb{E}$ such that $bn(\mathbb{E}) \cap \widetilde{b} = \emptyset$, we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$.

If $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, then there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = fn(o(C)) \setminus bn(C)$, and $P' = F \bullet \mathbb{E}\{C\}$.

Proof. We proceed by structural induction induction on P.

- Let $P = \overline{a}\langle P_1\rangle P_2$. We have $P \xrightarrow{\overline{a}} \langle P_1\rangle P_2 = C$. Let Q such that $Q \xrightarrow{a} F$ and $\mathbb{E}$ such that $\text{bn}(\mathbb{E}) \cap \widetilde{b} = \emptyset$. We have $F \bullet \mathbb{E}\{C\} = F \circ P_1 \mid \mathbb{E}\{P_2\}$. By Lemma 33, we have $Q \xmapsto{a,P_1} F \circ P_1$. Let $\widetilde{b} = \text{fn}(P_1)$; by rule HO$\pi$P-OUT, we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$ with $\widetilde{b} = \text{fn}(P_1) = \text{fn}(o(C)) \setminus \text{bn}(C)$ as wished.

  We now prove the reverse implication. We have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} Q' \mid \mathbb{E}\{P_2\}$ with $Q \xmapsto{a,P_1} Q'$ and $\widetilde{b} = \text{fn}(P_1)$. By Lemma 33, there exists F such that $Q \xrightarrow{a} F$ and $Q' = F \circ P_1$. Let $C = \langle P_1\rangle P_2$. We have $P \xrightarrow{\overline{a}} C$, $P' = F \bullet \mathbb{E}\{C\}$ and $\widetilde{b} = \text{fn}(P_1) = \text{fn}(o(C)) \setminus \text{bn}(C)$, as required.

- Let $P = P_1 \mid P_2$. Suppose we have $P \xrightarrow{\overline{a}} C$, which is possible only by rule CONTEXT-PAR. Consequently we have $P_1 \xrightarrow{a} C'$ and $C = C' \mid P_2$. Let $Q \xrightarrow{a} F$ and $\mathbb{E}$ be an evaluation context. By induction we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\Box \mid P_2\}}_{\widetilde{b}} F \bullet \mathbb{E}\{C' \mid P_2\}$ with $\widetilde{b} = \text{fn}(o(C')) \setminus \text{bn}(C')$. By rule HO$\pi$P-OUT-PAR we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$, and we have $\widetilde{b} = \text{fn}(o(C')) \setminus \text{bn}(C') = \text{fn}(o(C)) \setminus \text{bn}(C)$, as required.

  Suppose we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, which is possible only by rule HOπP-OUT-PAR. Consequently we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\Box \mid P_2\}}_{\widetilde{b}} P'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$ and $P' = F \bullet \mathbb{E}\{C \mid P_2\}$. Consequently by rule CONTEXT-PAR we have $P \xrightarrow{\overline{a}} C \mid P_2 = C'$ with $P' = F \bullet \mathbb{E}\{C'\}$ and $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C) = \text{fn}(o(C')) \setminus \text{bn}(C')$, as required.

- The locality case is similar to the parallel one for the evaluation rules (CONTEXT-LOC and HOπP-OUT-LOC), and to the message output one for the passivation rules (CONTEXT-PASSIV and HOπP-OUT-PASSIV).

- Let $P = \nu c.P_1$. Suppose first we have $P \xrightarrow{\overline{a}} C$. By rule CONTEXT-RESTR we have $P_1 \xrightarrow{\overline{a}} C'$ and $C = \nu b.C'$. Let $Q \xrightarrow{a} F$ and $\mathbb{E}$ be an evaluation context. We distinguish two cases:

  - If $c \in \text{fn}(o(C'))$, then we have $F \bullet \mathbb{E}\{\nu c.C'\} = \nu c.(F \bullet \mathbb{E}\{C'\})$. By induction we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P_1'$ with $\widetilde{b} = \text{fn}(o(C')) \setminus \text{bn}(C')$ and $P_1' = F \bullet \mathbb{E}\{C'\}$. Since $c \in \text{fn}(o(C'))$, we have $c \in \widetilde{b}$, so by rule HOπP-OUT-EXTR we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}\setminus\{c\}} \nu c.P_1' = F \bullet \mathbb{E}\{\nu c.C'\}$. We have $\text{fn}(o(C)) \setminus \text{bn}(C) = \text{fn}(o(C')) \setminus (\text{bn}(C') \cup \{c\}) = \widetilde{b} \setminus \{c\}$, hence the result holds.
  - If $c \notin \text{fn}(o(C'))$, then by induction we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu b.\Box\}}_{\widetilde{b}} P_1'$ with $\widetilde{b} = \text{fn}(o(C')) \setminus \text{bn}(C')$ and $P_1' = F \bullet \mathbb{E}\{\nu c.C'\} = F \bullet \mathbb{E}\{C\}$. By rule HO$\pi$P-OUT-RESTR we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$, and we have $\widetilde{b} = \text{fn}(o(C')) \setminus \text{bn}(C') = \text{fn}(o(C)) \setminus \text{bn}(C)$, as required.

  Suppose now that $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$. We have two cases:

  - Rule HOπP-OUT-RESTR: we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}\{\nu c.\Box\}}_{\widetilde{b}} P'$ with $c \notin \widetilde{b}$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$ and $P' = F \bullet \mathbb{E}\{\nu c.C\}$. By rule CONTEXT-RESTR we have $P \xrightarrow{\overline{a}} \nu c.C = C'$, and $\text{fn}(o(C')) \setminus \text{bn}(C') = \text{fn}(o(C)) \setminus (\text{bn}(C)) = \widetilde{b}$ since $c \notin \widetilde{b}$. We have $P' = F \bullet \mathbb{E}\{C'\}$, as required.

– Rule HOπP-OUT-EXTR: we have $P_1 \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}\cup\{c\}} P_1'$ with $P' = \nu c.P_1'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} \cup \{c\} = \text{fn}(o(C)) \setminus \text{bn}(C)$, and $P_1' = F \bullet \mathbb{E}\{C\}$. By rule CONTEXT-RESTR we have $P \xrightarrow{\overline{a}} \nu c.C = C'$. Since $\widetilde{b} \cup \{c\} = \text{fn}(o(C)) \setminus \text{bn}(C)$, we have $c \in \text{fn}(o(C))$, consequently we have $F \bullet \mathbb{E}\{C'\} = \nu c.(F \bullet \mathbb{E}\{C\}) = P'$. We also have $\widetilde{b} = \text{fn}(o(C)) \setminus (\text{bn}(C) \cup \{c\}) = \text{fn}(o(C')) \setminus \text{bn}(C')$, as required.

□

We extend the result to all evaluation contexts.

Lemma 35. *Let $\mathbb{E}$ be an evaluation and $\widetilde{b}$ be a set of names. Suppose bn$(\mathbb{E}) \cap \widetilde{b} = \{a_1 \dots a_n\} \neq \emptyset$. There exists contexts $\mathbb{E}_i$ such that $\mathbb{E} = \mathbb{E}_0\{\nu a_1.\mathbb{E}_1\{\dots \nu a_n.\mathbb{E}_n\}\}$ and for all i, we have bn$(\mathbb{E}_i) \cap \widetilde{b} = \emptyset$.*

Proof. We proceed by structural induction on $\mathbb{E}$.

- There is nothing to prove for $\mathbb{E} = \Box$.
- If $\mathbb{E} = \mathbb{F} \mid P$, then by induction there exists evaluation contexts $\mathbb{F}_i$ such that $\mathbb{F} = \mathbb{F}_0\{\nu a_1.\mathbb{F}_1\{\dots \nu a_n.\mathbb{F}_n\}\}$ and for all i, we have bn$(\mathbb{F}_i) \cap \widetilde{b} = \emptyset$. We have bn$(\mathbb{E}) \cap \widetilde{b} =$ bn$(\mathbb{F}) \cap \widetilde{b}$, $\mathbb{E} = \mathbb{F}_0\{\nu a_1.\mathbb{F}_1\{\dots \nu a_n.\mathbb{F}_n\}\} \mid P$, and bn$(\mathbb{F}_0 \mid P) =$ bn$(\mathbb{F}_0)$, hence the result holds.
- The proof is similar for $\mathbb{E} = a[\mathbb{F}]$.
- If $\mathbb{E} = \nu c.\mathbb{F}$, then there exists contexts $\mathbb{F}_i$ such that $\mathbb{F} = \mathbb{F}_0\{\nu a_1.\mathbb{F}_1\{\dots \nu a_n.\mathbb{F}_n\}\}$ and for all i, we have bn$(\mathbb{F}_i) \cap \widetilde{b} = \emptyset$. We have $\mathbb{E} = \nu c.\mathbb{F}_0\{\nu a_1.\mathbb{F}_1\{\dots \nu a_n.\mathbb{F}_n\}\}$. We distinguish two cases. If $c \notin \widetilde{x}$, then we have bn$(\nu c.\mathbb{F}_0) \cap \widetilde{b} = \emptyset$ and the result holds. Otherwise, we define $\mathbb{E}_0 = \Box$ and $\mathbb{E}_i = \mathbb{F}_{i-1}$ for all $i > 0$. We then have the required result.

□

Lemma 36. *Let P be an HOπP process.*

If $P \xrightarrow{\overline{a}} C$, then for all Q such that $Q \xrightarrow{a} F$ and for all $\mathbb{E}$, we have $P \xmapsto{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$ with $\widetilde{b} =$ fn$(o(C)) \setminus$ bn(C).

If $P \xmapsto{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$, then there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} =$ fn$(o(C)) \setminus$ bn(C), and $P' = F \bullet \mathbb{E}\{C\}$.

Proof. Let $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, and $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$. Let $\mathbb{E}$ be an evaluation context. If bn$(\mathbb{E}) \cap \widetilde{b} = \emptyset$, then by Lemma 34 we have $P \xrightarrow{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$ with $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$. By rule HO$\pi$P-OUT-CAPTURE-FREE we have the required result.

Otherwise, by Lemma 35, there exists $\mathbb{E}_i$ such that $\mathbb{E} = \mathbb{E}_0\{\nu a_1.\mathbb{E}_1\{\dots \nu a_n.\mathbb{E}_n\}\}$ and for all i, we have $\mathrm{bn}(\mathbb{E}_i) \cap \widetilde{b} = \emptyset$. By Lemma 34, we have $P \xrightarrow{\overline{a},Q,\mathbb{E}_0\{\mathbb{E}_1\{\dots\mathbb{E}_n\}\}}_{\widetilde{b}} P'$ with $P' = F \bullet \mathbb{E}_0\{\mathbb{E}_1\{\dots\mathbb{E}\{n\}C\}\}$. Using rule HO$\pi$P-OUT-CAPTURE-FREE once and rule HOπP-OUT-CAPTURE n times, we have $P \xmapsto{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} \nu(a_1 \dots a_n).F \bullet \mathbb{E}_0\{\mathbb{E}_1\{\dots\mathbb{E}\{n\}C\}\} = F \bullet \mathbb{E}\{C\}$, as required.

Let $P \xmapsto{\overline{a},Q,\mathbb{E}}_{\widetilde{b}} P'$. We have two cases. If the transition comes from rule HOπP-OUT-CAPTURE-FREE, we have $\mathrm{bn}(\mathbb{E}) \cap \widetilde{b} = \emptyset$, and we can use Lemma 34. Otherwise, rule HOπP-OUT-CAPTURE has been used and capture occurs in the context $\mathbb{E}$. By Lemma 35, there exists contexts $\mathbb{E}_i$ such that $\mathbb{E} = \mathbb{E}_0\{\nu a_1.\mathbb{E}_1\{\dots \nu a_n.\mathbb{E}_n\}\}$ and for all i, we have $\mathrm{bn}(\mathbb{E}_i) \cap \widetilde{b} = \emptyset$. We have $P \xrightarrow{\overline{a},Q,\mathbb{E}_0\{\mathbb{E}_1\{\dots\mathbb{E}_n\}\}}_{\widetilde{b}} P''$ with $P' = \nu(a_1 \dots a_n).P''$. By Lemma 34 there exists F, C such that $P \xrightarrow{\overline{a}} C$, $Q \xrightarrow{a} F$, $\widetilde{b} = \mathrm{fn}(o(C)) \setminus \mathrm{bn}(C)$, and $P'' = F \bullet \mathbb{E}_0\{\mathbb{E}_1\{\dots\mathbb{E}_n\{C\}\}\}$. We have $F \bullet \mathbb{E}\{C\} = \nu(a_1 \dots a_n).F \bullet \mathbb{E}_0\{\mathbb{E}_1\{\dots\mathbb{E}_n\{C\}\}\} = \nu(a_1 \dots a_n).P'' = P'$, as required.

□

Lemma 37. *Let P be an HOπP process. We have $P \xrightarrow{\tau} P'$ iff $P \xmapsto{\tau} P'$.*

Proof. We proceed by structural induction on P.

Let $P = P_1 \mid P_2$. By case analysis on the rule used to derive $P \xrightarrow{\tau} P'$:

- CONTEXT-PAR: in this case we have $P_1 \xrightarrow{\tau} P_1'$ and $P' = P_1' \mid P_2$. By induction we have $P_1 \xmapsto{\tau} P_1'$, hence by rule HOπP-PAR we have $P \xmapsto{\tau} P'$, as required.
- CONTEXT-HO: in this case, we have $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\overline{a}} C$, and $P' = F \bullet C$. By induction we have $P_2 \xmapsto{\overline{a},P_1,\square}_{\widetilde{b}} F \bullet C$, so by rule HO$\pi$P-HO we have $P \xmapsto{\tau} P'$, as required.

We now prove the reverse implication.

- HOπP-PAR: we have $P_1 \xmapsto{\tau} P_1'$ and $P' = P_1' \mid P_2$. By induction we have $P_1 \xrightarrow{\tau} P_1'$, hence we have $P \xrightarrow{\tau} P_1' \mid P_2$ by rule CONTEXT-PAR.
- HOπP-HO: we have $P_1 \xmapsto{\overline{a},P_2,\square}_{\widetilde{b}} P'$. By induction there exists F, C such that $P_1 \xrightarrow{\overline{a}} C$, $P_2 \xrightarrow{a} F$ and $P' = F \bullet C$. By rule CONTEXT-HO, we have $P \xrightarrow{\tau} P'$, as required.

The locality and restriction cases are easy. □

Lemma 38. *Let P be an HOπP process.*

- *We have $P \stackrel{\tau}{\Rightarrow} P'$ iff $P \stackrel{\tau}{\mapsto\!\!\!\Rightarrow} P'$.*
- *Let R be a closed process. If $P \stackrel{a}{\Rightarrow} F$ and $F \circ R \stackrel{\tau}{\Rightarrow} P'$ then we have $P \stackrel{a,R}{\Longmapsto} F \circ R$. If $P \stackrel{a,R}{\Longmapsto} P'$, then there exists F such that $P \stackrel{a}{\Rightarrow} F$ and $F \circ R \stackrel{\tau}{\Rightarrow} P'$.*

- *If* $P \stackrel{\overline{a}}{\Rightarrow} C$*, then for all* $Q, \mathbb{E}$ *such that* $Q \stackrel{a}{\Rightarrow} F$ *and* $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$*, we have* $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$ *with* $\widetilde{b} = fn(o(C)) \setminus bn(C)$*. If* $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$*, then there exists* F, C *such that* $P \stackrel{\overline{a}}{\Rightarrow} C$*,* $Q \stackrel{a}{\Rightarrow} F$*,* $\widetilde{b} = fn(o(C)) \setminus bn(C)$*, and* $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$*.*

Proof. By Lemma 37 we have $\stackrel{\tau}{\longrightarrow}=\stackrel{\tau}{\longmapsto}$, so we have $\stackrel{\tau}{\Rightarrow}=\stackrel{\tau}{\Mapsto}$.

If $P \stackrel{\tau}{\Rightarrow} P'' \stackrel{a}{\longrightarrow} F$ and $F \circ R \stackrel{\tau}{\Rightarrow} P'$, then we have $P \stackrel{\tau}{\Mapsto} P''$ and $F \circ R \stackrel{\tau}{\Mapsto} P'$ by the first result. By Lemma 33 we have $P'' \stackrel{a,R}{\longmapsto} F \circ R$, consequently we have $P \stackrel{a,R}{\Longmapsto} P'$. If $P \stackrel{\tau}{\Mapsto} P_1 \stackrel{a,R}{\longmapsto} P_2 \stackrel{\tau}{\Mapsto} P'$, then we have $P \stackrel{\tau}{\Rightarrow} P_1$ and $P_2 \stackrel{\tau}{\Rightarrow} P'$. By Lemma 33 there exists F such that $P_1 \stackrel{a}{\longrightarrow} F$ and $F \circ R = P_2$. Consequently we have $P \stackrel{a}{\Rightarrow} F$ and $F \circ R \stackrel{\tau}{\Rightarrow} P'$ as wished.

Let $P \stackrel{\tau}{\Rightarrow} P'' \stackrel{\overline{a}}{\longrightarrow} C$, $Q \stackrel{\tau}{\Rightarrow} Q'' \stackrel{a}{\longrightarrow} F$, and $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$. We have $P \stackrel{\tau}{\Mapsto} P''$, $Q \stackrel{\tau}{\Mapsto} Q''$ and $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Mapsto} P'$ by the first result. By Lemma 36 we have $P'' \stackrel{\overline{a},Q'',\mathbb{E}}{\longmapsto}_{\widetilde{b}} F \bullet \mathbb{E}\{C\}$ with $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$, so we have $P \stackrel{\overline{a},Q'',\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$. Consequently we have $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$, as required. If $P \stackrel{\overline{a},Q,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} P'$, then we have $P \stackrel{\tau}{\Mapsto} P_1 \stackrel{\overline{a},Q',\mathbb{E}}{\longmapsto}_{\widetilde{b}} P_2 \stackrel{\tau}{\Mapsto} P'$ with $Q \stackrel{\tau}{\Mapsto} Q'$. We have $P \stackrel{\tau}{\Rightarrow} P_1$, $P_2 \stackrel{\tau}{\Rightarrow} P'$, and $Q \stackrel{\tau}{\Rightarrow} Q'$ by the first result. By Lemma 36 there exists F, C such that $P_1 \stackrel{\overline{a}}{\longrightarrow} C$, $Q' \stackrel{a}{\longrightarrow} F$, $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$, and $P_2 = F \bullet \mathbb{E}\{C\}$. Consequently we have $P \stackrel{\overline{a}}{\Rightarrow} C$, $Q \stackrel{a}{\Rightarrow} F$, and $F \bullet \mathbb{E}\{C\} \stackrel{\tau}{\Rightarrow} P'$, as required. □

We now prove the correspondence between $\approx$ and $\approx_m$. The correspondence proof for $\sim$ and $\sim_m$ is similar.

Lemma 39. *If* $P \stackrel{\overline{a}}{\longrightarrow} C$ *then we have* $fn(C) \subseteq fn(P)$*.*

Proof. By induction on $P \stackrel{\overline{a}}{\longrightarrow} C$. □

Lemma 40. *Let* $P \approx Q$*. Let* $P \stackrel{\overline{a}}{\longrightarrow} C$*,* F *an abstraction, and* $Q \stackrel{\overline{a}}{\Rightarrow} C'$ *such that for all* $\mathbb{E}$*, there exists* Q' *such that* $F \bullet \mathbb{E}\{C'\} \stackrel{\tau}{\Rightarrow} Q'$ *and* $F \bullet \mathbb{E}\{C\} \approx Q'$*. Then we have* $fn(o(C)) \setminus bn(C) = fn(o(C')) \setminus bn(C')$*.*

Proof. Let $P \approx Q$ such that $P \stackrel{\overline{a}}{\longrightarrow} C$. Let F be an abstraction. By bisimilarity definition, there exists C' such that $Q \stackrel{\overline{a}}{\Rightarrow} C'$ and for all $\mathbb{E}$, we have $F \bullet \mathbb{E}\{C\} \approx F \bullet \mathbb{E}\{C'\}$. Let $\{x_i\} = \text{fn}(o(C)) \setminus \text{bn}(C)$ and $y_i = \text{fn}(o(C')) \setminus \text{bn}(C')$. Given two sets $\widetilde{z_i}, \widetilde{d_i}$ of pairwise distinct names with the same number of element, we define $\mathbb{E}_{\widetilde{z_i},\widetilde{d_i}}$ as

$$\mathbb{E}_{\widetilde{z_i},\widetilde{d_i}} = \nu b.(b[\nu \widetilde{z_i}.(\Box \mid (z_i.\mathbf{0} \mid \overline{z_i}.\overline{z_i}.d_i.\mathbf{0})^i] \mid b(X)(X \mid X))$$

A name d_{i_0} becomes observable after passivation and duplication of hidden locality b iff two communications on the corresponding name z_{i_0} happen, which is possible iff z_{i_0} is extruded outside b.

Let $\widetilde{d_i}$ be a set of names with the same number of elements than $\widetilde{x_i}$, pairwise distinct, and which do not appear in P, Q, F. We have $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C\} \approx F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C'\}$. By definitions of $\widetilde{x_i}$, all the names $\widetilde{x_i}$ are extruded in $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C\}$, hence we have

$F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C\} \stackrel{\tau}{\Rightarrow}\stackrel{d_i}{\longrightarrow}$ for all i. To match these transitions, the names $\widetilde{x_i}$ has to be extruded in $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C'\}$. However a name x is extruded in $F \bullet \mathbb{E}_{\widetilde{x_i},\widetilde{d_i}}\{C'\}$ iff we have $x \in \widetilde{y_i}$, consequently we have $\widetilde{x_i} \subseteq \widetilde{y_i}$.

With the same reasoning on $F \bullet \mathbb{E}_{\widetilde{y_i},\widetilde{e_i}}\{C\} \approx F \bullet \mathbb{E}_{\widetilde{y_i},\widetilde{e_i}}\{C'\}$ (for some names $\widetilde{e_i}$) and using transitions from $F \bullet \mathbb{E}_{\widetilde{y_i},\widetilde{e_i}}\{C'\}$, we have $\widetilde{y_i} \subseteq \widetilde{x_i}$. Consequently we have $\widetilde{y_i} = \widetilde{x_i}$, i.e. $\text{fn}(o(C)) \setminus \text{bn}(C) = \text{fn}(o(C')) \setminus \text{bn}(C')$ as wished.

□

Lemma 41. *If $P \approx Q$ then $P \approx_m Q$.*

Proof. We prove that $\approx$ is a weak complementary bisimulation. Let $P \approx Q$. We have $\text{fn}(P) = \text{fn}(Q)$ by definition.

- If $P \stackrel{\tau}{\longmapsto} P'$ then by Lemma 37 we have $P \stackrel{\tau}{\longrightarrow} P'$. By definition there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \approx Q'$. By Lemma 38 we have $Q \stackrel{\tau}{\Mapsto} Q'$, and we have $P' \approx Q'$ as wished.

- If $P \stackrel{a,R}{\longmapsto} P'$, then by Lemma 33 there exists F such that $P \stackrel{a}{\longrightarrow} F$ and $P' = F \circ R$. By definition there exists G, Q' such that $Q \stackrel{a}{\Rightarrow} G$, $G \bullet \langle R \rangle \mathbf{0} \stackrel{\tau}{\Rightarrow} Q'$ and $Q' \approx F \bullet \langle R \rangle \mathbf{0}$. We have $G \bullet \langle R \rangle \mathbf{0} \equiv G \circ R$ so by Lemma 38 we have $Q \stackrel{a,R}{\Longmapsto} Q' \approx F \bullet \langle R \rangle \mathbf{0} \equiv P'$ as wished.

- If $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$, then by Lemma 36 there exists F, C such that $T \stackrel{a}{\longrightarrow} F$, $P \stackrel{\overline{a}}{\longrightarrow} C$, $\widetilde{b} = \text{fn}(o(C)) \setminus \text{bn}(C)$ and $P' = F \bullet \mathbb{E}\{C\}$. By definition there exists D, Q' such that $Q \stackrel{\overline{a}}{\Rightarrow} D$, $F \bullet \mathbb{E}\{D\} \stackrel{\tau}{\Rightarrow} Q'$ and $F \bullet \mathbb{E}\{C\} \approx Q'$. By Lemma 40 we have $\text{fn}(o(D)) \setminus \text{bn}(D) = \text{fn}(o(C)) \setminus \text{bn}(C) = \widetilde{b}$. By Lemma 38 we have $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'$, and we have $P' \approx Q'$ as required.

□

The reverse inclusion requires the congruence of $\approx_m$, and is proved in the next section.

B.2 Congruence Proof

In this part, we extend bisimilarity $\approx_m$ to capture-free transition $P \stackrel{\overline{a},T,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'$ in the following way:

- If $P \stackrel{\overline{a},T,\mathbb{E}}{\longrightarrow}_{\widetilde{b}} P'$, then there exists T', Q' such that $T \stackrel{\tau}{\Mapsto} T'$, $Q \stackrel{\tau}{\Mapsto} \stackrel{\overline{a},T',\mathbb{E}}{\longrightarrow}_{\widetilde{b}} \stackrel{\tau}{\Mapsto} Q'$, and $P' \approx_m Q'$.

We first prove a result we extensively use in the following. We write $\stackrel{\lambda}{\longmapsto}$ for $\stackrel{\tau}{\longmapsto} \cup \stackrel{a,R}{\longmapsto} \cup \stackrel{\overline{a},Q,\mathbb{E}}{\longmapsto}_{\widetilde{b}} \cup \stackrel{\overline{a},Q,\mathbb{E}}{\longrightarrow}_{\widetilde{b}}$ and $\stackrel{\lambda}{\Mapsto}$ for the weak counterpart.

Lemma 42. *If $P \approx Q$ and $P \stackrel{\lambda}{\Mapsto} P'$ then there exists Q' such that $Q \stackrel{\lambda}{\Mapsto} Q'$ and $P' \approx Q'$.*

Proof. If $P \stackrel{\tau}{\Mapsto} P'$, we proceed by induction on the number of τ-steps. For 0 step, the result holds (chose $Q' = Q$). Suppose the result holds for n. If $P(\stackrel{\tau}{\longmapsto})^n P_n \stackrel{\tau}{\longmapsto} P'$, then by induction there exists Q'_n such that $Q \stackrel{\tau}{\Mapsto} Q'_n$ and $P'_n \approx Q'_n$. By bisimulation definition, there exists Q' such that $Q'_n \stackrel{\tau}{\Mapsto} Q'$ and $P' \approx Q'$. Since we have $Q \stackrel{\tau}{\Mapsto} Q'$, we have the required result.

If $P \stackrel{\tau}{\Mapsto} P_1 \stackrel{a,R}{\longmapsto} P_2 \stackrel{\tau}{\Mapsto} P'$, then by the first result there exists Q'_1 such that $Q \stackrel{\tau}{\Mapsto} Q'_1$ and $P_1 \approx Q'_1$. By bisimulation definition there exists Q'_2 such that $P \stackrel{a,R}{\Longmapsto} Q'_2$ and $P_2 \approx Q'_2$. By the first result there exists $Q'_2 \stackrel{\tau}{\Mapsto} Q'$ and $P' \approx Q'$. We have $Q \stackrel{a,R}{\Longmapsto} Q'$ hence the result holds.

If $P \stackrel{\tau}{\Mapsto} P_1 \stackrel{\overline{a},T',\mathbb{E}}{\longmapsto}_{\widetilde{b}} P_2 \stackrel{\tau}{\Mapsto} P'$ with $T \stackrel{\tau}{\Mapsto} T'$, then by the first result there exists Q'_1 such that $Q \stackrel{\tau}{\Mapsto} Q'_1$ and $P_1 \approx Q'_1$. By bisimulation definition there exists Q'_2 such that $Q'_1 \stackrel{\overline{a},T',\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'_2$ and $P_2 \approx Q'_2$. By the first result there exists Q' such that $Q'_2 \stackrel{\tau}{\Mapsto} Q'$ and $P' \approx Q'$. We have $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto}_{\widetilde{x}} Q'$ as wished. The proof is similar for $P \stackrel{\tau}{\Mapsto} \stackrel{\overline{a},T',\mathbb{E}}{\longmapsto}_{\widetilde{b}} \stackrel{\tau}{\Mapsto} P'$ with $T \stackrel{\tau}{\Mapsto} T'$.

□

We recall the definitions of open extension and Howe's closure of weak bisimilarity $\approx_m$.

Definition 20. *Let P and Q be two open processes. We have $P \approx_m^\circ Q$ iff $P\sigma \approx_m Q\sigma$ for all substitutions that close P and Q.*

Definition 21. *The Howe's closure $\approx_m^\bullet$ is the smallest relation verifying:*

- $\approx_m^\circ \subseteq \approx_m^\bullet$.
- $\approx_m^\bullet \approx_m^\circ \subseteq \approx_m^\bullet$.
- *For all operators op of the language, if $\widetilde{P} \approx_m^\bullet \widetilde{Q}$, then $op(\widetilde{P}) \approx_m^\bullet op(\widetilde{Q})$.*

Lemma 43. *$\approx_m^\bullet$ is reflexive.*

Proof. Because $\approx_m$ is reflexive. □

Lemma 44. *If $P \approx_m^\bullet Q$, then fn$(P) =$ fn(Q).*

Proof. By induction on the derivation of $P \approx_m^\bullet Q$.

- If $P \approx_m Q$, then we have $\text{fn}(P) = \text{fn}(Q)$ by definition.
- If $P \approx_m^\bullet T \approx_m Q$, then we have $\text{fn}(P) = \text{fn}(T)$ by induction, and $\text{fn}(T) = \text{fn}(Q)$ by bisimulation definition. Consequently we have $\text{fn}(P) = \text{fn}(Q)$.
- If $\widetilde{P} \approx_m^\bullet \widetilde{Q}$, we have $\text{fn}(P_i) = \text{fn}(Q_i)$ for each item on the list by induction, hence using definition of free names we have $\text{fn}(op(\widetilde{P})) = \text{fn}(op(\widetilde{Q}))$.

□

Lemma 45. *If $R \approx^{\bullet}_m R'$, then $P\{R/X\} \approx^{\bullet}_m P\{R'/X\}$.*

If $P \stackrel{a,R}{\longmapsto} P'$ and $R \approx^{\bullet}_m R'$, then there exists P'' such that $P \stackrel{a,R'}{\longmapsto} P''$ and $P' \approx^{\bullet}_m P''$.

Proof. The first item is done by structural induction on P:

- $P = \mathbf{0}$: the result holds.
- $P = X$: $P\{R/X\} = R \approx^{\bullet}_m R' = P\{R'/X\}$, hence the result holds.
- $P = Y \neq X$: the result holds.
- $P = P_1 \mid P_2$: by induction we have $P_1\{R/X\} \approx^{\bullet}_m P_1\{R'/X\}$ and $P_2\{R/X\} \approx^{\bullet}_m P_2\{R'/X\}$. Since $\approx^{\bullet}_m$ is a congruence we have $P\{R/X\} = P_1\{R/X\} \mid P_2\{R/X\} \approx^{\bullet}_m P_1\{R'/X\} \mid P_2\{R'/X\} = P\{R'/X\}$, as required.
- $P = a[P_1]$: similar to the case above.
- $P = \overline{a}\langle P_1\rangle P_2$: similar to the case above.
- $P = a(Y)P_1$: similar to the case above.
- $P = \nu a.P_1$. By induction we have $P_1\{R/X\} \approx^{\bullet}_m P_1\{R'/X\}$. Since $\approx^{\bullet}_m$ is a congruence, we have $P\{R/X\} = \nu a.(P_1\{R/X\}) \approx^{\bullet}_m \nu a.(P_1\{R'/X\}) = P\{R'/X\}$, as required.

The second item is proved by induction on the derivation of $P \stackrel{a,R}{\longmapsto} P'$:

- Rule HOπP-IN: we have $P = a(X)P_1 \stackrel{a,R}{\longmapsto} P_1\{R/X\}$. Using first item we have $P_1\{R/X\} \approx^{\bullet}_m P_1\{R'/X\}$, and by rule HO$\pi$P-IN we have $P \stackrel{a,R'}{\longmapsto} P_1\{R'/X\}$, as required.
- Rule HOπP-IN-PAR: we have $P = P_1 \mid P_2$ with $P_1 \stackrel{a,R}{\longmapsto} P_1'$ and $P' = P_1' \mid P_2$. By induction there exists P_1'' such that $P_1 \stackrel{a,R'}{\longmapsto} P_1''$ and $P_1' \approx^{\bullet}_m P_1''$. By rule HO$\pi$P-IN-PAR, we have $P \stackrel{a,R'}{\longmapsto} P_1'' \mid P_2 = P''$, and since $\approx^{\bullet}_m$ is a congruence, we have $P' \approx^{\bullet}_m P''$, as required.
- Rule HOπP-IN-LOC: similar to the case above.
- Rule HOπP-IN-RESTR: we have $P = \nu b.P_1$ with $P_1 \stackrel{a,R}{\longmapsto} P_1'$, $b \neq a$, and $P' = \nu b.P_1'$. By induction there exists P_1'' such that $P_1 \stackrel{a,R'}{\longmapsto} P_1''$ and $P_1' \approx^{\bullet}_m P_1''$. By rule HO$\pi$P-IN-RESTR we have $P \stackrel{a,R}{\longmapsto} \nu b.P_1'' = P''$, and since $\approx^{\bullet}_m$ is a congruence we have $P' \approx^{\bullet}_m P''$, as required.

□

Lemma 46. *For all $P \approx^{\bullet}_m Q$ and all $R \approx^{\bullet}_m R'$, we have $P\{R/X\} \approx^{\bullet}_m Q\{R'/X\}$.*

Proof. By induction on the derivation of $P \approx^{\bullet}_m Q$.

- $P \approx_m^\circ Q$: by Lemma 45, we have $P\{R/X\} \approx_m^\bullet P\{R'/X\}$. Let σ be a substitution which closes P and Q except for X. By open extension definition we have $P\{R'/X\}\sigma \approx_m Q\{R'/X\}\sigma$, i.e. we have $P\{R'/X\} \approx_m^\circ Q\{R'/X\}$. Hence we have $P\{R/X\} \approx_m^\bullet \approx_m^\circ Q\{R'/X\}$, i.e. $P\{R/X\} \approx_m^\bullet Q\{R'/X\}$, as required.

- $P \approx_m^\bullet T \approx_m^\circ Q$: by induction we have $P\{R/X\} \approx_m^\bullet T\{R'/X\}$, and using the same technique as in the first case we have $T\{R'/X\} \approx_m^\circ Q\{R'/X\}$, hence we have $P\{R/X\} \approx_m^\bullet Q\{R'/X\}$, as required.

- $op(\widetilde{P'}) \approx_m^\bullet op(\widetilde{Q'})$ with $\widetilde{P'} \approx_m^\bullet \widetilde{Q'}$. By induction we have $\widetilde{P'\{R/X\}} \approx_m^\bullet \widetilde{Q'\{R'/X\}}$, hence we have $op(\widetilde{P'\{R/X\}}) \approx_m^\bullet op(\widetilde{Q'\{R'/X\}})$ since $\approx_m^\bullet$ is congruence. Consequently we have $P\{R/X\} \approx_m^\bullet Q\{R'/X\}$, as required.

□

We write $(\approx_m)_c^\bullet$ the restriction of $\approx_m^\bullet$ to closed processes.

Lemma 47. *Let $P \sim_m^\bullet Q$. For every substitution σ, we have $P\sigma \sim_m^\bullet Q\sigma$ using a derivation of the same size.*

Proof. By induction on $P \sim_m^\bullet Q$. Most cases are immediate by induction. The base case is $P \sim_m^\circ Q$. We show that $P\sigma \sim_m^\circ Q\sigma$. Let σ' a substitution that closes $P\sigma$ and $Q\sigma$, then $\sigma\sigma'$ closes P and Q, thus $P\sigma\sigma' \sim_m Q\sigma\sigma'$. □

Lemma 48. *Let $P\ (\approx_m)_c^\bullet\ Q$. If $P \overset{a,R}{\longmapsto} P'$, then for all R' such that $R\ (\approx_m)_c^\bullet\ R'$, there exists Q' such that $Q \overset{a,R}{\Longmapsto} Q'$ and $P'\ (\approx_m)_c^\bullet\ Q'$.*

Proof. By induction on the size of the derivation of $P\ (\approx_m)_c^\bullet\ Q$.

- $P \approx_m^\circ Q$. Since P, R are closed, P' is closed. By Lemma 45 there exists P'' such that $P \overset{a,R'}{\longmapsto} P''$ and $P' \approx_m^\bullet P''$. Since P, Q are closed, we have $P \approx_m Q$; by bisimulation definition there exists Q' such that $Q \overset{a,R'}{\Longmapsto} Q'$ and $P'' \approx_m Q'$. Let σ be a substitution that closes P''. Since Q, R' are closed, Q' is closed and we have $P''\sigma \approx_m Q'$ by Lemma 46. Consequently, we have $P' \approx_m^\bullet \approx_m^\circ Q'$, and since P', Q' are closed, we have $P'\ (\approx_m)_c^\bullet\ Q'$, as required.

- $P \approx_m^\bullet T \approx_m^\circ Q$. Let σ be a substitution that closes T; since P is closed and by lemma 47, we have $P \approx_m^\bullet T\sigma$. By induction there exists T' such that $T\sigma \overset{a,R'}{\Longmapsto} T'$ and $P'\ (\approx_m)_c^\bullet\ T'$. By open extension definition and since Q is closed, we have $T\sigma \approx_m Q$. By Lemma 42 there exists Q' such that $Q \overset{a,R'}{\Longmapsto} Q'$ and $T' \approx_m^\bullet Q'$. Consequently we have $P' \approx_m^\bullet \approx_m^\circ Q'$, and since P, Q, R, R' are closed, P', Q' are closed too. Finally we have $P'\ (\approx_m)_c^\bullet\ Q'$ as required.

- $op(\widetilde{P}) \approx_m^\bullet op(\widetilde{Q})$ with $\widetilde{P} \approx_m^\bullet \widetilde{Q}$. By case analysis on op.

– $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$ with $P_1 \overset{a,R}{\longmapsto} P_1'$. By induction there exists Q_1' such that $Q_1 \overset{a,R'}{\Longmapsto} Q_1'$ and $P_1' \approx_m^\bullet Q_1'$. Using rules HO$\pi$P-PAR for τ-actions and HOπP-IN-PAR for the observable action, we have $Q \overset{a,R'}{\Longmapsto} Q_1' \mid Q_2$. Since $\approx_m^\bullet$ is a congruence, we have $P_1' \mid P_2 \approx_m^\bullet Q_1' \mid Q_2$. Since P, Q, R, R' are closed, all the involved processes are closed and we have $P_1' \mid P_2 \ (\approx_m)_c^\bullet \ Q_1' \mid Q_2$, as required.

– Locality: similar to the case above.

– $P = a(X)P_1$, $Q = a(X)Q_1$ with $P \overset{a,R}{\longmapsto} P_1\{R/X\}$. By Lemma 46, we have $P_1\{R/X\} \approx_m^\bullet Q_1\{R'/X\}$. Using rule HO$\pi$P-IN, we have $Q \overset{a,R'}{\longmapsto} Q_1\{R'/X\}$. Since the involved processes are closed, we have $P_1\{R/X\} \ (\approx_m)_c^\bullet \ Q_1\{R/X\}$ as required.

– $P = \nu b.P_1$ and $Q = \nu b.Q_1$. Similar to the parallel case.

□

We inductively define $\mathbb{E} \approx_m^\bullet \mathbb{F}$ as:

- $\Box \approx_m^\bullet \Box$
- If $\mathbb{E} \approx_m^\bullet \mathbb{F}$ and $P \approx_m^\bullet Q$ then $\mathbb{E} \mid P \approx_m^\bullet \mathbb{F} \mid Q$.
- If $\mathbb{E} \approx_m^\bullet \mathbb{F}$ then $\nu a.\mathbb{E} \approx_m^\bullet \nu a.\mathbb{F}$.
- If $\mathbb{E} \approx_m^\bullet \mathbb{F}$ then $a[\mathbb{E}] \approx_m^\bullet a[\mathbb{F}]$.

Lemma 49. *If* $\mathbb{E} \approx_m^\bullet \mathbb{F}$, $P \approx_m^\bullet Q$, *and* $\mathbb{E}' \approx_m^\bullet \mathbb{F}'$ *then* $\mathbb{E}\{P\} \approx_m^\bullet \mathbb{F}\{Q\}$ *and* $\mathbb{E}\{\mathbb{E}'\} \approx_m^\bullet \mathbb{F}\{\mathbb{F}'\}$.

Proof. By induction on $\mathbb{E} \approx_m^\bullet \mathbb{F}$.

- $\Box \approx_m^\bullet \Box$: the result holds.
- $\mathbb{E}_1 \mid P_1 \approx_m^\bullet \mathbb{F}_1 \mid Q_1$ by induction we have $\mathbb{E}_1\{P\} \approx_m^\bullet \mathbb{F}_1\{Q\}$ and $\mathbb{E}_1\{\mathbb{E}'\} \approx_m^\bullet \mathbb{F}_1\{\mathbb{F}'\}$. By congruence we have $\mathbb{E}_1\{P\} \mid P_1 \approx_m^\bullet \mathbb{F}_1\{Q\} \mid Q_1$ and $\mathbb{E}_1\{\mathbb{E}'\} \mid P_1 \approx_m^\bullet \mathbb{F}_1\{\mathbb{F}'\} \mid Q_1$, hence the result holds.
- Restriction, locality: similar to the parallel case.

□

We define $\text{fn}(\mathbb{E}) = \text{fn}(\mathbb{E}\{\mathbf{0}\})$.

Lemma 50. *If* $\mathbb{E} \approx_m^\bullet \mathbb{F}$ *then* $fn(\mathbb{E}) = fn(\mathbb{F})$.

Proof. By induction on the derivation of $\mathbb{E} \approx_m^\bullet \mathbb{F}$. □

Corollary 1. *Let* $\mathbb{E} \approx_m^\bullet \mathbb{F}$ *and* $P \approx_m^\bullet Q$. *We have* $\mathbb{E}\{\Box \mid P\} \approx_m^\bullet \mathbb{F}\{\Box \mid Q\}$, $\mathbb{E}\{\nu a.\Box\} \approx_m^\bullet \mathbb{F}\{\nu a.\Box\}$, *and* $\mathbb{E}\{a[\Box]\} \approx_m^\bullet \mathbb{F}\{a[\Box]\}$.

Lemma 51. *If $\mathbb{E} \approx_m^\bullet \mathbb{F}$ and $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, then there exists $\mathbb{F}_1, \mathbb{F}_2$ such that $\mathbb{E}_1 \approx_m^\bullet \mathbb{F}_1$, $\mathbb{E}_2 \approx_m^\bullet \mathbb{F}_2$, and $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$.*

Proof. By induction on $\mathbb{E} \approx_m^\bullet \mathbb{F}$

- $\mathbb{E} = \mathbb{E}' \mid P$, $\mathbb{F} = \mathbb{F}' \mid Q$ with $\mathbb{E}' \approx_m^\bullet \mathbb{F}'$ and $P \approx_m^\bullet Q$. There exists $\mathbb{E}'_1$ such that $\mathbb{E}' = \mathbb{E}'_1\{\nu c.\mathbb{E}_2\}$ and $\mathbb{E}_1 = \mathbb{E}'_1 \mid P$. By induction there exists $\mathbb{F}'_1$, $\mathbb{F}'_2$ such that $\mathbb{F}' = \mathbb{F}'_1\{\nu c.\mathbb{F}'_2\}$, $\mathbb{F}'_1 \approx_m^\bullet \mathbb{E}'_1$, and $\mathbb{F}'_2 \approx_m^\bullet \mathbb{E}_2$. We have $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}'_2\} \mid Q$ with $\mathbb{F}'_1 \mid Q \approx_m^\bullet \mathbb{E}'_1 \mid P$ by congruence, hence the result holds.
- $\mathbb{E} = \nu a.\mathbb{E}'$, $\mathbb{F} = \nu a.\mathbb{F}'$ with $\mathbb{E}' \approx_m^\bullet \mathbb{F}'$. If $c = a$, then we have $\mathbb{E}_1 = \Box$ and $\mathbb{E}_2 = \mathbb{E}'$. We define $\mathbb{F}_1 = \Box$ and $\mathbb{F}_2 = \mathbb{F}'$. We have the required result. If $c \neq a$, we use the same scheme as in the parallel case.
- Locality: similar to the parallel case.

□

Lemma 52. *Let $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T \approx_m^\bullet T'$, and $\mathbb{E} \approx_m^\bullet \mathbb{F}$, then there exists T'', P'' such that $T' \stackrel{\tau}{\Rightarrow} T''$, $P \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''$ and $P' \approx_m^\bullet P''$.*

Let $P \xmapsto{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T \approx_m^\bullet T'$, and $\mathbb{E} \approx_m^\bullet \mathbb{F}$, then there exists P'' such that $P \stackrel{\overline{a},T',\mathbb{F}}{\Longmapsto}_{\widetilde{b}} P''$ and $P' \approx_m^\bullet P''$.

Proof. By induction on the derivation of $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$.

- $P = \overline{a}\langle R\rangle S$ with $\mathrm{fn}(R) = \widetilde{b}$, $T \xmapsto{a,R} T_0$ and $P' = T_0 \mid \mathbb{E}\{S\}$. By Lemma 48 there exists T'' such that $T' \stackrel{a,R}{\Longmapsto} T''$ and $T_0 \approx_m^\bullet T''$. There exists T_1, T_2 such that $T_0 \stackrel{\tau}{\Rightarrow} T_1 \xmapsto{a,R} T_2 \stackrel{\tau}{\Rightarrow} T''$. By rule HO$\pi$P-OUT, we have $P \xrightarrow{\overline{a},T_1,\mathbb{F}}_{\widetilde{b}} T_2 \mid \mathbb{F}\{S\}$. With $T_2 \stackrel{\tau}{\Rightarrow} T''$, we have $T_2 \mid \mathbb{F}\{S\} \stackrel{\tau}{\Rightarrow} T'' \mid \mathbb{F}\{S\}$ by rule HOπP-PAR, so finally we have $P \xmapsto{\overline{a},T_1,\mathbb{F}}_{\widetilde{b}} T'' \mid \mathbb{F}\{S\} = P''$ with $T' \stackrel{\tau}{\Rightarrow} T_1$. Since $\approx_m^\bullet$ is a congruence, we have $P' \approx_m^\bullet P''$, as required.
- $P = b[P_1]$ and passivation occurs: similar to the case above.
- $P = b[P_1]$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}\{b[\Box]\}}_{\widetilde{b}} P'_1$. By induction there exists T'', P''_1 such that $P_1 \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}\{b[\Box]\}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''_1$ with $T' \stackrel{\tau}{\Rightarrow} T''$, and $P'_1 \approx_m^\bullet P''_1$. By rules HO$\pi$P-LOC and HO$\pi$P-OUT-LOC, we have $P \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''_1$ with $P'_1 \approx_m^\bullet P''_1$ as wished.
- Parallel: similar to the case above.
- $P = \nu c.P_1$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}\{\nu y.\Box\}}_{\widetilde{b}} P'_1$, $y \notin \widetilde{b}$. Similar to the case above.
- $P = \nu c.P_1$ with $P_1 \xrightarrow{\overline{a},T,\mathbb{E}}_{c\cup\widetilde{b}} P'_1$. By induction there exists T'', P''_1 such that $P_1 \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{c\cup\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''_1$, $T' \stackrel{\tau}{\Rightarrow} T''$, and $P'_1 \approx_m^\bullet P''_1$. Using HO$\pi$P-RESTR for

silent actions and HOπP-OUT-EXTR, we have $P \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} \nu c.P_1''$. Since $\approx_m^\bullet$ is a congruence, we have $\nu c.P_1' \approx_m^\bullet \nu c.P_1''$, as required.

We now prove the second item by induction on $P \xmapsto{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$.

- If $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, then by the first item, there exists T'', P'' such that $T' \stackrel{\tau}{\Rightarrow} T''$, $P \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''$ and $P' \approx_m^\bullet P''$. Using rule HOπP-OUT-CAPTURE-FREE we have $P \stackrel{\tau}{\Rightarrow} \xmapsto{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} P''$, hence we have $P \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} P''$, as wished.

- If $P \xmapsto{\overline{a},T,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}} P'$ and $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, then by Lemma 51, there exists $\mathbb{F}_1, \mathbb{F}_2$ such that $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$, $\mathbb{F}_1 \approx_m^\bullet \mathbb{E}_1$, $\mathbb{F}_2 \approx_m^\bullet \mathbb{E}_2$. By Lemma 49, we have $\mathbb{E}_1\{\mathbb{E}_2\} \approx_m^\bullet \mathbb{F}_1\{\mathbb{F}_2\}$, so by induction there exists P'' such that $P \xRightarrow{\overline{a},T',\mathbb{F}_1\{\mathbb{F}_2\}}_{\widetilde{b}} P''$ and $' \approx_m^\bullet P''$. Using rule HOπP-OUT-CAPTURE, we have $P \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} P''$ as required.

□

Lemma 53. *Let $P \ (\approx_m)_c^\bullet \ Q$.*

- *If $P \xmapsto{\tau} P'$ then there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $P' \ (\approx_m)_c^\bullet \ Q'$.*
- *If $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T \ (\approx_m)_c^\bullet \ T'$, and $\mathbb{E} \ (\approx_m)_c^\bullet \ \mathbb{F}$, then there exists T'', Q' such that $T' \stackrel{\tau}{\Rightarrow} T$", $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T'',\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$ and $P' \ (\approx_m)_c^\bullet \ Q'$.*
- *If $P \xmapsto{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$, $T \ (\approx_m)_c^\bullet \ T'$, and $\mathbb{E} \ (\approx_m)_c^\bullet \ \mathbb{F}$, then there exists Q' such that $Q \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} Q'$ and $P' \ (\approx_m)_c^\bullet \ Q'$.*

Proof. We proceed by induction on the size of the derivation of $P \ (\approx_m)_c^\bullet \ Q$.

- Suppose $P \approx_m^\circ Q$. Since P, Q are closed, we have $P \approx_m Q$. The first condition is true by definition. We now prove the third point, the proof for the second one is similar. By Lemma 52, there exists P'' such that $P \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} P''$ and $P' \approx_m^\bullet P''$. By Lemma 42, there exists Q' such that $Q \xRightarrow{\overline{a},T',\mathbb{F}}_{\widetilde{b}} Q'$ and $P'' \approx_m Q'$. Let σ be a substitution that closes P''. Since Q' is closed, we have $P''\sigma \approx_m Q'$ by Lemma 46. Consequently we have $P' \approx_m^\bullet \approx_m^\circ Q'$, and since the involved processes are closed, we have $P' \ (\approx_m)_c^\bullet \ Q'$ as required.
- Suppose $P \approx_m^\bullet R \approx_m^\circ Q$. Let σ be a substitution that closes R. Since P is closed, we have $P \approx_m^\bullet R\sigma$ by Lemma 47. Since Q is closed, we have $R\sigma \approx_m Q$ by open extension definition. We prove the first point, the proofs for the second and third point are similar. By induction, there exists R' such that $R \stackrel{\tau}{\Rightarrow} R'$ and $P' \approx_m^\bullet R'$. By Lemma 42, there exists Q' such that $Q \stackrel{\tau}{\Rightarrow} Q'$ and $R' \approx_m Q'$. Since R', Q' are closed, we have $R' \approx_m^\circ Q'$, consequently we have $P' \approx_m^\bullet \approx_m^\circ Q'$. The involved processes are closed, hence we have $P' \ (\approx_m)_c^\bullet \ Q'$ as wished.

- If $P = op(\widetilde{P})$ and $Q = op(\widetilde{Q})$ with $\widetilde{P}\ (\approx_m)^\bullet_c\ \widetilde{Q}$. We prove the first condition.
  - $P = P_1 \mid P_2$ with $P_1 \overset{\tau}{\longmapsto} P_1'$. By induction there exists Q_1' such that $Q_1 \overset{\tau}{\Mapsto} Q_1'$ and $P_1'\ (\approx_m)^\bullet_c\ Q_1'$. Using rule HO$\pi$P-PAR, we have $Q \overset{\tau}{\Mapsto} Q_1' \mid Q_2$ and since $\approx^\bullet_m$ is a congruence and the involved processes are closed, we have $P_1' \mid P_2\ (\approx_m)^\bullet_c\ Q_1' \mid Q_2$ as required.
  - Locality, restriction: similar to the case above.
  - Communication: $P = P_1 \mid P_2$ with $P_1 \overset{\overline{a},P_2,\square}{\longmapsto_{\widetilde{b}}} P'$. Since $P_2\ (\approx_m)^\bullet_c\ Q_2$, by induction (second item) there exists Q' such that $Q_1 \overset{\overline{a},Q_2,\square}{\Longmapsto_{\widetilde{b}}} Q'$ and $P'\ (\approx_m)^\bullet_c\ Q'$. We have $Q_1 \overset{\tau}{\Mapsto} Q_1' \overset{\overline{a},Q_2',\square}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Mapsto} Q'$ and $Q_2 \overset{\tau}{\Mapsto} Q_2'$. By HO$\pi$P-PAR, we have $Q \overset{\tau}{\Mapsto} Q_1' \mid Q_2'$; by HO$\pi$P-HO and HO$\pi$P-PAR, we have $Q_1' \mid Q_2' \overset{\tau}{\Mapsto} Q'$. Hence we have $Q \overset{\tau}{\Mapsto} Q'$ and $P'\ (\approx_m)^\bullet_c\ Q'$, as required.

  We now prove the second item.

  - $P = \overline{a}\langle P_1\rangle P_2$ and $Q = \overline{a}\langle Q_1\rangle Q_2$ with $T \overset{a,P_1}{\longmapsto} U$, $\widetilde{b} = \mathrm{fn}(P_1)$, and $P' = U \mid \mathbb{E}\{P_2\}$. Since $P_1\ (\approx_m)^\bullet_c\ Q_1$, we also have $\mathrm{fn}(Q_1) = \widetilde{b}$. By Lemma 48 there exists U' such that $T' \overset{a,Q_1}{\Longmapsto} U'$ and $U\ (\approx_m)^\bullet_c\ U'$. There exists U_1, U_2 such that $T' \overset{\tau}{\Rightarrow} U_1 \overset{a,Q_1}{\longmapsto} U_2 \overset{\tau}{\Mapsto} U'$. Consequently we have $Q \overset{\overline{a},U_1,\mathbb{F}}{\longmapsto_{\widetilde{b}}} U_2 \mid \mathbb{F}\{Q_2\}$. We have $T' \overset{\tau}{\Mapsto} U_1$ and $Q \overset{\tau}{\Mapsto} \overset{\overline{a},U_1,\mathbb{F}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Mapsto} U' \mid \mathbb{F}\{Q_2\} = Q'$. We have $P_2\ (\approx_m)^\bullet_c\ Q_2$ and $\mathbb{E}\ (\approx_m)^\bullet_c\ \mathbb{F}$, so we have $\mathbb{E}\{P_2\}\ (\approx_m)^\bullet_c\ \mathbb{F}\{Q_2\}$ by Lemma 49, hence we have $P'\ (\approx_m)^\bullet_c\ Q'$, as required.
  - $P = b[P_1]$ with passivation: similar to the case above.
  - $P = P_1 \mid P_2$ with $P_1 \overset{\overline{a},T,\mathbb{E}\{\square \mid P_2\}}{\longmapsto_{\widetilde{b}}} P'$. Since $P_2\ (\approx_m)^\bullet_c\ Q_2$ we have $\mathbb{E}\{\square \mid P_2\}\ (\approx_m)^\bullet_c\ \mathbb{F}\{\square \mid Q_2\}$. By induction there exists $T", Q'$ such that $T' \overset{\tau}{\Mapsto} T"$, $Q_1 \overset{\tau}{\Mapsto} \overset{\overline{a},T",\mathbb{F}\{\square \mid Q_2\}}{\Longmapsto_{\widetilde{b}}} \overset{\tau}{\Mapsto} Q'$ and $P'\ (\approx_m)^\bullet_c\ Q'$. By rules HO$\pi$P-PAR and HO$\pi$P-OUT-PAR we have $Q \overset{\tau}{\Mapsto} \overset{\overline{a},T",\mathbb{F}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Mapsto} Q'$, as required.
  - $P = b[P_1]$ without passivation: similar to the case above.
  - $P = \nu c.P_1$ with $P_1 \overset{\overline{c},f,a}{\longmapsto_T} \mathbb{E}\{\nu c.\square\}\widetilde{b}P_1'$ and $c \notin \widetilde{b}$. Similar to the case above.
  - $P = \nu c.P_1$ with $P_1 \overset{\overline{a},T,\mathbb{E}}{\longmapsto_{c\cup\widetilde{b}}} P_1'$. By induction there exists $T", Q_1'$ such that $T' \overset{\tau}{\Mapsto} T"$, $Q_1 \overset{\tau}{\Mapsto} \overset{\overline{a},T',\mathbb{F}}{\longmapsto_{c\cup\widetilde{b}}} \overset{\tau}{\Mapsto} Q_1'$ and $P_1'\ (\approx_m)^\bullet_c\ Q_1'$. By rules HO$\pi$P-PAR and HO$\pi$P-OUT-EXTR we have $Q \overset{\tau}{\Mapsto} \overset{\overline{a},T",\mathbb{F}}{\longmapsto_{\widetilde{b}}} \overset{\tau}{\Mapsto} \nu c.Q_1'$. Since $\approx^\bullet_m$ is a congruence and the involved processes are closed, we have $\nu c.P_1'\ (\approx_m)^\bullet_c\ \nu c.Q_1'$, as required.

  We now prove the last item. We have two cases. Suppose first that the derivation comes from rule HOπP-OUT-CAPTURE: we have $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, $c \in \widetilde{b}$,

and $P \xmapsto{\overline{a},T,\mathbb{E}_1\{\mathbb{E}_2\}}_{\widetilde{b}} P'$. By Lemma 51 there exists $\mathbb{F}_1, \mathbb{F}_2$ such that $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$, $\mathbb{F}_1 \approx^{\bullet}_m \mathbb{E}_1$, and $\mathbb{F}_2 \approx^{\bullet}_m \mathbb{E}_2$. By induction there exists Q' such that $Q \xmapsto{\overline{a},T',\mathbb{F}_1\{\mathbb{F}_2\}}_{\widetilde{b}} Q'$ and $P' \approx^{\bullet}_m Q'$. By rule HO$\pi$P-OUT-CAPTURE we have $Q \xmapsto{\overline{a},T',\mathbb{F}}_{\widetilde{b}} Q'$, hence the result holds.

Suppose now that the derivation comes from rule HOπP-OUT-CAPTURE-FREE: we have $P \xrightarrow{\overline{a},T,\mathbb{E}}_{\widetilde{b}} P'$. By induction, there exists $T", Q'$ such that $T' \stackrel{\tau}{\Rightarrow} T"$, $Q \stackrel{\tau}{\Rightarrow} \xrightarrow{\overline{a},T",\mathbb{E}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$, and $P' \ (\approx_m)^{\bullet}_c \ Q'$ Using rule HOπP-OUT-CAPTURE-FREE we have $Q \stackrel{\tau}{\Rightarrow} \xmapsto{\overline{a},T",\mathbb{F}}_{\widetilde{b}} \stackrel{\tau}{\Rightarrow} Q'$, so we have $Q \xmapsto{\overline{a},Q',T'}_{\mathbb{F}} \widetilde{b}Q'$, as wished.

□

Now we no longer need the extension of $\approx_m$ to capture-free transition, so we suppose that $\approx_m$ is the usual complementary bisimilarity. Notice that Lemmas 53 and 48 show that $(\approx_m)^{\bullet}_c$ is a weak complementary simulation.

Lemma 54. *If $P \ (\approx_m)^{\bullet}_c \ Q$ and $P \stackrel{\lambda}{\Rightarrow} P'$, there exists Q' such that $Q \stackrel{\lambda}{\Rightarrow} Q'$ and $P' \ (\approx_m)^{\bullet}_c \ Q'$.*

Proof. Similar to the one of Lemma 42, using Lemmas 53 and 48. □

Lemma 55. *Let $(\approx^{\bullet}_m)^*$ be the reflexive and transitive closure of $\approx^{\bullet}_m$.*

- *$(\approx^{\bullet}_m)^*$ is symmetric.*
- *$((\approx_m)^{\bullet}_c)^*$ is a weak complementary bisimulation.*

Proof. We prove that $(\approx^{\bullet}_m)^{-1} \subseteq (\approx^{\bullet}_m)^*$ by induction on the derivation of $P(\approx^{\bullet}_m)^{-1}Q$.

- If we have $Q \approx^{\circ}_m P$, then we have $P \approx^{\circ}_m Q$, i.e. we have $P(\approx^{\bullet}_m)^*Q$, as required.
- If we have $Q \approx^{\bullet}_m T \approx^{\circ}_m P$, by induction we have $T(\approx^{\bullet}_m)^*Q$. We have $P \approx^{\circ}_m T$, i.e. we have $P \approx^{\bullet}_m T$, so by transitivity we have $P(\approx^{\bullet}_m)^*Q$, as required.
- If we have $Q = Q_1 \mid Q_2$, $P = P_1 \mid P_2$ with $Q_1 \approx^{\bullet}_m P_1$ and $Q_2 \approx^{\bullet}_m P_2$. By induction we have $P_1(\approx^{\bullet}_m)^*Q_1$ and $P_2(\approx^{\bullet}_m)^*Q_2$. Since $\approx^{\bullet}_m$ is a congruence, we have $P_1 \mid P_2(\approx^{\bullet}_m)^*Q_1 \mid P_2$ and $Q_1 \mid P_2(\approx^{\bullet}_m)^*Q_1 \mid Q_2$, consequently we have $P(\approx^{\bullet}_m)^*Q$ by transitivity. The cases for other operators are similar.

We now prove that $((\approx_m)^{\bullet}_c)^*$ is a weak complementary bisimulation. Since $(\approx^{\bullet}_m)^*$ is symmetric, it is enough to prove that $((\approx_m)^{\bullet}_c)^*$ is a weak complementary simulation. Let $P((\approx_m)^{\bullet}_c)^*Q$; there exists k such that $P((\approx_m)^{\bullet}_c)^kQ$. We proceed by induction on k. The result holds for $k = 0$, suppose it holds for $l \leq k$, we prove for $k+1$. Let $P((\approx_m)^{\bullet}_c)^kP_k \ (\approx_m)^{\bullet}_c \ Q$.

- $\text{fn}(P) = \text{fn}(P_k) = \text{fn}(Q)$

- If $P \stackrel{\lambda}{\longmapsto} P'$, then by induction there exists a process P'_k such that $P_k \stackrel{\lambda}{\Longmapsto} P'_k$ and $P'((\approx_m)^\bullet_c)^* P'_k$. By Lemma 54, there exists Q' such that $Q \stackrel{\lambda}{\Longmapsto} Q'$ and $P'_k \ (\approx_m)^\bullet_c \ Q'$. The result then holds by transitivity.

□

Theorem 10. *$\approx_m$ is a congruence.*

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

Using the congruence theorem, we can prove the following inclusion between $\approx$ and $\approx_m$:

Lemma 56. *If $P \approx_m Q$ then $P \approx Q$.*

Proof. We prove that $\approx_m$ is a weak early context bisimulation.

- If $P \stackrel{\tau}{\longrightarrow} P'$, then by Lemma 37 we have $P \stackrel{\tau}{\longmapsto} P'$. By definition there exists Q' such that $Q \stackrel{\tau}{\Longmapsto} Q'$ and $P' \approx_m Q'$. By Lemma 38 we have $Q \stackrel{\tau}{\Rightarrow} Q'$, hence the result holds.

- Let $P \stackrel{a}{\longrightarrow} F$ and $C = \widetilde{\nu b}.RS$ be a closed concretion. By Lemma 33 we have $P \stackrel{a,R}{\longmapsto} F \circ R$. By definition there exists Q' such that $Q \stackrel{a,R}{\Longmapsto} Q'$ and $F \circ R \approx_m Q'$. By Lemma 38 there exists G such that $Q \stackrel{a}{\Rightarrow} G$ and $G \circ R \stackrel{\tau}{\Rightarrow} Q'$. Using CONTEXT-PAR and CONTEXT-RESTR, we have $G \bullet C = \widetilde{\nu b}.(G \circ R \mid S) \stackrel{\tau}{\Rightarrow} \widetilde{\nu b}.(Q' \mid S)$. Since $\approx_m$ is a congruence, we have $F \bullet C = \widetilde{\nu b}.(F \circ R \mid S) \approx_m \widetilde{\nu b}.(Q' \mid S)$, hence the result holds.

- Let $P \stackrel{\overline{a}}{\longrightarrow} C$ and F be a closed abstraction. By Lemma 36, for some T such that $T \stackrel{a}{\longrightarrow} F$ and some $\mathbb{E}$, we have $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} F \bullet \mathbb{E}\{C\} = P'$. By definition there exists Q' such that $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'$ and $P' \approx_m Q'$. By Lemma 38 there exists C' such that $Q \stackrel{\overline{a}}{\Rightarrow} C'$ and $F \bullet \mathbb{E}\{C'\} \stackrel{\tau}{\Rightarrow} Q'$, hence the result holds.

□

B.3 Completeness Proof

Definition 22. *A closed process P is image finite iff for all α, the set $\{P', P \stackrel{\lambda}{\Longmapsto} P'\}$ is finite.*

Definition 23. *The relation $\approx_{m,\omega}$ is defined on closed processes by:*

1. *We have $P \approx_{m,0} Q$ iff $fn(P) = fn(Q)$.*
2. *We have $P \approx_{m,k+1} Q$ iff*
   - *If $P \stackrel{\tau}{\longmapsto} P'$, then there exists Q' such that $Q \stackrel{\tau}{\Longmapsto} Q'$ and $P' \approx_{m,k} Q'$, and conversely if $Q \stackrel{\tau}{\longmapsto} Q'$.*

- *If* $P \stackrel{a,R}{\longmapsto} P'$*, then there exists* Q' *such that* $Q \stackrel{a,R}{\Longmapsto} Q'$ *and* $P' \mathcal{R} Q'$*, and conversely if* $Q \stackrel{a,R}{\longmapsto} Q'$*.*
- *If* $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$*, then there exists* Q' *such that* $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'$ *such that* $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto}_{\widetilde{b}} Q'$*, and conversely if* $Q \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} Q'$*.*

3. $\approx_{m,\omega} = \bigcap_k \approx_{m,k}$

Lemma 57. *The relations* $\approx_m$ *and* $\approx_{m,\omega}$ *coincide on image-finite processes.*

Proof. From the definition of $\approx_{m,\omega}$, we already have that $\approx_m \subset \approx_{m,\omega}$. We show the converse by proving that $\approx_{m,\omega}$ is a weak bisimulation. Let P, Q be image-finite processes such that $P \approx_{m,\omega} Q$. Since the relation is symmetrical, we make the proof for the transitions from P only. We have three cases to check:

- Assume $P \stackrel{\tau}{\longmapsto} P'$. For all integers k, there exists Q_k such that $Q \stackrel{\tau}{\Longmapsto} Q_k$ and $P' \approx_{m,k} Q_k$. Since Q is image-finite, the set $\{Q_i | Q \stackrel{\tau}{\Longmapsto} Q_i\}$ is finite. We now prove by contradiction that there exists Q' such that $Q \stackrel{\tau}{\Longmapsto} Q'$ and for all k, $P' \approx_{m,k} Q'$. Assume that for all Q_i such that $Q \stackrel{\tau}{\Longmapsto} Q_i$, there exists k_i such that $P' \not\approx_{m,k_i} Q_i$. Since $\approx_{m,j} \subset \approx_{m,l}$ if $l \leq j$, for all $j \geq k_i$, we have $P' \not\approx_{m,j} Q_i$. Since $\{Q_i | Q \stackrel{\tau}{\Longmapsto} Q_i\}$ is finite, the set $\{k_i\}$ is finite and has a greatest element J. For all Q' such that $Q \stackrel{\tau}{\Longmapsto} Q'$, we have $P' \not\approx_{m,j} Q'$ for all $j \geq J$. But for all k, there exists Q_k such that $Q \stackrel{\tau}{\Longmapsto} Q_k$ and $P' \approx_{m,k} Q_k$, hence a contradiction. Therefore there exists Q' such that $Q \stackrel{\tau}{\Longmapsto} Q'$ and for all k, $P' \approx_{m,k} Q'$, i.e. $P' \approx_{m,\omega} Q'$, as required.
- Assume $P \stackrel{a,R}{\longmapsto} P'$. Similar to the case above.
- Assume $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$. Similar to the case above.

□

For the following proof we define some notations (for P closed process):

$$P \oplus s = \overline{s}.\mathbf{0} \mid s.P$$
$$\sum_{i=1}^{n} P_i = \nu a.(\overline{a}\langle P_1 \rangle \mathbf{0} \mid \ldots \mid \overline{a}\langle P_n \rangle \mathbf{0} \mid a(X)X \mid \prod_{i=2}^{n} a(X_i)\mathbf{0})$$

We have the following properties :

- $P \oplus s \downarrow_s$
- $P \oplus s \longrightarrow P$
- For all $1 \leq i \leq n$, $\sum_{j=1}^{n} P_j \longrightarrow^n \sim_m P_i$

Lemma 58. *1. Let $T \stackrel{a,R}{\longmapsto} T'$ and $c \notin fn(T,R)$. There exists T_c, T'_c such that $T_c \stackrel{a,R}{\longmapsto} T'_c$, $T'_c \downarrow_c$ and $T'_c \stackrel{\tau}{\mapsto} T'$.*

2. Let $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ and $c \notin fn(P,T,\mathbb{E})$. There exists T_c, P'_c such that $P \stackrel{\overline{a},T_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'_c$, $P'_c \downarrow_c$ and $P'_c \stackrel{\tau}{\mapsto} P'$.

Proof. Let $T \stackrel{a,R}{\longmapsto} T'$ and $c \notin \text{fn}(T,R)$. We proceed by induction on $T \stackrel{a,R}{\longmapsto} T'$.

- $a(X)T_1 \stackrel{a,R}{\longmapsto} T_1\{R/X\}$. We define $T_C = a(X)T_1 \mid c.\mathbf{0} \mid \overline{c}.\mathbf{0}$ and $T'_c = T_1\{R/X\} \mid c.\mathbf{0} \mid \overline{c}.\mathbf{0}$. We verify easily the conditions of the first item.
- $T_1 \mid T_2 \stackrel{a,R}{\longmapsto} T'_1 \mid T_2$ with $T_1 \stackrel{a,R}{\longmapsto} T'_1$. Since c is fresh for T, c is also fresh for T_1, so by induction there exists $T_{1,c}, T'_{1,c}$ verifying the conditions of the first item w.r.t. T_1, T'_1. We define $T_c = T_{1,c} \mid T_2$, $T'_c = T'_{1,c} \mid T_2$ which respects the conditions of the first item with respect to T, T'.
- Locality case: similar to the case above.
- Restriction case: similar to the case above.

Let $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$ and $c \notin \text{fn}(P,T,\mathbb{E})$. We proceed by induction on $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'$.

- $\overline{a}\langle P_1\rangle P_2 \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{\widetilde{b}} T' \mid \mathbb{E}\{P_2\}$ with $T \stackrel{a,P_1}{\longmapsto} T'$. There exists T_c, T'_c verifying the conditions of the first item. Consequently by CONTEXT-CONCR we have $P \stackrel{\overline{a},T_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} T'_c \mid \mathbb{E}\{P_2\} = P'_c$. Since $T'_c \downarrow_c$, we have $P'_c \downarrow_c$, and since $T'_c \stackrel{\tau}{\mapsto} T'$, we have $P'_c \stackrel{\tau}{\mapsto} P'$ by rule HOπP-TAU-PAR.
- $P = b[P_1]$ and passivation occurs; similar to the case above.
- $P = b[P_1]$ and $P_1 \stackrel{\overline{a},T,\mathbb{E}\{b[\Box]\}}{\longmapsto}_{\widetilde{x}} P'$. Since $c \notin \text{fn}(P)$, we have $c \notin \text{fn}(P_1)$, so by induction there exists P'_c verifying conditions of the second item w.r.t. P_1. By rule HOπP-OUT-LOC we have $P \stackrel{\overline{a},T_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} P'_c$, as required.
- Parallel composition case: similar to the case above.
- Restriction case (without extrusion): similar to the case above.
- $P = \nu d.P_1$ with $P_1 \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto}_{d\cup\widetilde{b}} P'_1$. Since $c \notin \text{fn}(P)$, we have $c \notin \text{fn}(P_1)$ (in particular, $c \neq d$). By induction there exists $P'_{1,c}$ verifying conditions of the second item w.r.t. P_1. By rule HOπP-OUT-EXTR we have $P \stackrel{\overline{a},T_c,\mathbb{E}}{\longmapsto}_{\widetilde{b}} \nu d.P'_{1,c}$. We define $P'_c = \nu d.P'_{1,c}$. Since $d \neq c$ and $P'_{1,c} \downarrow_c$, we have $P'_c \downarrow_c$. Since $P'_{1,c} \stackrel{\tau}{\mapsto} P'_1$, we have $\nu d.P'_c \stackrel{\tau}{\mapsto} P'$ by rule HOπP-TAU-RESTR, hence the result holds.

□

Lemma 59. *Let P, Q two image-finite processes. For all integers k, if $P \not\approx_{m,k} Q$ then there exists a context $\mathbb{K}$ and a name d such that $\mathbb{K}\{P\} \oplus d \not\approx_b \mathbb{K}\{Q\} \oplus d$.*

Proof. We proceed by induction on k. For the case $k = 0$, we must have $\text{fn}(P) \neq \text{fn}(Q)$. Assume we have $a \in \text{fn}(P) \setminus \text{fn}(Q)$ for instance. We define

$$\begin{aligned}\mathbb{K} &= b[\nu a.\overline{c}\langle\Box\rangle\mathbf{0} \mid R] \mid S\\ R &= a.\mathbf{0} \mid \overline{a}.\overline{a}.d.\mathbf{0}\\ S &= c(X)b(Y)(Y \mid Y)\end{aligned}$$

where b, c, d are all distinct and do not occur in $\text{fn}(P, Q)$. Let f be a fresh name. We now prove by contradiction that $\mathbb{K}\{P\} \oplus f \not\approx_b \mathbb{K}\{Q\} \oplus f$. Assume that $\mathbb{K}\{P\} \oplus f \approx_b \mathbb{K}\{Q\} \oplus f$. We have $\mathbb{K}\{P\} \oplus f \longrightarrow \nu a.(b[R] \mid b(Y)(Y \mid Y)) = T_1$ (since $a \in \text{fn}(P)$ it has to be extruded during the communication). Since $\neg(T_1 \downarrow_c)$, the only way for $\mathbb{K}\{Q\} \oplus f$ to match this transition is with the transition $\mathbb{K}\{Q\} \oplus f \longrightarrow b[\nu a.R] \mid b(Y)(Y \mid Y) = U_1$ (we have $a \notin \text{fn}(Q)$, so a is not extruded). Now we have

$$T_1 \longrightarrow \nu a.(R \mid R) = T_2$$

which can only be matched by

$$U_1 \longrightarrow (\nu a.R) \mid (\nu a.R) = U_2$$

The reduction $T_2 \longrightarrow \nu a.(a.\mathbf{0} \mid \overline{a}.\overline{a}.d.\mathbf{0} \mid \overline{a}.d.\mathbf{0}) = T_3$ can be matched by $U_3 \longrightarrow (\nu a.\overline{a}.d.\mathbf{0}) \mid (\nu a.R) = U_3$. We have $T_3 \longrightarrow \nu a.(\overline{a}.\overline{a}.d.\mathbf{0} \mid d.\mathbf{0}) = T_4$, with $T_4 \downarrow_d$: this reduction cannot be matched by U_3. Hence a contradiction.

Assume the property holds for all $k \leq n$. We now prove it for $n+1$. Since $P \approx_m Q$ implies $P \approx_b Q$, to prove $P_1 \not\approx_b Q_1$, it suffices to show that $P_2 \not\approx_b Q_2$ with $P_1 \approx_m P_2$ and $Q_1 \approx_m Q_2$. We distinguish the following cases:

- $P \overset{\tau}{\mapsto} P'$. For all Q' such that $Q \overset{\tau}{\Mapsto} Q'$, we have $P' \not\approx_{m,k} Q'$. Since Q is image-finite, the set $\{Q'_i | Q \overset{\tau}{\Mapsto} Q'_i\}$ is finite (assume its cardinality is N). By induction, there are contexts $\mathbb{K}_i$ and names d_i such that $\mathbb{K}_i\{P'\} \oplus d_i \not\approx_b \mathbb{K}_i\{Q'_i\} \oplus d_i$ for all i. We define:

  $$\mathbb{K} = a[\Box] \mid a(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i))$$

  where a, s do not occur in P, Q. Let t be a fresh name. Assume that $\mathbb{K}\{P\} \oplus t \approx_b \mathbb{K}\{Q\} \oplus t$. Since $P \longrightarrow P'$, we have

  $$\mathbb{K}\{P\} \oplus t \longrightarrow a[P'] \mid a(X)(s \oplus \sum_j (\mathbb{K}_j\{X\} \oplus d_j)) = R_1$$

  Since $\neg R_1 \downarrow_t$ and $R_1 \downarrow_a$ (the passivation of locality a is not triggered), it can only be matched by

  $$\mathbb{K}\{Q\} \oplus t \Longrightarrow a[Q'_l] \mid a(X)(s \oplus \sum_j (\mathbb{K}_j\{X\} \oplus d_j)) = S_1$$

for some l. We now have

$$R_1 \longrightarrow s \oplus \sum_j (\mathbb{K}_j\{P'\} \oplus d_j) = R_2$$

Since we have $\neg R_2 \downarrow_a$ and $R_2 \downarrow_s$, it can only be matched by:

$$S_1 \Longrightarrow s \oplus \sum_j (\mathbb{K}_j\{Q'_i\} \oplus d_j) = S_2$$

with $Q'_l \Longrightarrow Q'_i$ for some i. We have $R_2 \longrightarrow^{N+1}\approx \mathbb{K}_i\{P'\} \oplus d_i = R_3$, which can only be matched by $S_2 \Longrightarrow\approx \mathbb{K}_i\{Q'_i\} \oplus d_i = S_3$, since $R_3 \downarrow_{d_i}$. Hence a contradiction, since $\mathbb{K}_i\{P'\} \oplus d_i \not\approx_b \mathbb{K}_i\{Q'_i\} \oplus d_i$, so we have $\mathbb{K}\{P\} \oplus t \not\approx_b \mathbb{K}\{Q\} \oplus t$, as required.

- $P \stackrel{a,R}{\longmapsto} P'$. For all Q' such that $Q \stackrel{a,R}{\Longmapsto} Q'$, we have $P' \not\approx_{m,k} Q'$. Since Q is image-finite, the set $\{Q'_i | Q \stackrel{a,R}{\Longmapsto} Q'_i\}$ is finite. By induction there exists contexts $\mathbb{K}_i$ and names d_i such that $\mathbb{K}_i\{P'\} \oplus d_i \not\approx_b \mathbb{K}_i\{Q'_i\} \oplus d_i$ for all i. We define

$$\mathbb{K} = b[\Box] \mid \overline{a}\langle R\rangle b(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i))$$

where b, s are distinct, and do not occur in R, P, Q. Let t be a fresh name. We have

$$\mathbb{K}\{P\} \oplus t \longrightarrow b[P'] \mid b(X)(s \oplus \sum_j (\mathbb{K}_j\{X\} \oplus d_j)) = R_1$$

Since $R_1 \downarrow_b$, it can only be matched by a

$$\mathbb{K}\{Q\} \oplus t \Longrightarrow b[Q'_l] \mid b(X)(s \oplus \sum_j (\mathbb{K}_j\{X\} \oplus d_j)) = S_1$$

for some l. From here, the proof is similar to the $P \stackrel{\tau}{\longmapsto} P'$ case.

- $P \stackrel{\overline{a},T,\mathbb{E}}{\longmapsto\!\!\!\!\!\sim}_b P'$. For all Q' such that $Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto\!\!\!\!\!\sim}_b Q'$, we have $P' \not\approx_{m,k} Q'$. Since Q is image-finite, the set $\{Q'_i | Q \stackrel{\overline{a},T,\mathbb{E}}{\Longmapsto\!\!\!\!\!\sim}_b Q'_i\}$ is finite. By induction there exists contexts $\mathbb{K}_i$ and names d_i such that $\mathbb{K}_i\{P'\} \oplus d_i \not\approx_b \mathbb{K}_i\{Q'_i\} \oplus d_i$ for all i. Let c be fresh for $P, Q, T, \mathbb{E}$. By Lemma 58 there exists T_c, P'_c such that $P \stackrel{\overline{a},T_c,\mathbb{E}}{\longmapsto\!\!\!\!\!\sim}_b P'_c$, $P'_c \downarrow_c$ and $P'_c \stackrel{\tau}{\longmapsto} P'$. We define:

$$\mathbb{K} = b[\mathbb{E} \mid T_c] \mid b(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i))$$

where b, s are distinct, and fresh for $P, Q, \mathbb{E}, T, c$. Let t be a fresh name. We have

$$\mathbb{K}\{P\} \oplus t \longrightarrow b[P'_c] \mid b(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i)) = R_1$$

Since we have $R_1 \downarrow_c$, it can only be matched by

$$\mathbb{K}\{Q\} \oplus t \Longrightarrow b[Q'_{m,c}] \mid b(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i)) = S_1$$

for some m. Now we have

$$\mathbb{K}\{P\} \oplus t \longrightarrow b[P'] \mid b(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i)) = R_2$$

Since we have $\neg R_2 \downarrow_c$ and $R_2 \downarrow_b$, it can only be matched by:

$$\mathbb{K}\{Q\} \oplus t \Longrightarrow b[Q'_l] \mid b(X)(s \oplus \sum_i (\mathbb{K}_i\{X\} \oplus d_i)) = S_2$$

for some l with $Q'_{m,c} \Longrightarrow Q'_l$. From here the proof is similar to the previous cases.

□

Remark 6. *In the concretion case, we have to add an observable c to T to be sure that Q match reduction from P by interacting with T (and not by any other internal action), and therefore to be sure that Q evolves towards one of the Q'_i.*

C Proof Sketches for Seal Calculus

Lemma 60. *If $P \approx_m Q$ and $P \overset{\lambda}{\Rightarrow} P'$, then there exists Q' such that $Q \overset{\lambda}{\Rightarrow} Q'$ and $P' \approx_m Q'$*

Proof. By case analysis on $P \overset{\lambda}{\Rightarrow} P'$, and by induction in the freeze and capsule cases. □

Lemma 61. *If $P \approx^\bullet_m Q$ then fn$(P) =$ fn(Q).*

Proof. By induction on $P \approx^\bullet_m Q$. □

Lemma 62. *Let $P\ (\approx_m)^\bullet_c\ Q$. If $P \overset{\mu}{\longmapsto} P'$ for $\mu \neq \tau$, then there exists Q' such that $Q \overset{\mu}{\Rightarrow} Q'$ and $P'\ (\approx_m)^\bullet_c\ Q'$.*

Proof. We first proof that $P \approx^\bullet_m Q$ implies $P\{\widetilde{v}/\widetilde{x}\} \approx^\bullet_m Q\{\widetilde{v}/\widetilde{x}\}$ by induction on $P \approx^\bullet_m Q$. We then prove the lemma by induction on $P \approx^\bullet_m Q$. □

Lemma 63. *If $P \overset{\gamma[a^\eta\{R\}]}{\longmapsto} P'$ then for all $R\ (\approx_m)^\bullet_c\ R'$, we have $P \overset{\gamma[a^\eta\{R'\}]}{\longmapsto} P''$ with $P'\ (\approx_m)^\bullet_c\ P''$.*

Let $P\ (\approx_m)^\bullet_c\ Q$. If $P \overset{\gamma[a^\eta\{R\}]}{\longmapsto} P'$ then for all $R\ (\approx_m)^\bullet_c\ R'$, we have $Q \overset{\gamma[a^\eta\{R'\}]}{\Longmapsto} Q'$ with $P'\ (\approx_m)^\bullet_c\ Q'$.

Proof. First item is proved by induction on $P \stackrel{\gamma[a^\eta\{R\}]}{\longmapsto} P'$. Suppose we have $P = a^\eta\{\widetilde{x}\}.P_1 \stackrel{*[a^\eta(R)]}{\longmapsto} P_1 \mid x_1[R] \mid \ldots \mid x_n[R] = P'$. Then we have $P \stackrel{*[a^\eta(R')]}{\longmapsto} P_1 \mid x_1[R'] \mid \ldots \mid x_n[R'] = P''$. Since $R \approx_m^\bullet R'$ and $\approx_m^\bullet$ is a congruence, we have $P' \approx_m^\bullet P''$ as wished.

Suppose $P = P_1 \mid P_2$, $P \stackrel{\gamma[a^\eta\{R\}]}{\longmapsto} P_1' \mid P_2 = P'$ with $P_1 \stackrel{\gamma[a^\eta\{R\}]}{\longmapsto} P_1'$. By induction there exists P_1'' such that $P_1 \stackrel{\gamma[a^\eta\{R'\}]}{\longmapsto} P_1''$ and $P_1' \approx_m^\bullet P_1''$. Using the same LTS rule we have $P \stackrel{\gamma[a^\eta\{R'\}]}{\longmapsto} P_1'' \mid P_2 = P''$. By congruence of $\approx_m^\bullet$ we have $P' \approx_m^\bullet P''$ as wished. The restriction and seal cases are similar.

Second item is proved by induction on $P \ (\approx_m)_c^\bullet \ Q$. If $P \approx_m^\circ Q$ then by first item there exists P'' such that $P \stackrel{\gamma[a^\eta\{R'\}]}{\longmapsto} P''$ and $P' \approx_m^\bullet P''$. By bisimilarity definition there exists Q' such that $Q \stackrel{\gamma[a^\eta\{R'\}]}{\Longmapsto} Q'$ and $P'' \approx_m^\circ Q'$. Hence we have $P' \approx_m^\bullet \approx_m^\circ Q'$, i.e. $P' \approx_m^\bullet Q'$ as wished.

If $P \approx_m^\bullet \approx_m^\circ Q$, then we use induction hypothesis and then Lemma 60.

If $P = op(\widetilde{P'})$ and $Q = op(\widetilde{Q'})$ with $\widetilde{P'} \approx_m^\bullet \widetilde{Q'}$, then we make a case analysis on op. Suppose $P = a^\eta\{\widetilde{x}\}.P_1$ and $Q = a^\eta\{\widetilde{x}\}.P_1$ with $P_1 \approx_m^\bullet Q_1$. We have $P \stackrel{*[a^\eta\{R\}]}{\longmapsto} P_1 \mid x_1[R] \mid \ldots \mid x_n[R] = P'$ and $Q \stackrel{*[a^\eta\{R'\}]}{\longmapsto} Q_1 \mid x_1[R'] \mid \ldots \mid x_n[R'] = Q'$. Since $P_1 \approx_m^\bullet Q_1$, $R \approx_m^\bullet R'$, and by congruence of $\approx_m^\bullet$, we have $P' \approx_m^\bullet Q'$ as required.

Suppose $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$ with $P_1 \approx_m^\bullet Q_1$ and $P_2 \approx_m^\bullet Q_2$. We have $P \stackrel{\gamma[a^\eta\{R\}]}{\longmapsto} P_1' \mid P_2 = P'$ with $P_1 \stackrel{\gamma[a^\eta\{R\}]}{\longmapsto} P_1'$. By induction there exists Q' such that $Q_1 \stackrel{\gamma[a^\eta\{R'\}]}{\Longmapsto} Q_1'$ and $P_1' \approx_m^\bullet Q_1'$. By LTS rules we have $Q \stackrel{\gamma[a^\eta\{R'\}]}{\Longmapsto} Q_1 \mid Q_2 = Q'$. By congruence of $\approx_m^\bullet$ we have $P' \approx_m^\bullet Q'$ as wished. The restriction and seal cases are similar to this one.

□

We have $\mathbb{E} \approx_m \mathbb{F}$ iff for all P, we have $\mathbb{E}\{P\} \approx_m \mathbb{F}\{P\}$. We also extend inductively extend $\approx_m^\bullet$ to evaluation contexts.

Lemma 64. *If $\mathbb{E}_1 \approx_m^\bullet \mathbb{F}_1$ and $\mathbb{E}_2 \approx_m^\bullet \mathbb{F}_2$ then $\mathbb{E}_1\{\mathbb{E}_2\} \approx_m^\bullet \mathbb{F}_1\{\mathbb{F}_2\}$*

Proof. By induction on $\mathbb{E}_1 \approx_m^\bullet \mathbb{F}_1$. □

Lemma 65. *If $P \approx_m^\bullet Q$ and $\mathbb{E} \approx_m^\bullet \mathbb{F}$, then we have $\mathbb{E}\{P\} \approx_m^\bullet \mathbb{F}\{Q\}$.*

Proof. Using the fact that $P \approx_m^\bullet Q$ implies $\mathbb{E}\{P\} \approx_m^\bullet \mathbb{E}\{Q\}$, and by induction on $\mathbb{E} \approx_m^\bullet \mathbb{F}$. □

Lemma 66. *If $P \stackrel{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{x}} P'$ then for all $R \ (\approx_m)_c^\bullet \ R'$, $S \ (\approx_m)_c^\bullet \ S'$, $\mathbb{E} \ (\approx_m)_c^\bullet \ \mathbb{E}'$, and $\mathbb{F} \ (\approx_m)_c^\bullet \ \mathbb{F}'$ we have $P \stackrel{a,b,S',R',\gamma,\mathbb{E}',\mathbb{F}'}{\Longmapsto}_{\widetilde{x}} P'$ with $P' \ (\approx_m)_c^\bullet \ P''$.*

Proof. By induction on $P \stackrel{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}{\longmapsto}_{\widetilde{x}} P'$. □

Lemma 67. *If $P \xmapsto{a,b,R,\gamma,\mathbb{F}}_{\widetilde{x}} P'$ then for all $R\ (\approx_m)^\bullet_c\ R'$, $\mathbb{F}\ (\approx_m)^\bullet_c\ \mathbb{F}'$ we have $P \xmapsto{a,b,R',\gamma,\mathbb{F}'}_{\widetilde{x}} P''$ with $P'\ (\approx_m)^\bullet_c\ P''$.*

Proof. By induction on $P \xmapsto{a,b,R,\gamma,\mathbb{F}}_{\widetilde{x}} P'$ □

Lemma 68. *Let $P\ (\approx_m)^\bullet_c\ Q$.*

- *If $P \overset{\tau}{\mapsto} P'$ then we have $Q \overset{\tau}{\mapsto} Q'$ with $P'\ (\approx_m)^\bullet_c\ Q'$.*
- *Let $P\ (\approx_m)^\bullet_c\ Q$. If $P \xmapsto{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}_{\widetilde{x}} P'$ then for all $R\ (\approx_m)^\bullet_c\ R'$, $S\ (\approx_m)^\bullet_c\ S'$, $\mathbb{E}\ (\approx_m)^\bullet_c\ \mathbb{E}'$, and $\mathbb{F}\ (\approx_m)^\bullet_c\ \mathbb{F}'$ we have $Q \xmapsto{a,b,S',R',\gamma,\mathbb{E}',\mathbb{F}'}_{\widetilde{x}} Q'$ with $P'\ (\approx_m)^\bullet_c\ Q'$.*
- *If $P \xmapsto{a,b,R,\gamma,\mathbb{F}}_{\widetilde{x}} P'$ then for all $R\ (\approx_m)^\bullet_c\ R'$, $\mathbb{F}\ (\approx_m)^\bullet_c\ \mathbb{F}'$ we have $Q \xmapsto{a,b,R',\gamma,\mathbb{F}'}_{\widetilde{x}} Q'$ with $P'\ (\approx_m)^\bullet_c\ Q'$.*

Proof. By induction on $P\ (\approx_m)^\bullet_c\ Q$.

If $P \approx^\circ_m Q$, then the result holds by definition for τ-actions. For higher-order labels, we use Lemmas 67 and 66 to define a Q' such that $P' \approx^\bullet_m \approx^\circ_m Q'$. If $P \approx^\bullet_m \approx^\circ_m Q$ then we use induction hypothesis and then Lemma 60. If $op(\widetilde{P}) \approx^\bullet_m op(\widetilde{Q})$ with $\widetilde{P} \approx^\bullet_m \widetilde{Q}$, we perform a case analysis on *op*.

Seal case $P = b[P_1]$ with $Q = z[Q_1]$ and $P_1 \approx^\bullet_m Q_1$.

- $P \xmapsto{a,b,S,R,*,\mathbb{E},\mathbb{F}}_{\widetilde{x}} P'$ with $S \xmapsto{\overline{a}^*\{b\}} T$, $R \xmapsto{*[a^*\{P_1\}]} U$, $\widetilde{x} = \text{fn}(P_1)$, and $P' = \mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid T\} \mid U$. By Lemmas 62 and 63, there exists T', U' such that $S' \xRightarrow{\overline{a}^*\{b\}} T'$, $R' \xRightarrow{*[a^*\{Q_1\}]} U'$, $T \approx^\bullet_m T'$ and $U \approx^\bullet_m U'$. By Lemma 61, we have $\text{fn}(Q_1) = \text{fn}(P_1) = \widetilde{x}$. By the LTS rules we have $Q \xmapsto{a,b,S',R',*,\mathbb{E}',\mathbb{F}'}_{\widetilde{x}} \mathbb{F}'\{\mathbb{E}'\{\mathbf{0}\} \mid T'\} \mid U' = Q'$. By congruence of $\approx^\bullet_m$ and by Lemma 65 we have $P' \approx^\bullet_m Q'$ as required.
- $P \xmapsto{a,b,S,R,*,\mathbb{E},\mathbb{F}}_{\widetilde{x}} P'$ with $S \xmapsto{\overline{a}^z\{b\}} T$, $R \xmapsto{z[a^\uparrow\{P_1\}]} U$, $\widetilde{x} = \text{fn}(P_1)$, and $P' = \mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid T\} \mid U$. Similar to the case above.
- $P \xmapsto{a,b,S,R,z,\mathbb{E},\mathbb{F}}_{\widetilde{x}} P'$ with $S \xmapsto{\overline{a}^\uparrow\{b\}} T$, $R \xmapsto{*[a^z\{P_1\}]} U$, $\widetilde{x} = \text{fn}(P_1)$, and $P' = z[\mathbb{F}\{\mathbb{E}\{\mathbf{0}\} \mid T\}] \mid U$. Similar to the case above.
- $P \xmapsto{a,c,R,*,\mathbb{F}}_{\widetilde{x}} P'$ with $P_1 \xmapsto{a,c,R,b,\mathbb{F}}_{\widetilde{x}} P'$. By induction there exists Q' such that $Q_1 \xRightarrow{a,c,R',b,\mathbb{F}'}_{\widetilde{x}} Q'$ and $P' \approx^\bullet_m Q'$. By the LTS rules we have $Q \xRightarrow{a,c,R',*,\mathbb{F}'}_{\widetilde{x}} Q'$ as required.
- $P \overset{\tau}{\mapsto} b[P_1']$ with $P_1 \overset{\tau}{\mapsto} P_1'$. By induction there exists Q_1' such that $P_1 \overset{\tau}{\mapsto} Q_1'$ and $P_1' \approx^\bullet_m Q_1'$. By the LTS rules we have $Q \overset{\tau}{\Rightarrow} b[Q_1']$, and by congruence of $\approx^\bullet_m$ we have $b[P_1'] \approx^\bullet_m b[Q_1']$ as required.

Restriction case $P = \nu y.P_1$, $Q = \nu y.Q_1$ and $P_1 \approx^\bullet_m Q_1$.

- $P \xmapsto{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}_{\widetilde{x}} P'$ with $P_1 \xmapsto{a,b,S,R,\gamma,\mathbb{E}\{\nu y.\Box\},\mathbb{F}}_{\widetilde{x}} P'$, $y \neq b$ and $y \notin \widetilde{x}$. By induction there exists Q' such that $Q_1 \stackrel{a,b,S',R',\mathbb{E}'\{\nu y.\Box\},\mathbb{F}',\widetilde{x}'}{\Longmapsto}_Q$ and $P' \approx^{\bullet}_m Q'$. Since $y \neq b$ and $y \notin \widetilde{x}$ we have $Q \stackrel{a,b,S',R',\mathbb{E}',\mathbb{F}',\widetilde{x}'}{\Longmapsto}_Q$ by the LTS rules. Hence we have the required result.

- $P \xmapsto{a,b,R,\gamma,\mathbb{F}}_{\widetilde{x}} P'$ with $P_1 \xmapsto{a,b,R,\gamma,\mathbb{F}\{\nu y.\Box\}}_{\widetilde{x}} P'$ and $y \notin \{a,b\} \cup \widetilde{x}$. By induction there exists Q' such that $Q_1 \stackrel{a,b,R',\gamma,\mathbb{F}'\{\nu y.\Box\}}{\Longmapsto}_{\widetilde{x}} Q'$ and $P' \approx^{\bullet}_m Q'$. Since $y \notin \{a,b\} \cup \widetilde{x}$ we have $Q \stackrel{a,b,R',\gamma,\mathbb{F}'}{\Longmapsto}_{\widetilde{x}} Q'$ by the LTS rules. Hence we have the required result.

- $P \xmapsto{\tau} \nu y.P'_1$ with $P_1 \xmapsto{\tau} P'_1$. By induction there exists Q'_1 such that $Q_1 \stackrel{\tau}{\Longmapsto} Q'_1$ and $P'_1 \approx^{\bullet}_m Q'_1$. By the LTS rule we have $Q \stackrel{\tau}{\Longmapsto} \nu y.Q'_1$ and by congruence of $\approx^{\bullet}_m$, we have $\nu y.P'_1 \approx^{\bullet}_m \nu y.Q'_1$ as required.

Parallel case $P = P_1 \mid P_2, Q = Q_1 \mid Q_2$ with $P_1 \approx^{\bullet}_m Q_1$ and $P_2 \approx^{\bullet}_m Q_2$.

- $P \xmapsto{a,b,S,R,\gamma,\mathbb{E},\mathbb{F}}_{\widetilde{x}} P'$ with $P_1 \xmapsto{a,b,S,R,\gamma,\mathbb{E}\{\Box \mid P_2\},\mathbb{F}}_{\widetilde{x}} P'$. By induction there exists Q' such that $Q_1 \stackrel{a,b,S',R',\gamma,\mathbb{E}'\{\Box \mid P_2\},\mathbb{F}'}{\Longmapsto}_{\widetilde{x}} Q'$ and $P' \approx^{\bullet}_m Q'$. By the LTS rules we have $Q \stackrel{a,b,S',R',\gamma,\mathbb{E}',\mathbb{F}'}{\Longmapsto}_{\widetilde{x}} Q'$, hence the result holds.

- $P \xmapsto{a,b,R,\gamma,\mathbb{F}}_{\widetilde{x}} P'$ with $P_1 \xmapsto{a,b,P_2,R,\gamma,\Box,\mathbb{F}}_{\widetilde{x}} P'$. By induction there exists Q' such that $Q_1 \stackrel{a,b,Q_2,R',\gamma,\Box,\mathbb{F}'}{\Longmapsto}_{\widetilde{x}} Q'$ and $P' \approx^{\bullet}_m Q'$. By the LTS rules we have $Q \stackrel{a,b,R',\gamma,\mathbb{F}}{\Longmapsto}_{\widetilde{x}} Q'$, hence the result holds.

- $P \xmapsto{a,b,R,\gamma,\mathbb{F}}_{\widetilde{x}} P'$ with $P_1 \xmapsto{a,b,R,\gamma,\mathbb{F}\{\Box \mid P_2\}}_{\widetilde{x}} P'$. By induction there exists Q' such that $Q_1 \stackrel{a,b,R',\gamma,\mathbb{F}\{\Box \mid P_2\}}{\Longmapsto}_{\widetilde{x}} Q'$ and $P' \approx^{\bullet}_m Q'$. By the LTS rules we have $Q \stackrel{a,b,R',\gamma,\mathbb{F}}{\Longmapsto}_{\widetilde{x}} Q'$, hence the result holds.

- $P \xmapsto{\tau} P'_1 \mid P_2$ with $P_1 \xmapsto{\tau} P'_1$. By induction there exists Q'_1 such that $Q_1 \stackrel{\tau}{\Longmapsto} Q'_1$ and $P'_1 \approx^{\bullet}_m Q'_1$. By the LTS rules we have $Q \stackrel{\tau}{\Longmapsto} Q'_1 \mid Q_2$ and by congruence of $\approx^{\bullet}_m$ we have $P'_1 \mid P_2 \approx^{\bullet}_m Q'_1 \mid Q_2$ as required.

- $P \xmapsto{\tau} \nu\widetilde{z}.(P'_1 \mid P'_2) = P'$ with $P_1 \xmapsto{(\nu\widetilde{z})*[\overline{x}^*(\widetilde{v})]} P'_1$ and $P_2 \xmapsto{*[x^*(\widetilde{v})]} P'_2$. By Lemma 62 there exists Q'_1, Q'_2 such that $Q_1 \stackrel{(\nu\widetilde{z})*[\overline{x}^*(\widetilde{v})]}{\Longmapsto} Q'_1$, $Q_2 \stackrel{*[x^*(\widetilde{v})]}{\Longmapsto} Q'_2$, $P'_1 \approx^{\bullet}_m Q'_1$, and $P'_2 \approx^{\bullet}_m Q'_2$. By the LTS rules we have $Q \stackrel{\tau}{\Longmapsto} \nu\widetilde{z}.(Q'_1 \mid Q'_2) = Q'$, and by congruence of $\approx^{\bullet}_m$, we have $P' \approx^{\bullet}_m Q'$ as required.

- $P \xmapsto{\tau} \nu\widetilde{z}.(P'_1 \mid P'_2) = P'$ with $P_1 \xmapsto{(\nu\widetilde{z})*[\overline{x}^a(\widetilde{v})]} P'_1$ and $P_2 \xmapsto{a[x^\uparrow(\widetilde{v})]} P'_2$. Similar to the case above.

- $P \xmapsto{\tau} \nu\widetilde{z}.(P'_1 \mid P'_2) = P'$ with $P_1 \xmapsto{(\nu\widetilde{z})a[\overline{x}^\uparrow(\widetilde{v})]} P'_1$ and $P_2 \xmapsto{*[x^a(\widetilde{v})]} P'_2$. Similar to the case above.

- $P \stackrel{\tau}{\longmapsto} P'$ with $P_1 \stackrel{a,b,P_2,*,\Box}{\longmapsto}_{\widetilde{x}} P'$. By induction there exists $Q_1 \stackrel{a,b,Q_2,*,\Box}{\Longmapsto}_{\widetilde{x}} Q'$ such that $P' \approx_m^\bullet Q'$. By the LTS rules we have $Q \stackrel{\tau}{\Longmapsto} Q'$, hence the result holds.

□

Lemma 69. *Let* $((\approx_m)_c^\bullet)^*$ *be the reflexive and transitive closure of* $(\approx_m)_c^\bullet$.

- $((\approx_m)_c^\bullet)^*$ *is symmetric.*
- $((\approx_m)_c^\bullet)^*$ *is a weak complementary bisimulation.*

Proof. For the first item, we prove by induction on the definition $(\approx_m^\bullet)^{-1}$ of that $(\approx_m^\bullet)^{-1} \subseteq (\approx_m^\bullet)^*$. For the second item, we prove that $(\approx_m^\bullet)$ is a simulation using Lemmas 62, 63, and 68. □

Lemma 70. $\approx_m$ *is a congruence.*

Proof. Because $\approx_m \subseteq (\approx_m)_c^\bullet \subseteq \approx_m$ □

Centre de recherche INRIA Grenoble – Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Centre de recherche INRIA Bordeaux – Sud Ouest : Domaine Universitaire - 351, cours de la Libération - 33405 Talence Cedex
Centre de recherche INRIA Lille – Nord Europe : Parc Scientifique de la Haute Borne - 40, avenue Halley - 59650 Villeneuve d'Ascq
Centre de recherche INRIA Nancy – Grand Est : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex
Centre de recherche INRIA Paris – Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex
Centre de recherche INRIA Rennes – Bretagne Atlantique : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex
Centre de recherche INRIA Saclay – Île-de-France : Parc Orsay Université - ZAC des Vignes : 4, rue Jacques Monod - 91893 Orsay Cedex
Centre de recherche INRIA Sophia Antipolis – Méditerranée : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399