



Bisimulations dans les calculs avec passivation

Sergueï Lenglet

► To cite this version:

Sergueï Lenglet. Bisimulations dans les calculs avec passivation. Informatique [cs]. Université Joseph-Fourier - Grenoble I, 2010. Français. NNT : . tel-00447857

HAL Id: tel-00447857

<https://theses.hal.science/tel-00447857>

Submitted on 16 Jan 2010

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

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

UNIVERSITÉ DE GRENOBLE

N° attribué par la bibliothèque

--	--	--	--	--	--	--	--	--	--

THÈSE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE GRENOBLE

Spécialité : Informatique

préparée au laboratoire LIG, projet SARDES,
dans le cadre de l'Ecole Doctorale

Mathématiques Sciences et Technologies de l'Information, Informatique

présentée et soutenue publiquement par

Sergueï LENGLET

le 15 Janvier 2010

*Bisimulations dans les calculs avec
passivation*

Directeur de thèse :

Jean-Bernard STEFANI

JURY

M.	Pierre-Louis	CURIEN	Président
M.	Matthew	HENNESSY	Rapporteur
M.	Davide	SANGIORGI	Rapporteur
M.	Jean-François	MONIN	Examineur
M.	Francesco	ZAPPA NARDELLI	Examineur
M.	Jean-Bernard	STEFANI	Directeur de thèse
M.	Alan	SCHMITT	Co-Directeur de thèse

à *Andrian*

Remerciements

Je remercie Alan Schmitt et Jean-Bernard Stefani pour la présence et le soutien dont ils ont fait preuve tout au long de cette thèse. Nos échanges m'ont permis de me poser les bonnes questions et de corriger mes erreurs. Merci pour toutes ces discussions, scientifiques ou non, qui ont participé à rendre agréables ces années de thèse.

Merci à l'ensemble des membres du jury, en particulier à Pierre-Louis Curien, qui a accepté d'en être le président, ainsi qu'à Matthew Hennessy et Davide Sangiorgi, qui ont bien voulu relire cette thèse, et dont les commentaires m'ont permis de sensiblement améliorer ce document.

Merci à Daniel Hirschhoff et Tom Hirschowitz, comme enseignants d'abord, pour m'avoir donné le goût de la recherche en informatique théorique, mais également pour s'être intéressés à mes travaux et pour m'avoir forcé à m'exprimer autrement que par monosyllabes.

Merci au projet Sardes de m'avoir accueilli et pour l'ambiance qui règne au sein de l'équipe. Merci pour les séminaires et les tablées de vingt personnes à midi qui participent à la bonne humeur générale. Merci à Benoît, Fabien $\times 2$, Jean, Michaël, Stéphane, Sylvain, Willy, etc. pour les parties de Tetrinet, Diplomacy, Wormux (bien que Worms soit meilleur), Can't Stop, etc. Merci à Thomas pour son niveau à Starcraft, et à Damien pour la technique du mass dropships. Merci à tous les membres de l'équipe que j'ai pu côtoyer, joueurs ou non.

Merci à Aurélien et Romain, maîtres en humour potache.

Enfin, merci à la ville de Grenoble, son air pur, son climat tempéré, et ses prix de l'immobilier abordables. Merci à l'INRIA de s'être installé à Montbonnot, un site particulièrement bien desservi par les transports publics, surtout pour ceux qui, comme moi, partent au travail dès l'aube.

Table des matières

1	Introduction	1
1.1	Calculs de processus et passivation	1
1.2	Équivalences comportementales	2
1.3	Contributions	3
1.4	Organisation du document	4
2	Bisimulations dans les calculs d'ordre supérieur	5
2.1	Le calcul $HO\pi$	5
2.1.1	Syntaxe et sémantique informelle	5
2.1.2	Système de transitions étiquetées	7
2.2	Théorie comportementale pour $HO\pi$	9
2.2.1	Congruence barbue	9
2.2.2	Bisimilarité d'ordre supérieur	10
2.2.3	Bisimilarité contextuelle	12
2.2.4	Bisimilarité normale	15
2.3	Équivalences dans les calculs avec passivation	16
2.3.1	Syntaxe et sémantique de $HO\pi P$	16
2.3.2	Bisimilarité contextuelle	17
2.4	État de l'art et conclusions	19
2.4.1	Le calcul minimal $HOcore$	19
2.4.2	Les calculs $CHOCS$ et Plain $CHOCS$	20
2.4.3	Les Ambients	20
2.4.4	Le Seal	21
2.4.5	Les calculs avec passivation	21
2.4.6	Bisimilarité environnementale	22
2.4.7	Conclusions	22
3	Bisimulation normale	25
3.1	Bisimulation normale pour HOP	25
3.1.1	Bisimulation d'ordre supérieur	25
3.1.2	Bisimilarité normale	28
3.2	Équivalence de fonctions pour $HO\pi P$	31
3.2.1	Les processus sans réception	31
3.2.2	Processus finis	32
3.2.3	Contre-exemples	33
3.3	Conclusions	35
4	Preuves de congruence	37
4.1	Preuve classique pour $HO\pi$	37
4.2	Preuve par progression	39
4.3	Méthode de Howe	42
4.3.1	Résumé de la méthode	43
4.3.2	Problème avec la communication d'ordre supérieur	44

4.4	Autres méthodes et conclusions	45
5	Sémantique à complément	47
5.1	Sémantique à complément pour $HO\pi$	47
5.1.1	Système de transitions étiquetées à complément	47
5.1.2	Bisimulation associée	49
5.2	Application à $HO\pi P$	50
5.2.1	Système de transitions étiquetées à complément	51
5.2.2	Bisimulation à complément	53
5.3	Conclusions	55
6	Application au Kell-calcul	57
6.1	Récepteurs joints	57
6.1.1	Le calcul $HO\pi J$	57
6.1.2	Sémantique à complément	59
6.1.3	Bisimilarité à complément	63
6.2	Sémantique à complément du Kell	64
6.2.1	Présentation du Kell	64
6.2.2	Syntaxe et sémantique contextuelle	65
6.2.3	Sémantique à complément : principe	68
6.2.4	Transitions inférieures	69
6.2.5	Transitions supérieures	73
6.2.6	Actions internes et jugements d'observation	75
6.2.7	Bisimilarité à complément	77
6.3	Conclusions	79
7	Conclusions et perspectives	81
A	Sémantique à complément	89
A.1	Résultats généraux sur la méthode de Howe	89
A.2	Preuves pour $HO\pi$	90
A.2.1	Correspondance des systèmes de transitions	90
A.2.2	Congruence de la bisimilarité à complément	92
A.2.3	Correspondance des bisimilarités	94
A.3	Preuves pour $HO\pi P$	95
A.3.1	Correspondance des systèmes de transitions	95
A.3.2	Congruence de la bisimilarité à complément	98
A.3.3	Correspondance des bisimilarités	101
A.3.4	Complétude	102
A.4	Preuves pour $HO\pi J$	106
A.5	Preuves pour le Kell	111
A.5.1	Système de transitions à complément	111
A.5.2	Congruence de la bisimilarité à complément	115
B	Preuves pour HOP	121
B.1	Congruence	121
B.2	Bisimilarité normale	122
C	Équivalences de fonctions en $HO\pi P$	127

Chapitre 1

Introduction

1.1 Calculs de processus et passivation

Les systèmes distribués sont constitués de nombreuses entités, de natures différentes, qui peuvent évoluer indépendamment et interagir entre elles, et dont la configuration peut changer dynamiquement. Décrire et raisonner sur les comportements de tels systèmes nécessite une modélisation qui fasse abstraction le plus possible de la nature des composants pour s'intéresser principalement à leurs interactions. C'est dans cet esprit qu'ont été conçus les *calculs de processus*, dans lesquels les systèmes concurrents et communicants sont représentés par des *processus* capables de s'échanger des messages. Les calculs de processus peuvent être classés en deux grandes familles : les calculs de *premier ordre* comme le π -calcul [34], dans lesquels seuls des noms (qui désignent des canaux de communication) peuvent être transmis, et les calculs d'*ordre supérieur* comme $\text{HO}\pi$ [41], dans lesquels des processus exécutables sont échangés. Ces derniers permettent de modéliser la migration de code au sein d'un réseau, comme par exemple le téléchargement d'un programme sur Internet. En $\text{HO}\pi$, la seule évolution possible est la communication synchrone ; par exemple dans la réduction

$$\bar{a}\langle P \rangle \mathbf{0} \mid a(X)Q \longrightarrow Q\{P/X\}$$

l'émetteur $\bar{a}\langle P \rangle \mathbf{0}$ transmet le processus P au récepteur $a(X)Q$. Le processus Q peut ensuite exécuter une ou plusieurs copies du processus P .

Dans le π -calcul ou en $\text{HO}\pi$, les processus s'exécutent tous en parallèle, au même niveau. Il est parfois nécessaire de disposer d'un contrôle plus fin de la distribution des processus, par exemple pour distinguer les machines membres d'un réseau local au sein d'un réseau global, ou pour regrouper les processus qui s'exécutent sur la même machine. Ces besoins ont favorisé l'émergence de nombreux calculs comportant une notion de *localité*, associée à des primitives pour la migration [55]. La mobilité peut concerner les processus ou les localités ; dans $\text{D}\pi$ [18] ou encore dans [1], seuls les processus peuvent migrer entre différentes localités qui sont toutes au même niveau. Dans les Ambients [10] ou le Seal [54], les localités peuvent être incluses les unes dans les autres, formant ainsi une *hiérarchie*, qui peut évoluer dynamiquement. Ces localités peuvent induire ou non des restrictions sur les communications : par exemple dans les Ambients ou en Seal, les messages ne peuvent franchir plusieurs limites de localités. En revanche, dans le Join-calcul distribué [13], les localités sont *transparentes* : elles n'empêchent en rien la communication ou la mobilité.

Dans cette thèse, nous nous intéressons aux calculs avec localités comportant un opérateur spécial appelé *passivation*. Cet opérateur permet de stopper un processus en cours d'exécution, et de conserver ou non son état ; le processus ainsi suspendu peut ensuite être répliqué ou transmis pour être réactivé. La passivation rend possible la modélisation d'opérations de reconfiguration dynamique, telles que la migration de code dynamique (l'exécution d'un programme est stoppée pour être poursuivie sur une autre machine), l'installation de correctifs ou de mises à jour, la récupération de pannes, ou encore les

comportements adaptatifs, dans lesquels un système se reconfigure pour s'adapter aux changements de son environnement d'exécution. Le calcul Homer [19], le M-calcul [46] et le Kell [47] comportent un opérateur de passivation ; de même, le langage de programmation Acute [48] inclut une forme de passivation de processus légers appelée *thunkification*.

Dans ce document, nous travaillons principalement avec le calcul $\text{HO}\pi\text{P}$, une extension minimale de $\text{HO}\pi$ avec un opérateur de passivation. Un exemple de passivation en $\text{HO}\pi\text{P}$ est donné par la réduction suivante

$$a[P] \mid a(X)Q \longrightarrow Q\{P/X\}$$

dans laquelle $a[P]$ est une localité nommée a et contenant un processus P , et $a(X)Q$ est un processus récepteur. Dans la transition ci-dessus, la localité a est détruite, et le processus P est passé en argument au récepteur $a(X)Q$. Une localité $a[\]$ est un contexte d'exécution transparent : si P peut se réduire en P' , alors $a[P]$ se réduit en $a[P']$, et P peut communiquer avec l'extérieur de a sans aucune contrainte. Cette forme de passivation est une simplification des opérateurs de passivation présents dans le Kell et Homer. En particulier, nous omettons l'utilisation des récepteurs joints du Kell, et les restrictions sur les communications présentes dans les deux calculs.

1.2 Équivalences comportementales

Dans les systèmes interactifs, remplacer un élément par un autre, pour des raisons d'optimisation par exemple, peut avoir des conséquences sur l'ensemble du système. Il faut donc s'assurer au préalable que la version optimisée a le *même comportement* que la version initiale. Pour formaliser cette notion de “même comportement”, nous définissons une *équivalence comportementale* sur les systèmes et leurs composantes. Un système peut communiquer avec son environnement, ou évoluer par lui-même. Selon les besoins, nous nous intéressons à une partie de ces actions seulement, que nous appelons *observables* (ou *barbes*). Par exemple, pour comparer un programme P à sa version optimisée P^* , nous considérons uniquement les communications avec l'extérieur et faisons abstraction des actions internes ; les observables sont alors les canaux de communication sur lesquels P et P^* peuvent interagir. Nous disons alors que P et P^* sont équivalents si et seulement si remplacer l'un par l'autre au sein d'un système \mathcal{S} ne change pas le comportement global de \mathcal{S} , et ce quel que soit le système considéré. Dans les calculs de processus, cette notion d'équivalence s'appelle la *congruence barbue* [35].

Si la définition de la congruence barbue est naturelle, elle est en revanche difficile à prouver formellement : pour montrer que deux processus sont équivalents, nous devons considérer tous les systèmes (ou *contextes*) qui peuvent les contenir. Nous cherchons donc à définir une équivalence comportementale plus simple à établir, tout en conservant un pouvoir discriminant semblable à celui de la congruence barbue. Au lieu d'exhiber le comportement d'un processus en le faisant réagir avec un contexte, nous pouvons essayer de raisonner directement sur les interactions offertes par ce processus. Pour cela, nous définissons des transitions $P \xrightarrow{\alpha} P'$, qui signifient que le processus P est capable de devenir P' en faisant l'action α . Par exemple dans le cas du π -calcul, l'action α peut être l'émission d'un nom, la réception d'un nom ou la synchronisation de deux processus. À partir de ce *système de transitions étiquetées*, nous pouvons définir coinductivement une équivalence sur les processus de la manière suivante : deux processus P, Q ont le même comportement si et seulement si pour toute action $P \xrightarrow{\alpha} P'$, il existe une transition $Q \xrightarrow{\alpha} Q'$ de sorte que P' et Q' ont le même comportement (et réciproquement pour les actions de Q). Une équivalence comportementale construite sur ce principe est appelée *bisimilarité*.

Le pouvoir discriminant d'une bisimilarité dépend du choix des actions α . Si ces actions ne sont pas assez détaillées (par exemple “émettre un message” sans préciser sur quel canal de communication), la bisimilarité peut mettre en relation des processus qui n'ont pas le même comportement selon la congruence barbue : on dit alors que la bisimilarité n'est pas

correcte. En revanche, si les actions sont trop précises, la bisimilarité peut être trop fine, et distinguer des processus équivalents selon la congruence barbue : dans ce cas, la bisimilarité n'est pas *complète*. Définir une bisimilarité correcte et complète ne pose habituellement pas de problème dans les calculs de premier ordre comme le π -calcul [45]. La situation est plus compliquée pour les calculs d'ordre supérieur. Il faut distinguer les équivalences *fortes*, qui traitent toutes les actions de la même manière, des équivalences *faibles*, dans lequel nous faisons abstraction des actions internes (cf. l'exemple de l'optimisation). La plupart des calculs d'ordre supérieur disposent d'une caractérisation de la congruence barbue dans le cas fort ; en revanche, seuls quelques uns, comme par exemple $\text{HO}\pi$ [42] ou les Ambients [32], bénéficient d'une caractérisation dans le cas faible. Dans les calculs avec passivation, seul Homer [19] disposait jusqu'à aujourd'hui d'une bisimilarité faible correcte mais non complète.

En outre, la caractérisation de la congruence dans les calculs d'ordre supérieur se fait généralement par une bisimilarité *contextuelle*, une forme de bisimilarité définie par Sangiorgi pour $\text{HO}\pi$ [42]. Dans une telle bisimilarité, les processus à comparer sont testés avec les contextes capables d'interagir avec ces processus. Par exemple, deux processus qui émettent sur un nom a sont comparés en les faisant interagir avec tous les récepteurs sur a . La quantification universelle sur les contextes de la congruence barbue a été remplacée par une quantification sur des contextes plus ciblés. Si la bisimilarité contextuelle est un progrès par rapport à la congruence barbue (elle reste plus facile à prouver, notamment grâce à l'utilisation de techniques *modulo* [43]), elle n'est pas complètement satisfaisante ; supprimer toute quantification universelle sur les contextes permettrait par exemple d'automatiser les preuves d'équivalences de processus. C'est pourquoi Sangiorgi définit une autre forme de bisimilarité, appelée bisimilarité *normale* [42]. Tout en restant correcte et complète, la bisimilarité normale teste les processus à l'aide d'un nombre fini de contextes bien choisis. À notre connaissance, une telle bisimilarité n'a été définie jusqu'ici que pour $\text{HO}\pi$ et certaines de ses variantes [42, 22] et pour une version concurrente de ML [21].

1.3 Contributions

Dans les calculs Homer [19] et le Kell [47], les bisimilarités contextuelles correctes et complètes définies dans le cas fort testent de nombreux contextes pour établir l'équivalence de processus. Nous cherchons à définir une caractérisation efficace de la congruence barbue, semblable à la bisimilarité normale de $\text{HO}\pi$. Nous étudions d'abord un calcul avec passivation mais sans opérateur de restriction, appelé HOP, dans lequel nous définissons une bisimilarité normale qui caractérise la congruence barbue. Notre résultat ne repose pas sur la définition d'une forme normale pour les processus, comme en $\text{HO}\pi$ [42], mais sur l'observation de la hiérarchie des localités au sein d'un processus. Nous montrons que cette définition de bisimilarité n'est pas correcte dans les calculs avec passivation et restriction tels que $\text{HO}\pi\text{P}$. Plus précisément, nous donnons plusieurs contre-exemples qui prouvent que tester différentes catégories de processus ne suffit pas à garantir l'équivalence de processus en $\text{HO}\pi\text{P}$. Nous conjecturons qu'il n'est pas possible de définir une bisimilarité normale correcte et complète dans les calculs avec passivation et restriction.

Les calculs Homer et Kell ne disposent pas de caractérisation de la congruence barbue dans le cas faible. La principale difficulté est de prouver la correction d'une bisimilarité candidate¹. Dans un premier temps, nous expliquons pourquoi les différentes techniques de preuve de correction ont échoué jusqu'ici. En particulier, nous expliquons pourquoi les bisimilarités contextuelles ne sont pas adaptées à l'utilisation de la *méthode de Howe*. La méthode de Howe [20, 2, 15] est une méthode de preuve systématique pour montrer qu'une bisimilarité est une congruence, qui s'applique dans les cas fort et faible. Dans leur travaux sur Homer [14], Godskesen et Hildebrandt ont adapté la méthode de Howe pour prouver la congruence d'une bisimilarité contextuelle faible ; malheureusement la relation

¹Une relation est dite candidate si elle est susceptible de caractériser la congruence barbue.

qu'ils définissent n'est pas complète. Nous proposons une nouvelle forme de système de transitions étiquetées, conçu de façon à permettre l'utilisation de la méthode de Howe pour prouver la correction de la bisimilarité associée. Nous présentons notre système de transitions et la bisimilarité correspondante (appelés ensemble *sémantique à complément*) en utilisant le calcul $HO\pi$, puis nous appliquons notre méthode à $HO\pi P$, avant de l'étendre au Kell. Nous prouvons la complétude des bisimilarités à complément forte et faible définies pour $HO\pi$ et $HO\pi P$; en revanche, nous donnons un contre-exemple qui montre que celles définies pour le Kell sont trop discriminantes, pour des raisons liées non pas à la passivation, mais à la présence de récepteurs joints.

1.4 Organisation du document

Ce document est organisé de la manière suivante. Dans le chapitre 2, nous faisons l'état de l'art des calculs d'ordre supérieur et de leur théorie comportementale. En particulier, nous présentons les calculs $HO\pi$ et $HO\pi P$, utilisés intensivement tout le long de cette thèse. Nous détaillons également les différentes formes de bisimilarités définies pour les calculs d'ordre supérieur. Enfin, nous expliquons pourquoi la définition de la bisimilarité contextuelle pour $HO\pi P$ est plus complexe que celle pour $HO\pi$. Dans le chapitre 3, nous cherchons à définir une bisimilarité normale correcte et complète dans différents calculs avec passivation. Nous montrons qu'il est possible de définir une telle relation dans HOP, un calcul muni d'un opérateur de passivation mais dépourvu de restriction. En revanche, nous donnons des contre-exemples qui nous laissent penser qu'il n'est pas possible de définir une bisimilarité normale dans $HO\pi P$.

Dans le chapitre 4, nous passons en revue les principales méthodes de preuve de correction (preuve pour $HO\pi$, preuve par progression et méthode de Howe), et nous expliquons pourquoi elles échouent pour la bisimilarité contextuelle faible dans les calculs avec passivation. Dans le chapitre 5, nous introduisons la sémantique à complément, que nous définissons d'abord pour $HO\pi$. Nous expliquons en quoi cette sémantique permet l'utilisation de la méthode de Howe pour prouver la correction, et nous montrons que les bisimilarités contextuelle et à complément coïncident. Nous définissons ensuite une bisimilarité à complément pour $HO\pi P$, dont nous prouvons la correction et la complétude dans les cas fort et faible, obtenant ainsi le premier résultat de caractérisation de la congruence barbue faible dans un calcul avec passivation.

Dans le chapitre 6, nous définissons une sémantique à complément pour le Kell. Par rapport à $HO\pi P$, la principale difficulté est la présence de récepteurs joints; c'est pourquoi nous étudions dans une première étape la sémantique à complément d'une extension de $HO\pi$ avec récepteurs joints. Le résultat que nous obtenons pour le Kell n'est pas totalement satisfaisant : la bisimilarité que nous définissons est correcte mais pas complète. Le chapitre 7 conclut cette thèse et présente quelques perspectives de recherche.

Les preuves des principaux résultats du chapitre 3 sont données dans les appendices B et C, et celles pour les chapitres 5 et 6 sont données dans l'appendice A. Les résultats présentés dans le chapitre 3 ont été publiés dans [28], et ceux de la section 5.2 ont été publiés dans [27]. Les résultats obtenus dans $HO\pi$ (section 5.1) et le Kell (chapitre 6) n'ont pas encore été soumis à publication.

Chapitre 2

Bisimulations dans les calculs d'ordre supérieur

Dans les calculs de processus *d'ordre supérieur*, les messages contiennent des processus exécutables. Nous présentons dans ce chapitre le calcul d'ordre supérieur $\text{HO}\pi$ [42], et une extension de ce calcul avec un opérateur de passivation, appelé $\text{HO}\pi\text{P}$ [28]. Nous rappelons également la théorie comportementale de ces deux calculs : nous présentons d'abord la relation de référence, la *congruence barbue*, qui permet de définir une notion d'équivalence comportementale dans n'importe quel langage muni d'une réduction. Cette relation est peu utilisable en pratique ; nous allons analyser les différentes relations proposées pour la remplacer. Nous complétons enfin notre état de l'art en décrivant rapidement la théorie comportementale des principaux calculs d'ordre supérieur connus à ce jour.

2.1 Le calcul $\text{HO}\pi$

2.1.1 Syntaxe et sémantique informelle

Le calcul $\text{HO}\pi$ [42] (Higher-Order π -calculus ; π -calcul d'ordre supérieur) est une variante du π -calcul [45] dans laquelle la communication de noms est remplacée par la communication de processus. Nous notons a, b, \dots les noms d'ordre supérieur, \bar{a}, \bar{b}, \dots les co-noms et la méta-variable γ représente les noms et co-noms. Les variables de processus sont notées X, Y, \dots . Un multi-ensemble est un ensemble dans lequel un élément peut apparaître plusieurs fois ; un multi-ensemble est dit fini si et seulement s'il comporte un nombre fini d'éléments. Un multi-ensemble fini $\{x_1, \dots, x_n\}$ est noté \tilde{x} .

La syntaxe du calcul, donnée en figure 2.1, comporte les constructions suivantes.

- Le processus inactif $\mathbf{0}$.
- La composition parallèle $P \mid Q$, où les processus P et Q s'exécutent de manière concurrente.
- La communication synchrone d'ordre supérieur sur un nom a , entre un récepteur $a(X)P$ et un émetteur $\bar{a}(Q)R$.
- La restriction de nom $\nu a.P$, dans laquelle la portée du nom a est restreinte au processus P .
- La réplication de processus $!P$, capable de fournir une infinité de copies de P .

Dans le processus $a(X)P$, la variable X est dite liée ; une variable non liée est dite libre. Nous notons $\text{fv}(P)$ les variables libres d'un processus P . Un processus comportant des variables libres est dit ouvert ; dans le cas contraire, il est dit clos. De la même manière,

$$P ::= \mathbf{0} \mid X \mid P \mid P \mid a(X)P \mid \bar{a}(P)P \mid \nu a.P \mid !P$$

FIG. 2.1 – Syntaxe de $\text{HO}\pi$

le nom a est lié dans le processus $\nu a.P$. Nous notons $\text{fn}(P)$ les noms libres et $\text{bn}(P)$ les noms liés d'un processus P .

Nous notons $P\{\tilde{Q}/\tilde{X}\}$ la substitution simultanée et sans capture de noms des variables \tilde{X} (supposées deux à deux distinctes) par les processus \tilde{Q} . Dans une communication synchrone $a(X)P \mid \bar{a}\langle Q \rangle R$, le processus $a(X)P$ attend un processus sur a , ici Q , pour exécuter ensuite le processus $P\{Q/X\}$. Le processus $\bar{a}\langle Q \rangle R$ est capable d'envoyer un message Q sur a avant que la continuation R ne s'exécute. Le déclenchement de la communication donne le processus $P\{Q/X\} \mid R$. Dans la suite, nous utilisons un cas particulier de communication d'ordre supérieur, la synchronisation sur un nom, dans laquelle aucune information n'est échangée. Nous notons $a.P$ un récepteur $a(X)P$ tel que $X \notin \text{fv}(P)$ et $\bar{a}.Q$ un émetteur $\bar{a}\langle \mathbf{0} \rangle Q$. La synchronisation $a.P \mid \bar{a}.Q$ donne $P \mid Q$. Un processus est dit préfixé si et seulement si il est de la forme $\gamma.P$.

Convention. Nous identifions les processus modulo α -conversion, c'est-à-dire modulo renommage des noms et variables liés. Les processus sont choisis de sorte que leurs noms et variables liés sont différents de leur noms et variables libres. Dans toute discussion ou preuve, nous supposons que les noms et variables liés de toute entité étudiée (processus, agents, actions, ...) sont choisis différents des noms et variables libres de toute autre entité considérée. Avec cette convention, nous écrivons par exemple $\nu a.(P \mid Q) \equiv P \mid \nu a.Q$ sans expliciter de conditions sur les noms libres de Q . Un nom est dit *frais* si et seulement s'il diffère des noms de toutes les entités considérées.

Remarque 2.1. *Comme dans beaucoup d'autres calculs d'ordre supérieur, la réplication de $\text{HO}\pi$ peut être encodée en utilisant les autres constructions du langage. Nous remarquons d'abord que la réplication peut être encodée avec la réplication de processus préfixé, en changeant $!P$ en $\nu a.(\bar{a}.\mathbf{0} \mid a.(P \mid \bar{a}.\mathbf{0}))$. Pour générer une copie de P , on génère une copie de $a.(P \mid \bar{a}.\mathbf{0})$ et on déclenche la synchronisation sur a .*

Par conséquent, il suffit d'encoder la réplication de processus préfixé $!a.P$. Soit b un nom frais; nous définissons $R \triangleq a.b(X)(P \mid X \mid \bar{b}\langle X \rangle \mathbf{0})$, et nous encodons $!a.P$ par $Q = \nu b.(\bar{b}\langle R \rangle \mathbf{0} \mid R)$. Le processus R est similaire au processus $a.P$, sauf qu'il attend une copie de lui-même sur b après communication sur a afin de générer une copie de P et de recréer le processus Q . Ainsi le processus Q se réduit en $P \mid Q$ après synchronisation sur a , de la même manière que le processus $!a.P$.

Cependant, cet encodage introduit une étape supplémentaire dans la création d'un processus répliqué. D'un point de vue comportemental, le processus $!P$ n'est donc pas fortement¹ équivalent à son encodage. Nous avons donc choisi de garder la réplication explicite dans le calcul.

Par la suite nous cherchons à prouver que diverses relations, notamment les équivalences comportementales, sont préservées par les opérateurs du langage. Ainsi, pour une relation \mathcal{R} , nous voulons montrer que $P \mathcal{R} Q$ implique $(P \mid R) \mathcal{R} (Q \mid R)$, $\nu a.P \mathcal{R} \nu a.Q$, etc. Les contextes permettent de composer un processus P quelconque avec un nombre arbitraire d'opérateurs du calcul.

Définition 2.1. *Un contexte \mathbb{C} est obtenu à partir d'un terme en remplaçant une occurrence de $\mathbf{0}$ par un trou \square .*

Ainsi, la syntaxe des contextes de $\text{HO}\pi$ est la suivante :

$$\mathbb{C} ::= \square \mid P \mid \mathbb{C} \mid \mathbb{C} \mid P \mid a(X)\mathbb{C} \mid \bar{a}\langle \mathbb{C} \rangle P \mid \bar{a}\langle P \rangle \mathbb{C} \mid \nu a.\mathbb{C} \mid !\mathbb{C}$$

Remplacer le trou d'un contexte \mathbb{C} par un terme P donne un processus noté $\mathbb{C}\{P\}$. Par exemple, avec $\mathbb{C} \triangleq \nu a.(\square \mid R)$, nous avons $\mathbb{C}\{P\} = \nu a.(P \mid R)$. Contrairement à la substitution de variable, l'instanciation de contexte peut éventuellement capturer des noms

¹dans le sens défini en section 2.2.1

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

FIG. 2.2 – Congruence structurelle

et variables libres. Par exemple, les occurrences de a libres dans P deviennent liées dans le processus $\mathbb{C}\{P\}$ ci-dessus.

Une relation stable par composition par contextes est appelée *congruence*.

Définition 2.2. Une relation d'équivalence \mathcal{R} est une congruence si et seulement si $P \mathcal{R} Q$ implique $\mathbb{C}\{P\} \mathcal{R} \mathbb{C}\{Q\}$ pour tout contexte \mathbb{C} .

La congruence est une caractéristique intéressante à prouver pour les équivalences comportementales. Avec cette propriété, nous pouvons par exemple décomposer les processus étudiés en sous-termes, prouver l'équivalence sur cette décomposition, et en déduire l'équivalence des termes initiaux par congruence.

Nous définissons une première équivalence sur les processus de HO π , la *congruence structurelle*, qui permet de mettre en relation les termes qui ne diffèrent que par la structure.

Définition 2.3. La congruence structurelle est la plus petite congruence qui satisfait les règles données en figure 2.2.

En particulier, la composition parallèle est commutative et associative, et admet $\mathbf{0}$ comme élément neutre. L'ordre des restrictions n'est pas important : nous abrégeons donc le processus $\nu a_1 \dots \nu a_n. P$ en $\nu a_1 \dots a_n. P$ ou en $\nu \tilde{a}. P$. La congruence structurelle permet également d'étendre la portée des restrictions ; cette propriété sera importante par la suite.

2.1.2 Système de transitions étiquetées

La sémantique opérationnelle de HO π est donnée sous forme de système de transitions étiquetées, dont les règles sont rappelées en figure 2.1, à l'exception du symétrique des règles PAR et HO. Un processus peut évoluer vers un autre processus (actions internes ou silencieuses $P \xrightarrow{\tau} P'$), une fonction (réception $P \xrightarrow{a} F = (X)Q$) ou une concrétion (émission $P \xrightarrow{\bar{a}} C = \nu \tilde{b}. \langle R \rangle S$). Dans une concrétion $\nu \tilde{b}. \langle R \rangle S$, les noms \tilde{b} sont supposés deux à deux distincts. Nous appelons *agents*, notés A , l'ensemble des processus, fonctions et concrétions ; ainsi, un processus évolue toujours vers un agent. Nous étendons la composition parallèle et la restriction à tous les agents (figure 2.1). La méta-variable α parcourt l'ensemble des étiquettes τ, γ .

La transition $P \xrightarrow{a} (X)Q$ signifie que P est capable de recevoir un message R sur a pour ensuite continuer comme $Q\{R/X\}$. La transition $P \xrightarrow{\bar{a}} \nu \tilde{b}. \langle R \rangle S$ signifie que P peut émettre le processus R sur a et continuer comme S , et la portée des noms \tilde{b} doit être étendue pour inclure le récepteur de R . L'interaction entre la fonction F et la concrétion C donne une communication d'ordre supérieur (règle HO). Nous définissons un opérateur de pseudo-application

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

en nous appuyant sur la convention sur les noms libres et liés données ci-dessus pour éviter toute capture de noms.

Notez que la règle RESTR n'effectue pas systématiquement l'extension de la portée du nom a ; par définition de l'extension de la restriction aux concrétions, la portée de a n'est étendue que si a appartient aux noms libres du message. Ainsi nous avons

$$\begin{aligned} \nu a. \bar{b} \langle a. \mathbf{0} \rangle a. \mathbf{0} &\xrightarrow{\bar{b}} \nu a. \langle a. \mathbf{0} \rangle a. \mathbf{0} \\ \nu a. \bar{b} \langle c. \mathbf{0} \rangle a. \mathbf{0} &\xrightarrow{\bar{b}} \langle c. \mathbf{0} \rangle \nu a. a. \mathbf{0} \end{aligned}$$

Agents :

Processus	P, Q, R, S	
Fonctions	F, G	$::= (X)P$
Concrétions	C, D	$::= \langle P \rangle Q \mid \nu a.C$
Agents	A, B	$::= P \mid F \mid C$

Extension des opérateurs à tous les agents

$$\begin{array}{ll}
(X)Q \mid P \triangleq (X)(Q \mid P) & (\nu \tilde{b}. \langle Q \rangle R) \mid P \triangleq \nu \tilde{b}. \langle Q \rangle (R \mid P) \\
P \mid (X)Q \triangleq (X)(P \mid Q) & P \mid (\nu \tilde{b}. \langle Q \rangle R) \triangleq \nu \tilde{b}. \langle Q \rangle (P \mid R) \\
\nu a.(X)Q \triangleq (X)\nu a.P & \nu a.(\nu \tilde{b}. \langle Q \rangle R) \triangleq \nu \tilde{b}. a. \langle Q \rangle R \text{ si } a \in \text{fn}(Q) \\
& \nu a.(\nu \tilde{b}. \langle Q \rangle R) \triangleq \nu \tilde{b}. \langle Q \rangle \nu a.R \text{ si } a \notin \text{fn}(Q)
\end{array}$$

Pseudo-application et application de processus

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

Règles du système de transitions étiquetées

$$\begin{array}{c}
a(X)P \xrightarrow{a} (X)P \text{ IN} \quad \bar{a}\langle Q \rangle P \xrightarrow{\bar{a}} \langle Q \rangle P \text{ OUT} \quad \frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} \text{ PAR} \\
\\
\frac{P \xrightarrow{\alpha} A \quad \alpha \notin \{a, \bar{a}\}}{\nu a.P \xrightarrow{\alpha} \nu a.A} \text{ RESTR} \quad \frac{P \xrightarrow{\alpha} A}{!P \xrightarrow{\alpha} A \mid !P} \text{ REPLIC} \\
\\
\frac{P \xrightarrow{a} F \quad P \xrightarrow{\bar{a}} C}{!P \xrightarrow{\tau} F \bullet C \mid !P} \text{ REPLIC-HO} \quad \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \text{ HO}
\end{array}$$

FIG. 2.3 – Sémantique opérationnelle de HO π

et donc pour un récepteur $b(X)P$, nous avons

$$\begin{aligned} b(X)P \mid \nu a.\bar{b}\langle a.\mathbf{0} \rangle a.\mathbf{0} &\xrightarrow{\tau} \nu a.(P\{a.\mathbf{0}/X\} \mid a.\mathbf{0}) \\ b(X)P \mid \nu a.\bar{b}\langle c.\mathbf{0} \rangle a.\mathbf{0} &\xrightarrow{\tau} P\{c.\mathbf{0}/X\} \mid \nu a.a.\mathbf{0} \end{aligned}$$

Cette extension de portée, dite *paresseuse* , est choisie dans la plupart des calculs d'ordre supérieur. Dans le cas de HO π , utiliser l'extension de portée paresseuse ou systématique (c'est-à-dire la portée est étendue que le nom appartienne ou non aux noms libres du message) n'influe pas sur la sémantique du calcul. Nous verrons que le choix de l'extension de portée est plus important pour les calculs avec passivation.

Remarque 2.2. *En toute rigueur, le calcul HO π défini dans [41] autorise également les fonctions dans les messages ; le calcul présenté dans cette section n'est donc que le fragment de second ordre de HO π . Nous donnons quelques résultats pour le calcul HO π d'ordre quelconque dans la section 2.2.4.*

2.2 Théorie comportementale pour HO π

2.2.1 Congruence barbue

Une première notion d'équivalence comportementale, largement utilisée dans les langages concurrents, est la *congruence barbue*, proposée par Milner et Sangiorgi [35]. Cette relation repose sur la réduction du calcul considéré et sur la définition d'*observables* pour un processus. Les observables ne sont pas définis de manière uniforme pour tous les calculs ; il s'agit de paramètres dont nous choisissons de suivre l'évolution au cours des réductions pour mettre en relation ou non les processus. De cette manière, nous définissons formellement le comportement d'un processus. Dans le cas de HO π , nous nous intéressons aux possibles interactions d'un processus avec son environnement ; c'est pourquoi nous choisissons comme observables les canaux γ sur lesquels une communication est possible.

Définition 2.4. *Le prédicat d'observabilité $P \downarrow_\gamma$ pour HO π est défini de la manière suivante :*

- Nous avons $P \downarrow_a$ ssi $P \equiv \nu \tilde{b}.(a(X)Q \mid R)$ avec $a \notin \tilde{b}$.
- Nous avons $P \downarrow_{\bar{a}}$ ssi $P \equiv \nu \tilde{b}.(\bar{a}\langle Q \rangle R \mid S)$ avec $a \notin \tilde{b}$.

Pour un calcul distribué, où les processus s'exécutent dans des localités nommées, une autre possibilité est de choisir par exemple d'observer les localités afin d'étudier le degré de distribution d'un terme.

Remarque 2.3. *Nous pouvons également définir les observables à partir du système de transitions étiquetées : nous avons $P \downarrow_\gamma$ si et seulement si $P \xrightarrow{\gamma} A$ pour un certain A .*

Les observables ainsi choisis, nous pouvons définir une première équivalence, la *bisimilarité barbue*.

Définition 2.5. *Une relation \mathcal{R} sur les processus clos est une simulation barbue forte si et seulement si $P \mathcal{R} Q$ implique :*

- pour tout $P \downarrow_\gamma$, nous avons $Q \downarrow_\gamma$;
- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$.

La relation \mathcal{R} est une bisimulation barbue forte ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations barbues fortes. La bisimilarité barbue forte est la plus grande bisimulation barbue forte.

La bisimilarité barbue forte est la plus grande relation qui préserve les observables par réduction. Cette relation n'est pas satisfaisante en tant qu'équivalence comportementale ; en effet, elle relie les processus $\bar{a}\langle b.\mathbf{0} \rangle \mathbf{0}$ et $\bar{a}\langle c.\mathbf{0} \rangle \mathbf{0}$, qui ne peuvent être considérés comme équivalents, étant donné qu'ils émettent des processus qui se synchronisent sur des noms différents. La bisimilarité barbue sert de base à une relation plus satisfaisante, la *congruence barbue*.

Définition 2.6. La congruence barbue forte \sim_b est la plus grande congruence incluse dans la bisimilarité barbue forte.

Ainsi, nous avons $P \sim_b Q$ si et seulement si pour tout contexte \mathbb{C} , les processus $\mathbb{C}\{P\}$ et $\mathbb{C}\{Q\}$ sont reliés par la bisimilarité barbue forte. La congruence barbue forte distingue bien les processus $\bar{a}\langle b.\mathbf{0} \rangle \mathbf{0}$ et $\bar{a}\langle c.\mathbf{0} \rangle \mathbf{0}$, en considérant le contexte $\mathbb{C} = \square \mid a(X)X$. Après une transition interne, nous obtenons $\mathbb{C}\{P\} \xrightarrow{\tau} b.\mathbf{0}$ et $\mathbb{C}\{Q\} \xrightarrow{\tau} c.\mathbf{0}$; les deux processus résultants n'ont pas les mêmes observables, et ne sont donc pas reliés par la bisimilarité barbue forte.

Les relations définies jusqu'ici sont qualifiées de *fortes* car un processus doit répondre à une transition $\xrightarrow{\tau}$ en effectuant une et une seule transition $\xrightarrow{\tau}$. Il peut être intéressant de considérer des équivalences de processus dans lesquelles un déséquilibre dans le nombre de transitions est autorisé, par exemple pour vérifier qu'un processus P et une version optimisée de P (qui effectue moins d'étapes de réduction) ont bien le même comportement. Dans ce but, nous notons \Rightarrow la clôture réflexive et transitive de $\xrightarrow{\tau}$, et nous définissons la bisimilarité barbue faible de la manière suivante :

Définition 2.7. Une relation \mathcal{R} sur les processus clos est une simulation barbue faible si et seulement si $P \mathcal{R} Q$ implique :

- pour tout $P \downarrow_\gamma$, nous avons $Q \Rightarrow \downarrow_\gamma$;
- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \Rightarrow Q'$ et $P' \mathcal{R} Q'$.

La relation \mathcal{R} est une bisimulation barbue faible ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations barbues faibles. La bisimilarité barbue faible est la plus grande bisimulation barbue faible.

Le processus Q peut donc effectuer un nombre arbitraire de transitions internes avant d'exhiber les mêmes observables que P , et peut répondre à une transition de P par un nombre quelconque (éventuellement nul) de transitions. La définition de congruence barbue faible est directe :

Définition 2.8. La congruence barbue faible \approx_b est la plus grande congruence incluse dans la bisimilarité barbue faible.

Remarque 2.4. Intuitivement, on peut imaginer une autre définition de bisimilarité barbue faible en remplaçant les clauses de la définition 2.7 par :

- pour tout $P \Rightarrow \downarrow_\gamma$, nous avons $Q \Rightarrow \downarrow_\gamma$;
- pour tout $P \Rightarrow P'$, il existe Q' tel que $Q \Rightarrow Q'$ et $P' \mathcal{R} Q'$.

Il est facile de vérifier que les deux définitions sont équivalentes ; la définition 2.7 reste néanmoins plus facile à manipuler.

La congruence barbue est une équivalence comportementale répandue car adaptable (la notion de comportement dépend du choix des observables) et naturelle : deux processus sont considérés équivalents si et seulement s'ils ne peuvent être distingués au sein d'un contexte quelconque. Montrer que deux processus ne sont pas en congruence barbue est simple : il suffit de trouver un contexte \mathbb{C} qui les distingue. En revanche, prouver que deux processus sont en congruence barbue est plus difficile, étant donné la quantification universelle sur les contextes \mathbb{C} dans la définition de la relation. C'est pourquoi il est utile de trouver des caractérisations de la congruence barbue, par exemple en utilisant la co-induction et une définition de bisimilarité appropriée. Nous allons maintenant étudier les différents types de définitions de bisimilarité, et donner les résultats de correspondances avec la congruence barbue de $\text{HO}\pi$.

2.2.2 Bisimilarité d'ordre supérieur

Nous reprenons ici les définitions et observations de Sangiorgi, qui a travaillé sur les définitions de bisimulations pour $\text{HO}\pi$ dans [42, 41]. Les bisimulations définies pour les

calculs de premier ordre tels que CCS [33] ou le π -calcul [45] ne sont pas adaptées pour les calculs d'ordre supérieur. Ces relations mettent en relation des processus émetteurs seulement si les messages émis sont syntaxiquement égaux ; elles distinguent donc par exemple les processus $\bar{a}\langle\mathbf{0}\rangle\mathbf{0}$ et $\bar{a}\langle\mathbf{0} \mid \mathbf{0}\rangle\mathbf{0}$, qui ne peuvent pourtant être différenciés par la congruence barbue. De telles bisimulations ne peuvent donc être complètes.

Une approche, développée par Thomsen pour ses calculs CHOCS [51] et Plain CHOCS [52], est de demander que les messages émis soient *bisimilaires* plutôt que syntaxiquement égaux. L'équivalence ainsi obtenue est appelée bisimilarité d'ordre supérieur ; adaptée à HO π , la définition formelle est la suivante.

Définition 2.9. *Une relation \mathcal{R} sur les processus clos est une simulation d'ordre supérieur ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, il existe F' telle que $Q \xrightarrow{a} F'$ et pour tout processus R , nous avons $F \circ R \mathcal{R} F' \circ R$;
- pour tout $P \xrightarrow{\bar{a}} \nu \tilde{b}. \langle R \rangle S$, il existe $\nu \tilde{b}'. \langle R' \rangle S'$ telle que $Q \xrightarrow{\bar{a}} \nu \tilde{b}'. \langle R' \rangle S'$, $R \mathcal{R} R'$ et $S \mathcal{R} S'$.

La relation \mathcal{R} est une bisimulation d'ordre supérieur ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations d'ordre supérieur. La bisimilarité d'ordre supérieur \sim est la plus grande bisimulation d'ordre supérieur.

Dans le cas de l'émission de message, la bisimilarité d'ordre supérieur ne prend pas en compte les noms extrudés. Ce traitement n'est pas satisfaisant ; considérons par exemple les processus suivants

$$P_1 \triangleq \bar{a}\langle\mathbf{0}\rangle\mathbf{0} \quad P_2 \triangleq \nu b. \bar{a}\langle b.\mathbf{0}\rangle\mathbf{0}$$

Seuls les messages émis sont différents. Cependant le nom b est restreint à P_2 et n'est pas connu de l'environnement. Si nous faisons réagir P_1 et P_2 avec un processus $a(X)R$ (nous rappelons que par convention sur l' α -conversion, nous avons $b \notin \text{fn}(R)$), nous obtenons

$$\begin{aligned} a(X)R \mid \bar{a}\langle\mathbf{0}\rangle\mathbf{0} &\xrightarrow{\tau} R\{\mathbf{0}/X\} \mid \mathbf{0} \\ a(X)R \mid \nu b. \bar{a}\langle b.\mathbf{0}\rangle\mathbf{0} &\xrightarrow{\tau} \nu b. (R\{b.\mathbf{0}/X\} \mid \mathbf{0}) \end{aligned}$$

Comme le nom b n'apparaît pas dans R , le processus $b.\mathbf{0}$ ne peut pas trouver de processus avec qui se synchroniser dans $\nu b. (R\{b.\mathbf{0}/X\} \mid \mathbf{0})$; il ne peut donc effectuer aucune transition et est donc équivalent à $\mathbf{0}$. Les processus résultants $R\{\mathbf{0}/X\} \mid \mathbf{0}$ et $\nu b. (R\{b.\mathbf{0}/X\} \mid \mathbf{0})$, et par conséquent P_1 et P_2 , ne peuvent être distingués par un contexte, et sont donc en congruence barbue forte. Or nous avons $P_1 \not\sim P_2$, car les processus émis $\mathbf{0}$ et $b.\mathbf{0}$ ne sont pas bisimilaires.

La bisimilarité d'ordre supérieur paraît trop discriminante également pour des processus qui ne font pas intervenir la restriction. Nous considérons maintenant les processus suivants :

$$P_1 \triangleq \bar{a}\langle\mathbf{0}\rangle!b.\mathbf{0} \quad P_2 \triangleq \bar{a}\langle b.\mathbf{0}\rangle!b.\mathbf{0}$$

Encore une fois, seuls les processus émis sont différents. En faisant réagir avec un processus récepteur $a(X)R$, nous obtenons

$$\begin{aligned} a(X)R \mid \bar{a}\langle\mathbf{0}\rangle!b.\mathbf{0} &\xrightarrow{\tau} R\{\mathbf{0}/X\} \mid !b.\mathbf{0} \\ a(X)R \mid \bar{a}\langle b.\mathbf{0}\rangle!b.\mathbf{0} &\xrightarrow{\tau} R\{b.\mathbf{0}/X\} \mid !b.\mathbf{0} \end{aligned}$$

Dans le processus $R\{b.\mathbf{0}/X\} \mid !b.\mathbf{0}$, il n'est pas possible d'observer la provenance des transitions \xrightarrow{b} : on ne peut distinguer par un contexte une transition \xrightarrow{b} provenant de $!b.\mathbf{0}$ d'une transition \xrightarrow{b} provenant des copies de $b.\mathbf{0}$ dans $R\{b.\mathbf{0}/X\}$. Le processus $!b.\mathbf{0}$ masque donc les différences entre $R\{\mathbf{0}/X\}$ et $R\{b.\mathbf{0}/X\}$. Les processus P_1 et P_2 sont donc en congruence barbue forte alors que nous avons $P_1 \not\sim P_2$.

La bisimilarité d'ordre supérieur, qui exige la bisimilarité des messages, est donc trop discriminante pour $\text{HO}\pi$: elle distingue des processus reliés par la congruence barbue. Il existe cependant des calculs pour lesquels la bisimilarité d'ordre supérieur caractérise la congruence barbue, comme par exemple le calcul HOP étudié dans ce document (chapitre 3).

2.2.3 Bisimilarité contextuelle

Dans le cas d'une émission de message, la bisimilarité d'ordre supérieur sépare message et continuation. Sangiorgi propose au contraire de les étudier ensemble, permettant notamment de mieux traiter leurs possibles interactions ainsi que les noms restreints qu'ils partagent. Son approche est de faire réagir une émission de message avec une réception, et de considérer le résultat de la communication dans les étapes de bisimulation. La bisimilarité ainsi obtenue est dite *contextuelle* car elle explicite les interactions possibles avec le contexte dans le cas d'une émission ou d'une réception.

Définition 2.10. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle forte précoce ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F' telle que $Q \xrightarrow{a} F'$ et $F \bullet C \mathcal{R} F' \bullet C$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C' telle que $Q \xrightarrow{\bar{a}} C'$, et $F \bullet C \mathcal{R} F \bullet C'$.

La relation \mathcal{R} est une bisimulation contextuelle forte précoce si et seulement si \mathcal{R} et \mathcal{R}^{-1} sont des simulations contextuelles fortes précoces. La bisimilarité contextuelle forte précoce \sim est la plus grande bisimulation contextuelle forte précoce.

La relation est dite *précoce* car le contexte de test (la concrétion C dans le cas de la réception ou la fonction F dans le cas de l'émission) est choisi avant que la réponse de Q ne soit donnée. La transition de Q dépend donc du contexte choisi : deux concrétions différentes peuvent engendrer deux transitions $Q \xrightarrow{a} F$ différentes dans le cas de la réception. Nous pouvons également définir une bisimilarité telle que les réponses de Q soient indépendantes des contextes choisis ; il suffit pour cela d'inverser l'ordre des quantifications.

Définition 2.11. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle forte tardive ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, il existe F' telle que $Q \xrightarrow{a} F'$ et pour tout C , on a $F \bullet C \mathcal{R} F' \bullet C$;
- pour tout $P \xrightarrow{\bar{a}} C$, il existe C' telle que $Q \xrightarrow{\bar{a}} C'$, et pour tout F , on a $F \bullet C \mathcal{R} F \bullet C'$.

La relation \mathcal{R} est une bisimulation contextuelle forte tardive si et seulement si \mathcal{R} et \mathcal{R}^{-1} sont des simulations contextuelles fortes tardives. La bisimilarité contextuelle forte tardive \sim_l est la plus grande bisimulation contextuelle forte tardive.

Dans le cas tardif, la réponse doit convenir quel que soit le contexte de test ; la condition est plus contraignante que dans le cas précoce, où la réponse ne doit convenir que pour le contexte dont elle dépend. Nous avons donc $\sim_l \subseteq \sim$. L'inclusion inverse n'est pas vraie en général ; par exemple en π -calcul [45], il existe des processus qui sont en bisimulation précoce mais pas en bisimulation tardive. Nous verrons que pour $\text{HO}\pi$, les deux relations coïncident.

Reprenons un des exemples de la section précédente

$$P_1 \triangleq \bar{a}\langle \mathbf{0} \rangle !b.\mathbf{0} \quad P_2 \triangleq \bar{a}(b.\mathbf{0}) !b.\mathbf{0}$$

Nous allons montrer que nous avons $P_1 \sim_l P_2$, en prouvant que la relation

$$\mathcal{R} \triangleq \{(R\{b.\mathbf{0}/X\} \mid !b.\mathbf{0}, R\{\mathbf{0}/X\} \mid !b.\mathbf{0})\}$$

est une bisimulation contextuelle forte tardive. Soit

$$P_{1,R} \triangleq R\{\mathbf{0}/X\} \mid !b.\mathbf{0}, P_{2,R} \triangleq R\{b.\mathbf{0}/X\} \mid !b.\mathbf{0}.$$

Nous montrons que $P_{1,R}$ répond aux transitions de $P_{2,R}$ modulo congruence structurale, en faisant une analyse de cas sur les types de transitions possibles de $P_{2,R}$:

- Transitions provenant de R ne faisant pas intervenir les processus $b.\mathbf{0}$; nous avons $P_{2,R} \xrightarrow{\alpha} A\{b.\mathbf{0}/X\} \mid !b.\mathbf{0}$ avec $R \xrightarrow{\alpha} A$. Nous avons alors également $P_{1,R} \xrightarrow{\alpha} A\{\mathbf{0}/X\} \mid !b.\mathbf{0}$. Nous traitons uniquement le cas de la concrétion $R \xrightarrow{\bar{a}} A = \nu\tilde{c}.\langle Q_1 \rangle Q_2$. Pour toute fonction F , nous avons

$$\begin{aligned} F \bullet A\{b.\mathbf{0}/X\} \mid !b.\mathbf{0} &= \nu\tilde{c}.(F \circ Q_1\{b.\mathbf{0}/X\} \mid Q_2\{b.\mathbf{0}/X\}) \mid !b.\mathbf{0} \\ &= (\nu\tilde{c}.(F \circ Q_1 \mid Q_2))\{b.\mathbf{0}/X\} \mid !b.\mathbf{0} \triangleq P_3 \\ F \bullet A\{\mathbf{0}/X\} \mid !b.\mathbf{0} &= (\nu\tilde{c}.(F \circ Q_1 \mid Q_2))\{\mathbf{0}/X\} \mid !b.\mathbf{0} \triangleq P_4 \end{aligned}$$

Nous avons $P_3 \mathcal{R} P_4$, comme souhaité.

- Transition \xrightarrow{b} d'un processus substitué $b.\mathbf{0}$, ou synchronisation entre un processus substitué $b.\mathbf{0}$ et une partie de R ; nous traitons ce dernier cas, le premier étant plus simple. Nous avons alors

$$P_{2,R} \xrightarrow{\tau} R'\{\mathbf{0}/X_0\}\{b.\mathbf{0}/X\} \mid !b.\mathbf{0} \triangleq P_3$$

avec $R \xrightarrow{\bar{b}} R'$; le processus $b.\mathbf{0}$ à la position X_0 se synchronise avec R . Nous considérons la transition

$$P_{1,R} \xrightarrow{\tau} R'\{\mathbf{0}/X_0\}\{\mathbf{0}/X\} \mid !b.\mathbf{0} \triangleq P_4$$

qui provient de la synchronisation de R avec une copie de $b.\mathbf{0}$ fournie par $!b.\mathbf{0}$. Toutes les instances de X sont remplacées par $\mathbf{0}$ dans P_4 , et en particulier l'instance X_0 ; nous l'exhibons pour montrer que nous avons bien $P_3 \mathcal{R} P_4$.

- Transition \xrightarrow{b} du processus répliqué $!b.\mathbf{0}$, ou synchronisation entre $!b.\mathbf{0}$ et une partie de R ; ce cas est similaire au précédent.

De la même manière, nous pouvons montrer que $P_{2,R}$ répond aux transitions de $P_{1,R}$. La relation \mathcal{R} est donc une bisimulation contextuelle forte tardive.

Nous donnons maintenant les résultats qui font de la bisimilarité contextuelle une équivalence intéressante.

Théorème 2.1. *Les relations \sim et \sim_l sont des congruences.*

Nous esquissons la preuve de ce résultat dans le chapitre 4, dans lequel nous étudions les différentes méthodes de preuve de congruence. En conséquence de ce théorème, et comme nous avons $P \downarrow_\gamma$ si et seulement si $P \xrightarrow{\gamma}$, nous avons le résultat suivant.

Corollaire 2.1. *Nous avons $\sim \subseteq \sim_b$.*

La bisimilarité est dite *correcte* par rapport à la congruence barbue. Nous pouvons également en déduire le résultat suivant, qui permet de simplifier les preuves de bisimilarité pour les processus préfixés.

Lemme 2.1. *Pour tout γ , et pour tout processus clos P, Q , nous avons $\gamma.P \sim \gamma.Q$ ssi $P \sim Q$ (de même pour \sim_l).*

L'implication suffisante est une conséquence directe du théorème 2.1. Nous donnons la preuve de l'implication inverse pour $\bar{a}.P \sim \bar{a}.Q$. Nous avons $\bar{a}.P \xrightarrow{\bar{a}} \langle \mathbf{0} \rangle P$. Soit $F = (X)\mathbf{0}$. Le processus $\bar{a}.Q$ ne peut répondre que par $\bar{a}.Q \xrightarrow{\bar{a}} \langle \mathbf{0} \rangle Q$, et nous avons $F \bullet \langle \mathbf{0} \rangle P \sim$

$F \bullet \langle 0 \rangle Q$, c'est-à-dire $P \sim Q$, comme souhaité. Par la suite, nous écrirons simplement les transitions des processus préfixés $\gamma.P \xrightarrow{\gamma} P$, et nous nous servirons implicitement du lemme 2.1 pour les preuves de bisimilarité.

Nous montrons maintenant que la bisimilarité contextuelle est *complète* par rapport à la congruence barbue, c'est-à-dire que nous avons le résultat suivant :

Théorème 2.2. *Nous avons $\sim_b \subseteq \sim$.*

Ainsi, la bisimilarité contextuelle forte précoce caractérise la congruence barbue forte. Nous esquissons la méthode de preuve, qui est la même que pour le π -calcul [45]. Nous définissons une famille de relations \sim_k , k entier, qui différencie les niveaux de bisimilarité. Nous avons $P \sim_k Q$ si et seulement si P imite Q sur les premières k transitions. Plus précisément, nous notons \sim_0 la relation universelle sur les processus, et nous avons $P \sim_k Q$ si et seulement si :

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \sim_{k-1} Q'$, et inversement pour tout $Q \xrightarrow{\tau} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F' telle que $Q \xrightarrow{a} F'$ et $F \bullet C \sim_{k-1} F' \bullet C$, et inversement pour tout $Q \xrightarrow{a} F$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et $F \bullet C \sim_{k-1} F \bullet C'$, et inversement pour tout $Q \xrightarrow{\bar{a}} C$.

Nous prouvons ensuite que $\cap_k \sim_k = \sim$, en nous appuyant sur la propriété suivante du système de transitions.

Lemme 2.2. *Pour tout P, α , l'ensemble $\{A, P \xrightarrow{\alpha} A\}$ est fini.*

Le système de transitions est dit à *image finie*. Par induction sur k , nous montrons alors que $P \sim_k Q$ implique l'existence d'un contexte \mathbb{C}_k tel que $\mathbb{C}_k\{P\} \sim_b \mathbb{C}_k\{Q\}$. Nous montrons alors la contraposée du théorème 2.2. Si $P \not\sim Q$, alors il existe k tel que $P \not\sim_k Q$, et donc il existe un contexte \mathbb{C} tel que $\mathbb{C}\{P\} \not\sim_b \mathbb{C}\{Q\}$. Par conséquent P et Q ne sont pas en congruence barbue.

Remarque 2.5. *Pour les calculs dans lesquels les bisimilarités précoce et tardive sont différentes, la bisimilarité tardive est généralement trop discriminante et n'est donc pas complète par rapport à la congruence barbue. On cherche donc à caractériser la congruence barbue par une bisimilarité précoce.*

Nous donnons maintenant les définitions et résultats pour le cas faible. Nous rappelons que \Rightarrow est la clôture réflexive et transitive de $\xrightarrow{\tau}$, et pour toute action γ , nous notons $\xRightarrow{\gamma}$ pour $\Rightarrow \xrightarrow{\gamma}$. Ce type de transitions, sans action interne après l'action visible, est qualifié de *semi-faible*. Les étapes d'ordre supérieur engendrent des fonctions et concrétions, qui ne peuvent évoluer par elles-mêmes. Les bisimilarités semi-faibles ne sont généralement pas complètes par rapport à la congruence barbue faible. Nous ajoutons donc des étapes internes après une action visible dans nos définitions de bisimilarités faibles.

Définition 2.12. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle faible précoce ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \Rightarrow Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F', Q' tels que $Q \xRightarrow{a} F'$, $F' \bullet C \Rightarrow Q'$ et $F \bullet C \mathcal{R} Q'$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C', Q' tels que $Q \xRightarrow{\bar{a}} C'$, $F \bullet C' \Rightarrow Q'$ et $F \bullet C \mathcal{R} Q'$.

La relation \mathcal{R} est une bisimulation contextuelle faible précoce si et seulement si \mathcal{R} et \mathcal{R}^{-1} sont des simulations contextuelles faibles précoces. La bisimilarité contextuelle faible précoce \approx est la plus grande bisimulation contextuelle faible précoce.

La version tardive \approx_l de la relation s'obtient en remplaçant les clauses d'ordre supérieur de la définition 2.12 par :

- pour tout $P \xrightarrow{a} F$, il existe F' telle que $Q \xrightarrow{a} F'$ et pour tout C , il existe Q' tel que $F' \bullet C \Rightarrow Q'$ et $F \bullet C \mathcal{R} Q'$;
- pour tout $P \xrightarrow{\bar{a}} C$, il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et pour tout F , il existe Q' tel que $F \bullet C' \Rightarrow Q'$ et $F \bullet C \mathcal{R} Q'$.

Les bisimilarités faibles ainsi définies sont correctes par rapport à la congruence barbue faible.

Théorème 2.3. *Nous avons $\approx \subseteq \approx_b$ et $\approx_l \subseteq \approx_b$.*

La méthode de preuve est la même que pour le cas fort. La complétude reste un problème ouvert : la preuve de complétude utilisée pour le cas fort ne permet pas de conclure dans le cas faible. En effet, les transitions faibles ne sont pas à image finie. Par exemple, pour $P \triangleq !(a.0 \mid \bar{a}.b.0)$, nous avons $P \Rightarrow b.0 \mid \dots b.0 \mid P$ avec k copies de $b.0$ pour tout k . Comme pour le π -calcul, nous pouvons cependant conclure sur les processus à image finie.

Définition 2.13. *Un processus P est à image finie ssi*

- l'ensemble $\{P', P \Rightarrow P'\}$ est fini;
- pour tout C , l'ensemble $\{P', \exists F, P \xrightarrow{a} F \wedge F \bullet C \Rightarrow P'\}$ est fini;
- pour tout F , l'ensemble $\{P', \exists C, P \xrightarrow{\bar{a}} C \wedge F \bullet C \Rightarrow P'\}$ est fini.

Nous pouvons alors prouver la complétude sur les processus à image finie en utilisant la même technique que pour le cas fort.

Théorème 2.4. *Pour tout P, Q à image finie, $P \approx_b Q$ implique $P \approx Q$.*

La bisimilarité contextuelle permet donc de caractériser la congruence barbue de manière coinductive. On peut néanmoins se demander si une telle relation est réellement plus simple à manipuler que la congruence barbue. En effet, on remplace une quantification universelle sur tous les contextes par une quantification sur les contextes interagissant avec les processus à comparer (une concrétion dans le cas d'une réception ou une fonction dans le cas d'une émission). La définition d'une bisimilarité contextuelle doit être vue comme une première étape, qui peut servir de base à des techniques de preuve permettant de simplifier les relations candidates (techniques modulo [36, 38, 32]), ou à la définition de relations plus simples, comme les bisimilarités normales.

2.2.4 Bisimilarité normale

La bisimilarité normale améliore la bisimilarité contextuelle faible en ne considérant qu'un seul agent de test pour chaque action d'ordre supérieur. Cette relation repose sur un encodage de HO π dans un calcul de premier ordre, qui illustre d'une certaine manière le peu de possibilités laissées par le calcul dans la manipulation des messages. Un processus P reçu peut être détruit, dupliqué ou transmis, une ou plusieurs fois, immédiatement ou après un certain nombre de transitions. Tous ces comportements peuvent être simulés en remplaçant P par un nom, utilisé pour déclencher l'exécution d'une copie de P au moment voulu. Formellement, Sangiorgi prouve le résultat suivant, appelé *théorème de factorisation*.

Théorème 2.5. *Pour tout agent A et processus P tels que $a \notin \text{fn}(A, P)$, nous avons $A\{P/X\} \approx_l \nu a.(A\{\bar{a}.0/X\} \mid !a.P)$.*

La preuve de ce résultat se trouve dans [42]. Le théorème de factorisation remplace chaque copie de P dans A par un déclencheur $\bar{a}.0$, qui peut activer une copie de P à tout moment grâce au processus associé $!a.P$. La bisimulation normale exploite cette mise sous forme normale des processus dans la définition de ses clauses.

Définition 2.14. *Une relation \mathcal{R} sur les processus clos est une simulation normale si et seulement si $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \Rightarrow Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout nom frais b , il existe F', Q' tels que $Q \xrightarrow{a} F'$, $F' \circ \bar{b}.0 \Rightarrow Q'$ et $F \circ \bar{b}.0 \mathcal{R} Q'$;
- pour tout $P \xrightarrow{\bar{a}} \nu \tilde{c}. \langle R \rangle S$, pour tout nom frais b , il existe $\nu \tilde{c}'. \langle R' \rangle S', Q'$ tels que $Q \xrightarrow{\bar{a}} \nu \tilde{c}'. \langle R' \rangle S'$, $\nu \tilde{c}'. (S' \mid !b.R') \Rightarrow Q'$ et $\nu \tilde{c}. (S \mid !b.R) \mathcal{R} Q'$.

La relation \mathcal{R} est une bisimulation normale ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations normales. La bisimilarité normale \approx_n est la plus grande bisimulation normale.

Il faut souligner que pour les actions d'ordre supérieur, le résultat de la comparaison des fonctions et concrétions est indépendant du nom choisi. Dans le cas de la réception, les fonctions sont testées avec seulement un déclencheur ; dans le cas de l'émission, les messages R, R' sont rendus disponibles sur un nom b . La bisimilarité normale ainsi définie caractérise la bisimilarité contextuelle faible, et donc la congruence barbue faible.

Théorème 2.6. *Nous avons $\approx_l = \approx_n$.*

Pour prouver ce résultat, Sangiorgi [42] traduit les processus de $\text{HO}\pi$ en processus déclenchés, dans lesquels seuls des déclencheurs $\bar{b}.0$ peuvent être émis. Sur les processus déclenchés, les bisimulations contextuelles et normales coïncident, et le théorème de factorisation permet de relier par \approx un processus à sa traduction déclenchée. Jeffrey et Rathke [21] utilisent la même méthode pour définir une bisimilarité normale correcte et complète dans une version concurrente de ML.

Dans la preuve de Sangiorgi, le théorème de factorisation (et donc le théorème 2.6) est une conséquence de la congruence de \approx . Il est possible de procéder de manière différente : dans [30], Li prouve d'abord le théorème de factorisation en comparant les transitions de $P\{R/X\}$ et de sa version factorisée, et en déduit ensuite la congruence de \approx . En utilisant des processus et transitions indexés, Cao [9] fait une analyse plus fine de la provenance des transitions de $P\{R/X\}$ et de sa version factorisée, ce qui lui permet de prouver le théorème de factorisation dans le cas fort et d'en déduire une bisimilarité normale forte.

La bisimilarité normale peut être définie dans le calcul $\text{HO}\pi$ d'ordre quelconque, dans lequel des fonctions peuvent être émises en plus des processus. Par exemple, la fonction $F \triangleq (X)X \circ Q$ attend une fonction en argument et l'applique au processus Q . Sangiorgi [41] définit une bisimilarité normale en s'appuyant sur le *type* des fonctions ; par exemple si \star est le type de tous les processus, alors F a pour type $(\star \rightarrow \star) \rightarrow \star$. Jeffrey et Rathke [22] ont étendu ce résultat aux types récursifs.

Remarque 2.6. *Du théorème 2.6, nous pouvons déduire l'égalité des bisimilarités précoce et tardive. Nous avons $\approx_l \subseteq \approx \subseteq \approx_n$ par définition, et nous avons $\approx_n \subseteq \approx_l$ par le théorème 2.6.*

2.3 Équivalences dans les calculs avec passivation

Nous allons maintenant étudier la théorie comportementale des calculs avec passivation tels que Homer [19] et le Kell [47]. Plutôt que de travailler dans un des ces deux formalismes, nous définissons un calcul plus simple, appelé $\text{HO}\pi\text{P}$ [28], qui étend $\text{HO}\pi$ avec un opérateur de passivation. De cette manière, nous évitons les particularités superfétatoires de chaque calcul (principalement le contrôle additionnel des communications), et nous pouvons comparer les bisimulations entre $\text{HO}\pi$ et $\text{HO}\pi\text{P}$.

2.3.1 Syntaxe et sémantique de $\text{HO}\pi\text{P}$

Nous ajoutons des unités de passivation $a[P]$, appelées *localités*, aux constructions de $\text{HO}\pi$. En utilisant les mêmes notations que pour $\text{HO}\pi$, la syntaxe du calcul est la suivante :

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

Tant que la passivation n'est pas déclenchée, une localité $a[P]$ est un contexte d'évaluation transparent : le processus P peut se réduire et communiquer librement avec des processus à l'extérieur de a . À n'importe quel moment, la passivation peut se déclencher et la localité $a[P]$ devient une concrétion $\langle P \rangle \mathbf{0}$. La passivation se traduit alors par une action interne τ seulement s'il existe un récepteur sur a capable de recevoir le contenu de la localité.

Remarque 2.7. *Le récepteur $a(X)P$ est utilisé pour la communication d'ordre supérieur et pour la passivation. Contrairement à Homer et au Kell, nous n'introduisons pas de récepteur spécifique à la passivation, afin de garder la définition du calcul $\text{HO}\pi P$ la plus simple possible.*

Nous étendons les localités à tous les agents : si $F = (X)P$, alors $a[F] \triangleq (X)a[P]$; si $C = \nu \tilde{b}. \langle Q \rangle R$, alors $a[C] \triangleq \nu \tilde{b}. \langle Q \rangle a[R]$. Nous obtenons le système de transitions étiquetées de $\text{HO}\pi P$ en ajoutant les règles suivantes à celles de $\text{HO}\pi$ (figure 2.1).

$$\frac{P \xrightarrow{\alpha} A}{a[P] \xrightarrow{\alpha} a[A]} \quad \text{LOC} \qquad a[P] \xrightarrow{\bar{a}} \langle P \rangle \mathbf{0} \quad \text{PASSIV}$$

Notez que l'extension de la localité aux concrétions et la règle LOC impliquent que la portée des noms restreints peut traverser les limites de localités. Comme pour $\text{HO}\pi$, l'extension de portée est paresseuse ; par exemple, nous avons

$$a[\nu bc. \bar{d} \langle b. \mathbf{0} \rangle c. \mathbf{0}] \mid d(X)X \xrightarrow{\tau} \nu b. (a[\nu c. c. \mathbf{0}] \mid b. \mathbf{0})$$

La portée du nom b est étendue à l'extérieur de a , alors que celle de c reste incluse dans a .

Dans les calculs avec passivation (plus généralement, dans les calculs distribués autorisant la duplication de localités, par exemple le Seal [54]), la politique choisie pour l'extension de portée (paresseuse ou systématique, traversant les localités ou non) a une influence importante sur la sémantique opérationnelle. En particulier, de tels calculs interdisent généralement la règle de congruence structurelle des Ambients [10] $a[\nu b. P] \equiv \nu b. a[P]$. Avec cette règle, deux processus en congruence structurelle pourraient ne pas être en congruence barbue. Par exemple, soit $Q \triangleq a[\nu b. P] \mid a(X)(X \mid X)$. En déclenchant la passivation, nous obtenons $Q \xrightarrow{\tau} (\nu b. P) \mid (\nu b. P) \triangleq Q_1$. Si la portée de b pouvait être étendue à l'extérieur de a par congruence structurelle, nous aurions $Q \equiv \nu b. (a[P] \mid a(X)(X \mid X)) \xrightarrow{\tau} \nu b. (P \mid P) \triangleq Q_2$. Dans le processus Q_1 , chaque instance de P a sa propre copie de b , alors que dans Q_2 , les deux instances de P partagent le même nom b . Avec un processus P bien choisi, comme par exemple $P \triangleq \bar{b}. \mathbf{0} \mid b. b. c. \mathbf{0}$, nous pouvons observer des barbes différentes. En effet, dans le premier cas, nous avons

$$Q_1 = (\nu b. (\bar{b}. \mathbf{0} \mid b. b. c. \mathbf{0})) \mid (\nu b. (\bar{b}. \mathbf{0} \mid b. b. c. \mathbf{0})) \xrightarrow{\tau} \xrightarrow{\tau} (\nu b. b. c. \mathbf{0}) \mid (\nu b. b. c. \mathbf{0})$$

Aucune autre transition n'est possible et le nom c n'est pas observable. En revanche, nous obtenons dans le second cas

$$Q_2 = \nu b. (\bar{b}. \mathbf{0} \mid \bar{b}. \mathbf{0} \mid b. b. c. \mathbf{0} \mid b. b. c. \mathbf{0}) \xrightarrow{\tau} \xrightarrow{\tau} \nu b. (c. \mathbf{0} \mid b. b. c. \mathbf{0})$$

Le nom c est observable.

Remarque 2.8. *L'extension de portée choisie pour $\text{HO}\pi P$ (paresseuse et traversant les localités) est la même que celle de Homer ou du Kell.*

2.3.2 Bisimilarité contextuelle

Nous cherchons maintenant à obtenir une caractérisation de la congruence barbue sur le modèle de la bisimilarité contextuelle de $\text{HO}\pi$. Les observables de $\text{HO}\pi P$ sont les noms et co-noms sur lesquels une communication ou une passivation peut avoir lieu. Les définitions de congruences barbues \sim_b et \approx_b sont les mêmes que pour $\text{HO}\pi$ (définition 2.7).

Remarque 2.9. *Tout au long de ce document, nous allons définir de nombreux calculs, et les équivalences comportementales associées. Plutôt que de définir une nouvelle notation pour chaque calcul, nous réutilisons les mêmes notations que pour $HO\pi$. Ainsi, les notations \sim_b et \approx_b désignent les congruences barbues forte et faible du calcul considéré ; \sim et \approx désignent les bisimilarités contextuelles fortes précoces, etc.*

Nous faisons d'abord remarquer que reprendre la définition de bisimilarité contextuelle de $HO\pi$ (définition 2.10) donne une relation qui n'est pas correcte par rapport à la congruence barbue dans $HO\pi P$. En effet, nous avons vu en section 2.2.3 que la bisimilarité contextuelle forte de $HO\pi$ relie les processus suivants

$$P_1 = \bar{a}(\mathbf{0})!b.\mathbf{0} \quad P_2 = \bar{a}(b.\mathbf{0})!b.\mathbf{0}$$

Or ces processus ne sont pas en congruence barbue en $HO\pi P$. Le contexte $\mathbb{C} \triangleq c[\square] \mid a(X)X \mid c(X)\mathbf{0}$ les distingue. Nous avons $\mathbb{C}\{P_1\} \xrightarrow{\tau} c[!b.\mathbf{0}] \mid \mathbf{0} \mid c(X)\mathbf{0} \triangleq P_3$ par communication sur a . Le processus $\mathbb{C}\{P_2\}$ ne peut répondre que par $\mathbb{C}\{P_2\} \xrightarrow{\tau} c[!b.\mathbf{0}] \mid b.\mathbf{0} \mid c(X)\mathbf{0} \triangleq P_4$. En déclenchant la passivation sur c , nous obtenons $P_3 \xrightarrow{\tau} \mathbf{0}$ et $P_4 \xrightarrow{\tau} b.\mathbf{0}$. Les deux processus résultants ne sont pas en congruence barbue.

Dans une concrétion $\nu\tilde{a}.\langle R \rangle S$, le message R peut être envoyé à l'extérieur d'une localité c alors que la continuation S reste dans c . Si la passivation sur c est déclenchée, la continuation S peut être détruite (comme cela se produit avec $\mathbb{C}\{P_1\}$ et $\mathbb{C}\{P_2\}$) ou être placée dans un contexte différent. Ainsi la passivation peut séparer les processus R et S et les placer dans des contextes différents, ce qui n'est pas possible dans un calcul sans passivation. Nous réglons ce problème de la même manière que Homer ou le Kell, en testant messages et continuations dans des *contextes d'évaluation* \mathbb{E} différents. Ces contextes, appliqués à une concrétion, prennent en compte la séparation entre un message et sa continuation : dans la définition de $a[C]$ pour une concrétion C , le message de C est sorti de la localité a , alors que la continuation reste à l'intérieur. La grammaire des contextes d'évaluation de $HO\pi P$ est la suivante :

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

Nous appelons ces contextes utilisés à des fins d'observation (et non pour la sémantique) des *contextes de bisimulation*. Nous définissons la bisimilarité contextuelle forte précoce pour $HO\pi P$ de la manière suivante :

Définition 2.15. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle forte précoce ssi $P \mathcal{R} Q$ implique $\text{fn}(P) = \text{fn}(Q)$ et :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F' telle que $Q \xrightarrow{a} F'$ et $F \bullet C \mathcal{R} F' \bullet C$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et pour tout \mathbb{E} , nous avons $F \bullet \mathbb{E}\{C\} \mathcal{R} F \bullet \mathbb{E}\{C'\}$.

La relation \mathcal{R} est une bisimulation contextuelle forte précoce si et seulement si \mathcal{R} et \mathcal{R}^{-1} sont des simulations contextuelles fortes précoces. La bisimilarité contextuelle forte précoce \sim est la plus grande bisimulation contextuelle forte précoce.

Cette définition est semblable à celles des bisimilarités contextuelles de Homer [19] et du Kell [47] (sauf que les contextes \mathbb{E} sont également utilisés dans le cas de la réception). La condition $\text{fn}(P) = \text{fn}(Q)$ est nécessaire à cause de l'extension de portée paresseuse à l'extérieur des localités, qui permet de distinguer deux processus avec des noms libres différents. Par exemple, un processus P bloqué mais avec un nom libre b (par exemple $\nu a.a.b.\mathbf{0}$) peut être distingué de $\mathbf{0}$ par un contexte $\mathbb{C} = c[\nu b.\bar{d}(\square)R] \mid d(X)c(Y)(Y \mid Y)$. Nous avons $\mathbb{C}\{P\} \xrightarrow{\tau} \nu b.(R \mid R)$ et $\mathbb{C}\{\mathbf{0}\} \xrightarrow{\tau} \nu b.R \mid \nu b.R$ par communication sur d suivie par une passivation sur c . Avec un processus R bien choisi, les deux processus obtenus peuvent avoir des transitions différentes, comme nous l'avons vu dans la sous section précédente.

Remarque 2.10. *On peut imaginer tester les concrétions avec une localité $F \bullet b[C]$, avec b frais, plutôt que de tester avec des contextes de bisimulation $F \bullet \mathbb{E}\{C\}$. Les deux tests ne diffèrent qu'au niveau de la capture des noms de C , permise dans le cas des contextes, et impossible dans le cas de localité. Ainsi, pour une concrétion $C = \nu \tilde{a}. \langle R \rangle S$, nous avons $F \bullet b[C] \mid b(X)Q \xrightarrow{\tau} \nu \tilde{a}. (F \circ R \mid Q\{S/X\})$ par passivation de b . Les noms libres de S ne peuvent être capturés dans $Q\{S/X\}$, alors qu'ils peuvent l'être dans $\mathbb{E}\{S\}$. Les contextes \mathbb{E} peuvent également capturer les noms libres de R . Autoriser la capture rend les preuves sur \sim plus simples; nous ne savons pas si tester des contextes sans capture est suffisant pour avoir la complétude.*

La bisimilarité contextuelle forte précoce caractérise la congruence barbue forte.

Théorème 2.7. *Nous avons $\sim = \sim_b$.*

Nous étudions les preuves de congruence dans le chapitre 4. La preuve de complétude suit le même principe que celle de $\text{HO}\pi$ (théorème 2.2). Nous donnons maintenant la définition dans le cas faible.

Définition 2.16. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle faible précoce ssi $P \mathcal{R} Q$ implique $\text{fn}(P) = \text{fn}(Q)$:*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \Rightarrow Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F', Q' tels que $Q \xRightarrow{a} F'$, $F' \bullet C \Rightarrow Q'$ et $F \bullet C \mathcal{R} Q'$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C' telle que $Q \xRightarrow{\bar{a}} C'$ et pour tout \mathbb{E} , il existe Q' tel que $F \bullet \mathbb{E}\{C'\} \Rightarrow Q'$ et $F \bullet C \mathcal{R} Q'$.

La relation \mathcal{R} est une bisimulation contextuelle faible précoce si et seulement si \mathcal{R} et \mathcal{R}^{-1} sont des simulations contextuelles faibles précoces. La bisimilarité contextuelle faible précoce \approx est la plus grande bisimulation contextuelle faible précoce.

Pour Homer comme pour le Kell, il n'existe pas de résultat de correction pour une bisimilarité contextuelle faible similaire à la définition 2.16. Nous verrons dans le chapitre 4 pourquoi les principales techniques de preuve de correction échouent avec la bisimilarité contextuelle faible.

2.4 État de l'art et conclusions

Nous présentons ici rapidement quelques calculs d'ordre supérieur et leurs résultats en matière de caractérisation de la congruence barbue. Nous mentionnons également une forme de bisimilarité proposée récemment pour les calculs d'ordre supérieur, la bisimilarité environnementale.

2.4.1 Le calcul minimal HOCORE

Le calcul HOCORE [23] est un calcul minimal ne comportant que les opérateurs nécessaires pour exprimer la communication asynchrone d'ordre supérieur, c'est-à-dire la réception de message, l'émission (sans continuation) et la composition parallèle. Malgré l'absence d'opérateurs tels que la restriction et la réplication, HOCORE est Turing complet, et la terminaison est indécidable.

Les bisimilarités vues dans ce chapitre (d'ordre supérieur, contextuelle et normale) ont été adaptées pour HOCORE , ainsi que la bisimilarité *ouverte*, qui relie les processus ouverts sans instanciation des variables, et la bisimilarité *d'entrée sortie*, qui ne comporte pas de clause pour les actions internes τ . La particularité de ce calcul est que ces différentes formes de bisimilarités coïncident et caractérisent la congruence barbue. Cela s'explique par le fait que la congruence barbue est très contraignante pour ce calcul, puisqu'elle correspond à

la congruence structurelle, étendue avec la loi suivante, dite de *distribution*

$$a(X)(P \mid \prod_{i=1}^{k-1} a(X)P) \equiv \prod_{i=1}^k a(X)P$$

où $\prod_1^k P$ désigne la composition parallèle des k processus P . Il est donc possible d'axiomatiser l'équivalence de processus en HOcore.

Lanese et coll. ont également montré que la bisimilarité forte de HOcore est décidable. En revanche, il suffit de rajouter quatre restrictions englobantes (à la racine des termes) pour que la bisimilarité devienne indécidable. La plupart de ces résultats restent valides en ajoutant une continuation aux émissions de message. Les résultats obtenus ne concernent que la bisimilarité forte ; aucun résultat n'est connu pour la bisimilarité faible. De même le problème de la décidabilité en présence de réplication reste ouvert.

2.4.2 Les calculs CHOCS et Plain CHOCS

Les calculs CHOCS et Plain CHOCS, proposés par Thomsen [51, 52], sont des calculs d'ordre supérieur similaires à $\text{HO}\pi$. Le calcul CHOCS diffère de Plain CHOCS par la gestion de la restriction. En CHOCS, la restriction est dite *dynamique* : un nom peut échapper à son lieu dans le cas d'une émission, et un nom peut être capturé lors d'une réception. Par exemple, dans la transition $(\nu a.\bar{b}\langle a.\mathbf{0} \rangle a.\mathbf{0}) \mid b(X)X \xrightarrow{\tau} (\nu a.a.\mathbf{0}) \mid a.\mathbf{0}$, le nom a dans le message échappe à son lieu et devient libre, alors que le nom a de la continuation reste lié. De même, dans $\bar{b}\langle a.\mathbf{0} \rangle \mathbf{0} \mid b(X)\nu a.X \xrightarrow{\tau} \nu a.a.\mathbf{0}$, le nom a est capturé et devient lié.

Par contre, la sémantique de Plain CHOCS est la même que $\text{HO}\pi$: les noms ne peuvent échapper à leur lieu et aucune capture ne peut avoir lieu lors d'une réception. La restriction est dite alors *statique* : les noms restreints ne peuvent pas changer de lieu. Thomsen définit une bisimilarité d'ordre supérieur pour ces deux calculs. Une telle relation est bien adaptée à CHOCS et à sa restriction dynamique. En revanche, nous avons vu en section 2.2.2 qu'elle est trop discriminante pour les calculs à restriction statique tels que $\text{HO}\pi$, Plain CHOCS et les calculs définis plus récemment.

2.4.3 Les Ambients

Les Ambients [10] est un calcul distribué avec localités hiérarchisées appelées *ambients*. Les ambients représentent des unités de calcul qui peuvent être incluses les unes dans les autres et se déplacer dans la hiérarchie de localités par elles-mêmes. Les ambients évoluent en exerçant trois types de *capacités*. Un ambient peut entrer dans un autre ambient $m[\text{in } n.P] \mid n[Q] \xrightarrow{\tau} n[m[P] \mid Q]$, sortir d'un ambient $m[n[\text{out } m.P] \mid Q] \xrightarrow{\tau} m[Q] \mid n[P]$, ou détruire la frontière d'un ambient $\text{open } m.P \mid m[Q] \xrightarrow{\tau} P \mid Q$. Notez que l'évolution des ambients ne nécessite pas de synchronisation avec un autre terme ; la mobilité est dite *subjective*.

De nombreux travaux ont portés sur la définition d'un système de transitions étiquetées et d'une bisimilarité associée afin de caractériser la congruence barbue des Ambients [32, 40, 5]. Par exemple dans [32], Merro et Zappa-Nardelli définissent des relations qui s'apparentent à la bisimilarité contextuelle de Sangiorgi (section 2.2.3). Par exemple, pour une action $m[\text{in } n.P] \xrightarrow{m.\text{enter } n}$ qui signifie que l'ambient m entre dans un ambient n , la bisimilarité a besoin d'un contexte de test $n[Q]$ pour compléter l'action considérée ; on obtient alors $m[\text{in } n.P] \xrightarrow{m.\text{enter } n} n[m[P] \mid Q]$. Des bisimilarités contextuelles forte et faible ont ainsi été définies, qui caractérisent une congruence barbue restreinte aux contextes d'évaluation.

Rathke et Sobociński [40] et Bonchi et coll. [5] cherchent à obtenir une définition systématique des systèmes de transitions étiquetées tels que la bisimilarité associée soit automatiquement une congruence. Les deux groupes ont appliqué leurs techniques différentes

aux Ambients et ont obtenu des systèmes de transitions étiquetées relativement similaires. Rathke et Sobociński obtiennent une caractérisation dans le cas fort, alors que Bonchi et coll. proposent des bisimilarités correctes et complètes dans les cas fort et faible. De nombreuses variantes des Ambients ont été proposées (par exemple les Safe Ambients[29], Secure Safe Ambients [7], Boxed Ambients [8] pour n'en citer que quelques unes), certaines pourvues de caractérisations de la congruence barbue par des bisimilarités, comme par exemple NBA [8]. Il n'existe pas à notre connaissance de bisimilarité normale pour les Ambients ou pour une de ses variantes.

2.4.4 Le Seal

Le Seal [54] est un calcul distribué avec localités hiérarchisées plus flexible que les Ambients sur la mobilité des localités. En effet, les localités peuvent être renommées, dupliquées ou détruites. La mobilité d'ordre supérieur nécessite l'interaction de trois processus : un processus émetteur $\bar{a}^{\eta_1}\{b\}.P$, un processus récepteur $a^{\eta_2}\{b_1, \dots, b_n\}.Q$ et la localité transférée $b[R]$. L'émetteur envoie le nom de la localité à transférer (ici b) ; le récepteur détruit la localité b pour la recréer n fois sous les noms $b_1 \dots b_n$ spécifiés. Si l'ensemble de noms du récepteur est vide $a^{\eta_2}\{ \}.Q$, la localité est définitivement détruite. Les directions η_1, η_2 ajoutent du contrôle sur les communications : la communication prend place si et seulement si les directions et les positions du récepteur par rapport à l'émetteur correspondent. Par exemple, dans $\bar{a}^c\{b\}.P \mid b[R] \mid c[a^\dagger\{d, e\}.Q]$, l'émetteur envoie le nom b à une localité fille c , alors que le récepteur dans c attend un message provenant du père ; les positions sont valides, la communication peut donc avoir lieu, et on obtient $\bar{a}^c\{b\}.P \mid b[R] \mid c[a^\dagger\{d, e\}.Q] \xrightarrow{\tau} P \mid c[Q \mid d[R] \mid e[R]]$. Dans le Seal, une localité peut traverser au plus une frontière de localité au cours d'une communication.

Dans [11], les auteurs définissent pour le Seal un système de transitions étiquetées et une bisimilarité contextuelle semi-faible associée². Le système de transitions proposé contient des étiquettes intermédiaires pour les processus partiellement synchronisés, c'est-à-dire les processus contenant un ou deux des trois termes nécessaires à une communication. Certaines de ces actions partielles ne sont pas observables par un contexte [12]. En effet, le processus $P \triangleq \nu a.(\bar{a}^*\{b\}.\mathbf{0} \mid a^*\{b\}.\mathbf{0})$ peut récupérer le contenu d'une localité b , pour le placer dans une localité portant le même nom b . Cette action ne peut pas être observée par un contexte : en présence d'une localité $b[Q]$, nous obtenons $P \mid b[Q] \xrightarrow{\tau} b[Q]$. Le processus P est donc en congruence barbue faible avec $\mathbf{0}$, alors qu'il peut se synchroniser partiellement selon le système de transitions de [11]. La bisimilarité distingue donc les processus P et $\mathbf{0}$, elle n'est donc pas complète.

2.4.5 Les calculs avec passivation

Bien que le Seal soit plus expressif que les Ambients, il n'est pas encore suffisamment expressif : il permet juste de renommer les copies des localités, pas d'en modifier le contenu. Par exemple, il est impossible d'étendre le contenu d'une localité $a[P]$ en $a[P \mid Q]$. Les calculs avec passivation tels que Homer [19] et le Kell [47] permettent entre autres ce genre de comportement. Les deux calculs diffèrent uniquement dans le contrôle des communications. En Homer, les messages ne peuvent que descendre dans la hiérarchie de localité, et les contenus de localité ne peuvent que remonter par passivation. Par exemple, dans $T \triangleq P \mid a[b[Q] \mid c[R] \mid S]$, le processus P peut envoyer un message à Q , R ou S , S peut envoyer un message à Q ou R mais pas à P , et les processus Q et R ne peuvent pas communiquer à l'extérieur de leur localité respective. De même le processus S peut passiver la localité b ou c , mais ne peut pas passiver une localité dans P . Pour qu'un message M passe de la localité b à c , il faut que Q contienne une localité avec pour corps M , que le processus S passive cette localité pour ensuite envoyer le message à R .

²appelée par les auteurs *hoe bisimilarity*, soit littéralement bisimilarité à binette

Les restrictions du Kell sont différentes. Toujours dans le processus T , P peut envoyer un message à S , S peut envoyer un message à P , Q , ou R : les messages traversent au plus une frontière de localité au cours d'une communication. La passivation est restreinte de la même manière : P peut passiver a mais pas b ou c . Le processus Q ne peut communiquer avec R qu'en utilisant S pour transmettre le message. Le Kell autorise également les récepteurs joints, c'est-à-dire des récepteurs attendant plusieurs messages simultanés sur différents canaux. Par exemple, le processus $a(X) \mid b(Y) \triangleright X \mid Y$ attend un message sur a et sur b , avant d'exécuter le contenu des deux messages en parallèle. Le Kell sera présenté en détail au chapitre 6.

Comme expliqué en section 2.3, une bisimilarité contextuelle correcte et complète semblable à celle de $\text{HO}\pi\text{P}$ (définition 2.15) a été définie dans le cas fort pour les deux calculs. En revanche il n'existe pas de résultat de caractérisation dans le cas faible. Seule une bisimilarité contextuelle semi-faible correcte [14] a été définie pour Homer.

2.4.6 Bisimilarité environnementale

La bisimilarité environnementale [44, 50, 49] est une forme de bisimilarité adaptée aux formalismes d'ordre supérieur tels que le λ -calcul ou les calculs d'ordre supérieur. Deux processus P, Q sont comparés à l'aide d'un environnement \mathcal{E} , qui représente la connaissance qu'un observateur a de ces processus. Cette connaissance évolue avec les transitions des processus : par exemple, lors d'une émission, les messages sont disponibles à l'observateur et sont donc ajoutés à l'environnement \mathcal{E} . Nous notons $P \mathcal{R}_{\mathcal{E}} Q$ pour signifier que P et Q sont reliés sous l'environnement \mathcal{E} . La clause de bisimulation pour l'émission s'écrit grossièrement de la manière suivante :

- Si $P \mathcal{R}_{\mathcal{E}} Q$ et $P \xrightarrow{a} \langle R \rangle S$, alors il existe $\langle R' \rangle S'$ tel que $Q \xrightarrow{a} \langle R' \rangle S'$ et $S \mathcal{R}_{\mathcal{E} \cup \{(R, R')\}} S'$.

Dans le cas de la réception, l'observateur peut tester les fonctions avec des processus qu'il connaît, c'est-à-dire appartenant à \mathcal{E} , mais il peut également construire des processus de test à partir de \mathcal{E} et des opérateurs du calcul. Si on note \mathcal{E}^* la clôture de \mathcal{E} par les constructions du langage, la clause (tardive) pour la réception est semblable à :

- Si $P \mathcal{R}_{\mathcal{E}} Q$ et $P \xrightarrow{a} F$, alors il existe F' tel que $Q \xrightarrow{a} F'$ et pour tout $(R, R') \in \mathcal{E}^*$, on a $F \circ R \mathcal{R}_{\mathcal{E}} F' \circ R'$.

Enfin la bisimilarité environnementale comporte des clauses qui traduisent les manipulations de l'environnement possibles pour l'observateur. Ces clauses sont spécifiques aux langages considérés. Par exemple dans $\text{HO}\pi$ [44], l'observateur peut à tout moment exécuter les processus reliés par \mathcal{E} .

- Si $P \mathcal{R}_{\mathcal{E}} Q$ et $(R, R') \in \mathcal{E}$, alors on a $P \mid R \mathcal{R}_{\mathcal{E}} Q \mid R'$.

La bisimilarité environnementale pour $\text{HO}\pi$ caractérise la congruence barbue. Comme la bisimilarité contextuelle, les clauses de bisimilarité environnementale comportent des quantifications universelles sur les contextes à tester. Cependant, il est possible de définir des techniques modulo qui simplifient les preuves de bisimilarité. Nous ne savons pas si la définition d'une bisimilarité environnementale en $\text{HO}\pi\text{P}$ permet d'obtenir des résultats de caractérisation dans le cas faible.

2.4.7 Conclusions

Parmi les calculs d'ordre supérieur, $\text{HO}\pi$ est à notre connaissance le seul qui dispose d'une théorie comportementale bien développée : la congruence barbue, équivalence de processus naturelle mais inutilisable en pratique à cause des tests sur tous les contextes, peut être remplacée par la bisimilarité normale, une relation qui n'a besoin de tester qu'un contexte par action à chaque étape du jeu de bisimulation. Dans des calculs plus expressifs tels que les calculs distribués, la caractérisation prend souvent la forme d'une bisimilarité contextuelle, qui, pour les actions d'ordre supérieur, teste les contextes capables d'interagir avec les processus à comparer.

Certains calculs ne disposent d'aucun résultat de caractérisation dans le cas faible, comme par exemple les calculs avec passivation, tels que Homer et le Kell. Pour de tels calculs, il est possible de définir une bisimilarité contextuelle qui caractérise la congruence barbue dans le cas fort, mais la relation ainsi définie nécessite de nombreux contextes de tests pour comparer deux émissions de processus (définition 2.15).

Nous cherchons à obtenir de meilleurs résultats de caractérisations de la congruence barbue dans les calculs avec passivation. Dans un premier temps, nous essayons d'obtenir une relation correcte et complète plus simple que la bisimilarité contextuelle. Nous allons ensuite étudier les techniques de preuves de congruence afin d'obtenir un résultat de caractérisation dans le cas faible.

Chapitre 3

Bisimulation normale

Dans le chapitre précédent, nous avons vu que les bisimilarités contextuelles définies jusqu'ici dans les calculs avec passivation nécessitent de lourdes quantifications sur les contextes, notamment dans le cas de l'émission (définition 2.15). Nous étudions ici la possibilité de réduire ces quantifications, voire d'obtenir une relation similaire à la bisimilarité normale de $\text{HO}\pi$ (définition 2.14), c'est-à-dire une relation pour laquelle il suffit de tester un nombre fini de contextes (fonctions ou concrétions) dans le cas d'une action d'ordre supérieur. Dans un premier temps (section 3.1), nous étudions un calcul avec passivation mais sans restriction appelé HOP [28], pour lequel nous définissons une théorie comportementale complète : il est possible de définir une caractérisation de la congruence barbue sous forme de bisimilarités normales, dans les cas fort et faible. Ces résultats ne peuvent malheureusement pas s'étendre à des calculs avec restriction et passivation tels que $\text{HO}\pi\text{P}$; en section 3.2, nous donnons différents contre-exemples qui suggèrent qu'il n'est pas possible de réduire les quantifications de la bisimilarité contextuelle de $\text{HO}\pi\text{P}$ dans le cas de la réception de message

3.1 Bisimulation normale pour HOP

Le calcul HOP est obtenu en enlevant l'opérateur de restriction du calcul $\text{HO}\pi\text{P}$ et en ajoutant la somme gardée (nécessaire pour prouver la complétude de la bisimilarité d'ordre supérieur). Nous donnons la syntaxe, les règles de la congruence structurelle et du système de transitions étiquetées en figure 3.1, à l'exception du symétrique des règles SUM, PAR et HO. Une concrétion s'écrit désormais simplement $\langle P \rangle Q$, et la pseudo application est définie par $(X)P \bullet \langle R \rangle Q \triangleq P\{R/X\} \mid Q$. Malgré l'absence de restriction, HOP est Turing complet, en tant qu'extension de HOCORE [23].

3.1.1 Bisimulation d'ordre supérieur

Comme pour $\text{HO}\pi\text{P}$, les observables d'un processus P sont les noms et co-noms γ sur lesquels une communication ou une passivation est possible immédiatement (c'est-à-dire tels que $P \xrightarrow{\gamma}$). Nous proposons une bisimilarité d'ordre supérieur comme première caractérisation de la congruence barbue. En effet, comme souligné en section 2.3.2, la passivation peut séparer message et continuation et les placer dans des contextes différents. En outre, ils ne peuvent plus partager de noms restreints en HOP ; nous pouvons donc comparer séparément messages et continuations sans être trop discriminant comme en $\text{HO}\pi$ (section 2.2.2).

Définition 3.1. Une relation \mathcal{R} sur les processus clos est une simulation forte d'ordre supérieure ssi $P \mathcal{R} Q$ implique :

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout processus clos R , il existe F' tel que $Q \xrightarrow{a} F'$ et $F \circ R \mathcal{R} F' \circ R$;

Syntaxe :

$$\begin{aligned} P &::= \mathbf{0} \mid X \mid P \mid P \mid !P \mid M \\ M &::= M + M \mid a(X)P \mid \bar{a}\langle P \rangle P \end{aligned}$$

Règles de la congruence structurelle

$$\begin{aligned} P \mid (Q \mid R) &\equiv (P \mid Q) \mid R & P \mid Q &\equiv Q \mid P & P \mid \mathbf{0} &\equiv P & !P &\equiv P \mid !P \\ P + (Q + R) &\equiv (P + Q) + R & P + Q &\equiv Q + P \end{aligned}$$

Extension des opérateurs à tous les agents

$$\begin{aligned} (X)Q \mid P &\triangleq (X)(Q \mid P) & (\langle Q \rangle R) \mid P &\triangleq \langle Q \rangle (R \mid P) \\ P \mid (X)Q &\triangleq (X)(P \mid Q) & P \mid (\langle Q \rangle R) &\triangleq \langle Q \rangle (P \mid R) \\ a[(X)Q] &\triangleq (X)a[P] & a[\langle Q \rangle R] &\triangleq \langle Q \rangle a[R] \end{aligned}$$

Règles du système de transitions étiquetées

$$\begin{aligned} a(X)P &\xrightarrow{a} (X)P \quad \text{IN} & \bar{a}\langle Q \rangle P &\xrightarrow{\bar{a}} \langle Q \rangle P \quad \text{OUT} & a[P] &\xrightarrow{\bar{a}} \langle P \rangle \mathbf{0} \quad \text{PASSIV} \\ \frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q} &\text{PAR} & \frac{P \xrightarrow{\alpha} A}{!P \xrightarrow{\alpha} A \mid !P} &\text{REPLIC} & \frac{P \xrightarrow{\alpha} A}{a[P] \xrightarrow{\alpha} a[A]} &\text{LOC} \\ \frac{P \xrightarrow{\alpha} A}{P + Q \xrightarrow{\alpha} A} &\text{SUM} & \frac{P \xrightarrow{a} F \quad Q \xrightarrow{\bar{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} &\text{HO} & \frac{P \xrightarrow{a} F \quad P \xrightarrow{\bar{a}} C}{!P \xrightarrow{\tau} F \bullet C \mid !P} &\text{REPLIC-HO} \end{aligned}$$

FIG. 3.1 – Syntaxe et sémantique opérationnelle de HOP

- pour tout $P \xrightarrow{\bar{a}} \langle R \rangle S$, il existe $\langle R' \rangle S'$ tel que $Q \xrightarrow{\bar{a}} \langle R' \rangle S'$, $R \mathcal{R} R'$ et $S \mathcal{R} S'$.

La relation \mathcal{R} est une bisimulation forte d'ordre supérieur ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations fortes d'ordre supérieur. La bisimilarité forte d'ordre supérieure, notée \sim , est la plus grande bisimulation forte d'ordre supérieure.

Dans la suite, nous utilisons également la variante tardive de la bisimilarité, notée \sim_l , qui est obtenue en remplaçant la clause sur la réception par :

- pour tout $P \xrightarrow{a} F$, il existe F' tel que $Q \xrightarrow{a} F'$ et pour tout processus clos R , on a $F \circ R \mathcal{R} F' \circ R$.

Nous prouvons plus tard que les versions précoce et tardive de la bisimilarité coïncident (comme pour $\text{HO}\pi$). La bisimilarité forte d'ordre supérieur est une caractérisation de la congruence barbue forte :

Théorème 3.1. *Nous avons $P \sim Q$ ssi $P \sim_b Q$.*

La preuve de correction, donnée en appendice B.1, repose sur la *méthode de Howe*, une méthode de preuve systématique pour démontrer la congruence de bisimulations, étudiée en détail dans le chapitre 4. La preuve de complétude est la même que celle de $\text{HO}\pi$ (théorème 2.2).

Nous donnons maintenant les définitions dans le cas faible.

Définition 3.2. *Une relation \mathcal{R} sur les processus clos est une simulation faible d'ordre supérieure ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout processus clos R , il existe F', Q' tels que $Q \xrightarrow{a} F'$, $F' \circ R \xrightarrow{\tau} Q'$ et $F \circ R \mathcal{R} Q'$;
- pour tout $P \xrightarrow{\bar{a}} \langle R \rangle S$, il existe $\langle R' \rangle S'', S'$ tels que $Q \xrightarrow{\bar{a}} \langle R' \rangle S''$, $S'' \xrightarrow{\tau} S'$, $R \mathcal{R} R'$ et $S \mathcal{R} S'$.

La relation \mathcal{R} est une bisimulation faible d'ordre supérieur ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations faibles d'ordre supérieur. La bisimilarité faible d'ordre supérieure, notée \approx , est la plus grande bisimulation faible d'ordre supérieure.

La bisimilarité d'ordre supérieur faible tardive, notée \approx_l , est obtenue en remplaçant la clause de réception par :

- pour tout $P \xrightarrow{a} F$, il existe F' tel que $Q \xrightarrow{a} F'$ et pour tout processus clos R , il existe Q' tel que $F' \circ R \xrightarrow{\tau} Q'$ et $F \circ R \mathcal{R} Q'$.

Comme dans le cas fort, nous prouvons la correction de \approx grâce à la méthode de Howe.

Théorème 3.2. *Si $P \approx Q$, alors on a $P \approx_b Q$.*

La complétude est prouvée sur les processus à image finie, en utilisant la même preuve que pour $\text{HO}\pi$ (théorème 2.4).

Définition 3.3. *Un processus P de HOP est à image finie ssi*

- l'ensemble $\{P', P \Rightarrow P'\}$;
- pour tout R , l'ensemble $\{P', \exists F, P \xrightarrow{a} F \wedge F \circ R \Rightarrow P'\}$ est fini ;
- l'ensemble $\{(R, P'), \exists S, P \xrightarrow{\bar{a}} \langle R \rangle S \wedge S \Rightarrow P'\}$ est fini.

Théorème 3.3. *Pour tout processus P, Q à image finie, si $P \approx_b Q$, alors on a $P \approx Q$.*

Il faut remarquer que les bisimulations d'ordre supérieur pour HOP sont plus faciles à utiliser que les bisimulations contextuelles : il n'y a pas de quantification universelle dans la clause d'émission de message. Dans la section suivante, nous montrons que la quantification sur les messages R dans la clause de réception est superflue.

3.1.2 Bisimilarité normale

Nous montrons dans cette section qu'il est possible de définir une bisimilarité correcte et complète pour HOP sans quantification universelle dans le cas de la réception, semblable à la bisimulation normale pour HO π (définition 2.14). Nous rappelons qu'en HO π , les fonctions sont comparées en les appliquant au processus $m.\mathbf{0}$. Ce test n'est pas suffisant pour garantir la bisimilarité des fonctions en HOP. En effet, on considère les processus suivants :

$$P_1 \triangleq !a[X] \mid !a[\mathbf{0}] \quad Q_1 \triangleq X \mid P_1$$

Nous définissons $P_m \triangleq P_1\{\bar{m}.\mathbf{0}/X\}$, $Q_m \triangleq Q_1\{\bar{m}.\mathbf{0}/X\}$, $P_{m,n} \triangleq P_1\{\bar{m}.\bar{n}.\mathbf{0}/X\}$ et $Q_{m,n} \triangleq Q_1\{\bar{m}.\bar{n}.\mathbf{0}/X\}$, où m, n n'apparaissent pas dans P_1, Q_1 .

Nous montrons d'abord pourquoi nous avons $P_m \sim_l Q_m$. La correspondance entre les transitions de P_m et Q_m est facile, sauf pour la transition

$$Q_m \xrightarrow{\bar{m}} \mathbf{0} \mid P_m$$

Le processus P_m ne peut répondre que par une transition

$$P_m \xrightarrow{\bar{m}} a[\mathbf{0}] \mid P_m$$

provenant d'une localité répliquée. La différence entre $\mathbf{0} \mid P_m$ et $a[\mathbf{0}] \mid P_m$ est masquée par le processus répliqué $!a[\mathbf{0}]$ dans P_m . Nous avons donc $\mathbf{0} \mid P_m \sim_l a[\mathbf{0}] \mid P_m$, et plus généralement $P_m \sim_l Q_m$.

En revanche, nous avons $P_{m,n} \not\sim_l Q_{m,n}$. En effet, la transition

$$Q_{m,n} \xrightarrow{\bar{m}} \bar{n}.\mathbf{0} \mid P_{m,n} \triangleq Q'_{m,n}$$

ne peut être imitée que par une transition

$$P_{m,n} \xrightarrow{\bar{m}} a[\bar{n}.\mathbf{0}] \mid P_{m,n} \triangleq P'_{m,n}$$

Les processus $P'_{m,n}$ et $Q'_{m,n}$ ne sont pas bisimilaires ; en déclenchant la passivation dans $P'_{m,n}$, on obtient

$$P'_{m,n} \xrightarrow{\bar{a}} \langle \bar{n}.\mathbf{0} \rangle P_{m,n}$$

Les seuls messages qui peuvent être émis par $Q'_{m,n}$ sont $\bar{m}.\bar{n}.\mathbf{0}$ et $\mathbf{0}$, qui ne sont pas bisimilaires à $\bar{n}.\mathbf{0}$. Nous avons donc $P'_{m,n} \not\sim_l Q'_{m,n}$ et donc $P_{m,n} \not\sim_l Q_{m,n}$.

On peut penser que le déclencheur $\bar{m}.\mathbf{0}$ ne suffit pas à distinguer les fonctions parce que les localités sont complètement transparentes, et donc on ne peut observer la provenance d'un message. Cependant, l'existence de localités englobant une émission de message a des effets indirects qui peuvent être observés. En effet, la passivation transforme un contexte d'évaluation (une localité) en un message qui peut être détruit. Un déclencheur de la forme $\bar{m}.\bar{n}.\mathbf{0}$ permet de détecter un contexte d'évaluation (il y a une émission sur m) qui disparaît (il n'y a pas d'émission ensuite sur n), et donc la présence de localités englobantes.

Nous pouvons généraliser cette idée et montrer qu'il est possible de situer l'occurrence d'une variable X dans l'arbre des localités. Soient P et Q tels que $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q\{\bar{m}.\bar{n}.\mathbf{0}/X\}$, avec m, n frais. On suppose que P est capable de faire une transition $P \xrightarrow{\bar{m}} P'$, et que Q répond par $Q \xrightarrow{\bar{m}} Q'$. Comme m et n sont frais pour P et Q , ces transitions proviennent de copies de $\bar{m}.\bar{n}.\mathbf{0}$ qui sont en contextes d'évaluation dans P et Q . Les processus P' et Q' peuvent alors déclencher exactement une transition $\xrightarrow{\bar{n}}$ provenant d'un processus $\bar{n}.\mathbf{0}$. On suppose désormais que ce processus $\bar{n}.\mathbf{0}$ est dans une localité a dans P' . Par passivation de a , on a la transition $P' \xrightarrow{\bar{a}} \langle R \rangle S$, avec $R \xrightarrow{\bar{n}}$. Le processus Q' doit répondre par $Q' \xrightarrow{\bar{a}} \langle R' \rangle S'$ avec en particulier $R \sim_l R'$. Comme on a $R \xrightarrow{\bar{n}}$, on doit

avoir $R' \xrightarrow{\bar{n}}$, c'est-à-dire que le processus unique $\bar{n}.\mathbf{0}$ qui était en contexte d'évaluation dans Q' est désormais dans un message sur a , ce qui est possible si et seulement si $\bar{n}.\mathbf{0}$ était dans une localité a dans Q' . En raisonnant de la même manière sur R et R' , on prouve que la hiérarchie de localités englobant $\bar{n}.\mathbf{0}$ est la même dans P' et Q' . Cette observation est formalisée par le lemme suivant.

Lemme 3.1. *Soient P, Q tels que $\text{fv}(P, Q) \subseteq \{X\}$ et m, n qui n'apparaissent pas dans P, Q . Supposons $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q\{\bar{m}.\bar{n}.\mathbf{0}/X\}$ et que la transition $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Y\} \triangleq P_n$ est imitée par $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Y\} \triangleq Q_n$ avec $P_n \sim_l Q_n$. Nous avons deux possibilités :*

- soit il existe $P_1 \sim_l Q_1$ tels que $P_n \equiv \bar{n}.\mathbf{0} \mid P_1$, $Q_n \equiv \bar{n}.\mathbf{0} \mid Q_1$ et $P_1 \sim_l Q_1$;
- ou alors il existe $k > 0$, $a_1 \dots a_k$, $P_1 \dots P_{k+1}$, $Q_1 \dots Q_{k+1}$ tels que

$$\begin{aligned} P_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1 \\ Q_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1 \end{aligned}$$

et pour tout $1 \leq j \leq k+1$, on a $P_j \sim_l Q_j$.

Ce lemme nous permet de décomposer P'_n, Q'_n en processus deux-à-deux bisimilaires. Par exemple, si nous avons $P_n \equiv a[b[\bar{n}.\mathbf{0} \mid P_3] \mid P_2] \mid P_1$ with $P_n \sim_l Q_n$, alors nous avons $Q_n \equiv a[b[\bar{n}.\mathbf{0} \mid Q_3] \mid Q_2] \mid Q_1$ avec $P_1 \sim_l Q_1$, $P_2 \sim_l Q_2$ et $P_3 \sim_l Q_3$. La preuve est donnée en appendice B.2. Remarquez que nous ne décomposons pas les processus initiaux P et Q , mais ce résultat nous suffit pour prouver le théorème suivant :

Théorème 3.4. *Soient P, Q deux processus tels que $\text{fv}(P, Q) \subseteq \{X\}$ et m, n deux noms qui n'apparaissent pas dans P, Q . Si $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q\{\bar{m}.\bar{n}.\mathbf{0}/X\}$, alors pour tout processus clos R , on a $P\{R/X\} \sim_l Q\{R/X\}$*

Nous esquissons la preuve de ce théorème pour expliquer comment nous utilisons le lemme 3.1 ; la preuve complète se trouve en appendice 2.4.

Esquisse. Nous montrons que la relation

$$\mathcal{R} \triangleq \{(P\{R/X\}, Q\{R/X\}) \mid P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q\{\bar{m}.\bar{n}.\mathbf{0}/X\}, m, n \text{ frais}\}$$

est une bisimulation d'ordre supérieure tardive. Nous procédons par analyse de cas sur la transition effectuée par $P\{R/X\}$. Nous traitons ici seulement le cas

$$P\{R/X\} \xrightarrow{\tau} P'\{R'/X_i\}\{R/X\}$$

où une copie de R à la position X_i effectue une action interne $R \xrightarrow{\tau} R'$. La copie X_i est donc dans un contexte d'évaluation ; on en déduit que

$$P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{m} P'\{\bar{n}.\mathbf{0}/X_i\}\{\bar{m}.\bar{n}.\mathbf{0}/X\} \triangleq P'_n$$

Cette transition est imitée par

$$Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{m} Q'\{\bar{n}.\mathbf{0}/X_j\}\{\bar{m}.\bar{n}.\mathbf{0}/X\} \triangleq Q'_n$$

avec $P'_n \sim_l Q'_n$. Comme X_j est également dans un contexte d'évaluation, on a

$$Q\{R/X\} \xrightarrow{\tau} Q'\{R'/X_j\}\{R/X\}$$

Nous devons maintenant prouver que

$$P'\{R'/X_i\}\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q'\{R'/X_j\}\{\bar{m}.\bar{n}.\mathbf{0}/X\}$$

pour montrer que le couple $(P'\{R'/X_i\}\{R/X\}, Q'\{R'/X_j\}\{R/X\})$ est dans la relation.

Par le lemme 3.1 nous pouvons décomposer P'_n, Q'_n en

$$\begin{aligned} P'_n &\equiv a_1[\dots a_k[\bar{n}.\mathbf{0} \mid P_{k+1}] \mid P_k \dots] \mid P_1 \\ Q'_n &\equiv a_1[\dots a_k[\bar{n}.\mathbf{0} \mid Q_{k+1}] \mid Q_k \dots] \mid Q_1 \end{aligned}$$

où $(P_r), (Q_r)$ sont des familles de processus deux à deux bisimilaires pour $r \in \{1 \dots k+1\}$. Comme $P_{k+1} \sim_l Q_{k+1}$ et \sim_l est une congruence, on a

$$a_k[R' \mid P_{k+1}] \sim_l a_k[R' \mid Q_{k+1}]$$

Par induction sur $r \in \{k \dots 1\}$, on montre que

$$a_r[\dots a_k[R' \mid P_{k+1}] \mid P_k \dots] \mid P_j \sim_l a_r[\dots a_k[R' \mid Q_{k+1}] \mid Q_k \dots] \mid Q_j$$

Pour $r = 1$, on obtient

$$P'\{R'/X_i\}\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q'\{R'/X_j\}\{\bar{m}.\bar{n}.\mathbf{0}/X\}$$

comme souhaité. □

En utilisant ce résultat, nous pouvons définir une bisimulation normale pour HOP.

Définition 3.4. Une relation \mathcal{R} sur les processus clos est une simulation normale forte ssi $P \mathcal{R} Q$ implique :

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, il existe F' tel que $Q \xrightarrow{a} F'$ et pour un couple de noms m, n qui n'apparaissent pas dans P, Q , nous avons $F \circ \bar{m}.\bar{n}.\mathbf{0} \mathcal{R} F' \circ \bar{m}.\bar{n}.\mathbf{0}$;
- pour tout $P \xrightarrow{\bar{a}} \langle R \rangle S$, il existe R', S' tels que $Q \xrightarrow{\bar{a}} \langle R' \rangle S'$, $R \mathcal{R} R'$ et $S \mathcal{R} S'$.

Une relation \mathcal{R} est une bisimulation normale forte ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations normales fortes. La bisimilarité normale forte \sim_n est la plus grande bisimulation normale forte.

Comme conséquence du théorème 3.4, nous avons le résultat suivant :

Corollaire 3.1. Nous avons $\sim_l = \sim_n = \sim$.

Par définition, nous avons $\sim_l \subseteq \sim \subseteq \sim_n$. L'inclusion $\sim_n \subseteq \sim_l$ est une conséquence du Théorème 3.4.

Nous pouvons également définir une bisimilarité normale faible qui coïncide avec la bisimilarité d'ordre supérieur faible.

Définition 3.5. Une relation \mathcal{R} sur les processus clos est une simulation normale faible ssi $P \mathcal{R} Q$ implique :

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a} F$, il existe F' tel que $Q \xrightarrow{a} F'$ et pour un couple de noms m, n qui n'apparaissent pas dans P, Q , il existe Q' tel que $F' \circ \bar{m}.\bar{n}.\mathbf{0} \xrightarrow{\tau} Q'$ et $F \circ \bar{m}.\bar{n}.\mathbf{0} \mathcal{R} Q'$;
- pour tout $P \xrightarrow{\bar{a}} \langle R \rangle S$, il existe R', S'', S' tels que $Q \xrightarrow{\bar{a}} \langle R' \rangle S''$, $S'' \xrightarrow{\tau} S'$, $R \mathcal{R} R'$ et $S \mathcal{R} S'$.

Une relation \mathcal{R} est une bisimulation normale faible ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations normales faibles. La bisimilarité normale faible \approx_n est la plus grande bisimulation normale faible.

Théorème 3.5. Nous avons $\approx_n = \approx = \approx_l$

La technique de preuve est la même, en utilisant des variantes faibles du lemme 3.1 et du théorème 3.4. Dans un calcul avec passivation et sans restriction, nous pouvons donc définir dans les cas fort et faible une bisimilarité correcte et complète et dont les clauses ne comporte pas de quantification universelle.

Pour l'équivalence de fonctions dans HO π , il suffit d'observer combien de fois et à quel moment le message reçu est activé, ce qui peut se faire en utilisant un processus $\overline{m}.0$ (section 2.2.4). Dans HOP, nous devons en plus observer à quel endroit dans la hiérarchie de localité le processus est activé, pour prendre en compte les effets de la passivation. Nous pouvons observer la passivation en HOP grâce à un processus $\overline{m}.\overline{n}.0$ (la transition $\xrightarrow{\overline{m}}$ n'est pas suivie de la transition $\xrightarrow{\overline{n}}$), et donc la présence de localités. Il n'est en revanche pas possible d'observer la hiérarchie de localités autour d'une variable en HO π P : la restriction permet de masquer certaines localités. Nous allons voir dans la prochaine section que les résultats obtenus pour HOP ne sont plus valables pour HO π P.

3.2 Équivalence de fonctions pour HO π P

Dans cette, nous présentons des contre-exemples pour montrer qu'une simplification similaire à celles de HOP n'est pas possible en HO π P. Nous prouvons que tester de larges sous classes de processus de HO π P (les *processus sans réception* et les *processus finis*) n'est pas suffisant pour garantir la bisimilarité de fonctions. Nous présentons d'abord un contre-exemple qui repose sur l'extension de portée paresseuse, puis une famille de contre-exemples qui ne nécessitent pas ce mécanisme (mais qui demande de rajouter la somme non gardée à HO π P).

3.2.1 Les processus sans réception

Par la suite, nous omettons les zéros en fin de processus pour améliorer la lisibilité ; dans la définition d'un agent, nous utilisons m pour $m.0$. Nous écrivons également $\nu a.b.P$ pour $\nu a.\nu b.P$, et nous définissons $0_m \triangleq \nu n.n.m$. Le processus 0_m ne peut effectuer de transitions, comme 0 , mais dispose d'un nom libre m . Nous définissons les fonctions suivantes.

$$\begin{aligned} (X)P &\triangleq (X)\nu n b.(b[X \mid \nu m.\overline{a}\langle 0_m \rangle(m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y)) \\ (X)Q &\triangleq (X)\nu m n b.(b[X \mid \overline{a}\langle 0 \rangle(m \mid n \mid \overline{m}.\overline{m}.p)] \mid \overline{n}.b(Y)(Y \mid Y)) \end{aligned}$$

Les deux fonctions diffèrent par le message émis sur a et par la position de la restriction sur m (à l'intérieur ou à l'extérieur de b). Un processus sans réception est un processus construit sur la syntaxe d'HO π P à l'exception de la réception de message $a(X)P$.

Lemme 3.2. *Soit R un processus sans réception. Nous avons $(X)P \circ R \sim (X)Q \circ R$.*

Comme R est sans réception, il ne peut pas recevoir le message émis sur le seul nom libre a ; par conséquent, R ne peut interagir avec P ou Q . Soient $P_{m,R} \triangleq \nu n b.(b[R \mid m \mid n \mid \overline{m}.\overline{m}.p] \mid \overline{n}.b(Y)(Y \mid Y))$, F une fonction et \mathbb{E} un contexte de bisimulation tel que $m \notin \text{fn}(\mathbb{E}, F)$. Nous montrons maintenant que la transition $(X)P \circ R \xrightarrow{\overline{a}} \nu m.\langle 0_m \rangle P_{m,R}$ répond à $(X)Q \circ R \xrightarrow{\overline{a}} \langle 0 \rangle \nu m.P_{m,R}$, c'est-à-dire que nous avons $\nu m.(F \circ 0_m \mid \mathbb{E}\{P_{m,R}\}) \sim F \circ 0 \mid \mathbb{E}\{\nu m.P_{m,R}\}$. Comme $m \notin \text{fn}(\mathbb{E}, F)$, il ne peut y avoir de synchronisation sur m entre F et $P_{m,R}$ ou entre \mathbb{E} et $P_{m,R}$. Les transitions de $\nu m.(F \circ 0_m \mid \mathbb{E}\{P_{m,R}\})$ tirent leur origine des actions de F, \mathbb{E}, R (ou des interactions impliquant ces agents) et des actions internes dans $P_{m,R}$, auxquelles le processus $F \circ 0 \mid \mathbb{E}\{\nu m.P_{m,R}\}$ peut répondre par les mêmes transitions.

Remarque 3.1. *La preuve complète du lemme 3.2 est fastidieuse mais directe : il suffit d'énumérer les réductions possibles de $(X)P \circ R$ et de $(X)Q \circ R$ et de montrer qu'elles sont en bisimulation forte précoce.*

En revanche, les fonctions $(X)P$ et $(X)Q$ ont des comportements différents avec un argument qui peut recevoir sur a , tel $a(Z)q$, avec $p \neq q$. En communiquant sur a , nous avons

$$(X)Q \circ a(Z)q \xrightarrow{\tau} \nu mn b.(b[q \mid m \mid n \mid \bar{m}.\bar{m}.p] \mid \bar{n}.b(Y)(Y \mid Y)) \triangleq Q_1$$

Comme Q_1 peut effectuer une transition \xrightarrow{q} , $(X)P \circ a(Z)Q$ ne peut répondre que par

$$(X)P \circ a(Z)q \xrightarrow{\tau} \nu nb.(b[\nu m.(q \mid m \mid n \mid \bar{m}.\bar{m}.p)] \mid \bar{n}.b(Y)(Y \mid Y)) \triangleq P_1$$

Notez que dans P_1 , la portée de la restriction sur m reste dans la localité cachée b , alors qu'elle est entendue hors de b dans Q_1 .

Après synchronisation sur n et passivation de b , nous avons

$$Q_1(\xrightarrow{\tau})^2 \nu mn b.(q \mid q \mid m \mid m \mid \bar{m}.\bar{m}.p \mid \bar{m}.\bar{m}.p) \triangleq Q_2$$

(le processus à l'intérieur de b dans Q_1 est dupliqué). Après deux synchronisations sur m , nous avons

$$Q_2(\xrightarrow{\tau})^2 \nu mn b.(q \mid q \mid p \mid \bar{m}.\bar{m}.p) \triangleq Q_3$$

et Q_3 peut effectuer une transition \xrightarrow{p} . Le processus P_1 ne peut répondre à cette série de transitions. En effectuant la duplication, nous obtenons

$$P_1(\xrightarrow{\tau})^2 \nu nb.(\nu m.(q \mid m \mid \bar{m}.\bar{m}.p) \mid \nu m.(q \mid m \mid \bar{m}.\bar{m}.p)) \triangleq P_2$$

Chaque copie du sous-processus $q \mid m \mid \bar{m}.\bar{m}.p$ de P_2 dispose de sa propre copie du nom m . Quelles que soient les transitions effectuées depuis P_2 , nous ne pouvons obtenir l'observable p . Plus généralement, le processus P_1 ne peut répondre à la suite de transitions $Q_1(\xrightarrow{\tau})^4 \xrightarrow{p}$, par conséquent les processus $(Q) \circ a(Z)q$ et $(X)P \circ a(Z)q$ ne sont pas bisimilaires.

Le contre-exemple développé ici montre que tester les fonctions avec des processus sans réception (tels que $\bar{m}.\mathbf{0}$ ou $\bar{m}.\bar{n}.\mathbf{0}$) n'est pas suffisant pour exhiber des comportements différents. Ce contre-exemple repose essentiellement sur l'extension de portée paresseuse, utilisée également dans Homer et le Kell. Utiliser une politique différente pour l'extension de portée, par exemple l'extension de portée systématique, n'est malheureusement pas une solution ; dans la section suivante, nous présentons une famille de contre-exemples, qui ne repose pas sur l'extension de portée paresseuse, et qui montre que tester une classe de processus finis ne permet pas de garantir l'équivalence de fonctions.

3.2.2 Processus finis

Nous définissons les processus finis de la manière suivante.

Définition 3.6. *Un processus fini de $HO\pi P$ est un processus construit selon la grammaire suivante :*

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

Informellement, un processus fini ne peut initier une suite infinie de transitions. Notez que dans le cas de l'émission, le message n'est pas important et peut être un processus quelconque. Nous n'autorisons pas la variable de processus X dans la syntaxe ; par conséquent, les processus finis comprennent seulement les réceptions $a(X)P_F$ telles que $X \notin P_F$ ou telles que X apparaît uniquement dans un ou plusieurs messages. Autrement dit, un processus reçu peut-être transféré mais ne peut être activé. Avec une réception de message quelconque, nous serions capable d'encoder la réplication (comme expliqué en remarque 2.1), et donc d'obtenir des suites infinies de transitions.

Remarque 3.2. Notre définition de processus n'inclut pas tous les processus à comportement fini, comme par exemple $a(X)\nu b.b.X$. Le calcul $\text{HO}\pi\text{P}$ est Turing complet, la terminaison est donc indécidable.

Nous étendons la définition à tous les agents de la manière suivante : une concrétion $\nu\tilde{b}.(R)S$ est dite finie si et seulement si S est fini. Une fonction $(X)P$ est dite finie si et seulement si P est fini. Nous notons A_F l'ensemble des agents finis. Nous donnons d'abord quelques propriétés des agents finis.

Lemme 3.3. Soit F une fonction finie. Pour tout P , le processus $F \circ P$ est fini.

Soit P_F un processus fini.

- Pour tout α, A tel que $P_F \xrightarrow{\alpha} A$, A est fini.
- L'ensemble $\{\alpha, \exists A, P_F \xrightarrow{\alpha} A\}$ est fini.
- Pour tout α , l'ensemble $\{A, P_F \xrightarrow{\alpha} A\}$ est fini.
- Soient une suite de processus (P_i) telle que P_0 est un processus fini et telle que pour tout i , on a $P_i \xrightarrow{\tau} P_{i+1}$ ou $P_i \xrightarrow{\tilde{a}} \nu\tilde{b}.(R)P_{i+1}$ ou $P_i \xrightarrow{a} F$ avec $F \circ P = P_{i+1}$ pour un certain P . La suite (P_i) est finie.

Les premières propriétés sont faciles à prouver par induction sur P_F ou F , et la preuve de la dernière est donnée en appendice C. Comme les transitions sont à branchement fini (par les deuxième et troisième propriétés du lemme 3.3), et que les suites de transitions initiée par P_F sont finies (dernière propriété), nous pouvons parler de la longueur de la plus grande de ces suites, appelées *profondeur*.

Définition 3.7. Nous définissons inductivement la profondeur d'un agent fini A_F , notée $d(A_F)$, de la manière suivante :

- On a $d(P_F) = 0$ ssi P_F ne peut pas faire de transition.
- On a $d(P_F) = 1 + \max \{d(A) \mid \exists \alpha, P_F \xrightarrow{\alpha} A\}$ autrement.
- Pour toute concrétion finie $\nu\tilde{b}.(P)P_F$, on a $d(\nu\tilde{b}.(P)P_F) = d(P_F)$.
- Pour toute fonction finie $(X)P_F$, on a $d((X)P_F) = d(P_F)$.

Notez que la profondeur d'une fonction est toujours la même quelle que soit l'argument à laquelle on l'applique ; une variable X ne peut apparaître que dans un message, et la définition de profondeur d'une concrétion ne prend en compte que la continuation. Formellement, nous avons le résultat suivant :

Lemme 3.4. Pour tout processus P , nous avons $d(F \circ P) = d(F)$.

3.2.3 Contre-exemples

Nous utilisons la notion de profondeur d'un agent fini pour définir une famille de contre-exemples qui montre que tester les fonctions avec des processus finis n'est pas suffisant pour garantir la bisimilarité des fonctions. Plus précisément, nous définissons inductivement deux familles de fonctions $(F_n), (G_n)$ telles que pour tout processus fini P_F tel que $d(P_F) \leq n$, nous avons $F_n \circ P_F \sim G_n \circ P_F$, mais pour un certain processus Q_{n+1} de profondeur $n + 1$, nous avons $F_n \circ Q_{n+1} \not\sim Q_{n+1} \circ P_F$.

Pour un nom a et une fonction $F = (X)P$, nous notons $a.F$ le processus $a(X)P$. Nous définissons également $\tau.P \triangleq \nu a.(\bar{a}.0 \mid a.P)$ pour $a \notin \text{fn}(P)$. Nous supposons pour ce contre-exemple que la somme non gardée est ajoutée au calcul. Nous définissons

$$F_0 \triangleq (X_0)X_0, G_0 \triangleq (X_0)(X_0 \mid X_0)$$

et pour $n > 0$, nous définissons

$$F_n \triangleq (X_n)(\nu a_n.(a_n[X_n] \mid a_n.F_{n-1}) + R_n)$$

$$G_n \triangleq (X_n)(\nu a_n.(a_n[X_n] \mid a_n.G_{n-1}) + S_n)$$

avec $R_n \triangleq \nu a_n. \tau. G_{n-1} \circ X_n$ et $S_n \triangleq \nu a_n. \tau. F_{n-1} \circ X_n$. Notez que R_n imite la passivation de la localit   a_n dans G_n , alors que S_n imite la passivation de a_n dans F_n .

Soit P_F un processus fini tel que $d(P_F) \leq n$. Nous   tudions les transitions de $F_n \circ P_F$ et $G_n \circ P_F$. Si $n = 0$, c'est-  dire si P_F ne peut pas faire de transition, alors nous avons clairement $P_F \sim P_F \mid P_F$. Autrement, nous avons trois   volutions possibles pour $F_n \circ P_F$. Nous supposons d'abord que l'action interne du sous-processus R_n se d  clenche : nous avons alors

$$F_n \circ P_F \xrightarrow{\tau} \nu a_n. G_{n-1} \circ P_F$$

Le processus $G_n \circ P_F$ r  pond par passivation de la localit   a_n : nous obtenons

$$G_n \circ P_F \xrightarrow{\tau} \nu a_n. G_{n-1} \circ P_F$$

les deux processus r  sultants sont identiques. De la m  me mani  re, si $F_n \circ P_F$ effectue la passivation

$$F_n \circ P_F \xrightarrow{\tau} \nu a_n. F_{n-1} \circ P_F$$

alors $G_n \circ P_F$ r  pond par la τ -action de son sous-processus S_n ; nous avons

$$G_n \circ P_F \xrightarrow{\tau} \nu a_n. F_{n-1} \circ P_F$$

Nous supposons maintenant que P_F effectue une ou plusieurs transitions dans $F_n \circ P_F$, avant que la passivation de la localit   a_n ne se d  clenche. Informellement, nous avons une suite de transitions

$$F_n \circ P_F \xrightarrow{\alpha_1} \dots \xrightarrow{\alpha_k} \nu a_n. (a_n[P'_F] \mid a_n.F_{n-1}) \xrightarrow{\tau} \nu a_n. (F_{n-1} \circ P'_F)$$

avec $d(P'_F) \leq n - 1$, auxquelles $G_n \circ P_F$ peut r  pondre par les m  mes transitions ; nous avons

$$G_n \circ P_F \xrightarrow{\alpha_1} \dots \xrightarrow{\alpha_k} \nu a_n. (a_n[P'_F] \mid a_n.G_{n-1}) \xrightarrow{\tau} \nu a_n. (G_{n-1} \circ P'_F)$$

Nous obtenons donc deux processus bisimilaires    $F_{n-1} \circ P'_F$ et $G_{n-1} \circ P'_F$ avec $d(P'_F) \leq n - 1$. Nous pouvons donc prouver le r  sultat suivant en proc  dant par induction sur n :

Lemme 3.5. *Soit P_F un processus fini tel que $d(P_F) \leq n$. Nous avons $F_n \circ P_F \sim G_n \circ P_F$.*

La preuve est donn  e en appendice C. Maintenant, soit (m_k) une famille de noms frais deux    deux distincts. Soit $Q_1 = m_1. \mathbf{0}$ et $Q_{k+1} = m_{k+1}. Q_k$ pour tout $k > 1$. Nous expliquons pourquoi $F_n \circ Q_{n+1}$ n'est pas bisimilaire    $G_n \circ Q_{n+1}$. Nous consid  rons la transitions m_{n+1} , suivie par la passivation de a_n : nous obtenons

$$F_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n. (a_n[Q_n] \mid a_n.F_{n-1}) \xrightarrow{\tau} \sim F_{n-1} \circ Q_n$$

Le processus ne peut r  pondre    cette suite de transitions que par

$$G_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n. (a_n[Q_n] \mid a_n.G_{n-1}) \xrightarrow{\tau} \sim G_{n-1} \circ Q_n$$

Nous obtenons donc $F_{n-1} \circ Q_n$    comparer    $G_{n-1} \circ Q_n$; en r  p  tant cette suite de transitions $n - 1$ fois, nous obtenons $F_0 \circ Q_1 = m_1. \mathbf{0}$ et $G_0 \circ Q_1 = m_1. \mathbf{0} \mid m_1. \mathbf{0}$, qui ne sont clairement pas bisimilaires. La preuve, par induction sur n , est donn  e en appendice C. Par cons  quent, nous avons $F_n \circ Q_{n+1} \not\sim G_n \circ Q_{n+1}$. Les fonctions F_n et G_n sont donc bisimilaires avec un argument de profondeur inf  rieure    n , mais sont distingu  es par un message de profondeur $n + 1$.

3.3 Conclusions

Dans le calcul HOP, pourvu d'un opérateur de passivation mais sans restriction, nous pouvons caractériser la congruence barbue par une congruence d'ordre supérieur (définition 3.1), une relation plus facile à manipuler que la bisimilarité contextuelle de $\text{HO}\pi$ (définition 2.10) ou de $\text{HO}\pi\text{P}$ (définition 2.15). En effet, une bisimilarité d'ordre supérieur ne comporte une quantification sur les contextes de test que dans le cas de la réception. Il est également possible de se passer de cette quantification, et définir ainsi une bisimilarité normale correcte et complète, dans les cas fort et faible (définitions 3.4 et 3.5).

La bisimilarité normale de HOP ne repose pas sur un encodage des processus en termes du premier ordre, comme en $\text{HO}\pi$ (section 2.2.4). La passivation, construction intrinsèquement d'ordre supérieur, empêche tout encodage de cette nature. Nous simplifions les tests de la clause de réception en HOP en observant la hiérarchie des localités autour des occurrences de la variable X (lemme 3.1). Un processus $\overline{m}.n.\mathbf{0}$ permet d'observer le déclenchement d'une passivation (une action sur m n'est pas suivie d'une action sur n) et donc la présence d'une localité.

En revanche, un processus $\overline{m}.n.\mathbf{0}$ ne suffit plus à observer les localités dans un calcul avec passivation et restriction tel que $\text{HO}\pi\text{P}$: certaines localités peuvent être restreintes et donc non observables. Plus généralement, nous avons montré que tester de grandes classes de processus (les processus sans réception et les processus finis) ne suffit pas pour établir la bisimilarité entre fonctions en $\text{HO}\pi\text{P}$. Nous conjecturons qu'il n'est pas possible de définir une bisimilarité correcte et complète plus simple (c'est-à-dire avec moins de quantification dans ses clauses) que la bisimilarité contextuelle (définition 2.15) dans $\text{HO}\pi\text{P}$. La difficulté dans la définition d'une théorie comportementale des calculs tels que Homer et le Kell est donc l'interaction entre passivation et restriction, et non la passivation seule.

Chapitre 4

Preuves de congruence

Nous avons vu dans le chapitre 2 qu'il n'existe pas de preuve de congruence en $\text{HO}\pi\text{P}$ pour la bisimilarité contextuelle faible précoce (définition 2.16), candidate habituellement considérée dans les calculs d'ordre supérieur pour caractériser la congruence barbue faible. Nous étudions dans ce chapitre les principales méthodes de preuve de congruence, en particulier celles utilisées pour Homer [19, 14] et le Kell [47], afin de comprendre pourquoi elles échouent avec les relations faibles. Nous étudions d'abord la méthode proposée par Sangiorgi pour $\text{HO}\pi$ [42], et nous montrons qu'elle n'est pas applicable aux calculs avec passivation. Nous décrivons ensuite la méthode utilisée pour le Kell, qui consiste à prouver que la plus petite congruence contenant \sim ou \approx est une bisimulation contextuelle forte ou faible. Nous expliquons que la preuve de bisimulation, par *progression* [45], ne s'applique pas dans le cas faible. Enfin, nous étudions la *méthode de Howe* [20], une méthode de preuve systématique pour prouver qu'une bisimulation est une congruence, qui a été appliquée à Homer.

4.1 Preuve classique pour $\text{HO}\pi$

Comme souligné par Sangiorgi [42], la principale difficulté dans les calculs d'ordre supérieur est de prouver la congruence par rapport à l'émission, c'est-à-dire de montrer que $P \sim Q$ implique $\bar{a}\langle P \rangle R \sim \bar{a}\langle Q \rangle R$. Comme les messages sont testés au sein de toutes les fonctions, nous devons montrer que la bisimilarité est préservée par rapport à la substitution. C'est pourquoi les preuves de congruence des bisimilarités contextuelles forte et faible de $\text{HO}\pi$ reposent sur le lemme suivant, appelé *lemme de substitution*.

Lemme 4.1. *Soient A un agent et P, Q deux processus de $\text{HO}\pi$. Si $P \sim Q$ (respectivement $P \approx Q$), alors on a $A\{P/X\} \sim A\{Q/X\}$ (respectivement $A\{P/X\} \approx A\{Q/X\}$).*

Nous pouvons résumer la méthode de preuve de ce lemme dans [42] de la manière suivante :

- Le résultat est prouvé pour les contextes d'évaluation (la composition parallèle, la réplication et la restriction de nom).
- Le résultat est ensuite étendu à tous les contextes, en utilisant la première étape.

Cette distinction s'explique par le fait que si A est un contexte d'évaluation, alors les transitions de $A\{P/X\}$ peuvent provenir de A comme de P , alors que si A n'est pas un contexte d'évaluation, P ne peut pas évoluer. La preuve du lemme 4.1 repose sur la définition de simulation contextuelle forte précoce *modulo* \sim .

Définition 4.1. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle forte précoce modulo \sim ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \sim \mathcal{R} \sim Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F' telle que $Q \xrightarrow{a} F'$ et $F \bullet C \sim \mathcal{R} \sim F' \bullet C$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et $F \bullet C \sim \mathcal{R} \sim F \bullet C'$.

Autoriser la composition par \sim permet de prouver la bisimilarité de manière plus flexible.

Lemme 4.2. *Si \mathcal{R} est une simulation contextuelle forte précoce modulo \sim , alors nous avons $\mathcal{R} \subseteq \sim$.*

La preuve de ce lemme se fait en montrant que $\sim \mathcal{R} \sim$ est une bisimulation contextuelle forte précoce. La méthode est applicable également dans le cas faible, en prenant la définition de simulation modulo \approx suivante.

Définition 4.2. *Une relation \mathcal{R} sur les processus clos est une simulation contextuelle faible précoce modulo \approx ssi $P \mathcal{R} Q$ implique :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \Rightarrow Q'$ et $P' \sim \mathcal{R} \approx Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout C , il existe F', Q' tels que $Q \xrightarrow{a} F'$, $F' \bullet C \Rightarrow Q'$ et $F \bullet C \sim \mathcal{R} \approx Q'$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C', Q' tels que $Q \xrightarrow{\bar{a}} C'$, $F \bullet C' \Rightarrow Q'$ et $F \bullet C \sim \mathcal{R} \approx Q'$.

Notez qu'on compose par \sim à gauche et par \approx à droite ; cette dissymétrie est nécessaire pour avoir le résultat suivant.

Lemme 4.3. *Si \mathcal{R} est une simulation contextuelle faible précoce modulo \approx , alors nous avons $\mathcal{R} \subseteq \approx$.*

Nous expliquons pourquoi définir une simulation modulo \approx en composant à droite et à gauche par \approx pose problème en section 4.2 (remarque 4.2). La preuve de congruence sur les contextes d'exécution se fait opérateur par opérateur : par exemple dans le cas de la composition parallèle, Sangiorgi prouve que la relation

$$\mathcal{R} \triangleq \{(\nu \tilde{a}.(P \mid R), \nu \tilde{a}.(Q \mid R)), P \sim Q\} \cup \sim$$

est une simulation contextuelle forte précoce modulo \sim . Des relations similaires sont ensuite définies pour prouver la congruence par rapport à la restriction et à la réplication, dans les cas fort et faible.

La preuve du lemme de substitution par la méthode de Sangiorgi échoue en $\text{HO}\pi\text{P}$. Contrairement à $\text{HO}\pi$, un contexte d'évaluation en $\text{HO}\pi\text{P}$ peut devenir un contexte qui interdit toute transition ; par exemple, une localité peut devenir une émission de processus, empêchant toute évolution de la part du message. Concrètement, pour prouver la première étape de la méthode de Sangiorgi dans le cas de la localité, nous devrions montrer que $P \sim Q$ implique $a[P] \sim a[Q]$. Nous aurions à construire une relation \mathcal{R} telle que (avec $P \sim Q$) :

$$\begin{array}{ccc} a[P] - \frac{\mathcal{R}}{} - a[Q] & & \\ \downarrow \bar{a} & & \downarrow \bar{a} \\ \langle P \rangle \mathbf{0} - \frac{\mathcal{R}}{} - \langle Q \rangle \mathbf{0} & & \end{array}$$

et telle que \mathcal{R} est une bisimulation. En conséquence, pour toute fonction $(X)R$, nous aurions $R\{P/X\} \mathcal{R} R\{Q/X\}$. Pour prouver un sous-cas du lemme de substitution, nous devrions considérer la relation $\mathcal{R} = \{(R\{P/X\}, R\{Q/X\}), P \sim Q\}$ et montrer que \mathcal{R} est une bisimulation. Cela revient à prouver directement le lemme de substitution, sans passer par le schéma de preuve de Sangiorgi. Cette technique ne peut donc être appliquée en $\text{HO}\pi\text{P}$, et de manière générale dans les calculs avec passivation.

Remarque 4.1. *Les preuves de congruence en HOCORE [23] et en Seal [12] reposent sur une méthode similaire. En HOCORE , Lanese et coll. prouvent la congruence pour la plus simple des équivalences définies pour ce calcul, la bisimilarité d'entrée sortie. Cette bisimilarité*

relie les processus en comparant uniquement les actions d'ordre supérieur, ce qui élimine les cas les plus complexes comme la communication d'ordre supérieur. De ce fait, la preuve de congruence opérateur par opérateur est très simple.

La preuve du Seal semble suivre le même schéma ; cependant le cas du gel d'une localité (action FREEZE du système de transition), qui ressemble à la passivation d'une localité en $HO\pi P$, n'est pas traité dans [12].

4.2 Preuve par progression

Nous allons maintenant détailler la méthode utilisée pour prouver la congruence de la bisimilarité contextuelle forte de Plain CHOCS [52] et du Kell [47]. Cette méthode s'applique aux relations tardive comme précoce ; pour le reste de cette section, nous travaillons avec la bisimilarité précoce. Comme pour $HO\pi$, la preuve par progression repose sur un lemme de substitution.

Lemme 4.4. *Soient A un agent et P, Q deux processus de $HO\pi P$. Si $P \sim Q$, alors on a $A\{P/X\} \sim A\{Q/X\}$.*

Nous cherchons à prouver de manière directe ce lemme. Pour deux ensembles finis $\tilde{P} = (P_i)_{i \in \mathcal{I}}$ et $\tilde{Q} = (Q_i)_{i \in \mathcal{I}}$ de même taille et pour une relation \mathcal{R} , nous notons $\tilde{P} \mathcal{R} \tilde{Q}$ ssi nous avons $P_i \mathcal{R} Q_i$ pour tout $i \in \mathcal{I}$. Nous considérons la relation

$$\mathcal{R} = \{(\mathbb{C}\{R\{\tilde{P}/\tilde{Y}\}\}, \mathbb{C}\{R\{\tilde{Q}/\tilde{Y}\}\}), \text{fv}(R) = \tilde{Y}, \tilde{P} \sim \tilde{Q}\}$$

et nous prouvons que sa clôture réflexive et transitive \mathcal{R}^* est une bisimulation contextuelle précoce forte. Nous expliquons d'abord le choix de notre relation candidate \mathcal{R} . Dans un agent $A\{P/X\}$, la variable X peut apparaître plusieurs fois, et chaque copie de P apparaissant aux différentes positions de X peut évoluer indépendamment ; c'est pourquoi nous considérons une substitution simultanée de plusieurs processus $R\{\tilde{P}/\tilde{Y}\}$ dans la relation candidate. Nous ajoutons également un contexte \mathbb{C} dans la définition de \mathcal{R} pour prendre en compte les captures de noms. Nous rappelons que la clause d'émission de bisimulation contextuelle en $HO\pi P$ repose sur des contextes de bisimulation \mathbb{E} qui peuvent capturer des noms (définition 2.15).

Nous expliquons maintenant pourquoi nous prouvons que \mathcal{R}^* , et non pas \mathcal{R} elle-même, est une bisimulation. Nous procédons par induction sur la structure de \mathbb{C} , et par induction imbriquée sur la dérivation de la transition $\mathbb{C}\{R\{\tilde{P}/\tilde{Y}\}\} \xrightarrow{a} R'$. Supposons $\mathbb{C} = \square$. Nous considérons le cas de la composition parallèle $R = R^1 \mid R^2$, et nous supposons que la transition est une communication d'ordre supérieur. Pour un agent A et des processus \tilde{P} , nous notons $A_{\tilde{P}}$ pour $A\{\tilde{P}/\tilde{Y}\}$. Nous voulons clore le diagramme suivant :

$$\begin{array}{ccc} R_{\tilde{P}}^1 \mid R_{\tilde{P}}^2 & \xrightarrow{\mathcal{R}} & R_{\tilde{Q}}^1 \mid R_{\tilde{Q}}^2 \\ \downarrow \tau & & \\ F_{\tilde{P}'} \bullet C_{\tilde{P}''} & & \end{array}$$

sachant que $R_{\tilde{P}}^1 \xrightarrow{a} F_{\tilde{P}'}$ et $R_{\tilde{P}}^2 \xrightarrow{\bar{a}} C_{\tilde{P}''}$ pour un certain a . Par définition nous avons $R_{\tilde{P}}^1 \mathcal{R} R_{\tilde{Q}}^1$, donc en choisissant $C_{\tilde{P}''}$ comme récepteur (nous travaillons avec la bisimulation précoce, nous devons donc choisir la concrétion avant d'obtenir une transition correspondante), il existe $F_{\tilde{Q}'}$ par induction tel que

$$\begin{array}{ccc} R_{\tilde{P}}^1 & \xrightarrow{\mathcal{R}} & R_{\tilde{Q}}^1 \\ \downarrow a & & \downarrow a \\ F_{\tilde{P}'} & \xrightarrow{\mathcal{R}} & F_{\tilde{Q}'} \end{array}$$

et $F_{\widetilde{P'}} \bullet C_{\widetilde{P''}} \mathcal{R} F_{\widetilde{Q'}} \bullet C_{\widetilde{P''}}$.

A partir de $R_{\widetilde{P}}^2 \mathcal{R} R_{\widetilde{Q}}^2$ et de la fonction $F_{\widetilde{Q'}}$, nous obtenons

$$\begin{array}{ccc} R_{\widetilde{P}}^2 & \xrightarrow{\mathcal{R}} & R_{\widetilde{Q}}^2 \\ \downarrow \bar{a} & & \downarrow \bar{a} \\ C_{\widetilde{P''}} & \xrightarrow{\mathcal{R}} & C_{\widetilde{Q''}} \end{array}$$

avec $F_{\widetilde{Q'}} \bullet C_{\widetilde{P''}} \mathcal{R} F_{\widetilde{Q'}} \bullet C_{\widetilde{Q''}}$. De ces deux résultats, nous pouvons conclure que :

$$\begin{array}{ccc} R_{\widetilde{P}}^1 \mid R_{\widetilde{P}}^2 & \xrightarrow{\mathcal{R}} & R_{\widetilde{Q}}^1 \mid R_{\widetilde{Q}}^2 \\ \tau \downarrow & & \downarrow \tau \\ F_{\widetilde{P'}} \bullet C_{\widetilde{P''}} \xrightarrow{\mathcal{R}} F_{\widetilde{Q'}} \bullet C_{\widetilde{P''}} \xrightarrow{\mathcal{R}} F_{\widetilde{Q'}} \bullet C_{\widetilde{Q''}} \end{array}$$

Finalement, nous avons donc :

$$\begin{array}{ccc} R_{\widetilde{P}} & \xrightarrow{\mathcal{R}} & R_{\widetilde{Q}} \\ \tau \downarrow & & \downarrow \\ R'_{\widetilde{P'} \cup \widetilde{P''}} \xrightarrow{\mathcal{R}^2} R'_{\widetilde{Q'} \cup \widetilde{Q''}} \end{array}$$

alors que nous voulions $R'_{\widetilde{P'} \cup \widetilde{P''}} \mathcal{R} R'_{\widetilde{Q'} \cup \widetilde{Q''}}$. Plus généralement, nous montrons que \mathcal{R} progresse vers sa clôture réflexive et transitive \mathcal{R}^* , en suivant la définition de [45].

Définition 4.3. Soient \mathcal{R} et \mathcal{S} deux relations sur les processus clos de $HO\pi P$. La relation \mathcal{R} progresse fortement et de manière précoce vers \mathcal{S} , noté $\mathcal{R} \rightsquigarrow \mathcal{S}$, ssi pour tout $P \mathcal{R} Q$:

- si $P \xrightarrow{\tau} P'$, il existe Q' tel que $P' \mathcal{S} Q'$;
- si $P \xrightarrow{a} F$, pour tout C , il existe F' tel que $Q \xrightarrow{a} F'$ et $F \bullet C \mathcal{S} F' \bullet C$;
- si $P \xrightarrow{\bar{a}} C$, pour tout F , il existe C' tel que $Q \xrightarrow{\bar{a}} C'$ et pour tout \mathbb{E} , on a $F \bullet \mathbb{E}\{C\} \mathcal{S} F \bullet \mathbb{E}\{C'\}$.

Notez qu'une relation \mathcal{S} est une simulation contextuelle forte précoce ssi \mathcal{S} progresse vers \mathcal{S} . Nous synthétisons la progression $\mathcal{R} \rightsquigarrow \mathcal{S}$ sous forme de diagramme de la manière suivante :

$$\begin{array}{ccc} P & \xrightarrow{\mathcal{R}} & Q \\ \alpha \downarrow & & \downarrow \alpha \\ A & \xrightarrow{\mathcal{S}} & A' \end{array}$$

Pour notre relation \mathcal{R} , nous montrons donc que $\mathcal{R} \rightsquigarrow \mathcal{R}^*$. Dans le cas fort, cela suffit pour montrer que \mathcal{R}^* est une bisimulation contextuelle forte précoce. Soient P, Q tels que $P \mathcal{R}^* Q$. Il existe P_1, \dots, P_n tels que $P \mathcal{R} P_1 \mathcal{R} \dots P_n \mathcal{R} Q$. Nous voulons clore le diagramme suivant :

$$\begin{array}{ccc} P & \xrightarrow{\mathcal{R}} & P_1 \dots P_n \xrightarrow{\mathcal{R}} Q \\ \alpha \downarrow & & \\ A & & \end{array}$$

Comme nous avons $\mathcal{R} \rightsquigarrow \mathcal{R}^*$, nous pouvons construire $A_1 \dots A_n, A'$ par induction sur n tels que :

$$\begin{array}{ccccc} P & \xrightarrow{\approx} & P_1 & \xrightarrow{\mathcal{R}} & P_2 & \xrightarrow{\approx} & Q \\ \downarrow \tau & & & & & & \\ P' & & & & & & \end{array}$$

Par définition de \approx , nous avons par exemple :

$$\begin{array}{ccccc}
 P & \xrightarrow{\approx} & P_1 & \xrightarrow{\mathcal{R}} & P_2 & \xrightarrow{\approx} & Q \\
 \downarrow \tau & & \downarrow \tau & & \downarrow \tau & & \\
 & & P_{12} & & & & \\
 & & \downarrow \tau & & & & \\
 & & P_{13} & & & & \\
 & & \downarrow \tau & & & & \\
 & & \downarrow \tau & & & & \\
 P' & \text{---} & P'_1 & & & &
 \end{array}$$

en supposant que P_1 se réduit au moins deux fois. Nous utilisons la progression $\mathcal{R} \rightsquigarrow \approx \mathcal{R} \approx$

$$\begin{array}{ccccc}
 P & \xrightarrow{\approx} & P_1 & \xrightarrow{\mathcal{R}} & P_2 & \xrightarrow{\approx} & Q \\
 \downarrow \tau & & \downarrow \tau & & \downarrow \tau & & \\
 & & P_{12} & \xrightarrow{\approx \mathcal{R} \approx} & P_{22} & & \\
 & & \downarrow \tau & & \downarrow \tau & & \\
 & & P_{13} & & & & \\
 & & \downarrow \tau & & & & \\
 & & \downarrow \tau & & & & \\
 P' & \text{---} & P'_1 & & & &
 \end{array}$$

Le schéma P, Q, P' se répète en P_{12}, P_{22}, P_{13} . Sangiorgi évite ce problème dans la preuve du lemme de substitution pour la bisimulation faible de $HO\pi$ [42] en définissant une bisimulation modulo \approx asymétrique (définition 4.2) : \mathcal{R} est une bisimulation modulo \approx si et seulement si \mathcal{R} progresse faiblement vers $\sim \mathcal{R} \approx$. Nous pouvons alors clore le diagramme

$$\begin{array}{ccccc}
 P & \xrightarrow{\sim} & P_1 & \xrightarrow{\mathcal{R}} & P_2 & \xrightarrow{\approx} & Q \\
 \downarrow \tau & & \downarrow \tau & & \downarrow \tau & & \downarrow \tau \\
 P' & \xrightarrow{\sim} & P'_1 & \xrightarrow{\sim \mathcal{R} \approx} & P'_2 & \xrightarrow{\approx} & Q'
 \end{array}$$

et conclure que $\sim \mathcal{R} \approx$ est une bisimilarité faible par transitivité de \sim et \approx .

La méthode échoue donc dans le cas faible parce que nous prouvons que \mathcal{R}^* , et non \mathcal{R} , est une bisimulation, et nous devons considérer \mathcal{R}^* à cause de la communication d'ordre supérieur. En effet, pour relier $F_P \bullet C_P$ à $F_Q \bullet C_Q$, nous devons passer par une étape intermédiaire $F_P \bullet C_Q$ ou $F_Q \bullet C_P$. Le problème n'est donc pas spécifique aux calculs avec passivation : la méthode échoue également avec la bisimilarité faible de $HO\pi$ par exemple. En revanche, la méthode fonctionne avec la bisimilarité faible des Ambients [32]. La mobilité des ambients étant asynchrone, aucune transition ne nécessite l'évolution simultanée de plusieurs processus, comme au cours d'une communication de $HO\pi$ ou $HO\pi P$: les actions ne proviennent que d'un seul processus migrant. La clôture \mathcal{R} de la bisimilarité par les opérateurs du langage progresse donc directement vers \mathcal{R} , ce qui permet de prouver la congruence dans les cas fort et faible.

4.3 Méthode de Howe

Nous avons vu dans la section précédente que prouver qu'une congruence est une bisimulation engendre des problèmes de transitivité, qui rendent la preuve impossible directement dans le cas faible. La méthode de Howe permet de contourner ces difficultés, grâce à une relation annexe, la *clôture de Howe*, et un résultat de pseudo-simulation qui contiennent tous les deux une part de transitivité dans leur énoncé. Contrairement à la preuve par progression, la méthode de Howe peut s'appliquer dans le cas faible.

4.3.1 Résumé de la méthode

La méthode de Howe [20, 2, 15] est une méthode de preuve systématique pour montrer qu'une simulation ou une bisimulation \mathcal{R} est une congruence. Elle a initialement été utilisée pour prouver la congruence de simulations dans les langages fonctionnels paresseux [20]. Elle a ensuite été adaptée aux calculs de processus par Baldamus et Frauenstein [3] pour prouver la congruence de différentes formes de bisimilarités dans des variantes de Plain CHOCS.

La méthode peut se résumer en trois étapes : d'abord, prouver quelques propriétés de base de la clôture de Howe \mathcal{R}^\bullet de la relation. Par construction, \mathcal{R}^\bullet est une congruence et contient \mathcal{R} . En supposant que la simulation ou bisimulation \mathcal{R} est basée sur un système de transitions étiquetées $P \xrightarrow{\lambda} A$, il faut ensuite montrer une propriété de pseudo-simulation, calquée sur le schéma suivant :

Soient P, Q tels que $P \mathcal{R}^\bullet Q$. Si $P \xrightarrow{\lambda} A$, alors pour tout $\lambda \mathcal{R}^\bullet \lambda'$, il existe B tel que $Q \xrightarrow{\lambda'} B$ et $A \mathcal{R}^\bullet B$.

Cette clause est plus forte que celle de bisimilarité classique, ce qui permet de la prouver par induction : nous n'avons pas les problèmes de transitivité rencontrés dans la preuve par progression (section 4.2). Enfin, la dernière étape consiste à montrer que \mathcal{R} et \mathcal{R}^\bullet coïncident sur les processus clos. Comme \mathcal{R}^\bullet est une congruence, nous pouvons en conclure que \mathcal{R} en est une également.

La définition de la clôture de Howe repose sur l'extension de \mathcal{R} aux processus ouverts (c'est-à-dire avec une ou plusieurs variables de processus libres), notée \mathcal{R}° .

Définition 4.4. *Soient P, Q deux processus ouverts. Nous avons $P \mathcal{R}^\circ Q$ si et seulement si nous avons $P\sigma \mathcal{R} Q\sigma$ pour toute substitution σ qui clôt P et Q .*

La clôture est définie par induction comme la plus petite congruence qui contient \mathcal{R}° et est close par composition à droite avec \mathcal{R}° .

Définition 4.5. *La clôture de Howe \mathcal{R}^\bullet d'une relation \mathcal{R} est la plus petite relation vérifiant :*

- $\mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$;
- $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$;
- pour tout opérateur op du calcul, $\tilde{P} \mathcal{R}^\bullet \tilde{Q}$ implique $op(\tilde{P}) \mathcal{R}^\bullet op(\tilde{Q})$.

Par définition, \mathcal{R}^\bullet est une congruence, et la composition avec \mathcal{R}° permet d'utiliser la transitivité dans certaines preuves et de montrer certaines propriétés supplémentaires.

Remarque 4.3. *Dans la littérature (par exemple [20, 15, 19]), la clôture de Howe est habituellement définie par induction par la règle suivante, dérivée pour chacun des opérateurs op du calcul :*

$$\frac{\tilde{P} \mathcal{R}^\bullet \tilde{R} \quad op(\tilde{R}) \mathcal{R}^\circ Q}{op(\tilde{P}) \mathcal{R}^\bullet Q}$$

Les deux définitions sont équivalentes (cf. [15] pour la preuve). Nous pensons que la définition 4.5 est plus facile à comprendre et à manipuler dans les preuves.

Nous souhaitons montrer qu'une bisimilarité \mathcal{R} est une congruence. Par définition, nous avons $\mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$, et donc $\mathcal{R} \subseteq \mathcal{R}^\bullet$ sur les termes clos. Pour établir l'inclusion inverse, nous montrons que la restriction de \mathcal{R}^\bullet aux termes clos est une bisimulation. Pour cela, nous devons montrer deux propriétés classiques de la clôture de Howe.

Lemme 4.5. *Soit \mathcal{R} une relation réflexive. Si $P \mathcal{R}^\bullet Q$ et $R \mathcal{R}^\bullet S$, alors on a $P\{R/X\} \mathcal{R}^\bullet Q\{S/X\}$.*

Ce lemme est utilisé pour établir le résultat de pseudo-simulation (deuxième étape de la méthode). Nous esquissons la preuve, donnée en appendice A.1, pour justifier en quoi la clause $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$ est utile dans la définition 4.5. La preuve est par induction sur la dérivation de $P \mathcal{R}^\bullet Q$. Nous traitons uniquement le cas de base $P \mathcal{R}^\circ Q$. Comme nous avons $R \mathcal{R}^\bullet S$ et que \mathcal{R}^\bullet est une congruence, nous avons $P\{R/X\} \mathcal{R}^\bullet P\{S/X\}$. Soit σ une substitution qui clôt S et P, Q sauf pour X . Par définition de \mathcal{R}° , nous avons $P\{S\sigma/X\} \mathcal{R} Q\{S\sigma/X\}$, c'est-à-dire $P\{S/X\} \mathcal{R}^\circ Q\{S/X\}$. Par conséquent nous avons $P\{R/X\} \mathcal{R}^\bullet \mathcal{R}^\circ Q\{S/X\}$, c'est-à-dire $P\{R/X\} \mathcal{R}^\bullet Q\{S/X\}$.

Remarque 4.4. *On peut également définir une clôture de Howe en considérant $\mathcal{R}^\circ \mathcal{R}^\bullet \subseteq \mathcal{R}^\bullet$ comme clause transitive à la place de $\mathcal{R}^\bullet \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet$. Cependant la composition à gauche avec \mathcal{R}° pose problème dans le cas faible, alors que la composition à droite fonctionne dans les cas fort et faible.*

La propriété de pseudo-simulation permet seulement de déduire que \mathcal{R}^\bullet (restreint aux termes clos) est une simulation. Pour prouver que \mathcal{R}^\bullet est une bisimulation, nous avons besoin du lemme suivant, dont la preuve est donnée en appendice A.1.

Lemme 4.6. *Soit \mathcal{R} une relation d'équivalence. La clôture réflexive et transitive $(\mathcal{R}^\bullet)^*$ de \mathcal{R}^\bullet est symétrique.*

Nous prouvons alors que la restriction de $(\mathcal{R}^\bullet)^*$ aux termes clos est une bisimulation. Nous avons donc $\mathcal{R} \subseteq \mathcal{R}^\bullet \subseteq (\mathcal{R}^\bullet)^* \subseteq \mathcal{R}$ sur les termes clos, ce qui permet de conclure que \mathcal{R} est une congruence.

La principale difficulté dans l'application de la méthode est d'établir et de prouver le résultat de pseudo-simulation pour la clôture de Howe. Dans la partie suivante, nous expliquons pourquoi donner un tel résultat pose problème pour les bisimilarités contextuelles précoces (définitions 2.15 et 2.16). Nous justifions ainsi pourquoi cette méthode n'a pas été utilisée avec de telles équivalences jusqu'ici.

4.3.2 Problème avec la communication d'ordre supérieur

L'étape cruciale de la méthode de Howe est la définition et la preuve de la propriété de pseudo-simulation pour \mathcal{R}^\bullet . Nous rappelons que ce résultat doit suivre le format suivant :

Soient P, Q tels que $P \mathcal{R}^\bullet Q$. Si $P \xrightarrow{\lambda} A$, alors pour tout $\lambda \mathcal{R}^\bullet \lambda'$, il existe B tel que $Q \xrightarrow{\lambda'} B$ et $A \mathcal{R}^\bullet B$.

En particulier, la clôture de Howe doit être étendue aux étiquettes λ . Dans le cas d'une bisimilarité précoce, un processus ne répond que s'il dispose de toutes les informations nécessaires. Par exemple dans le cas d'une émission, la réponse se fait en connaissance de la fonction qui reçoit le message. Pour une bisimilarité d'ordre supérieur basée sur un système de transitions avec fonctions et concrétions, cela revient à placer la fonction choisie dans l'étiquette pour l'émission, et la concrétion dans l'étiquette pour la réception. Cette observation conduit alors à chercher à prouver la propriété de pseudo-simulation suivante pour la bisimilarité contextuelle précoce \sim de $\text{HO}\pi\text{P}$:

Conjecture 4.1. *Si $P \sim^\bullet Q$, alors :*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \sim^\bullet Q'$;
- pour tout $P \xrightarrow{a} F$, pour tout $C \sim^\bullet C'$, il existe F' telle que $Q \xrightarrow{a} F'$ et $F \bullet C \sim^\bullet F' \bullet C'$;
- pour tout $P \xrightarrow{\bar{a}} C$, pour tout $F \sim^\bullet F'$, $\mathbb{E} \sim^\bullet \mathbb{E}'$, il existe C' tel que $Q \xrightarrow{\bar{a}} C'$ et $F \bullet \mathbb{E}\{C\} \sim^\bullet F' \bullet \mathbb{E}'\{C'\}$.

Ces clauses soulèvent plusieurs problèmes : nous avons d'abord à trouver des extensions de la clôture de Howe aux fonctions et concrétions qui respectent le caractère précoce de la bisimilarité. Même en supposant l'existence de telles extensions, il existe des difficultés

dans la preuve de la conjecture 4.1, notamment dans le cas de la communication d'ordre supérieur. La preuve se fait par induction sur la dérivation de $P \sim^\bullet Q$. Supposons que $P \sim^\bullet Q$ a été dérivé du troisième cas de la définition 4.5 pour l'opérateur de composition parallèle. Nous avons donc $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, avec $P_1 \sim^\bullet Q_1$ et $P_2 \sim^\bullet Q_2$. Nous nous plaçons dans le cas d'une transition $P \xrightarrow{\tau} P'$ obtenue par communication d'ordre supérieur (règle HO) : il existe F, C tels que $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\bar{a}} C$ et $P' = F \bullet C$.

Nous voulons trouver Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \sim^\bullet Q'$ en utilisant la même règle HO ; nous devons donc trouver F', C' tels que $Q \xrightarrow{\tau} F' \bullet C'$. Cependant nous ne pouvons pas utiliser la clause de réception de l'hypothèse d'induction avec P_1, Q_1 : pour déduire l'existence de F' tel que $Q \xrightarrow{a} F'$, nous devons d'abord fournir une concrétion C' telle que $C \sim^\bullet C'$. De même, nous ne pouvons pas utiliser la clause d'émission avec P_1, Q_2 : pour déduire l'existence de C' tel que $Q_2 \xrightarrow{\bar{a}} C'$, nous devons fournir une fonction F' telle que $F \sim^\bullet F'$. Nous ne pouvons pas contourner cette dépendance mutuelle, la preuve par induction de la conjecture 4.1 échoue donc dans le cas de la communication d'ordre supérieur.

Remarque 4.5. *Notez que le problème présenté ici dépend plus de la bisimilarité que du calcul : nous avons le même problème avec la bisimilarité contextuelle précoce de $HO\pi$, du $Kell$, de $Homer$, etc.*

Remarque 4.6. *Dans le cas d'une bisimilarité tardive, la réponse à une transition se fait indépendamment du contexte de test choisi. Par exemple, la réponse à une émission se fait sans connaître le récepteur, et la correspondance entre les deux concrétions doit avoir lieu quel que soit la fonction choisie pour réagir. Nous n'avons donc pas le même problème d'interdépendance ; la méthode peut s'appliquer pour prouver la congruence d'une bisimilarité tardive [19].*

Une manière simple de casser l'interdépendance entre fonctions et concrétions est d'assouplir le caractère précoce de la bisimilarité. Une approche, utilisée dans [14], est d'écrire la clause d'émission dans un style tardif : une émission répond à une autre émission indépendamment de la fonction qui reçoit le message. La bisimilarité obtenue est alors dite *semi-précoce*, ou précoce sur les fonctions, notée \sim_{ie} . Cette définition permet de casser la symétrie et l'interdépendance dans le problème de la communication : on peut alors d'abord déterminer la réponse C' , avant d'en déduire la réponse F' qui dépend de C' . Concrètement, la clôture de Howe est étendue aux concrétions $C \sim_{ie}^\bullet C'$ (dans un style tardif), et une propriété de pseudo-simulation similaire à la conjecture 4.1 est prouvée, sauf que la clause pour l'émission est changée en :

- pour tout $P \xrightarrow{\bar{a}} C$, il existe C' tel que $Q \xrightarrow{\bar{a}} C'$ et $C \sim_{ie}^\bullet C'$.

Cependant, cette approche ne permet pas d'obtenir un résultat de caractérisation de la congruence barbue dans le cas faible. En effet, la bisimilarité semi-précoce doit être écrite dans un style semi-faible, dans lequel les actions internes ne sont pas autorisées après une action visible. Le style semi-faible est nécessaire pour garder la clause sur les concrétions indépendante des fonctions. Cette stratégie n'est pas complètement satisfaisante, étant donné que les bisimilarités semi-faibles ne sont généralement pas complètes.

4.4 Autres méthodes et conclusions

Plutôt que de prouver la congruence en raisonnant sur la bisimilarité, il est possible de définir le système de transitions étiquetées de telle sorte que la bisimilarité associée soit automatiquement une congruence. Nous décrivons rapidement trois méthodes qui reposent sur ce principe : les formats de règles [37], la génération à partir de la réduction [39, 40] et l'encodage dans les systèmes réactifs [5].

Les formats de règles [16, 53, 4] permettent de garantir la congruence de la bisimilarité associée à un système de transitions étiquetées en posant des contraintes sur l'écriture des

règles de ce système. Vérifier qu'un ensemble de règles respecte les contraintes d'un format est généralement plus simple que de prouver directement la congruence de la bisimilarité. Pour les calculs d'ordre supérieurs, Mousavi et coll. [37] proposent les formats Promoted et Higher-Order PANTH. Le format Promoted PANTH garantit que la bisimilarité classique (dans laquelle la réponse à une action doit être la même action) est une congruence, et le format Higher-Order PANTH assure la congruence de la bisimilarité d'ordre supérieur (dans laquelle la réponse à une action peut être une action bisimilaire, cf. section 2.2.2). Les auteurs montrent qu'il est facile de vérifier que la bisimilarité d'ordre supérieur de CHOCS [51] est une congruence. Cependant, les formats proposés permettent de conclure uniquement dans le cas fort. En outre, ils interdisent l'écriture de conditions annexes sur les lieux et les noms (par exemple $a \in \text{fn}(R)$), ce qui empêche toute extension de portée paresseuse comme en $\text{HO}\pi\text{P}$.

Dans [39, 40], les règles du système de transitions étiquetées sont générées automatiquement à partir des règles de réduction et des observables de telle sorte que la bisimilarité associée est une congruence. Les règles de réduction sont décomposées pour identifier le sous-terme en cours de réduction et le contexte que doit fournir l'environnement pour que la réduction ait lieu. Appliquée à $\text{HO}\pi$ [39], la méthode permet de retrouver la bisimilarité contextuelle de Sangiorgi [42]. Dans les Ambients [40], la bisimilarité obtenue est une congruence par rapport à tous les opérateurs du langage, ce qui est une amélioration par rapport à la relation définie dans [32], qui n'est une congruence que sur les contextes d'évaluation. Néanmoins, la méthode n'a été appliquée jusqu'ici que dans le cas fort.

Les calculs de processus peuvent être vus comme des *systèmes réactifs* [24], dans lesquels l'évolution d'un terme $\mathbb{C}\{P\}$ vers Q s'écrit $P \xrightarrow{\mathbb{C}} Q$. L'enjeu est alors de trouver le contexte \mathbb{C} minimal pour lequel une interaction peut se déclencher. Ainsi, Bonchi et coll. [5] proposent pour les Ambients un système de transitions étiquetées dérivé des systèmes réactifs, et définissent des caractérisations des congruences barbues forte et faible sous forme de bisimilarités barbues. Nous ne savons pas s'il est possible d'encoder un calcul avec passivation sous forme de système réactif.

Les preuves de congruence les plus courantes échouent avec la bisimilarité contextuelle faible précoce dans les calculs avec passivation pour des raisons souvent sans rapport avec la passivation. Ainsi, la preuve par progression échoue dans le cas faible à cause de la communication d'ordre supérieur synchrone, et la méthode de Howe ne peut aboutir à cause du caractère précoce de la bisimilarité. La méthode de Sangiorgi, dans laquelle la congruence est prouvée d'abord sur les contextes d'évaluation avant d'être étendue à tous les contextes, ne s'applique pas avec un opérateur de passivation, qui peut transformer un contexte d'évaluation en un contexte quelconque.

Dans le prochain chapitre, nous proposons une bisimilarité dont le caractère précoce est légèrement relâché, pour permettre l'application de la méthode de Howe dans le cas faible, tout en gardant le pouvoir discriminant de la bisimilarité contextuelle faible précoce.

Chapitre 5

Sémantique à complément

Dans ce chapitre, nous proposons un nouveau type de système de transitions étiquetées ainsi que la bisimulation associée, appelés ensemble *sémantique à complément*. L'objectif est de permettre l'utilisation de la méthode Howe pour prouver la congruence d'une bisimulation précoce faible. Nous avons vu dans le chapitre précédent (section 4.3.2) que la bisimilarité précoce uniquement sur la réception permet l'application de la méthode de Howe, mais uniquement pour des bisimulations semi-faibles. Dans notre bisimilarité, nous considérons une clause pour l'émission ni précoce ni tardive : la réponse à une émission ne dépend plus d'une fonction, mais d'un processus qui peut recevoir le message (qui peut donc se réduire vers une fonction).

Ce changement, en apparence infime, nous permet de casser le problème de symétrie apparaissant dans le cas de la communication dans la preuve de pseudo-simulation (section 4.3.2). Nous rappelons que dans ce cas, nous avons P_1 et P_2 en relation respectivement avec Q_1 et Q_2 , $P_1 \xrightarrow{a} F$ et $P_2 \xrightarrow{\bar{a}} C$. Nous cherchons F' et C' tels que $Q_1 \xrightarrow{a} F'$, $Q_2 \xrightarrow{\bar{a}} C'$ et $F \bullet C$ est directement en relation avec $F' \bullet C'$ (sans étape de transitivité). Avec notre nouvelle bisimulation, la transition $Q_2 \xrightarrow{\bar{a}} C'$ correspondant à la transition $P_2 \xrightarrow{\bar{a}} C$ dépend du processus P_1 , et non plus d'une fonction inconnue. Nous pouvons alors trouver une fonction F' depuis Q_1 qui correspond à la transition $P_1 \xrightarrow{a} F$; cette fonction dépend de C' dans un style précoce classique.

Techniquement, notre nouvelle sémantique n'utilise plus de fonctions ni de concrétions. Dans le système de transitions étiquetées, lorsqu'une communication entre P et Q a lieu et que le message provient de P , une transition d'origine P est créée avec pour étiquette Q (règle HO^π en figure 5.1 ou HO_7^π en figure 5.2). Plus haut dans l'arbre de dérivation, nous trouvons le message émis par P , et nous passons alors à l'étude de la réception de message par Q , tout en connaissant exactement le message émis. La preuve de pseudo-simulation pour la relation de Howe repose sur cette sérialisation dans le système de transitions, qui illustre la cassure dans la symétrie. En outre, la différence entre une relation complètement précoce et notre relation est suffisamment petite, nous permettant ainsi de montrer qu'en fait elles coïncident.

5.1 Sémantique à complément pour $\text{HO}\pi$

Dans cette section, nous définissons une sémantique à complément pour $\text{HO}\pi$ afin de montrer en quoi cette sémantique est adaptée à l'application de la méthode de Howe.

5.1.1 Système de transitions étiquetées à complément

Nous proposons un système de transitions étiquetées $P \xrightarrow{\lambda} P'$ dans lequel un processus évolue toujours vers un autre processus. Il existe trois types de transitions : les actions internes $P \xrightarrow{\tau} P'$, les réceptions de message $P \xrightarrow{a,R} P'$ et les émissions de messages $P \xrightarrow{\bar{a},R} P'$. L'étiquette λ contient le contexte complémentaire utilisé pour établir la bisimilarité

$$\begin{array}{c}
\frac{a(X)P \xrightarrow{a,R} P\{R/X\}}{\text{IN}^\pi} \quad \frac{R \xrightarrow{a,P_1} R'}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a},R} R' \mid P_2} \text{OUT}^\pi \quad \frac{P_1 \xrightarrow{\lambda} P'_1}{P_1 \mid P_2 \xrightarrow{\lambda} P'_1 \mid P_2} \text{PAR}^\pi \\
\\
\frac{P \xrightarrow{\lambda} P' \quad a \neq n(\lambda)}{\nu a.P \xrightarrow{\lambda} \nu a.P'} \text{RESTR}^\pi \quad \frac{P \xrightarrow{\lambda} P'}{!P \xrightarrow{\lambda} P' \mid !P} \text{REPLIC}^\pi \\
\\
\frac{P \xrightarrow{\bar{a},P} P'}{!P \xrightarrow{\tau} P' \mid !P} \text{REPLIC-HO}^\pi \quad \frac{P \xrightarrow{\bar{a},Q} P'}{P \mid Q \xrightarrow{\tau} P'} \text{HO}^\pi
\end{array}$$

FIG. 5.1 – Système à complément pour $\text{HO}\pi$

entre deux processus ; pour $\text{HO}\pi$, nous avons juste besoin d'un processus R , employé de manière différente entre les jugements de réception et d'émission.

Les règles du système sont données en figure 5.1, à l'exception du symétrique des règles PAR^π et HO^π . Pour les étiquettes d'ordre supérieur, on définit $n(a, R) = n(\bar{a}, R) = a$. Le jugement d'action interne $P \xrightarrow{\tau} P'$ a la même signification que son équivalent en sémantique contextuelle. Les règles de déduction sont également similaires, à l'exception de la règle HO^π , qui repose sur le jugement d'émission ; nous expliquerons cette règle ultérieurement. Le jugement de réception $P \xrightarrow{a,R} P'$ signifie que P devient P' après avoir reçu le message R sur a . En sémantique contextuelle, cela signifie qu'il existe une fonction F telle que $P \xrightarrow{a} F$ et $P' = F \circ R$. Le jugement de réception de la sémantique à complément est juste une reformulation de son équivalent contextuel en style précoce.

La principale différence entre les deux sémantiques est dans le jugement d'émission. La transition $P \xrightarrow{\bar{a},R} P'$ signifie que P est capable d'envoyer un message sur a qui peut être reçu par R , et le résultat de la communication entre P et R donne P' . Ce n'est pas une simple réécriture de la transition contextuelle $P \xrightarrow{\bar{a}} C$ en style précoce ; le label d'émission en sémantique à complément contient un processus R et non une fonction F . Le lien entre les deux sémantiques est informellement le suivant : la transition $P \xrightarrow{\bar{a},R} P'$ signifie qu'il existe F et C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$ et $P' = F \bullet C$.

Contrairement à la règle contextuelle équivalente OUT , la règle OUT^π a une prémisse $R \xrightarrow{a,P_1} R'$, afin de vérifier que R est bien capable de recevoir le message P_1 sur a . Le processus R' obtenu est alors mis en parallèle avec la continuation P_2 : nous obtenons $\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a},R} R' \mid P_2$. Le résultat est donc bien la communication entre $\bar{a}\langle P_1 \rangle P_2$ et Q . Les règles PAR^π , REPLIC^π et RESTR^π sont classiques ; cependant il est à noter que la règle RESTR^π étend la portée de a que a appartienne ou non aux noms libres du message émis. Il faut remarquer que le message émis n'apparaît pas dans un jugement d'émission : écrire l'extension de portée paresseuse, telle qu'elle est définie en sémantique contextuelle, rend le système de transitions plus complexe, comme nous le verrons avec $\text{HO}\pi\text{P}$. La politique choisie pour l'extension de portée n'a pas d'influence sur la sémantique de $\text{HO}\pi$, c'est pourquoi nous utilisons l'extension de portée systématique, plus simple à écrire dans notre système de transitions.

La règle de communication HO^π a pour seule prémisse $P \xrightarrow{\bar{a},Q} P'$; par définition P' est le résultat de la communication de P avec Q , donc nous pouvons en déduire directement la conclusion souhaitée $P \mid Q \xrightarrow{\tau} P'$. La sémantique à complément est conforme à la sémantique contextuelle, comme l'indique le lemme suivant :

Lemme 5.1. *Soit P un processus de $\text{HO}\pi$.*

- Nous avons $P \xrightarrow{\tau} \equiv P'$ ssi $P \xrightarrow{\tau} \equiv P'$.
- Si $P \xrightarrow{a} F$, alors pour tout R , nous avons $P \xrightarrow{a,R} F \circ R$. Si $P \xrightarrow{a,R} P'$, alors il existe

- F tel que $P \xrightarrow{a} F$ et $P' = F \circ R$.
- Si $P \xrightarrow{\bar{a}} C$, alors pour tout R tel qu'il existe F tel que $R \xrightarrow{a} F$, nous avons $P \xrightarrow{\bar{a}, R} \equiv F \bullet C$. Si $P \xrightarrow{\bar{a}, R} P'$, alors il existe F et C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$ et $P' \equiv F \bullet C$.

La preuve est donnée en appendice A.2.1. La correspondance entre les systèmes de transition est modulo congruence structurelle à cause de l'extension de portée, qui est systématique en sémantique à complément et paresseuse en sémantique contextuelle. Par exemple, pour $P \triangleq a(X)X \mid \nu b.\bar{a}\langle c.0 \rangle b.0$, nous avons $P \xrightarrow{\tau} c.0 \mid \nu b.b.0$ et $P \xrightarrow{\tau} \nu b.(c.0 \mid b.0)$.

5.1.2 Bisimulation associée

Nous définissons maintenant la bisimilarité à complément et prouvons sa correction en utilisant le méthode de Howe. Le résultat en lui-même, à savoir la définition d'une bisimilarité correcte en $\text{HO}\pi$, n'est pas nouveau (cf. section 2.2.3); le but de cette section est d'expliquer pourquoi la sémantique à complément est adaptée à l'utilisation de la méthode de Howe.

La bisimulation forte à complément est simplement la bisimulation associée au système de transition à complément :

Définition 5.1. Une relation \mathcal{R} sur les termes clos est une simulation forte à complément ssi pour tout $P \mathcal{R} Q$, si $P \xrightarrow{\lambda} P'$, alors il existe Q' tel que $Q \xrightarrow{\lambda} Q'$ et $P' \mathcal{R} Q'$.

Une relation \mathcal{R} est une bisimulation forte à complément ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations fortes à complément. La bisimilarité forte à complément \sim_m est la plus grande bisimulation forte à complément.

Dans le cas de l'émission de message $P \xrightarrow{\bar{a}, R} P'$, la réponse Q' dépend du processus récepteur R . La bisimulation est donc proche d'une bisimulation précoce, bien que nous ne savons pas précisément de quelle manière R consomme le message (c'est-à-dire quelle fonction reçoit le message). Cette différence nous permet d'appliquer la méthode de Howe pour établir la congruence de \sim_m . Nous rappelons que la méthode de Howe repose sur une propriété de pseudo simulation de la clôture de Howe \sim_m^\bullet .

Lemme 5.2. Soient P et Q deux processus clos. Si $P \sim_m^\bullet Q$, alors

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $P' \sim_m^\bullet Q'$;
- pour tout R clos tel que $P \xrightarrow{a, R} P'$, pour tout R' clos tel que $R \sim_m^\bullet R'$, il existe Q' tel que $Q \xrightarrow{a, R'} Q'$ et $P' \sim_m^\bullet Q'$;
- pour tout R clos tel que $P \xrightarrow{\bar{a}, R} P'$, pour tout R' clos tel que $R \sim_m^\bullet R'$, il existe Q' tel que $Q \xrightarrow{\bar{a}, R'} Q'$ et $P' \sim_m^\bullet Q'$.

La preuve du lemme 5.2, donnée en appendice A.2.2, se fait par induction sur la dérivation du jugement $P \sim_m^\bullet Q$. Cependant, nous n'avons pas de problème dans le cas de la communication, comme avec la sémantique contextuelle (section 4.3.2). Nous rappelons que dans ce cas, nous avons $P = P_1 \mid P_2$, $Q = Q_1 \mid Q_2$, avec $P_1 \sim_m^\bullet Q_1$ et $P_2 \sim_m^\bullet Q_2$. La transition $P \xrightarrow{\tau} P'$ provient de la règle $\text{HO}\pi$, donc nous avons $P_1 \xrightarrow{\bar{a}, P_2} P'$.

Nous avons $P_1 \sim_m^\bullet Q_1$, $P_2 \sim_m^\bullet Q_2$ et $P_1 \xrightarrow{\bar{a}, P_2} P'$; nous pouvons appliquer directement la clause d'émission de l'hypothèse d'induction. Il existe donc Q' tel que $Q_1 \xrightarrow{\bar{a}, Q_2} Q'$ et $P' \sim_m^\bullet Q'$. Ainsi nous avons $Q \xrightarrow{\tau} Q'$ par la règle $\text{HO}\pi$, nous avons donc le résultat souhaité dans ce cas. Le reste de la preuve de Howe ne pose pas de difficulté, et nous avons donc le résultat suivant :

Théorème 5.1. La relation \sim_m est une congruence

La preuve complète se trouve en appendice A.2.2. Il nous reste à prouver que la bisimilarité à complément est aussi discriminante que la bisimilarité contextuelle précoce. Ce résultat découle principalement de la correspondance entre les systèmes à transitions étiquetées (lemme 5.1). Les deux relations diffèrent dans leur traitement des réceptions de message : la bisimilarité à complément teste avec un processus, alors que la bisimilarité contextuelle teste avec une concrétion. En particulier la bisimilarité contextuelle teste les concrétions de la forme $\langle P \rangle \mathbf{0}$, ce qui revient à tester avec un processus P .

Lemme 5.3. *Nous avons $\sim \subseteq \sim_m$.*

La preuve se fait en montrant que \sim est une bisimulation à complément (modulo \equiv). L'inclusion opposée repose sur la congruence de \sim_m (théorème 5.1).

Lemme 5.4. *Nous avons $\sim_m \subseteq \sim$.*

Nous montrons que \sim_m est une bisimulation contextuelle précoce forte. Dans le cas de la réception, nous avons informellement $P'\{R/X\} \sim_m Q'\{R/X\}$. Par congruence, cela implique $\nu \tilde{b}.(P'\{R/X\} \mid S) \sim_m \nu \tilde{b}.(Q'\{R/X\} \mid S)$, soit $(X)P' \bullet \nu \tilde{b}.\langle R \rangle S \sim_m (X)Q' \bullet \nu \tilde{b}.\langle R \rangle S$, ce qui est le résultat souhaité. Les preuves des lemmes 5.3 et 5.4 sont données en appendice A.2.3.

Des résultats similaires peuvent être obtenu dans le cas faible. On note $\xRightarrow{\tau}$ la clôture réflexive et transitive de $\xrightarrow{\tau}$, et on définit $\xRightarrow{a,R} \triangleq \xRightarrow{\tau} \xrightarrow{a,R} \xRightarrow{\tau}$. La définition faible du jugement d'émission de message $\xRightarrow{\bar{a},R}$ est plus complexe : nous devons prendre en compte le fait qu'une transition $P \xrightarrow{\bar{a},R} P'$ contient une communication entre les processus P et R . Or dans le cas faible, le processus R peut effectuer des actions internes avant de recevoir le message de P . Nous définissons donc $P \xRightarrow{\bar{a},R} P'$ comme $P \xRightarrow{\tau} \xrightarrow{\bar{a},R'} \xRightarrow{\tau} P'$, avec R' tel que $R \xRightarrow{\tau} R'$.

Définition 5.2. *Une relation \mathcal{R} sur les termes clos est une simulation faible à complément ssi pour tout $P \mathcal{R} Q$, si $P \xRightarrow{\lambda} P'$, alors il existe Q' tel que $Q \xRightarrow{\lambda} Q'$ et $P' \mathcal{R} Q'$.*

Une relation \mathcal{R} est une bisimulation faible à complément ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations faibles à complément. La bisimilarité faible à complément \approx_m est la plus grande bisimulation faible à complément.

En utilisant les mêmes techniques de preuves que dans le cas fort, nous obtenons les résultats suivants :

Théorème 5.2. *La relation \approx_m est une congruence.*

Lemme 5.5. *Nous avons $\approx = \approx_m$.*

Li et Liu [31] ont défini un système de transitions étiquetées similaire à celui que nous proposons, et ont prouvé la correspondance entre la bisimilarité associée, la congruence barbue et la bisimilarité contextuelle dans le cas fort. La preuve de correction de leur relation est ad hoc, et ne repose pas sur la méthode de Howe

5.2 Application à $\text{HO}\pi\text{P}$

Nous avons vu que la sémantique à complément, en considérant des processus et non plus des fonctions dans le jugement d'émission, permet l'utilisation de la méthode de Howe pour prouver la congruence de la bisimilarité associée. Nous allons maintenant définir une sémantique à complément pour $\text{HO}\pi\text{P}$.

$$\begin{array}{c}
\frac{a(X)P \xrightarrow{a,R} P\{R/X\}}{\text{IN}_i^p} \qquad \frac{P \xrightarrow{\mu} P'}{P \mid Q \xrightarrow{\mu} P' \mid Q} \text{PAR}_{i\tau}^p \\
\\
\frac{P \xrightarrow{\mu} P' \quad a \neq n(\mu)}{\nu a.P \xrightarrow{\mu} \nu a.P'} \text{RESTR}_{i\tau}^p \qquad \frac{P \xrightarrow{\bar{a},P,\square} P'}{!P \xrightarrow{\tau} P' \mid !P} \text{REPLIC-HO}_\tau^p \\
\\
\frac{P \xrightarrow{\mu} P'}{!P \xrightarrow{\mu} P' \mid !P} \text{REPLIC}_{i\tau}^p \qquad \frac{P \xrightarrow{\mu} P'}{a[P] \xrightarrow{\mu} a[P']} \text{LOC}_{i\tau}^p \qquad \frac{P \xrightarrow{\bar{a},Q,\square} P'}{P \mid Q \xrightarrow{\tau} P'} \text{HO}_\tau^p
\end{array}$$

FIG. 5.2 – Sémantique à complément pour HO π P : actions internes et réception de message

5.2.1 Système de transitions étiquetées à complément

Par rapport à HO π , nous devons faire face à deux difficultés supplémentaires. Nous devons d'abord introduire dans nos étiquettes les contextes de bisimulation \mathbb{E} , utilisés dans les clauses de bisimulations (définitions 2.15 et 2.16). Nous devons également traiter plus finement l'extension de portée paresseuse, étant donné que les noms restreints peuvent sortir des localités par communication mais pas par congruence structurelle. Nous ne pouvons plus systématiquement étendre la portée des noms, et obtenir une sémantique équivalente à la sémantique contextuelle (modulo \equiv) comme pour HO π .

Les jugements d'action interne $P \xrightarrow{\tau} P'$ et de réception de message $P \xrightarrow{a,R} P'$ sont les mêmes que pour HO π , à l'exception des règles que nous devons rajouter pour les localités. On note $\xrightarrow{\mu}$ pour $\xrightarrow{\tau}$ ou $\xrightarrow{a,R}$. Les règles pour les transitions $\xrightarrow{\mu}$ sont données en figure 5.2, à l'exception du symétrique des règles $\text{PAR}_{i\tau}^p$ et HO_τ^p . La règle HO_τ^p dépend du jugement d'émission et sera expliquée par la suite.

Les règles pour le jugement d'émission $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$ sont données en figure 5.3, à l'exception du symétrique de la règle PAR_o^p . Nous rappelons que la bisimilarité contextuelle de HO π P (définition 2.15) compare les concrétions en les faisant réagir avec une fonction F et un contexte de bisimulation \mathbb{E} . En sémantique à complément, nous remplaçons les fonctions par des processus R , et nous introduisons les contextes \mathbb{E} dans les étiquettes. Ainsi, la transition $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$ signifie que P , placé dans le contexte \mathbb{E} , émet un message sur a et R le reçoit ; nous avons $\mathbb{E}\{P\} \mid R \xrightarrow{\tau} P'$ par communication sur a . En sémantique contextuelle, cela équivaut à l'existence de F et C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$ et $P' = F \bullet \mathbb{E}\{C\}$.

Nous rappelons que le jugement d'émission $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$ ne mentionne pas le message émis ; or nous avons besoin de connaître les noms libres du message pour effectuer l'extension de portée paresseuse. C'est pourquoi le jugement garde l'ensemble des noms \tilde{b} dont la portée peut être étendue. L'extension de portée peut être nécessaire pour le processus P considéré (par exemple $P = \nu c.\bar{a}\langle P_1 \rangle P_2$ avec $c \in \text{fn}(P_1)$) ou peut être provoquée par le contexte de bisimulation (par exemple $P = \bar{a}\langle P_1 \rangle P_2$ et $\mathbb{E} = d[\nu c.(\square \mid \bar{c}\langle \mathbf{0} \rangle \mathbf{0})]$ avec $c \in \text{fn}(P_1)$). Nous définissons d'abord un jugement auxiliaire $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$ qui interdit le second type de capture, avant de généraliser les transitions à tout contexte \mathbb{E} .

La règle OUT_o^p gère l'émission de message $\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a},R,\mathbb{E}} R' \mid \mathbb{E}\{P_2\}$. Comme pour HO π , nous avons la prémisse $R \xrightarrow{a,P_1} R'$. Nous définissons pour l'instant le jugement sans capture des noms libres du message $\text{fn}(P_1) = \tilde{b}$, c'est pourquoi nous ajoutons la prémisse $\text{bn}(\mathbb{E}) \cap \tilde{b} = \emptyset$. Nous gardons les noms \tilde{b} dans l'étiquette pour permettre aux règles EXTR_o^p et RESTR_o^p d'effectuer ou non l'extension de portée.

$$\begin{array}{c}
\frac{\text{fn}(P_1) = \tilde{b} \quad R \xrightarrow{a, P_2} R' \quad \text{bn}(\mathbb{E}) \cap \tilde{b} = \emptyset}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} R' \mid \mathbb{E}\{P_1\}} \text{OUT}_o^p \\
\\
\frac{\text{fn}(P) = \tilde{b} \quad R \xrightarrow{a, P} R' \quad \text{bn}(\mathbb{E}) \cap \tilde{b} = \emptyset}{a[P] \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} R' \mid \mathbb{E}\{\mathbf{0}\}} \text{PASSIV}_o^p \quad \frac{P \xrightarrow{\bar{a}, R, \mathbb{E}\{b[\square]\}}_{\tilde{b}} P'}{b[P] \xrightarrow{\bar{a}, Q, \mathbb{E}}_{\tilde{b}} P'} \text{LOC}_o^p \\
\\
\frac{P \xrightarrow{\bar{a}, R, \mathbb{E}\{\square \mid !P\}}_{\tilde{b}} P'}{!P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'} \text{REPLIC}_o^p \quad \frac{P_1 \xrightarrow{\bar{a}, R, \mathbb{E}\{\square \mid P_2\}}_{\tilde{b}} P'}{P_1 \mid P_2 \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'} \text{PAR}_o^p \\
\\
\frac{P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P' \quad c \neq a \quad c \in \tilde{b}}{\nu c.P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b} \setminus c} \nu c.P'} \text{EXTR}_o^p \quad \frac{P \xrightarrow{\bar{a}, R, \mathbb{E}\{\nu c.\square\}}_{\tilde{b}} P' \quad c \neq a \quad c \notin \tilde{b}}{\nu c.P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'} \text{RESTR}_o^p \\
\\
\frac{P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'}{P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'} \text{CFREE}_o^p \quad \frac{P \xrightarrow{\bar{a}, R, \mathbb{E}\{\mathbb{F}\}}_{\tilde{b}} P' \quad c \in \tilde{b}}{P \xrightarrow{\bar{a}, R, \mathbb{E}\{\nu c.\mathbb{F}\}}_{\tilde{b}} \nu c.P'} \text{CAPT}_o^p
\end{array}$$

FIG. 5.3 – Sémantique à complément pour HO π P : émission de message

Par exemple, soient $P = \bar{a}\langle P_1 \rangle P_2$, $c \in \text{fn}(P_1)$ et R tels que $R \xrightarrow{a, P_1} R'$. Lorsque $\nu c.P$ émet le message P_1 , la portée de c doit être étendue pour inclure le récepteur R de P_1 : nous voulons donc obtenir $\nu c.(R' \mid \mathbb{E}\{P_2\})$ comme processus résultant. Par la règle EXTR_o^p , nous déduisons $\nu c.P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b} \setminus c} \nu c.P'$ à partir de $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$. Ici nous avons $P' = R' \mid \mathbb{E}\{P_2\}$; la portée de c dans $\nu c.P'$ inclut donc bien le récepteur R' du message P_1 . Notez que nous enlevons le nom c de l'ensemble des noms \tilde{b} en conclusion de la règle EXTR_o^p . Dans une transition $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, \tilde{b} est l'ensemble des noms dont la portée peut éventuellement être étendue. Pour une concrétion $\nu \tilde{a}.\langle P_1 \rangle P_2$, cet ensemble correspond à $\text{fn}(P_1) \setminus \tilde{a}$.

Considérons maintenant les mêmes processus P et R , en supposant désormais $c \notin \text{fn}(P_1)$. Dans ce cas, la portée de c ne doit englober que la continuation P_2 : nous voulons obtenir $R' \mid \mathbb{E}\{\nu c.P_2\}$. Pour cela, nous considérons $P \xrightarrow{\bar{a}, R, \mathbb{E}\{\nu c.\square\}}_{\tilde{b}} P'$ comme prémisse de la règle RESTR_o^p . Dans le processus P' ainsi obtenu, la continuation est placée dans le contexte $\mathbb{E}\{\nu c.\square\}$, donc sous la portée de c . Pour notre exemple, nous obtenons $\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, R, \mathbb{E}\{\nu c.\square\}}_{\tilde{b}} R' \mid \mathbb{E}\{\nu c.P_2\} = P'$. Le processus P' est donc bien le résultat attendu pour la transition $\nu c.P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, ce que justifie la conclusion de la règle RESTR_o^p .

La règle PASSIV_o^p suit le même principe que la règle OUT_o^p , alors que les règles PAR_o^p , REPLIC_o^p et LOC_o^p ressemblent à RESTR_o^p . Il ne nous reste plus qu'à donner les règles pour le jugement d'émission $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, qui autorise la capture par le contexte \mathbb{E} . La règle CFREE_o^p affirme simplement qu'une transition sans capture $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$ donne une émission de message $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$.

Si le contexte \mathbb{E} capture un nom c , il existe des contextes $\mathbb{E}_1, \mathbb{E}_2$ tels que $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$ (d'autres captures par \mathbb{E}_1 et \mathbb{E}_2 sont possibles). La règle CAPT_o^p considère la transition $P \xrightarrow{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}}_{\tilde{b}} P'$, sans capture sur c , et conclut par $P \xrightarrow{\bar{a}, R, \mathbb{E}_1\{\nu c.\mathbb{E}_2\}}_{\tilde{b}} \nu c.P'$, étendant ainsi la portée de c . Par exemple, soient $P = \bar{a}\langle P_1 \rangle P_2$, R tel que $R \xrightarrow{a, P_1} R'$ et $\mathbb{E} = d[\nu c.(\square \mid \bar{c}(\mathbf{0})\mathbf{0})]$ avec $c \in \text{fn}(P_1)$. Le contexte \mathbb{E} se décompose en $\mathbb{E}_1\{\nu c.\mathbb{E}_2\}$ avec $\mathbb{E}_1 = d[\square]$ et $\mathbb{E}_2 = \square \mid \bar{c}(\mathbf{0})\mathbf{0}$. Par les règles OUT_o^p et CFREE_o^p , on a $P \xrightarrow{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}}_{\tilde{b}} R' \mid d[P_2 \mid \bar{c}(\mathbf{0})\mathbf{0}]$. Par

la règle $CAPT_o^p$, on a $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} \nu c.(R' \mid d[P_2 \mid \bar{c}\langle \mathbf{0} \rangle \mathbf{0}])$; la portée de c a été étendue hors de d et englobe R' , comme souhaité.

Comme pour $HO\pi$, la règle pour la communication HO_τ^p (figure 5.2) dépend du jugement d'émission. La prémisses $P \xrightarrow[\tilde{b}]{\bar{a}, Q, \square} P'$ signifie que P , placé dans le contexte \square , communique sur a avec Q , donnant ainsi P' . Nous en déduisons donc directement la conclusion de la règle $P \mid Q \xrightarrow{\tau} P'$. L'extension de portée ne peut plus avoir lieu; les noms \tilde{b} n'apparaissent donc plus dans la conclusion.

Le système de transitions ainsi défini a la même sémantique que le système de transitions contextuel. Pour une concrétion $C = \nu \tilde{a}. \langle P_1 \rangle P_2$, on définit $extr(C) \triangleq \text{fn}(P_1) \setminus \tilde{a}$.

Lemme 5.6. *Soit P un processus de $HO\pi P$.*

- Nous avons $P \xrightarrow{\tau} P'$ ssi $P \xrightarrow{\tau} P'$.
- Si $P \xrightarrow{a} F$, alors pour tout R , nous avons $P \xrightarrow{a, R} F \circ R$. Si $P \xrightarrow{a, R} P'$, alors il existe F tel que $P \xrightarrow{a} F$ et $P' = F \circ R$.
- Si $P \xrightarrow{\bar{a}} C$, alors pour tout R et F tels que $R \xrightarrow{a} F$, et pour tout \mathbb{E} , nous avons $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}}_{extr(C)} F \bullet \mathbb{E}\{C\}$. Si $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'$, alors il existe F et C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$, $\tilde{b} = extr(C)$ et $P' = F \bullet \mathbb{E}\{C\}$.

La correspondance entre les deux systèmes est exacte car l'extension de portée est bien effectuée de manière paresseuse par les règles $EXTR_o^p$, $RESTR_o^p$ et $CAPT_o^p$. La preuve se trouve en appendice A.3.1.

Remarque 5.1. *Nous pouvons étendre les étiquettes du système à complément de $HO\pi$ avec un contexte \mathbb{E} et des noms \tilde{b} pour effectuer l'extension de portée paresseuse de la même manière qu'en $HO\pi P$. Cette modification rend néanmoins les règles de déduction, les définitions de bisimulations et les preuves pour $HO\pi$ inutilement compliquées.*

5.2.2 Bisimulation à complément

Nous présentons les définitions et résultats sur les bisimulations à complément. Nous donnons uniquement les preuves des résultats pour le cas faible en appendice A.3; les preuves pour le cas fort sont similaires. La définition de la bisimilarité forte est la suivante :

Définition 5.3. *Une relation \mathcal{R} sur les termes clos est une simulation forte à complément ssi $P \mathcal{R} Q$ implique $\text{fn}(P) = \text{fn}(Q)$, et pour tout $P \xrightarrow{\lambda} P'$, il existe Q' tel que $Q \xrightarrow{\lambda} Q'$ et $P' \mathcal{R} Q'$.*

Une relation \mathcal{R} est une bisimulation forte à complément ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations fortes à complément. La bisimilarité forte à complément \sim_m est la plus grande bisimulation forte à complément.

Notez que nous avons toujours une contrainte sur les noms libres des processus en relation, comme pour la bisimilarité contextuelle (définition 2.15). Nous prouvons que \sim_m est une congruence en utilisant la méthode de Howe. Pour cela, nous définissons la clôture de Howe sur les contextes de bisimulation $\mathbb{E} \sim_m^\bullet \mathbb{F}$ comme étant la plus petite congruence qui étend \sim_m^\bullet avec la règle $\square \sim_m^\bullet \square$.

Définition 5.4. *L'extension de \sim_m^\bullet aux contextes de bisimulation est la plus petite relation vérifiant :*

- $\square \sim_m^\bullet \square$;
- si $\mathbb{E} \sim_m^\bullet \mathbb{F}$ et $P \sim_m^\bullet Q$, alors on a $\mathbb{E} \mid P \sim_m^\bullet \mathbb{F} \mid Q$;
- si $\mathbb{E} \sim_m^\bullet \mathbb{F}$, alors on a $\nu a. \mathbb{E} \sim_m^\bullet \nu a. \mathbb{F}$;
- si $\mathbb{E} \sim_m^\bullet \mathbb{F}$, alors on a $a[\mathbb{E}] \sim_m^\bullet a[\mathbb{F}]$.

Nous montrons alors le lemme de pseudo simulation suivant

Lemme 5.7. *Soient P et Q deux processus clos. Si $P \sim_m^\bullet Q$, alors*

- pour tout $P \xrightarrow{\tau} P'$, il existe Q' tel que $P' \sim_m^\bullet Q'$;
- pour tout R clos tel que $P \xrightarrow{a,R} P'$, pour tout R' clos tel que $R \sim_m^\bullet R'$, il existe Q' tel que $Q \xrightarrow{a,R'} Q'$ et $P' \sim_m^\bullet Q'$;
- pour tout R, \mathbb{E} clos tel que $P \xrightarrow{\bar{a},R,\mathbb{E}}_b P'$, pour tout R', \mathbb{F} clos tel que $R \sim_m^\bullet R'$ et $\mathbb{E} \sim_m^\bullet \mathbb{F}$, il existe Q' tel que $Q \xrightarrow{\bar{a},R',\mathbb{F}}_b Q'$ et $P' \sim_m^\bullet Q'$.

La preuve du lemme 5.7 et l'application de la méthode de Howe de manière générale ne posent pas de difficulté. Nous avons donc le résultat suivant :

Théorème 5.3. *La relation \sim_m est une congruence*

En utilisant la même technique que pour $\text{HO}\pi$ (théorème 2.2), nous pouvons montrer la complétude de la bisimilarité à complément. Nous pouvons donc en conclure le résultat suivant.

Théorème 5.4. *Nous avons $\sim_m = \sim_b$.*

Nous étudions maintenant la correspondance entre \sim et \sim_m . La relation \sim_m diffère de \sim en deux points. Premièrement, si $P \sim_m Q$ et $P \xrightarrow{\bar{a},R,\mathbb{E}}_b P'$, alors la transition correspondante $Q \xrightarrow{\bar{a},R,\mathbb{E}}_b Q' \sim_m P'$ doit comporter le même ensemble \tilde{b} de noms dont la portée peut être étendue. Nous n'avons pas de contrainte similaire dans la définition de bisimilarité contextuelle. Le lemme suivant montre que cette contrainte sur les noms est en fait une propriété de la relation \sim .

Lemme 5.8. *Soient P, Q tels que $P \sim Q$ et $P \xrightarrow{\bar{a}} C$. Soient F, C' tels que $Q \xrightarrow{\bar{a}} C'$ et pour tout \mathbb{E} , on a $F \bullet \mathbb{E}\{C\} \sim F \bullet \mathbb{E}\{C'\}$. On a alors $\text{extr}(C) = \text{extr}(C')$.*

Grâce à ce lemme, nous pouvons prouver le résultat suivant.

Lemme 5.9. *Nous avons $\sim \subseteq \sim_m$.*

Nous pouvons donc en déduire la correction de \sim .

Corollaire 5.1. *Nous avons $\sim \subseteq \sim_b$.*

En outre, si $P \sim_m Q$ et $P \xrightarrow{\bar{a},R,\mathbb{E}}_b P'$, la réponse $Q \xrightarrow{\bar{a},R,\mathbb{E}}_b Q'$ se fait pour un contexte \mathbb{E} fixé, alors que dans la définition de bisimilarité contextuelle (définition 2.15), la réponse de Q doit être valable pour tous les contextes \mathbb{E} . La bisimilarité à complément est donc précoce par rapport aux contextes de bisimulation \mathbb{E} , alors que la bisimilarité contextuelle est tardive par rapport à ces mêmes contextes. L'inclusion $\sim_m \subseteq \sim$ reste un problème ouvert ; nous conjecturons que cette inclusion est vraie.

Remarque 5.2. *Nous pouvons définir la bisimilarité contextuelle de manière précoce sur les contextes en changeant la clause d'émission de la définition 2.15 en*

- pour tout $P \xrightarrow{\bar{a}} C$, pour tout F, \mathbb{E} , il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et $F \bullet \mathbb{E}\{C\} \mathcal{R} F \bullet \mathbb{E}\{C'\}$.

Nous pouvons alors prouver que la bisimilarité ainsi modifiée \sim' est correcte (en utilisant la preuve par progression) et complète (en utilisant le schéma de preuve classique). Nous avons alors $\sim' = \sim_b$ et $\sim_m = \sim_b$, donc $\sim_m = \sim'$. Nous pouvons prouver la congruence de \sim' indépendamment de \sim_m uniquement dans le cas fort ; ce raisonnement est donc impossible dans le cas faible.

Nous cherchons maintenant à étendre ces résultats au cas faible. Comme pour $\text{HO}\pi$, on note $\xRightarrow{\tau}$ la clôture réflexive et transitive de $\xrightarrow{\tau}$, et on définit $\xRightarrow{a,R} \triangleq \xRightarrow{\tau} \xrightarrow{a,R} \xRightarrow{\tau}$. Enfin, nous définissons $P \xRightarrow{\bar{a},R,\mathbb{E}}_b P'$ comme $P \xRightarrow{\tau} \xrightarrow{\bar{a},R,\mathbb{E}}_b P'$, avec R' tel que $R \xRightarrow{\tau} R'$.

Définition 5.5. Une relation \mathcal{R} sur les termes clos est une simulation faible à complément ssi $P \mathcal{R} Q$ implique $fn(P) = fn(Q)$ et pour tout $P \xRightarrow{\lambda} P'$, il existe Q' tel que $Q \xRightarrow{\lambda} Q'$ et $P' \mathcal{R} Q'$.

Une relation \mathcal{R} est une bisimulation faible à complément ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations faibles à complément. La bisimilarité faible à complément \approx_m est la plus grande bisimulation faible à complément.

En utilisant les mêmes techniques de preuves que dans le cas fort, nous obtenons les résultats suivants :

Théorème 5.5. La relation \approx_m est une congruence.

Lemme 5.10. Nous avons $\approx \subseteq \approx_m$.

La preuve de ce résultat repose sur une version faible du lemme 5.8 ; plus de détails sont donnés en appendice A.3.3.

Corollaire 5.2. Nous avons $\approx \subseteq \approx_b$.

Nous montrons la complétude de \approx_m sur les processus à image finie, obtenant ainsi le premier résultat de caractérisation de la congruence barbue faible dans un calcul avec passivation et restriction.

Définition 5.6. Un processus P est à image finie ssi pour toute étiquette λ , l'ensemble $\{P', P \xRightarrow{\lambda} P'\}$ est fini.

Théorème 5.6. Soient P, Q deux processus à image finie. Nous avons $P \approx_m Q$ ssi $P \approx_b Q$.

Les théorèmes 5.5 et 5.6 sont prouvés en appendice A.3.

5.3 Conclusions

Dans ce chapitre nous avons présenté un système de transitions étiquetées qui permet l'utilisation de la méthode de Howe pour prouver la congruence de la bisimulation associée. Le principe est de s'écarter d'une définition précoce dans le cas de l'émission de message, en considérant un processus capable de recevoir un message plutôt qu'une fonction. La bisimilarité ainsi obtenue a le même pouvoir discriminant qu'une bisimilarité contextuelle précoce, et nous pouvons appliquer la méthode aussi bien dans le cas fort que faible. En particulier, nous avons défini une sémantique à complément pour $\text{HO}\pi\text{P}$, obtenant ainsi une bisimilarité correcte et complète sur les processus à image finie dans le cas faible. À notre connaissance, il s'agit du premier résultat de caractérisation dans un calcul avec restriction et passivation dans le cas faible.

Cette méthode peut s'appliquer à d'autres calculs : dans [26], nous donnons une sémantique à complément pour le calcul Seal [54], et nous prouvons que la bisimilarité faible associée est correcte. Contrairement à $\text{HO}\pi\text{P}$, le Seal demande la synchronisation entre trois processus ; pour compléter un processus, nous devons donc considérer un à deux autres processus dans l'étiquette. En outre, nous devons prendre en compte le contrôle sur les communications : par exemple, les localités du calcul ne peuvent traverser plus d'une frontière de localité lors d'une migration. Notre travail sur le Seal demande à être poursuivi ; il nous reste à prouver que la sémantique à complément correspond à la réduction du Seal, et en déduire un résultat de complétude pour la bisimilarité faible à complément. Dans le chapitre suivant, nous cherchons à définir une sémantique à complément pour le Kell, un calcul pour lequel il n'existe pas de preuve de congruence pour une bisimilarité faible. Nous verrons les problèmes que posent les récepteurs joints du Kell.

Chapitre 6

Application au Kell-calcul

Dans ce chapitre nous cherchons à définir une sémantique à complément pour le Kell afin d'obtenir un résultat de correction dans le cas faible. La sémantique du Kell rend la définition d'un système de transitions à complément difficile, notamment à cause de l'extension de portée paresseuse hors des localités, le contrôle sur les communications et surtout la présence de récepteurs joints de taille quelconque. En effet, hormis le processus récepteur Q , l'étiquette d'une transition d'émission de P doit comporter plusieurs processus émetteurs (P_i) , tels que la combinaison de P , Q et des (P_i) engendre une communication ; les émissions de P et (P_i) doivent donc correspondre au récepteur joint de Q .

Avant de travailler sur le Kell et l'ensemble de ses constructions, nous nous intéressons d'abord spécifiquement aux récepteurs joints (section 6.1) ; nous définissons un calcul simple avec des récepteurs joints, appelé $\text{HO}\pi\text{J}$, et nous cherchons à définir une sémantique à complément pour ce calcul. En utilisant les principes de construction donnés dans cette première partie, nous définissons une sémantique à complément pour le Kell en section 6.2. Nous rappelons d'abord la syntaxe et la sémantique du Kell telles qu'elles sont définies dans [47] (plus précisément d'une instance du Kell appelée jK), et nous définissons une variante de bisimilarité faible à complément et prouvons sa congruence grâce à la méthode de Howe.

6.1 Récepteurs joints

Dans cette section, nous proposons une sémantique à complément pour $\text{HO}\pi\text{J}$, une extension de $\text{HO}\pi$ comportant des récepteurs joints. L'objectif est de comprendre comment nous pouvons définir une sémantique à complément pour les récepteurs joints dans un cas simple, avant de passer au cas plus complexe du Kell.

6.1.1 Le calcul $\text{HO}\pi\text{J}$

Le calcul $\text{HO}\pi\text{J}$ étend $\text{HO}\pi$ avec une construction de récepteur joint $a_1(X_1) \mid \dots \mid a_n(X_n) \triangleright P$. Lorsque des messages $R_1 \dots R_n$ sont disponibles simultanément sur $a_1 \dots a_n$, la communication se déclenche, et le récepteur joint évolue vers $P\{\tilde{R}/\tilde{X}\}$. Dans la suite, nous notons $\prod_i P_i$ pour le processus $P_1 \mid \dots \mid P_n$ et $\prod_i a_i(X_i)$ pour le récepteur joint $a_1(X_1) \mid \dots \mid a_n(X_n)$. Pour un récepteur joint $\pi = \prod_i a_i(X_i)$, nous notons $\text{fn}(\pi) \triangleq \{a_1 \dots a_n\}$ ses noms et $\text{fv}(\pi) \triangleq \{X_1 \dots X_n\}$ ses variables.

La syntaxe et sémantique de $\text{HO}\pi\text{J}$ sont données en figure 6.1, avec les mêmes conventions et notations que pour $\text{HO}\pi$, sauf que nous modifions les définitions de fonction et de concrétion. Nous notons \uplus l'union de multi-ensembles. Un récepteur π est bien formé si et seulement si ses variables sont deux à deux distinctes ; tout au long de ce chapitre, nous supposons que les récepteurs joints sont bien formés. Comme en $\text{HO}\pi$, un processus de $\text{HO}\pi\text{J}$ peut évoluer vers un processus $P \xrightarrow{\tau} P'$, une fonction $P \xrightarrow{\tilde{a}} F$, ou une concrétion

Syntaxe :

$$\begin{aligned} P &::= \mathbf{0} \mid X \mid P \mid P \mid \nu a.P \mid \bar{a}\langle P \rangle P \mid \pi \triangleright P \\ \pi &::= \pi \mid \pi \mid a(X) \end{aligned}$$

Règles de la congruence structurelle

$$\begin{aligned} P \mid (Q \mid R) &\equiv (P \mid Q) \mid R & P \mid Q &\equiv Q \mid P & P \mid \mathbf{0} &\equiv P & \nu a.\nu b.P &\equiv \nu b.\nu a.P \\ \nu a.\mathbf{0} &\equiv \mathbf{0} & \nu a.(P \mid Q) &\equiv P \mid \nu a.Q \end{aligned}$$

Congruence structurelle sur les récepteurs joints :

$$\pi_1 \mid \pi_2 \equiv \pi_2 \mid \pi_1 \qquad \pi_1 \mid (\pi_2 \mid \pi_3) \equiv (\pi_1 \mid \pi_2) \mid \pi_3$$

Agents :

$$\begin{aligned} \text{Fonctions} \quad F, G &::= (\pi)P \\ \text{Concrétions} \quad C, D &::= \langle a, \widetilde{P} \rangle Q \mid \nu a.C \end{aligned}$$

Composition parallèle des concrétions :

$$\nu \widetilde{b}.\langle \widetilde{a}, \widetilde{R} \rangle P \mid \nu \widetilde{b}'.\langle \widetilde{a}', \widetilde{R}' \rangle Q \triangleq \nu \widetilde{b} \cup \widetilde{b}'.\langle \widetilde{a}, \widetilde{R} \uplus \widetilde{a}', \widetilde{R}' \rangle P \mid Q$$

Pseudo-application

$$\frac{\pi = \prod a(\widetilde{X})}{(\pi)P \bullet \nu \widetilde{b}.\langle \widetilde{a}, \widetilde{R} \rangle Q \triangleq \nu \widetilde{b}.(P\{\widetilde{R}/\widetilde{X}\} \mid Q)}$$

Règles du système de transitions étiquetées :

$$\begin{aligned} &\frac{\text{fn}(\pi) = \widetilde{a}}{\pi \triangleright P \xrightarrow{\widetilde{a}} (\pi)P} \text{ IN} & \bar{a}\langle Q \rangle P \xrightarrow{\bar{a}} \langle a, Q \rangle P \text{ OUT} & \frac{P \xrightarrow{\alpha_j} A}{P \mid Q \xrightarrow{\alpha_j} A \mid Q} \text{ PAR} \\ &\frac{P \xrightarrow{\widetilde{a}} C \quad Q \xrightarrow{\widetilde{a'}} C'}{P \mid Q \xrightarrow{\widetilde{a} \uplus \widetilde{a'}} C \mid C'} \text{ PAR-OUT} & \frac{P \xrightarrow{\alpha_j} A \quad a \notin \alpha_j}{\nu a.P \xrightarrow{\alpha_j} \nu a.A} \text{ RESTR} \\ &\frac{P \xrightarrow{\widetilde{a}} F \quad Q \xrightarrow{\widetilde{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \text{ HO} & \frac{P \equiv P' \quad P' \xrightarrow{\alpha_j} Q' \quad Q' \equiv Q}{P \xrightarrow{\alpha_j} Q} \text{ CONGR} \end{aligned}$$

FIG. 6.1 – Syntaxe et sémantique opérationnelle de HO π J

$P \xrightarrow{\bar{a}} C$. La méta-variable α_j parcourt l'ensemble des étiquettes. Une fonction $F \triangleq (\pi)P$ est paramétrée par un récepteur joint π ; une concrétion $\nu \bar{b}. \langle \bar{a}, R \rangle Q$ contient le multi-ensemble des paires canal de diffusion - message émis. Une réaction a lieu entre fonction et concrétion si et seulement si les canaux de réception et de diffusion correspondent, comme le reflète la définition de pseudo-application.

Le système de transitions étiquetées contextuel de $\text{HO}\pi\text{J}$ est défini modulo congruence structurelle, pour réorganiser les processus afin de permettre notamment le regroupement des émetteurs par la règle PAR-OUT. Par exemple, le processus

$$\nu a. (\bar{a} \langle c. \mathbf{0} \rangle a. \mathbf{0} \mid (a(X) \mid b(Y)) \triangleright (X \mid Y)) \mid \bar{b} \langle d. \mathbf{0} \rangle \mathbf{0}$$

ne permet pas l'application des règles PAR-OUT et HO alors que le processus équivalent

$$\nu a. (\bar{a} \langle c. \mathbf{0} \rangle \mathbf{0} \mid \bar{b} \langle d. \mathbf{0} \rangle \mathbf{0} \mid (a(X) \mid b(Y)) \triangleright (X \mid Y))$$

le permet.

Comme $\text{HO}\pi\text{J}$ n'est qu'un calcul annexe dans notre étude, nous ne cherchons pas à définir de bisimilarité contextuelle à laquelle comparer notre bisimilarité à complément. Nous définissons directement un système de transitions à complément, et nous prouvons la congruence de la bisimilarité associée, en pointant les différences avec les sémantiques définies dans le chapitre 5.

6.1.2 Sémantique à complément

En $\text{HO}\pi$, dans le cas d'une émission de P vers Q , la sémantique à complément analyse d'abord P à la recherche du message émis, tout en gardant Q dans l'étiquette. Lorsque le message est découvert, nous nous intéressons à Q , à la recherche du récepteur. En $\text{HO}\pi\text{J}$, cette sérialisation est plus difficile : nous n'avons plus un mais potentiellement plusieurs messages à découvrir dans P . Lorsqu'un premier message R_1 est découvert, nous devons chercher les autres messages avant de passer à la transition de Q . Cependant, nous ne pouvons pas stocker R_1 dans l'étiquette, comme nous le faisons pour Q ; cela reviendrait à définir une transition précoce qui ne permet pas l'application de la méthode de Howe.

Plutôt que de stocker les messages dans l'étiquette, nous proposons de les passer directement au récepteur dès leur découverte; les variables $X_1 \dots X_n$ du récepteur joint de Q sont donc instanciées une par une, et non plus simultanément comme dans la sémantique donnée en figure 6.1. Illustrons sur un exemple notre manière de procéder : soient l'émetteur $P \triangleq \bar{a} \langle R \rangle S \mid \bar{b} \langle T \rangle U$ et le récepteur $Q \triangleq (a(X) \mid b(Y)) \triangleright (c.X \mid d.Y)$. Nous souhaitons obtenir la transition

$$P \xrightarrow{\{\bar{a}, \bar{b}\}, Q} S \mid U \mid c.R \mid d.T$$

Nous nous intéressons d'abord au message sur \bar{a} : nous stockons donc l'émission sur \bar{b} pour analyse ultérieure :

$$\frac{\bar{a} \langle R \rangle S \xrightarrow{\{\bar{a}, \bar{b}\}, Q, \bar{b} \langle T \rangle U} S \mid U \mid c.R \mid d.T}{P \xrightarrow{\{\bar{a}, \bar{b}\}, Q} S \mid U \mid c.R \mid d.T}$$

Le message R sur a est passé en argument à Q ; Q évolue alors vers une *réception partielle* notée $I = b(Y) \blacktriangleright c.R \mid d.Y$. Maintenant que nous avons trouvé le message sur a , nous pouvons passer au processus $\bar{b} \langle T \rangle U$ que nous avons stocké dans l'étiquette. Nous le faisons réagir avec I et obtenons le résultat souhaité. L'arbre de dérivation complet est le suivant :

$$\frac{\frac{Q \xrightarrow{a, R} I \quad \frac{I \xrightarrow{b, T} c.R \mid d.T}{\bar{b} \langle T \rangle U \xrightarrow{\{\bar{b}\}, I} U \mid c.R \mid d.T}}{\bar{a} \langle R \rangle S \xrightarrow{\{\bar{a}, \bar{b}\}, Q, \bar{b} \langle T \rangle U} S \mid U \mid c.R \mid d.T}}{P \xrightarrow{\{\bar{a}, \bar{b}\}, Q} S \mid U \mid c.R \mid d.T}$$

Syntaxe :

$$\begin{aligned} I &::= \pi \blacktriangleright P \mid \mathbf{0} \blacktriangleright P \\ E &::= I \mid P \end{aligned}$$

Extension de la composition parallèle et de la restriction :

$$\begin{aligned} (\pi \blacktriangleright P) \mid Q &\triangleq \pi \blacktriangleright (P \mid Q) \\ Q \mid (\pi \blacktriangleright P) &\triangleq \pi \blacktriangleright (Q \mid P) \\ \nu b.(\pi \blacktriangleright P) &\triangleq \pi \blacktriangleright (\nu b.P) \text{ ssi } b \notin \text{fn}(\pi) \end{aligned}$$

Règles du jugement de réception partielle :

$$\begin{array}{c} \frac{\pi \equiv a(X) \mid \pi'}{\pi \triangleright P \xrightarrow{a,R} \pi' \blacktriangleright P\{R/X\}} \text{PROC}_{pi}^j \qquad \frac{\pi \equiv a(X) \mid \pi'}{\pi \blacktriangleright P \xrightarrow{a,R} \pi' \blacktriangleright P\{R/X\}} \text{PART-IN}_{pi}^j \\[10pt] \frac{P \xrightarrow{a,R} I}{P \mid Q \xrightarrow{a,R} I \mid Q} \text{PAR}_{pi}^j \qquad \frac{P \xrightarrow{a,R} I \quad b \notin a \cup n(I)}{\nu b.P \xrightarrow{a,R} \nu b.I} \text{RESTR}_{pi}^j \end{array}$$

FIG. 6.2 – Réception partielle en HO π J

Une réception partielle $I = \pi \blacktriangleright P$ est obtenue en instanciant successivement les éléments $a_i(X_i)$ d'un récepteur joint $\prod_i a_i(X_i) \triangleright P'$. La méta-variable E parcourt l'ensemble des processus et des réceptions partielles. Contrairement aux récepteurs joints, nous acceptons les schémas $\pi = \mathbf{0}$: cela correspond aux réceptions partielles complètement instanciées. Par convention nous identifions $\mathbf{0} \blacktriangleright P = P$. Nous étendons la composition parallèle et la restriction aux réceptions partielles, et nous donnons les règles du jugement d'instanciation partielle $E \xrightarrow{a,R} I$ en figure 6.2, à l'exception du symétrique de la règle PAR_{pi}^j . Nous notons $n(I)$ l'ensemble des noms a_i d'une réception partielle $I = \prod_i a_i(X_i) \blacktriangleright P$. Les règles PROC_{pi}^j , PAR_{pi}^j et RESTR_{pi}^j définissent la première réception, qui transforme un processus (contenant un récepteur joint) en réception partielle. Dans le cas de la restriction (règle RESTR_{pi}^j), nous vérifions que la restriction ne capture un des noms sur lequel a lieu la réception. Une réception partielle ne peut que recevoir un message pour évoluer vers une autre réception partielle (règle PART-IN_{pi}^j).

Comme souligné en section 6.1.1, un processus de HO π J dans lequel une synchronisation est possible, comme par exemple

$$Q \triangleq \nu a.(\bar{a}\langle c.\mathbf{0} \rangle a.\mathbf{0} \mid (a(X) \mid b(Y)) \triangleright (X \mid Y)) \mid \bar{b}\langle d.\mathbf{0} \rangle \mathbf{0}$$

ne se présente pas toujours sous la forme $Q = Q_1 \mid Q_2$, avec Q_1 contenant toutes les émissions, et Q_2 contenant uniquement le récepteur. En sémantique contextuelle, nous travaillons modulo congruence structurelle, pour réécrire les termes suivant ce schéma. Faire de même avec la sémantique à complément ferait échouer la preuve de congruence par la méthode de Howe. En effet, les preuves par induction sur \mathcal{R}^\bullet repose sur la structure des termes, notamment dans le cas où $P \mathcal{R}^\bullet Q$ provient de $P = op(\tilde{P}_i)$, $Q = op(\tilde{Q}_i)$ avec $\tilde{P}_i \mathcal{R}^\bullet \tilde{Q}_i$. Autoriser les règles de transition à modifier les termes par congruence structurelle rendrait impossible les preuves par induction sur \mathcal{R}^\bullet .

Pour palier à cette difficulté, nous utilisons un jugement de *synchronisation partielle* $P \xrightarrow{\theta} I$ en plus du jugement d'émission $P \xrightarrow{\tilde{a},E,\tilde{R}} I$. La synchronisation partielle $P \xrightarrow{\theta} I$ est possible si et seulement si P contient un récepteur joint et des émissions de message capables d'interagir avec ce récepteur ; la transition effectue alors la synchronisation partielle

$$\begin{array}{c}
\frac{E \xrightarrow{a, P_1} I}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, E, \emptyset} I \mid P_2} \text{ OUT-EMPTY}_o^j \qquad \frac{E \xrightarrow{a, P_1} I \quad R_j \xrightarrow{\tilde{b}, I, \tilde{R}} J}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\tilde{b} \uplus \bar{a}, E, \tilde{R} \uplus R_j} J \mid P_2} \text{ OUT} \\
\\
\frac{P \xrightarrow{\tilde{a}, E, \tilde{R} \uplus R_j} I}{P \mid R_j \xrightarrow{\tilde{a}, E, \tilde{R}} I} \text{ PAR-OUT}_o^j \qquad \frac{P_1 \xrightarrow{\tilde{a}, E, \tilde{R}} I}{P_1 \mid P_2 \xrightarrow{\tilde{a}, E, \tilde{R}} I \mid P_2} \text{ PAR}_o^j \\
\\
\frac{P \xrightarrow{\tilde{a}, E, \tilde{R}} I \quad b \notin \tilde{a} \cup n(I)}{\nu b. P \xrightarrow{\tilde{a}, E, \tilde{R}} \nu b. I} \text{ RESTR}_o^j
\end{array}$$

FIG. 6.3 – Sémantique à complément de HO π J : émission de message

entre ces entités. Par exemple, le processus Q ci-dessus peut être décomposé en $Q_1 \mid Q_2$ avec $Q_1 = \nu a.(\bar{a}\langle c.\mathbf{0} \rangle a.\mathbf{0} \mid (a(X) \mid b(Y)) \triangleright (X \mid Y))$ et $Q_2 = \bar{b}\langle d.\mathbf{0} \rangle \mathbf{0}$. Le processus Q_1 est capable de se synchroniser partiellement sur a , générant ainsi la réception partielle $J = b(Y) \blacktriangleright \nu a.(a.\mathbf{0} \mid c.\mathbf{0} \mid Y)$.

Le jugement d'émission $P \xrightarrow{\tilde{a}, E, \tilde{R}} I$ signifie que les processus P et \tilde{R} envoient des messages sur les canaux \tilde{a} , et l'interaction de ces processus avec l'entité réceptrice E donne I . Informellement, nous avons

$$E \mid P \mid \prod \tilde{R} \xrightarrow{\tau} I$$

par communication sur \tilde{a} . Ce jugement n'effectue aucune communication à l'intérieur de E ; si E est un processus capable de se synchroniser partiellement (comme Q_1), il donc faut au préalable utiliser le jugement $\xrightarrow{\theta}$. Par exemple, dans la transition $Q_2 \xrightarrow{\bar{b}, J, \emptyset} \mathbf{0} \blacktriangleright \nu a.(a.\mathbf{0} \mid c.\mathbf{0} \mid d.\mathbf{0})$, nous faisons réagir le résultat J de la synchronisation de Q_1 avec Q_2 . Nous en déduisons alors $Q \xrightarrow{\tau} \nu a.(a.\mathbf{0} \mid c.\mathbf{0} \mid d.\mathbf{0})$, comme souhaité.

Les règles pour l'émission de message sont données en figure 6.3, à l'exception du symétrique des règles PAR_o^j et PAR-OUT_o^j . Les règles OUT_o^j et OUT-EMPTY_o^j traitent de l'émission $\bar{a}\langle P_1 \rangle P_2$. Dans les deux règles, le message P_1 est passé en argument au récepteur E ; nous avons $E \xrightarrow{a, P_1} I$. S'il ne reste plus de message à trouver, c'est-à-dire si le multi-ensemble \tilde{R} est vide, le résultat I est simplement mis en parallèle avec la continuation P_2 ; nous obtenons $P \xrightarrow{\bar{a}, E, \emptyset} I \mid P_2$ en conclusion de la règle OUT-EMPTY_o^j . En revanche, s'il reste des processus en étiquette à explorer (règle OUT_o^j), nous faisons réagir I avec ces processus. Pour cela, nous choisissons un processus R_j dans l'étiquette, et nous considérons la transition $R_j \xrightarrow{\tilde{b}, I, \tilde{R}} J$. Par communication sur \tilde{b} , nous avons donc informellement

$$I \mid R_j \mid \prod \tilde{R} \xrightarrow{\tau} J$$

Comme I est le résultat de la réception de P_1 par E , nous avons donc

$$E \mid \bar{a}\langle P_1 \rangle P_2 \mid R_j \mid \prod \tilde{R} \xrightarrow{\tau} J \mid P_2$$

Nous en déduisons la conclusion $\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\tilde{b} \uplus \bar{a}, E, \tilde{R} \uplus R_j} J \mid P_2$ de la règle OUT_o^j .

Les règles PAR_o^j et PAR-OUT_o^j gèrent les deux comportements possibles avec la composition parallèle : soit le processus en parallèle interagit avec E , soit il est inerte. Dans le premier cas, le processus est mis dans l'étiquette pour analyse ultérieure (règle PAR-OUT_o^j) ; sinon il est juste mis en parallèle dans le processus résultant (règle PAR_o^j). La

$$\begin{array}{c}
\frac{P_2 \xrightarrow{\tilde{a}, P_1, \emptyset} I}{P_1 \mid P_2 \xrightarrow{\theta} I} \text{ SYNC}_{ps}^j \quad \frac{P_1 \xrightarrow{\theta} I \quad P_2 \xrightarrow{\tilde{a}, I, \emptyset} J}{P_1 \mid P_2 \xrightarrow{\theta} J} \text{ PAR}_{ps}^j \quad \frac{P \xrightarrow{\theta} I \quad a \notin n(I)}{\nu a. P \xrightarrow{\theta} \nu a. I} \text{ RESTR}_{ps}^j
\end{array}$$

FIG. 6.4 – Sémantique à complément de HO π J : synchronisation partielle

$$\begin{array}{c}
\frac{\pi = \prod_i a_i(X_i)}{\pi \triangleright P \xrightarrow{\tilde{a}, \tilde{R}} P\{\tilde{R}/\tilde{X}\}} \text{ IN}_i^j \quad \frac{P_1 \xrightarrow{\mu_j} P'}{P_1 \mid P_2 \xrightarrow{\mu_j} P' \mid P_2} \text{ PAR}_{i\tau}^j \\
\frac{P \xrightarrow{\mu_j} P' \quad a \notin \text{fn}(\mu_j)}{\nu a. P \xrightarrow{\mu_j} \nu a. P'} \text{ RESTR}_{i\tau}^j \quad \frac{P_2 \xrightarrow{\tilde{a}, P_1, \emptyset} \mathbf{0} \blacktriangleright P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{ HO}_{\tau}^j \\
\frac{P_1 \xrightarrow{\theta} I \quad P_2 \xrightarrow{\tilde{a}, I, \emptyset} \mathbf{0} \blacktriangleright P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{ HO-SYNC}_{\tau}^j
\end{array}$$

FIG. 6.5 – Sémantique à complément de HO π J : réception et action interne

règle RESTR_o^j traite le cas de la restriction. À partir de $P \xrightarrow{\tilde{b}, E, \tilde{R}} I$, nous en déduisons $\nu a. P \xrightarrow{\tilde{b}, E, \tilde{R}} \nu a. I$: la restriction englobe I , qui contient le récepteur E des messages. Comme dans la sémantique à complément de HO π (figure 5.1), l'extension de portée de a est donc systématiquement pratiquée, que a appartienne ou non aux noms libres des messages de P et de \tilde{R} .

Les règles pour la synchronisation partielle sont données en figure 6.4, à l'exception du symétrique des règles SYNC_{ps}^j et PAR_{ps}^j . Les règles SYNC_{ps}^j et PAR_{ps}^j traitent le cas de la composition parallèle $P_1 \mid P_2$, en supposant que le récepteur joint est dans P_1 (sinon, il faut utiliser le symétrique de ces règles). Si aucune synchronisation n'est nécessaire à l'intérieur de P_1 , le processus P_2 se synchronise partiellement avec P_1 grâce à la transition $P_2 \xrightarrow{\tilde{a}, P_1, \emptyset} I$ (règle SYNC_{ps}^j). Sinon, nous effectuons d'abord la synchronisation partielle $P_1 \xrightarrow{\theta} I$, puis nous faisons interagir P_2 et I au moyen de la transition $P_2 \xrightarrow{\tilde{a}, I, \emptyset} J$. Le résultat J est alors le résultat de la synchronisation partielle de $P_1 \mid P_2$ (règle PAR_{ps}^j). Dans la règle RESTR_{ps}^j , la prémisses $a \notin n(I)$ vérifie que la restriction ne capture pas les réceptions non instanciées de I . En revanche, cette règle n'interdit pas les synchronisations partielles sur un nom restreint, comme par exemple avec $Q_1 = \nu a. (\bar{a}\langle c.\mathbf{0} \rangle a.\mathbf{0} \mid (a(X) \mid b(Y))) \triangleright (X \mid Y)$.

$$\frac{\bar{a}\langle c.\mathbf{0} \rangle a.\mathbf{0} \mid (a(X) \mid b(Y)) \triangleright (X \mid Y) \xrightarrow{\theta} b(Y) \blacktriangleright a.\mathbf{0} \mid c.\mathbf{0} \mid Y}{Q_1 \xrightarrow{\theta} b(Y) \blacktriangleright \nu a.(a.\mathbf{0} \mid c.\mathbf{0} \mid Y)}$$

Dans la figure 6.5, nous donnons les règles pour la réception $P \xrightarrow{\tilde{a}, \tilde{R}} P'$ et les actions internes $P \xrightarrow{\tau} P'$; le symétrique des règles $\text{PAR}_{i\tau}^j$, HO_{τ}^j et HO-SYNC_{τ}^j ont été omises. La méta-variable μ_j parcourt l'ensemble des étiquettes $\tau, \tilde{a}, \tilde{R}$, et nous définissons $\text{fn}(\tau) \triangleq \emptyset$ et $\text{fn}(\tilde{a}, \tilde{R}) \triangleq \tilde{a}$. La réception $P \xrightarrow{\tilde{a}, \tilde{R}} P'$ signifie que le récepteur joint de P reçoit les messages \tilde{R} sur les canaux \tilde{a} . Du point de vue de la sémantique, ce jugement est redondant avec la réception partielle $E \xrightarrow{\tilde{a}, \tilde{R}} I$. En effet, une succession de réception partielles permet d'exprimer une réception $\xrightarrow{\tilde{a}, \tilde{R}}$, et les émissions et actions internes reposent uniquement

sur les transitions partielles. Cependant, du point de vue de la bisimilarité, les deux types de transitions ne sont pas nécessairement équivalentes, comme nous le verrons avec le Kell.

Les règles pour les actions internes sont classiques, à l'exception de la règle HO-SYNC₇^j. Supposons qu'une communication a lieu au sein d'un processus $P_1 \mid P_2$, et que le processus P_1 contient le récepteur joint. Si P_1 ne nécessite pas de synchronisation partielle, nous pouvons utiliser la transition d'émission $P_2 \xrightarrow{\tilde{a}, P_1, \emptyset} \mathbf{0} \blacktriangleright P'$ (règle HO₇^j). Dans le cas contraire, nous devons d'abord effectuer la synchronisation partielle dans P_1 (règle HO-SYNC₇^j). Les règles HO₇^j et HO-SYNC₇^j sont construites comme les règles SYNC_{ps}^j et PAR_{ps}^j.

6.1.3 Bisimilarité à complément

La définition de bisimilarité à complément qui nous intéresse est la suivante.

Définition 6.1. Une relation \mathcal{R} sur les termes clos est une simulation forte à complément ssi pour tout $P \mathcal{R} Q$:

- si $P \xrightarrow{\mu_j} P'$, alors il existe Q' tel que $Q \xrightarrow{\mu_j} Q'$ et $P' \mathcal{R} Q'$;
- si $P \xrightarrow{\tilde{a}, S, \tilde{R}} \mathbf{0} \blacktriangleright P'$, alors il existe Q' tel que $Q \xrightarrow{\tilde{a}, S, \tilde{R}} \mathbf{0} \blacktriangleright Q'$ et $P' \mathcal{R} Q'$.

Une relation \mathcal{R} est une bisimulation forte à complément ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations fortes à complément. La bisimilarité forte à complément \sim_m est la plus grande bisimulation forte à complément.

Cependant nous ne pouvons pas prouver directement la congruence de cette relation en utilisant la méthode de Howe. En effet, la preuve du résultat de pseudo-simulation sur \sim_m^\bullet contient une analyse de cas sur les règles de déduction utilisées ; or pour certaines règles, nous avons besoin de résultats supplémentaires impliquant les jugements d'instanciation partielle $E \xrightarrow{a, R} I$ et de synchronisation partielle $P \xrightarrow{\theta} I$. C'est pourquoi nous définissons une bisimilarité à complément étendue aux réceptions partielles.

Définition 6.2. Une relation \mathcal{R} sur les termes clos est une simulation forte à complément sur les réceptions partielles ssi $P \mathcal{R} Q$ implique :

- pour tout $P \xrightarrow{\mu_j} P'$, il existe Q' tel que $Q \xrightarrow{\mu_j} Q'$ et $P' \mathcal{R} Q'$;
- si $P \xrightarrow{\tilde{a}, S, \tilde{R}} \mathbf{0} \blacktriangleright P'$, alors il existe Q' tel que $Q \xrightarrow{\tilde{a}, S, \tilde{R}} \mathbf{0} \blacktriangleright Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a, R} I$, il existe I' telle que $Q \xrightarrow{a, R} I'$ et $I \mathcal{R} I'$;
- pour tout $P \xrightarrow{\theta} I$, il existe I' telle que $Q \xrightarrow{\theta} I'$ et $I \mathcal{R} I'$.

Nous avons $\pi \blacktriangleright P \mathcal{R} \pi' \blacktriangleright Q$ ssi $\pi = \pi'$ et pour tout substitution σ qui clôt P et Q , nous avons $P\sigma \mathcal{R} Q\sigma$.

Une relation \mathcal{R} est une bisimulation forte à complément sur les réceptions partielles ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations fortes à complément sur les réceptions partielles. La bisimilarité forte à complément sur les réceptions partielles \sim_{pi} est la plus grande bisimulation de ce type.

Nous pouvons prouver la correction de cette relation grâce à la méthode de Howe :

Théorème 6.1. La relation \sim_{pi} est une congruence.

La principale difficulté est de prouver la clause de pseudo-simulation sur les émissions :

Lemme 6.1. Si $P \sim_{pi}^\bullet Q$ et $P \xrightarrow{\tilde{a}, E, \tilde{R}} P'$ alors pour tout $E \sim_{pi}^\bullet E'$ et $\tilde{R} \sim_{pi}^\bullet \tilde{R}'$, il existe Q' tel que $Q \xrightarrow{\tilde{a}, E', \tilde{R}'} Q'$ et $P' \sim_{pi}^\bullet Q'$.

La preuve se fait en deux étapes : le résultat est prouvé pour un nombre de messages émis égal à 1 (c'est-à-dire avec le multi-ensemble \tilde{a} de taille 1), avant d'être étendu par induction à un nombre quelconque de messages. Les preuves sont données en appendice A.4.

Par définition, nous avons directement $\sim_{pi} \subseteq \sim_m$. Les deux bisimilarités ne sont pas égales dans le cas général : la clause de réception de \sim_m est écrite dans le style précoce, alors que la clause sur les réceptions partielles de \sim_{pi} est écrite dans le style tardif, puisque I et I' doivent être en relation pour toute substitution σ qui les clôt. Pour $\text{HO}\pi\text{J}$, nous conjecturons que les deux relations coïncident. Plus précisément, nous conjecturons l'existence d'une bisimilarité normale \sim_n , sur le même modèle que celle de $\text{HO}\pi$ (avec, dans le cas de la réception, autant de déclencheurs frais $n.\mathbf{0}$ que de variables dans le récepteur joint π), qui coïncide avec les relations \sim_m et \sim_{pi} . Pour le Kell, nous donnerons un contre-exemple qui montre que l'inclusion ci-dessus est stricte, et que la relation étendue aux réceptions partielles est trop discriminante.

Remarque 6.1. *Écrire la clause sur les réceptions partielles dans un style précoce, par exemple en demandant que I et I' soient en relation pour une substitution σ donnée, ne permet pas de prouver la congruence avec la méthode de Howe : lors d'une émission $P \xrightarrow{\tilde{a}, E, \tilde{R}} J$, nous devons considérer la substitution σ des messages reçus par E à une étape de la preuve où ne nous connaissons pas tous les messages émis par P et \tilde{R} .*

6.2 Sémantique à complément du Kell

6.2.1 Présentation du Kell

Le Kell [47] est un calcul distribué conçu pour étudier la programmation distribuée par composants, et notamment le modèle Fractal [6]. Plusieurs variantes du calcul peuvent être définies, en fonction de la syntaxe choisie pour les réceptions $\pi \triangleright P$. Dans cette section, nous nous intéressons à la variante appelée jK dans [47], qui autorise les récepteurs joints. Le Kell est un calcul d'ordre supérieur avec localités hiérarchisées, appelées *kells*, et qui permet un contrôle accru sur les communications. Contrairement à $\text{HO}\pi\text{P}$, les localités du Kell admettent des continuations.

Les réceptions en Kell précisent la provenance des messages, en indiquant la position que doit occuper l'émetteur par rapport au récepteur. Un récepteur $a(X) \triangleright P$ attend un message local sur a , c'est-à-dire émis par un processus en parallèle, au même niveau dans la hiérarchie des kells. Le récepteur $a^\uparrow(X) \triangleright P$ attend un message provenant du kell parent (message dit *supérieur* par la suite), alors que $a^\downarrow(X) \triangleright P$ attend un message provenant d'un kell fils (message dit *inférieur* par la suite). Enfin, $a[X] \triangleright P$ peut passer un kell local a . Les messages peuvent traverser au plus une frontière de localité, alors que la passivation ne peut se faire qu'au même niveau. Dans le processus $P \mid a[b[Q]\mathbf{0} \mid R]\mathbf{0}$, P ne peut pas communiquer avec Q mais peut communiquer avec R , et R peut communiquer avec Q . Le processus P peut passer le kell a mais pas le kell b , et R peut passer b .

Des réceptions de types différents peuvent être combinées dans un récepteur joint. Ainsi le processus

$$R_1 \triangleq b^\uparrow(X) \mid c^\downarrow(Y) \triangleright X \mid Y$$

a besoin d'un message supérieur sur b et d'un message inférieur sur c . Par exemple nous avons

$$\bar{b}\langle T_1 \rangle \mathbf{0} \mid d[R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1] S_2 \xrightarrow{\tau} d[T_1 \mid T_2 \mid e[\mathbf{0}] S_1] S_2$$

Notez qu'avec ces restrictions, deux processus dans des kells en parallèle

$$a[\bar{c}\langle P \rangle \mathbf{0}] \mathbf{0} \mid b[c(X) \triangleright X] \mathbf{0}$$

ne peuvent communiquer directement : le kell parent doit transmettre le message.

$$\begin{aligned} & c^\downarrow(X) \triangleright \bar{c}\langle X \rangle \mathbf{0} \mid a[\bar{c}\langle P \rangle \mathbf{0}] \mathbf{0} \mid b[c^\uparrow(X) \triangleright X] \mathbf{0} \\ & \xrightarrow{\tau} \bar{c}\langle P \rangle \mathbf{0} \mid a[\mathbf{0}] \mathbf{0} \mid b[c^\uparrow(X) \triangleright X] \mathbf{0} \\ & \xrightarrow{\tau} a[\mathbf{0}] \mathbf{0} \mid b[P] \mathbf{0} \end{aligned}$$

$$\begin{aligned}
P &::= \mathbf{0} \mid X \mid P \mid P \mid \nu a.P \mid \bar{a}\langle P \rangle P \mid \pi \triangleright P \mid a[P]P \\
\pi &::= \pi \mid \pi \mid a(X) \mid a[X] \mid a^\uparrow(X) \mid a^\downarrow(X)
\end{aligned}$$

FIG. 6.6 – Syntaxe de jK

Notations :

$$\begin{aligned}
\text{Fonctions} \quad F, G &::= (\pi)P \\
\text{Concrétions} \quad C, D &::= \langle \widetilde{a^\eta}, P \rangle Q \mid \nu a.C \\
\text{Provenance} \quad \eta &::= * \mid p \mid \downarrow \mid \uparrow
\end{aligned}$$

Extension des opérateurs aux agents :

$$\begin{aligned}
(\nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle P) \mid Q &\triangleq \nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle (P \mid Q) \\
\nu c. (\nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle P) &\triangleq \nu \widetilde{b}. c. \langle \widetilde{a^\eta}, R \rangle P \text{ si } c \in \bigcup \widetilde{\text{fn}}(R) \\
\nu c. (\nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle P) &\triangleq \nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle \nu c.P \text{ si } c \notin \bigcup \widetilde{\text{fn}}(R) \\
c[\nu \widetilde{b}. \langle \widetilde{a^*}, R \rangle P]Q &\triangleq \nu \widetilde{b}. \langle \widetilde{a^\downarrow}, R \rangle c[P]Q \\
((\pi)P) \mid Q &\triangleq (\pi)(P \mid Q) \\
\nu c. ((\pi)P) &\triangleq (\pi)(\nu c.P) \\
c[(\prod \widetilde{a^\uparrow(X)})P]Q &\triangleq (\prod \widetilde{a^*(X)})c[P]Q
\end{aligned}$$

Composition parallèle des concrétions :

$$\nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle P \mid \nu \widetilde{b'}. \langle \widetilde{a^{\eta'}}, R' \rangle Q \triangleq \nu \widetilde{b \cup b'}. \langle \widetilde{a^\eta}, R \uplus \widetilde{a^{\eta'}}, R' \rangle P \mid Q$$

FIG. 6.7 – Fonctions et concrétions en jK

6.2.2 Syntaxe et sémantique contextuelle

La syntaxe de jK est donnée en figure 6.6, et les fonctions et concrétions sont définies en figure 6.7. Dans une concrétion $\nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle S$, nous indiquons la provenance η des messages : $*$ indique un message émis à la racine du processus, p indique un message issu d'une passivation, et \downarrow indique un message inférieur. Nous n'avons pas de messages annotés par \uparrow ; cette étiquette est utilisée uniquement pour la réception. Pour simplifier l'écriture des règles du système de transitions, nous écrivons le récepteur joint π d'une fonction $(\pi)P$ sous la forme $\prod \widetilde{a^\eta(X)}$. Cela revient à réécrire $a(X)$ en $a^*(X)$ et $a[X]$ en $a^p(X)$. Nous définissons l'ensemble des provenances d'une fonction $F = (\prod \widetilde{a^\eta(X)})P$ par $\eta(F) \triangleq \bigcup \widetilde{\eta}$ et les provenances d'une concrétion $C = \nu \widetilde{b}. \langle \widetilde{a^\eta}, R \rangle S$ par $\eta(C) \triangleq \bigcup \widetilde{\eta}$.

Comme pour les calculs précédents, nous étendons les opérateurs à tous les agents. Notez que la composition d'un kell $c[\square]Q$ et d'une fonction $(\prod \widetilde{a^\eta(X)})P$ est possible si et seulement si le récepteur joint attend uniquement des messages supérieurs, c'est-à-dire si et seulement si les provenances $\widetilde{\eta}$ sont toutes \uparrow . Dans la fonction résultante $(\prod \widetilde{a^*(X)})c[P]Q$, les provenances sont changées en $*$; nous verrons par la suite pourquoi. De même, la composition d'un kell et d'une concrétion est possible si et seulement si les provenances des messages sont toutes $*$; dans la concrétion résultante, ces provenances sont changées en \downarrow .

Les règles du système de transitions étiquetées de jK sont données en figure 6.8, à l'exception du symétrique des règles PAR, PAR-OUT, PART-HO et HO. La transition $P \xrightarrow{\widetilde{a}} F$ signifie que P contient un récepteur joint capable de recevoir simultanément sur

Pseudo-application

$$(\prod \widetilde{a^\eta(X)})P \bullet \nu \widetilde{b}. \langle \widetilde{a^\eta}, \widetilde{R} \rangle S \triangleq \nu \widetilde{b}. (P\{\widetilde{R}/\widetilde{X}\} \mid S) \quad \bullet\text{-PROC}$$

$$(\prod \widetilde{a^\eta(X)} \mid \pi)P \bullet \nu \widetilde{b}. \langle \widetilde{a^\eta}, \widetilde{R} \rangle S \triangleq (\pi) \nu \widetilde{b}. (P\{\widetilde{R}/\widetilde{X}\} \mid S) \quad \bullet\text{-ABS}$$

Règles du système de transitions étiquetées :

$$\pi \triangleright P \xrightarrow{\widetilde{a}} (\pi)P \quad \text{IN} \qquad \bar{a}\langle Q \rangle P \xrightarrow{\bar{a}} \langle a^*, Q \rangle P \quad \text{OUT} \qquad a[Q]P \xrightarrow{\bar{a}} \langle a^p, Q \rangle P \quad \text{PASSIV}$$

$$\frac{P \xrightarrow{\alpha_k} A}{P \mid Q \xrightarrow{\alpha_k} A \mid Q} \quad \text{PAR} \qquad \frac{P \xrightarrow{\widetilde{a}} C \quad Q \xrightarrow{\widetilde{a'}} C'}{P \mid Q \xrightarrow{\widetilde{a} \uplus \widetilde{a'}} C \mid C'} \quad \text{PAR-OUT}$$

$$\frac{P \xrightarrow{\alpha_k} A \quad a \notin \text{fn}(\alpha_k)}{\nu a.P \xrightarrow{\alpha_k} \nu a.A} \quad \text{RESTR} \qquad \frac{P \xrightarrow{\widetilde{a}} C \quad \eta(C) = \{*\}}{c[P]Q \xrightarrow{\widetilde{a}} c[C]Q} \quad \text{LOC-OUT}$$

$$\frac{P \xrightarrow{\widetilde{a}} F \quad \eta(F) = \{\uparrow\}}{c[P]Q \xrightarrow{\widetilde{a}} c[F]Q} \quad \text{LOC-IN} \qquad \frac{P \xrightarrow{\tau} P'}{a[P]Q \xrightarrow{\tau} a[P']Q} \quad \text{LOC-TAU}$$

$$\frac{P \xrightarrow{\delta} \widetilde{a}F \quad Q \xrightarrow{\widetilde{a}} C}{P \mid Q \xrightarrow{\tau} F \bullet C} \quad \text{HO} \qquad \frac{P \xrightarrow{\delta} \widetilde{a} \uplus \widetilde{a'}F \quad Q \xrightarrow{\widetilde{a}} C \quad \widetilde{a'} \neq \emptyset}{P \mid Q \xrightarrow{\delta} \widetilde{a'}F \bullet C} \quad \text{PART-HO}$$

FIG. 6.8 – Système de transitions étiquetées de jK

\tilde{a} . La transition $P \xrightarrow{\tilde{a}} C$ signifie que P est capable d'émettre des messages sur \tilde{a} . Les actions internes sont classiquement notées τ . La méta-variable α_k parcourt l'ensemble des étiquettes, et nous définissons $\text{fn}(\tau) \triangleq \emptyset$ et $\text{fn}(\tilde{a}) = \text{fn}(\tilde{a}) \triangleq \tilde{a}$.

La communication du Kell repose sur la position relative dans l'arbre des localités des émetteurs par rapport au récepteur, ce qui rend difficile l'écriture du systèmes de transitions étiquetées. Reprenons les processus

$$\begin{aligned} R_1 &\triangleq b^\dagger(X) \mid c^\downarrow(Y) \triangleright X \mid Y \\ R_2 &\triangleq \bar{b}\langle T_1 \rangle \mathbf{0} \mid d[R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1] S_2 \end{aligned}$$

Il n'est pas possible de décomposer R_2 en $P \mid Q$, avec P processus récepteur et Q processus émetteur (qui contient tous les envois de messages), même en utilisant la congruence structurelle comme en $\text{HO}\pi\text{J}$. En revanche, nous pouvons distinguer le processus $\bar{b}\langle T_1 \rangle \mathbf{0}$ du processus $d[R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1] S_2$ qui peut se synchroniser partiellement. L'opérateur de pseudo-application \bullet autorise donc les synchronisations partielles entre une fonction F et une concrétion C . Si C propose strictement moins de messages que n'en demande le récepteur joint de F , l'agent $F \bullet C$ obtenu est une fonction paramétrée par les réceptions non instanciées par C (règle $\bullet\text{-ABS}$). Si les messages émis par C complètent exactement le récepteur joint de F , l'agent $F \bullet C$ obtenu est un processus classique (règle $\bullet\text{-PROC}$). La synchronisation de R_2 peut donc se faire en deux étapes : d'abord la synchronisation partielle dans le kell d puis la synchronisation du processus R_2 entier.

Les règles OUT et PASSIV annotent les messages en fonction de leur origine. Les règles de congruence PAR et RESTR sont classiques. Comme en $\text{HO}\pi\text{J}$, la règle PAR-OUT permet de combiner les émissions de messages en une concrétions plus importantes. Les règles LOC-TAU , LOC-OUT et LOC-IN traitent la composition par un kell, et assurent le contrôle sur les communications. Dans le cas d'une émission $P \xrightarrow{\tilde{a}} C$, tous les messages doivent être locaux (prémisse $\eta(C) = *$ de la règle LOC-OUT), interdisant toute émission de message inférieur ou issu d'une passivation. Leur annotation devient alors \downarrow dans $c[C]Q$. Par exemple, nous avons l'émission suivante dans R_2 :

$$\frac{\bar{c}\langle T_2 \rangle \mathbf{0} \xrightarrow{\bar{c}} \langle c^*, T_2 \rangle \mathbf{0}}{e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1 \xrightarrow{\bar{c}} \langle c^\downarrow, T_2 \rangle e[\mathbf{0}] S_1}$$

Le message émis sur c a donc la provenance attendue par R_1 , nous avons donc par synchronisation sur c (règle PART-HO)

$$\frac{R_1 \xrightarrow{b,c} (b^\dagger(X) \mid c^\downarrow(Y))X \mid Y \quad e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1 \xrightarrow{\bar{c}} \langle c^\downarrow, T_2 \rangle e[\mathbf{0}] S_1}{R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1 \xrightarrow{b} (b^\dagger(X))(X \mid T_2 \mid e[\mathbf{0}] S_1)}$$

Lorsqu'une fonction F est plongée dans un kell $c[\square]Q$, nous vérifions que le récepteur joint de F ne contient que des récepteurs $a^\dagger(X)$ (prémisse $\eta(F) = \{\uparrow\}$ de la règle LOC-IN). Cette vérification assure que la fonction $c[F]Q$ est capable de se synchroniser. En effet, un récepteur joint contenant une annotation $*$, p , ou \downarrow , comme par exemple $a^\downarrow(X) \triangleright X$, est bloqué une fois placé dans un kell : le processus $c[a^\downarrow(X) \triangleright X]Q$ ne peut pas recevoir de message sur a . En outre, les messages supérieurs que doit recevoir la fonction F sont émis au même niveau que $c[F]Q$; les messages attendus sont donc locaux (c'est-à-dire émis en parallèle) par rapport à $c[F]Q$. C'est pourquoi nous changeons les provenances du récepteur de $c[F]Q$ en $*$. Par exemple nous avons dans R_2 :

$$\frac{R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1 \xrightarrow{b} (b^\dagger(X))(X \mid T_2 \mid e[\mathbf{0}] S_1)}{d[R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}] S_1] S_2 \xrightarrow{b} (b^*(X))d[X \mid T_2 \mid e[\mathbf{0}] S_1] S_2}$$

Syntaxe :

$$\begin{aligned} I &::= \pi \blacktriangleright_{\delta} P \mid \mathbf{0} \blacktriangleright_{\delta} P \\ E &::= I \mid P \\ \delta &::= * \mid \square \end{aligned}$$

Extension des opérateurs du langage :

$$\begin{aligned} (\pi \blacktriangleright_{\delta} P) \mid Q &\triangleq \pi \blacktriangleright_{\delta} (P \mid Q) \\ Q \mid (\pi \blacktriangleright_{\delta} P) &\triangleq \pi \blacktriangleright_{\delta} (Q \mid P) \\ \nu b.(\pi \blacktriangleright_{\delta} P) &\triangleq \pi \blacktriangleright_{\delta} \nu b.P \\ b[\pi \blacktriangleright_{*} P]Q &\triangleq \pi \blacktriangleright_{\square} b[P]Q \end{aligned}$$

Règles du jugement de réception partielle :

$$\begin{aligned} &\frac{\pi \equiv a^{\eta}(X) \mid \pi' \quad \tilde{b} = \text{fn}(\pi)}{\pi \triangleright P \xrightarrow{a^{\eta}, R} \pi' \blacktriangleright_{*} P\{R/X\}} \text{PROC}_{pi}^k && \frac{\pi \equiv a^{\eta}(X) \mid \pi'}{\pi \blacktriangleright_{\delta} P \xrightarrow{a^{\eta}, R} \pi' \blacktriangleright_{\delta} P\{R/X\}} \text{PART-IN}_{pi}^k \\ &\frac{P \xrightarrow{a^{\eta}, R} I}{P \mid Q \xrightarrow{a^{\eta}, R} I \mid Q} \text{PAR}_{pi}^k && \frac{P \xrightarrow{a^{\eta}, R} I \quad b \notin n(I)}{\nu b.P \xrightarrow{a^{\eta}, R} \nu b.I} \text{RESTR}_{pi}^k \\ &\frac{P \xrightarrow{a^{\eta}, R} I \quad \delta(I) = *}{b[P]Q \xrightarrow{a^{\eta}, R} b[I]Q} \text{LOC}_{pi}^k \end{aligned}$$

FIG. 6.9 – Réception partielle en jK

La synchronisation est maintenant possible sur b par la règle HO :

$$\frac{d[R_1 \mid e[\bar{c}\langle T_2 \rangle \mathbf{0}]S_1]S_2 \xrightarrow{b} (b^*(X))d[X \mid T_2 \mid e[\mathbf{0}]S_1]S_2 \quad \bar{b}\langle T_1 \rangle \mathbf{0} \xrightarrow{\bar{b}} \langle b^*, T_1 \rangle \mathbf{0}}{R_2 \xrightarrow{\tau} d[T_1 \mid T_2 \mid e[\mathbf{0}]S_1]S_2}$$

Schmitt et Stefani proposent dans [47] une bisimilarité contextuelle précoce qui caractérise la congruence barbue forte du Kell. Leur relation repose sur des *contextes applicatifs*, c'est-à-dire des contextes qui peuvent réagir avec les processus testés. Par exemple, pour tester le processus $b^{\dagger}(X) \mid c^{\downarrow}(Y) \triangleright X \mid Y$, la bisimilarité utilise tous les contextes de la forme $C_1 \mid d[\square \mid C_2]U$, où C_1 émet un seul message sur b et C_2 un seul message sur c . Comme expliqué dans le chapitre 4, la méthode de preuve utilisée pour la congruence échoue dans le cas faible.

6.2.3 Sémantique à complément : principe

La sémantique à complément de jK est construite selon le même principe que celle de HO π J : nous parcourons le processus émetteur à la recherche des messages, que nous passons au récepteur au fur et à mesure de leur découverte. La définition des transitions d'émission est rendue complexe par le contrôle des communications. Ainsi, pour compléter une émission $P = \bar{a}\langle R \rangle S$ avec un récepteur joint $Q_1 = a^{\downarrow}(X) \mid b^{\downarrow}(X) \mid c^{\downarrow}(X) \triangleright Q$, nous devons placer P dans un kell, et ajouter deux émetteurs P_2, P_3 sur b et c , qui doivent également émettre depuis un ou plusieurs kells. Plusieurs configurations sont possibles : les émissions de P, P_2, P_3 peuvent provenir du même kell, ou de deux ou trois kells différents. De même pour compléter P avec un récepteur $Q_2 = a^{\downarrow}(X) \mid b^{\dagger}(X) \triangleright Q'$, nous devons

placer P dans un kell a_1 , plonger ce kell en parallèle avec Q_2 dans un autre kell a_2 , pour permettre la communication avec un émetteur supérieur P_2 sur b . Notre sémantique à complément doit être capable de construire tous les environnements de test possibles.

Comme pour $\text{HO}\pi\text{J}$, nous utilisons les réceptions partielles $\pi \blacktriangleright_\delta P$, qui sont instanciées progressivement grâce au jugement d'instanciation partielle $E \xrightarrow{a^\eta, R}_\delta I$. La syntaxe et les règles de dérivation sont données en figure 6.9. Notez que la réception partielle contient une information de localisation δ , indiquant la provenance du récepteur joint, qui peut être soit la racine du processus $*$, soit un kell fils quelconque \square . Pour une réception partielle $I = \prod \widetilde{a^\eta(X)} \blacktriangleright_\delta P$, nous définissons la localisation de I , $\delta(I) \triangleq \delta$ et l'ensemble des provenances de I , $\eta(I) \triangleq \bigcup \widetilde{\eta}$. La règle Loc_{pi}^k autorise ainsi une réception partielle de $b[P]Q$ si et seulement si la réception $P \xrightarrow{a^\eta, R}_\delta I$ a lieu à la racine de P , c'est-à-dire si et seulement si $\delta(I) = *$.

6.2.4 Transitions inférieures

Nous définissons deux types d'émission, en fonction de la position relative des émetteurs par rapport au récepteur dans la hiérarchie des localités. Nous nous intéressons d'abord aux transitions dites *inférieures*, dans lesquelles les émetteurs sont au même niveau ou en dessous de l'entité réceptrice, comme par exemple dans le processus $(a^*(X) \mid b^\downarrow(Y)) \triangleright (X \mid Y) \mid \bar{a}\langle c.0 \rangle 0 \mid d[\bar{b}\langle c.0 \rangle] 0$. Le résultat d'une transition inférieure peut ne pas être complètement instancié, si le récepteur joint attend un message supérieur, comme par exemple $a(X) \mid b^\uparrow(Y) \triangleright Q$. Nous obtenons alors une réception partielle I , que nous complétons avec les transitions *supérieures* d'émission, que nous détaillons en section 6.2.5.

Comme pour $\text{HO}\pi\text{J}$, nous définissons un jugement (inférieur) de synchronisation partielle $P \xrightarrow{\leq, \theta}_\delta I$, qui affirme que P contient un récepteur joint et des émissions de messages inférieurs, et que la synchronisation partielle de ces processus donne I . Nous définissons également un jugement d'émission

$$P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n} \{ \widetilde{P}^{c_n} \}}_{\widetilde{b}} I$$

dans lequel les processus émetteurs $P, \widetilde{P}^*, \biguplus_{c_n} \widetilde{P}^{c_n}$ émettent des messages locaux, inférieurs ou issus de passivation sur \widetilde{a} , et se synchronisent avec E pour donner I . Aucune synchronisation partielle n'a lieu à l'intérieur de E .

Nous détaillons d'abord le jugement d'émission. Dans ce jugement, les messages sont traités un par un ; la provenance du message de P considéré est donné par l'étiquette ξ . Si $\xi = *$, le message est local ; si $\xi = p$, le message provient d'une passivation, et enfin si $\xi = c_n$, le message provient d'un kell nommé c . Comme un processus peut contenir plusieurs kells nommés c , nous différencions les instances de c à l'aide d'un indice $n \in \mathcal{N}$.

Informellement, pour $\xi \in \{*, p\}$, la transition $P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n} \{ \widetilde{P}^{c_n} \}}_{\widetilde{b}} I$ signifie que nous avons

$$E \mid \mathbb{E}^* \{ P \mid \prod \widetilde{P}^* \mid \prod_{c_n} \mathbb{K}^{c_n} \{ \prod \widetilde{P}^{c_n} \} \} \xrightarrow{\tau} I$$

par synchronisation sur \widetilde{a} . Les émetteurs sont plongés dans les contextes $\mathbb{E}^*, \mathbb{K}^{c_n}$; pour expliciter le contrôle sur les communications, nous distinguons les contextes inclus dans un kell \mathbb{K} des autres contextes d'évaluation \mathbb{E} .

$$\begin{aligned} \mathbb{E} &::= \square \mid \nu a. \square \mid P \mid \square \mid \square \mid P \\ \mathbb{K} &::= a[\mathbb{E}]P \end{aligned}$$

Les contextes kell \mathbb{K}^{c_n} sont annotés avec le nom du kell numéroté c_n qu'ils contiennent. Les processus et contextes sont classés selon leur provenance : les processus \widetilde{P}^* émettent

des messages locaux ou des processus passivés, et les processus $\widetilde{P^{c_n}}$ émettent des messages inférieurs depuis le contexte \mathbb{K}^{c_n} . Les processus $\widetilde{P^*}, \mathbb{K}^{c_n}\{\prod \widetilde{P^{c_n}}\}$ sont tous plongés dans le contexte \mathbb{E}^* pour la communication. Le processus P est également placé dans un contexte, en fonction de ξ : si $\xi \in \{*, p\}$, alors P est placé dans le contexte \mathbb{E}^* , et si $\xi = c_n$, alors P est placé dans le contexte correspondant \mathbb{K}^{c_n} .

Les règles de déduction pour l'émission inférieure sont données en appendice A.5 ; nous détaillons ici les règles les plus importantes. Chaque règle comporte généralement deux versions selon la provenance ξ : le nom des règles concernant les messages locaux ou les passivations est indicé par $=$, alors que celles concernant les messages inférieurs sont indicées par $<$. Nous rappelons que l'extension de portée est paresseuse dans le Kell ; nous procédons de la même manière qu'en $\text{HO}\pi\text{P}$ (section 5.2), en indiquant l'ensemble des noms \widetilde{b} dont la portée peut être étendue. De même les contextes $\mathbb{E}^*, \mathbb{K}^{c_n}$ peuvent capturer les noms libres des messages : nous définissons donc d'abord des transitions sans capture par les contextes $P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{c_n}\{\widetilde{P^{c_n}}\}}_{\widetilde{b}} I$, avant de définir les transitions avec capture.

Nous donnons d'abord les règles pour l'émission d'un message local $\bar{a}\langle P_1 \rangle P_2$. La règle $\text{OUT}_{1,=}^k$ traite le cas dans lequel les multi-ensembles de processus en étiquettes sont vides, c'est-à-dire qu'il ne reste plus de messages à trouver.

$$\frac{E \xrightarrow{a^*, P_1} I \quad \text{fn}(P_1) = \widetilde{b} \quad \text{bn}(\mathbb{E}^*) \cap \widetilde{b} = \emptyset}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, *, E, \mathbb{E}^*, \emptyset, \emptyset}_{\widetilde{b}} I \mid \mathbb{E}^*\{P_2\}} \text{OUT}_{1,=}^k$$

Il suffit alors de mettre en parallèle la réception I (obtenue après instantiation du message P_1) et la continuation P_2 dans le contexte \mathbb{E}^* . La condition $\text{bn}(\mathbb{E}^*) \cap \widetilde{b} = \emptyset$ assure l'absence de capture par \mathbb{E}^* . Si les multi-ensembles $\widetilde{P^*}$ ou $\biguplus_{c_n} \widetilde{P^{c_n}}$ sont non-vides, il reste des messages à découvrir ; le prochain processus P' à investiguer peut être choisi dans $\widetilde{P^*}$ ou dans un des $\widetilde{P^{c_n}}$.

$$\frac{\begin{array}{c} E \xrightarrow{a^*, P_1} I \quad \text{fn}(P_1) = \widetilde{b} \quad \xi \in \{*, p\} \\ \text{bn}(\mathbb{E}^*) \cap (\widetilde{b} \cup \widetilde{b}') = \emptyset \quad P' \xrightarrow{\widetilde{a}', \xi, I, \mathbb{E}^*\{\square \mid P_2\}, \widetilde{P^*}, \mathbb{K}^{c_n}\{\widetilde{P^{c_n}}\}}_{\widetilde{b}'} I' \end{array}}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\widetilde{a}' \uplus \bar{a}, *, E, \mathbb{E}^*, \widetilde{P^*} \uplus P', \mathbb{K}^{c_n}\{\widetilde{P^{c_n}}\}}_{\widetilde{b}' \uplus \widetilde{b}} I'} \text{OUT}_{2,=}^k$$

Dans la règle $\text{OUT}_{2,=}^k$, le processus P' est choisi dans $\widetilde{P^*}$. La réception partielle I , obtenue en appliquant le processus P_1 à E , est utilisée comme récepteur dans la transition

$$P' \xrightarrow{\widetilde{a}', \xi, I, \mathbb{E}^*\{\square \mid P_2\}, \widetilde{P^*}, \mathbb{K}^{c_n}\{\widetilde{P^{c_n}}\}}_{\widetilde{b}'} I'$$

Cette transition fournit le résultat I' de la communication de I avec les processus P' , $\widetilde{P^*}$, $\biguplus_{c_n} \widetilde{P^{c_n}}$, placés dans le contexte $\mathbb{E}^*\{\square \mid P_2\}$. Nous avons donc informellement

$$I \mid \mathbb{E}^*\{P' \mid P_2 \mid \prod \widetilde{P^*} \mid \prod_{c_n} \mathbb{K}^{c_n}\{\prod \widetilde{P^{c_n}}\}\} \xrightarrow{\tau} I'$$

Comme I est le résultat de la communication partielle de E avec $\bar{a}\langle P_1 \rangle P_2$ et comme \mathbb{E}^* ne capture pas de noms de P_1 , la transition précédente peut s'écrire

$$E \mid \mathbb{E}^*\{P' \mid \bar{a}\langle P_1 \rangle P_2 \mid \prod \widetilde{P^*} \mid \prod_{c_n} \mathbb{K}^{c_n}\{\prod \widetilde{P^{c_n}}\}\} \xrightarrow{\tau} I'$$

La réception partielle I' est donc bien le résultat de la communication de E avec les processus $\bar{a}\langle P_1 \rangle P_2$, P' , $\widetilde{P^*}$, $\biguplus_{c_n} \widetilde{P^{c_n}}$ placés dans le contexte \mathbb{E}^* , comme le reflète la conclusion de

la règle $\text{OUT}_{2,=}^k$. La règle $\text{OUT}_{3,=}^k$ est construite de la même manière, sauf que le processus P' est ici choisi dans un des multi-ensembles $\widetilde{P^{c_n}}$.

$$\frac{E \xrightarrow{a^*, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*) \cap (\tilde{b} \cup \tilde{b}') = \emptyset}{\frac{P' \xrightarrow{\tilde{a}', c_{n_0}, I, \mathbb{E}^* \{\square | P_2\}, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}}}\}}}{\tilde{b}'} I'}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, *, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}} \uplus P'}\}}}{\tilde{b}' \cup \tilde{b}} I'} \text{OUT}_{3,=}^k$$

Les règles pour la passivation $a[P_1]P_2$ sont construites comme les règles locales correspondantes. Par exemple, la règle $\text{PASSIV}_{1,=}^k$ est la suivante :

$$\frac{E \xrightarrow{a^p, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*) \cap \tilde{b} = \emptyset}{a[P_1]P_2 \xrightarrow{\bar{a}, p, E, \mathbb{E}^*, \emptyset, \emptyset}{\tilde{b}} I \mid \mathbb{E}^* \{P_2\}} \text{PASSIV}_{1,=}^k$$

Nous avons également deux règles $\text{PASSIV}_{2,=}^k$ et $\text{PASSIV}_{3,=}^k$ construites comme $\text{OUT}_{2,=}^k$ et $\text{OUT}_{3,=}^k$.

Supposons maintenant que le message de P provient du kell c_{n_0} . Nous devons prendre en compte le contexte $\mathbb{K}^{c_{n_0}}$ en plus de \mathbb{E}^* . Par exemple, dans le cas où les multi-ensembles de processus sont vides, nous avons :

$$\frac{E \xrightarrow{a^\downarrow, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{c_n}) \cap \tilde{b} = \emptyset}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\bar{a}, c_n, E, \mathbb{E}^*, \emptyset, \mathbb{K}^{c_n} \{\emptyset\}}{\tilde{b}} I \mid \mathbb{E}^* \{\mathbb{K}^{c_n} \{P_2\}\}} \text{OUT}_{1,<}^k$$

En outre, nous devons distinguer plusieurs cas en fonction de $\widetilde{P^{c_{n_0}}}$. Si $\widetilde{P^{c_{n_0}}} \neq \emptyset$, les règles sont construites comme précédemment.

$$\frac{E \xrightarrow{a^\downarrow, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{c_{n_0}}) \cap (\tilde{b} \cup \tilde{b}') = \emptyset}{\frac{\widetilde{P^{c_{n_0}}} \neq \emptyset \quad \xi \in \{*, p\} \quad P' \xrightarrow{\tilde{a}', \xi, I, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}} | P_2\}}}{\tilde{b}'} I'}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}}}\}}}{\tilde{b}' \cup \tilde{b}} I'} \text{OUT}_{2,<}^k$$

Nous choisissons un processus P' parmi les processus $\widetilde{P^*}$ pour le faire réagir avec I , et nous modifions le contexte $\mathbb{K}^{c_{n_0}}$ pour y inclure la continuation P_2 . Nous avons également une règle $\text{OUT}_{3,<}^k$, dans laquelle le processus P' est choisi parmi les processus inférieurs.

En revanche, si $\widetilde{P^{c_{n_0}}} = \emptyset$, tous les messages émis depuis le kell c_{n_0} ont été découverts, le contexte $\mathbb{K}^{c_{n_0}}$ n'englobe donc plus aucun processus et peut être enlevé de l'étiquette.

$$\frac{E \xrightarrow{a^\downarrow, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{c_{n_0}}) \cap (\tilde{b} \cup \tilde{b}') = \emptyset}{\frac{c_{n_0} \notin \tilde{c}_n \quad \xi \in \{*, p\} \quad P' \xrightarrow{\tilde{a}', \xi, I, \mathbb{E}^* \{\square | \mathbb{K}^{c_{n_0}} \{P_2\}\}, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}}}{\tilde{b}'} I'}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\emptyset\}}}{\tilde{b}' \cup \tilde{b}} I'} \text{OUT}_{4,<}^k$$

Nous rappelons que les contextes \mathbb{K}^{c_n} sont eux-mêmes inclus dans le contexte \mathbb{E}^* ; c'est pourquoi dans la prémisse de la règle $\text{OUT}_{4,<}^k$, le contexte \mathbb{E}^* est étendu avec le processus $\mathbb{K}^{c_{n_0}} \{P_2\}$. Le processus P' peut aussi être choisi parmi les processus inférieurs (règle $\text{OUT}_{5,<}^k$).

Les règles de congruence sont à rapprocher pour la plupart de celles de $\text{HO}\pi\text{P}$ (figure 5.3). Par exemple, prenons le cas de la composition parallèle $P_1 \mid P_2$, dans lequel P_2 ne

participe pas à la communication.

$$\frac{P_1 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*\{\square|P_2\}, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I \quad \xi \in \{*, p\}}{P_1 \mid P_2 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I} \text{PAR}_{\leq}^k$$

Nous souhaitons mettre P_2 en parallèle avec la continuation de P_1 dans la réception partielle I résultante. Si P_1 est un message local ou une passivation (c'est-à-dire si $\xi \in \{*, p\}$), le contexte \mathbb{E}^* est modifié dans la prémisse de la règle PAR_{\leq}^k pour englober P_2 . Si P_1 émet un message depuis un kell c_{n_0} , le contexte $\mathbb{K}^{c_{n_0}}$ est modifié dans la règle équivalente $\text{PAR}_{<}^k$.

$$\frac{P_1 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\} \cup \mathbb{K}^{c_{n_0}}\{\widetilde{P}^{c_{n_0}}|P_2\}} \widetilde{b} I}{P_1 \mid P_2 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I} \text{PAR}_{<}^k$$

Si P_2 interagit avec le récepteur, alors comme en $\text{HO}\pi\text{J}$, le processus P_2 est conservé dans l'étiquette. Si $\xi \in \{*, p\}$, alors P_2 est placé dans \widetilde{P}^* (règle PAR-OUT_{\leq}^k), et si $\xi = c_{n_0}$, P_2 est placé dans $\widetilde{P}^{c_{n_0}}$ (règle équivalente $\text{PAR-OUT}_{<}^k$).

$$\frac{P_1 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^* \uplus P_2, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I \quad \xi \in \{*, p\}}{P_1 \mid P_2 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I} \text{PAR-OUT}_{\leq}^k$$

Les règles RESTR_{\leq}^k et $\text{RESTR}_{<}^k$ pour la restriction sans capture sont semblables à PAR_{\leq}^k et $\text{PAR}_{<}^k$. En cas de capture, la portée de la restriction est étendue pour englober l'entité réceptrice E .

$$\frac{P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I \quad d \in \widetilde{b} \quad d \notin \widetilde{a}}{\nu d.P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} \setminus d \nu d.I} \text{EXTR}_{\leq}^k$$

Enfin, dans la règle de congruence par rapport à l'opérateur kell

$$\frac{P_1 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\} \cup \mathbb{K}^{c_{n_0}}\{\emptyset\}} \widetilde{b} I \quad \mathbb{K}^{c_{n_0}} = c[\square]P_2 \quad c_{n_0} \notin \widetilde{c}_n}{c[P_1]P_2 \xrightarrow{\widetilde{a}, *, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I} \text{LOC}_{\leq}^k$$

nous créons un environnement $\mathbb{K}^{c_{n_0}} = c[\square]P_2$, dans lequel n_0 est un indice frais. Nous vérifions ensuite que P_1 est capable d'émettre depuis c_{n_0} avec la prémisse

$$P_1 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\} \cup \mathbb{K}^{c_{n_0}}\{\emptyset\}} \widetilde{b} I$$

Nous donnons maintenant les règles pour le jugement d'émission

$$P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I$$

qui autorise la capture par les contextes. Si aucune capture n'a lieu, nous dérivons la transition d'émission à partir de la transition sans capture.

$$\frac{P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I}{P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} \widetilde{b} I} \text{CFREE}_{\leq}^k$$

Sinon, le contexte \mathbb{E}^* peut capturer les noms des messages locaux, provenant de passivation ou de kells.

$$\frac{P \vdash_{\tilde{a}, \xi, E, \mathbb{E}_1^* \{\mathbb{E}_2^*\}, \widetilde{P^*}, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I \quad d \in \tilde{b}}{P \vdash_{\tilde{a}, \xi, E, \mathbb{E}_1^* \{\nu d. \mathbb{E}_2^*\}, \widetilde{P^*}, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} \nu d. I} \text{CAPT}_{\leq}^k$$

En revanche, un contexte $\mathbb{K}^{c_{n_0}}$ ne peut capturer que les noms des messages de provenance c_{n_0} .

$$\frac{P \vdash_{\tilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}_1^{c_{n_0}} \{\mathbb{E}_2^{c_{n_0}} \{\widetilde{P^{c_{n_0}}}\}\}} \rightarrow_{\tilde{b}} I \quad d \in \tilde{b}}{P \vdash_{\tilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}_1^{c_{n_0}} \{\nu d. \mathbb{E}_2^{c_{n_0}} \{\widetilde{P^{c_{n_0}}}\}\}} \rightarrow_{\tilde{b}} \nu d. I} \text{CAPT}_{<}^k$$

Dans les deux cas, la portée de la restriction du nom capturé d est étendue pour englober l'entité réceptrice E .

Nous donnons maintenant les règles de dérivation pour le jugement inférieur de synchronisation partielle $P \vdash_{\leq, \theta} I$. Les règles sont semblables à celle de la synchronisation partielle en $\text{HO}\pi\text{J}$ (figure 6.4).

$$\begin{array}{c} \frac{P_2 \vdash_{\tilde{a}, \xi, P_1, \square, \emptyset, \emptyset} \rightarrow_{\tilde{b}} I}{P_1 \mid P_2 \vdash_{\leq, \theta} I} \text{SYNC}_{\leq}^k \quad \frac{P_1 \vdash_{\leq, \theta} I \quad P_2 \vdash_{\tilde{a}, \xi, I, \square, \emptyset, \emptyset} \rightarrow_{\tilde{b}} J}{P_1 \mid P_2 \vdash_{\leq, \theta} J} \text{SYNC-PAR}_{\leq}^k \\ \\ \frac{P \vdash_{\leq, \theta} I \quad a \notin n(I)}{\nu a. P \vdash_{\leq, \theta} \nu a. I} \text{SYNC-RESTR}_{\leq}^k \end{array}$$

Dans le cas de la composition parallèle $P_1 \mid P_2$, en supposant que le récepteur joint est dans P_1 , nous avons deux possibilités. Si P_1 ne nécessite aucune synchronisation, nous pouvons utiliser le jugement d'émission (règle SYNC_{\leq}^k) ; sinon, nous synchronisons partiellement P_1 , et le résultat de cette synchronisation \tilde{I} est utilisé comme récepteur par P_2 (règle SYNC-PAR_{\leq}^k). Nous avons également une règle pour la restriction (règle $\text{SYNC-RESTR}_{\leq}^k$).

6.2.5 Transitions supérieures

Nous définissons maintenant les transitions *supérieures* dans lesquelles les émetteurs sont au-dessus (dans la hiérarchie des localités) du récepteur. Nous définissons un jugement supérieur de synchronisation partielle $P \vdash_{>, \theta} I$, et un jugement d'émission supérieur $P \vdash_{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_{\tilde{b}} I$, dans lequel les processus P et $\widetilde{P^\uparrow}$ se synchronisent avec E . Informellement, ce jugement signifie que nous avons

$$E \mid \mathbb{E}^\uparrow \{P \mid \widetilde{P^\uparrow}\} \xrightarrow{\tau} I$$

par communication sur \tilde{a} . Le récepteur joint dans E doit être inclus dans un kell, et doit contenir uniquement des récepteurs étiquetés \uparrow .

Le jugement d'émission supérieur $P \vdash_{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_{\tilde{b}} I$ est construit en suivant les mêmes principes que pour son équivalent inférieur. Les règles sont données en figure 6.10, à l'exception du symétrique des règles $\text{PAR}_{>}^k$ et $\text{PAR-OUT}_{>}^k$. Comme précédemment, nous définissons un jugement annexe $P \vdash_{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_{\tilde{b}} I$ qui interdit la capture des noms \tilde{b} par le contexte \mathbb{E}^\uparrow . Dans le cas d'une émission de message (règles $\text{OUT}_{1, >}^k$ et $\text{OUT}_{2, >}^k$), nous vérifions que le récepteur joint est bien dans un kell grâce à la condition $\delta(I) = \square$. Hormis

Émission de message

$$\begin{array}{c}
\frac{E \xrightarrow{a^\dagger, P_1} I \quad \delta(I) = \square \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^\dagger) \cap \tilde{b} = \emptyset}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, \uparrow, E, \mathbb{E}^\dagger, \emptyset} \tilde{b} I \mid \mathbb{E}^\dagger \{P_2\}} \text{OUT}_{1,>}^k \\
\\
\frac{E \xrightarrow{a^\dagger, P_1} I \quad \delta(I) = \square \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^\dagger) \cap (\tilde{b} \cup \tilde{b}') = \emptyset \quad P' \xrightarrow{\tilde{a}', \uparrow, I, \mathbb{E}^\dagger \{\square \mid P_2\}, \tilde{P}^\dagger} \tilde{b}' I'}{P \xrightarrow{\tilde{a}' \uplus \bar{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger \uplus P'} \tilde{b} \cup \tilde{b}' I'} \text{OUT}_{2,>}^k
\end{array}$$

Congruence :

$$\begin{array}{c}
\frac{P_1 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger \{\square \mid P_2\}, \tilde{P}^\dagger} \tilde{b} P'}{P_1 \mid P_2 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} P'} \text{PAR}_{>}^k \quad \frac{P_1 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger \uplus P_2} \tilde{b} P'}{P_1 \mid P_2 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} P'} \text{PAR-OUT}_{>}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} P' \quad d \in \tilde{b} \quad d \notin \tilde{a}}{\nu d.P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^*, \tilde{P}^\dagger} \tilde{b} \setminus d \nu d.P'} \text{EXTR}_{>}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger \{\nu d, \square\}, \tilde{P}^\dagger} \tilde{b} P' \quad d \notin \tilde{b} \quad d \notin \tilde{a}}{\nu d.P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} P'} \text{RESTR}_{>}^k
\end{array}$$

Capture par les contextes :

$$\begin{array}{c}
\frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} P'}{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} P'} \text{CFREE}_{>}^k \quad \frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}_1^\dagger \{\mathbb{E}_2^\dagger\}, \tilde{P}^\dagger} \tilde{b} P' \quad d \in \tilde{b}}{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}_1^\dagger \{\nu d, \mathbb{E}_2^\dagger\}, \tilde{P}^\dagger} \tilde{b} \nu d.P'} \text{CAPT}_{>}^k
\end{array}$$

FIG. 6.10 – Jugement d'émission supérieure

$$\begin{array}{c}
\frac{P_1 \xrightarrow{\tilde{a}, \uparrow, P_2, \square, \emptyset} \tilde{b} I}{P_1 \mid P_2 \xrightarrow{>, \theta} I} \text{SYNC}_{>}^k \quad \frac{P_1 \xrightarrow{>, \theta} I \quad P_2 \xrightarrow{\tilde{a}, \uparrow, I, \square, \emptyset} \tilde{b} J}{P_1 \mid P_2 \xrightarrow{\leq, \theta} J} \text{SYNC-PAR}_{>}^k \\
\\
\frac{P \xrightarrow{>, \theta} I \quad a \notin n(I)}{\nu a.P \xrightarrow{>, \theta} \nu a.I} \text{SYNC-RESTR}_{>}^k \quad \frac{P_1 \xrightarrow{\leq, \theta} I \quad \eta(I) = \{\uparrow\}}{a[P_1]P_2 \xrightarrow{>, \theta} a[I]P_2} \text{SYNC-LOC}_{>}^k
\end{array}$$

FIG. 6.11 – Jugement supérieur de synchronisation partielle

ce point, les règles d'émission, de congruence et de capture sont semblables aux règles inférieures analogues.

Les règles du jugement supérieur de synchronisation partielle sont données en figure 6.11, à l'exception du symétrique des règles $\text{SYNC}_{>}^k$ et $\text{SYNC-PAR}_{>}^k$. En plus des règles $\text{SYNC}_{>}^k$, $\text{SYNC-PAR}_{>}^k$ et $\text{SYNC-RESTR}_{>}^k$, semblables aux règles correspondantes du jugement inférieur, nous avons une règle de congruence par rapport à la construction de kell $\text{SYNC-LOC}_{>}^k$. Dans ce cas, nous effectuons la synchronisation partielle à l'intérieur du kell, à l'aide du jugement inférieur de synchronisation partielle $P_1 \xrightarrow{\leq, \theta} I$, et nous vérifions que le résultat I n'attend que des messages supérieurs. Par exemple, nous avons

$$\bar{c}\langle d.\mathbf{0} \rangle \mathbf{0} \mid (b^\dagger(X) \mid c^*(Y)) \triangleright (X \mid Y) \xrightarrow{\leq, \theta} b^\dagger(X) \blacktriangleright_* X \mid d.\mathbf{0}$$

donc nous avons

$$a[\bar{c}\langle d.\mathbf{0} \rangle \mathbf{0} \mid (b^\dagger(X) \mid c^*(Y)) \triangleright (X \mid Y)] \mathbf{0} \xrightarrow{\geq, \theta} b^\dagger(X) \blacktriangleright_\square a[X \mid d.\mathbf{0}] \mathbf{0} \triangleq I$$

La réception partielle I obtenue peut être complétée à l'aide d'une émission supérieure.

6.2.6 Actions internes et jugements d'observation

Nous donnons en figure 6.12 les règles de déduction pour les jugements d'observation $P \xrightarrow{\lambda_k} P'$, à l'exception du symétrique des règles $\text{PAR}_{i\tau}^k$, HO_{\leq}^k , HO-SYNC_{\leq}^k , $\text{HO}_{>}^k$ et $\text{HO-SYNC}_{>}^k$. Les actions internes sont notées $P \xrightarrow{\tau} P'$, les réceptions $P \xrightarrow{\delta[a^\eta, \widetilde{R}]} P'$, et les émissions $P \xrightarrow{\widetilde{a}, \Xi, \mathbb{E}^\dagger\{\widetilde{P}^\dagger\}, \Delta, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} P'$. La méta-variable μ parcourt l'ensemble des étiquettes $\tau, \delta[a^\eta, \widetilde{R}]$, et nous définissons $n(\delta[a^\eta, \widetilde{R}]) \triangleq \widetilde{a}$. Le jugement $P \xrightarrow{\delta[a^\eta, \widetilde{R}]} P'$ signifie que P est capable de recevoir les processus \widetilde{R} sur \widetilde{a}^η pour évoluer vers P' ; δ indique la localisation du récepteur joint dans P . Comme pour $\text{HO}\pi\text{J}$, les réceptions $P \xrightarrow{\delta[a^\eta, \widetilde{R}]} P'$ ne sont pas utilisées dans la communication et sont définies uniquement pour l'observation. Les règles pour les actions internes et la réception sont classiques, sauf que nous avons quatre règles pour la communication d'ordre supérieur. Les règles HO_{\leq}^k et HO-SYNC_{\leq}^k traitent les synchronisations qui ne nécessitent que des messages inférieurs ou locaux, et les règles $\text{HO}_{>}^k$ et $\text{HO-SYNC}_{>}^k$ traitent les synchronisations qui impliquent des messages supérieurs. Dans le cas d'une communication, nous devons obtenir des réceptions partielles complètement instanciées $\mathbf{0} \blacktriangleright_\delta P'$.

Les transitions supérieures et inférieures ne permettent pas de construire tous les environnements de tests pour une émission : par exemple, nous ne pouvons pas tester le processus $\bar{a}\langle P_1 \rangle P_2$ avec un récepteur $a(X) \mid b^\dagger(Y) \triangleright Q$. C'est pourquoi nous définissons le jugement $P \xrightarrow{\widetilde{a}, \Xi, \mathbb{E}^\dagger\{\widetilde{P}^\dagger\}, \Delta, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n}\{\widetilde{P}^{c_n}\}} P'$ utilisé uniquement pour l'observation. La provenance des messages de P est indiquée par $\Xi \in \{\xi, \uparrow\}$. Le récepteur Q , en parallèle avec les émetteurs locaux et inférieurs, peut être placé dans un kell si nécessaire à l'aide du contexte $\Delta ::= \square \mid a[\square]P$. Par exemple, les processus $a(X) \mid b^\dagger(Y) \triangleright Q$ et $\bar{a}\langle P_1 \rangle P_2$ doivent être plongés dans un kell avant de pouvoir interagir avec un émetteur sur b . Ainsi avec $\Xi = *$, le jugement d'émission signifie que nous avons

$$\mathbb{E}^\dagger\{\prod \widetilde{P}^\dagger\} \mid \Delta\{Q \mid \mathbb{E}^*\{P \mid \prod \widetilde{P}^* \mid \prod_{c_n} \mathbb{K}^{c_n}\{\prod \widetilde{P}^{c_n}\}\}\} \xrightarrow{\tau} P'$$

par communication sur \widetilde{a} . Le jugement d'émission est défini à partir des émissions inférieures et supérieures, en considérant tous les cas possibles pour Ξ .

$$\begin{array}{c}
\frac{\pi = \prod \widetilde{a^\eta(X)}}{\pi \triangleright P \xrightarrow{*[a^\eta, R]} P\{\widetilde{R}/\widetilde{X}\}} \text{IN}_i^k \qquad \frac{P_1 \xrightarrow{\mu} P'_1}{P_1 \mid P_2 \xrightarrow{\mu} P'_1 \mid P_2} \text{PAR}_{i\tau}^k \\
\\
\frac{P \xrightarrow{\mu} P' \quad a \notin n(\mu)}{\nu a. P \xrightarrow{\mu} \nu a. P'} \text{RESTR}_{i\tau}^k \qquad \frac{P \xrightarrow{\tau} P'}{a[P]Q \xrightarrow{\tau} a[P']Q} \text{LOC}_\tau^k \\
\\
\frac{P \xrightarrow{*[a^\eta, R]} P'}{b[P]Q \xrightarrow{[a^\eta, R]} b[P']Q} \text{LOC}_i^k \qquad \frac{P_2 \xrightarrow{\widetilde{a}, \xi, P_1, \square, \emptyset, \emptyset} \widetilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO}_{\leq}^k \\
\\
\frac{P_1 \xrightarrow{\leq, \theta} I \quad P_2 \xrightarrow{\widetilde{a}, \xi, I, \square, \emptyset, \emptyset} \widetilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO-SYNC}_{\leq}^k \qquad \frac{P_2 \xrightarrow{\widetilde{a}, \uparrow, P_1, \square, \emptyset, \emptyset} \widetilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO}_{>}^k \\
\\
\frac{P_1 \xrightarrow{>, \theta} I \quad P_2 \xrightarrow{\widetilde{a}, \uparrow, I, \square, \emptyset} \widetilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO-SYNC}_{>}^k \\
\\
\frac{P \xrightarrow{\widetilde{a}, \xi, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}} \widetilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P \xrightarrow{\widetilde{a}, \xi, \emptyset, \square, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}} \widetilde{b} P'} \text{OUT-OBS}_{1, \leq}^k \\
\\
\frac{P \xrightarrow{\widetilde{a}, \xi, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}} \widetilde{b} I \quad P_2 \xrightarrow{\widetilde{a}', \uparrow, \Delta\{I\}, \mathbb{E}^\uparrow, \widetilde{P}^\uparrow} \widetilde{b'} \mathbf{0} \blacktriangleright_\delta P'}{P \xrightarrow{\widetilde{a}, \xi, \mathbb{E}^\uparrow\{\widetilde{P}^\uparrow \uplus P_2\}, \Delta, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}} \widetilde{b} P'} \text{OUT-OBS}_{2, \leq}^k \\
\\
\frac{P \xrightarrow{\widetilde{a}, \uparrow, \Delta\{Q\} \mathbb{E}^*\{\prod \widetilde{P}^* \mid \prod_{cn} \mathbb{K}^{cn}\{\prod \widetilde{P}^{cn}\}\}, \mathbb{E}^\uparrow, \widetilde{P}^\uparrow} \widetilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P \xrightarrow{\widetilde{a}, \uparrow, \mathbb{E}^\uparrow\{\widetilde{P}^\uparrow\}, \Delta, Q, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}} \widetilde{b} P'} \text{OUT-OBS}_{>}^k
\end{array}$$

FIG. 6.12 – Système de transitions étiquetées pour l'observation

Remarque 6.2. Nous pouvons définir le jugement général d'émission

$$P \xrightarrow[\text{b}]{\widetilde{a}, \Xi, \mathbb{E}^\dagger \{\widetilde{P^\dagger}\}, \Delta, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}} P'$$

directement, sans définir de jugements d'émission inférieure ou supérieure. Cependant, écrire les règles pour ce jugement revient à combiner les règles des émissions inférieure et supérieure ; les règles ainsi obtenues sont très difficiles à lire.

6.2.7 Bisimilarité à complément

Comme il existe déjà un résultat de congruence (et de complétude) dans le cas fort [47], nous cherchons à établir un résultat de correction pour les relations faibles uniquement. Nous définissons les transitions faibles $\xrightarrow{\lambda_k}$ de la manière suivante : nous notons $\xrightarrow{\tau}$ la clôture réflexive et transitive de $\xrightarrow{\tau}$, $\xrightarrow[\text{b}]{\delta[a^\eta, R]}$ pour $\xrightarrow{\tau} \xrightarrow[\text{b}]{\delta[a^\eta, R]} \xrightarrow{\tau}$, et $\xrightarrow[\text{b}]{\widetilde{a}, \Xi, \mathbb{E}^\dagger \{\widetilde{P^\dagger}\}, \Delta, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}}$ pour

$$\xrightarrow{\tau} \xrightarrow[\text{b}]{\widetilde{a}, \Xi, \mathbb{E}^\dagger \{\widetilde{P'^\dagger}\}, \Delta, Q', \mathbb{E}^*, \widetilde{P'^*}, \mathbb{K}^{cn} \{\widetilde{P'^{cn}}\}} \xrightarrow{\tau}$$

avec $Q \xrightarrow{\tau} Q'$, $P_i^\dagger \xrightarrow{\tau} P_i'^\dagger$ pour tout $P_i^\dagger \in \widetilde{P^\dagger}$, $P_i^* \xrightarrow{\tau} P_i'^*$ pour tout $P_i^* \in \widetilde{P^*}$, et $P_i^{cn} \xrightarrow{\tau} P_i'^{cn}$ pour tout $P_i^{cn} \in \cup_{cn} \widetilde{P^{cn}}$. En nous restreignant aux étiquettes pour l'observation, la définition de la bisimilarité faible à complément est la suivante.

Définition 6.3. Une relation \mathcal{R} sur les termes clos est une simulation faible à complément ssi $P \mathcal{R} Q$ implique $fn(P) = fn(Q)$ et pour tout $P \xrightarrow{\lambda_k} P'$, alors il existe Q' tel que $Q \xrightarrow{\lambda_k} Q'$ et $P' \mathcal{R} Q'$.

Une relation \mathcal{R} est une bisimulation faible à complément ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations faibles à complément. La bisimilarité faible à complément \approx_m est la plus grande bisimulation faible à complément.

Comme pour $\text{HO}\pi\text{J}$, la méthode de Howe ne permet pas de prouver la congruence de cette relation ; nous devons inclure les réceptions partielles à la définition, ainsi que certains jugements intermédiaires. Nous définissons les transitions faibles $\xrightarrow[\text{b}]{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}}$ et $\xrightarrow[\text{b}]{\widetilde{a}, \uparrow, E, \mathbb{E}^\dagger, \widetilde{P^\dagger}}$ selon le même principe que $\xrightarrow[\text{b}]{\widetilde{a}, \Xi, \mathbb{E}^\dagger \{\widetilde{P^\dagger}\}, \Delta, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}}$.

Définition 6.4. Une relation \mathcal{R} sur les termes clos est une simulation faible à complément sur les réceptions partielles ssi $P \mathcal{R} Q$ implique $fn(P) = fn(Q)$ et :

- pour tout $P \xrightarrow{\lambda_k} P'$, il existe Q' tel que $Q \xrightarrow{\lambda_k} Q'$ et $P' \mathcal{R} Q'$;
- pour tout $P \xrightarrow{a^\eta, R} I$, il existe I' telle que $Q \xrightarrow{\tau} \xrightarrow{a^\eta, R} I'$ et $I \mathcal{R} I'$;
- pour tout $P \xrightarrow{\leq, \theta} I$, il existe I' telle que $Q \xrightarrow{\tau} \xrightarrow{\leq, \theta} I'$ et $I \mathcal{R} I'$;
- pour tout $P \xrightarrow{>, \theta} I$, il existe I' telle que $Q \xrightarrow{\tau} \xrightarrow{>, \theta} I'$ et $I \mathcal{R} I'$;
- pour tout $P \xrightarrow[\text{b}]{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}} I$, il existe une réception partielle I' telle que $Q \xrightarrow[\text{b}]{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}} I'$ et $I \mathcal{R} I'$;
- pour tout $P \xrightarrow[\text{b}]{\widetilde{a}, \uparrow, E, \mathbb{E}^\dagger, \widetilde{P^\dagger}} I$, il existe I' tel que $Q \xrightarrow[\text{b}]{\widetilde{a}, \uparrow, E, \mathbb{E}^\dagger, \widetilde{P^\dagger}} I'$ et $I \mathcal{R} I'$.

Nous avons $\pi \triangleright_\delta P \mathcal{R} \pi' \triangleright_{\delta'} Q$ ssi $\pi = \pi'$, $\delta = \delta'$ et pour tout substitution σ qui clos P et Q , nous avons $P\sigma \mathcal{R} Q\sigma$.

Une relation \mathcal{R} est une bisimulation faible à complément sur les réceptions partielles ssi \mathcal{R} et \mathcal{R}^{-1} sont des simulations faibles sur les réceptions partielles. La bisimilarité faible à complément sur les réceptions partielles \approx_{pi} est la plus grande bisimulation de ce type.

Comme les réceptions partielles I ne peuvent effectuer de τ -actions, les transitions faibles qui génèrent de telles réceptions (comme $Q \xRightarrow{\tau, \leq, \theta} I$) sont écrites dans le style semi-faible.

Théorème 6.2. *La relation \approx_{pi} est une congruence.*

La preuve, donnée en appendice A.5 suit le même schéma que celle de $\text{HO}\pi\text{J}$, en intégrant des résultats similaires à ceux de $\text{HO}\pi\text{P}$ sur les contextes apparaissant dans les étiquettes.

Par définition, nous avons $\approx_{pi} \subseteq \approx_m$; nous allons maintenant montrer que cette inclusion est stricte, et que la relation \approx_{pi} est trop discriminante. Pour cela, nous supposons qu'un opérateur de choix indéterminé $+$ est ajouté au calcul, et nous définissons les processus suivants :

$$\begin{aligned} P_1 &\triangleq a(X) \mid a(Y) \triangleright \nu bc.b[c[X \mid Y \mid \bar{c}\langle e^\uparrow \rangle \mathbf{0}]] \\ P_2 &\triangleq a(X) \mid a(Y) \triangleright \nu bc.b[c[X \mid Y \mid \bar{c}\langle e^\uparrow \rangle \mathbf{0} \mid c(Z) \triangleright \mathbf{0}] \mid d^\uparrow] \\ P &\triangleq P_1 + P_2 \\ Q &\triangleq P + (a(X) \mid a(Y) \triangleright \nu bc.b[c[X \mid Y] \mid e^\downarrow(Z) \triangleright d^\uparrow]) \end{aligned}$$

Pour plus de lisibilité, nous avons omis les continuations $\mathbf{0}$ des kells b, c , et nous notons d^\uparrow le processus $d^\uparrow(X) \triangleright \mathbf{0}$. Le contexte $\nu bc.b[c[\square]]$ agit comme un pare-feu : comme les messages ne peuvent traverser deux frontières de kell, aucune communication n'est permise entre le contenu de c et l'extérieur de b . De même le contexte $\nu bc.b[c[\square] \mid d^\uparrow]$ peut uniquement recevoir un message émis sur d à l'extérieur de b . Enfin, le contexte $\nu bc.b[c[\square] \mid e^\downarrow(Z) \triangleright d^\uparrow]$ est capable de recevoir sur d si et seulement si le contenu de c est capable d'émettre sur e . Les processus $\bar{c}\langle e^\uparrow \rangle \mathbf{0}$ et $\bar{c}\langle e^\uparrow \rangle \mathbf{0} \mid c(Z) \triangleright \mathbf{0}$ ont été ajoutés à P_1 et P_2 pour égaliser les noms libres de P et Q ; plus de détails sont donnés dans la remarque 6.3.

Nous montrons d'abord que nous avons $P \approx_m Q$; en particulier nous montrons que P peut répondre à la transition

$$Q \xRightarrow{*[a^*, R_1; a^*, R_2]} \nu bc.b[c[R_1 \mid R_2] \mid e^\downarrow(Z) \triangleright d^\uparrow] \triangleq Q'.$$

Si $R_1 \mid R_2$ peut émettre faiblement sur e , alors Q' peut (faiblement) recevoir sur d ; dans ce cas, P peut répondre par une transition

$$P \xRightarrow{*[a^*, R_1; a^*, R_2]} \nu bc.b[c[R'_1 \mid R'_2 \mid \bar{c}\langle e^\uparrow \rangle \mathbf{0} \mid c(Z) \triangleright \mathbf{0}] \mid d^\uparrow] \triangleq P'_2$$

avec $R_1 \mid R_2 \xRightarrow{\tau} R'_1 \mid R'_2$. Si $R_1 \mid R_2$ ne peut pas émettre faiblement sur e , alors Q' ne peut pas recevoir sur d ; dans ce cas P répond par une transition

$$P \xRightarrow{*[a^*, R_1; a^*, R_2]} \nu bc.b[c[R'_1 \mid R'_2 \mid \bar{c}\langle e^\uparrow \rangle \mathbf{0}]] \triangleq P'_1$$

avec $R_1 \mid R_2 \xRightarrow{\tau} R'_1 \mid R'_2$.

Remarque 6.3. *Si $R_1 \mid R_2$ peut émettre faiblement sur e , P répond par P'_2 , qui contient le processus $\bar{c}\langle e^\uparrow \rangle \mathbf{0} \mid c(Z) \triangleright \mathbf{0}$. Ce processus permet d'égaliser les noms libres de Q' et P'_2 . Le nom e peut disparaître de Q' dans la communication sur e avec $R_1 \mid R_2$; le processus P' peut également faire disparaître son occurrence de e en déclenchant la communication sur c .*

Si $R_1 \mid R_2$ ne peut pas émettre faiblement sur e , P répond par P'_1 , qui contient le processus $\bar{c}\langle e^\uparrow \rangle \mathbf{0}$. Comme la synchronisation sur e dans Q' ne peut pas avoir lieu, le nom e sera toujours libre dans Q' . De même, le processus $\bar{c}\langle e^\uparrow \rangle \mathbf{0}$ ne peut pas réagir dans P'_1 , le nom e sera donc toujours libre dans P'_1 .

En revanche nous avons $P \not\approx_{pi} Q$. Pour un processus R_1 qui ne peut pas émettre faiblement sur e , nous considérons

$$Q \xrightarrow{a^*, R_1} a(Y) \blacktriangleright_* \nu bc.b[c[R_1 \mid Y] \mid e^\downarrow(Z) \triangleright d^\uparrow] \triangleq I.$$

Si P répond par $P \xRightarrow{\tau} \xrightarrow{a^*, R_1} a(Y) \blacktriangleright_* \nu bc.b[c[R_1 \mid Y \mid \bar{c}(e^\uparrow)\mathbf{0}]] \triangleq J$, alors I et J sont distinguées par la substitution $\sigma \triangleq Y \mapsto \bar{c}(\mathbf{0})\mathbf{0}$: le processus $I\sigma$ est capable de recevoir sur d , ce qui n'est pas le cas de $J\sigma$. Si P répond par

$$P \xRightarrow{\tau} \xrightarrow{a^*, R_1} a(Y) \blacktriangleright_* \nu bc.b[c[R_1 \mid Y \mid \bar{c}(e^\uparrow)\mathbf{0} \mid c(Z) \triangleright \mathbf{0}] \mid e^\downarrow(Z) \triangleright d^\uparrow] \triangleq J'$$

alors I et J' sont distinguées par la substitution $\sigma \triangleq Y \mapsto \mathbf{0}$: $J'\sigma$ est capable de recevoir sur d , ce qui n'est pas le cas de $I\sigma$. Le processus P ne peut donc pas répondre à la réception partielle de Q . En outre, P et Q ne peuvent être distingués par un contexte, la relation \approx_{pi} n'est donc pas complète.

6.3 Conclusions

La définition d'une sémantique à complément est problématique pour les calculs avec récepteurs joints, tels que le Kell. La solution décrite dans ce chapitre repose sur les réceptions partielles I , qui sont instanciées au fur et à mesure de la découverte des messages lors d'une transition d'émission. De cette manière, nous pouvons définir une sémantique à complément et prouver la congruence d'une bisimilarité précoce faible \approx_{pi} pour le Kell, obtenant ainsi un résultat inédit de correction dans le cas faible pour ce calcul. Cependant la relation ainsi définie n'est pas entièrement satisfaisante : comme l'illustre le contre-exemple donné en section 6.2.7, la bisimilarité \approx_{pi} est trop discriminante.

Ce résultat en demi-teinte soulève plusieurs questions. En premier lieu, on peut se demander quelle équivalence, entre \approx_{pi} et une bisimilarité semi-faible semi-précoce semblable à celle définie pour Homer [14], est la plus intéressante, c'est-à-dire laquelle met en relation le plus grand nombre de processus. En outre, on peut se demander si la nécessité de considérer \approx_{pi} est une conséquence liée à la sémantique à complément ou à la méthode de Howe elle-même. La première possibilité signifie simplement que la sémantique à complément n'est pas adaptée aux calculs avec récepteurs joints, et qu'il est peut-être possible d'utiliser la méthode de Howe avec une autre sémantique. Par exemple, nous pensons qu'il est possible définir une relation semblable à la bisimilarité à complément tout en conservant une sémantique contextuelle ; plus de détails sur cette piste de recherche sont donnés dans le chapitre de conclusion. La seconde hypothèse suggère que quelle que soit la sémantique considérée, la preuve de Howe ne peut être menée qu'avec une bisimilarité qui prend en compte les réceptions partiellement instanciées. Dans ce cas, la méthode de Howe elle-même n'est pas adaptée aux calculs avec récepteurs joints.

Chapitre 7

Conclusions et perspectives

Notre travail sur les bisimilarités dans les calculs avec passivation a porté sur la définition de ces relations et la preuve de leur correction. Nous avons d'abord cherché à simplifier les définitions de bisimilarités contextuelles proposées pour Homer et le Kell. Nous avons montré qu'il est possible de définir une bisimilarité normale qui caractérise la congruence barbue dans HOP, un calcul avec passivation mais dépourvu de restriction. Dans $\text{HO}\pi$ [42], la bisimilarité normale provient d'un encodage de la communication d'ordre supérieur dans un calcul du premier ordre, qui n'est plus valable dans les calculs avec passivation. La bisimilarité normale de HOP dépend d'un processus $\overline{m}.n.0$ qui permet d'observer les localités au sein d'une fonction et d'en déduire une décomposition de deux fonctions équivalentes en sous-processus bisimilaires. Nous nous demandons s'il est possible d'aller encore plus loin, en donnant une axiomatisation de la congruence barbue en HOP. Une piste intéressante pour répondre à cette question est d'étendre les résultats de Lanese et coll. sur l'axiomatisation de la congruence barbue en HOCore [23] à un calcul minimal avec passivation.

Il n'est malheureusement pas possible d'étendre la définition de bisimilarité normale de HOP aux calculs avec passivation et restriction. La restriction peut masquer des localités qui ne peuvent être détectées avec notre processus $\overline{m}.n.0$. En outre, la position des restrictions dans la hiérarchie de localités a une grande influence sur le comportement des processus, notamment à cause de l'extension de portée hors des localités. Concrètement, nous avons donné plusieurs contre-exemples en $\text{HO}\pi\text{P}$ qui montrent que tester de larges classes de processus (les processus sans réception, et les processus finis) ne permettent pas de garantir l'équivalence de fonctions. Nous conjecturons qu'il n'existe pas de caractérisation de la congruence barbue de $\text{HO}\pi\text{P}$ (et, plus largement, des calculs avec passivation et restriction) qui teste moins de contextes que la bisimilarité contextuelle.

Dans notre analyse des preuves de correction, nous avons constaté que la méthode de Howe échouait avec les bisimilarités contextuelles précoces à cause de l'interdépendance entre les clauses d'émission et de réception. Pour casser cette dépendance, nous avons défini un système de transitions, dans lequel les émissions dépendent non pas d'une fonction, mais d'un processus qui peut se réduire vers une fonction qui n'est elle-même pas explicitement mentionnée dans la transition. Cette modification assouplit le caractère précoce de la bisimilarité associée et permet l'utilisation de la méthode de Howe pour prouver la congruence. Notre méthode est applicable dans le cas fort comme dans le cas faible, sans avoir recours à une définition de relation semi-faible.

Nous avons défini une sémantique à complément pour $\text{HO}\pi$, $\text{HO}\pi\text{P}$, et le Kell (ainsi que pour le Seal dans [26]). Dans $\text{HO}\pi$, la bisimilarité à complément est correcte et complète (sur les processus à image finie dans le cas faible), et coïncide avec la bisimilarité contextuelle précoce. Dans $\text{HO}\pi\text{P}$, nous avons obtenu des résultats identiques, excepté l'égalité entre les deux formes de bisimilarité. En effet, la sémantique à complément mentionne un observable additionnel, les noms dont la portée peut être étendue, ce qui rend difficile la

comparaison entre les deux relations. Si nous avons pu faire coïncider les bisimilarités fortes (cf. remarque 5.2), nous avons montré uniquement l'inclusion de la relation contextuelle dans celle à complément dans le cas faible ; nous conjecturons que l'inclusion réciproque est vraie.

Les récepteurs joints du Kell compliquent la définition d'une sémantique à complément ; dans une transition d'émission, nous devons considérer un processus récepteur, ainsi que d'autres processus émetteurs pour compléter le récepteur joint. Nous avons proposé une sémantique dans laquelle les récepteurs joints sont instanciés progressivement, au fur et à mesure de la découverte des messages. Pour que la méthode de Howe puisse s'appliquer, nous devons considérer une bisimilarité qui prend en compte ces instanciations partielles. La relation que nous avons obtenue est correcte (dans les cas fort et faible), mais elle n'est pas complète : nous avons donné un contre-exemple qui prouve qu'elle est trop discriminante. En effet, les réceptions partielles ne correspondent pas à une interaction entre le processus testé et son environnement ; seules les réceptions totalement instanciées sont pertinentes. Nous pensons néanmoins qu'il est possible de définir une bisimilarité à complément correcte et complète dans un Kell sans récepteurs joints ou dans Homer.

L'étape cruciale dans la définition d'une sémantique à complément est la définition du système de transitions, notamment les règles pour l'émission. Si les règles respectent certaines contraintes, la preuve de congruence de la bisimilarité à complément ne pose pas de problème. Dans un travail futur, nous souhaitons expliciter ces contraintes, pour faciliter la définition d'une sémantique à complément dans un calcul quelconque. Par exemple, il n'est pas possible d'utiliser des règles définies modulo congruence structurelle, semblables à la règle CONGR de $\text{HO}\pi\text{J}$ (figure 6.1). Dans les preuves par induction sur $P \mathcal{R}^\bullet Q$, le cas $P = \text{op}(\tilde{P}_i)$, $Q = \text{op}(\tilde{Q}_i)$ avec $\tilde{P}_i \mathcal{R}^\bullet \tilde{Q}_i$ se traite grâce à la décomposition en sous-termes reliés par la clôture de Howe ; cette décomposition n'est plus possible si les règles sont définies modulo congruence structurelle. De même, la règle classique pour la réplication

$$\frac{P \mid !P \xrightarrow{\alpha} A}{!P \xrightarrow{\alpha} A}$$

fait échouer les preuves par induction, car le processus $P \mid !P$ à l'origine de la transition de la prémisse n'est pas un sous-terme de $!P$. Identifier l'ensemble de ces contraintes peut mener à la création d'un format de règles qui garantirait la congruence de la bisimilarité à complément associée, semblable aux formats d'ordre supérieur Higher-Order et Promoted PANTH [37].

Une autre piste de recherche est de transposer la bisimilarité à complément dans une sémantique contextuelle. Nous avons vu avec le Kell que la bisimilarité associée au système de transitions à complément n'est pas toujours complète. Nous cherchons à régler ce problème en revenant à la sémantique contextuelle. Dans la bisimilarité à complément, la clause d'émission dépend d'un processus qui peut recevoir le message. Pour une bisimilarité contextuelle, cela revient à considérer la clause suivante.

- Si $P \xrightarrow{\bar{a}} C$, alors pour tout processus R , il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et pour toute fonction F telle que $R \xrightarrow{a} F$, nous avons $F \bullet C \mathcal{R} F \bullet C'$.

La réponse C' de Q dépend bien de R et non de F . Nous pensons qu'il est possible de prouver la congruence d'une telle bisimilarité grâce à la méthode de Howe, en prouvant le résultat de pseudo-simulation suivant :

- Si $P \xrightarrow{\bar{a}} C$, alors pour tout $R \mathcal{R}^\bullet R'$, il existe C' telle que $Q \xrightarrow{\bar{a}} C'$ et pour toute fonction F telle que $R \xrightarrow{a} F$, il existe F' telle que $R' \xrightarrow{a} F'$ et $F \bullet C \mathcal{R}^\bullet F' \bullet C'$.

Si notre intuition s'avère exacte, cela permettrait d'appliquer la méthode de Howe directement avec une bisimilarité contextuelle. Nous espérons prouver de cette manière la congruence de la bisimilarité contextuelle faible du Kell définie dans [47].

Enfin nous comptons explorer de nouvelles pistes pour étudier la théorie comportementale des calculs avec passivation. En particulier nous voulons étudier l'existence d'un modèle coalgébrique pour les calculs avec passivation. Il existe une notion de bisimilarité

naturelle associée à une coalgèbre ; il serait intéressant de comparer cette notion aux bisimilarités contextuelles et à complément. Ce travail a déjà été mené notamment pour les Ambients [17].

Bibliographie

- [1] R. M. Amadio, G. Boudol, and Cédric Lhoussaine. The receptive distributed pi-calculus, 1999.
- [2] M. Baldamus. *Semantics and Logic of Higher-Order Processes : Characterizing Late Context Bisimulation*. PhD thesis, Berlin University of Technology, 1998.
- [3] M. Baldamus and T. Frauenstein. Congruence proofs for weak bisimulation equivalences on higher-order process calculi. Technical report, Berlin University of Technology, 1995.
- [4] K. L. Bernstein. A congruence theorem for structured operational semantics of higher-order languages. In *LICS '98*, pages 153–164. IEEE Computer Society Press, 1997.
- [5] F. Bonchi, F. Gadducci, and G.V. Monreale. Reactive systems, barbed semantics, and the mobile ambients. In *FOSSACS '09*, pages 272–287. Springer, 2009.
- [6] E. Bruneton, T. Coupaye, M. Leclercq, V. Quéma, and J-B. Stefani. An open component model and its support in Java. In *CBSE '04*, volume 3054 of *LNCS*, pages 7–22. Springer, 2004.
- [7] M. Bugliesi and G. Castagna. Secure safe ambients. In *POPL '01*, pages 222–235. ACM Press, 2001.
- [8] M. Bugliesi, S. Crafa, M. Merro, and V. Sassone. Communication and mobility control in boxed ambients. *Information and Computation*, 202, 2005.
- [9] Z. Cao. More on bisimulations for higher order pi-calculus. In *FoSSaCS '06*, volume 3921 of *LNCS*, pages 63–78. Springer, 2006.
- [10] L. Cardelli and A. D. Gordon. Mobile ambients. In *FoSSaCS '98*, volume 1378 of *LNCS*, pages 140–155. Springer, 1998.
- [11] G. Castagna and F. Zappa Nardelli. The seal calculus revisited : Contextual equivalence and bisimilarity. In *FSTTCS '02*, volume 2556 of *LNCS*, pages 85–96. Springer, 2002.
- [12] G. Castagna, J. Vitek, and F. Zappa Nardelli. The Seal Calculus. *Information and Computation*, 201(1) :1–54, 2005.
- [13] Cedric Fournet and Georges Gonthier. The join calculus : A language for distributed mobile programming. In *Applied Semantics Summer School*, pages 268–332. Springer-Verlag, 2000.
- [14] J. C. Godskesen and T. 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.
- [15] A. D. Gordon. Bisimilarity as a theory of functional programming. Mini-course. Notes Series NS-95-3, BRICS, University of Cambridge Computer Laboratory, July 1995. iv+59 pp.
- [16] J.F. Groote. Transition system specifications with negative premises. *Theoretical Computer Science*, 118(2) :263–299, 1993.
- [17] D. Hausmann, T. Mossakowski, and L. Schröder. A coalgebraic approach to the semantics of the ambient calculus. *Theoretical Computer Science*, 366(1) :121–143, 2006.

- [18] Matthew Hennessy and James Riely. Resource access control in systems of mobile agents. *Information and Computation*, 173 :2002, 1998.
- [19] T. Hildebrandt, J. C. Godskesen, and M. Bundgaard. Bisimulation congruences for Homer — a calculus of higher order mobile embedded resources. Technical Report ITU-TR-2004-52, IT University of Copenhagen, 2004.
- [20] D. J. Howe. Proving congruence of bisimulation in functional programming languages. *Information and Computation*, 124(2) :103–112, 1996.
- [21] A. Jeffrey and J. Rathke. A theory of bisimulation for a fragment of concurrent ML with local names. *Theoretical Computer Science*, 323 :1–48, 2004.
- [22] A. Jeffrey and J. Rathke. Contextual equivalence for higher-order pi-calculus revisited. *Logical Methods in Computer Science*, 1(1), 2005.
- [23] I. Lanese, J. A. Pérez, D. Sangiorgi, and A. Schmitt. On the expressiveness and decidability of higher-order process calculi. In *LICS*, 2008. To appear.
- [24] J. J. Leifer and R. Milner. Deriving bisimulation congruences for reactive systems. In *CONCUR '00*, volume 1877 of *Lecture Notes in Computer Science*, pages 243–258. Springer, 2000.
- [25] S. Lenglet, A. Schmitt, and J.-B. Stefani. Normal bisimulations in process calculi with passivation. Technical Report RR 6664, INRIA, 2008.
- [26] S. Lenglet, A. Schmitt, and J.B. Stefani. Howe’s method for early bisimilarities. Technical Report RR 6773, INRIA, 2008.
- [27] S. Lenglet, A. Schmitt, and J.-B. Stefani. Howe’s method in calculi with passivation. In *CONCUR '09*, volume 5710 of *LNCS*, pages 448–462. Springer, 2009.
- [28] S. Lenglet, A. Schmitt, and J.-B. Stefani. Normal bisimulations in process calculi with passivation. In *FoSSaCS '09*, volume 5504 of *LNCS*, pages 257–271. Springer, 2009.
- [29] F. Levi and D. Sangiorgi. Mobile safe ambients. *ACM Trans. Program. Lang. Syst.*, 25(1) :1–69, 2003.
- [30] Y. Li. Contextual labelled semantics for higher-order process calculi. In *FGUC '04*, volume 138 of *EN TCS*, pages 61–77, 2005.
- [31] Y. Li and X. Liu. Towards a theory of bisimulation for the higher-order process calculi. *Journal of Computer Science and Technology*, 19(3) :352–363, 2004.
- [32] M. Merro and F. Zappa Nardelli. Behavioral theory for mobile ambients. *Journal of the ACM*, 52(6) :961–1023, 2005.
- [33] R. Milner. *A Calculus of Communicating Systems*, volume 92. Springer, 1980.
- [34] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, i. *Information and Computation*, 100(1) :1–40, 1992.
- [35] R. Milner and D. Sangiorgi. Barbed bisimulation. In *ICALP '92*, volume 623 of *LNCS*. Springer, 1992.
- [36] R. Milner and D. Sangiorgi. Techniques of weak bisimulation up-to. In *CONCUR '92*, volume 630 of *LNCS*, 1992.
- [37] M. Mousavi, M. J. Gabbay, and M. A. Reniers. Sos for higher order processes (extended abstract). In *CONCUR'05*, volume 3653 of *LNCS*, pages 308–322. Springer, 2005.
- [38] D. Pous. Up-to techniques for weak bisimulation. In *ICALP '05*, volume 3580 of *LNCS*, pages 730–741. Springer, 2005.
- [39] J. Rathke and P. Sobocinski. Deconstructing behavioural theories of mobility. In *IFIP TCS '08*, volume 273 of *IFIP*, pages 507–520. Springer, 2008.
- [40] J. Rathke and P. Sobocinski. Deriving structural labelled transitions for mobile ambients. In *CONCUR '08*, volume 5201 of *LNCS*, pages 462–476. Springer, 2008.

- [41] D. Sangiorgi. *Expressing Mobility in Process Algebras : First-Order and Higher-Order Paradigms*. PhD thesis, Department of Computer Science, University of Edinburgh, 1992.
- [42] D. Sangiorgi. Bisimulation for higher-order process calculi. *Information and Computation*, 131(2) :141–178, 1996.
- [43] D. Sangiorgi. On the bisimulation proof method. *Mathematical Structures in Computer Science*, 8(5) :447–479, 1998.
- [44] D. Sangiorgi, N. Kobayashi, and E. Sumii. Environmental bisimulations for higher-order languages. In *LICS '07*, pages 293–302. IEEE Computer Society, 2007.
- [45] D. Sangiorgi and D. Walker. *The Pi-Calculus : A Theory of Mobile Processes*. Cambridge University Press, 2001.
- [46] A. Schmitt and J.-B. Stefani. The m-calculus : A higher-order distributed process calculus. In *POPL '03*, pages 50–61, New Orleans, LA, USA, January 2003.
- [47] A. Schmitt and J.-B. Stefani. The Kell Calculus : A Family of Higher-Order Distributed Process Calculi. In *Global Computing 2004 workshop*, volume 3267 of *LNCS*, 2004.
- [48] P. Sewell, J. Leifer, K. Wansbrough, F. Zappa Nardelli, M. Allen-Williams, P. Habouzit, and V. Vafeiadis. Acute : High-level programming language design for distributed computation. *Journal of Functional Programming*, 17(4-5), 2007.
- [49] E. Sumii. A theory of non-monotone memory (or : Contexts for free). In *ESOP '09*, volume 5502 of *LNCS*, pages 237–251. Springer, 2009.
- [50] E. Sumii and B.C. Pierce. A bisimulation for type abstraction and recursion. *SIGPLAN Not.*, 40(1) :63–74, 2005.
- [51] B. Thomsen. A calculus of higher order communicating systems. In *POPL '89*, pages 143–154. ACM, 1989.
- [52] B. Thomsen. Plain chocs : A second generation calculus for higher order processes. *Acta Informatica*, 30(1) :1–59, 1993.
- [53] C. Verhoef. A congruence theorem for structured operational semantics with predicates and negative premises. *Nordic Journal of Computing*, 2(2) :274–302, 1995.
- [54] J. Vitek and G. 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.
- [55] S. Dal Zilio. Mobile processes : a commented bibliography. In *Modeling and verification of parallel processes*, volume 2067 of *LNCS*, pages 206–222. Springer, 2001.

Annexe A

Sémantique à complément

Nous regroupons dans cette section les preuves de congruence des bisimulations à compléments des différents calculs.

A.1 Résultats généraux sur la méthode de Howe

Nous prouvons ici des propriétés de la méthode de Howe qui ne dépendent pas des calculs ou des bisimilarités considérés. Les deux premiers résultats sont classiques pour la relation de Howe.

Lemme A.1. *Pour tout relation réflexive \mathcal{R} , la relation \mathcal{R}^\bullet est réflexive.*

Démonstration. Pour tout P , on a $P \mathcal{R} P$, donc $P \mathcal{R}^\circ P$, donc $P \mathcal{R}^\bullet P$. \square

Lemme A.2. *Pour toute relation \mathcal{R} , $P \mathcal{R}^\bullet Q$ et $R \mathcal{R}^\bullet S$ impliquent $P\{R/X\} \mathcal{R}^\bullet Q\{S/X\}$.*

Démonstration. Par induction sur la preuve de $P \mathcal{R}^\bullet Q$.

Supposons $P \mathcal{R}^\circ Q$. La relation $R \mathcal{R}^\bullet S$ et la congruence de \mathcal{R}^\bullet impliquent $P\{R/X\} \mathcal{R}^\bullet P\{S/X\}$. Soit σ une substitution qui clôt S et P, Q à l'exception de X . Par définition de \mathcal{R}° , nous avons $P\{S\sigma/X\}\sigma \mathcal{R} Q\{S\sigma/X\}\sigma$, c'est-à-dire $P\{S/X\}\sigma \mathcal{R} Q\{S/X\}\sigma$; nous avons donc $P\{S/X\} \mathcal{R}^\circ Q\{S/X\}$. Finalement nous avons $P\{R/X\} \mathcal{R}^\bullet \mathcal{R}^\circ Q\{S/X\}$, c'est-à-dire $P\{R/X\} \mathcal{R}^\bullet Q\{S/X\}$, comme souhaité.

Supposons $P \mathcal{R}^\bullet T \mathcal{R}^\circ Q$. Par induction nous avons $P\{R/X\} \mathcal{R}^\bullet T\{S/X\}$. Soit σ une substitution qui clôt S et T, Q à l'exception de X . Nous avons $T\{S\sigma/X\}\sigma \mathcal{R} Q\{S\sigma/X\}\sigma$, c'est-à-dire $T\{S/X\}\sigma \mathcal{R} Q\{S/X\}\sigma$; nous avons donc $T\{S/X\} \mathcal{R}^\circ Q\{S/X\}$. Finalement nous avons $P\{R/X\} \mathcal{R}^\bullet \mathcal{R}^\circ Q\{S/X\}$, c'est-à-dire $P\{R/X\} \mathcal{R}^\bullet Q\{S/X\}$, comme souhaité.

Supposons $op(\widetilde{P'}) \mathcal{R}^\bullet op(\widetilde{Q'})$ avec $\widetilde{P'} \mathcal{R}^\bullet \widetilde{Q'}$. Par induction nous avons $\widetilde{P'}\{R/X\} \mathcal{R}^\bullet \widetilde{Q'}\{S/X\}$, et par congruence de \mathcal{R}^\bullet nous avons $op(\widetilde{P'}\{R/X\}) \mathcal{R}^\bullet op(\widetilde{Q'}\{S/X\})$, c'est-à-dire $P\{R/X\} \mathcal{R}^\bullet Q\{S/X\}$, comme souhaité. \square

Le résultat suivant est un détail technique, permettant de raisonner par induction sur la taille de la dérivation d'un jugement $P \mathcal{R}^\bullet Q$.

Lemme A.3. *Soit $P \mathcal{R}^\bullet Q$. Pour toute substitution σ , nous avons $P\sigma \mathcal{R}^\bullet Q\sigma$ en utilisant une dérivation de la même taille que celle de $P \mathcal{R}^\bullet Q$.*

Démonstration. Par induction sur $P \mathcal{R}^\bullet Q$. Si $P \mathcal{R}^\circ Q$, alors nous montrons que nous avons $P\sigma \mathcal{R}^\circ Q\sigma$. Soit σ' une substitution qui clôt $P\sigma$ et $Q\sigma$. Comme $\sigma\sigma'$ clôt P et Q , nous avons $P\sigma\sigma' \mathcal{R} Q\sigma\sigma'$. Les autres cas sont faciles par induction. \square

Les résultats suivants permettent de conclure la méthode en prouvant la congruence.

Lemme A.4. *Pour toute relation d'équivalence \mathcal{R} , $(\mathcal{R}^\bullet)^*$ est symétrique.*

Démonstration. Nous montrons par induction sur $P (\mathcal{R}^\bullet)^{-1} Q$ que $P (\mathcal{R}^\bullet)^{-1} Q$ implique $P (\mathcal{R}^\bullet)^* Q$.

Supposons $Q \mathcal{R}^\circ P$. Comme \mathcal{R} est symétrique, \mathcal{R}° est symétrique, donc nous avons $P \mathcal{R}^\circ Q$. Comme nous avons $\mathcal{R}^\circ \subseteq \mathcal{R}^\bullet \subseteq (\mathcal{R}^\bullet)^*$, nous avons le résultat souhaité.

Supposons $Q \mathcal{R}^\bullet T \mathcal{R}^\circ P$. Par induction, nous avons $T (\mathcal{R}^\bullet)^* Q$. Par symétrie de \mathcal{R}° , nous avons $P \mathcal{R}^\circ T$, donc $P \mathcal{R}^\bullet Q$. Nous avons $P \mathcal{R}^\bullet (\mathcal{R}^\bullet)^* Q$, et donc $P (\mathcal{R}^\bullet)^* Q$ par transitivité de $(\mathcal{R}^\bullet)^*$.

Supposons $op(\widetilde{Q}') \mathcal{R}^\bullet op(\widetilde{P}')$ avec $\widetilde{Q}' \mathcal{R}^\bullet \widetilde{P}'$. Par induction nous avons $\widetilde{P}' (\mathcal{R}^\bullet)^* \widetilde{Q}'$. Par congruence de \mathcal{R}^\bullet , nous avons $op(\widetilde{P}') (\mathcal{R}^\bullet)^* op(\widetilde{Q}')$, comme souhaité. \square

Lemme A.5. *Si $\mathcal{R}^{\bullet*} \subseteq \mathcal{R}$, alors \mathcal{R} est une congruence.*

Démonstration. Par définition nous avons $\mathcal{R} \subseteq \mathcal{R}^\circ \subseteq \mathcal{R}^\bullet \subseteq \mathcal{R}^{\bullet*} \subseteq \mathcal{R}$, donc $\mathcal{R} = \mathcal{R}^\bullet$, donc \mathcal{R} est une congruence. \square

Lorsque \mathcal{R} est une bisimilarité, il suffit de prouver que $\mathcal{R}^{\bullet*}$ est une bisimulation (induite par la bisimilarité) pour montrer que \mathcal{R} est une congruence.

A.2 Preuves pour $\text{HO}\pi$

Nous prouvons ici les résultats donnés en section 5.2.

A.2.1 Correspondance des systèmes de transitions

Lemme A.6. *Si $P \xrightarrow{a} F$, alors pour tout R , nous avons $P \xrightarrow{a,R} F \circ R$. Si $P \xrightarrow{a,R} P'$, alors il existe F tel que $P \xrightarrow{a} F$ et $P' = F \circ R$.*

Démonstration. Par induction sur la structure de P .

Supposons $P = a(X)P'$. Par la règle IN, nous avons $P \xrightarrow{a} (X)P'$, et nous avons $P \xrightarrow{a,R} P' \{R/X\} = F \circ R$ par la règle IN^π . Par conséquent nous avons le résultat voulu.

Soit $P = P_1 \mid P_2$. Supposons que le message est reçu par P_1 , le cas symétrique se traite de la même manière. Si $P \xrightarrow{a} F$, alors par la règle PAR nous avons $P_1 \xrightarrow{a} F_1$ et $F = F_1 \mid P_2$. Par induction nous avons $P_1 \xrightarrow{a,R} F_1 \circ R$, donc par la règle PAR^π nous avons $P \xrightarrow{a,R} F_1 \circ R \mid P_2 = F_1 \mid P_2 \circ R = F \circ R$, comme souhaité. Si $P \xrightarrow{a,R} P'$, alors par la règle PAR^π il existe P'_1 tel que $P_1 \xrightarrow{a,R} P'_1$ et $P' = P'_1 \mid P_2$. Par induction il existe F_1 tel que $P_1 \xrightarrow{a} F_1$ et $P'_1 = F_1 \circ R$. Par la règle PAR nous avons $P \xrightarrow{a} F_1 \mid P_2 \triangleq F$, et nous avons $F \circ R = F_1 \circ R \mid P_2 = P'$ comme souhaité.

Les cas de la restriction et de la réplication se traitent comme la composition parallèle. \square

Lemme A.7. *Soit P un processus de $\text{HO}\pi$.*

- Nous avons $P \xrightarrow{\tau} \equiv P'$ ssi $P \xrightarrow{\tau} \equiv P'$.
- Si $P \xrightarrow{\bar{a}} C$, alors pour tout Q tel que $Q \xrightarrow{a} F$, nous avons $P \xrightarrow{\bar{a},Q} \equiv F \bullet C$. Si $P \xrightarrow{\bar{a},Q} P'$, il existe F, C tels que $P \xrightarrow{a} F$, $Q \xrightarrow{\bar{a}} C$ et $P' \equiv F \bullet C$.

Démonstration. Par induction sur la structure de P .

Supposons $P = \bar{a}\langle P_1 \rangle P_2$. Nous avons $P \xrightarrow{\bar{a}} \langle P_1 \rangle P_2$ par OUT. Soit Q tel que $Q \xrightarrow{a} F$. Par le lemme A.6, nous avons $Q \xrightarrow{a,P_1} F \circ P_1$. Par la règle OUT^π , nous avons $P \xrightarrow{\bar{a},Q} F \circ P_1 \mid P_2 = F \bullet C$. Nous prouvons maintenant l'implication inverse : supposons $P \xrightarrow{\bar{a},Q} P'$. Par OUT^π nous avons $Q \xrightarrow{a,P_1} Q'$ et $P' = Q' \mid P_2$. Par le lemme A.6, il existe F telle que $Q \xrightarrow{a} F$ et $Q' = F \circ P_1$. Nous avons donc $P' = F \circ P_1 \mid P_2 = F \bullet \langle P_1 \rangle P_2$, avec

$P \xrightarrow{\bar{a}} \langle P_1 \rangle P_2$ (règle OUT) comme souhaité.

Supposons $P = P_1 \mid P_2$. Nous montrons d'abord que $P \xrightarrow{\tau} P'$ implique $P \xrightarrow{\tau} \equiv P'$, par analyse de cas sur la règle utilisée pour dériver $P \xrightarrow{\tau} \equiv P'$.

- Dans le cas de la règle PAR, nous avons $P_1 \xrightarrow{\tau} P'_1$ et $P' \equiv P'_1 \mid P_2$. Par induction nous avons $P_1 \xrightarrow{\tau} \equiv P'_1$, et nous avons donc $P \xrightarrow{\tau} \equiv P'$ par la règle PAR $^\pi$.
- Dans le cas de la règle HO, nous avons $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\bar{a}} C$ et $P' \equiv F \bullet C$. Par induction nous avons $P_2 \xrightarrow{\bar{a}, P_1} \equiv F \bullet C$, donc par la règle HO $^\pi$ nous avons $P \xrightarrow{\tau} \equiv P'$ comme voulu.

Nous prouvons l'implication inverse, par analyse de cas sur la règle utilisée pour dériver $P \xrightarrow{\tau} \equiv P'$.

- Dans le cas PAR $^\pi$, nous avons $P_1 \xrightarrow{\tau} P'_1$ et $P' \equiv P'_1 \mid P_2$. Par induction nous avons $P_1 \xrightarrow{\tau} P'_1$; par PAR nous avons donc $P \xrightarrow{\tau} P'_1 \mid P_2 \equiv P'$ comme souhaité.
- Dans le cas HO $^\pi$, nous avons $P_1 \xrightarrow{\bar{a}, P_2} \equiv P'$. Par induction, il existe F, C tels que $P_1 \xrightarrow{\bar{a}} C$, $P_2 \xrightarrow{a} F$ et $P' \equiv F \bullet C$. Par la règle HO, nous avons $P \xrightarrow{\tau} \equiv F \bullet C$ comme souhaité.

Nous prouvons maintenant le résultat sur les émissions de messages, en supposant que le message provient de P_1 , le cas symétrique étant traité de manière analogue. Si $P \xrightarrow{\bar{a}} C$, alors par la règle PAR il existe C_1 tel que $P_1 \xrightarrow{\bar{a}} C_1$ et $C = C_1 \mid P_2$. Soit $Q \xrightarrow{\bar{a}} F$. Par induction nous avons $P_1 \xrightarrow{\bar{a}, Q} \equiv F \bullet C_1$; par la règle PAR $^\pi$ nous avons $P \xrightarrow{\bar{a}, Q} \equiv (F \bullet C_1) \mid P_2 = F \bullet (C_1 \mid P_2) = F \bullet C$ comme souhaité.

Si $P \xrightarrow{\bar{a}, Q} P'$, alors par la règle PAR $^\pi$ il existe P'_1 tel que $P_1 \xrightarrow{\bar{a}, Q} P'_1$ et $P' = P'_1 \mid P_2$. Par induction il existe F, C_1 tels que $P_1 \xrightarrow{\bar{a}} C_1$, $Q \xrightarrow{a} F$ et $P'_1 \equiv F \bullet C_1$. Par la règle PAR nous avons $P \xrightarrow{\bar{a}} C_1 \mid P_2 \triangleq C$, et nous avons $F \bullet C = F \bullet C_1 \mid P_2 \equiv P'_1 \mid P_2 = P'$ comme voulu.

Supposons $P = !P_1$. Les transitions peuvent provenir des règles REPLIC (par une τ -action ou une émission de message) ou REPLIC-HO. Le cas de REPLIC se traite comme PAR, et le cas de REPLIC-HO se traite comme HO. Réciproquement, les transitions provenant de la règle REPLIC $^\pi$ se traite comme PAR $^\pi$ et REPLIC-HO $^\pi$ se traite comme HO $^\pi$.

Supposons $P = \nu b.P_1$. Si $P \xrightarrow{\tau} \equiv P'$, alors par RESTR il existe P'_1 tel que $P_1 \xrightarrow{\tau} P'_1$ et $P' \equiv \nu b.P'_1$. Par induction nous avons $P_1 \xrightarrow{\tau} \equiv P'_1$, donc par RESTR $^\pi$ nous avons $P \xrightarrow{\tau} \nu b.P'_1 \equiv P'$ comme souhaité. Si $P \xrightarrow{\tau} \equiv P'$, alors par RESTR $^\pi$ il existe P'_1 tel que $P_1 \xrightarrow{\tau} P'_1$ et $\nu b.P'_1 \equiv P'$. Par induction nous avons $P_1 \xrightarrow{\tau} \equiv P'_1$, donc par RESTR nous avons $P \xrightarrow{\tau} \nu b.P_1 \equiv P'$ comme voulu.

Si $P \xrightarrow{\bar{a}} C$, alors par RESTR il existe C_1 tel que $P_1 \xrightarrow{\bar{a}} C_1$ et $C = \nu b.C_1$. Soit $Q \xrightarrow{\bar{a}} F$. Par induction nous avons $P_1 \xrightarrow{\bar{a}, Q} P'_1$ avec $P'_1 \equiv F \bullet C_1$. Par la règle RESTR $^\pi$ nous avons $P \xrightarrow{\bar{a}, Q} \equiv \nu b.(F \bullet C_1)$. Si b est libre dans le message de C_1 , alors $\nu b.(F \bullet C_1) = F \bullet \nu b.C_1$, sinon $\nu b.(F \bullet C_1) \equiv F \bullet \nu b.C_1$. Dans les deux cas nous avons $P \xrightarrow{\bar{a}, Q} \equiv F \bullet C$ comme souhaité.

Si $P \xrightarrow{\bar{a}, Q} P'$, alors par RESTR $^\pi$ il existe P'_1 tel que $P_1 \xrightarrow{\bar{a}, Q} P'_1$. Par induction il existe C_1, F tels que $P_1 \xrightarrow{\bar{a}} C_1$, $Q \xrightarrow{a} F$ et $P'_1 \equiv F \bullet C_1$. Par la règle RESTR, nous avons $P \xrightarrow{\bar{a}} \nu b.C_1 \triangleq C$. Si b est libre dans le message de C_1 , nous avons $F \bullet C = \nu b.(F \bullet C_1) \equiv \nu b.P'_1 = P'$, sinon nous avons $F \bullet C \equiv \nu b.(F \bullet C_1) \equiv \nu b.P'_1 = P'$. Dans les deux cas nous avons le résultat voulu.

□

A.2.2 Congruence de la bisimilarité à complément

Nous prouvons la congruence uniquement dans le cas fort ; le cas faible, dont la preuve est très similaire, est traité dans le cas de $\text{HO}\pi\text{P}$ (section A.3). Nous notons $(\sim_m)^\bullet_c$ la restriction de \sim_m^\bullet aux termes clos.

Lemme A.8. *Si $P \xrightarrow{a,R} P'$, pour tout $R \sim_m^\bullet R'$, il existe P'' tel que $P \xrightarrow{a,R'} P''$ et $P' \sim_m^\bullet P''$.*

Soit $P (\sim_m)^\bullet_c Q$. Si $P \xrightarrow{a,R} P'$, alors pour tout $R (\sim_m)^\bullet_c R'$, il existe Q' tel que $Q \xrightarrow{a,R'} Q'$ et $P' (\sim_m)^\bullet_c Q'$.

Démonstration. Nous prouvons le premier résultat par induction sur la dérivation de $P \xrightarrow{a,R} P'$. Si la règle utilisée est IN^π , nous avons $P = a(X)P_1 \xrightarrow{a,R} P_1\{R/X\}$. Soit $R \sim_m^\bullet R'$. Nous avons $P \xrightarrow{a,R'} P_1\{R'/X\}$, et par congruence de \sim_m^\bullet , nous avons $P_1\{R/X\} \sim_m^\bullet P_1\{R'/X\}_1$, comme souhaité.

Si la dernière règle utilisée est PAR^π , nous avons $P = P_1 \mid P_2 \xrightarrow{a,R} P'_1 \mid P_2$ avec $P_1 \xrightarrow{a,R} P'_1$. Soit $R \sim_m^\bullet R'$; par induction il existe P''_1 tel que $P_1 \xrightarrow{a,R'} P''_1$ et $P'_1 \sim_m^\bullet P''_1$. Par la règle PAR^π nous avons $P \xrightarrow{a,R'} P''_1 \mid P_2$, et par congruence de \sim_m^\bullet nous avons $P'_1 \mid P_2 \sim_m^\bullet P''_1 \mid P_2$ comme voulu.

Si la dernière règle utilisée est REPLIC^π , nous avons $P = !P_1 \xrightarrow{a,R} P'_1 \mid !P_1$ avec $P_1 \xrightarrow{a,R} P'_1$. Soit $R \sim_m^\bullet R'$; par induction il existe P''_1 tel que $P_1 \xrightarrow{a,R'} P''_1$ et $P'_1 \sim_m^\bullet P''_1$. Par la règle REPLIC^π nous avons $P \xrightarrow{a,R'} P''_1 \mid !P_1$, et par congruence de \sim_m^\bullet nous avons $P'_1 \mid !P_1 \sim_m^\bullet P''_1 \mid !P_1$ comme voulu.

Si la dernière règle utilisée est RESTR^π , nous avons $P = \nu b.P_1 \xrightarrow{a,R} \nu b.P'_1$ avec $P_1 \xrightarrow{a,R} P'_1$. Soit $R \sim_m^\bullet R'$; par induction il existe P''_1 tel que $P_1 \xrightarrow{a,R'} P''_1$ et $P'_1 \sim_m^\bullet P''_1$. Par la règle RESTR^π nous avons $P \xrightarrow{a,R'} \nu b.P''_1$, et par congruence de \sim_m^\bullet nous avons $\nu b.P'_1 \sim_m^\bullet \nu b.P''_1$ comme voulu.

Nous montrons maintenant le deuxième résultat par induction sur la taille de la dérivation de $P (\sim_m)^\bullet_c Q$.

Supposons $P \sim_m^\circ Q$; comme P et Q sont clos nous avons $P \sim_m Q$. Par le premier résultat il existe P'' tel que $P \xrightarrow{a,R'} P''$ et $P' \sim_m^\bullet P''$. Par définition de la bisimilarité, il existe Q' tel que $Q \xrightarrow{a,R'} Q'$ et $P'' \sim_m Q'$. Comme P, Q, R' sont clos, P', P'' et Q' sont clos, et nous avons $P'' \sim_m^\circ Q'$. Nous avons donc $P' \sim_m^\bullet \mathcal{R}^\circ Q'$, et donc $P' (\sim_m)^\bullet_c Q'$ comme souhaité.

Supposons $P \sim_m^\bullet T \sim_m^\circ Q$. Soit σ une substitution qui clôt T . Par le lemme A.3 et comme P est clos, nous avons $P (\sim_m)^\bullet_c T\sigma$ par une preuve de la même taille. Par induction il existe T' tel que $T\sigma \xrightarrow{a,R'} T'$ et $P' (\sim_m)^\bullet_c T'$. Par définition nous avons $T\sigma \sim_m Q$, donc par bisimilarité il existe Q' tel que $Q \xrightarrow{a,R'} Q'$ et $T' \sim_m Q'$. Comme T' et Q' sont clos, nous avons $T' \sim_m^\circ Q'$; nous avons donc $P' \sim_m^\bullet \sim_m^\circ Q'$ avec P' et Q' , nous obtenons donc $P' (\sim_m)^\bullet_c Q'$ comme souhaité.

Supposons $op(\tilde{P}) (\sim_m)^\bullet_c op(\tilde{Q})$ avec $\tilde{P} (\sim_m)^\bullet_c \tilde{Q}$. Nous procédons par analyse de cas sur op .

- Si $P = a(X)P_1$ et $Q = a(X)Q_1$, alors la transition de P provient de la règle IN^π : nous avons $P \xrightarrow{a,R} P_1\{R/X\} = P'$. Nous avons $Q \xrightarrow{a,R'} Q_1\{R'/X\}$, et par le lemme A.2 nous avons $P_1\{R/X\} (\sim_m)^\bullet_c Q_1\{R'/X\} \triangleq Q'$. Comme les processus impliqués sont clos, nous avons $P' (\sim_m)^\bullet_c Q'$ comme souhaité.
- Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, alors la transition de P ne peut provenir que de la règle PAR^π : nous avons $P_1 \xrightarrow{a,R} P'_1$ avec $P' = P'_1 \mid P_2$. Par induction il existe Q'_1 tel

- que $Q_1 \xrightarrow{a,R'} Q'_1$ et $P'_1 (\sim_m)_c^\bullet Q'_1$. Par PAR^π nous avons $Q \xrightarrow{a,R'} Q'_1 \mid Q_2 \triangleq Q'$. Par congruence de \sim_m^\bullet nous avons $P' (\sim_m)_c^\bullet Q'$ comme demandé.
- Si $P = !P_1$ et $Q = !Q_1$, alors la transition de P ne peut provenir que de la règle REPLIC^π : nous avons $P_1 \xrightarrow{a,R} P'_1$ avec $P' = P'_1 \mid !P_1$. Par induction il existe Q'_1 tel que $Q_1 \xrightarrow{a,R'} Q'_1$ et $P'_1 (\sim_m)_c^\bullet Q'_1$. Par REPLIC^π nous avons $Q \xrightarrow{a,R'} Q'_1 \mid !Q_1 \triangleq Q'$. Par congruence de \sim_m^\bullet nous avons $P' (\sim_m)_c^\bullet Q'$ comme demandé.
 - Si $P = \nu b.P_1$ et $Q = \nu b.Q_1$, alors la transition de P ne peut provenir que de la règle RESTR^π : nous avons $P_1 \xrightarrow{a,R} P'_1$ avec $P' = \nu b.P'_1$. Par induction il existe Q'_1 tel que $Q_1 \xrightarrow{a,R'} Q'_1$ et $P'_1 (\sim_m)_c^\bullet Q'_1$. Par RESTR^π nous avons $Q \xrightarrow{a,R'} \nu b.Q'_1 \triangleq Q'$. Par congruence de \sim_m^\bullet nous avons $P' (\sim_m)_c^\bullet Q'$ comme demandé.

□

Lemme A.9. Si $P \xrightarrow{\bar{a},R} P'$, alors pour tout $R \sim_m^\bullet R'$, il existe P'' tel que $P \xrightarrow{\bar{a},R'} P''$ et $P' \sim_m^\bullet P''$.

Démonstration. Par induction sur la dérivation de $P \xrightarrow{\bar{a},R} P'$.

Si la règle utilisée est OUT^π , nous avons $P = \bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a},R} S \mid P_2 = P'$ avec $R \xrightarrow{a,P_1} S$. Par le lemme A.8, il existe S' tel que $R' \xrightarrow{a,P_1} S'$ et $S \sim_m^\bullet S'$. Par la règle OUT^π nous avons $P \xrightarrow{\bar{a},R'} S' \mid P_2 \triangleq P''$. Comme \sim_m^\bullet est une congruence, nous avons $P' \sim_m^\bullet P''$, comme souhaité.

Si la dernière règle utilisée est PAR^π , nous avons $P = P_1 \mid P_2 \xrightarrow{\bar{a},R} P'_1 \mid P_2 = P'$ avec $P_1 \xrightarrow{\bar{a},R} P'_1$. Par induction il existe P''_1 tel que $P_1 \xrightarrow{\bar{a},R'} P''_1$ et $P'_1 \sim_m^\bullet P''_1$. Par la règle PAR^π nous avons $P \xrightarrow{\bar{a},R'} P''_1 \mid P_2 \triangleq P''$, et comme \sim_m^\bullet est une congruence, nous avons $P' \sim_m^\bullet P''$ comme voulu. Les cas de la restriction (règle RESTR^π) et de la réplication (règle REPLIC^π) se traitent de la même manière.

□

Lemme A.10. Soit $P (\sim_m)_c^\bullet Q$.

- Si $P \xrightarrow{\tau} P'$, alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' (\sim_m)_c^\bullet Q'$.
- Si $P \xrightarrow{\bar{a},R} P'$, alors pour tout $R (\sim_m)_c^\bullet R'$, il existe Q' tel que $Q \xrightarrow{\bar{a},R'} Q'$ et $P' (\sim_m)_c^\bullet Q'$.

Démonstration. Par induction sur la taille de la dérivation de $P (\sim_m)_c^\bullet Q$.

Si $P \sim_m^\circ Q$, alors comme les processus sont clos nous avons $P \sim_m Q$. La première clause est vraie par bisimilarité. Nous prouvons maintenant la seconde clause. Par le lemme A.9, il existe P'' tel que $P \xrightarrow{\bar{a},R'} P''$ et $P' \sim_m^\bullet P''$. Par bisimilarité il existe Q' tel que $Q \xrightarrow{\bar{a},R'} Q'$ et $P' \sim_m Q'$. Comme P, Q, R, R' sont clos, P' et Q' sont clos, et nous avons $P' \sim_m^\bullet \sim_m^\circ Q'$, donc nous avons $P' (\sim_m)_c^\bullet Q'$ comme souhaité.

Si $P \sim_m^\bullet T \sim_m^\circ Q$, alors pour toute substitution σ qui clôt T , nous avons $P (\sim_m)_c^\bullet T\sigma$ avec une dérivation de la même taille d'après le lemme A.3. Par induction il existe T' tel que $T\sigma \xrightarrow{\tau} T'$ et $P' (\sim_m)_c^\bullet T'$. Nous avons $T\sigma \sim_m Q$, donc par définition il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $T' \sim_m^\bullet Q'$. Les processus T' et Q' sont clos, donc nous avons $T' \sim_m^\circ Q'$. Finalement nous avons $P' \sim_m^\bullet \sim_m^\circ Q'$, donc $P' (\sim_m)_c^\bullet Q'$ comme voulu. La clause pour l'émission se prouve de la même manière.

Si $P = \text{op}(\tilde{P})$ et $Q = \text{op}(\tilde{Q})$ avec $\tilde{P} (\sim_m)_c^\bullet \tilde{Q}$, alors nous procédons par analyse de cas sur op .

- Si $P = \bar{a}\langle P_1 \rangle P_2$ et $Q = \bar{a}\langle Q_1 \rangle Q_2$, alors la seule transition possible est $P \xrightarrow{\bar{a},R} S \mid P_2 = P'$, avec $R \xrightarrow{a,R} S$. Par le lemme A.8, il existe S' tel que $R' \xrightarrow{a,Q_1} S'$ et $S (\sim_m)_c^\bullet S'$. Par la règle OUT^π nous avons $Q \xrightarrow{\bar{a},R'} S' \mid Q_2 \triangleq Q'$. Par congruence de \sim_m^\bullet et comme les termes impliqués sont clos, nous avons $P' (\sim_m)_c^\bullet Q'$, comme souhaité.

- Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, alors les transitions de P peuvent provenir des règles PAR^π et HO^π (ou de leur symétrique). Dans le cas de PAR^π , nous avons $P_1 \xrightarrow{\lambda} P'_1$ ($\lambda = \tau$ ou $\lambda = \bar{a}, R$), et $P' = P'_1 \mid P_2$. Par induction il existe Q'_1 tel que $Q'_1 \xrightarrow{\lambda'} Q'_1$ et $P'_1 (\sim_m)_c^\bullet Q'_1$ (avec $\lambda' = \tau$ ou $\lambda' = \bar{a}, R'$). Par PAR^π nous avons $Q \xrightarrow{\lambda'} Q'_1 \mid Q_2 \triangleq Q'$, et comme \sim_m^\bullet est une congruence, nous avons $P' (\sim_m)_c^\bullet Q'$ comme souhaité.
 Dans le cas de HO^π , nous avons $P_1 \xrightarrow{\bar{a}, P_2} P'$. Par induction il existe Q' tel que $Q_1 \xrightarrow{\bar{a}, Q_2} Q'$ et $P' (\sim_m)_c^\bullet Q'$, et par HO^π nous avons $Q \xrightarrow{\tau} Q'$.
- Si $P = !P_1$ et $Q = !Q_1$, alors les transitions de P peuvent provenir des règles REPLIC^π et REPLIC-HO^π . Dans le cas de REPLIC^π , nous avons $P_1 \xrightarrow{\lambda} P'_1$ ($\lambda = \tau$ ou $\lambda = \bar{a}, R$), et $P' = P'_1 \mid !P_1$. Par induction il existe Q'_1 tel que $Q'_1 \xrightarrow{\lambda'} Q'_1$ et $P'_1 (\sim_m)_c^\bullet Q'_1$ (avec $\lambda' = \tau$ ou $\lambda' = \bar{a}, R'$). Par REPLIC^π nous avons $Q \xrightarrow{\lambda'} Q'_1 \mid !Q_1 \triangleq Q'$, et comme \sim_m^\bullet est une congruence, nous avons $P' (\sim_m)_c^\bullet Q'$ comme souhaité.
 Dans le cas de REPLIC-HO^π , nous avons $P_1 \xrightarrow{\bar{a}, P_1} P'_1$ et $P' = P'_1 \mid !P_1$. Par induction il existe Q'_1 tel que $Q_1 \xrightarrow{\bar{a}, Q_1} Q'_1$ et $P'_1 (\sim_m)_c^\bullet Q'_1$, et par REPLIC-HO^π nous avons $Q \xrightarrow{\tau} Q'_1 \mid !Q_1 \triangleq Q'$. Par congruence de \sim_m^\bullet nous avons $P' (\sim_m)_c^\bullet Q'$ comme voulu.
- Si $P = \nu b.P_1$ et $Q = \nu b.Q_1$, alors la seule transition possible est $P \xrightarrow{\lambda} \nu b.P'_1$ avec $P_1 \xrightarrow{\lambda} P'_1$ et $\lambda = \tau$ ou $\lambda = \bar{a}, R$. Par induction il existe Q'_1 tel que $Q_1 \xrightarrow{\lambda'} Q'_1$ et $Q_1 (\sim_m)_c^\bullet Q'_1$, avec $\lambda' = \tau$ ou $\lambda' = \bar{a}, R'$. Par RESTR^π , nous avons $Q \xrightarrow{\lambda'} \nu b.Q'_1 \triangleq Q'$ et par congruence de \sim_m^\bullet , nous avons $P' (\sim_m)_c^\bullet Q'$ comme souhaité.

□

Lemme A.11. *La relation $(\sim_m)_c^{\bullet*}$ est une bisimulation forte à complément.*

Démonstration. D'après le lemme A.4, $(\sim_m)_c^{\bullet*}$ est symétrique, il suffit donc de prouver que c'est une simulation. Les lemmes A.8 et A.10 impliquent directement que $(\sim_m)_c^\bullet$ est une simulation forte à complément, donc $(\sim_m)_c^{\bullet*}$ est une simulation forte à complément.

□

Théorème A.1. *La relation \sim_m est une congruence.*

Démonstration. Immédiat par les lemmes A.11 et A.5.

□

A.2.3 Correspondance des bisimilarités

Nous prouvons maintenant que les bisimilarités \sim et \sim_m coïncident.

Définition A.1. *Une relation \mathcal{R} est une bisimulation à complément modulo \equiv ssi pour tout $P \mathcal{R} Q$ et $P \xrightarrow{\tau} P'$, il existe Q' tel que $P' \equiv \mathcal{R} \equiv Q'$, et inversement pour $Q \xrightarrow{\tau} Q'$.*

Lemme A.12. *Soit \mathcal{R} une bisimulation à complément modulo \equiv ; nous avons $\mathcal{R} \subseteq \sim_m$.*

Démonstration. En montrant que $\equiv \mathcal{R} \equiv$ est une bisimulation forte à complément.

□

Lemme A.13. *Nous avons $\sim \subseteq \sim_m$.*

Démonstration. Nous montrons que \sim est une bisimulation à complément modulo \equiv . Soit $P \sim Q$.

Si $P \xrightarrow{\tau} P'$, alors par le lemme A.7 nous avons $P \xrightarrow{\tau} \equiv P'$. Il existe donc Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \equiv \sim Q'$. Par le lemme A.7 nous avons donc $Q \xrightarrow{\tau} \equiv Q'$, le résultat est donc vrai.

Si $P \xrightarrow{a, R} P'$, alors par le lemme A.6 il existe F tel que $P \xrightarrow{a} F$ et $P' = F \circ R$. Il existe donc F' tel que $Q \xrightarrow{a} F'$ et $F \bullet \langle R \rangle \mathbf{0} \sim F' \bullet \langle R \rangle \mathbf{0}$. Par le lemme A.6 nous avons $Q \xrightarrow{a, R} F' \circ R$, et nous avons $P' \equiv F \bullet \langle R \rangle \mathbf{0} \sim F' \bullet \langle R \rangle \mathbf{0} \equiv F' \circ R$, comme souhaité.

Si $P \xrightarrow{\bar{a}, R} P'$, alors par le lemme A.7 il existe F, C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$ et $P' \equiv F \bullet C$. Il existe donc C' tel que $Q \xrightarrow{\bar{a}} C'$ et $F \bullet C \sim F \bullet C'$. Par le lemme A.7 nous avons $Q \xrightarrow{\bar{a}, R} F \bullet C'$, le résultat est donc vrai. \square

Lemme A.14. *Nous avons $\sim_m \subseteq \sim$.*

Démonstration. Nous montrons que \sim_m est une bisimulation contextuelle forte modulo \equiv . Soit $P \sim_m Q$.

Si $P \xrightarrow{\tau} P'$, alors par le lemme A.7 nous avons $P \xrightarrow{\tau} \equiv P'$. Il existe donc Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \equiv \sim_m Q'$. Par le lemme A.7 nous avons $Q \xrightarrow{\tau} \equiv Q'$, le résultat est donc vrai.

Si $P \xrightarrow{a} F$ et $C = \nu \tilde{b}. \langle R \rangle S$, alors par le lemme A.6 nous avons $P \xrightarrow{a, R} F \circ R$. Il existe donc Q' tel que $Q \xrightarrow{a, R} Q'$ et $F \circ R \sim Q'$. Par le lemme A.6 il existe F' tel que $Q \xrightarrow{a} F'$ et $Q' = F' \circ R$. Comme \sim_m est une congruence, nous avons $F \bullet C = \nu \tilde{b}. (F \circ R \mid S) \sim_m \nu \tilde{b}. (F' \circ R \mid S) = F' \bullet C$, le résultat est donc vrai.

Soit $P \xrightarrow{\bar{a}} C$ et $F = (X)R$ une fonction. Par le lemme A.7 nous avons $P \xrightarrow{\bar{a}, a(X)R} F \bullet C$. Il existe donc Q' tel que $Q \xrightarrow{\bar{a}, a(X)R} Q'$ et $F \bullet C \equiv \sim_m Q'$. Par le lemme A.7 il existe C' tel que $Q \xrightarrow{\bar{a}} C'$ et $Q' \equiv F \bullet C'$. Nous avons $F \bullet C \equiv \sim_m \equiv F \bullet C'$ comme souhaité. \square

A.3 Preuves pour HO π P

Nous prouvons ici les résultats donnés en section 5.2

A.3.1 Correspondance des systèmes de transitions

Lemme A.15. *Si $P \xrightarrow{a} F$, alors pour tout R nous avons $P \xrightarrow{a, R} F \circ R$. Si $P \xrightarrow{a, R} P'$, il existe F telle que $P \xrightarrow{a} F$ et $P' = F \circ R$.*

Démonstration. Par induction structurale sur P . La preuve est similaire à celle pour HO π (lemme A.6) : la localité (règles LOC et LOC $_{itr}^p$) se traite comme la composition parallèle. \square

Lemme A.16. *Si $P \xrightarrow{\bar{a}} C$, alors pour tout R tel que $R \xrightarrow{a} F$ et \mathbb{E} tel que $\text{bn}(\mathbb{E}) \cap \text{extr}(C) = \emptyset$, nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} F \bullet \mathbb{E}\{C\}$.*

Si $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, alors il existe F, C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$, $\tilde{b} = \text{extr}(C)$ et $P' = F \bullet \mathbb{E}\{C\}$.

Démonstration. Par induction structurale sur P .

Supposons $P = \bar{a}\langle P_1 \rangle P_2$. La transition $P \xrightarrow{\bar{a}} C$ vient de la règle OUT : nous avons $C = \langle P_1 \rangle P_2$. Soient R, \mathbb{E} tels que $R \xrightarrow{a} F$ et $\mathbb{E} \cap \text{fn}(P_1) = \emptyset$. Par le lemme A.15 nous avons $R \xrightarrow{a, P_1} F \circ P_1$. Par la règle OUT $_o^p$, nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{fn}(P_1)} F \circ P_1 \mid \mathbb{E}\{P_2\} = F \bullet \mathbb{E}\{C\}$, le résultat est donc vrai. Réciproquement, la transition $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$ provient de la règle OUT $_o^p$: nous avons $\tilde{b} = \text{fn}(P_1)$, $R \xrightarrow{a, P_1} R'$ et $P' = R' \mid \mathbb{E}\{P_2\}$. Par le lemme A.15, il existe F tel que $R \xrightarrow{a} F$ et $R' = F \circ P_1$. Nous avons donc $P' = F \circ P_1 \mid \mathbb{E}\{P_2\} = F \bullet \mathbb{E}\{\langle P_1 \rangle P_2\}$, et nous avons $P \xrightarrow{\bar{a}} \langle P_1 \rangle P_2$ par la règle OUT, le résultat est donc vrai.

Supposons $P = P_1 \mid P_2$. La transition $P \xrightarrow{\bar{a}} C$ vient de la règle PAR ou de sa symétrique. Nous supposons que nous avons $C = C_1 \mid P_2$ avec $P_1 \xrightarrow{\bar{a}} C_1$, le cas symétrique est analogue. Soient R, \mathbb{E} tels que $R \xrightarrow{a} F$ et $\mathbb{E} \cap \text{extr}(C) = \emptyset$. Nous avons $\text{extr}(C) = \text{extr}(C_1)$ et $\text{bn}(\mathbb{E} \{\square \mid P_2\}) \cap \text{extr}(C_1) = \emptyset$, donc par induction nous avons $P_1 \xrightarrow{\bar{a}, R, \mathbb{E} \{\square \mid P_2\}}_{\text{extr}(C_1)} F \bullet \mathbb{E}\{C_1 \mid P_2\}$.

Par la règle PAR_o^p nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} F \bullet \mathbb{E}\{C\}$ comme souhaité. Réciproquement, la transition $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$ provient de la règle PAR_o^p : nous avons $P_1 \xrightarrow{\bar{a}, R, \mathbb{E}\{\square | P_2\}}_{\text{extr}(C_1)} P'$. Par induction il existe F, C_1 tels que $P_1 \xrightarrow{\bar{a}} C_1$, $R \xrightarrow{a} F$, $\text{extr}(C_1) = \tilde{b}$ et $P' = F \bullet \mathbb{E}\{C_1 \mid P_2\}$. Par la règle PAR nous avons $P \xrightarrow{\bar{a}} C_1 \mid P_2 \triangleq C$, et nous avons $\text{extr}(C) = \text{extr}(C_1) = \tilde{b}$ et $F \bullet \mathbb{E}\{C\} = F \bullet \mathbb{E}\{C_1 \mid P_2\} = P'$ comme voulu.

Si $P = a[P_1]$, la transition de P peut provenir des règles de passivation PASSIV et PASSIV_o^p ou des règles de congruence LOC et LOC_o^p . Le cas de la passivation se traite comme l'émission de message, et la congruence se traite comme la composition parallèle. De même la réplication se traite comme la composition parallèle.

Supposons $P = \nu c.P_1$. La transition $P \xrightarrow{\bar{a}} C$ provient de la règle RESTR : nous avons $P_1 \xrightarrow{\bar{a}} C_1$ et $C = \nu c.C_1$. Soient R, \mathbb{E} tels que $R \xrightarrow{a} F$ et $\mathbb{E} \cap \text{extr}(C) = \emptyset$. Nous avons deux possibilités.

- Si c est libre dans le message de C_1 , nous avons $F \bullet \mathbb{E}\{C\} = \nu c.F \bullet \mathbb{E}\{C_1\}$. Par induction nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C_1)} F \bullet \mathbb{E}\{C_1\}$. Nous avons $\text{extr}(C_1) = \text{extr}(C) \cup c$, donc par la règle EXTR_o^p nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} \nu c.F \bullet \mathbb{E}\{C_1\} = F \bullet \mathbb{E}\{C\}$, comme souhaité.
- Si c n'apparaît pas dans le message de C_1 , nous avons $F \bullet \mathbb{E}\{C\} = F \bullet \mathbb{E}\{\nu c.C_1\}$. Par induction nous avons $P_1 \xrightarrow{\bar{a}, R, \mathbb{E}\{\nu c.\square\}}_{\text{extr}(C_1)} F \bullet \mathbb{E}\{\nu c.C_1\}$. Nous avons $\text{extr}(C) = \text{extr}(C_1)$ et $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} F \bullet \mathbb{E}\{\nu c.C_1\} = F \bullet \mathbb{E}\{C\}$ par la règle RESTR_o^p , le résultat est donc vrai.

Réciproquement, la transition $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$ peut provenir de deux dérivations :

- Si la transition vient de la règle RESTR_o^p , nous avons $P_1 \xrightarrow{\bar{a}, R, \mathbb{E}\{\nu c.\square\}}_{\tilde{b}} P'$ et $c \notin \tilde{b}$. Par induction il existe F, C_1 tels que $P_1 \xrightarrow{\bar{a}} C_1$, $R \xrightarrow{a} F$, $\tilde{b} = \text{extr}(C_1)$ et $P' = F \bullet \mathbb{E}\{\nu c.C_1\}$. Par la règle RESTR , nous avons $P \xrightarrow{\bar{a}} \nu c.C_1 = C$, et nous avons $P' = F \bullet \mathbb{E}\{\nu c.C_1\} = F \bullet \mathbb{E}\{C\}$ et $\text{extr}(C) = \text{extr}(C_1) = \tilde{b}$, le résultat est donc vrai.
- Si la transition vient de la règle EXTR_o^p , nous avons $P_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b} \cup c} P'_1$ et $P' = \nu c.P'_1$. Par induction il existe F, C_1 tels que $P_1 \xrightarrow{\bar{a}} C_1$, $R \xrightarrow{a} F$, $\tilde{b} \cup c = \text{extr}(C_1)$ et $P'_1 = F \bullet \mathbb{E}\{C_1\}$. Par la règle RESTR , nous avons $P \xrightarrow{\bar{a}} \nu c.C_1 = C$. Comme $c \in \text{extr}(C_1)$, le nom c est dans le message de C_1 , donc dans la portée de c est étendue dans $F \bullet \mathbb{E}\{C\}$: nous avons donc $F \bullet \mathbb{E}\{C\} = \nu c.F \bullet \mathbb{E}\{C_1\} = \nu c.P'_1 = P'$ et $\tilde{b} = \text{extr}(C_1) \setminus c = \text{extr}(C)$, le résultat est donc vrai.

□

Lemme A.17. Si $P \xrightarrow{\bar{a}} C$, alors pour tout R, \mathbb{E} tel que $R \xrightarrow{a} F$, nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} F \bullet \mathbb{E}\{C\}$.

Si $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, alors il existe F, C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$, $\tilde{b} = \text{extr}(C)$ et $P' = F \bullet \mathbb{E}\{C\}$.

Démonstration. Soit R, \mathbb{E} tel que $R \xrightarrow{a} F$. Le premier résultat est par induction sur le nombre de capture par \mathbb{E} , c'est-à-dire le nombre de noms dans $\text{bn}(\mathbb{E}) \cap \text{extr}(C)$. Si ce nombre est nul, le lemme A.16 s'applique. Si ce nombre est $n > 0$, il existe un nom c tel que $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$ et $c \in \text{extr}(C)$. L'ensemble $\text{bn}(\mathbb{E}_1\{\mathbb{E}_2\}) \cap \text{extr}(C)$ est de taille $n - 1$, donc par induction nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}}_{\text{extr}(C)} F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}$. Par la règle CAPT_o^p nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} \nu c.F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}$, et comme $c \in \text{extr}(C)$, nous avons $F \bullet \mathbb{E}\{C\} = \nu c.F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}$, le résultat est donc vrai.

La réciproque est par induction sur la dérivation de $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$. Si la dernière règle appliquée est CFREE_o^p , nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, et le résultat est vrai par le lemme A.16.

Sinon, nous avons $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}} P''$ avec $P' = \nu c.P''$, $c \in \tilde{b}$ et $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$. Par induction, il existe F, C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$, $\tilde{b} = \text{extr}(C)$ et $P'' = F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\}$. Comme $c \in \tilde{b} = \text{extr}(C)$, nous avons $F \bullet \mathbb{E}\{C\} = \nu c.F \bullet \mathbb{E}_1\{\mathbb{E}_2\{C\}\} = \nu c.P'' = P'$, le résultat est donc vrai. \square

Lemme A.18. *Nous avons $P \xrightarrow{\tau} P'$ ssi $P \xrightarrow{\tau} P'$.*

Démonstration. Par induction structurelle sur P .

Supposons $P = P_1 \mid P_2$. La transition $P \xrightarrow{\tau} P'$ provient des règles PAR ou HO ou de leur symétrique. Dans le cas de HO, nous avons $P_1 \xrightarrow{a} F$, $P_2 \xrightarrow{\bar{a}C}$ et $P' = F \bullet C$. Par le lemme A.17, nous avons $P_1 \xrightarrow[\tilde{b}]{\bar{a}, P_2, \square} F \bullet C = P'$, donc par la règle HO π nous avons $P \xrightarrow{\tau} P'$, comme souhaité. Dans le cas de PAR, nous avons $P_1 \xrightarrow{\tau} P'_1$ et $P' = P'_1 \mid P_2$. Par induction nous avons $P_1 \xrightarrow{\tau} P'_1$, donc par PAR $_{i\tau}^p$ nous avons $P \xrightarrow{\tau} P'_1 \mid P_2$ comme souhaité.

Réciproquement, la transition $P \xrightarrow{\tau} P'$ provient de la règle PAR $_{i\tau}^p$ ou HO π . Dans le cas de HO π , nous avons $P_1 \xrightarrow[\tilde{b}]{\bar{a}, P_2, \square} P'$ donc par le lemme A.17, il existe F, C tels que $P_1 \xrightarrow{\bar{a}} C$, $P_2 \xrightarrow{a} F$ et $P' = F \bullet C$. Par HO, nous avons $P \xrightarrow{\tau} F \bullet C = P'$, le résultat est donc vrai. Dans le cas PAR $_{i\tau}^p$, nous avons $P_1 \xrightarrow{\tau} P'_1$ et $P' = P'_1 \mid P_2$. Par induction nous avons $P_1 \xrightarrow{\tau} P'_1$, donc par la règle PAR $P \xrightarrow{\tau} P'_1 \mid P_2 = P'$, le résultat est donc vrai.

La restriction et la localité se traitent comme les règles de congruence de la composition parallèle. Si $P = !P_1$, les transitions proviennent des règles de congruence ou de communication : ces deux cas se traitent comme les cas correspondants de la composition parallèle. \square

Lemme A.19. *Soit P un processus de HO π P :*

- Nous avons $P \xrightarrow{\tau} P'$ ssi $P \xrightarrow{\tau} P'$.
- Si $P \xrightarrow{a} F$ et $F \circ R \xrightarrow{\tau} P'$, alors nous avons $P \xrightarrow[\tau]{a, R} P'$. Si $P \xrightarrow[\tau]{a, R} P'$, alors il existe F tel que $P \xrightarrow{a} F$ et $F \circ R \xrightarrow{\tau} P'$.
- Si $P \xrightarrow{\bar{a}} C$, alors pour tout R, \mathbb{E} tels que $R \xrightarrow{\bar{a}} F$ et $F \bullet \mathbb{E}\{C\} \xrightarrow{\tau} P'$, nous avons $P \xrightarrow[\tau]{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} P'$. Si $P \xrightarrow[\tau]{\bar{a}, R, \mathbb{E}}_{\tilde{b}} P'$, il existe F, C tels que $P \xrightarrow{a} F$, $R \xrightarrow{\bar{a}} C$, $\tilde{b} = \text{extr}(C)$ et $F \bullet \mathbb{E}\{C\} \xrightarrow{\tau} P'$.

Démonstration. Par le lemme A.18, nous avons $\xrightarrow{\tau} = \xrightarrow{\tau}$, donc nous avons $\xrightarrow{\tau} = \xrightarrow{\tau}$.

Si $P \xrightarrow{\tau} P_1 \xrightarrow{a} F$ et $F \circ R \xrightarrow{\tau} P'$, alors nous avons $P \xrightarrow{\tau} P_1$ et $F \circ R \xrightarrow{\tau} P'$ par le premier résultat. Par le lemme A.15 nous avons $P_1 \xrightarrow[\tau]{a, R} F \circ R$, donc au final nous avons $P \xrightarrow[\tau]{a, R} P'$. Si $P \xrightarrow{\tau} P_1 \xrightarrow[\tau]{a, R} P_2 \xrightarrow{\tau} P'$, par le premier résultat nous avons $P \xrightarrow{\tau} P_1$ et $P_2 \xrightarrow{\tau} P'$. Par le lemme A.15 il existe F tel que $P_1 \xrightarrow{a} F$ et $P_2 = F \circ R$. Nous avons donc $P \xrightarrow{a} F$ et $F \circ R \xrightarrow{\tau} P'$ comme voulu.

Soient $P \xrightarrow{\tau} P_1 \xrightarrow{\bar{a}} C$, R tel que $R \xrightarrow{\tau} R_1 \xrightarrow{a} F$ et $F \bullet \mathbb{E}\{C\} \xrightarrow{\tau} P'$. Par le premier résultat nous avons $P \xrightarrow{\tau} P_1$, $R \xrightarrow{\tau} R_1$ et $F \bullet \mathbb{E}\{C\} \xrightarrow{\tau} P'$. Par le lemme A.17, nous avons $P_1 \xrightarrow[\tau]{\bar{a}, R_1, \mathbb{E}}_{\text{extr}(C)} F \bullet \mathbb{E}\{C\}$. Nous avons donc $P \xrightarrow[\tau]{\bar{a}, R_1, \mathbb{E}}_{\text{extr}(C)} P'$ avec $R \xrightarrow{\tau} R_1$, c'est-à-dire $P \xrightarrow[\tau]{\bar{a}, R, \mathbb{E}}_{\text{extr}(C)} P'$ comme voulu. Réciproquement, si $P \xrightarrow{\tau} P_1 \xrightarrow[\tau]{\bar{a}, R_1, \mathbb{E}}_{\tilde{b}} P_2 \xrightarrow{\tau} P'$ avec $R \xrightarrow{\tau} R_1$, nous avons $P \xrightarrow{\tau} P_1$, $P_2 \xrightarrow{\tau} P'$ et $R \xrightarrow{\tau} R_1$ par le premier résultat. Par le lemme A.17, il existe F, C tels que $P_1 \xrightarrow{\bar{a}} C$, $R_1 \xrightarrow{a} F$, $\tilde{b} = \text{extr}(C)$ et $P_2 = F \bullet \mathbb{E}\{C\}$. Nous avons donc $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$ et $F \bullet \mathbb{E}\{C\} \xrightarrow{\tau} P'$ comme souhaité. \square

A.3.2 Congruence de la bisimilarité à complément

Lemme A.20. Si $P \approx_m Q$ et $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'$, alors il existe Q', R' tels que $Q \xrightarrow[\tilde{b}]{\tau, \bar{a}, R, \mathbb{E}} Q'$, $R \xrightarrow[\tilde{b}]{\tau} R'$ et $P' \approx_m Q'$.

Démonstration. Comme nous avons $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'$, nous avons $\text{bn}(\mathbb{E}) \cap \tilde{b} = \emptyset$, et $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'$ par CFREE_o^p . Il existe donc Q' tel que $Q \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} Q'$ et $P' \approx_m Q'$. Par définition il existe R' tel que $R \xrightarrow[\tilde{b}]{\tau} R'$ et $Q \xrightarrow[\tilde{b}]{\tau, \bar{a}, R', \mathbb{E}} Q'$. Comme $\text{bn}(\mathbb{E}) \cup \tilde{b} = \emptyset$, la transition $\xrightarrow[\tilde{b}]{\bar{a}, R', \mathbb{E}}$ provient de la règle CFREE_o^p , nous avons donc $Q \xrightarrow[\tilde{b}]{\tau, \bar{a}, R', \mathbb{E}} Q'$ comme souhaité. \square

Lemme A.21. Soient $P \approx_m Q$.

Si $P \xrightarrow[\tilde{b}]{\lambda} P'$, alors il existe Q' tel que $Q \xrightarrow[\tilde{b}]{\lambda} Q'$ et $P' \approx_m Q'$.

Si $P \xrightarrow[\tilde{b}]{\tau, \bar{a}, R', \mathbb{E}} P'$ avec $R \xrightarrow[\tilde{b}]{\tau} R'$, alors il existe R'', Q' tels que $R \xrightarrow[\tilde{b}]{\tau} R''$, $Q \xrightarrow[\tilde{b}]{\tau, \bar{a}, R'', \mathbb{E}} Q'$ et $P' \approx_m Q'$.

Démonstration. Si $P \xrightarrow[\tilde{b}]{\tau} P'$, le résultat se prouve facilement par induction sur le nombre d'étapes τ .

Si $P \xrightarrow[\tilde{b}]{\tau} P_1 \xrightarrow[\tilde{b}]{a, R} P_2 \xrightarrow[\tilde{b}]{\tau} P'$, alors par le premier résultat il existe Q_1 tel que $Q \xrightarrow[\tilde{b}]{\tau} Q_1$ et $P_1 \approx_m Q_1$. Par bisimilarité il existe Q_2 tel que $Q_1 \xrightarrow[\tilde{b}]{a, R} Q_2$ et $P_2 \approx_m Q_2$. Enfin par le premier résultat il existe Q' tel que $Q_2 \xrightarrow[\tilde{b}]{\tau} Q'$ et $P' \approx_m Q'$. Au final nous avons donc $Q \xrightarrow[\tilde{b}]{a, R} Q'$ comme souhaité.

Si $P \xrightarrow[\tilde{b}]{\tau} P_1 \xrightarrow[\tilde{b}]{\bar{a}, R', \mathbb{E}} P'$ avec $R \xrightarrow[\tilde{b}]{\tau} R'$, alors par le premier résultat il existe Q_1 tel que $Q \xrightarrow[\tilde{b}]{\tau} Q_1$ et $P_1 \approx_m Q_1$. Par bisimilarité il existe R'', Q_2 tels que $R \xrightarrow[\tilde{b}]{\tau} R''$, $Q_1 \xrightarrow[\tilde{b}]{\tau, \bar{a}, R'', \mathbb{E}} Q_2$ et $P_2 \approx_m Q_2$. Par le premier résultat il existe Q' tel que $Q_2 \xrightarrow[\tilde{b}]{\tau} Q'$ et $P' \approx_m Q'$. Nous avons donc $Q \xrightarrow[\tilde{b}]{\tau, \bar{a}, R', \mathbb{E}} Q'$, c'est-à-dire $Q \xrightarrow[\tilde{b}]{\tau, \bar{a}, R, \mathbb{E}} Q'$ comme souhaité. La preuve est similaire pour $P \xrightarrow[\tilde{b}]{\tau, \bar{a}, R', \mathbb{E}} P'$ en remplaçant l'utilisation de la bisimilarité par le lemme A.20. \square

Lemme A.22. Si $P \approx_m^\bullet Q$, alors $\text{fn}(P) = \text{fn}(Q)$.

Démonstration. Par induction sur la dérivation de $P \approx_m^\bullet Q$.

Soient $P \approx_m^\circ Q$ et σ la substitution qui clôt P et Q avec des processus $\mathbf{0}$. Nous avons $P\sigma \approx_m Q\sigma$, donc $\text{fn}(P\sigma) = \text{fn}(Q\sigma)$, donc $\text{fn}(P) = \text{fn}(Q)$.

Si $P \approx_m^\bullet R \approx_m^\circ Q$, alors nous avons $\text{fn}(P) = \text{fn}(R)$ par induction, et en utilisant la même technique que pour le premier cas, nous avons $\text{fn}(R) = \text{fn}(Q)$.

Si $P = \text{op}(\tilde{P})$ et $Q = \text{op}(\tilde{Q})$ avec $\tilde{P} \approx_m^\bullet \tilde{Q}$, alors par induction nous avons $\widetilde{\text{fn}(\tilde{P})} = \widetilde{\text{fn}(\tilde{Q})}$. Nous vérifions alors facilement opérateur par opérateur que nous avons $\text{fn}(P) = \text{fn}(Q)$. \square

Lemme A.23. Si $P \xrightarrow[\tilde{b}]{a, R} P'$, pour tout $R \approx_m^\bullet R'$, il existe P'' tel que $P \xrightarrow[\tilde{b}]{a, R'} P''$ et $P' \approx_m^\bullet P''$.

Soient $P (\approx_m)_c^\bullet Q$. Si $P \xrightarrow[\tilde{b}]{a, R} P'$, pour tout $R (\approx_m)_c^\bullet R'$, il existe Q' tel que $Q \xrightarrow[\tilde{b}]{a, R'} Q'$ et $P' (\approx_m)_c^\bullet Q'$.

Démonstration. Similaire à celle du lemme A.8. \square

Lemme A.24. Si $\mathbb{E} \approx_m^\bullet \mathbb{F}$, $\mathbb{E}' \approx_m^\bullet \mathbb{F}'$ et $P \approx_m^\bullet Q$, alors nous avons $\mathbb{E}\{\mathbb{E}'\} \approx_m^\bullet \mathbb{F}\{\mathbb{F}'\}$ et $\mathbb{E}\{P\} \approx_m^\bullet \mathbb{F}\{Q\}$.

Démonstration. Facile par induction sur $\mathbb{E} \approx_m^\bullet \mathbb{F}$. \square

Corollaire A.1. Si $\mathbb{E} \approx_m^\bullet \mathbb{F}$ et $P \approx_m^\bullet Q$, alors nous avons $\mathbb{E}\{\nu a.\square\} \approx_m^\bullet \mathbb{F}\{\nu a.\square\}$, $\mathbb{E}\{a[\square]\} \approx_m^\bullet \mathbb{F}\{a[\square]\}$, $\mathbb{E}\{\square \mid P\} \approx_m^\bullet \mathbb{F}\{\square \mid Q\}$ et $\mathbb{E}\{\square \mid !P\} \approx_m^\bullet \mathbb{F}\{\square \mid !Q\}$.

Lemme A.25. Si $\mathbb{E} \approx_m^\bullet \mathbb{F}$, alors $\text{bn}(\mathbb{E}) = \text{bn}(\mathbb{F})$.

Démonstration. Facile par induction sur $\mathbb{E} \approx_m^\bullet \mathbb{F}$. \square

Lemme A.26. Si $P \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} P'$, $R (\approx_m)_c^\bullet R'$ et $\mathbb{E} (\approx_m)_c^\bullet \mathbb{F}$, alors il existe R'', P'' tels que $R' \xRightarrow{\tau} R''$, $P \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} P''$ et $P' (\approx_m)_c^\bullet P''$.

Démonstration. Par induction sur la dérivation de $P \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} P'$.

Si la règle utilisée est OUT_o^p , nous avons $P = \bar{a}\langle P_1 \rangle P_2 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} R_1 \mid \mathbb{E}\{P_2\} = P'$ avec $R \xrightarrow{a, P_1} R_1$. Par le lemme A.23, il existe R'', R'_1, R'_2 tels que $R' \xRightarrow{\tau} R'' \xrightarrow{a, P_1} R'_2 \xRightarrow{\tau} R'_1$ et $R_1 (\approx_m)_c^\bullet R'_1$. Par la règle OUT_o^p nous avons $P \xrightarrow[\sim]{\bar{a}, R'', \mathbb{F}} R'_2 \mid \mathbb{F}\{P_2\}$, donc nous avons $P \xrightarrow[\sim]{\bar{a}, R'', \mathbb{F}} R'_1 \mid \mathbb{F}\{P_2\} \triangleq P''$. Par congruence de \approx_m^\bullet et le lemme A.24, nous avons $P' (\approx_m)_c^\bullet P''$. Le cas de la règle PASSIV_o^p se traite de la même manière.

Si la dernière règle est PAR_o^p , nous avons $P = P_1 \mid P_2$ avec $P_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}\{\square \mid P_2\}} P'$. Par le corollaire A.1 nous avons $\mathbb{E}\{\square \mid P_2\} (\approx_m)_c^\bullet \mathbb{F}\{\square \mid P_2\}$, donc par induction il existe R'', P'' tels que $R' \xRightarrow{\tau} R''$, $P_1 \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}\{\square \mid P_2\}} P''$ et $P' (\approx_m)_c^\bullet P''$. En utilisant la règle $\text{PAR}_{i\tau}^p$ pour les τ -actions et PAR_o^p pour l'émission, nous avons $P \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} P''$, comme voulu. Les règles LOC_o^p , RESTR_o^p et REPLIC_o^p se traitent de la même manière.

Si la dernière règle utilisée est EXTR_o^p , nous avons $P = \nu c.P_1$ avec $P_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} P'_1$, $c \in \tilde{b}$ et $P' = \nu c.P'_1$. Par induction il existe R'', P''_1 tels que $R' \xRightarrow{\tau} R''$, $P_1 \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} P''_1$ et $P'_1 (\approx_m)_c^\bullet P''_1$. Par les règles $\text{RESTR}_{i\tau}^p$ (pour les τ -actions) et EXTR_o^p (pour l'émission), nous avons $P \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} \nu c.P''_1 \triangleq P''$. Par congruence de $(\approx_m)_c^\bullet$ nous avons $P' (\approx_m)_c^\bullet P''$, comme souhaité. \square

Lemme A.27. Si $P (\approx_m)_c^\bullet Q$, alors pour tout $P \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} P'$, $R (\approx_m)_c^\bullet R'$ et $\mathbb{E} (\approx_m)_c^\bullet \mathbb{F}$, il existe R'', Q' tels que $R' \xRightarrow{\tau} R''$, $Q \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} Q'$ et $P' (\approx_m)_c^\bullet Q'$.

Démonstration. Par induction sur la taille de la dérivation de $P (\approx_m)_c^\bullet Q$.

Supposons $P \approx_m^\circ Q$; comme P et Q sont clos, nous avons $P \approx_m Q$. Par le lemme A.26, il existe R_1, P'' tels que $R' \xRightarrow{\tau} R_1$ et $P \xRightarrow[\sim]{\bar{a}, R_1, \mathbb{F}} P''$. Par le lemme A.21, il existe R'', Q' tel que $Q \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} Q'$ et $P' \approx_m^\bullet Q'$. Les processus impliqués sont clos donc nous avons $P' (\approx_m)_c^\bullet Q'$ comme souhaité.

Supposons $P \approx_m^\bullet T \approx_m^\circ Q$. Soit σ une substitution qui clôt T ; nous avons $P (\approx_m)_c^\bullet T\sigma$ par le lemme A.2. Par induction, il existe R_1, T' tels que $R' \xRightarrow{\tau} R_1$, $T\sigma \xRightarrow[\sim]{\bar{a}, R_1, \mathbb{F}} T' \xRightarrow{\tau} T'$ et $P' (\approx_m)_c^\bullet T'$. Nous avons $T\sigma \approx_m Q$, donc par le lemme A.21, il existe R'', Q' tels que $R' \xRightarrow{\tau} R''$, $Q \xRightarrow[\sim]{\bar{a}, R'', \mathbb{F}} Q'$ et $P' \approx_m^\bullet Q'$. Nous avons $P' (\approx_m)_c^\bullet T' \approx_m Q'$, et comme les processus sont clos nous avons $P' (\approx_m)_c^\bullet Q'$ comme voulu.

Supposons $P = \text{op}(\tilde{P}_i)$ et $Q = \text{op}(\tilde{Q}_i)$ avec $\tilde{P}_i (\approx_m)_c^\bullet \tilde{Q}_i$. Par analyse de cas sur op :

- Si $P = \bar{a}\langle P_1 \rangle P_2$ et $Q = \bar{a}\langle Q_1 \rangle Q_2$, nous avons $P \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} R_1 \mid \mathbb{E}\{P_2\} = P'$ avec $R \xRightarrow{\tau} R_1$, $\text{fn}(P_1) = \tilde{b}$ et $\text{bn}(\mathbb{E}) \cap \tilde{b} = \emptyset$. Par le lemme A.25, nous avons $\text{bn}(\mathbb{E}) = \text{bn}(\mathbb{F})$, et par le lemme A.22, nous avons $\text{fn}(P_1) = \text{fn}(Q_1)$. Nous avons donc $\text{fn}(Q_1) = \tilde{b}$ et $\text{bn}(\mathbb{F}) \cap \tilde{b} = \emptyset$. Par le lemme A.23, il existe R'', R'_1 tels que $R' \xRightarrow{\tau} R'' \xrightarrow{a, Q_1} R'_1$. Par

les règles OUT_o^p et $\text{PAR}_{i\tau}^p$, nous avons $Q \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{F}}^{\tau} R'_1 \mid \mathbb{F}\{Q_2\} \stackrel{\Delta}{=} Q'$. Par le lemme A.24 et par congruence de $(\approx_m)_c^\bullet$, nous avons $P' (\approx_m)_c^\bullet Q'$ comme voulu. Le cas de la passivation (règle PASSIV_o^p) se traite de la même manière.

- Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, nous avons $P_1 \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}\{\square \mid P_2\}} P'$. Par le corollaire A.1, nous avons $\mathbb{E}\{\square \mid P_2\} (\approx_m)_c^\bullet \mathbb{F}\{\square \mid Q_2\}$, donc par induction il existe R'', Q' tels que $R' \xrightarrow{\tau} R'', Q_1 \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{F}\{\square \mid Q_2\}}^{\tau} Q'$ et $P' (\approx_m)_c^\bullet Q'$. Par les règles $\text{PAR}_{i\tau}^p$ et PAR_o^p nous avons $Q \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{F}}^{\tau} Q'$ et $P' (\approx_m)_c^\bullet Q'$, comme souhaité. Les règles LOC_o^p , REPLIC_o^p et RESTR_o^p se traitent de la même manière.
- Si $P = \nu c.P_1$ et $Q = \nu c.Q_1$ et que la transition de P vient de la règle EXTR_o^p , nous avons $P_1 \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'_1$, $c \in \tilde{b}$ et $P' = \nu c.P'_1$. Par induction il existe R'', Q'_1 tels que $R' \xrightarrow{\tau} R'', Q_1 \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{F}}^{\tau} Q'_1$ et $P'_1 (\approx_m)_c^\bullet Q'_1$. Par les règles $\text{RESTR}_{i\tau}^p$ et EXTR_o^p , nous avons $Q \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{F}}^{\tau} Q'$, et nous avons $P' (\approx_m)_c^\bullet Q'$ par congruence de $(\approx_m)_c^\bullet$. \square

Lemme A.28. Si $\mathbb{E} \approx_m^\bullet \mathbb{F}$ et $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, il existe $\mathbb{F}_1, \mathbb{F}_2$ tels que $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$, $\mathbb{E}_1 \approx_m^\bullet \mathbb{F}_1$ et $\mathbb{E}_2 \approx_m^\bullet \mathbb{F}_2$.

Démonstration. Facile par induction sur $\mathbb{E} \approx_m^\bullet \mathbb{F}$. \square

Lemme A.29. Soient $P (\approx_m)_c^\bullet Q$. Si $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'$, $R (\approx_m)_c^\bullet R'$ et $\mathbb{E} (\approx_m)_c^\bullet \mathbb{F}$, il existe Q' tel que $Q \xrightarrow[\tilde{b}]{\bar{a}, R', \mathbb{F}}^{\tau} Q'$ et $P' (\approx_m)_c^\bullet Q'$.

Démonstration. Par induction sur le nombre de noms de l'ensemble $\text{bn}(\mathbb{E}) \cap \tilde{b}$.

Si ce nombre est nul, la transition de P provient de la règle CFREE_o^p . Nous avons donc $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}} P'$. Par le lemme A.27 il existe R'', Q' tels que $R' \xrightarrow{\tau} R'', Q \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{E}}^{\tau} Q'$ et $P' (\approx_m)_c^\bullet Q'$. Par la règle CFREE_o^p nous avons $Q \xrightarrow[\tilde{b}]{\bar{a}, R'', \mathbb{E}}^{\tau} Q'$, nous avons donc $Q \xrightarrow[\tilde{b}]{\bar{a}, R', \mathbb{F}}^{\tau} P'$.

Sinon, la dérivation provient de la règle CAPT_o^p . Nous avons $P \xrightarrow[\tilde{b}]{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}} P'_1$ avec $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, $c \in \tilde{b}$ et $P' = \nu c.P_1$. Par le lemme A.28, il existe $\mathbb{F}_1, \mathbb{F}_2$ tels que $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$, $\mathbb{E}_1 (\approx_m)_c^\bullet \mathbb{F}_1$ et $\mathbb{E}_2 (\approx_m)_c^\bullet \mathbb{F}_2$. Par le lemme A.24, nous avons $\mathbb{E}_1\{\mathbb{E}_2\} (\approx_m)_c^\bullet \mathbb{F}_1\{\mathbb{F}_2\}$, donc par induction il existe Q'_1 tel que $Q \xrightarrow[\tilde{b}]{\bar{a}, R', \mathbb{F}_1\{\mathbb{F}_2\}}^{\tau} Q'_1$ et $P'_1 (\approx_m)_c^\bullet Q'_1$. Par la règle CAPT_o^p nous avons $Q \xrightarrow[\tilde{b}]{\bar{a}, R', \mathbb{F}}^{\tau} \nu c.Q'_1 \stackrel{\Delta}{=} Q'$ et nous avons $P' (\approx_m)_c^\bullet Q'$ par congruence de \approx_m^\bullet . \square

Lemme A.30. Soient $P (\approx_m)_c^\bullet Q$. Si $P \xrightarrow{\tau} P'$, alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' (\approx_m)_c^\bullet Q'$.

Démonstration. Par induction sur la taille de la dérivation de $P (\approx_m)_c^\bullet Q$.

Supposons $P \approx_m^\circ Q$; comme les processus sont clos, nous avons $P \approx_m Q$. Le résultat est vrai par bisimilarité.

Supposons $P \approx_m^\bullet T \approx_m^\circ Q$. Soit σ une substitution qui clôt T ; nous avons $P (\approx_m)_c^\bullet T\sigma$ par le lemme A.2. Par induction, il existe T' tel que $T\sigma \xrightarrow{\tau} T'$ et $P' (\approx_m)_c^\bullet T'$. Nous avons $T\sigma \approx_m Q$, donc par le lemme A.21, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \approx_m^\bullet Q'$. Nous avons $P' (\approx_m)_c^\bullet T' \approx_m Q'$, et comme les processus sont clos nous avons $P' (\approx_m)_c^\bullet Q'$ comme voulu.

Supposons $P = \text{op}(\tilde{P}_i)$ et $Q = \text{op}(\tilde{Q}_i)$ avec $\tilde{P}_i \approx_m^\bullet \tilde{Q}_i$. Nous procédons par analyse de cas sur op . Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, la transition de P peut provenir des règles $\text{PAR}_{i\tau}^p$ et HO_τ^p et de leur symétrique. Dans le cas de la règle HO_τ^p , nous avons $P_1 \xrightarrow[\tilde{b}]{\bar{a}, P_2, \square} P'$.

Par le lemme A.29, il existe Q'_2, Q' tels que $Q_2 \xrightarrow{\tau} Q'_2$, $Q_1 \xrightarrow{\tau} \xrightarrow{\bar{a}, Q'_2, \mathbb{E}} \xrightarrow{\tau} Q'$ et $P' (\approx_m)_c^\bullet Q'$. Nous avons $Q \xrightarrow{\tau} Q_1 \mid Q'_2 \xrightarrow{\tau} Q'$ par les règles $\text{PAR}_{i\tau}^p$ et HO_τ^p , le résultat est donc vrai.

Si la transition provient de la règle $\text{PAR}_{i\tau}^p$, nous avons $P_1 \xrightarrow{\tau} P'_1$ et $P' = P'_1 \mid P_2$. Par induction il existe Q'_1 tel que $Q_1 \xrightarrow{\tau} Q'_1$ et $P'_1 (\approx_m)_c^\bullet Q'_1$. Par la règle $\text{PAR}_{i\tau}^p$ nous avons $Q \xrightarrow{\tau} Q'_1 \mid Q_2 \xrightarrow{\tau} Q'$, et comme $(\approx_m)_c^\bullet$ est une congruence, nous avons $P' (\approx_m)_c^\bullet Q'$ comme voulu. Les règles $\text{RESTR}_{i\tau}^p$, $\text{REPLIC}_{i\tau}^p$ et $\text{LOC}_{i\tau}^p$ se traitent de la même manière. \square

Lemme A.31. *If $P (\approx_m)_c^\bullet Q$ et $P \xRightarrow{\lambda} P'$, il existe Q' tel que $Q \xRightarrow{\lambda} Q'$ et $P' (\approx_m)_c^\bullet Q'$.*

Démonstration. Similaire à celle du lemme A.21, en utilisant les lemmes A.23, A.29 et A.30. \square

Lemme A.32. *La relation $(\approx_m)_c^{\bullet*}$ est une bisimulation faible à complément.*

Démonstration. Par le lemme A.4, $(\approx_m)_c^{\bullet*}$ est symétrique, et le lemme A.31 permet de montrer que $(\approx_m)_c^{\bullet*}$ est une simulation faible à complément, \square

Théorème A.2. *La relation \approx_m est une congruence.*

Démonstration. Immédiat par les lemmes A.32 et A.5. \square

A.3.3 Correspondance des bisimilarités

Lemme A.33. *Soient $P \approx Q$, $P \xrightarrow{\bar{a}} C$, F une fonction, et $Q \xrightarrow{\bar{a}} C$ tel que pour tout \mathbb{E} , il existe Q' tel que $F \bullet \mathbb{E}\{C'\} \xrightarrow{\tau} Q'$ et $F \bullet \mathbb{E}\{C\} \approx Q'$. Nous avons $\text{extr}(C) = \text{extr}(C')$.*

Démonstration. Soient $b, e \notin \text{fn}(P, Q)$. Pour deux ensembles de noms deux-à-deux distincts \tilde{c}_i, \tilde{d}_i de même taille, nous définissons

$$\mathbb{E}_{\tilde{c}_i, \tilde{d}_i} \triangleq \nu b e. b[\nu \tilde{c}_i. e[\Box] \mid e(Y)(\prod_i c_i. \mathbf{0} \mid \bar{c}_i. \bar{c}_i. d_i. \mathbf{0})] \mid b(Z)Z \mid Z$$

Si la portée d'un nom c_{i_0} est étendue hors de b , après passivation de e et duplication du contenu de b , la double synchronisation sur c_{i_0} devient possible et le nom d_{i_0} devient observable. Si d_{i_0} devient observable, la passivation sur e a été déclenchée, et une synchronisation sur c_{i_0} était possible. Comme la passivation détruit toute éventuelle occurrence de c_{i_0} contenue dans e , cette synchronisation n'est possible que si la portée de c_{i_0} est étendue hors de b avant la duplication du contenu de b . Le nom d_{i_0} devient donc observable ssi la portée de c_{i_0} est étendue hors de b .

Soit \tilde{d}_i un ensemble de noms deux-à-deux disjoints de même taille que $\text{extr}(C)$, et tel que $\tilde{d}_i \cap \text{fn}(P, Q, F) = \emptyset$. Soit $P' \triangleq F \bullet \mathbb{E}_{\text{extr}(C), \tilde{d}_i}\{C\}$. Il existe Q' tel que $F \bullet \mathbb{E}_{\text{extr}(C), \tilde{d}_i}\{C'\} \xrightarrow{\tau} Q'$ et $P' \approx Q'$. Soit $c_{i_0} \in \text{extr}(C)$; par définition, la portée de c_{i_0} est étendue hors de b dans P' , donc d_{i_0} devient observable dans P' . Comme $P' \approx Q'$, d_{i_0} devient observable également dans Q' , ce qui est possible seulement si la portée de c_{i_0} est étendue hors de b dans Q' , c'est-à-dire seulement si $c_{i_0} \in \text{extr}(C')$. Nous avons donc $\text{extr}(C) \subseteq \text{extr}(C')$. Réciproquement, soit \tilde{d}_i un ensemble de noms deux-à-deux disjoints de même taille que $\text{extr}(C')$, et tel que $\tilde{d}_i \cap \text{fn}(P, Q, F) = \emptyset$. Soit $P' \triangleq F \bullet \mathbb{E}_{\text{extr}(C'), \tilde{d}_i}\{C\}$. Il existe Q' tel que $F \bullet \mathbb{E}_{\text{extr}(C'), \tilde{d}_i}\{C'\} \xrightarrow{\tau} Q'$ et $P' \approx Q'$. En raisonnant sur les observables faibles de Q' , nous pouvons montrer de la même manière que nous avons $\text{extr}(C') \subseteq \text{extr}(C)$. \square

Lemme A.34. *Si $P \approx Q$, alors $P \approx_m Q$.*

Démonstration. Nous montrons d'abord que \approx est une bisimulation faible à complément. Nous avons $\text{fn}(P) = \text{fn}(Q)$ par définition.

Si $P \xrightarrow{\tau} P'$, alors nous avons $P \xrightarrow{\tau} P'$ par le lemme A.18. Par définition il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \approx Q'$. Nous avons $Q \xrightarrow{\tau} Q'$ par le lemme A.19.

Si $P \xrightarrow{a,R} P'$, alors il existe F telle que $P \xrightarrow{a} F$ et $P' = F \circ R$ par le lemme A.15. Par définition il existe F', Q' tels que $Q \xrightarrow{a} F'$, $F' \circ R \equiv F' \circ \langle R \rangle \mathbf{0} \xrightarrow{\tau} Q'$ et $F \bullet \langle R \rangle \mathbf{0} \approx Q'$. Par le lemme A.19 nous avons $Q \xrightarrow{a,R} Q'$ comme souhaité.

Si $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$, alors il existe F, C tels que $P \xrightarrow{\bar{a}} C$, $R \xrightarrow{a} F$, $\tilde{b} = \text{extr}(C)$ et $P' = F \bullet \mathbb{E}\{C\}$. Par définition il existe C', Q' tels que $Q \xrightarrow{\bar{a}} C'$, $F \bullet \mathbb{E}\{C'\} \xrightarrow{\tau} Q'$ et $F \bullet \mathbb{E}\{C'\} \approx Q'$. Par le lemme A.33, nous avons $\text{extr}(C') = \text{extr}(C) = \tilde{b}$, donc par le lemme A.19, nous avons $Q \xrightarrow{\bar{a},R,\mathbb{E}} Q'$ comme voulu. □

A.3.4 Complétude

Nous prouvons la complétude de \approx_m , le schéma de preuve est semblable dans le cas fort.

Définition A.2. *Nous définissons la suite de relation $(\approx_m^k)_{k \geq 0}$ par :*

- nous avons $P \approx_m^0 Q$ ssi $\text{fn}(P) = \text{fn}(Q)$;
- nous avons $P \approx_m^{k+1} Q$ ssi $\text{fn}(P) = \text{fn}(Q)$ et pour tout $P \xrightarrow{\lambda} P'$, il existe Q' tel que $Q \xrightarrow{\lambda} Q'$ et $P' \approx_m^k Q'$, et réciproquement pour $Q \xrightarrow{\lambda} Q'$.

La relation \approx_m^ω est définie par $\approx_m^\omega \triangleq \bigcap_{k \in \mathbb{N}} \approx_m^k$.

Notez que par définition, nous avons $\approx_{k+1} \subseteq \approx_k$ pour tout k .

Lemme A.35. *Nous avons $\approx_m = \approx_m^\omega$ sur les processus à image finie.*

Démonstration. Par définition de \approx_m^ω , nous avons $\approx_m \subseteq \approx_m^\omega$. Nous prouvons l'inclusion inverse sur les processus à image finie en montrant que \approx_m^ω est une bisimulation contextuelle précoce faible.

Supposons $P \xrightarrow{\lambda} P'$. Pour tout k , il existe Q'_k tel que $Q \xrightarrow{\lambda} Q'_k$ et $P' \approx_m^k Q'_k$. Comme Q est à image finie, il existe Q' tel que $Q \xrightarrow{\lambda} Q'$ et $Q' = Q_k$ pour une infinité de k . Nous avons donc $P' \approx_m^k Q'$ pour une infinité de k , donc nous avons $P' \approx_m^\omega Q'$. □

Lemme A.36. *Pour tout $R \xrightarrow{a,P} R''$, il existe $\mathbb{E}, a(X)R'$ tels que $R = \mathbb{E}\{a(X)R'\}$, $R'' = \mathbb{E}\{R'\{P/X\}\}$.*

Démonstration. Immédiat par induction sur R . □

Le résultat suivant permet d'ajouter des observables à une transition $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$.

Lemme A.37. *Pour tout $P \xrightarrow{\bar{a},R,\mathbb{E}} P'$, il existe $R_c = \mathbb{F}\{R'\} \mid \bar{c}.\mathbf{0}$ tel que*

- $R = \mathbb{F}\{a(X)R'\}$;
- nous avons $P \xrightarrow{\bar{a},a(X)R_c,\mathbb{E}} P' \mid \bar{c}.\mathbf{0}$;
- pour tout Q tel que $Q \xrightarrow{\bar{a},R,\mathbb{E}} Q'$, il existe Q', Q_c tels que $Q \xrightarrow{\bar{a},a(X)R_c,\mathbb{E}} Q_c$, $Q \xrightarrow{\bar{a},R,\mathbb{E}} Q'$ et $Q_c \equiv Q' \mid \bar{c}.\mathbf{0}$.

Démonstration. Nous prouvons l'existence de R' et la première propriété par induction sur $P \xrightarrow{\bar{a}, R, \mathbb{E}}_b P'$. Si la règle utilisée est CFREE_o^p , nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}}_b P'$; nous montrons par induction sur la dérivation de $P \xrightarrow{\bar{a}, R, \mathbb{E}}_b P'$ qu'il existe R_c tel que $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b \equiv P' \mid \bar{c}.0$

Si la règle utilisée est OUT_o^p , nous avons $P = \bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, R, \mathbb{E}}_b R_1 \mid \mathbb{E}\{P_2\} = P'$ avec $R \xrightarrow{a, P_1} R_1$. Il existe $\mathbb{F}, a(X)R'$ tels que $R = \mathbb{F}\{a(X)R'\}$ et $R_1 = \mathbb{F}\{R'\{P_1/X\}\}$. Nous définissons $R_c = \mathbb{F}\{R'\} \mid \bar{c}.0$. Nous avons $a(X)R_c \xrightarrow{a, P_1} R_1 \mid \bar{c}.0$, donc nous avons $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b R_1 \mid \bar{c}.0 \mid \mathbb{E}\{P_2\} \equiv P' \mid \bar{c}.0$, comme souhaité. La règle PASSIV_o^p se traite de la même manière.

Si la règle utilisée est PAR_o^p , nous avons $P = P_1 \mid P_2 \xrightarrow{\bar{a}, R, \mathbb{E}}_b P'$ avec $P_1 \xrightarrow{\bar{a}, R, \mathbb{E}\{\square \mid P_2\}}_b P'$. Par induction il existe R_c tel que $P_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}\{\square \mid P_2\}}_b \equiv P' \mid c.0$. Nous avons donc $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b \equiv P' \mid \bar{c}.0$, le résultat est vrai. Les règles RESTR_o^p , REPLIC_o^p et LOC_o^p se traitent de la même manière.

Si la règle utilisée est EXTR_o^p , nous avons $P = \nu d.P_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_b \nu d.P'_1 = P'$ avec $P_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_b P'_1$. Par induction il existe R_c tel que $P_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b \equiv P'_1 \mid \bar{c}.0$. Nous avons $P \xrightarrow{\bar{a}, R_c, \mathbb{E}}_b \equiv \nu d.(P'_1 \mid \bar{c}.0) \equiv (\nu d.P'_1) \mid \bar{c}.0 = P' \mid \bar{c}.0$, le résultat est vrai.

Le résultat intermédiaire étant prouvé, nous revenons à l'induction principale. Il existe donc R_c tel que $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b \equiv P' \mid \bar{c}.0$, donc nous avons $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b \equiv P' \mid c.0$ par la règle CFREE_o^p .

Si la règle est CAPT_o^p , nous avons $P \xrightarrow{\bar{a}, R, \mathbb{E}_1\{\nu d.\mathbb{E}_2\}}_b \nu d.P'_1 = P'$ avec $P \xrightarrow{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}}_b P'_1$. Par induction, il existe R_c tel que $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}_1\{\mathbb{E}_2\}}_b \equiv P'_1 \mid \bar{c}.0$. Par la règle CAPT_o^p , nous avons $P \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}_1\{\nu d.\mathbb{E}_2\}}_b \equiv \nu d.(P'_1 \mid \bar{c}.0) \equiv (\nu d.P'_1) \mid \bar{c}.0 = P' \mid \bar{c}.0$, comme souhaité.

Soit Q tel que $Q \xrightarrow{\bar{a}, R, \mathbb{E}}_b$; par définition il existe R_1, Q_1 tels que $R \xrightarrow{\tau} R_1$ et $Q \xrightarrow{\tau} Q_1 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b \xrightarrow{\tau}$. Nous montrons par induction sur $Q_1 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b$ qu'il existe Q', Q'_c tels que $Q_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b Q'_c$, $Q_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_b Q'$ et $Q_c \equiv Q' \mid \bar{c}.0$.

Si que la transition provient CFREE_o^p , nous avons $Q \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b$. Nous montrons par induction sur $Q_1 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b$ qu'il existe Q', Q'_c tels que $Q_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b Q'_c$, $Q_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_b Q'$ et $Q_c \equiv Q' \mid \bar{c}.0$.

Si la règle utilisée est OUT_o^p , nous avons $Q_1 = \bar{a}\langle Q^1 \rangle Q^2 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b R'_1 \mid \mathbb{E}\{Q^2\}$ avec $R_1 \xrightarrow{a, Q^1} R'_1$. Nous avons $R_c = \mathbb{F}\{R'\} \mid \bar{c}.0$ et $R = \mathbb{F}\{a(X)R'\}$, donc nous avons $a(X)R_c \xrightarrow{a, Q^1} R'_c$ et $R \xrightarrow{a, Q^1} R''$ avec $R'_c = R'' \mid \bar{c}.0$. Nous avons donc $Q_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b R'_c \mid \mathbb{E}\{Q^2\} \triangleq Q_c$ et $Q_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_b R'' \mid \mathbb{E}\{Q^2\} \triangleq Q'$. Nous avons bien $Q_c \equiv Q' \mid \bar{c}.0$ comme souhaité. La règle PASSIV_o^p se traite de la même manière.

Si la règle utilisée est PAR_o^p , nous avons $Q_1 = Q^1 \mid Q^2 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b$ avec $Q^1 \xrightarrow{\bar{a}, R_1, \mathbb{E}\{\square \mid P_2\}}_b$. Par induction il existe Q', Q_c tels que $Q_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}\{\square \mid Q^2\}}_b Q_c$, $Q_1 \xrightarrow{\bar{a}, R, \mathbb{E}\{\square \mid Q^2\}}_b Q'$ et $Q_c \equiv Q' \mid \bar{c}.0$. Nous avons $Q \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b Q_c$ et $Q \xrightarrow{\bar{a}, R, \mathbb{E}}_b Q'$, le résultat est donc vrai. Les règles RESTR_o^p , LOC_o^p et REPLIC_o^p se traitent de la même manière.

Si la règle utilisée est EXTR_o^p , nous avons $Q_1 = \nu d.Q^1 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_{b \setminus d}$ avec $Q^1 \xrightarrow{\bar{a}, R_1, \mathbb{E}}_b$. Par induction il existe Q_c^1, Q'^1 tels que $Q_1 \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_b Q_c^1$ et $Q_1 \xrightarrow{\bar{a}, R, \mathbb{E}}_b Q'^1$ avec $Q_c^1 \equiv Q'^1 \mid \bar{c}.0$. Nous avons donc $Q \xrightarrow{\bar{a}, a(X)R_c, \mathbb{E}}_{b \setminus d} \nu d.Q_c^1 \triangleq Q_c$ et $Q \xrightarrow{\bar{a}, R, \mathbb{E}}_{b \setminus d} \nu d.Q'^1 \triangleq Q'$. Nous avons $Q_c \equiv \nu d.Q_c^1 \equiv \nu d.(Q'^1 \mid \bar{c}.0) \equiv (\nu d.Q'^1) \mid \bar{c}.0 = Q' \mid \bar{c}.0$, le résultat est donc vrai.

Le résultat intermédiaire étant prouvé, nous revenons à l'induction principale. Il existe

donc Q', Q'_c tels que $Q_1 \xrightarrow[\sim]{\bar{a}, a(X)R_c, \mathbb{E}} Q'_c$, $Q_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} Q'$ et $Q_c \equiv Q' \mid \bar{c}.0$. Par la règle CFREE_o^p , nous avons $Q_1 \xrightarrow[\sim]{\bar{a}, a(X)R_c, \mathbb{E}} Q'_c$ et $Q_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} Q'$, le résultat est donc vrai.

Si la transition provient de la règle CAPT_o^p , nous avons $Q \xrightarrow[\sim]{\bar{a}, R_1, \mathbb{E}} Q'$ avec $Q \xrightarrow[\sim]{\bar{a}, R_1, \mathbb{E}_1\{\mathbb{E}_2\}} Q'$ et $\mathbb{E} = \mathbb{E}_1\{\nu d.\mathbb{E}_2\}$. Par induction, il existe Q'', Q'_c tels que $Q_1 \xrightarrow[\sim]{\bar{a}, a(X)R_c, \mathbb{E}_1\{\mathbb{E}_2\}} Q'_c$, $Q_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}_1\{\mathbb{E}_2\}} Q''$ et $Q'_c \equiv Q'' \mid \bar{c}.0$. Par la règle CAPT_o^p , nous avons $Q_1 \xrightarrow[\sim]{\bar{a}, a(X)R_c, \mathbb{E}} \nu d.Q'_c \triangleq Q'_c$ et $Q_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} \nu d.Q'' \triangleq Q'$. Nous avons $Q'_c \equiv \nu d.(Q'' \mid \bar{c}.0) \equiv (\nu d.Q'') \mid \bar{c}.0 = Q' \mid \bar{c}.0$, comme souhaité.

L'induction étant prouvée, il existe Q', Q'_c tels que $Q_1 \xrightarrow[\sim]{\bar{a}, a(X)R_c, \mathbb{E}} Q'_c$, $Q_1 \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} Q'$ et $Q_c \equiv Q' \mid \bar{c}.0$. Nous avons $Q \xrightarrow[\sim]{\tau, \bar{a}, a(X)R_c, \mathbb{E}} Q'_c$ et $Q \xrightarrow[\sim]{\tau, \bar{a}, R, \mathbb{E}} Q'$, c'est-à-dire $Q \xrightarrow[\sim]{\bar{a}, a(X)R_c, \mathbb{E}} Q'_c$ et $Q \xrightarrow[\sim]{\bar{a}, R, \mathbb{E}} Q'$, comme voulu. \square

Dans la suite, nous omettons les 0 en fin de processus ; en particulier nous écrivons a pour le processus $a.0$. Nous définissons également un opérateur \oplus par :

$$\bigoplus_{j=1}^n P_j \triangleq \nu a.(\bar{a}\langle P_1 \rangle 0 \mid \dots \mid \bar{a}\langle P_n \rangle 0 \mid a(X)X \mid \prod_{j=2}^n a(X_j)0)$$

L'opérateur \oplus est un opérateur de choix ; une fois un processus P_i choisi (c'est-à-dire reçu par le processus $a(X)X$), le processus $\prod_{j=2}^n a(X_j)0$ détruit les processus P_j pour $j \neq i$. Cette opération est nécessaire pour supprimer les noms libres des $(P_j)_{j \neq i}$ du processus P' résultant, pour avoir $P' \approx_m P_i$.

L'opérateur \oplus a les propriétés suivantes :

- $P \oplus a \downarrow_a$;
- pour tout $i \in \{1 \dots n\}$, nous avons $\sum_{j=1}^n P_j \xrightarrow[\sim]{\tau} \approx_m P_i$.

Lemme A.38. Soit P, Q deux processus à image finie. Pour tout k , si $P \not\approx_m^k Q$, alors il existe \mathbb{C}, e tels que $\mathbb{C}\{P\} \oplus e \not\approx_b \mathbb{C}\{Q\} \oplus d$.

Démonstration. Nous procédons par induction sur k . Pour $k = 0$, nous avons $\text{fn}(P) \neq \text{fn}(Q)$: supposons que nous avons par exemple $a \in \text{fn}(P) \setminus \text{fn}(Q)$. Nous définissons :

$$\mathbb{C} \triangleq b[\nu a.(\bar{c}\langle \square \rangle 0 \mid a \mid \bar{a}.\bar{a}.d) \mid c(X)b(Y)(Y \mid Y)]$$

avec b, c, d non libres dans P et Q . Soit e un nom frais ; supposons $\mathbb{C}\{P\} \oplus e \approx_b \mathbb{C}\{Q\} \oplus e$. Par communication sur c , nous avons

$$\mathbb{C}\{P\} \oplus e \xrightarrow[\sim]{\tau} \nu a.(b[a \mid \bar{a}.\bar{a}.d] \mid b(Y)(Y \mid Y)) \triangleq P_1$$

Comme a est libre dans P , la portée de la restriction νa est étendue hors de b . Le processus P_1 a b comme observable mais pas c , cette transition ne peut donc être imitée que par

$$\mathbb{C}\{Q\} \oplus e \xrightarrow[\sim]{\tau} b[\nu a.R_a] \mid b(Y)(Y \mid Y) \triangleq Q_1$$

avec $R_a = a \mid \bar{a}.\bar{a}.d$ ou $R_a = \bar{a}.d$. Nous avons

$$P_1 \xrightarrow[\sim]{\tau} \nu a.(a \mid \bar{a}.\bar{a}.d \mid a \mid \bar{a}.\bar{a}.d) \triangleq P_2$$

par passivation de b . Comme b n'est plus observable dans P_2 , cette transition ne peut être imitée que par

$$Q_1 \xrightarrow[\sim]{\tau} (\nu a.R'_a) \mid (\nu a.R''_a) \triangleq Q_2$$

avec $R_a \xrightarrow{\tau} R'_a$ et $R_a \xrightarrow{\tau} R''_a$. La transition $P_2 \xrightarrow{\tau} \nu a.(d \mid \bar{a}.a.d)$ ne peut pas être imitée par Q_2 , étant donné que les processus R'_a et R''_a ont chacun leur copie de a et ne peuvent pas se synchroniser pour que d devienne observable. Nous avons une contradiction, donc $\mathbb{C} \oplus e$ différencie P et Q .

Supposons la proposition vraie pour tout $l \leq k$. Soit $P \approx_{k+1} Q$; nous distinguons trois cas.

Si $P \xrightarrow{\tau} P'$, alors pour tout Q' tel que $Q \xrightarrow{\tau} Q'$, nous avons $P' \not\approx_m^k Q'$. Comme Q est à image finie, l'ensemble $\{Q_i, Q \xrightarrow{\tau} Q_i\}$ est fini. Par induction il existe \mathbb{C}_i, e_i tels que $\mathbb{C}_i\{P'\} \oplus e_i \approx_b \mathbb{C}_i\{Q_i\} \oplus e_i$ pour tout i . Soit

$$\mathbb{C} \triangleq a[\square \mid a(X)(b \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j)$$

avec a, b frais pour P, Q . Soit e un nom frais. Supposons $\mathbb{C}\{P\} \oplus e \approx_b \mathbb{C}\{Q\} \oplus e$. Nous avons

$$\mathbb{C}\{P\} \oplus e \xrightarrow{\tau} \approx_m a[P'] \mid a(X)(b \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq P_1$$

Le processus P_1 a le nom a comme observable, mais pas t , cette transition ne peut être imitée que par

$$\mathbb{C}\{Q\} \oplus e \xrightarrow{\tau} \approx_m a[Q'_l] \mid a(X)(b \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq Q_1$$

pour un certain l . Nous avons

$$P_1 \xrightarrow{\tau} b \oplus \bigoplus_j \mathbb{C}_j\{P'\} \oplus e_j \triangleq P_2$$

Le nom b est observable dans P_2 , cette transition ne peut être imitée que par

$$Q_1 \xrightarrow{\tau} b \oplus \bigoplus_j \mathbb{C}_j\{Q'_j\} \oplus e_j \triangleq P_2$$

avec $Q'_l \xrightarrow{\tau} Q'_i$. Nous avons $P_2 \xrightarrow{\tau} \approx_m \mathbb{C}_i\{P'\} \oplus e_i \triangleq P_3$; comme $P_3 \downarrow_{e_i}$, cette transition ne peut être imitée que par $Q_2 \xrightarrow{\tau} \approx_m \mathbb{C}_i\{Q'_i\} \oplus e_i \triangleq Q_3$. Nous avons $\mathbb{C}_i\{P'\} \oplus e_i \not\approx_b \mathbb{C}_i\{Q'_i\} \oplus e_i$, d'où une contradiction.

Si $P \xrightarrow{a,R} P'$, alors pour tout Q' tel que $Q \xrightarrow{a,R} Q'$, nous avons $P' \not\approx_m^k Q'$. Comme Q est à image finie, l'ensemble $\{Q_i, Q \xrightarrow{a,R} Q_i\}$ est fini. Par induction il existe \mathbb{C}_i, e_i tels que $\mathbb{C}_i\{P'\} \oplus e_i \approx_b \mathbb{C}_i\{Q_i\} \oplus e_i$ pour tout i . Soit

$$\mathbb{C} \triangleq c[\square \mid \bar{a}(R)\bar{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j)$$

avec c, d, f non libres dans P, Q, R . Soit e un nom frais; nous avons

$$\mathbb{C}\{P\} \oplus e \xrightarrow{\tau} \approx_m c[P' \mid \bar{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq P_1$$

L'observable \bar{d} permet de s'assurer que la communication a eu lieu. Comme nous avons $P_1 \downarrow_{\bar{d}}$, cette transition ne peut être imitée que par

$$\mathbb{C}\{Q\} \oplus e \xrightarrow{\tau} \approx_m c[Q'_l \mid \bar{d}.\mathbf{0}] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq Q_1$$

pour un certain l . Nous avons

$$P_1 \xrightarrow{\tau} c[P'] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq P_2$$

Comme nous avons $P_2 \downarrow_c$, cette transition ne peut être imitée que par

$$Q_1 \xrightarrow{\tau} c[Q'_i] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq Q_2$$

avec $Q'_i \xrightarrow{\tau} Q'_i$. À partir de ce point, la preuve se termine comme dans le cas précédent.

Si $P \xrightarrow{\bar{a}, R, \mathbb{E}}_{\bar{b}} P'$, alors pour tout Q' tel que $Q \xrightarrow{\bar{a}, R, \mathbb{E}}_{\bar{b}} Q'$, nous avons $P' \not\approx_m^k Q'$. Comme Q est à image finie, l'ensemble $\{Q_i, Q \xrightarrow{\bar{a}, R, \mathbb{E}}_{\bar{b}} Q_i\}$ est fini. Par induction il existe \mathbb{C}_i, e_i tels que $\mathbb{C}_i\{P'\} \oplus e_i \approx_b \mathbb{C}_i\{Q_i\} \oplus e_i$ pour tout i . Soit $d \notin \text{fn}(P, Q, R, \mathbb{E})$. Par le lemme A.37, il existe R_d tel que $P \xrightarrow{\bar{a}, a(X)R_d, \mathbb{E}}_{\bar{b}} P' \mid \bar{d}.0$. Soit

$$\mathbb{C} \triangleq c[\square \mid a(X)R_d] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j)$$

avec c, f non libres dans P, Q, R, \mathbb{E} . Soit e un nom frais; nous avons

$$\mathbb{C}\{P\} \oplus e \xrightarrow{\tau} \approx_m c[P' \mid \bar{d}.0] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq P_1$$

L'observable \bar{d} permet de s'assurer que la communication a eu lieu. Comme nous avons $P_1 \downarrow_{\bar{d}}$, le processus Q communique avec $a(X)R_d$; le lemme A.37 permet de dire que le résultat de cette communication est bisimilaire à un processus Q'_i . Nous avons donc

$$\mathbb{C}\{Q\} \oplus e \xrightarrow{\tau} \approx_m c[Q'_i \mid \bar{d}.0] \mid d.c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq Q_1.$$

Nous avons

$$P_1 \xrightarrow{\tau} c[P'] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq P_2$$

Comme nous avons $P_2 \downarrow_c$, cette transition ne peut être imitée que par

$$Q_1 \xrightarrow{\tau} c[Q'_i] \mid c(X)(f \oplus \bigoplus_j \mathbb{C}_j\{X\} \oplus e_j) \triangleq Q_2$$

avec $Q'_i \xrightarrow{\tau} Q'_i$. À partir de ce point, la preuve se termine comme dans les cas précédents. □

A.4 Preuves pour HO π J

Pour la méthode de Howe, nous considérons la réception partielle $\pi \blacktriangleright P$ comme un opérateur du langage : $P \sim_{pi}^\bullet Q$ implique donc $\pi \blacktriangleright P \sim_{pi}^\bullet \pi \blacktriangleright Q$.

Lemme A.39. *Si $\pi \blacktriangleright P \sim_{pi}^\bullet \pi' \blacktriangleright Q$, alors nous avons $\pi = \pi'$ et $P \sim_{pi}^\bullet Q$.*

Démonstration. Par induction sur $\pi \blacktriangleright P \sim_{pi}^\bullet \pi' \blacktriangleright Q$.

Supposons $\pi \blacktriangleright P \sim_{pi}^\circ \pi' \blacktriangleright Q$. Pour toute substitution σ qui clôt $\pi \blacktriangleright P$ et $\pi' \blacktriangleright Q$, nous avons $\pi \blacktriangleright (P\sigma) \sim_{pi} \pi' \blacktriangleright (Q\sigma)$, donc par bisimilarité nous avons $\pi = \pi'$. Soit σ une substitution qui clôt P et Q ; σ peut s'écrire $\sigma_1 \cup \sigma_2$, avec σ_1 une substitution qui clôt les variables de π , et σ_2 qui clôt les autres variables. Nous avons $\pi \blacktriangleright (P\sigma_2) \sim_{pi} \pi \blacktriangleright (Q\sigma_2)$,

donc par bisimilarité nous avons $P\sigma_2\sigma_1 \sim_{pi} Q\sigma_2\sigma_1$, c'est-à-dire $P\sigma \sim_{pi} Q\sigma$. Nous avons donc $P \sim_{pi}^\circ Q$, donc $P \sim_{pi}^\bullet Q$.

Supposons $\pi \triangleright \sim_{pi}^\bullet R \sim_{pi}^\circ \pi' \triangleright Q$. Pour tout σ qui clôt R et $\pi' \triangleright Q$, nous avons $R\sigma \sim_{pi} \pi' \triangleright (Q\sigma)$, donc $R\sigma$ s'écrit $\pi'' \triangleright (R'\sigma)$, donc $R = \pi'' \triangleright R'$. Par induction nous avons $\pi = \pi''$ et $P \sim_{pi}^\bullet R'$, et en suivant le même raisonnement que dans le premier cas, nous avons $\pi'' = \pi'$ et $R' \sim_{pi}^\circ Q$. Nous avons donc $\pi = \pi'$ et $P \sim_{pi}^\bullet \sim_{pi}^\circ Q$, donc $P \sim_{pi}^\bullet Q$.

Dans le dernier cas, nous avons $\pi = \pi'$ et $P \sim_{pi}^\bullet Q$ directement. \square

Lemme A.40. Si $P \xrightarrow{\widetilde{a,R}} P'$, alors pour tout $\widetilde{R} \sim_{pi}^\bullet \widetilde{R'}$, il existe P'' tel que $P \xrightarrow{\widetilde{a,R'}} P''$ et $P' \sim_{pi}^\bullet P''$.

Si $P (\sim_{pi})_c^\bullet Q$ et $P \xrightarrow{\widetilde{a,R}} P'$, alors pour tout $\widetilde{R} (\sim_{pi})_c^\bullet \widetilde{R'}$, il existe Q' tel que $Q \xrightarrow{\widetilde{a,R'}} Q'$ et $P' (\sim_{pi})_c^\bullet Q'$.

Démonstration. Similaire à celle du lemme A.8. \square

Lemme A.41. Si $I \sim_{pi} J$ et $I \xrightarrow{a,R} I'$ avec R clos, il existe J' tel que $J \xrightarrow{a,R} J'$ et $I' \sim_{pi} J'$.

Démonstration. Nous avons $I = \pi \triangleright P$, $J = \pi \triangleright Q$ avec $P\sigma \sim_{pi} Q\sigma$ pour tout σ qui clôt P, Q . Par la règle PART-IN $_{pi}^j$, nous avons $\pi \equiv a(X) \mid \pi'$ et $I \xrightarrow{a,R} \pi' \triangleright P\{R/X\}$. Nous avons $J \xrightarrow{a,R} \pi' \triangleright Q\{R/X\} \triangleq J'$ par la même règle. Soit σ une substitution qui clôt $P\{R/X\}, Q\{R/X\}$. La substitution $\sigma, X \mapsto R$ clôt P, Q , donc nous avons $P\{R/X\}\sigma \sim_{pi} Q\{R/X\}\sigma$ comme voulu. \square

Lemme A.42. Si $E \xrightarrow{a,R} I'$, alors pour tout $R \sim_{pi}^\bullet R'$, il existe I'' tel que $E \xrightarrow{a,R'} I''$ et $I' \sim_{pi}^\bullet I''$.

Si $E (\sim_{pi})_c^\bullet E'$ et $E \xrightarrow{a,R} I$, alors pour tout $R (\sim_{pi})_c^\bullet R'$, il existe J tel que $E' \xrightarrow{a,R'} J$ et $I (\sim_{pi})_c^\bullet J$.

Démonstration. Nous devons distinguer les cas processus et réception partielle; le cas processus se traite classiquement comme pour le lemme A.8, nous ne traitons donc que le cas de la réception partielle.

Pour la première clause, nous avons $I = \pi \triangleright P$, $\pi \equiv a(X) \mid \pi'$ et $I \xrightarrow{a,R} \pi' \triangleright P\{R/X\} = I'$ par PART-IN $_{pi}^j$. Nous avons $I \xrightarrow{a,R'} \pi' \triangleright P\{R'/X\} \triangleq I''$ par la même règle. Nous avons $P\{R/X\} \sim_{pi}^\bullet P\{R'/X\}$ par le lemme A.2, et par congruence de \sim_{pi}^\bullet nous avons $I \sim_{pi}^\bullet I''$ comme souhaité.

Le second résultat se prouve par induction sur la taille de $I (\sim_{pi})_c^\bullet J$.

Supposons $I \sim_{pi}^\circ J$. Comme les termes sont clos, nous avons $I \sim_{pi} J$. Par la première clause, il existe I'' tel que $I \xrightarrow{a,R'} I''$ et $I' (\sim_{pi})_c^\bullet I''$. Par le lemme A.41, il existe J' tel que $J \xrightarrow{a,R'} J'$ et $I'' \sim_{pi} J'$. Nous avons $I' \sim_{pi}^\bullet \sim_{pi} J'$ et comme les termes sont clos, nous avons $I' (\sim_{pi})_c^\bullet J'$ comme souhaité.

Supposons $I \sim_{pi}^\bullet K \sim_{pi}^\circ J$; pour tout σ qui clôt K , nous avons $I (\sim_{pi})_c^\bullet K\sigma$ avec une preuve de la même taille d'après le lemme A.3. Par induction il existe K' tel que $K\sigma \xrightarrow{a,R'} K'$ et $I' (\sim_{pi})_c^\bullet K'$. Nous avons $K\sigma \sim_{pi} J$ donc par le lemme A.41, il existe J' tel que $J \xrightarrow{a,R'} J'$ et $K' \sim_{pi} J'$. Comme les termes sont clos, nous avons $K' \sim_{pi}^\circ J'$ et donc $I' (\sim_{pi})_c^\bullet J'$ comme voulu.

Supposons $I = \pi \triangleright P$, $J = \pi \triangleright Q$ avec $P (\sim_{pi})_c^\bullet Q$. Par la règle PART-IN $_{pi}^j$, nous avons $\pi \equiv a(X) \mid \pi'$ et $I \xrightarrow{a,R} \pi' \triangleright P\{R/X\} = I'$. Par la même règle, nous avons $J \xrightarrow{a,R'}$

$\pi' \blacktriangleright Q\{R'/X\} \triangleq J'$. Par le lemme A.2, nous avons $P\{R/X\} \sim_{pi}^\bullet Q\{R'/X\}$, donc par congruence de \sim_{pi}^\bullet , nous avons $I' (\sim_{pi})_c^\bullet J'$. □

Lemme A.43. *La dérivation d'un jugement $P \xrightarrow{\bar{a}, E, \tilde{R}} I$ n'utilise pas la règle PAR-OUT_o^j, et nous avons $\tilde{R} = \emptyset$.*

Démonstration. Si la règle PAR-OUT_o^j est utilisée, la dérivation contient un jugement de la forme $P_1 \xrightarrow{\bar{a}, E, \tilde{R}'} I$ avec \tilde{R}' au moins de taille 1. Comme $\tilde{R}' \neq \emptyset$, la règle OUT_o^j est utilisée, donc le multi-ensemble de noms \tilde{a} sur lequel P émet des messages est au moins de taille 2 alors qu'il est de taille 1 par hypothèse, contradiction.

À partir de ce premier résultat, nous pouvons montrer par induction sur $P \xrightarrow{\bar{a}, E, \tilde{R}} I$ que nous avons $\tilde{R} = \emptyset$. □

Lemme A.44. *Si $P \xrightarrow{\bar{a}, E, \emptyset} I$, alors pour tout $E (\sim_{pi})_c^\bullet E'$, il existe I' tel que $P \xrightarrow{\bar{a}, E', I'} I'$ et $I (\sim_{pi})_c^\bullet I'$.*

Si $P (\sim_{pi})_c^\bullet Q$ et $P \xrightarrow{\bar{a}, E, \emptyset} I$, alors pour tout $E (\sim_{pi})_c^\bullet E'$, il existe I' tel que $Q \xrightarrow{\bar{a}, E', \emptyset} I'$ et $I (\sim_{pi})_c^\bullet I'$.

Démonstration. Nous prouvons la première clause par induction sur $P \xrightarrow{\bar{a}, E, \emptyset} I$. D'après le lemme A.43 cette dérivation ne peut provenir de la règle PAR-OUT_o^j. La preuve est semblable à celle du lemme correspondant pour HO π (lemme A.9).

La deuxième clause se prouve par induction sur la taille de la dérivation de $P (\sim_{pi})_c^\bullet Q$. La preuve encore une fois semblable à celle du lemme correspondant pour HO π (lemme A.10), en remarquant que les récepteurs joints n'interviennent pas (lemme A.43). □

Lemme A.45. *Si $P \xrightarrow{\tilde{a}, E, \tilde{R}} I$, alors pour tout $E (\sim_{pi})_c^\bullet E'$, $\tilde{R} (\sim_{pi})_c^\bullet \tilde{R}'$, il existe I' tel que $P \xrightarrow{\tilde{a}, E', \tilde{R}'} I'$ et $I (\sim_{pi})_c^\bullet I'$.*

Si $P (\sim_{pi})_c^\bullet Q$ et $P \xrightarrow{\tilde{a}, E, \tilde{R}} I$, alors pour tout $E (\sim_{pi})_c^\bullet E'$, $\tilde{R} (\sim_{pi})_c^\bullet \tilde{R}'$, il existe I' tel que $Q \xrightarrow{\tilde{a}, E', \tilde{R}'} I'$ et $I (\sim_{pi})_c^\bullet I'$.

Démonstration. Nous prouvons les deux résultats simultanément par induction sur le nombre d'élément de \tilde{a} . Si ce nombre est 1, nous avons $\tilde{R} = \emptyset$ par le lemme A.43, le résultat est donc vrai par le lemme A.44.

Supposons que les deux résultats sont vrais pour un \tilde{a} de taille n . Supposons $P \xrightarrow{\tilde{a}, E, \tilde{R}} I$ avec \tilde{a} de taille $n + 1$. Nous prouvons le premier résultat par une sous-induction sur $P \xrightarrow{\tilde{a}, E, \tilde{R}} I$.

Si la règle utilisée est OUT_o^j : nous avons $P = \bar{a}(P_1)P_2 \xrightarrow{\tilde{b} \uplus \bar{a}, E, \tilde{R} \uplus R_j} J_2 \mid P_2 = I$ avec $E \xrightarrow{a, P_1} J_1$, $R_j \xrightarrow{\tilde{b}, J_1, \tilde{R}} J_2$. Par le lemme A.42 il existe J'_1 tel que $E' \xrightarrow{a, P_1} J'_1$ et $J_1 (\sim_{pi})_c^\bullet J'_1$. Par l'hypothèse d'induction principale, il existe J'_2 tel que $R'_j \xrightarrow{\tilde{b}, J'_1, \tilde{R}'} J'_2$ et $J_2 (\sim_{pi})_c^\bullet J'_2$. Par la règle OUT_o^j nous avons $P \xrightarrow{\tilde{b} \uplus \bar{a}, E', \tilde{R}' \uplus R'_j} J'_2 \mid P_2 \triangleq I'$ et par congruence de $(\sim_{pi})_c^\bullet$, nous avons $I (\sim_{pi})_c^\bullet I'$.

Si la dernière règle utilisée est PAR-OUT_o^j, nous avons $P = P_1 \mid R_j \xrightarrow{\tilde{a}, E, \tilde{R}} I$ avec $P_1 \xrightarrow{\tilde{a}, E, \tilde{R} \uplus R_j} I$. Par l'hypothèse de sous-induction il existe I' tel que $P_1 \xrightarrow{\tilde{a}, E', \tilde{R}' \uplus R_j} I'$ et $I (\sim_{pi})_c^\bullet I'$. Par la règle PAR-OUT_o^j nous avons $P \xrightarrow{\tilde{a}, E', \tilde{R}'} I'$, le résultat est donc vrai.

Si la dernière règle utilisée est PAR_o^j , nous avons $P = P_1 \mid P_2 \xrightarrow{\tilde{a}, E, \tilde{R}} I_1 \mid P_2 = I$ avec $P_1 \xrightarrow{\tilde{a}, E, \tilde{R}} I_1$. Par la sous-induction il existe I'_1 tel que $P_1 \xrightarrow{\tilde{a}, E', \tilde{R}'} I'_1$ et $I_1 (\sim_{pi})_c^\bullet I'_1$. Par la règle PAR_o^j nous avons $P \xrightarrow{\tilde{a}, E', \tilde{R}'} I'_1 \mid P_2 \triangleq I'$ et par congruence de $(\sim_{pi})_c^\bullet$ nous avons $I (\sim_{pi})_c^\bullet I'$ comme souhaité. La règle RESTR_o^j se traite de la même manière.

Le premier résultat est donc vrai pour \tilde{a} de taille $n + 1$. Nous prouvons maintenant le second résultat par une sous-induction sur la taille de la dérivation de $P (\sim_{pi})_c^\bullet Q$.

Supposons $P \sim_{pi}^\circ Q$; comme les termes sont clos, nous avons $P \sim_m Q$. Par le premier résultat il existe J tel que $P \xrightarrow{\tilde{a}, E', \tilde{R}'} J$ et $I (\sim_{pi})_c^\bullet J$. Par bisimilarité il existe I' tel que $Q \xrightarrow{\tilde{a}, E', \tilde{R}'} I'$ et $J \sim_{pi} I'$. Comme les termes sont clos, nous avons $J \sim_{pi}^\circ I'$, nous avons donc $I (\sim_{pi})_c^\bullet I'$ comme souhaité.

Supposons $P \sim_{pi}^\bullet T \sim_{pi}^\circ Q$. Soit σ une substitution qui clôt T ; nous avons $P (\sim_{pi})_c^\bullet T\sigma$. Par sous-induction il existe T' tel que $T\sigma \xrightarrow{\tilde{a}, E', \tilde{R}'} J$ et $I (\sim_{pi})_c^\bullet J$. Nous avons $T\sigma \sim_{pi} Q$ donc il existe I' tel que $Q \xrightarrow{\tilde{a}, E', \tilde{R}'} I'$ et $J \sim_{pi} I'$. Comme les termes sont clos, nous avons $J \sim_{pi}^\circ I'$; finalement nous avons donc $I (\sim_{pi})_c^\bullet I'$ comme souhaité.

Supposons $P = op(\tilde{P}_i)$, $Q = op(\tilde{Q}_i)$ avec $\tilde{P}_i (\sim_{pi})_c^\bullet \tilde{Q}_i$. Nous procédons par analyse de cas sur op .

Si $P = \bar{a}\langle P_1 \rangle P_2$ et $Q = \bar{a}\langle Q_1 \rangle Q_2$, la transition de P ne peut provenir que de la règle OUT_o^j . Nous avons $P \xrightarrow{\tilde{b} \uplus \bar{a}, E, \tilde{R} \uplus R_j} J_2 \mid P_2 = I$ avec $E \xrightarrow{a, P_1} J_1$ et $R_j \xrightarrow{\tilde{b}, J_1, \tilde{R}} J_2$. Par le lemme A.42 il existe J'_1 tel que $E' \xrightarrow{a, Q_1} J'_1$ et $J_1 (\sim_{pi})_c^\bullet J'_1$. Par l'hypothèse d'induction principale il existe J'_2 tel que $R'_j \xrightarrow{\tilde{b}, J'_1, \tilde{R}'} J'_2$ et $J_2 (\sim_{pi})_c^\bullet J'_2$. Par la règle OUT_o^j nous avons $Q \xrightarrow{\tilde{b} \uplus \bar{a}, E', \tilde{R}' \uplus R'_j} J'_2 \mid Q_2 \triangleq I'$. Par congruence de $(\sim_{pi})_c^\bullet$ nous avons $I (\sim_{pi})_c^\bullet I'$ comme souhaité.

Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, la transition de P peut provenir des règles PAR-OUT_o^j , PAR_o^j ou de leur symétrique. Dans le cas de PAR-OUT_o^j , nous avons $P_1 \xrightarrow{\tilde{a}, E, \tilde{R} \uplus P_2} I$. Par sous-induction il existe I' tel que $Q_1 \xrightarrow{\tilde{a}, E', \tilde{R}' \uplus Q_2} I'$ et $I (\sim_{pi})_c^\bullet I'$. Par PAR-OUT_o^j nous avons $Q \xrightarrow{\tilde{a}, E', \tilde{R}'} I'$, le résultat est donc vrai.

Dans le cas de PAR_o^j , nous avons $P \xrightarrow{\tilde{a}, E, \tilde{R}} I_1 \mid P_2 = I$ avec $P_1 \xrightarrow{\tilde{a}, E, \tilde{R}} I_1$. Par sous-induction il existe I'_1 tel que $Q_1 \xrightarrow{\tilde{a}, E', \tilde{R}'} I'_1$ et $I_1 (\sim_{pi})_c^\bullet I'_1$. Par PAR_o^j nous avons $Q \xrightarrow{\tilde{a}, E', \tilde{R}'} I'_1 \mid Q_2 \triangleq I'$; par congruence de $(\sim_{pi})_c^\bullet$, nous avons $I (\sim_{pi})_c^\bullet I'$ comme souhaité. La restriction (règle RESTR_o^j) se traite de la même manière. \square

Lemme A.46. Si $P (\sim_{pi})_c^\bullet Q$ et $P \xrightarrow{\theta} I$, il existe I' tel que $Q \xrightarrow{\theta} I'$ et $I (\sim_{pi})_c^\bullet I'$.

Démonstration. Par induction sur la taille de la dérivation de $P (\sim_{pi})_c^\bullet Q$.

Si $P \sim_{pi}^\circ Q$, comme les termes sont clos nous avons $P \sim_{pi} Q$, le résultat est vrai par bisimilarité.

Supposons $P \sim_{pi}^\bullet T \sim_{pi}^\circ Q$. Soit σ une substitution qui clôt T ; nous avons $P (\sim_{pi})_c^\bullet T\sigma$. Par induction il existe I_1 tel que $T\sigma \xrightarrow{\theta} I_1$ et $I (\sim_{pi})_c^\bullet I_1$. Nous avons $T\sigma \sim_{pi} Q$ donc il existe I' tel que $Q \xrightarrow{\theta} I'$ et $I_1 \sim_{pi} I'$. Comme les termes sont clos nous avons $I_1 \sim_{pi}^\circ I'$; finalement nous avons $I (\sim_{pi})_c^\bullet I'$ comme souhaité.

Supposons $P = op(\tilde{P}_i)$, $Q = op(\tilde{Q}_i)$ avec $\tilde{P}_i (\sim_{pi})_c^\bullet \tilde{Q}_i$. Nous procédons par analyse de cas sur op .

Supposons $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$. La transition de P peut provenir des règles SYNC_{ps}^j , PAR_{ps}^j ou de leur symétrique. Dans le cas de SYNC_{ps}^j , nous avons $P_1 \xrightarrow{\tilde{\beta}, P_2, \emptyset} I$. Par le lemme A.45, il existe I' tel que $Q_1 \xrightarrow{\tilde{\beta}, Q_2, \emptyset} I'$ et $I (\sim_{pi})_c^\bullet I'$. Nous avons $Q \xrightarrow{\theta} I'$ par SYNC_{ps}^j , le résultat est donc vrai. Dans le cas de PAR_{ps}^j , nous avons $P_1 \xrightarrow{\theta} J$ et $P_2 \xrightarrow{\tilde{\beta}, J, \emptyset} I$. Par induction il existe J' tel que $Q \xrightarrow{\theta} J'$ et $J (\sim_{pi})_c^\bullet J'$. Par le lemme A.45, il existe I' tel que $Q_2 \xrightarrow{a, J', \emptyset} I'$ et $I (\sim_{pi})_c^\bullet I'$. Nous avons $Q \xrightarrow{\theta} I'$ par PAR_{ps}^j , le résultat est donc vrai.

Supposons $P = \nu a.P_1$ et $Q = \nu a.Q_1$. La transition de P ne peut provenir que de la règle RESTR_{ps}^j : nous avons $P_1 \xrightarrow{\theta} I_1$ et $I = \nu a.I_1$. Par induction il existe I'_1 tel que $Q_1 \xrightarrow{\theta} I'_1$ et $I_1 (\sim_{pi})_c^\bullet I'_1$. Par la règle RESTR_{ps}^j nous avons $Q \xrightarrow{\theta} \nu a.I'_1$, le résultat est donc vrai par congruence de $(\sim_{pi})_c^\bullet$. Le cas $P = !P_1$, $Q = !Q_1$ se traite de la même manière. \square

Lemme A.47. *Si $P (\sim_{pi})_c^\bullet Q$ et $P \xrightarrow{\tau} P'$, alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' (\sim_{pi})_c^\bullet Q'$.*

Démonstration. Par induction sur la taille de la dérivation de $P (\sim_{pi})_c^\bullet Q$.

Si $P \sim_{pi}^\circ Q$, comme les termes sont clos nous avons $P \sim_{pi} Q$, le résultat est vrai par bisimilarité.

Supposons $P \sim_{pi}^\bullet T \sim_{pi}^\circ Q$. Soit σ une substitution qui clôt T ; nous avons $P (\sim_{pi})_c^\bullet T\sigma$. Par induction il existe T' tel que $T\sigma \xrightarrow{\tau} T'$ et $P' (\sim_{pi})_c^\bullet T'$. Nous avons $T\sigma \sim_{pi} Q$ donc il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $T' \sim_{pi} Q'$. Comme les termes sont clos nous avons $T' \sim_{pi}^\circ Q'$; finalement nous avons $P' (\sim_{pi})_c^\bullet Q'$ comme souhaité.

Supposons $P = op(\tilde{P}_i)$, $Q = op(\tilde{Q}_i)$ avec $\tilde{P}_i (\sim_{pi})_c^\bullet \tilde{Q}_i$. Nous procédons par analyse de cas sur op .

Supposons $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$. La transition de P peut provenir des règles $\text{PAR}_{i\tau}^j$, HO_τ^j , HO-SYNC_τ^j ou de leur symétrique. Dans le cas de HO_τ^j , nous avons $P_1 \xrightarrow{\tilde{a}, P_2, \emptyset} \mathbf{0} \blacktriangleright P'$. Par le lemme A.45 il existe I' tel que $Q_1 \xrightarrow{\tilde{a}, Q_2, \emptyset} I'$ et $\mathbf{0} \blacktriangleright P' (\sim_{pi})_c^\bullet I'$. Par le lemme A.39, il existe Q' tel que $I' = \mathbf{0} \blacktriangleright Q'$ et $P' (\sim_{pi})_c^\bullet Q'$. Par la règle HO_τ^j nous avons $Q \xrightarrow{\tau} Q'$, le résultat est donc vrai.

Dans le cas de HO-SYNC_τ^j , nous avons $P_1 \xrightarrow{\theta} I$ et $P_2 \xrightarrow{\tilde{a}, I, \emptyset} \mathbf{0} \blacktriangleright P'$. Par le lemme A.46 il existe I' tel que $Q_1 \xrightarrow{\theta} I'$ et $I (\sim_{pi})_c^\bullet I'$. Par le lemme A.45, il existe I'' tel que $Q_2 \xrightarrow{\tilde{a}, I', \emptyset} I''$ et $\mathbf{0} \blacktriangleright P' (\sim_{pi})_c^\bullet I''$. Par le lemme A.39, il existe Q' tel que $I'' = \mathbf{0} \blacktriangleright Q'$ et $P' (\sim_{pi})_c^\bullet Q'$. Par la règle HO-SYNC_τ^j nous avons $Q \xrightarrow{\tau} Q'$, le résultat est donc vrai.

Dans le cas de $\text{PAR}_{i\tau}^j$, nous avons $P_1 \xrightarrow{\tau} P'_1$ et $P' = P'_1 \mid P_2$. Par induction il existe Q'_1 tel que $Q_1 \xrightarrow{\tau} Q'_1$ et $P'_1 (\sim_{pi})_c^\bullet Q'_1$. Par $\text{PAR}_{i\tau}^j$ nous avons $Q \xrightarrow{\tau} Q'_1 \mid Q_2 \triangleq Q'$ et par congruence de $(\sim_{pi})_c^\bullet$, nous avons $P' (\sim_{pi})_c^\bullet Q'$. La restriction (règle $\text{RESTR}_{i\tau}^j$) se traite de la même manière. \square

Lemme A.48. *Nous avons $(\sim_{pi})_c^{\bullet*} \subseteq \sim_{pi}$.*

Démonstration. Les lemmes A.40, A.42, A.45, A.46 et A.47 permettent de montrer que $(\sim_{pi})_c^{\bullet*}$ est une simulation forte à complément sur les réceptions partielles, et $(\sim_{pi})_c^{\bullet*}$ est symétrique par le lemme A.4 \square

Théorème A.3. *La relation \sim_{pi} est une congruence.*

Démonstration. Immédiat par les lemmes A.48 et A.5. \square

A.5 Preuves pour le Kell

A.5.1 Système de transitions à complément

Nous donnons ici toutes les règles du système de transition à complément de \mathbf{jK} , en commençant par le jugement d'émission inférieure.

Émission de message : règles locales.

$$\begin{array}{c}
\frac{E \xrightarrow{a^*, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*) \cap \tilde{b} = \emptyset}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, *, E, \mathbb{E}^*, \emptyset, \emptyset} \tilde{b} \mid \mathbb{E}^*\{P_2\}} \text{OUT}_{1,=}^k \\
\\
\frac{E \xrightarrow{a^*, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \xi \in \{*, p\} \quad \text{bn}(\mathbb{E}^*) \cap (\tilde{b} \cup \tilde{b}') = \emptyset \quad P' \xrightarrow{\tilde{a}', \xi, I, \mathbb{E}^*\{\square \mid P_2\}, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\}} \tilde{b}' I'}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, *, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{cn}\{\widetilde{P^{cn}}\}} \tilde{b}' \uplus \tilde{b} I'} \text{OUT}_{2,=}^k \\
\\
\frac{E \xrightarrow{a^*, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*) \cap (\tilde{b} \cup \tilde{b}') = \emptyset \quad P' \xrightarrow{\tilde{a}', c_{n_0}, I, \mathbb{E}^*\{\square \mid P_2\}, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\} \cup \mathbb{K}^{cn_0}\{\widetilde{P^{cn_0}}\}} \tilde{b}' I'}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, *, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\} \cup \mathbb{K}^{cn_0}\{\widetilde{P^{cn_0}} \uplus P'\}} \tilde{b}' \cup \tilde{b} I'} \text{OUT}_{3,=}^k
\end{array}$$

Passivation.

$$\begin{array}{c}
\frac{E \xrightarrow{a^p, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*) \cap \tilde{b} = \emptyset}{a[P_1]P_2 \xrightarrow{\bar{a}, p, E, \mathbb{E}^*, \emptyset, \emptyset} \tilde{b} \mid \mathbb{E}^*\{P_2\}} \text{PASSIV}_{1,=}^k \\
\\
\frac{E \xrightarrow{a^p, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \xi \in \{*, p\} \quad \text{bn}(\mathbb{E}^*) \cap (\tilde{b} \cup \tilde{b}') = \emptyset \quad P' \xrightarrow{\tilde{a}', \xi, I, \mathbb{E}^*\{\square \mid P_2\}, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\}} \tilde{b}' I'}{a[P_1]P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, p, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{cn}\{\widetilde{P^{cn}}\}} \tilde{b}' \cup \tilde{b} I'} \text{PASSIV}_{2,=}^k \\
\\
\frac{E \xrightarrow{a^p, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*) \cap (\tilde{b} \cup \tilde{b}') = \emptyset \quad P' \xrightarrow{\tilde{a}', c_{n_0}, I, \mathbb{E}^*\{\square \mid P_2\}, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\} \cup \mathbb{K}^{cn_0}\{\widetilde{P^{cn_0}}\}} \tilde{b}' I'}{a[P_1]P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, p, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\} \cup \mathbb{K}^{cn_0}\{\widetilde{P^{cn_0}} \uplus P'\}} \tilde{b}' \cup \tilde{b} I'} \text{PASSIV}_{3,=}^k
\end{array}$$

Émission de message : règles inférieures.

$$\begin{array}{c}
\frac{E \xrightarrow{a^\perp, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{cn}) \cap \tilde{b} = \emptyset}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\bar{a}, c_n, E, \mathbb{E}^*, \emptyset, \mathbb{K}^{cn}\{\emptyset\}} \tilde{b} \mid \mathbb{E}^*\{\mathbb{K}^{cn}\{P_2\}\}} \text{OUT}_{1,<}^k \\
\\
\frac{\widetilde{P^{cn_0}} \neq \emptyset \quad \xi \in \{*, p\} \quad E \xrightarrow{a^\perp, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{cn_0}) \cap (\tilde{b} \cup \tilde{b}') = \emptyset \quad P' \xrightarrow{\tilde{a}', \xi, I, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P^{cn}}\} \cup \mathbb{K}^{cn_0}\{\widetilde{P^{cn_0}}\} \mid P_2\}} \tilde{b}' I'}{\bar{a}\langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{cn}\{\widetilde{P^{cn}}\} \cup \mathbb{K}^{cn_0}\{\widetilde{P^{cn_0}}\}} \tilde{b}' \cup \tilde{b} I'} \text{OUT}_{2,<}^k
\end{array}$$

$$\begin{array}{c}
\frac{E \xrightarrow{a^\perp, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{c_{n_0}}) \cap (\tilde{b} \cup \tilde{b}') = \emptyset}{\frac{\widetilde{P^{c_{n_0}}} \neq \emptyset \quad P' \xrightarrow{\tilde{a}', c'_n, I, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}} | P_2\}} \cup \mathbb{K}^{c'_n} \{\widetilde{P^{c'_n}}\}} \rightarrow_{\tilde{b}'} I'}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}}\}} \cup \mathbb{K}^{c'_n} \{\widetilde{P^{c'_n} \uplus P'}\}} \rightarrow_{\tilde{b}' \cup \tilde{b}} I'} \text{OUT}_{3,<}^k} \\
\\
\frac{E \xrightarrow{a^\perp, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{c_{n_0}}) \cap (\tilde{b} \cup \tilde{b}') = \emptyset}{\frac{c_{n_0} \notin \tilde{c}_n \quad \xi \in \{*, p\} \quad P' \xrightarrow{\tilde{a}', \xi, I, \mathbb{E}^* \{\square | \mathbb{K}^{c_{n_0}} \{P_2\}\}, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}'} I'}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\emptyset\}} \rightarrow_{\tilde{b}' \cup \tilde{b}} I'} \text{OUT}_{4,<}^k} \\
\\
\frac{E \xrightarrow{a^\perp, P_1} I \quad \text{fn}(P_1) = \tilde{b} \quad \text{bn}(\mathbb{E}^*, \mathbb{K}^{c_{n_0}}) \cap (\tilde{b} \cup \tilde{b}') = \emptyset}{\frac{c_{n_0} \notin \tilde{c}_n \cup c'_n \quad P' \xrightarrow{\tilde{a}', c'_n, I, \mathbb{E}^* \{\square | \mathbb{K}^{c_{n_0}} \{P_2\}\}, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c'_n} \{\widetilde{P^{c'_n}}\}} \rightarrow_{\tilde{b}'} I'}{\bar{a} \langle P_1 \rangle P_2 \xrightarrow{\tilde{a}' \uplus \bar{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^* \uplus P', \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\emptyset\} \cup \mathbb{K}^{c'_n} \{\widetilde{P^{c'_n} \uplus P'}\}} \rightarrow_{\tilde{b}' \cup \tilde{b}} I'} \text{OUT}_{5,<}^k}
\end{array}$$

Règles de congruence : messages locaux. Nous omettons le symétrique des règles PAR_{\leq}^k et PAR-OUT_{\leq}^k .

$$\begin{array}{c}
\frac{P_1 \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^* \{\square | P_2\}, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I \quad \xi \in \{*, p\}}{P_1 \mid P_2 \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I} \text{PAR}_{\leq}^k \\
\\
\frac{P_1 \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \tilde{P}^* \uplus P_2, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I \quad \xi \in \{*, p\}}{P_1 \mid P_2 \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I} \text{PAR-OUT}_{\leq}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I \quad d \in \tilde{b} \quad d \notin \tilde{a}}{\nu d.P \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b} \setminus d} \nu d.I} \text{EXTR}_{\leq}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^* \{\nu d.\square\}, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I \quad \xi \in \{*, p\} \quad d \notin \tilde{b} \quad d \notin \tilde{a}}{\nu d.P \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I} \text{RESTR}_{\leq}^k \\
\\
\frac{P_1 \xrightarrow{\tilde{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\emptyset\}} \rightarrow_{\tilde{b}} I \quad \mathbb{K}^{c_{n_0}} = c[\square]P_2 \quad c_{n_0} \notin \tilde{c}_n}{c[P_1]P_2 \xrightarrow{\tilde{a}, *, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I} \text{LOC}_{\leq}^k
\end{array}$$

Règles de congruence : messages inférieurs. Nous omettons le symétrique des règles $\text{PAR}_{<}^k$ et $\text{PAR-OUT}_{<}^k$.

$$\frac{P_1 \xrightarrow{\tilde{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\} \cup \mathbb{K}^{c_{n_0}} \{\widetilde{P^{c_{n_0}} | P_2\}} \rightarrow_{\tilde{b}} I}{P_1 \mid P_2 \xrightarrow{\tilde{a}, c_{n_0}, E, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P^{c_n}}\}} \rightarrow_{\tilde{b}} I} \text{PAR}_{<}^k$$

$$\begin{array}{c}
\frac{P_1 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} \cup \mathbb{K}^{cn_0} \{ \widetilde{P^{cn_0}} \} } \widetilde{b} I}{P_1 \mid P_2 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} } \widetilde{b} I} \text{PAR-OUT}_{<}^k \\
\\
\frac{P \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} \cup \mathbb{K}^{cn_0} \{ \nu d. \widetilde{P^{cn_0}} \} } \widetilde{b} I} \quad d \notin \widetilde{b} \quad d \notin \widetilde{a}}{\nu d. P \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} } \widetilde{b} I} \text{RESTR}_{<}^k
\end{array}$$

Transitions inférieures : capture par les contextes.

$$\begin{array}{c}
\frac{P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} } \widetilde{b} I}{P \vdash \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} } \widetilde{b} I} \text{CFREE}_{\leq}^k \\
\\
\frac{P \vdash \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}_1^* \{ \mathbb{E}_2^* \}, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} } \widetilde{b} I} \quad d \in \widetilde{b}}{P \vdash \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}_1^* \{ \nu d. \mathbb{E}_2^* \}, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} } \widetilde{b} \nu d. I} \text{CAPT}_{\leq}^k \\
\\
\frac{P \vdash \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} \cup \mathbb{K}_1^{cn_0} \{ \mathbb{E}_2^{cn_0} \{ \widetilde{P^{cn_0}} \} \} } \widetilde{b} I} \quad d \in \widetilde{b}}{P \vdash \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \} \cup \mathbb{K}_1^{cn_0} \{ \nu d. \mathbb{E}_2^{cn_0} \{ \widetilde{P^{cn_0}} \} \} } \widetilde{b} \nu d. I} \text{CAPT}_{<}^k
\end{array}$$

Transitions inférieures : synchronisation partielle. Nous omettons le symétrique des règles SYNC_{\leq}^k et SYNC-PAR_{\leq}^k .

$$\begin{array}{c}
\frac{P_2 \xrightarrow{\widetilde{a}, \xi, P_1, \square, \emptyset, \emptyset} \widetilde{b} I}{P_1 \mid P_2 \xrightarrow{\leq, \theta} I} \text{SYNC}_{\leq}^k \quad \frac{P_1 \xrightarrow{\leq, \theta} I \quad P_2 \xrightarrow{\widetilde{a}, \xi, I, \square, \emptyset, \emptyset} \widetilde{b} J}{P_1 \mid P_2 \xrightarrow{\leq, \theta} J} \text{SYNC-PAR}_{\leq}^k \\
\\
\frac{P \xrightarrow{\leq, \theta} I \quad a \notin n(I)}{\nu a. P \xrightarrow{\leq, \theta} \nu a. I} \text{SYNC-RESTR}_{\leq}^k
\end{array}$$

Transitions supérieures : émission de message.

$$\begin{array}{c}
\frac{E \xrightarrow{a^\dagger, P_1} I \quad \delta(I) = \square \quad \text{fn}(P_1) = \widetilde{b} \quad \text{bn}(\mathbb{E}^\dagger) \cap \widetilde{b} = \emptyset}{\overline{a} \langle P_1 \rangle P_2 \xrightarrow{\overline{a}, \uparrow, E, \mathbb{E}^\dagger, \emptyset} \widetilde{b} I \mid \mathbb{E}^\dagger \{ P_2 \}} \text{OUT}_{1, >}^k \\
\\
\frac{E \xrightarrow{a^\dagger, P_1} I \quad \delta(I) = \square \quad \text{fn}(P_1) = \widetilde{b} \quad \text{bn}(\mathbb{E}^\dagger) \cap (\widetilde{b} \cup \widetilde{b}') = \emptyset \quad P' \xrightarrow{\widetilde{a}', \uparrow, I, \mathbb{E}^\dagger \{ \square \mid P_2 \}, \widetilde{P}^\dagger} \widetilde{b'} I'}{P \xrightarrow{\widetilde{a}' \uplus \overline{a}, \uparrow, E, \mathbb{E}^\dagger, \widetilde{P}^\dagger \uplus P'} \widetilde{b \cup b'} I'} \text{OUT}_{2, >}^k
\end{array}$$

Transitions supérieures : congruence. Nous omettons le symétrique des règles $\text{PAR}_{>}^k$ et $\text{PAR-OUT}_{>}^k$.

$$\begin{array}{c}
\frac{P_1 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger \{\square \mid P_2\}, \tilde{P}^\dagger} \tilde{b} I}{P_1 \mid P_2 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} I} \text{PAR}_{>}^k \quad \frac{P_1 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger \uplus P_2} \tilde{b} I}{P_1 \mid P_2 \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} I} \text{PAR-OUT}_{>}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} I \quad d \in \tilde{b} \quad d \notin \tilde{a}}{\nu d. P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^*, \tilde{P}^\dagger} \tilde{b} \setminus d \nu d. I} \text{EXTR}_{>}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger \{\nu d. \square\}, \tilde{P}^\dagger} \tilde{b} I \quad d \notin \tilde{b} \quad d \notin \tilde{a}}{\nu d. P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} I} \text{RESTR}_{>}^k
\end{array}$$

Transitions supérieures : capture par les contextes.

$$\begin{array}{c}
\frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} I}{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\dagger, \tilde{P}^\dagger} \tilde{b} I} \text{CFREE}_{>}^k \quad \frac{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}_1^\dagger \{\mathbb{E}_2^\dagger\}, \tilde{P}^\dagger} \tilde{b} I \quad d \in \tilde{b}}{P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}_1^\dagger \{\nu d. \mathbb{E}_2^\dagger\}, \tilde{P}^\dagger} \tilde{b} \nu d. I} \text{CAPT}_{>}^k
\end{array}$$

Transitions supérieures : synchronisation partielle. Nous omettons le symétrique des règles $\text{SYNC}_{>}^k$ et $\text{SYNC-PAR}_{>}^k$.

$$\begin{array}{c}
\frac{P_1 \xrightarrow{\tilde{a}, \uparrow, P_2, \square, \emptyset} \tilde{b} I}{P_1 \mid P_2 \xrightarrow{\geq, \theta} I} \text{SYNC}_{>}^k \quad \frac{P_1 \xrightarrow{\geq, \theta} I \quad P_2 \xrightarrow{\tilde{a}, \uparrow, I, \square, \emptyset} \tilde{b} J}{P_1 \mid P_2 \xrightarrow{\leq, \theta} J} \text{SYNC-PAR}_{>}^k \\
\\
\frac{P \xrightarrow{\geq, \theta} I \quad a \notin n(I)}{\nu a. P \xrightarrow{\geq, \theta} \nu a. I} \text{SYNC-RESTR}_{>}^k \quad \frac{P_1 \xrightarrow{\leq, \theta} I \quad \eta(I) = \{\uparrow\}}{a[P_1]P_2 \xrightarrow{\geq, \theta} a[I]P_2} \text{SYNC-LOC}_{>}^k
\end{array}$$

Système de transitions étiquetées pour l'observation. Nous omettons le symétrique des règles $\text{PAR}_{i\tau}^k$, HO_{\leq}^k , HO-SYNC_{\leq}^k , $\text{HO}_{>}^k$ et $\text{HO-SYNC}_{>}^k$.

$$\begin{array}{c}
\frac{\pi = \prod a^\eta(\tilde{X})}{\pi \triangleright P \xrightarrow{*[a^\eta, \tilde{R}]} P\{\tilde{R}/\tilde{X}\}} \text{IN}_i^k \quad \frac{P_1 \xrightarrow{\mu} P'_1}{P_1 \mid P_2 \xrightarrow{\mu} P'_1 \mid P_2} \text{PAR}_{i\tau}^k \\
\\
\frac{P \xrightarrow{\mu} P' \quad a \notin n(\mu)}{\nu a. P \xrightarrow{\mu} \nu a. P'} \text{RESTR}_{i\tau}^k \quad \frac{P \xrightarrow{\tau} P'}{a[P]Q \xrightarrow{\tau} a[P']Q} \text{LOC}_\tau^k \\
\\
\frac{P \xrightarrow{*[a^\eta, \tilde{R}]} P'}{b[P]Q \xrightarrow{\square[a^\eta, \tilde{R}]} b[P']Q} \text{LOC}_i^k \quad \frac{P_2 \xrightarrow{\tilde{a}, \xi, P_1, \square, \emptyset, \emptyset} \tilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO}_{\leq}^k \\
\\
\frac{P_1 \xrightarrow{\leq, \theta} I \quad P_2 \xrightarrow{\tilde{a}, \xi, I, \square, \emptyset, \emptyset} \tilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO-SYNC}_{\leq}^k \quad \frac{P_2 \xrightarrow{\tilde{a}, \uparrow, P_1, \square, \emptyset} \tilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO}_{>}^k \\
\\
\frac{P_1 \xrightarrow{\geq, \theta} I \quad P_2 \xrightarrow{\tilde{a}, \uparrow, I, \square, \emptyset} \tilde{b} \mathbf{0} \blacktriangleright_\delta P'}{P_1 \mid P_2 \xrightarrow{\tau} P'} \text{HO-SYNC}_{>}^k
\end{array}$$

$$\begin{array}{c}
\frac{P \xrightarrow{\tilde{a}, \xi, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b \mathbf{0} \blacktriangleright_\delta P'}{P \xrightarrow{\tilde{a}, \xi, \emptyset, \square, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b P'} \text{ OUT-OBS}_{1, \leq}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \xi, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b I \quad P_2 \xrightarrow{\tilde{a}', \uparrow, \Delta \{ I \}, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_{b'} \mathbf{0} \blacktriangleright_\delta P'}{P \xrightarrow{\tilde{a}, \xi, \mathbb{E}^\uparrow \{ \widetilde{P^\uparrow} \uplus P_2 \}, \Delta, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b P'} \text{ OUT-OBS}_{2, \leq}^k \\
\\
\frac{P \xrightarrow{\tilde{a}, \uparrow, \Delta \{ Q | \mathbb{E}^* \{ \prod \widetilde{P^*} | \prod_{cn} \mathbb{K}^{cn} \{ \prod \widetilde{P^{cn}} \} \}, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_b \mathbf{0} \blacktriangleright_\delta P'}{P \xrightarrow{\tilde{a}, \uparrow, \mathbb{E}^\uparrow \{ \widetilde{P^\uparrow} \}, \Delta, Q, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b P'} \text{ OUT-OBS}_{>}^k
\end{array}$$

A.5.2 Congruence de la bisimilarité à complément

Comme pour $\text{HO}\pi\text{J}$, nous considérons la réception partielle comme un opérateur du langage.

Lemme A.49. Soient $P \approx_{pi} Q$.

Si $P \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b I$, alors il existe $\widetilde{P^*}, \widetilde{P^{cn}}, E', I'$ tels que $\widetilde{P^*} \xrightarrow{\tau} \widetilde{P'^*}, \widetilde{P^{cn}} \xrightarrow{\tau} \widetilde{P'^{cn}}, E \xrightarrow{\tau} E', Q \xrightarrow{\tau} \xrightarrow{\tilde{a}, \xi, E', \mathbb{E}^*, \widetilde{P'^*}, \mathbb{K}^{cn} \{ \widetilde{P'^{cn}} \}} \rightarrow_b I'$ et $I \approx_{pi}^\bullet I'$.

Si $P \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_b I$, alors il existe $\widetilde{P^\uparrow}, E', I'$ tels que nous avons $\widetilde{P^\uparrow} \xrightarrow{\tau} \widetilde{P'^\uparrow}, E \xrightarrow{\tau} E', Q \xrightarrow{\tau} \xrightarrow{\tilde{a}, \uparrow, E', \mathbb{E}^\uparrow, \widetilde{P'^\uparrow}} \rightarrow_b I'$ et $I \approx_{pi}^\bullet I'$.

Démonstration. Similaire à celle du lemme A.20. \square

Lemme A.50. Soient $P \approx_{pi} Q$.

Si $P \xrightarrow{\lambda_k} P'$, alors il existe Q' tel que $Q \xrightarrow{\lambda_k} Q'$ et $P' \approx_m Q'$.

Si $P \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b I$, alors il existe I' telle que $Q \xrightarrow{\tilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{ \widetilde{P^{cn}} \}} \rightarrow_b I'$ et $I \approx_{pi} I'$.

Si $P \xrightarrow{\tau} \xrightarrow{\leq, \theta} I$, alors il existe I' telle que $Q \xrightarrow{\tau} \xrightarrow{\leq, \theta} I'$ et $I \approx_{pi} I'$.

Si $P \xrightarrow{\tau} \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_b I$, alors il existe I' tel que $Q \xrightarrow{\tau} \xrightarrow{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P^\uparrow}} \rightarrow_b I'$ et $I \approx_{pi} I'$.

Si $P \xrightarrow{\tau} \xrightarrow{>, \theta} I$, alors il existe I' telle que $Q \xrightarrow{\tau} \xrightarrow{>, \theta} I'$ et $I \approx_{pi} I'$.

Si $P \xrightarrow{\tau} \xrightarrow{\tilde{a}, \xi, E', \mathbb{E}^*, \widetilde{P'^*}, \mathbb{K}^{cn} \{ \widetilde{P'^{cn}} \}} \rightarrow_b I$ avec $E \xrightarrow{\tau} E', \widetilde{P^*} \xrightarrow{\tau} \widetilde{P'^*}$ et $\widetilde{P^{cn}} \xrightarrow{\tau} \widetilde{P'^{cn}}$, alors il existe $\widetilde{P''^*}, \widetilde{P''^{cn}}, E'', I'$ tels que $\widetilde{P^*} \xrightarrow{\tau} \widetilde{P''^*}, \widetilde{P^{cn}} \xrightarrow{\tau} \widetilde{P''^{cn}}, E \xrightarrow{\tau} E'', Q \xrightarrow{\tau} \xrightarrow{\tilde{a}, \xi, E'', \mathbb{E}^*, \widetilde{P''^*}, \mathbb{K}^{cn} \{ \widetilde{P''^{cn}} \}} \rightarrow_b I'$ et $I \approx_{pi}^\bullet I'$.

Si $P \xrightarrow{\tau} \xrightarrow{\tilde{a}, \uparrow, E', \mathbb{E}^\uparrow, \widetilde{P'^\uparrow}} \rightarrow_b I$ avec $E \xrightarrow{\tau} E'$ et $\widetilde{P^\uparrow} \xrightarrow{\tau} \widetilde{P'^\uparrow}$, alors il existe $\widetilde{P''^\uparrow}, E'', I'$ tels que $\widetilde{P^\uparrow} \xrightarrow{\tau} \widetilde{P''^\uparrow}, E \xrightarrow{\tau} E'', Q \xrightarrow{\tau} \xrightarrow{\tilde{a}, \uparrow, E'', \mathbb{E}^\uparrow, \widetilde{P''^\uparrow}} \rightarrow_b I'$ et $I \approx_{pi}^\bullet I'$.

Démonstration. Similaire à celle du lemme A.21. \square

Lemme A.51. Si $P \approx_{pi}^\bullet Q$, alors $\text{fn}(P) = \text{fn}(Q)$.

Démonstration. Semblable à celle du lemme A.22. \square

Lemme A.52. Si $P \xrightarrow{\delta[a\widetilde{R}]} P'$, pour tout $\widetilde{R} \approx_{pi}^\bullet \widetilde{R'}$, il existe P'' tel que $P \xrightarrow{\delta[a, \widetilde{R'}]} P''$ et $P' \approx_{pi}^\bullet P''$.

Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\delta[a,R]} P'$, pour tout $R (\approx_{pi})_c^\bullet R'$, il existe Q' tel que $Q \xrightarrow{\delta[a,R']} Q'$ et $P' (\approx_{pi})_c^\bullet Q'$.

Démonstration. Similaire à celle du lemme A.8. \square

Lemme A.53. Si $I \approx_{pi} J$ et $I \xrightarrow{a^\eta, R} I'$ avec R clos, il existe J' tel que $J \xrightarrow{a^\eta} RJ'$ et $I' \approx_{pi} J'$.

Démonstration. Similaire à celle du lemme A.41. \square

Lemme A.54. Si $E \xrightarrow{a^\eta, R} I'$, alors pour tout $R \approx_{pi}^\bullet R'$, il existe I'' tel que $E \xRightarrow{\tau} \xrightarrow{a^\eta, R'} I''$ et $I' \approx_{pi}^\bullet I''$.

Si $E (\approx_{pi})_c^\bullet E'$ et $E \xrightarrow{a^\eta, R} I$, alors pour tout $R (\approx_{pi})_c^\bullet R'$, il existe J tel que $E' \xRightarrow{\tau} \xrightarrow{a^\eta, R'} J$ et $I (\approx_{pi})_c^\bullet J$.

Démonstration. Similaire à celle du lemme A.42. \square

Lemme A.55. Si $\mathbb{E} \approx_{pi}^\bullet \mathbb{F}$, $\mathbb{E}' \approx_{pi}^\bullet \mathbb{F}'$ et $P \approx_{pi}^\bullet Q$, alors nous avons $\mathbb{E}\{\mathbb{E}'\} \approx_{pi}^\bullet \mathbb{F}\{\mathbb{F}'\}$ et $\mathbb{E}\{P\} \approx_{pi}^\bullet \mathbb{F}\{Q\}$. Nous avons un résultat similaire pour $\mathbb{K} \approx_{pi}^\bullet \mathbb{K}'$.

Démonstration. Facile par induction sur $\mathbb{E} \approx_{pi}^\bullet \mathbb{F}$ ou $\mathbb{K} \approx_{pi}^\bullet \mathbb{K}'$. \square

Corollaire A.2. Si $\mathbb{E} \approx_{pi}^\bullet \mathbb{F}$ et $P \approx_{pi}^\bullet Q$, alors nous avons $\mathbb{E}\{\nu a. \square\} \approx_{pi}^\bullet \mathbb{F}\{\nu a. \square\}$, $\mathbb{E}\{\square \mid P\} \approx_{pi}^\bullet \mathbb{F}\{\square \mid Q\}$ et $\mathbb{E}\{\square \mid !P\} \approx_{pi}^\bullet \mathbb{F}\{\square \mid !Q\}$. Nous avons un résultat similaire pour $\mathbb{K} \approx_{pi}^\bullet \mathbb{K}'$.

Lemme A.56. Si $\mathbb{E} \approx_{pi}^\bullet \mathbb{F}$, alors $bn(\mathbb{E}) = bn(\mathbb{F})$, de même pour $\mathbb{K} \approx_{pi}^\bullet \mathbb{K}'$.

Démonstration. Facile par induction sur $\mathbb{E} \approx_{pi}^\bullet \mathbb{F}$ ou $\mathbb{K} \approx_{pi}^\bullet \mathbb{K}'$. \square

Lemme A.57. La dérivation d'un jugement $P \xrightarrow{\bar{a}, \xi, E, \mathbb{E}^*, \widetilde{P^*}, \mathbb{K}^{cn} \{\widetilde{P^{cn}}\}} \widetilde{b} I$ n'utilise pas la règle $\text{PAR-OUT}_{=}^k$ ou $\text{PAR-OUT}_{<}^k$. En outre nous avons $\widetilde{P^*} = \mathbb{K}^{cn} \{\widetilde{P^{cn}}\} = \emptyset$ si $\xi \in \{*, p\}$, et $\widetilde{P^*} = \emptyset$ et $\mathbb{K}^{cn} \{\widetilde{P^{cn}}\} = \mathbb{K}^{cn_0} \{\emptyset\}$ si $\xi = c_{n_0}$.

Démonstration. Similaire à celle du lemme A.43. \square

Lemme A.58. Si $P \xrightarrow{\bar{a}, \xi, E, \mathbb{E}^*, \emptyset, \emptyset} \widetilde{b} I$ avec $\xi \in \{*, p\}$, alors pour tout $E (\approx_{pi})_c^\bullet E', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*$, il existe I' telle que $P \xrightarrow{\bar{a}, \xi, E', \mathbb{E}'^*, \emptyset, \emptyset} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Si $P \xrightarrow{\bar{a}, c_n, E, \mathbb{E}^*, \emptyset, \mathbb{K}^{cn} \{\emptyset\}} \widetilde{b} I$, alors $\forall E (\approx_{pi})_c^\bullet E', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*, \mathbb{K}^{cn} (\approx_{pi})_c^\bullet \mathbb{K}'^{cn}$, il existe I' telle que $P \xrightarrow{\bar{a}, c_n, E', \mathbb{E}'^*, \emptyset, \mathbb{K}'^{cn} \{\emptyset\}} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\bar{a}, \xi, E, \mathbb{E}^*, \emptyset, \emptyset} \widetilde{b} I$ avec $\xi \in \{*, p\}$, alors pour tout $E (\approx_{pi})_c^\bullet E', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*$, il existe E'', I' tels que $E' \xRightarrow{\tau} E''$ et $Q \xRightarrow{\tau} \xrightarrow{\bar{a}, \xi, E'', \mathbb{E}'^*, \emptyset, \emptyset} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\bar{a}, c_n, E, \mathbb{E}^*, \emptyset, \mathbb{K}^{cn} \{\emptyset\}} \widetilde{b} I$, alors $\forall E (\approx_{pi})_c^\bullet E', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*, \mathbb{K}^{cn} (\approx_{pi})_c^\bullet \mathbb{K}'^{cn}$, il existe E'', I' tels que $E' \xRightarrow{\tau} E''$, $Q \xRightarrow{\tau} \xrightarrow{\bar{a}, c_n, E'', \mathbb{E}'^*, \emptyset, \mathbb{K}'^{cn} \{\emptyset\}} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Ces transitions impliquent un seul émetteur et un seul récepteur, les preuves sont donc semblables à celles des lemmes A.26 et A.27 pour $\text{HO}\pi\text{P}$. \square

Lemme A.59. Si $P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_b I$, alors $\forall E (\approx_{pi})_c^\bullet E', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*, \mathbb{K}^{cn} (\approx_{pi})_c^\bullet \mathbb{K}'^{cn}, \widetilde{P}^* (\approx_{pi})_c^\bullet \widetilde{P}'^*, \widetilde{P}^{cn} (\approx_{pi})_c^\bullet \widetilde{P}'^{cn}$, il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'$ tels que $\widetilde{P}'^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}'^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E'', P \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I'$ et $I (\approx_{pi})_c^\bullet I'$.

Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_b I$, alors pour tout $E (\approx_{pi})_c^\bullet E', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*, \mathbb{K}^{cn} (\approx_{pi})_c^\bullet \mathbb{K}'^{cn}, \widetilde{P}^* (\approx_{pi})_c^\bullet \widetilde{P}'^*, \widetilde{P}^{cn} (\approx_{pi})_c^\bullet \widetilde{P}'^{cn}$, il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'$ tels que $Q \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I', \widetilde{P}'^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}'^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E''$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Par induction sur le nombre de noms dans \widetilde{a} . Si \widetilde{a} est de taille 1, le résultat est vrai par le lemme A.58. Supposons les deux résultats vrais pour \widetilde{a} de taille n . Nous prouvons le premier résultat par une sous-induction sur la dérivation de $P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_b I$.

Supposons que la règle $\text{OUT}_{2,=}^k$ a été utilisée : nous avons $P = \bar{a}(P_1)P_2, E \xrightarrow{a^*, P_1} J, P_j \xrightarrow{\widetilde{a}', \xi, J, \mathbb{E}^*\{\square|P_2\}, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_{b'} I$ avec $\xi \in \{*, p\}$. Par le lemme A.54, il existe E_1, J' tel que $E' \xrightarrow{\tau} E_1 \xrightarrow{a^*, P_1} J'$ et $J (\approx_{pi})_c^\bullet J'$. Par l'hypothèse d'induction principale il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'$ tels que nous avons $\widetilde{P}'^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}'^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E_1 \xrightarrow{\tau} E'', P_j' \xrightarrow{\tau} P''^j \xrightarrow{\widetilde{a}', \xi, E'', \mathbb{E}'^*\{\square|P_2\}, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_{b'} I',$ et $I (\approx_{pi})_c^\bullet I'$. Par la règle $\text{OUT}_{2,=}^k$ nous avons $P \xrightarrow{\widetilde{a}' \uplus \bar{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^* \uplus P''^j, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_{b' \cup b} I'$ avec $E' \xrightarrow{\tau} E''$, le résultat est donc vrai. Les autres règles d'émission ou de passivation se traitent de la même manière.

Pour la règle PAR_{\leq}^k , nous avons $P = P_1 \mid P_2$ et $P_1 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*\{\square|P_2\}, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_b I$. Par l'hypothèse de sous-induction il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'$ tels que $\widetilde{P}'^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}'^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E'', P_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*\{\square|P_2\}, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I'$ et $I (\approx_{pi})_c^\bullet I'$. Par les règles PAR_{it}^k et PAR_{\leq}^k nous avons $P \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I'$, le résultat est donc vrai. Les règles $\text{PAR}_{<}^k, \text{RESTR}_{\leq}^k$ et $\text{RESTR}_{<}^k$ se traitent de la même manière.

Pour PAR-OUT_{\leq}^k , nous avons $P = P_1 \mid P_2$ et $P_1 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^* \uplus P_2, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_b I$. Par l'hypothèse de sous-induction il existe $\widetilde{P}''^*, P''_2, \widetilde{P}''^{cn}, E'', I'$ tels que $\widetilde{P}'^* \xrightarrow{\tau} \widetilde{P}''^*, P_2 \xrightarrow{\tau} P''_2, \widetilde{P}'^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E'', P_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^* \uplus P''_2, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I'$ et $I (\approx_{pi})_c^\bullet I'$. Par PAR_{it}^k et PAR_{\leq}^k nous avons $P \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I'$, le résultat est donc vrai. La règle $\text{PAR-OUT}_{<}^k$ se traite de la même manière.

Pour EXTR_{\leq}^k , nous avons $P = \nu d.P_1, P_1 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\}}_b I_1, d \in \widetilde{b}, d \notin \widetilde{a}$ et $I = \nu d.I_1$. Par l'hypothèse de sous-induction il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'_1$ tels que $\widetilde{P}'^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}'^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E'', P_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b I'_1$ et $I_1 (\approx_{pi})_c^\bullet I'_1$. Par RESTR_{it}^k et EXTR_{\leq}^k nous avons $P \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn}\{\widetilde{P}''^{cn}\}}_b \nu d.I'_1 \triangleq I'$, et nous avons $I (\approx_{pi})_c^\bullet I'$ par congruence de $(\approx_{pi})_c^\bullet$.

Pour LOC_{\leq}^k , nous avons $P = c[P_1]P_2$ et $P_1 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{cn}\{\widetilde{P}^{cn}\} \cup \mathbb{K}^{cn_0}\{\emptyset\}}_b I$ avec $\mathbb{K}^{cn_0} = c[\square]P_2$ et $c_{n_0} \notin \widetilde{c}_n$. Par l'hypothèse de sous-induction il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'',$

I' tels que $P_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \} \cup \mathbb{K}^{cn_0} \{ \emptyset \}} \xrightarrow{\tau} I', \widetilde{P}''^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}''^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E''$
et $I (\approx_{pi})_c^\bullet I'$. Par les règles LOC_{τ}^k et $\text{LOC}_{=}^k$ nous avons $P \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$, le résultat est donc vrai.

Nous prouvons maintenant le second résultat par induction sur la taille de $P \approx_{pi}^\bullet Q$.

Supposons $P \approx_{pi}^\circ Q$; comme les termes sont clos nous avons $P \approx_{pi} Q$. Par le premier résultat il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', J$ tels que $\widetilde{P}''^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}''^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E''$,
 $P \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} J$ et $I (\approx_{pi})_c^\bullet J$. Par le lemme A.50 il existe I' telle que
 $Q \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$ et $J \approx_{pi} I'$. Comme les termes sont clos, nous avons
 $J \approx_{pi}^\circ I'$, nous avons donc $I (\approx_{pi})_c^\bullet I'$ comme souhaité.

Supposons $P \approx_{pi}^\bullet T \approx_{pi}^\circ Q$. Soit σ une substitution qui clôt T : nous avons $P (\approx_{pi})_c^\bullet T \sigma$.
Par induction il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', J$ tels que $\widetilde{P}''^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}''^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E''$,
 $T \sigma \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} J$ et $I (\approx_{pi})_c^\bullet J$. Nous avons $T \sigma \approx_{pi} Q$ donc il existe I' telle
que $Q \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$ et $J \approx_{pi} I'$ par le lemme A.50. Comme les termes sont
clos, nous avons $J \approx_{pi}^\circ I'$, nous avons donc $I (\approx_{pi})_c^\bullet I'$ comme souhaité.

Supposons $P = op(\widetilde{P}_i)$ et $Q = op(\widetilde{Q}_i)$ avec $\widetilde{P}_i (\approx_{pi})_c^\bullet \widetilde{Q}_i$. Nous procédons par analyse de cas sur $op()$.

Si $P = \bar{a}\langle P_1 \rangle P_2$ et $Q = \bar{a}\langle Q_1 \rangle Q_2$, la transition de P peut provenir des règles $\text{OUT}_{2,=}^k$,
 $\text{OUT}_{3,=}^k$, $\text{OUT}_{2,<}^k$, $\text{OUT}_{3,<}^k$, $\text{OUT}_{5,<}^k$ ou $\text{OUT}_{4,<}^k$. Nous traitons que le cas $\text{OUT}_{2,=}^k$, les autres
étant similaires; nous avons $P_j \xrightarrow{\tau} \xrightarrow{\widetilde{a}', \xi, J, \mathbb{E}^* \{ \square | P_2 \}, \widetilde{P}''^*, \mathbb{K}^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I$ avec $E \xrightarrow{a^*, P_1} J$ et $\xi \in \{*, p\}$.
Par le lemme A.54, il existe E_1, J' tel que $E' \xrightarrow{\tau} E_1 \xrightarrow{a^*, Q_1} J'$ et $J (\approx_{pi})_c^\bullet J'$. Par l'hypothèse
d'induction principale il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'$ tels que $\widetilde{P}''^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}''^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E_1 \xrightarrow{\tau} E''$,
 $P'_j \xrightarrow{\tau} P''_j \xrightarrow{\tau} \xrightarrow{\widetilde{a}', \xi, E'', \mathbb{E}'^* \{ \square | Q_2 \}, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$, et $I (\approx_{pi})_c^\bullet I'$. Par la règle $\text{OUT}_{2,=}^k$ nous
avons $Q \xrightarrow{\tau} \xrightarrow{\widetilde{a}' \uplus \bar{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^* \uplus P''_j, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I' \cup_b I'$ avec $E' \xrightarrow{\tau} E''$, le résultat est donc vrai. Le
cas de la passivation se traite de la même manière.

Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, la transition de P peut provenir de $\text{PAR}_{=}^k$, $\text{PAR}_{<}^k$,
 $\text{PAR-OUT}_{=}^k$ ou $\text{PAR-OUT}_{<}^k$. Pour la règle $\text{PAR}_{=}^k$, nous avons $P_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^* \{ \square | P_2 \}, \widetilde{P}''^*, \mathbb{K}^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I$.
Par l'hypothèse de sous-induction il existe $\widetilde{P}''^*, \widetilde{P}''^{cn}, E'', I'$ tels que nous avons
 $Q_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^* \{ \square | Q_2 \}, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I', \widetilde{P}''^* \xrightarrow{\tau} \widetilde{P}''^*, \widetilde{P}''^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}, E' \xrightarrow{\tau} E''$ et $I (\approx_{pi})_c^\bullet I'$.
Par les règles $\text{PAR}_{i\tau}^k$ et $\text{PAR}_{=}^k$ nous avons $Q \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$, le résultat est
donc vrai. Le cas de $\text{PAR}_{<}^k$ se traite de la même manière.

Pour $\text{PAR-OUT}_{=}^k$, nous avons $P_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}''^* \uplus P_2, \mathbb{K}^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I$. Par l'hypothèse de sous-
induction il existe $\widetilde{P}''^*, Q''_2, \widetilde{P}''^{cn}, E'', I'$ tels que $\widetilde{P}''^* \xrightarrow{\tau} \widetilde{P}''^*, Q_2 \xrightarrow{\tau} Q''_2, \widetilde{P}''^{cn} \xrightarrow{\tau} \widetilde{P}''^{cn}$,
 $E' \xrightarrow{\tau} E''$, $Q_1 \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^* \uplus Q''_2, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$ et $I (\approx_{pi})_c^\bullet I'$. Par $\text{PAR}_{i\tau}^k$ et $\text{PAR}_{=}^k$ nous
avons $Q \xrightarrow{\tau} \xrightarrow{\widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{cn} \{ \widetilde{P}''^{cn} \}} \xrightarrow{\tau} I'$, le résultat est donc vrai. La règle $\text{PAR-OUT}_{<}^k$ se
traite de la même manière.

Si $P = \nu d.P_1$ et $Q = \nu d.Q_1$, la transition de P peut provenir de $\text{RESTR}_{<}^k$, $\text{RESTR}_{=}^k$
ou $\text{EXTR}_{<}^k$. Les règles $\text{RESTR}_{<}^k$ et $\text{RESTR}_{=}^k$ se traitent comme $\text{PAR}_{=}^k$. Pour $\text{EXTR}_{<}^k$, nous

avons $P_1 \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P}^{c_n}\}} \widetilde{b} I_1$, $d \in \widetilde{b}$, $d \notin \widetilde{a}$ et $I = \nu d.I_1$. Par l'hypothèse de sous-induction il existe \widetilde{P}''^* , \widetilde{P}''^{c_n} , E'' , I'_1 tels que $\widetilde{P}^* \xrightarrow{\tau} \widetilde{P}''^*$, $\widetilde{P}^{c_n} \xrightarrow{\tau} \widetilde{P}''^{c_n}$, $E' \xrightarrow{\tau} E''$, $Q_1 \xrightarrow{\tau} \widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{c_n} \{\widetilde{P}''^{c_n}\} \widetilde{b} I'_1$ et $I_1 (\approx_{pi})_c^\bullet I'_1$. Par $\text{RESTR}_{i\tau}^k$ et EXTR_{\leq}^k nous avons $Q \xrightarrow{\tau} \widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{c_n} \{\widetilde{P}''^{c_n}\} \widetilde{b} \nu d.I'_1 \triangleq I'$, et nous avons $I (\approx_{pi})_c^\bullet I'$ par congruence de $(\approx_{pi})_c^\bullet$.

Si $P = c[P_1]P_2$ et $Q = c[Q_1]Q_2$, la transition de P provient de la règle LOC_{\leq}^k : nous avons $P_1 \xrightarrow{\widetilde{a}, c_{n_0}, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P}^{c_n}\} \cup \mathbb{K}^{c_{n_0}} \{\emptyset\}} \widetilde{b} I$ avec $\mathbb{K}^{c_{n_0}} = c[\square]P_2$ et $c_{n_0} \notin \widetilde{c}_n$. Soit $\mathbb{K}'^{c_{n_0}} = c[\square]Q_2$. Par l'hypothèse de sous-induction il existe \widetilde{P}''^* , \widetilde{P}''^{c_n} , E'' , I' tels que $Q_1 \xrightarrow{\tau} \widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{c_n} \{\widetilde{P}''^{c_n}\} \cup \mathbb{K}'^{c_{n_0}} \{\emptyset\} \widetilde{b} I'$, $\widetilde{P}^* \xrightarrow{\tau} \widetilde{P}''^*$, $\widetilde{P}^{c_n} \xrightarrow{\tau} \widetilde{P}''^{c_n}$, $E' \xrightarrow{\tau} E''$ et $I (\approx_{pi})_c^\bullet I'$. Par les règles LOC_{τ}^k et LOC_{\leq}^k nous avons $Q \xrightarrow{\tau} \widetilde{a}, \xi, E'', \mathbb{E}'^*, \widetilde{P}''^*, \mathbb{K}'^{c_n} \{\widetilde{P}''^{c_n}\} \widetilde{b} I'$, le résultat est donc vrai. \square

Lemme A.60. Si $\mathbb{E} \approx_m^\bullet \mathbb{F}$ et $\mathbb{E} = \mathbb{E}_1\{\nu c.\mathbb{E}_2\}$, il existe $\mathbb{F}_1, \mathbb{F}_2$ tels que $\mathbb{F} = \mathbb{F}_1\{\nu c.\mathbb{F}_2\}$, $\mathbb{E}_1 \approx_m^\bullet \mathbb{F}_1$ et $\mathbb{E}_2 \approx_m^\bullet \mathbb{F}_2$. Nous avons un résultat similaire avec $\mathbb{K} \approx_m^\bullet \mathbb{K}'$

Démonstration. Facile par induction sur $\mathbb{E} \approx_m^\bullet \mathbb{F}$ ou $\mathbb{K} \approx_m^\bullet \mathbb{K}'$. \square

Lemme A.61. Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\widetilde{a}, \xi, E, \mathbb{E}^*, \widetilde{P}^*, \mathbb{K}^{c_n} \{\widetilde{P}^{c_n}\}} \widetilde{b} I$, alors pour tout $E (\approx_{pi})_c^\bullet E'$, $\mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*$, $\mathbb{K}^{c_n} (\approx_{pi})_c^\bullet \mathbb{K}'^{c_n}$, $\widetilde{P}^* (\approx_{pi})_c^\bullet \widetilde{P}'^*$, $\widetilde{P}^{c_n} (\approx_{pi})_c^\bullet \widetilde{P}'^{c_n}$, il existe I' telle que $Q \xrightarrow{\widetilde{a}, \xi, E', \mathbb{E}'^*, \widetilde{P}'^*, \mathbb{K}'^{c_n} \{\widetilde{P}'^{c_n}\}} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Par induction sur le nombre de captures par les contextes. La preuve est semblable à celle du lemme A.29 pour $\text{HO}\pi\text{P}$. \square

Lemme A.62. Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\leq, \theta} I$, il existe I' telle que $Q \xrightarrow{\tau, \leq, \theta} I'$ et $I \approx_m^\bullet I'$.

Démonstration. Par induction sur la taille de $P (\approx_{pi})_c^\bullet Q$. \square

Lemme A.63. La dérivation d'un jugement $P \xrightarrow{\widetilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P}^\uparrow} \widetilde{b} I$ n'utilise pas la règle $\text{PAR-OUT}_{>}^k$. En outre nous avons $\widetilde{P}^\uparrow = \emptyset$.

Démonstration. Similaire à celle du lemme A.43. \square

Lemme A.64. Si $P \xrightarrow{\widetilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \emptyset} \widetilde{b} I$, alors pour tout $E (\approx_{pi})_c^\bullet E'$, $\mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*$, il existe I' tel que $P \xrightarrow{\widetilde{a}, \uparrow, E', \mathbb{E}'^*, \emptyset} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\widetilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \emptyset} \widetilde{b} I$, alors pour tout $E (\approx_{pi})_c^\bullet E'$, $\mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*$, il existe E'' , I' tels que $E' \xrightarrow{\tau} E''$ et $Q \xrightarrow{\tau, \widetilde{a}, \uparrow, E'', \mathbb{E}'^*, \emptyset} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Similaire à celle du lemme A.58. \square

Lemme A.65. Si $P \xrightarrow{\widetilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P}^\uparrow} \widetilde{b} I$, alors pour tout $E (\approx_{pi})_c^\bullet E'$, $\mathbb{E}^\uparrow (\approx_{pi})_c^\bullet \mathbb{E}'^\uparrow$, $\widetilde{P}^\uparrow (\approx_{pi})_c^\bullet \widetilde{P}'^\uparrow$, il existe \widetilde{P}''^\uparrow , E'' , I' tels que $\widetilde{P}^\uparrow \xrightarrow{\tau} \widetilde{P}''^\uparrow$, $E' \xrightarrow{\tau} E''$, $P \xrightarrow{\tau, \widetilde{a}, \uparrow, E'', \mathbb{E}'^\uparrow, \widetilde{P}''^\uparrow} \widetilde{b} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{\widetilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \widetilde{P}^\uparrow} \widetilde{b} I$, alors pour tout $E (\approx_{pi})_c^\bullet E'$, $\mathbb{E}^\uparrow (\approx_{pi})_c^\bullet \mathbb{E}'^\uparrow$, $\widetilde{P}^\uparrow (\approx_{pi})_c^\bullet \widetilde{P}'^\uparrow$, il existe \widetilde{P}''^\uparrow , E'' , I' tels que $Q \xrightarrow{\tau, \widetilde{a}, \uparrow, E', \mathbb{E}'^\uparrow, \widetilde{P}'^\uparrow} \widetilde{b} I'$, $\widetilde{P}^\uparrow \xrightarrow{\tau} \widetilde{P}''^\uparrow$, $E' \xrightarrow{\tau} E''$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Similaire à celle du lemme A.59. \square

Lemme A.66. Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow[\sim]{\tilde{a}, \uparrow, E, \mathbb{E}^\uparrow, \tilde{P}^\uparrow} I$, alors pour tout $E (\approx_{pi})_c^\bullet E', \mathbb{E}^\uparrow (\approx_{pi})_c^\bullet \mathbb{E}'^\uparrow, \tilde{P}^\uparrow (\approx_{pi})_c^\bullet \tilde{P}'^\uparrow$, il existe I' tel que $Q \xrightarrow[\sim]{\tilde{a}, \uparrow, E', \mathbb{E}'^\uparrow, \tilde{P}'^\uparrow} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Par induction sur le nombre de captures par les contextes. La preuve est semblable à celle du lemme A.29 pour $\text{HO}\pi\text{P}$. \square

Lemme A.67. Si $P (\approx_{pi})_c^\bullet Q$ et $P \xrightarrow{> \theta} I$, il existe I' telle que $Q \xrightarrow{\tau} \xrightarrow{> \theta} I'$ et $I (\approx_{pi})_c^\bullet I'$.

Démonstration. Par induction sur la taille de $P (\approx_{pi})_c^\bullet Q$. \square

Lemme A.68. Soient $P (\approx_{pi})_c^\bullet Q$.

Si $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' (\approx_{pi})_c^\bullet Q'$.

Si $P \xrightarrow[\sim]{\tilde{a}, \Xi, \mathbb{E}^\uparrow \{\tilde{P}^\uparrow\}, \Delta, R, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{cn} \{\tilde{P}^{cn}\}} P'$, alors $\forall \mathbb{E}^\uparrow (\approx_{pi})_c^\bullet \mathbb{E}'^\uparrow, \Delta (\approx_{pi})_c^\bullet \Delta', \mathbb{E}^* (\approx_{pi})_c^\bullet \mathbb{E}'^*, \mathbb{K}^{cn} (\approx_{pi})_c^\bullet \mathbb{K}'^{cn}, \tilde{P}^\uparrow (\approx_{pi})_c^\bullet \tilde{P}'^\uparrow, R (\approx_{pi})_c^\bullet R', \tilde{P}^* (\approx_{pi})_c^\bullet \tilde{P}'^*, \tilde{P}^{cn} (\approx_{pi})_c^\bullet \tilde{P}'^{cn}$, il existe Q' tel que $Q \xrightarrow[\sim]{\tilde{a}, \Xi, \mathbb{E}'^\uparrow \{\tilde{P}'^\uparrow\}, \Delta', R', \mathbb{E}'^*, \tilde{P}'^*, \mathbb{K}'^{cn} \{\tilde{P}'^{cn}\}} Q'$ et $P' (\approx_{pi})_c^\bullet Q'$.

Démonstration. La première clause est prouvée classiquement par induction sur la taille de $P (\approx_{pi})_c^\bullet Q$, en utilisant les lemmes A.61, A.62, A.66 et A.67 pour les règles de communication.

La deuxième clause est prouvée par analyse de cas sur $P \xrightarrow[\sim]{\tilde{a}, \Xi, \mathbb{E}^\uparrow \{\tilde{P}^\uparrow\}, \Delta, R, \mathbb{E}^*, \tilde{P}^*, \mathbb{K}^{cn} \{\tilde{P}^{cn}\}} P'$ à l'aide des lemmes A.61 et A.66. \square

Lemme A.69. La relation $(\approx_{pi})_c^{\bullet*}$ est une bisimulation faible à complément sur les réceptions partielles.

Démonstration. Les lemmes A.52, A.54, A.61, A.62, A.66, A.67 et A.68 permettent de montrer que $(\approx_{pi})_c^{\bullet*}$ est une simulation faible à complément sur les réceptions partielles, et la relation est symétrique par le lemme A.4. \square

Théorème A.4. La relation \approx_{pi} est une congruence.

Démonstration. Immédiat par les lemmes A.69 et A.5. \square

Annexe B

Preuves pour HOP

B.1 Congruence

Nous prouvons la congruence de la bisimilarité d'ordre supérieur en utilisant la méthode de Howe. Nous traitons uniquement le cas de la bisimilarité précoce forte, les preuves dans les cas faibles et/ou tardifs sont similaires. Nous notons \sim^\bullet la clôture de Howe de \sim^\bullet , et nous notons \sim_c^\bullet la restriction aux termes clos de \sim^\bullet .

Lemme B.1. Soient $P \sim_c^\bullet Q$.

- Si $P \xrightarrow{\tau} P'$, il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $P' \sim_c^\bullet Q'$.
- Si $P \xrightarrow{a} F$, pour tout $R \sim_c^\bullet R'$, il existe F' tel que $Q \xrightarrow{a} F'$ et $F \circ R \sim_c^\bullet F' \circ R'$.
- Si $P \xrightarrow{\bar{a}} \langle R \rangle S$, il existe R', S' tels que $Q \xrightarrow{\bar{a}} \langle R' \rangle S'$, $R \sim_c^\bullet R'$ et $S \sim_c^\bullet S'$.

Démonstration. Par induction sur la taille de la preuve de $P \sim_c^\bullet Q$.

Supposons $P \sim^\circ Q$. Comme les processus sont clos, nous avons $P \sim Q$. La première et la dernière clause sont vraies par définition de la bisimilarité. Si $P \xrightarrow{a} F$, alors il existe F' telle que $Q \xrightarrow{a} F'$ et $F \circ R' \sim F' \circ R'$; comme les termes sont clos, nous avons $F \circ R' \sim^\circ F' \circ R'$. Par congruence de \sim^\bullet , nous avons $F \circ R \sim^\bullet F' \circ R'$. Nous avons donc $F \circ R \sim^\bullet \sim^\circ F' \circ R'$, comme voulu.

Supposons $P \sim^\bullet T \sim^\circ Q$. Soit σ une substitution qui clôt T . Par le lemme A.3, nous avons $P \sim_c^\bullet T\sigma$ avec une dérivation de même taille. Si $P \xrightarrow{\tau} P'$, alors par induction il existe T' tel que $T \xrightarrow{\tau} T'$ et $P' \sim_c^\bullet T'$. Nous avons $T\sigma \sim Q$, donc par bisimilarité il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $T' \sim Q'$. Comme les termes sont clos, nous avons $T' \sim^\circ Q'$; nous avons donc $P' \sim^\bullet \sim^\circ Q'$, soit $P' \sim_c^\bullet Q'$ comme P' et Q' sont clos. Le cas de l'émission se traite de la même manière. Si $P \xrightarrow{a} F$, alors par induction il existe F' telle que $T\sigma \xrightarrow{a} F'$ et $F \circ R \sim^\bullet F' \circ R'$. Nous avons $T\sigma \sim Q$, donc par bisimilarité, il existe F'' tel que $Q \xrightarrow{a} F''$ et $F' \circ R' \sim F'' \circ R'$. Comme les termes sont clos, nous avons $F' \circ R' \sim^\circ F'' \circ R'$, donc nous avons $F \circ R \sim_c^\bullet \sim^\circ F'' \circ R'$, soit $F \circ R \sim_c^\bullet F'' \circ R'$ comme souhaité.

Supposons $P = op(\tilde{P}_i)$, $Q = op(\tilde{Q}_i)$ avec $\tilde{P}_i \sim_c^\bullet \tilde{Q}_i$. Nous procédons par analyse de cas sur op .

Si $P = a(X)P_1$ et $Q = a(X)Q_1$, la seule transition possible pour P est $P \xrightarrow{a} (X)P_1$. Nous avons également $Q \xrightarrow{a} (X)Q_1$, et par le lemme A.2, nous avons $P_1\{R/X\} \sim_c^\bullet Q_1\{R'/X\}$. Nous avons donc $(X)P_1 \circ R \sim_c^\bullet (X)Q_1 \circ R'$ comme voulu.

Si $P = \bar{a}\langle P_1 \rangle P_2$ et $Q = \bar{a}\langle Q_1 \rangle Q_2$, la seule transition possible pour P est $P \xrightarrow{\bar{a}} \langle P_1 \rangle P_2$. Nous avons également $Q \xrightarrow{\bar{a}} \langle Q_1 \rangle Q_2$ avec $P_1 \sim_c^\bullet Q_1$ et $P_2 \sim_c^\bullet Q_2$ comme souhaité.

Si $P = P_1 \mid P_2$ et $Q = Q_1 \mid Q_2$, les transitions de P peuvent provenir des règles PAR, HO ou de leur symétrique. Si $P \xrightarrow{\tau} P'_1 \mid P_2 \triangleq P'$ avec $P_1 \xrightarrow{\tau} P'_1$, alors par induction il existe Q'_1 tel que $Q_1 \xrightarrow{\tau} Q'_1$ et $P_1 \sim_c^\bullet Q'_1$. Par la règle PAR nous avons $Q \xrightarrow{\tau} Q'_1 \mid Q_2 \triangleq Q'$, et par congruence de \sim^\bullet nous avons $P' \sim_c^\bullet Q'$ comme souhaité. Le cas de l'émission en

provenance de P_1 se traite de la même manière. Si $P \xrightarrow{a} F_1 \mid P_2 \triangleq F$ avec $P_1 \xrightarrow{a} F_1$, alors par induction il existe F'_1 telle que $Q_1 \xrightarrow{a} F'_1$ et $F_1 \circ R \sim_c^\bullet F'_1 \circ R'$. Par la règle PAR nous avons $Q \xrightarrow{a} F'_1 \mid P_2 \triangleq F'$, et par congruence de \sim_c^\bullet nous avons $F_1 \circ R \mid P_2 \sim_c^\bullet F'_1 \circ R' \mid P_2$, soit $F \circ R \sim_c^\bullet F' \circ R'$ comme souhaité. Si $P \xrightarrow{\tau} F \bullet \langle R \rangle S \triangleq P'$ avec $P_1 \xrightarrow{a} F$ et $P_2 \xrightarrow{\bar{a}} \langle R \rangle S$, alors par induction il existe R', S' tels que $Q_2 \xrightarrow{\bar{a}} \langle R' \rangle S'$, $R \sim_c^\bullet R'$ et $S \sim_c^\bullet S'$. Il existe également F' telle que $Q_1 \xrightarrow{a} F'$ et $F \circ R \sim_c^\bullet F' \circ R'$. Par HO nous avons $Q \xrightarrow{\tau} F' \bullet \langle R' \rangle S' \triangleq Q'$, et par congruence nous avons $F \circ R \mid S \sim_c^\bullet F' \circ R' \mid S'$, soit $F \bullet \langle R \rangle S \sim_c^\bullet F' \bullet \langle R' \rangle S'$ comme souhaité.

Si $P = a[P_1]$, les transitions provenant de la passivation se traitent comme l'émission de message, et les transitions provenant de la règle LOC se traitent comme celles provenant de PAR. Le cas $P = P_1 + P_2$ est facile. Si $P = !P_1$, alors les transitions provenant de la règle REPLIC se traitent comme celles provenant de PAR, et celles provenant de REPLIC-HO se traitent comme celles ayant pour origine HO. \square

Lemme B.2. *La relation $\sim_c^{\bullet*}$ est une bisimilarité forte d'ordre supérieur.*

Démonstration. Le lemme B.1 permet de montrer que $\sim_c^{\bullet*}$ est une similarité forte d'ordre supérieur, et $\sim_c^{\bullet*}$ est symétrique par le lemme A.4. \square

Les preuves de complétude dans les cas fort et faible sont disponibles dans [25]. Elles suivent le principe décrit en section 2.2.3 et mis en œuvre avec la bisimilarité à complément de HO π P (section A.3.4).

B.2 Bisimilarité normale

Lemme B.3. *Soit \mathbb{E} un contexte d'évaluation. Si $P \xrightarrow{\alpha} A$, alors il existe \mathbb{E}' tel que $\mathbb{E}\{P\} \xrightarrow{\alpha} \mathbb{E}'\{A\}$, et le trou \square n'est pas sous un opérateur de réplication ou de somme dans \mathbb{E}' .*

Démonstration. Immédiat par induction sur \mathbb{E} et d'après les règles REPLIC et SUM. \square

Lemme B.4. *Soient P, Q tels que $fv(P, Q) \subseteq \{X\}$ et m, n qui n'apparaissent pas dans P, Q . Supposons que $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q\{\bar{m}.\bar{n}.\mathbf{0}/X\}$ et que la transition $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Y\} \triangleq P_n$ est imitée par $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Y\} \triangleq Q_n$ avec $P_n \sim_l Q_n$. Nous avons deux possibilités :*

- soit il existe $P_1 \sim_l Q_1$ tels que $P_n \equiv \bar{n}.\mathbf{0} \mid P_1$, $Q_n \equiv \bar{n}.\mathbf{0} \mid Q_1$ et $P_1 \sim_l Q_1$;
- ou alors il existe $k \geq 0$, a_1, \dots, a_k , $P_1 \dots P_{k+1}$, $Q_1 \dots Q_{k+1}$ tels que

$$\begin{aligned} P_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.\mathbf{0} \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1 \\ Q_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.\mathbf{0} \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1 \end{aligned}$$

et pour tout $1 \leq j \leq k+1$, on a $P_j \sim_l Q_j$.

Démonstration. Nous avons $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} P_n$ et $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} Q_n$, donc les occurrences de $\bar{m}.\bar{n}.\mathbf{0}$ qui se réduisent dans P et Q se trouvent dans des contextes d'évaluation. D'après le lemme B.3, les occurrences de $\bar{n}.\mathbf{0}$ dans P_n et Q_n se trouvent uniquement sous des compositions parallèles ou dans des localités. Comme n est frais pour P et Q , P_n et Q_n peuvent effectuer chacun exactement une transition $\xrightarrow{\bar{n}}$.

Supposons que $\bar{n}.\mathbf{0}$ n'est pas dans une localité dans P_n . Si $\bar{n}.\mathbf{0}$ est dans une localité dans Q_n , alors il existe une transition $Q_n \xrightarrow{\bar{a}} \langle R_n \rangle S$ avec $R_n \xrightarrow{\bar{n}}$. Comme nous avons $P_n \sim_l Q_n$, le processus $\bar{n}.\mathbf{0}$ dans P_n peut être émis, alors qu'il est dans un contexte d'évaluation. Ce n'est possible seulement si $\bar{n}.\mathbf{0}$ est dans une localité, contradiction. Donc $\bar{n}.\mathbf{0}$ n'est pas

dans une localité dans Q_n . Donc il existe P_1, Q_1 tels que $P_n \equiv \bar{n}.0 \mid P_1$ et $Q_n \equiv \bar{n}.0 \mid Q_1$. Comme la transition $P_n \xrightarrow{\bar{n}} P_1$ ne peut être imitée que par $Q_n \xrightarrow{\bar{n}} Q_1$, nous avons $P_1 \sim_l Q_1$. Nous pouvons également montrer que si $\bar{n}.0$ n'est pas dans une localité dans Q_n , alors il n'est pas dans une localité dans P_n , et nous pouvons décomposer P_n et Q_n de la même manière.

Supposons maintenant que $\bar{n}.0$ est sous la hiérarchie de localités $a_1 \dots a_k$ dans P_n et sous la hiérarchie $b_1 \dots b_l$ dans Q_n . Supposons $k > l$. Nous avons $P_n \xrightarrow{\bar{a}_1} \langle R_n^1 \rangle P_1$ avec $R_n^1 \xrightarrow{\bar{n}}$; comme $P_n \sim_l Q_n$, il existe R_n^1, Q_1 tels que $Q_n \xrightarrow{\bar{a}_1} \langle R_n^1 \rangle Q_1$, $R_n^1 \sim_l R_n^1$ et $P_1 \sim_l Q_1$. Le processus $\bar{n}.0$ est sous $k-1$ localités dans R_n^1 et sous $l-i$ localités dans R_n^l , avec $i > 0$. En considérant $l-1$ passivations successives, nous définissons R_n^l issu de P_n et R_n^l issu de Q_n tels que $R_n^l \sim_l R_n^l$ et de sorte que $\bar{n}.0$ est sous $k-l > 0$ localités dans R_n^l et n'est pas dans une localité dans R_n^l : contradiction. Avec le même raisonnement, nous prouvons que le cas $k < l$ est impossible, nous avons donc $k = l$. En considérant les réponses de Q_n aux k passivations successives de P_n , nous montrons également que nous avons $a_i = b_i$ pour tout $i \in \{1 \dots k\}$.

Il existe donc $P_1 \dots P_{k+1}, Q_1 \dots Q_{k+1}$, tels que

$$\begin{aligned} P_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.0 \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1 \\ Q_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.0 \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1 \end{aligned}$$

Nous notons R_n^i (respectivement R_n^i) le processus à l'intérieur de la localité a_i dans P_n (respectivement Q_n). Nous avons $P_n \xrightarrow{\bar{a}_1} \langle R_n^1 \rangle P_1$; cette transition ne peut être imitée que par $Q_n \xrightarrow{\bar{a}_1} \langle R_n^1 \rangle P_1$, en raisonnant comme précédemment sur le nombre de localités englobant $\bar{n}.0$. Nous avons donc $R_n^1 \sim_l R_n^1$ et $P_1 \sim_l Q_1$. Par induction sur $j \in \{1 \dots k\}$, nous montrons que nous avons $R_n^j \sim_l R_n^j$ et $P_j \sim_l Q_j$. Pour $j = k$, nous avons $R_n^k \sim_l R_n^k$, c'est-à-dire $\bar{n}.0 \mid P_{k+1} \sim_l \bar{n}.0 \mid Q_{k+1}$. La transition $R_n^k \xrightarrow{\bar{n}} P_{k+1}$ ne peut être imitée que par $R_n^k \xrightarrow{\bar{n}} Q_{k+1}$, nous avons donc $P_{k+1} \sim_l Q_{k+1}$. □

Lemme B.5. Soient P, Q tels que $fv(P, Q) \subseteq \{X\}$ et m, n qui n'apparaissent pas dans P, Q . Supposons que $P\{\bar{m}.\bar{n}.0/X\} \sim_l Q\{\bar{m}.\bar{n}.0/X\}$ et que la transition $P\{\bar{m}.\bar{n}.0/X\} \xrightarrow{\bar{m}} P'\{\bar{m}.\bar{n}.0/X\}\{\bar{n}.0/Y\} \triangleq P_n$ est imitée par $Q\{\bar{m}.\bar{n}.0/X\} \xrightarrow{\bar{m}} Q'\{\bar{m}.\bar{n}.0/X\}\{\bar{n}.0/Y\} \triangleq Q_n$ avec $P_n \sim_l Q_n$. Soit $R \sim_l R'$; nous avons $\{\{\bar{m}.\bar{n}.0/P'\}R/Y\} \sim_l Q'\{\bar{m}.\bar{n}.0/X\}\{R'/Y\}$.

Démonstration. D'après le lemme B.4, nous avons deux possibilités.

Si $P_n \equiv \bar{n}.0 \mid P_1, Q_n \equiv \bar{n}.0 \mid Q_1$ avec $P_1 \sim_l Q_1$, alors par congruence et transitivité de \sim_l nous avons $R \mid P_1 \sim_l R' \mid Q_1$.

Si

$$\begin{aligned} P_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.0 \mid P_{k+1}] \mid P_k] \mid P_{k-1} \dots] \mid P_1 \\ Q_n &\equiv a_1[\dots a_{k-1}[a_k[\bar{n}.0 \mid Q_{k+1}] \mid Q_k] \mid Q_{k-1} \dots] \mid Q_1 \end{aligned}$$

alors par induction sur $j \in \{1 \dots k\}$, nous montrons que nous avons $a_j[\dots a_k[R \mid P_{k+1}] \mid P_k \dots] \mid P_j \sim_l a_j[\dots a_k[R' \mid Q_{k+1}] \mid Q_k \dots] \mid Q_j$, en utilisant la congruence et la transitivité de \sim_l . Le résultat est alors vrai en prenant $j = 1$. □

Théorème B.1. Soient P, Q deux processus tels que $fv(P, Q) \subseteq \{X\}$ et m, n deux noms qui n'apparaissent pas dans P, Q . Si $P\{\bar{m}.\bar{n}.0/X\} \sim_l Q\{\bar{m}.\bar{n}.0/X\}$, alors pour tout processus clos R , on a $P\{R/X\} \sim_l Q\{R/X\}$

Démonstration. Soit

$$\mathcal{R} \triangleq \{(P\{R/X\}, Q\{R/X\}), P\{\bar{m}.\bar{n}.0/X\} \sim_l Q\{\bar{m}.\bar{n}.0/X\}\}.$$

Nous montrons que \mathcal{R} est une bisimulation tardive d'ordre supérieure. La relation est symétrique, il suffit donc de montrer qu'il s'agit d'une simulation. Nous procédons par analyse de cas sur les transitions de $P\{R/X\}$.

Si la transition est engendrée uniquement par P , nous avons $P\{R/X\} \xrightarrow{\alpha} A\{R/X\}$ avec $P \xrightarrow{\alpha} A$. Nous avons donc $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} A\{\bar{m}.\bar{n}.\mathbf{0}/X\}$. La transition $\xrightarrow{\alpha}$ provient de P , qui ne contient pas d'occurrences de m, n , donc m, n n'apparaissent pas dans α . Nous distinguons les trois cas possibles pour A .

- Supposons que A est un processus P' . Comme $P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q\{\bar{m}.\bar{n}.\mathbf{0}/X\}$, il existe Q' tel que $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} Q'$ et $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l Q'$. Comme $m, n \notin \alpha$, la transition $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} Q'$ provient de Q : il existe Q'' tel que $Q \xrightarrow{\alpha} Q''$ et $Q' = Q''\{\bar{m}.\bar{n}.\mathbf{0}/X\}$. Nous avons donc $Q\{R/X\} \xrightarrow{\alpha} Q''\{R/X\}$ avec $P'\{R/X\} \mathcal{R} Q''\{R/X\}$, comme voulu.
- Supposons que A est une fonction F . Il existe F' telle que $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} F'$ et $(F\{\bar{m}.\bar{n}.\mathbf{0}/X\}) \circ T \sim_l F' \circ T$ pour tout processus T . Comme $m, n \notin \alpha$, la transition $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} F'$ provient de Q : il existe F'' tel que $Q \xrightarrow{\alpha} F''$ et $F' = F''\{\bar{m}.\bar{n}.\mathbf{0}/X\}$. Nous avons donc $Q\{R/X\} \xrightarrow{\alpha} F''\{R/X\}$, et pour tout T clos, nous avons $(F\{R/X\}) \circ T = (F \circ T)\{R/X\}$ et $(F''\{R/X\}) \circ T = (F'' \circ T)\{R/X\}$. Nous avons également $(F \circ T)\{\bar{m}.\bar{n}.\mathbf{0}/X\} = (F\{\bar{m}.\bar{n}.\mathbf{0}/X\}) \circ T \sim_l (F''\{\bar{m}.\bar{n}.\mathbf{0}/X\}) \circ T = (F'' \circ T)\{\bar{m}.\bar{n}.\mathbf{0}/X\}$. Finalement nous avons donc $(F \circ T)\{R/X\} \mathcal{R} (F'' \circ T)\{R/X\}$ comme voulu.
- Supposons que $A = \langle S \rangle T$. Il existe S' et T' tels que $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} \langle S' \rangle T'$, $S\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l S'$ et $T\{\bar{m}.\bar{n}.\mathbf{0}/X\} \sim_l T'$. Comme nous avons $m, n \notin \alpha$, la transition $Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\alpha} \langle S' \rangle T'$ provient de Q : il existe S'' , T'' tels que $Q \xrightarrow{\alpha} \langle S'' \rangle T''$, $S' = S''\{\bar{m}.\bar{n}.\mathbf{0}/X\}$ et $T' = T''\{\bar{m}.\bar{n}.\mathbf{0}/X\}$. Par conséquent, nous avons $Q\{R/X\} \xrightarrow{\alpha} \langle S'' \rangle T''\{R/X\}$ avec $S\{R/X\} \mathcal{R} S''\{R/X\}$ et $T\{R/X\} \mathcal{R} T''\{R/X\}$, comme voulu.

Supposons que la transition provient uniquement d'une copie de R : nous avons $P\{R/X\} \xrightarrow{\alpha} P'\{R/X\}\{A/Y\}$ avec $R \xrightarrow{\alpha} A$. Cette copie de R se trouve dans un contexte d'évaluation, nous avons donc

$$P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Y\} \triangleq P_n.$$

Par l'hypothèse de bisimilarité, il existe Q' tel que

$$Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Y\} \triangleq Q_n$$

et $P_n \sim_l Q_n$. Nous avons donc $Q\{R/X\} \xrightarrow{\alpha} Q'\{R/X\}\{A/Y\}$. Nous distinguons les différents cas pour A .

- Supposons $A = R'$. Nous avons $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{R'/Y\} \sim_l Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{R'/Y\}$ par le lemme B.5. Par conséquent nous avons $P'\{R/X\}\{R'/Y\} \mathcal{R} Q'\{R/X\}\{R'/Y\}$ comme voulu.
- Supposons $A = F$. Pour tout processus T , nous avons $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ T/Y\} \sim_l Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ T/Y\}$ par le lemme B.5. Nous avons donc $P'\{R/X\}\{F \circ T/Y\} \mathcal{R} Q'\{R/X\}\{F \circ T/Y\}$ comme voulu.
- Supposons $A = \langle S \rangle T$. Nous avons $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{T/Y\} \sim_l Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{T/Y\}$ par le lemme B.5. Nous avons $P'\{R/X\}\{T/Y\} \mathcal{R} Q'\{R/X\}\{T/Y\}$ et $S \mathcal{R} S$ comme voulu.

Si la transition de P provient de la communication entre une copie de R et un sous-processus P' de P , nous avons deux cas à considérer. Si le message est émis par P' , alors il existe F, S, T tels que $R \xrightarrow{a} F$ et $P' \xrightarrow{\bar{a}} \langle S\{R/X\} \rangle T\{R/X\}$ pour un certain a . Nous avons la transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_R^1\{\mathbb{E}_R^2\{F \circ (S\{R/X\})\} \mid \mathbb{E}_R^3\{T\{R/X\}\}\}$$

pour certains contextes $\mathbb{E}_R^1, \mathbb{E}_R^2, \mathbb{E}_R^3$ (nous notons en indice le processus substitué aux variables des contextes, ici R). Nous avons

$$P\{\overline{m}.\overline{n}.\mathbf{0}/X\} \xrightarrow{\overline{m}} \xrightarrow{\overline{a}} \langle S\{\overline{m}.\overline{n}.\mathbf{0}/X\} \rangle \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^2 \{ \overline{n}.\mathbf{0} \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^3 \{ T\{\overline{m}.\overline{n}.\mathbf{0}/X\} \} \} \}$$

donc par l'hypothèse de bisimilarité, il existe S', \mathbb{E}' tels que

$$Q\{\overline{m}.\overline{n}.\mathbf{0}/X\} \xrightarrow{\overline{m}} \xrightarrow{\overline{a}} \langle S'\{\overline{m}.\overline{n}.\mathbf{0}/X\} \rangle \mathbb{E}'_{\overline{m}.\overline{n}.\mathbf{0}} \{ \overline{n}.\mathbf{0} \}$$

et les messages et continuations sont bisimilaires, c'est-à-dire

$$S\{\overline{m}.\overline{n}.\mathbf{0}/X\} \sim_l S'\{\overline{m}.\overline{n}.\mathbf{0}/X\}$$

et

$$\mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^2 \{ \overline{n}.\mathbf{0} \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^3 \{ T\{\overline{m}.\overline{n}.\mathbf{0}/X\} \} \} \} \sim_l \mathbb{E}'_{\overline{m}.\overline{n}.\mathbf{0}} \{ \overline{n}.\mathbf{0} \}$$

De la bisimilarité des messages, on déduit par congruence de \sim_l

$$F \circ (S\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \sim_l F \circ (S'\{\overline{m}.\overline{n}.\mathbf{0}/X\})$$

Donc par le lemme B.5 et par la bisimilarité des continuations, nous avons

$$\begin{aligned} \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^2 \{ F \circ (S\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^3 \{ T\{\overline{m}.\overline{n}.\mathbf{0}/X\} \} \} \} \\ \sim_l \mathbb{E}'_{\overline{m}.\overline{n}.\mathbf{0}} \{ F \circ (S'\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \} \end{aligned}$$

Nous avons $Q\{R/X\} \xrightarrow{\tau} \mathbb{E}'_R \{ F \circ (S'\{R/X\}) \}$ et

$$\mathbb{E}_R^1 \{ \mathbb{E}_R^2 \{ F \circ (S\{R/X\}) \} \mid \mathbb{E}_R^3 \{ T\{R/X\} \} \} \mathcal{R} \mathbb{E}'_R \{ F \circ (S'\{R/X\}) \}$$

Le résultat est donc vrai.

Si le message est émis par R , il existe F, S, T tels que $R \xrightarrow{\overline{a}} \langle S \rangle T$ et $P' \xrightarrow{a} F\{R/X\}$ pour un certain a . Nous avons la transition

$$P\{R/X\} \xrightarrow{\tau} \mathbb{E}_R^1 \{ \mathbb{E}_R^2 \{ T \} \mid \mathbb{E}_R^3 \{ (F\{R/X\}) \circ S \} \}$$

pour certains contextes $\mathbb{E}_R^1, \mathbb{E}_R^2, \mathbb{E}_R^3$. Nous avons

$$P\{\overline{m}.\overline{n}.\mathbf{0}/X\} \xrightarrow{\overline{m}} \xrightarrow{a} \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^2 \{ \overline{n}.\mathbf{0} \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^3 \{ F\{\overline{m}.\overline{n}.\mathbf{0}/X\} \} \}$$

donc il existe $F', \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^1, \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^2, \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^3$ tels que

$$Q\{\overline{m}.\overline{n}.\mathbf{0}/X\} \xrightarrow{\overline{m}} \xrightarrow{a} \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^2 \{ \overline{n}.\mathbf{0} \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^3 \{ F'\{\overline{m}.\overline{n}.\mathbf{0}/X\} \} \}$$

et

$$\begin{aligned} \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^2 \{ \overline{n}.\mathbf{0} \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^3 \{ (F\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \circ S \} \} \} \\ \sim_l \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^2 \{ \overline{n}.\mathbf{0} \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^3 \{ (F'\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \circ S \} \} \} \end{aligned}$$

Par le lemme B.5, nous avons

$$\begin{aligned} \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^2 \{ T \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}^3 \{ (F\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \circ S \} \} \} \\ \sim_l \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^1 \{ \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^2 \{ T \} \mid \mathbb{E}_{\overline{m}.\overline{n}.\mathbf{0}}'^3 \{ (F'\{\overline{m}.\overline{n}.\mathbf{0}/X\}) \circ S \} \} \} \end{aligned}$$

Nous avons $Q\{R/X\} \xrightarrow{\tau} \mathbb{E}'_R \{ \mathbb{E}_R'^2 \{ T \} \mid \mathbb{E}_R'^3 \{ (F'\{R/X\}) \circ S \} \}$ et

$$\mathbb{E}_R^1 \{ \mathbb{E}_R^2 \{ T \} \mid \mathbb{E}_R^3 \{ (F\{R/X\}) \circ S \} \} \mathcal{R} \mathbb{E}'_R \{ \mathbb{E}_R'^2 \{ T \} \mid \mathbb{E}_R'^3 \{ (F'\{R/X\}) \circ S \} \}$$

le résultat est donc vrai.

Si la transition de $P\{R/X\}$ provient de la communication entre deux copies de R , alors il existe a, F, S, T tels que $R \xrightarrow{a} F$ et $R \xrightarrow{\bar{a}} \langle S \rangle T$. La transition de $P\{R/X\}$ peut s'écrire $P\{R/X\} \xrightarrow{\tau} P'\{R/X\}\{F \circ T/Z\}\{T/Y\}$.

En particulier nous avons $P\{R/X\} \xrightarrow{a} P'\{R/X\}\{F/Z\}\{R/Y\}$. Comme Z est dans un contexte d'évaluation, nous avons

$$P\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Z\}\{\bar{m}.\bar{n}.\mathbf{0}/Y\}.$$

Il existe donc Q' tel que

$$Q\{\bar{m}.\bar{n}.\mathbf{0}/X\} \xrightarrow{\bar{m}} Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Z\}$$

et $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Z\}\{\bar{m}.\bar{n}.\mathbf{0}/Y\} \sim_l Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{\bar{n}.\mathbf{0}/Z\}$. Comme nous avons $F \circ S \sim_l F \circ S$, nous avons $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{\bar{m}.\bar{n}.\mathbf{0}/Y\} \sim_l Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}$ par le lemme B.5.

Comme Y est dans un contexte d'évaluation, nous avons

$$P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{\bar{m}.\bar{n}.\mathbf{0}/Y\} \xrightarrow{\bar{m}} P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{\bar{n}.\mathbf{0}/Y\}.$$

Il existe donc Q'' tel que

$$Q'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\} \xrightarrow{\bar{m}} Q''\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{\bar{n}.\mathbf{0}/Y\}$$

et $P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{\bar{n}.\mathbf{0}/Y\} \sim Q''\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{\bar{n}.\mathbf{0}/Y\}$. Comme nous avons $T \sim_l T$, nous avons

$$P'\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{T/Y\} \sim Q''\{\bar{m}.\bar{n}.\mathbf{0}/X\}\{F \circ S/Z\}\{T/Y\}$$

par le lemme B.5. Finalement nous avons $Q\{R/X\} \xrightarrow{\tau} Q''\{R/X\}\{F \circ S/Z\}\{T/Y\}$ avec $P'\{R/X\}\{F \circ S/Z\}\{T/Y\} \mathcal{R} Q''\{R/X\}\{F \circ S/Z\}\{T/Y\}$ comme voulu. □

Annexe C

Équivalences de fonctions en $\text{HO}\pi\text{P}$

Nous prouvons les résultats sur les processus finis donnés en Section 3.2.2.

Lemme C.1. *Soit F une fonction finie. Pour tout processus P , $F \circ P$ est fini.
Soit P_F un processus fini. Pour tout $P_F \xrightarrow{\alpha} A$, l'agent A est fini.*

Démonstration. Nous prouvons le premier résultat. Soit $F = (X)P_F$ une fonction finie. Nous avons $X \notin \text{fv}(P_F)$, ou X apparaît uniquement dans les messages de P . Nous avons donc $P_F\{P/X\} = P_F$, ou alors P apparaît uniquement dans les messages de $P_F\{P/X\}$. Dans les deux cas, le processus $F \circ P$ est fini.

Nous prouvons le second résultat par induction structurelle sur P_F . Il n'y a rien à prouver dans le cas **0**. Si $P_F = \bar{a}\langle P^1 \rangle P_F^2$, la seule transition possible est $P_F \xrightarrow{\bar{a}} \langle P^1 \rangle P_F^2$. Le processus P_F^2 est fini, donc $\langle P^1 \rangle P_F^2$ est finie par définition.

Si $P_F = a(X)P'_F$, alors la seule transition possible est $P_F \xrightarrow{a} (X)P'_F$. Comme P'_F est fini, $(X)P'_F$ est finie.

Si $P_F = P_F^1 \mid P_F^2$, alors les transitions de P_F peuvent provenir des règles PAR, HO ou de leur symétrique. Dans le cas de PAR, nous avons $P_F^1 \xrightarrow{\alpha} A_1$ et $P_F \xrightarrow{\alpha} A_1 \mid P_F^2$. Par induction, A_1 est fini, donc $A_1 \mid P_F^2$ est fini. Dans le cas de HO, nous avons $P_F^1 \xrightarrow{a} F$, $P_F^2 \xrightarrow{\bar{a}} C$ et $P_F \xrightarrow{\tau} F \bullet C$. Par induction F et C sont finies, et par le premier résultat, $F \bullet C$ est fini ; le résultat est donc vrai.

Si $P_F = a[P'_F]$, les transitions de P_F peuvent provenir de PASSIV ou LOC ; le cas de la passivation se traite comme l'émission de message, et la règle de congruence se traite comme la règle PAR. De même, si $P_F = \nu a.P'_F$, les transitions de P_F proviennent de la règle RESTR : ce cas se traite comme la règle PAR.

□

Lemme C.2. *Soit P_F un processus fini.*

- L'ensemble $\{\alpha, P_F \xrightarrow{\alpha}\}$ est fini.
- Pour tout α , l'ensemble $\{A, P_F \xrightarrow{\alpha} A\}$ est fini.

Démonstration. Facile par induction structurelle sur P_F .

□

Nous prouvons maintenant que les processus finis terminent. Pour cela, nous définissons la taille d'un agent fini.

Définition C.1. *La taille d'un processus fini P_F , notée $s(P_F)$, est définie inductivement par*

$$\begin{aligned} s(\mathbf{0}) &= 0 & s(P_F^1 \mid P_F^2) &= s(P_F^1) + s(P_F^2) & s(\nu a.P_F) &= s(P_F) \\ s(\bar{a}\langle P^1 \rangle P_F^2) &= 1 + s(P_F^2) & s(a(X)P_F) &= 1 + s(P_F) & s(a[P_F]) &= 1 + s(P_F) \end{aligned}$$

La taille d'une concrétion finie est définie comme étant la taille de sa continuation, et la taille d'une fonction finie est définie comme étant la taille du corps de la fonction.

Lemme C.3. Soit F une abstraction finie. Pour tout P , nous avons $s(F \circ P) = s(F)$.

Soit P_F un processus fini. Pour tout $P_F \xrightarrow{\alpha} A_F$, nous avons $s(A_F) < s(P_F)$.

Démonstration. Soit $F = (X)P_F$ une abstraction finie; par définition nous avons $s(F) = s(P_F)$. Par définition nous avons $X \notin \text{fv}(P_F)$ ou X n'apparaît que dans les messages de P_F . Comme le contenu des messages n'intervient pas dans le calcul de la taille, nous avons $s(P_F\{P/X\}) = s(P_F) = s(F)$.

Nous prouvons le second résultat par induction structurelle sur P_F . Il n'y a rien à prouver pour $P_F = \mathbf{0}$. Si $P_F = \bar{a}\langle P^1 \rangle P_F^2$, nous avons $P_F \xrightarrow{\bar{a}} \langle P^1 \rangle P_F^2$, $s(P_F) = 1 + s(P_F^2)$ et $s(\langle P^1 \rangle P_F^2) = s(P_F^2)$, le résultat est donc vrai.

Si $P_F = a(X)P'_F$, nous avons $P_F \xrightarrow{a} (X)P'_F$, $s(P_F) = 1 + s(P'_F)$ et $s((X)P'_F) = s(P'_F)$, le résultat est donc vrai.

Si $P_F = P_F^1 \mid P_F^2$, la transition de P_F provient des règles PAR, HO ou de leur symétrique. Dans le cas de PAR, nous avons $P_F^1 \xrightarrow{\alpha} A_F^1$ et $P_F \xrightarrow{\alpha} A_F^1 \mid P_F^2$. Par induction nous avons $s(A_F^1) < s(P_F^1)$, donc nous avons $s(A_F^1) + s(P_F^2) < s(P_F^1) + s(P_F^2)$, c'est-à-dire $s(A_F^1 \mid P_F^2) < s(P_F)$, comme voulu. Dans le cas de HO, nous avons $P_F^1 \xrightarrow{a} F$, $P_F^2 \xrightarrow{\bar{a}} C = \nu \tilde{b}. \langle R \rangle S_F$ et $P_F \xrightarrow{\tau} F \bullet C$. Par le premier résultat nous avons $s(F \circ R) = s(F)$, donc nous avons $s(\nu \tilde{b}.(F \circ R \mid S_F)) = s(F \circ R) + s(S_F) = s(F) + s(C)$. Par induction nous avons $s(F) < s(P_F^1)$ et $s(C) < s(P_F^2)$, donc nous avons $s(F) + s(C) < s(P_F^1) + s(P_F^2)$, c'est-à-dire $s(F \bullet C) < s(P_F)$, comme demandé.

Si $P_F = a[P'_F]$, nous avons deux cas à considérer. Si $P_F \xrightarrow{\bar{a}} \langle P'_F \rangle \mathbf{0}$, nous avons $s(P_F) = 1 + s(P'_F) > s(\mathbf{0}) = 0$, le résultat est donc vrai. Si $P'_F \xrightarrow{\alpha} A'_F$ et $P_F \xrightarrow{\alpha} a[A'_F]$, alors par induction nous avons $s(P'_F) > s(A'_F)$, donc nous avons $1 + s(P'_F) > 1 + s(A'_F)$, c'est-à-dire $s(P_F) > s(a[A'_F])$, le résultat est donc vrai. De même, si $P_F = \nu a.P'_F$, $P'_F \xrightarrow{\alpha} A'_F$ et $P_F \xrightarrow{\alpha} \nu a.A'_F$, alors par induction nous avons $s(P'_F) > s(A'_F)$, c'est-à-dire $s(P_F) > s(\nu a.A'_F)$, comme voulu. □

Lemme C.4. Soit P_F un processus fini. Il n'existe pas de suite infinie de processus $(P_i)_{i \in \mathbb{N}}$ telle que $P_0 = P_F$ et pour tout i :

- $P_i \xrightarrow{\tau} P_{i+1}$ ou ;
- $P_i \xrightarrow{a} F$ et il existe R tel que $F \circ R = P_{i+1}$ ou ;
- $P_i \xrightarrow{\bar{a}} \nu \tilde{b}. \langle R \rangle P_{i+1}$.

Démonstration. S'il existe une telle suite, alors la suite des tailles $(s(P_i))_{i \in \mathbb{N}}$ est une suite d'entiers naturels strictement décroissante par le lemme C.3, absurde. □

Nous rappelons la définition des fonctions $(F_n), (G_n)$ données en section 3.2.3.

$$F_0 \triangleq (X_0)X_0, G_0 \triangleq (X_0)(X_0 \mid X_0)$$

et pour tout $n > 0$

$$\begin{aligned} F_n &\triangleq (X_n)R_n^1 + R_n^2 \\ G_n &\triangleq (X_n)S_n^1 + S_n^2 \end{aligned}$$

avec

$$\begin{aligned} R_n^1 &\triangleq \nu a_n.(a_n[X_n] \mid a_n.F_{n-1}) \\ R_n^2 &\triangleq \nu a_n.\tau.(G_{n-1} \circ X_n) \\ S_n^1 &\triangleq \nu a_n.(a_n[X_n] \mid a_n.G_{n-1}) \\ S_n^2 &\triangleq \nu a_n.\tau.(F_{n-1} \circ X_n) \end{aligned}$$

Dans les preuves qui vont suivre, pour tous processus P, R et toute fonction F tels que $\text{fv}(P) = \{X\}$ et X apparaît exactement une fois dans P , nous définissons $P \circ R \triangleq P\{R/X\}$ et $P \circ F \triangleq P\{F/X\}$.

Lemme C.5. *Pour tout P_F tel que $d(P_F) = 0$, nous avons $F_0 \circ P_F \sim G_0 \circ P_F$.*

Démonstration. Comme $d(P_F) = 0$, P_F ne peut pas effectuer de transition, tout comme le processus $P_F \mid P_F$. Nous avons $\text{fn}(P_F) = \text{fn}(P_F \mid P_F)$, donc nous avons $F_0 \circ P_F \sim G_0 \circ P_F$. \square

Lemme C.6. *Soit $n > 0$. Pour tout P_F tel que $d(P_F) \leq n$, nous avons $F_n \circ P_F \sim G_n \circ P_F$.*

Démonstration. Nous prouvons que la relation

$$\mathcal{R}_n \triangleq \{(\mathbb{C}\{P\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l / \tilde{X}}\}\}, \mathbb{C}\{P\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l / \tilde{X}}\}\}), \\ d(P_F^k) \leq k \leq n \wedge d(P_F^l) \leq l - 1 \leq n\}$$

est une bisimulation contextuelle précoce forte.

Soient $P_1 \mathcal{R}_n P_2$. Nous procédons par analyse de cas sur la transition de P_1 .

Si la transition est initiée par P ou \mathbb{C} sans interaction avec les processus $F_k \circ P_F^k$, alors P_2 répond avec la même transition.

Supposons que la transition de P_1 provient d'un processus $F_{k_0} \circ P_F^{k_0}$, dans lequel la passivation de la localité a_{k_0} s'est déclenchée. Nous avons alors

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0} \cdot (F_{k_0-1} \circ P_F^{k_0}) / X_{k_0}\} \{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l / (\tilde{X} \setminus X_{k_0})}\}\} \triangleq P'_1.$$

Nous distinguons deux cas; supposons d'abord que nous avons $d(P_F^{k_0}) \leq k_0 - 1$. Le processus P_2 répond alors par la passivation de a_{k_0} dans $G_{k_0} \circ P_F^{k_0}$, c'est-à-dire

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0} \cdot (G_{k_0-1} \circ P_F^{k_0}) / X_{k_0}\} \{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l / (\tilde{X} \setminus X_{k_0})}\}\} \triangleq P'_2.$$

Soit $P' \triangleq P\{\nu a_{k_0} \cdot X_{k_0} / X_{k_0}\}$. Les processus P'_1 et P'_2 peuvent s'écrire

$$\begin{aligned} P'_1 &= \mathbb{C}\{P'\{\widetilde{F_k \circ P_F^k}, \widetilde{F_{k_0-1} \circ P_F^{k_0}}, \widetilde{R_l^1 \circ P_F^l / \tilde{X}}\}\} \\ P'_2 &= \mathbb{C}\{P'\{\widetilde{G_k \circ P_F^k}, \widetilde{G_{k_0-1} \circ P_F^{k_0}}, \widetilde{S_l^1 \circ P_F^l / \tilde{X}}\}\} \end{aligned}$$

et comme nous avons $d(P_F^{k_0}) \leq k_0 - 1 \leq n$, nous avons $P'_1 \mathcal{R}_n P'_2$, comme souhaité.

Dans le cas $d(P_F^{k_0}) = k_0$, le processus P_2 répond par l'action interne de S_{k_0} , sous-processus de $G_{k_0} \circ P_F^{k_0}$. Nous avons alors

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0} \cdot (F_{k_0-1} \circ P_F^{k_0}) / X_{k_0}\} \{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l / (\tilde{X} \setminus X_{k_0})}\}\} \triangleq P'_2$$

Soit $P' \triangleq P\{\nu a_{k_0} \cdot (F_{k_0-1} \circ P_F^{k_0}) / X_{k_0}\}$; P'_1 et P'_2 peuvent s'écrire

$$\begin{aligned} P'_1 &= \mathbb{C}\{P'\{\widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l / (\tilde{X} \setminus X_{k_0})}\}\} \\ P'_2 &= \mathbb{C}\{P'\{\widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l / (\tilde{X} \setminus X_{k_0})}\}\} \end{aligned}$$

Nous avons donc $P'_1 \mathcal{R}_n P'_2$ comme souhaité.

Supposons que la transition de P_1 provient d'un processus $R_{l_0}^1 \circ P_F^{l_0}$, dans lequel la passivation de la localité a_{l_0} s'est déclenchée. Nous avons $d(P_F^{l_0}) \leq l_0 - 1$ par définition,

ce cas se traite donc comme le premier sous-cas du cas précédent.

Supposons que la transition de P_1 provient d'un processus $F_{k_0} \circ P_F^{k_0}$, dans lequel la τ -action du processus R_{k_0} se déclenche. Nous avons alors

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0} \cdot (G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq P'_1.$$

Le processus P_2 répond par la passivation de a_{k_0} dans le processus $G_{k_0} \circ P_F^{k_0}$, c'est-à-dire

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{\nu a_{k_0} \cdot (G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq P'_2$$

Soit $P' \triangleq P\{\nu a_{k_0} \cdot (G_{k_0-1} \circ P_F^{k_0})/X_{k_0}\}$; P'_1 et P'_2 peuvent s'écrire

$$\begin{aligned} P'_1 &= \mathbb{C}\{P'\{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \\ P'_2 &= \mathbb{C}\{P'\{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \end{aligned}$$

donc nous avons $P'_1 \mathcal{R}_n P'_2$.

Supposons que la transition de P_1 provient d'un processus $F_{k_0} \circ P_F^{k_0}$, dans lequel $P_F^{k_0}$ effectue une action interne $P_F^{k_0} \xrightarrow{\tau} P_F^{k_0}$. Nous avons alors

$$P_1 \xrightarrow{\tau} \mathbb{C}\{P\{R_{k_0}^1 \circ P_F^{k_0}/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq P'_1.$$

Le processus P_2 répond par une transition similaire

$$P_2 \xrightarrow{\tau} \mathbb{C}\{P\{S_{k_0}^1 \circ P_F^{k_0}/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq P'_2.$$

Par définition de la profondeur, nous avons $d(P_F^{k_0}) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$, donc nous avons $P'_1 \mathcal{R}_n P'_2$.

Supposons que la transition de P_1 provient d'un processus $F_{k_0} \circ P_F^{k_0}$, dans lequel $P_F^{k_0}$ effectue une réception $P_F^{k_0} \xrightarrow{a} F$. Nous avons alors

$$P_1 \xrightarrow{a} \mathbb{C}\{P\{R_{k_0}^1 \circ F/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq F_1.$$

Soit $C = \nu \tilde{b} \cdot \langle T \rangle U$. Le processus P_2 répond par une transition similaire

$$P_2 \xrightarrow{a} \mathbb{C}\{P\{S_{k_0}^1 \circ F/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq F_2.$$

Nous avons

$$\begin{aligned} F_1 \bullet C &= \nu \tilde{b} \cdot (\mathbb{C}\{P\{R_{k_0}^1 \circ (F \circ T)/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \mid U) \\ F_2 \bullet C &= \nu \tilde{b} \cdot (\mathbb{C}\{P\{S_{k_0}^1 \circ (F \circ T)/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \mid U) \end{aligned}$$

Soit $\mathbb{C}' \triangleq \nu \tilde{b} \cdot (\mathbb{C} \mid U)$; $F_1 \bullet C$ et $F_2 \bullet C$ peuvent s'écrire

$$\begin{aligned} F_1 \bullet C &= \mathbb{C}'\{P\{R_{k_0}^1 \circ (F \circ T)/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \\ F_2 \bullet C &= \mathbb{C}'\{P\{S_{k_0}^1 \circ (F \circ T)/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \end{aligned}$$

Par définition de la profondeur nous avons $d(F \circ T) = d(F) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$, donc nous avons $F_1 \bullet C \mathcal{R}_n F_2 \bullet C$.

Supposons que la transition de P_1 provient d'un processus $F_{k_0} \circ P_F^{k_0}$, dans lequel $P_F^{k_0}$ effectue une émission $P_F^{k_0} \xrightarrow{\bar{a}} C = \nu \tilde{b}. \langle T \rangle U$. Nous avons alors

$$P_1 \xrightarrow{\bar{a}} \nu \tilde{b}, \tilde{b}'. \langle T \rangle \mathbb{C}' \{P\{R_{k_0}^1 \circ U/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq C_1$$

où \tilde{b}' est l'ensemble des noms capturés par \mathbb{C} et \mathbb{C}' est le contexte obtenu à partir de \mathbb{C} en supprimant les restrictions sur \tilde{b}' . Soit F une abstraction et \mathbb{E} un contexte d'évaluation. Le processus P_2 répond par une transition similaire

$$P_2 \xrightarrow{\bar{a}} \nu \tilde{b}, \tilde{b}'. \langle T \rangle \mathbb{C}' \{P\{S_{k_0}^1 \circ U/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \triangleq C_2.$$

Nous avons

$$F \bullet \mathbb{E}\{C_1\} = \nu \tilde{b}, \tilde{b}', \tilde{b}'' . (F \circ T \mid \mathbb{E}' \{ \mathbb{C}' \{ P\{R_{k_0}^1 \circ U/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \})$$

$$F \bullet \mathbb{E}\{C_2\} = \nu \tilde{b}, \tilde{b}', \tilde{b}'' . (F \circ T \mid \mathbb{E}' \{ \mathbb{C}' \{ P\{S_{k_0}^1 \circ U/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \})$$

où \tilde{b}'' et \mathbb{E}' sont définis de la même manière que \tilde{b}' et \mathbb{C}' .

Soit $\mathbb{C}'' \triangleq \nu \tilde{b}, \tilde{b}', \tilde{b}'' . (F \circ T \mid \mathbb{E}' \{ \mathbb{C}' \})$; $F \bullet \mathbb{E}\{C_1\}$ et $F \bullet \mathbb{E}\{C_2\}$ peuvent s'écrire

$$\begin{aligned} F \bullet \mathbb{E}\{C_1\} &= \mathbb{C}'' \{ P\{R_{k_0}^1 \circ U/X_{k_0}\} \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \\ F \bullet \mathbb{E}\{C_2\} &= \mathbb{C}'' \{ P\{S_{k_0}^1 \circ U/X_{k_0}\} \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l} / (\tilde{X} \setminus X_{k_0}) \} \} \end{aligned}$$

Par définition de la profondeur nous avons $d(U) = d(C) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$, donc nous avons $F \bullet \mathbb{E}\{C_1\} \mathcal{R}_n F \bullet \mathbb{E}\{C_2\}$.

Supposons que la transition de P_1 provient d'une communication entre deux processus finis, entre un processus fini et le processus P , ou entre un processus fini et le contexte \mathbb{C} . Nous traitons seulement le cas de la communication entre deux processus $P_F^{k_0}$ et $P_F^{k_1}$, les autres étant similaires. Supposons le cas $P_F^{k_0} \xrightarrow{a} F$ et $P_F^{k_1} \xrightarrow{\bar{a}} C = \nu \tilde{b}. \langle T \rangle U$. Nous avons alors

$$P_1 \xrightarrow{\tau} \mathbb{C} \{ P' \{ \widetilde{F_k \circ P_F^k}, \widetilde{R_l^1 \circ P_F^l}, R_{k_0}^1 \circ (F \circ T), R_{k_1}^1 \circ U/\tilde{X}, X_{k_0}, X_{k_1} \} \} \triangleq P'_1$$

où P' est obtenu à partir de P en plaçant \tilde{b} de manière à englober X_{k_0} et X_{k_1} . Le processus P_2 répond par une transition similaire :

$$P_2 \xrightarrow{\tau} \mathbb{C} \{ P' \{ \widetilde{G_k \circ P_F^k}, \widetilde{S_l^1 \circ P_F^l}, S_{k_0}^1 \circ (F \circ T), S_{k_1}^1 \circ U/\tilde{X}, X_{k_0}, X_{k_1} \} \} \triangleq P'_2$$

Nous avons $d(F \circ T) = d(F) \leq d(P_F^{k_0}) - 1 \leq k_0 - 1 \leq n$ et $d(S) = d(C) \leq d(P_F^{k_1}) - 1 \leq k_1 - 1 \leq n$, donc nous avons $P'_1 \mathcal{R}_n P'_2$, comme souhaité.

De la même manière, nous pouvons montrer que \mathcal{R}_n^1 est une simulation contextuelle forte précoce. □

Soit (m_k) une suite de noms frais deux-à-deux distincts. Soit $Q_1 \triangleq m_1. \mathbf{0}$ et $Q_{k+1} \triangleq m_{k+1}. Q_k$ pour tout $k > 1$.

Lemme C.7. *Pour tout n , nous avons $F_n \circ Q_{n+1} \approx G_n \circ Q_{n+1}$.*

Démonstration. Nous procédons par induction sur n . Pour $n = 0$, nous avons $F_0 \circ m_1.\mathbf{0} = m_1.\mathbf{0} \approx m_1.\mathbf{0} \mid m_1.\mathbf{0} = G_0 \circ m_1.\mathbf{0}$, comme souhaité.

Soit $n > 0$. Nous avons

$$F_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.F_{n-1}) \triangleq P_1,$$

auquel $G_n \circ Q_{n+1}$ peut répondre uniquement par

$$G_n \circ Q_{n+1} \xrightarrow{m_{n+1}} \nu a_n.(a_n[Q_n] \mid a_n.G_{n-1}) \triangleq P_2.$$

Après passivation de a_n , nous obtenons

$$P_1 \xrightarrow{\tau} \nu a_n.(F_{n-1} \circ Q_n),$$

auquel P_2 répond par

$$P_2 \xrightarrow{\tau} \nu a_n.(G_{n-1} \circ Q_n).$$

Comme nous avons $a_n \notin \text{fn}(F_{n-1} \circ Q_n)$ (respectivement $a_n \notin \text{fn}(G_{n-1} \circ Q_n)$), nous avons $\nu a_n.(F_{n-1} \circ Q_n) \sim F_{n-1} \circ Q_n$ (respectivement $\nu a_n.(G_{n-1} \circ Q_n) \sim G_{n-1} \circ Q_n$). Par induction, nous avons $F_{n-1} \circ Q_n \approx G_{n-1} \circ Q_n$, donc nous avons $F_n \circ Q_{n+1} \approx G_n \circ Q_{n+1}$. \square