Mathematical Structures in Computer Science (2025), **35**, e2, pp. 1–55
doi:10.1017/S0960129525000015

CAMBRIDGE UNIVERSITY PRESS

PAPER

On higher-order communication in ambient calculi

Xian Xu, Yan Huang and Zhihuan Yao

East China University of Science and Technology, Shanghai, China
Corresponding author: Xian Xu; Email: xuxian@ecust.edu.cn

(Received 30 January 2022; revised 24 December 2024; accepted 7 January 2025)

Abstract

We revisit the communication primitive in ambient calculi. Previously, such communication was confined to first-order (FO) mode (e.g., merely names or capabilities of ambients can be sent), local mode (e.g., the communication only occurs inside an ambient), or particular cross-hierarchy mode (e.g., parent-child communication). In this work, we explore further higher-order (HO) communication in ambient calculi. Specifically, such a communication mechanism allows sending a whole piece of a program across the borders of ambients and is the only form of communication that can happen exactly between ambients. Since ambients are basically of HO nature (i.e., those being moved may be ambients themselves), in a sense, it appears more natural to have HO communication than FO communication. We stipulate that communications merely occur between equally positioned ambients in a peer-to-peer fashion (e.g., between sibling ambients). Following this line, we drop the local or other forms of communication that violate this criterion. As the workbench, we work on a variant of Fair Ambients extended with HO communication, FAHO. This variant also strengthens the original version in that entirely real-identity interaction is guaranteed. We study the semantics, bisimulation, and expressiveness of FAHO. Particularly, we provide the operational semantics using a labeled transition system. Over the semantics, we define the bisimulation in line with the standard notion of bisimulation for ambients and prove that the bisimulation equivalence (i.e., bisimilarity) is a congruence. In addition, we demonstrate that bisimilarity coincides with observational congruence (i.e., barbed congruence). Moreover, we show that FAHO can encode a minimal Turing-complete HO calculus and thus is computationally complete.

Keywords: Ambient calculus; communication; higher-order; processes; encoding

1. Introduction

Ambient calculi are a family of process models that formalize computation at positions in a concurrent distributed environment (Cardelli and Gordon, 2000). Roughly, an ambient is a process residing in an explicitly stated computational context (or location). For computing, ambients must evolve by interacting with one another. There are two basic kinds of interactions between ambients. One is by the movement of ambients (being tied to the capabilities of ambients as the elementary interacting particles), and the other is by communication (subject to some requirement over the forms of interacting parts). With respect to movement, there have been quite some works in the literature, and we will briefly review those relevant to this work. With respect to communication, most of the mechanism is based on message-passing (e.g., name-passing or capability-passing), and the communication can happen between ambients as well as non-ambients (e.g., some piece of code, i.e., segregated from the boundaries of any ambient). Ambient calculi provide a useful formal model for the study of location-based concurrent programming

© The Author(s), 2025. Published by Cambridge University Press

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

languages, mobile autonomous computing, popular distributed computing such as cloud and edge computing, and cyber-physical and intelligent systems. In particular, it can be employed in the modeling and verification of mobile systems that take advantage of explicit computation contexts and various service-oriented computing. Indeed, ambient calculi have attracted great attention since they were proposed, and in subsequent years, they continued to find relevant development in both theory and pragmatics (Charatonik et al., 2003; Cruz and Aguirre, 2005; Tomásek 2007; Coronato and Pietro, 2010; Siewe et al., 2011; Cerone et al., 2012; Sun 2015; Mylonakis, 2017) (see also the related work below).

In this work, we are interested in incorporating higher-order (HO, in brief) communication in ambient interaction. We will review relevant concepts and available works on communication for ambients, so to motivate us. In the following subsection, we first present an overview of ambient calculi and outline our work. Then we survey the literature and demonstrate our contributions upfront.

1.1 Related concepts and informal account

An ambient, $a[P]$, models some computing resource, P, running in an explicitly named place a with boundary, denoted by []. The primary computing behavior of ambients is through mobility, that is, moving between different locations. Mobility is how ambients interact with each other and "compute" to achieve, say, computational completeness from the viewpoint of computation. To this end, ambients are actually of HO nature; in the interaction between ambients, the objects that move (or transmit) can be precisely the ambients themselves, analogous to the process-passing in HO process calculi. So ambient calculi can be regarded as a kind of HO model. Ambients can be used to model distributed systems and simulate their behavior. In retrospect, since its introduction, a good number of works have been done to examine semantics, equivalence theory, and expressiveness. With respect to both computation and interaction in applications, ambients provide a valuable tool for understanding concurrent distributed systems.

The core conceptual behavior of an ambient has two basic types: in (entering) and out (exiting). The "in" movement depicts the scenario that an ambient enters another, whereas the "out" movement depicts that an ambient exits another. Capable of in and out movements, an ambient can (theoretically) walk anywhere it is allowed and run its code thereby. There is also an operation that appears more potent than the moving primitives, that is, the open operation, which enables one to dissolve the boundary of an ambient. The formal semantics of these operations underwent some period of evolution, depending on the control design perspective, which we will review in related works.

In addition to the moving capability, ambients can also explicitly send messages. As usual, the messages are transmitted over channel names (sometimes anonymous), that is, ambient names in the setting of ambient calculi. There are two types of messages. The first type is communicating (ambient) names, that is, ambients communicate the names through their names as channels. This type reminds one of the first-order (FO) name-passing pi-calculus (Milner et al., 1992), so we name it FO communication. Nevertheless, in ambients, such name-passing interplays with boundaries and thus becomes more involved. The other type is communicating ambients themselves, that is, ambients communicate themselves through their names as channels. This type certainly makes one recall the HO process-passing pi-calculus (Sangiorgi, 1993). Again, besides the difficulty like that for FO communication (i.e., boundaries), HO communication is intrinsically harder to tackle (e.g., semantics, equivalence, and congruence in behavioral theory). This intricacy increases the complexity in building process-passing in ambient calculi and is an important reason why ambients with HO communication were not studied immediately and less examined than the FO communication. In this work, we study ambients with HO communication. In particular, this paper presents an ambient model with a strictly HO communication mechanism (by "strictly," we mean that there is no FO communication). The model is developed based on Fair Ambients (FA)

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

(Fu, 2007), a relatively new formalism of ambient calculi. We make this choice because its moving capabilities are easy to cope with, and there has been successful work on its (FO) communication and expressiveness. We believe this work can be referential to other variants of ambients concerning (HO) communication. We explain our work from the informal (conceptual) viewpoint below.

- As the elementary constituent of a concurrent system, an ambient is the basic individual unit (i.e., object) and the only qualified subject that can engage a HO communication, hence the keyword "fair." This principle was first proposed by Fu in FA (with FO communication) (Fu, 2007). Following this line, an ambient's input and output (comprising a HO communication) must designate clearly which ambient the message is going from or to. Moreover, to be fair, the other participant of the same communication must declare clearly which ambient it is willing to interact with. In other words, HO communications are supposed to happen between equally positioned ambients in a peer-to-peer way.
- Unlike many ambient models in the field, including FA, the out-moving procedure must be completely real name (or real identity), that is, no anonymous ambients are allowed to step outside. In general, what we mean by "real name" is that the name of an ambient should be well-known by the process interacting with it and cannot be hidden. Concerning the out-movement, our viewpoint is that an ambient should be able to know and have control over which one (viz., resource) is moving out of its domain. This requirement also makes out-moving in line with the in-moving capability, which is real name from the very beginning of the design of mobility. So our ambient calculus is a strictly real-name model.
- Due to the HO characteristics, the behavioral theory for ambients is always a nontrivial job in itself. Enabling HO communication adds to this complexity, particularly concerning the equivalence and congruence properties since these properties are always hard for HO processes in their own right. So the bisimulation for the ambient calculus of this paper needs to be very carefully designed. One has to consider the target place into which an ambient might go. In the case of HO communication, an ambient can go anywhere in the target ambient, not necessarily the top level of that ambient. This fact leads to a concept similar to the context bisimulation in HO pi-calculus, only different in that the context is now surrounded by an ambient. We will define this formally in Section 3. Only based on this design can we prove that the bisimulation equivalence (also called the bisimulation equality (Sangiorgi, 2011), i.e., bisimilarity) we defined is indeed both an equivalence and a congruence. The proof, which is rather involved, takes advantage of the proof method of equivalence and congruence for HO pi-calculus (Sangiorgi, 1993; Sangiorgi and Walker, 2001) and tailors it to the situation of ambients. We also define the barbed congruence (Sangiorgi and Walker, 2001; Fu, 2007) and show that it is characterized by bisimilarity. The observables (i.e., barbs) now involve ambient boundaries. Due to the prudent design of the bisimulation, the proof of the coincidence between bisimilarity and barbed congruence becomes more tractable. In particular, the cases of HO input and output essentially exploit the design and consequent properties of the context bisimulation.
- To test the computational capability of the ambient calculus of this work, we construct an encoding from the minimal HO pi-calculus (notation Π), that is, the HO processes with only input, output, and composition. Since Π is Turing complete (Lanese et al., 2011), this encoding entails that our ambient calculus is also computationally complete. The encoding borrows an idea from that for encoding FO pi-calculus into FA. The major difference is that the model here is purely HO; meanwhile, the out-moving capability (and thus the entire calculus) is completely real name. So the encoding has to cater to this very feature. We show that the encoding is fully abstract with respect to the (standard) bisimulation equivalence on either side.

In the following, we look through the relevant work in the literature on ambient calculi and explain the motivation of this work.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

1.2 Related work

This section reviews the work on ambient calculi in the field.

1.2.1 Mobile Ambients

Ambient calculi were proposed by Cardelli and Gordon in Mobile Ambients (MA) (Cardelli and Gordon, 2000). The very first purpose of this kind of calculi is to capture the feature of concurrent computation with explicit location boundary. For example, $a[P]$ stands for an ambient named a with process P running inside. Indeed, MA describe mobile computation within a hierarchical framework (i.e., tree structure), which structures the processes with respect to locations and allows them to move under control. Such control is implemented by three capabilities in MA: *entry* (in-movement), *exit* (out-movement), and *open* (absorption). In addition, ambients can communicate, and the communication happens inside ambients (i.e., locally) in an anonymous manner. The capabilities and the local anonymous communication can be exemplified by the following reductions:

$$a[in\ b.P \mid Q] \mid b[R] \rightarrow b[a[P \mid Q] \mid R] \qquad \text{in-movement}$$

$$b[a[out\ b.P \mid Q] \mid R] \rightarrow a[P \mid Q] \mid b[R] \qquad \text{out-movement}$$

$$open\ a.P \mid a[Q] \rightarrow P \mid Q \qquad \text{open}$$

$$a[(X)P \mid Q \mid \langle M \rangle \mid R] \rightarrow a[P\{M/X\} \mid Q \mid R] \qquad \text{communication}$$

In the first reduction, ambient a moves into ambient b with the help of the capability *in* b. The relative position of the two ambients changes from sibling to parent-child (i.e., a becomes part of b). In the second reduction, ambient a moves out of b with the help of the capability *out* b. The relative position of the two ambients changes from parent-child to sibling (i.e., a is now on the same level as b). The third reduction permits dissolving the boundary of ambient a, whose content becomes part of the surrounding environment (here involving P). The last reduction represents a communication inside ambient a, where $\langle M \rangle$ delivers the resource M, and $(X)P$ reads M and continues as P in which every occurrence of the variable X is instantiated as M.

The design of the movement in MA is quite simple and easy to understand. The control is monolateral; that is, only one side of the interacting ambients has full control. Though quite prototypical, the formulation of the ambient calculus is of great referential significance to upfront works, including the syntax, reduction-based semantics, and (barbed) bisimulation thereof.

1.2.2 Safe Ambients

Safe Ambients (SA) (Levi and Sangiorgi, 2003; Merro and Hennessy, 2006) are a variant of the original MA that strengthens the control of ambient movements to resolve the interference issue as one primary purpose. Every action of the entering, exiting, and opening of an ambient is no longer arbitrary and takes place on the agreement of both participants of the action. To be more specific, an action of an ambient now needs a coaction to enable interaction, that is, $\overline{in}$, $\overline{out}$, $\overline{open}$, respectively, for paring with *in*, *out*, *open*. For example, the following movements exhibit the situation of the three capabilities that have the same intuitive meaning as those in MA:

$$a[in\ b.P_1 \mid P_2] \mid b[\overline{in}\ b.Q_1 \mid Q_2] \rightarrow b[a[P_1 \mid P_2] \mid Q_1 \mid Q_2] \qquad \text{in-movement}$$

$$b[a[out\ b.P_1 \mid P_2] \mid \overline{out}\ b.Q_1 \mid Q_2] \rightarrow a[P_1 \mid P_2] \mid b[Q_1 \mid Q_2] \qquad \text{out-movement}$$

$$open\ a.P \mid a[\overline{open}\ a.Q_1 \mid Q_2] \rightarrow P \mid Q_1 \mid Q_2 \qquad \text{open}$$

SA are somewhat more robust in control without reducing the expressiveness of MA, and most of the properties of MA can be adapted to SA. However, the change in moving primitives leads

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

to more difficulty in proving properties like congruence and coincidence between labeled transition system (LTS)-based bisimulation and reduction-based barbed congruence. To make SA more tractable in these properties, SA with passwords were proposed (Merro and Hennessy, 2006), where a password is some information attached to the capabilities to enhance the control power further so that the desirable properties can be achieved. In these variants of MA, however, no HO communications are considered.

1.2.3 Boxed Ambients

Boxed Ambients (BA) (Bugliesi et al., 2001) are a variant of MA that removes the open capability (which is deemed overly powerful) and introduces more versatile communication methods. Such communications are still anonymous; that is, no explicit channels are declared. More specifically, the mobility in BA is inherited from MA (e.g., entering and exiting) with the same semantics, so it preserves the computational properties of MA. BA rely on different communication models, resulting from dropping the open capability. The communications in BA can be local as in MA (or its similar variants) or across ambient boundaries anonymously. In Bonelli et al. (2007), BA are extended with a type system aiming at providing explicitly flexible communication policy, that is, directed input/output operations. In that way, BA enhance the flexibility of typed communications over MA and provide important observations for the relationship between synchronous and asynchronous input/output. Although in Bonelli et al. (2007), the communication channels are not hidden as in the original BA, the aim of that work is different from this work, mainly in that we are more interested in the basic communication mechanism between ambients without typing assertion.

1.2.4 Fair Ambients

FA (Fu, 2007) are built on several principles that rebase the semantics of ambients on top of a corresponding LTS, which further reshapes the previous ambient calculi concerning fairness to be glossed over shortly. A central design idea is that the elementary participants of interaction should be ambients themselves rather than part of them (e.g., a moving prefix or a process not residing in any ambient). Meanwhile, the interaction between ambients must be peer to peer, in other words, equally positioned or even displaced. For example, in the out-moving, the ambient that is called out should be explicitly informed who is doing this. This is what "fair" means. Our model in this work, as somewhat an extension of FA, also adheres to this principle of fairness. More specifically, the semantical rules for the capabilities are exemplified as follows. Following the original formulation in (Fu, 2007), we use τ for an interaction:

$$b[in\ a.Q \mid N] \mid a[\overline{in}\ b.P \mid L] \xrightarrow{\tau} a[b[Q \mid N] \mid P \mid L] \qquad \text{in-movement}$$

$$a[c[out\ b.Q \mid O] \mid L] \mid b[\overline{out}\ a.P \mid N] \xrightarrow{\tau} a[L] \mid c[Q \mid O] \mid b[P \mid N] \qquad \text{out-movement}$$

$$b[open\ a.Q \mid N] \mid a[\overline{open}\ b.P \mid L] \xrightarrow{\tau} b[P \mid L \mid Q \mid N] \qquad \text{open}$$

In the in-movement, ambient b is capable of entering ambient a, provided that the latter is willing to give permission to the former. In the out-movement, ambient c specifies from whose call (here, ambient b) it may move out of ambient a, provided that ambient b indeed has this request. We notice here that ambient b does not explicitly indicate who inside a it is requesting to exit, and thus, the out-movement is anonymous (i.e., not real identity). We will, as part of this work, revisit this mechanism. In the open operation, both ambient a and b know each other and authorize the other's actions in an explicit way. Unlike previous counterparts, in FA, the open capability enables ambient b to exhaust the entire internal resources of a for its own interest (we often say the capability of an ambient to mean its control over the mobility of the involved ambients). The open capability is a very strong/mighty operation, which somewhat behaves like a virus, robbing the

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

codes of another application. Due to this downside, here in this work, we drop the open capability, like in BA. Based on the operational semantics, the standard bisimilarity is studied and proven to coincide with observational bisimilarity (or barbed bisimilarity).

FA also enable FO communication, in line with the fair principle imposed on ambients, so that the two sides of a communication are equally essential and clearly controlled concerning how and with whom an ambient is exchanging messages. As shown below, ambient a sends a message c, being a name itself, to ambient b, formalized by the action prefix $\overline{b}c$; correspondingly, ambient b receives and prepares its use with that message c from ambient a, formalized by the action prefix $a(x)$:

$$a[\overline{b}c.P \mid M] \mid b[a(x).Q \mid N] \xrightarrow{\tau} a[P \mid M] \mid b[Q\{c/x\} \mid N]$$

As an important result on computability, Fu shows that the FO pi-calculus is a sub-calculus of FA (Fu, 2007). The communication in FA and related works on expressiveness guide the design of HO communication in this work.

In the abovementioned works, however, no explicit HO communications are considered. A likely reason is that FO communication (if any) seems more tractable, and HO communication appears unnecessary due to the moving capacity of ambients. This is more than debatable. First, HO communication is not known to be derivable in the ambient settings. Second, programming with HO primitives can usually offer more flexibility and convenience in practice, as they appear more "direct" in interaction/computation, in contrast to address-passing. Besides, for process models without explicit (physical) locations, it is well-known that hHO processes can be implemented with FO processes, but not the other way around (Sangiorgi, 1993; Xu, 2012). To the best of our knowledge, the relationship between HO and FO communications is barely known in the setting of ambients. To address this, a well-established theory of HO communication for ambients has to be developed in the first place.

1.2.5 SA with (restricted) local higher-order communication

In Cao (2011, 2012, 2013), Cao studies the SA extended with local HO communication, that is, within an ambient only. Such (local) communication is not allowed between ambients, for example, parent-child or between-sibling ones, and moreover, the communication is anonymous; that is, no explicit channel names are designated. In such a setting, labeled bisimulation and barbed bisimulation are proven to be coincident, and the capability of encoding plain HO processes is established. The encoding can somewhat be thought of as transplanting HO concurrency into ambients, and similar results are presented for FO processes, that is, from FO processes to ambients capable of (anonymous) FO communication. Although not very surprising, the results provide some useful techniques for related works. It would be interesting to study more flexible HO communication, for example, those across ambients, like in BA (Bugliesi et al., 2001; Bonelli et al., 2007) or FA (Fu, 2007). In turn, the possibility of encoding FO communication would be worth exploring so that, among others, the encodability of FO processes in ambients without the same communication mechanism can be demonstrated.

1.2.6 More relevant works concerning higher-order extension of ambient calculi

In Coppo and Dezani-Ciancaglini (2002), Coppo and Dezani-Ciancaglini define a model for a variant of MA with synchronous HO value-passing and a new "selfopen" primitive. The main aim of that paper is to develop a denotational model (called the filter model) for the proposed model. This model is proven to be fully abstract with respect to the contextual equivalence with the observables being ambients (names) at the top level. The filter model is associated with a sophisticated type system to achieve full abstraction. In the variant ambient calculus of Coppo and Dezani-Ciancaglini (2002), processes can be passed as values only in a local manner, that is,

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

inside an ambient. In particular, these design decisions make it possible to establish a fully abstract filter model. In the same line, the selfopen is used to ensure full abstraction. In contrast, due to different motivations and out of distinct design principles, our ambient model does not have local HO communication or open operation. What we are more interested in here is to come by an ambient model that facilitates peer-to-peer HO communication between ambients themselves with mutual awareness of the parts involved in the interaction.

Schmitt and Stefani present the M-calculus (Schmitt and Stefani, 2003), a distributed process calculus that extends the (distributed) Join calculus (Fournet and Gonthier, 1996; Fournet et al., 1996; Fournet 1998) with call-by-value HO functions, programmable localities, and dynamic binding. To strengthen the control over migration, M-calculus implements the unification of communication and process migration, by means of fine-grained ambient-like routing control whose correctness is guaranteed by a type system. A passivation operator is also defined for programming different kinds of control in terms of localities. The main purpose of Schmitt and Stefani (2003) is to improve on the weak points of the Join calculus, for example, inadequate control over communication and mobility, lack of dynamic binding, and limited local semantics. Unlike our work, the HO communication facilitated by M-calculus is local, and the control mechanism does not consider fairness of the participants as our model does. In addition, M-calculus has an associated type system for M-processes to function correctly, which might add to the complexity of potential applications.

The Kell calculus (Kell for short) is proposed as a family of HO process calculi with ambient-like hierarchical localities (Schmitt and Stefani, 2004). The main design principles of Kell include programmable distributed membranes, dynamic binding, and local actions based on which HO communication is defined. The syntax and semantics of Kell are defined, several instances of Kell calculus are discussed, and some examples are given to illustrate the expressive power of these calculi. A notion of contextual equivalence, as well as a co-inductive characterization of the contextual equivalence (called strong context bisimulation), is studied for Kell. Kell supports various HO communications, including those within a (local) location, those crossing tree-structured hierarchies (i.e., parent-child), and even a kind called passivation that destroys the boundary of a location. Differently, the HO communication mechanism in this work permits neither local nor parent-child ones. Moreover, the control mechanism of movement and communication follows the principle of fairness, on which we rest our design of the semantics and behavioral theory.

For the sake of clarity, in what follows, we highlight the main difference of this work concerning the works above, especially about design decisions:

(1) The HO communication mechanism is quite different. Particularly in the works above, HO communication does not happen between parallel ambients on an equal hierarchical level. That is, either parent-child or local HO communication is permitted in the models proposed by these works. By contrast, we choose to disallow both local and inter-hierarchy parent-child communication. This choice not only makes the model small but more importantly complies with the design idea that communication merely happens between equally leveled ambients via a peer-to-peer manner (e.g., concurrent sibling ambients). The obtained model turns out not to lose any computational power.

(2) The open operation (or its variant) may be admitted in some of the works above; for example, the calculus of Coppo and Dezani-Ciancaglini (2002) defines a "selfopen" operation. As explained previously, we cancel the open-like operation because it stands in the way of accommodating ambients as the first-class participants of interactions, including HO communication. What is more, open is a programming primitive that appears overly powerful concerning the inter-operation of processes (Bugliesi et al., 2001).

(3) From the overall viewpoint, the models in the above works are quite different. For example, Kell has sequential/passivation semantics; that is, a process can follow an ambient, and the whole content of that ambient can be sent to another process (not necessarily an ambient). M-calculus also has a kind of passivation that follows the line of the Join calculus. None of these constructs

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

is formalized in our model since we only allow interactions between equally positioned ambients (like Fu (2007)). Moreover, in all these works, type systems are needed to formulate the calculus for various purposes. For example, in the M-calculus, a type system is employed to facilitate the unification of communication and process migration; in the variant ambient model of Coppo and Dezani-Ciancaglini (2002), a type system is required to achieve full abstraction. By contrast, type systems are not necessary for our work, and this might make some difference in potential applications of the results of this work.

(4) None of these works has investigated, through explicit encoding, the computational completeness of the corresponding calculus. As a primary goal of this work, we accomplish the Turing completeness of our calculus, to our knowledge, for the first time for an ambient calculus with HO communication. The accompanying results and techniques may be of independent importance for further work.

1.3 Motivation

We now explain the motivation for this work.

1.3.1 Ambients with higher-order communication

As commented above, the start idea of this work is to enable HO (i.e., higher-order) communication for ambients. Interactions in ambient calculi are of HO nature; that is, ambients can move around between ambients. As such, it makes sense to allow ambients to be passed around, as an alternative (and probably more natural) method of interaction. Moreover, arguably, this ambient-passing communication is better over explicitly designated channel names, exactly like those in the HO pi-calculus. First, the formalism of the HO pi-calculus (or similar calculi) can be reused to some extent. Second, from the practical viewpoint, this kind of explicit HO communication appears more controllable because the locations are well-defined before the interaction happens. Also, this conforms to the rationale that interactions occur between ambients alone in a fair fashion, as discussed above. In a sense, HO communication offers a measure of quick-passage moving; that is, it can transmit a piece of (ambient) code deep into an ambient's enclosure, rather than stepwise moving. This can make a big difference in the eyes of a programmer. More importantly, to be certain, such HO communications in effect cannot be derived using only the mobility of ambients (i.e., the basic moving capability of ambients); for example, HO communications can send a piece of code to a position beneath a prefix, whereas by no means can the basic movement manage to do this.

As an example, we have the following HO communication in our ambient calculus, which appears to be beyond the basic moving capability of ambients:

$$a[\overline{b}A.M \mid N] \mid b[a(X).R \mid O] \quad \xrightarrow{\tau} \quad a[M \mid N] \mid b[R\{A/X\} \mid O]$$

In this example, prefix $\overline{b}A.M$ means "send A to ambient b and continue as M," and prefix $a(X).R$ means "receive a term from ambient a to instantiate the variable X in R." So one can see that the HO communication relies on the names of both ambients taking part in the interaction. We will formally define this in Section 2.

1.3.2 The capability of exiting

Concerning the exiting capability, we use a more precise and, as such, more secure out-moving capability. That is, the requester has to clearly say which ambient is being called for moving out of the surrounding ambient, that is, real-name (or real-identity) moving. This real-name stipulation

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

makes the exporting of programs more exact and thus more trustworthy and meanwhile helps reduce the possibility of interference. We see an example as follows:

$$a[\overline{out}\ cd.M \mid N] \mid c[d[out\ ca.O \mid A] \mid B] \quad \xrightarrow{\tau} \quad a[M \mid N] \mid c[B] \mid d[O \mid A] \tag{1}$$

In this example, $\overline{out}\ cd$ means "invite ambient d to come out of ambient c," and $out\ ca$ means "called by ambient a to exit (the surrounding) ambient c." Here we require that the name of the ambient that is invited to exit the ambient containing it should be explicitly designated by the ambient that makes the exit call. Specifically, in equation (1), ambient a knows the name of ambient d (i.e., d) that it is calling to get out of c. Previously, in FA, this is not mandatory (see Section 1.2); that is, a does not need to be aware of the name of the ambient that is to move out, and thus, any ambient in c can exit, hence the term "anonymous exit." More to this point, if d changes its name to, say f, anonymous exit still works. However, in our model, since anonymity is disallowed and precise name is enforced, that is not possible. This is what we mean exactly by real name.

We note that $out\ ca$ can be simplified to be $out\ a$, since c is obviously the ambient from which ambient d is moving out, and actually can be detected during run-time. From a pragmatic standpoint, this simple form of out-moving is more flexible and easier to implement and maintain than hard-coding the name of the surrounding ambient. So we can reformulate the above example as follows:

$$a[\overline{out}\ cd.M \mid N] \mid c[d[out\ a.O \mid A] \mid B] \quad \xrightarrow{\tau} \quad a[M \mid N] \mid c[B] \mid d[O \mid A] \tag{2}$$

The new out-moving capability eliminates the possibility of moving anonymously. That is, every movement of an ambient should be explicitly and precisely set up in communicating sessions. We stress that this strengthens the entirely real-name and mutually fair interaction between ambients and removes one loose design end of FA, that is, allowing anonymous out-moving (in fact, this may also be attributed to some technical convenience in the discussion of FA). The concept of anonymity here is somewhat different from that in the paradigm of security, where the notion of anonymity captures the requirement for privacy; for example, a ciphertext should not leak any information about the key or sender/recipient. Here there is no ciphertext but actions (or instructions) instead. So the anonymity in the formalism of ambients is more or less an attribute of unnecessary flavor, at least pertaining to the moving capacity.

If one insists on somehow moving an anonymous ambient around, for example, ambient c in $a[(c)c[M] \mid N]$, then the HO communication can be used to achieve this in a different yet still effective manner. Intuitively, HO communication enables one to transmit some (anonymous) sub-ambient from one ambient to another. For example, we have the following:

$$a[\overline{b}A.M' \mid N] \mid b[a(X).X \mid O] \quad \xrightarrow{\tau} \quad a[M' \mid N] \mid b[A \mid O]$$
$$A \stackrel{\text{def}}{=} (c)c[M]$$

Besides, as to another point, the example above can be tuned to implement scope extrusion. That is,

$$a[(c)\overline{b}A'.M' \mid N] \mid b[a(X).X \mid O] \quad \xrightarrow{\tau} \quad (c)(a[M' \mid N] \mid b[A' \mid O])$$
$$A' \stackrel{\text{def}}{=} c[M] \text{ and } c \notin \text{fn}O(N, O) \text{ (i.e., } c \text{ does not appear free in } N \text{ and } O)$$

This reminds one of the standard bound output in the HO pi-calculus.

1.3.3 Other points

We do not allow parent-child communication for the same reason as in FA. In a nutshell, we stick to the principle that interaction only happens between standalone independent ambients, whereas allowing parent-child communication is as undesirable as allowing communication between an ambient and a non-ambient.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Moreover, in establishing the computational completeness of our ambient calculus, it seems that allowing father-child communication would defeat the purpose of encoding a Turing-complete model: FO pi-calculus in the case of FA and HO pi-calculus in the case of this work. The reason is that the following process would be very arduous to interpret correctly:

$$\overline{a}A.a(X).0$$

Roughly, the encoding of this process would have an internal action between the ambient encoding prefix $\overline{a}$ and the inside ambient encoding prefix $a(X)$, leading to a case that breaks full abstraction. However, this reminds us of asynchronous communication. To this point, parent-child communication is likely essential to encode processes enabling asynchrony.

We drop the open capability for a similar reason as BA. In addition, from the viewpoint of software reuse, directly merging the source code of two ambients is not efficient and easy to raise errors. It would break modularity and render the system hard to test and maintain. A more feasible approach is to use the (third-party) codes as some kind of service (or library). This way, the imported codes are ensured to run correctly, as long as it has been thoroughly tested and properly configured, and, moreover, to delimit the error rate to the greatest extent.

1.4 Contribution

We now summarize the contribution. In this paper, we put forward an ambient calculus called FAHO, evolving from FA, which is purely HO and capable of between-ambient HO communication by means of explicit message-passing and is free of the open capability and FO communication. In addition, the calculus also strengthens FA by demanding real identity in the "exit" out-moving capability; that is, no anonymous ambients can cross the border of the surrounding ambient. The calculus is given a complete examination after being carefully defined. Specifically, this paper makes the following contributions:

1. The calculus, named FAHO, is defined, including the syntax and LTS-based operational semantics. In particular, the out-moving capability requires that both parties (honest or corrupted, from the viewpoint of multiparty security) must report their identities, thus ruling out the mobility of anonymous codes. This comes closer to the original observation and design of FA and is more feasible for implementation. In our calculus, all the interactions are bound to be fair (peer to peer). In particular, the semantic rules for HO communication are given. Basically, they allow a system (of ambients) to be transferred from one ambient to another (again in a peer-to-peer fashion). The following two examples roughly depict the out-moving and HO communication, where τ stands for an interaction and $Q\{A/X\}$ for (syntactically) substituting A for X in Q:

$$\begin{aligned} a[b[out\ c.P] \mid Q] \mid c[\overline{out}\ ab.R] &\xrightarrow{\tau} a[Q] \mid b[P] \mid c[R] \\ a[\overline{b}A.P] \mid b[a(X).Q] &\xrightarrow{\tau} a[P] \mid b[Q\{A/X\}] \end{aligned}$$

   In the out-moving case, ambient b in a is called by c, by prefix *out* c, to move out (of a), and this is paired with the action $\overline{out}\ ab$ in ambient c that interprets as requesting b to move out of a. One can see clearly that every ambient is explicitly designated in the interaction. In the HO communication, ambient a wants to send a process A to ambient b, and this is paired with the action by b, which means receiving from a an input that would then become part of b.
2. We define the bisimulation for FAHO. The bisimulation evolves from the standard concepts in the field and is different in several aspects concerning out-moving and particularly HO communication. In the former, since we restrict to real-name out-moving, the matching clause for anonymous exiting disappears. In the latter, the design turns out to be rather tricky, specifically in the output situation. The crux is that the HO output has to consider

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

the environment it is going into, so it ends up looking like the context bisimulation in the HO process calculi (Sangiorgi, 1993). Moreover, since the environment is now composed of ambients, the context should also be constructed on top of ambients. In addition to all these design issues, one has to be even more careful so that it would nicely keep compatible with the rest of the clauses in the bisimulation, so to ensure the congruence and equivalence properties. Thanks to the delicate design of the bisimulation, we are able to prove that the bisimulation equality (i.e., bisimilarity) is indeed an equivalence and a congruence. For equivalence, we essentially use a somewhat universal lemma called bisimulation lemma (first proposed in Fu (2007), stated in Lemma 6 of this paper). As a byproduct, we also show that the delayed style of HO communication (Sangiorgi, 1993; Sangiorgi and Walker, 2001) coincides with the non-delayed standard version. The proof of this property involves some fresh-prefix technique; that is, two processes are congruent if only they are so in some context made of some fresh names (this kind of technique is seen in other process calculi in the literature). The congruence proof exploits the method similar to related works (e.g., SA and FA). Nevertheless, the proof is rather tedious and tricky in many parts (e.g., those concerning out-moving and HO output). With the help of careful design of these clauses of bisimulation, we are eventually able to establish the congruence of the bisimilarity.

3. We build observational congruence for the bisimilarity. The observational congruence resembles that for FA. There are two contributing points here. One is that we design the parts corresponding to out-moving and HO input and output. Since we have made cautious choices in defining the bisimulation, it becomes relatively tractable to achieve the characterization catering to these two parts. The other point, which might be equally important, is that we prove the coincidence between the barbed congruence and the bisimulation equality in the absence of the open capability. Notably, this also appears to be a novel technical contribution since the previous work heavily uses the open operation when designing the contexts for showing the coincidence. Free of the open capability, we have to design the matching/pinpointing contexts more fine-grained and rigorously. Fortunately, this turns out to be achievable.
4. We exploit the expressiveness of FAHO. Usually, a process model would be expected to be computationally complete, that is, powerful enough to encode the Turing machine or the equivalent. We show that it is the case with FAHO. Specifically, we show that FAHO is able to encode, in a fully abstract way, the minimal HO pi-calculus, which is well-known to be computationally complete (Lanese et al., 2011). The encoding borrows some idea from encoding the FO pi-calculus into FA (Fu, 2007), but goes beyond that since we are using the real-identity exiting. The absence of anonymous exiting, as used by the encoding in (Fu, 2007), renders the encoding tricky, but still implementable. To tackle this, we somewhat presume a registered name set so that ambients with names in this set can be effectively contacted and controlled. The correctness of the encoding then implies that FAHO is a complete model from the standpoint of computation. Besides, the technical approach also makes sense from the interactive viewpoint because ambient calculi, including the one in this work, are essentially HO models, and encoding another HO Turing-complete model would nicely comply with intuition as well as technical feasibility.

Organization

The remainder of this paper is organized as follows. Section 2 defines the ambient calculus of this work, including its syntax, semantics, and related conventions. Section 3 presents the behavioral theory of our ambient calculus, including the bisimulation equality (i.e., bisimilarity), and its equivalence and congruence properties. Section 4 investigates the observational theory. We define the barbed congruence and show its coincidence with bisimilarity. Section 5 demonstrates

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

the expressiveness of the ambient calculus. We exploit an encoding of the minimal HO calculus. Section 5.3.2 concludes the paper with some future work.

2. Definition of FAHO

This section defines the syntax and operational semantics of the ambient calculus in this work. We call this ambient calculus FAHO.

2.1 Syntax

The grammar of FAHO is as follows:

$$
\begin{aligned}
P &:= 0 \mid a[T] \mid P \mid P \mid (c)P \mid !P \\
T &:= 0 \mid X \mid \vartheta.T \mid a[T] \mid T \mid T \mid (c)T \mid !T \\
\vartheta &:= in\ a \mid \overline{in}\ a \mid out\ a \mid \overline{out}\ ab \mid \overline{a}T \mid a(X)
\end{aligned}
$$

Processes are denoted by P, Q and terms by T. At the top level of processes, one only observes ambients; that is, actions all come from inside ambients. By default, we work on processes. We use L, M, N, O, G, H, A, B to range over processes or terms. Names of ambients are ranged over by lowercase letters. There are no other names than ambient names. Free/bound names or variables are defined in the usual way (Sangiorgi and Walker, 2001); that is, $(c)M$ binds c, and $a(X).M$ binds the (process) variable X. Operations fn(·), bn(·), fv(·), bv(·) respectively return the free names, bound names, free variables, and bound variables of the objects under consideration. For convenience, these operations may take a sequence of objects, for example, $\mathrm{fn}(\mathrm{P}_1, \ldots, \mathrm{P}_k)$. By default, we deal with closed processes, that is, those having no free variables. Notation $P\{A/X\}$ means substituting A for every (free) occurrence of X in P. We denote by $\mathfrak{N}$ the set of natural numbers, and $\widetilde{\cdot}$ a tuple, for example, $\widetilde{c}$ and $\widetilde{M}$. Sometimes we write $d \in \widetilde{c}$ (respectively $d \notin \widetilde{c}$) to mean that d is (respectively not) an element of $\widetilde{c}$. Substitution can be extended to tuples in a pointwise fashion.

The reason why we use two identifiers in the out-moving capability has been addressed in Section 1. The in-moving capability is similar to that of FA (Fu, 2007). Intuitively, the prefixes have the following meanings.

$in\ a$	request to move into a
$\overline{in}\ a$	allow a to move in
$out\ a$	called by a to move out
$\overline{out}\ ab$	request b to move out of a
$\overline{a}T$	send T to a
$a(X)$	receive input from a

These will be made precise in the formal semantics. We note that the replication operation can be defined in the domain of HO process calculi, but it is not clear to us if it can be defined in the current setting, which is why we keep the replication primitive.

2.1.1 Context

A context is a process or term with some subprocess replaced by the hole $[\cdot]$. Formally, a context, ranged over by C, is defined by the following grammar. A context is either a process context or a term context. By default, process contexts are considered. In the discussion concerning terms where both contexts are involved, we assume that the contexts switch (or override) correspondingly, so we may simply say contexts for the sake of conciseness.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Definition 1. *The notion of (process) contexts is defined as follows.*

$$\text{Process context: } C_p \stackrel{\text{def}}{=} [\cdot] \mid a[C_t] \mid C_p \mid P \mid (c)C_p \mid !C_p$$
$$\text{Term context: } \quad C_t \stackrel{\text{def}}{=} [\cdot] \mid \vartheta.C_t \mid \overline{a}C_t.T \mid a[C_t] \mid C_t \mid T \mid (c)C_t \mid !C_t$$

We denote by $C[A]$ the term obtained by filling in the hole in C with A. Contexts can be extended to those with multiple occurrences of the hole; that is, the hole can appear several times (see Sangiorgi and Walker, 2001, for a general notion of multiple-hole contexts). In that case, $C[A]$ means replacing each of the holes with A. This may frequently appear when dealing with high-order communication, in which the received term can be used more than once.

2.2 Semantics

We denote by $\equiv$ the standard structural congruence (Milner et al., 1992; Cardelli and Gordon, 2000; Sangiorgi and Walker, 2001; Fu, 2007) over terms, that is, the smallest relation satisfying the monoid laws for parallel composition, commutative laws for both composition and restriction and a distributive law. The specific definition is as follows:

$$P \mid 0 \equiv P, \qquad P \mid (P' \mid P'') \equiv (P \mid P') \mid P'', \qquad P \mid P' \equiv P' \mid P$$
$$(c)(d)P \equiv (d)(c)P, \qquad (c)(P \mid P') \equiv (c)P \mid P' \text{ if } c \notin \text{fn}(P')$$

Conventionally, structurally congruent processes are considered the same. Notation $(\widetilde{c})\langle M \between N\rangle$, sometimes called a concretion in the field, means the ambient M is in transit with N as the residual and $\widetilde{c}$ as the restricted names shared between them. We use D to range over this kind of term. We set as an extension of the structural congruence to concretions, for an apparent reason, that $(\widetilde{c})\langle M \between N\rangle \mid M' \equiv (\widetilde{c})\langle M \between (N \mid M')\rangle$ assuming no name capture. In Figure 1, we define the operational semantics using the LTS.

We focus on processes; that is, ambients are the basic interacting parts of a concurrent system. In terms of the semantics, it is straightforward to see that a process indeed evolves into another process through an interaction. In the out-moving interaction rule (*Inact−out*), there is somewhat an authentication/verification when parallel components engage choreography by action labels. Recall example (2) on page 4, and we illustrate how the semantics works for it. Somehow the semantics come with a certain kind of match in the moving-action labels.

$$\dfrac{\dfrac{\dfrac{}{\overline{out}\ cd.M \xrightarrow{\overline{out}\ cd} M}\,(\text{Prefix1})}{\overline{out}\ cd.M \mid N \xrightarrow{\overline{out}\ cd} M \mid N}\,(\text{Par})}{a[\overline{out}\ cd.M \mid N] \xrightarrow{\overline{out}\ cda} a[M \mid N]}\,(\text{Mov-coout}) \quad \dfrac{\dfrac{\dfrac{\dfrac{}{out\ a.O \xrightarrow{out\ a} O}\,(\text{Prefix1})}{out\ a.O \mid A \xrightarrow{out\ a} O \mid A}\,(\text{Par})}{d[out\ a.O \mid A] \xrightarrow{out\ da} \langle d[O \mid A] \between 0\rangle}\,(\text{Mov-out1})}{d[out\ a.O \mid A] \mid B \xrightarrow{out\ da} \langle d[O \mid A] \between B\rangle}\,(\text{Par})}{c[d[out\ a.O \mid A] \mid B] \xrightarrow{out\ cda} c[B] \mid d[O \mid A]}\,(\text{Mov-out2})$$
$$\dfrac{}{a[\overline{out}\ cd.M \mid N] \mid c[d[out\ a.O \mid A] \mid B] \xrightarrow{\tau} a[M \mid N] \mid c[B] \mid d[O \mid A]}\,(\text{Intact-out})$$

For the sake of readability, it would be convenient to understand action *out da* as "d is called by a to move outward," action *out cda* as "d is called by a to move out of c," and action $\overline{out}$ *cda* as "a asks d to move outside c."

The in-movement action is similar to that of FA, except that the action label is more explicit about the involved ambients' action path, so to correspond to the out-movement. Here is an example.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

$$(Struc)\quad \frac{N \equiv M \qquad M \xrightarrow{\lambda} M' \qquad M' \equiv N'}{N \xrightarrow{\lambda} N'} \qquad (Inher)\quad \frac{M \xrightarrow{\tau} M'}{a[M] \xrightarrow{\tau} a[M']}$$

$$(Par)\quad \frac{M \xrightarrow{\lambda} M'}{M \mid N \xrightarrow{\lambda} M' \mid N} \qquad (Res)\quad \frac{M \xrightarrow{\lambda} M' \qquad a \notin \mathrm{n}(\lambda)}{(a)M \xrightarrow{\lambda} (a)M'} \qquad (Prefix1)\quad \frac{\vartheta \text{ is not } a(X)}{\vartheta.M \xrightarrow{\vartheta} M}$$

$$(Prefix2)\quad \frac{}{a(X).M \xrightarrow{a(M')} M\{M'/X\}}$$

$$(Mov{-}in)\quad \frac{M \xrightarrow{in\, b} M'}{a[M] \xrightarrow{in\, ab} \langle a[M'] \between 0\rangle} \qquad (Mov{-}coin)\quad \frac{M \xrightarrow{\overline{in}\, b} M'}{a[M] \xrightarrow{\overline{in}\, ba} a[M' \mid [\cdot]]}$$

$$(Intact{-}in)\quad \frac{M \xrightarrow{in\, ab} (\widetilde{c})\langle M_1 \between M_2\rangle \qquad N \xrightarrow{\overline{in}\, ab} C[\cdot]}{M \mid N \xrightarrow{\tau} (\widetilde{c})(M_2 \mid C[M_1])}$$

$$(Mov{-}out1)\quad \frac{M \xrightarrow{out\, a} M'}{b[M] \xrightarrow{out\, ba} \langle b[M'] \between 0\rangle} \qquad (Mov{-}out2)\quad \frac{M \xrightarrow{out\, ba} (\widetilde{d})\langle M_1 \between M_2\rangle \qquad c \notin \widetilde{d}}{c[M] \xrightarrow{out\, cba} (\widetilde{d})(c[M_2] \mid M_1)}$$

$$(Mov{-}coout)\quad \frac{M \xrightarrow{\overline{out}\, cb} M'}{a[M] \xrightarrow{\overline{out}\, cba} a[M']} \qquad (Intact{-}out)\quad \frac{M \xrightarrow{out\, cba} M' \qquad N \xrightarrow{\overline{out}\, cba} N'}{M \mid N \xrightarrow{\tau} M' \mid N'}$$

$$(HOcom{-}input)\quad \frac{M \xrightarrow{b(M')} M_1}{a[M] \xrightarrow{ab(M')} a[M_1]} \qquad (HOcom{-}output)\quad \frac{M \xrightarrow{\overline{b}M'} M_1}{a[M] \xrightarrow{\overline{ab}M'} a[M_1]}$$

$$(HOcom{-}res{-}output1)\quad \frac{M \xrightarrow{(\widetilde{c})\overline{b}M'} M_1 \qquad d \in \mathrm{fn}(M') - \widetilde{c}}{(d)M \xrightarrow{(d\widetilde{c})\overline{b}M'} M_1}$$

$$(HOcom{-}res{-}output2)\quad \frac{M \xrightarrow{(\widetilde{c})\overline{b}M'} M_1}{a[M] \xrightarrow{(\widetilde{c})\overline{ab}M'} a[M_1]}$$

$$(HOcom{-}res{-}output3)\quad \frac{M \xrightarrow{(\widetilde{c})\overline{ab}M'} M_1 \qquad d \in \mathrm{fn}(M') - \widetilde{c}}{(d)M \xrightarrow{(d\widetilde{c})\overline{ab}M'} M_1}$$

$$(HOIntact)\quad \frac{M \xrightarrow{ab(M')} M_1 \qquad N \xrightarrow{(\widetilde{c})\overline{ba}M'} N_1}{M \mid N \xrightarrow{\tau} (\widetilde{c})(M_1 \mid N_1)}$$

$$(Rep)\quad \frac{M \xrightarrow{\lambda} M'}{!M \xrightarrow{\lambda} M' \mid !M} \qquad (Rep1)\quad \frac{M \xrightarrow{in\, ab} (\widetilde{c})\langle M_1 \between M_2\rangle \qquad M \xrightarrow{\overline{in}\, ab} C[\cdot]}{!M \xrightarrow{\tau} (\widetilde{c})(M_2 \mid C[M_1]) \mid !M}$$

$$(Rep2)\quad \frac{M \xrightarrow{out\, cba} M' \qquad M \xrightarrow{\overline{out}\, cba} M''}{!M \xrightarrow{\tau} (M' \mid M'') \mid !M} \qquad (Rep3)\quad \frac{M \xrightarrow{ab(M')} M_1 \qquad M \xrightarrow{(\widetilde{c})\overline{ba}M'} M_2}{!M \xrightarrow{\tau} (\widetilde{c})(M_1 \mid M_2) \mid !M}$$

Figure 1. LTS for FAHO.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{in\,b.M \xrightarrow{in\,b} M}\,(\text{Prefix1})}{in\,b.M \mid N \xrightarrow{in\,b} M \mid N}\,(\text{Par})}{a[in\,b.M \mid N] \xrightarrow{in\,ab} \langle a[M \mid N] \between 0\rangle}\,(\text{Mov-in})}{a[in\,b.M \mid N] \mid c[O] \xrightarrow{in\,ab} \langle a[M \mid N] \between c[O]\rangle}\,(\text{Par}) \qquad \dfrac{\dfrac{\dfrac{}{\overline{in}\,a.A \xrightarrow{\overline{in}\,a} A}\,(\text{Prefix1})}{\overline{in}\,a.A \mid B \xrightarrow{\overline{in}\,a} A \mid B}\,(\text{Par})}{b[\overline{in}\,a.A \mid B] \xrightarrow{\overline{in}\,ab} b[A \mid B \mid [\cdot]]}\,(\text{Mov-coin})}{a[in\,b.M \mid N] \mid c[O] \mid b[\overline{in}\,a.A \mid B] \xrightarrow{\tau} c[O] \mid b[A \mid B \mid a[M \mid N]]}\,(\text{Intact-in})$$

To cater for readability, one can treat action *in ab* as "*a* wants to move into *b*," and action $\overline{in}\,ab$ as "*b* allows *a* to be inside."

In rule (*HOIntact*), there is a name-path duality/pairing. Label $ab(M')$ means "*a* receives from *b* term M'" $\overline{ab}M'$, sometimes written $\overline{ab}(M')$, means "*a* sends to *b* term M'." The interaction can involve some local names $\widetilde{c}$ that can be empty, brought along by the output action. We give an example below.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\overline{b}A.M \xrightarrow{\overline{b}A} M}\,(\text{Prefix1})}{\overline{b}A.M \mid O_1 \xrightarrow{\overline{b}A} M \mid O_1}\,(\text{Par})}{a[\overline{b}A.M \mid O_1] \xrightarrow{\overline{ab}A} a[M \mid O_1]}\,(\text{HOcom-output}) \qquad \dfrac{\dfrac{\dfrac{}{a(X).N \xrightarrow{a(A)} N\{A/X\}}\,(\text{Prefix2})}{a(X).N \mid O_2 \xrightarrow{a(A)} N\{A/X\} \mid O_2}\,(\text{Par})}{b[a(X).N \mid O_2] \xrightarrow{ba(A)} b[N\{A/X\} \mid O_2]}\,(\text{HOcom-input})}{a[\overline{b}A.M \mid O_1] \mid b[a(X).N \mid O_2] \xrightarrow{\tau} a[M \mid O_1] \mid b[N\{A/X\} \mid O_2]}\,(\text{HOIntact})$$

We emphasize that the communication part of the semantics does not include FO communication, and other forms of HO communication either. There are, however, possibilities of extending the communication inspired by the works in the literature, for example, explicit parent-child HO communication (anonymous counterpart can also be defined similarly), as demonstrated below.

$$a[\overline{b}A.M \mid b[a(X).N]] \xrightarrow{\tau} a[M \mid b[N\{A/X\}]]$$

To some extent, this is not a peer-to-peer communication since it happens in a local environment if one thinks of *a* as a global context; also recall the discussion in Section 1. We currently do not include such a kind of communication in this work.

We note that by the semantics, the ambient calculus prohibits any form of anonymous interaction, including moving and communicating. This distinguishes the calculus here from FA, which allows anonymous exit, or other ambient calculi that allow arbitrary anonymous movement. Though arguable, the point is that it may no longer be feasible to permit anonymous protocols in a world that calls for increasingly more assertive real-identity transactions; see also the explanation in Section 1.

We have three rules (*HOcom−res−output*1), (*HOcom−res−output*2), (*HOcom−res−output*3) for scope extrusion during HO communications, for the reason that the restriction can occur both inside and outside an ambient. With these rules, names inside the transmitted process can become extruded, so to connect the receiver and sender. By contrast, there is no scope extrusion during in-movement or out-movement; that is, a restricted ambient (name) finds no way to be outputted to a remote ambient to be shared for interaction employing only moving in or out.

The rules (*Rep*), (*Rep*1), (*Rep*2), (*Rep*3) use a de facto standard recourse to defining the behavior of replication; see (Sangiorgi and Walker, 2001) for a reference. Intuitively, it captures that !*P* may be imagined as a composition of infinitely many *P*'s. So the same process can interact with its clone, for example, $M \mid M$ in which $M \stackrel{\text{def}}{=} a[in\,b.0] \mid b[\overline{in}\,a.0]$.

Actions from processes are ranger over by α, β, λ. In total, there are eight kinds of actions (labels). The notions of free/bound names or variables naturally extend to actions. As mentioned, we sometimes write $\overline{ab}(A)$ instead of $\overline{ab}A$ for the sake of clarity. As usual, we use $\Longrightarrow$ for the

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

reflexive transitive closure of τ actions, $\stackrel{\alpha}{\Longrightarrow}$ for $\Longrightarrow \stackrel{\alpha}{\rightarrow} \Longrightarrow$, and $\stackrel{\widehat{\alpha}}{\Longrightarrow}$ for $\stackrel{\alpha}{\Longrightarrow}$ if α is not τ and $\Longrightarrow$ otherwise. Additionally, $P \stackrel{\widehat{\alpha}}{\rightarrow} P'$ stands for $P \stackrel{\alpha}{\rightarrow} P'$ if α is not τ and $P \equiv P'$ otherwise.

Example

Before going ahead, we provide an example that makes use of both the HO communication and moving capabilities, so to illustrate how they interplay with each other and how potentially they can be used in realistic scenes. The example implements a multistep protocol that may appear as part of sophisticated schemes in modern distributed computing, such as pervasive and blockchain systems.

The protocol is described as follows:

1. We intend to implement somewhat a delegated computation. Here, an ambient may be considered as a computing node in the distributed environment. Ambient a (Alice), collaborating with c (Charles), wants to execute some code in b (Bob) that might have more resources of GPU. The code to be run is contributed by both Alice and Charles (and actually, the parts, respectively, supplied by them can even interact to trigger more custom functionality at Bob's place).
2. Alice hopes to carry out the protocol in a controlled manner (e.g., authentication facilitated). So somehow, a three-party (i.e., Alice, Bob, and Charles) handshake activation is necessary for the execution to start.
3. Basically, what is to be run at Bob's is uploaded in two phases. In the first phase, Alice sends the code of her part (jumping ahead, it is O_1 in the formulation shortly) to Bob, using HO communication since the code is going somewhere behind some controlling code (i.e., some prefix) at Bob's. In the second phase, Charles sends Bob the code of his part (jumping ahead, it is O_2 in the formulation shortly), using simply the movement capabilities (here, O_1 also helps to get O_2 into position since it is already in Bob's place). The two phases are interwoven with handshake synchronizations, so to ensure that the uploading interactions are done in the correct way. These synchronizations are also realized by communications.
4. Now, all the code has been appropriately transferred to Bob and is ready to kick off. In turn, Bob can run O_1 and O_2 (possibly incurring more interactions with the other part of Bob) in probably a much more efficient fashion by taking his hardware advantage.
5. Then, Alice and Bob move on to the remainder of their programs, respectively, continuing as computing nodes in the distributed network.

Now we formulate the protocol in FAHO. The processes P_{client} (Alice, with her collaborator Charles c) and P_{server} (Bob) represent two peers in the interaction, with the former as the client and the latter the server. For the sake of convenience, we use two shortcuts: $a.T \stackrel{\text{def}}{=} a(X).T$ in which X does not appear in T and $\overline{a}.T \stackrel{\text{def}}{=} \overline{a}0.T$. We may also omit the trailing 0 processes, for example, a and $\overline{a}$ represent $a.0$ and $\overline{a}.0$, respectively.

$$
\begin{aligned}
P_{\text{client}} &\stackrel{\text{def}}{=} (de)(a[\overline{b}O_1.b.\overline{c}.O_{10}] \mid c[a.\overline{b}.in\ b.O_2]) \\
P_{\text{server}} &\stackrel{\text{def}}{=} b[a(X).\overline{a}.(c.X \mid O_3) \mid \overline{in}\ c.O_4] \\
&\text{where} \\
O_1 &\stackrel{\text{def}}{=} d[\overline{out}\ ce.O_5] \\
O_2 &\stackrel{\text{def}}{=} e[out\ d.O_6] \\
O_5 &\stackrel{\text{def}}{=} \overline{e}O_7.O_8 \\
O_6 &\stackrel{\text{def}}{=} d(Y).O_9
\end{aligned}
$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

The auxiliary terms O_i $(i = 1, 2, \ldots, 10)$ are used to make the system modular, so to have a more readable flow of the protocol. For simplicity, $O_3, O_4, O_7, O_8, O_9, O_{10}$ are not specified, and this allows for more contents of design in the protocol. We also assume that O_3 is free of X.

As stipulated by the protocol description, the system $P_{\text{client}} \mid P_{\text{server}}$ computes as follows:

$$\begin{aligned}
& P_{\text{client}} \mid P_{\text{server}} \\
\xrightarrow{\tau}\ & (de)((a[b.\overline{c}.O_{10}] \mid c[a.\overline{b}.in\ b.O_2]) \mid b[\overline{a}.(c.O_1 \mid O_3) \mid \overline{in}\ c.O_4]) \\
\xrightarrow{\tau}\ & (de)((a[\overline{c}.O_{10}] \mid c[a.\overline{b}.in\ b.O_2]) \mid b[(c.O_1 \mid O_3) \mid \overline{in}\ c.O_4]) \\
\xrightarrow{\tau}\ & \equiv (de)(a[O_{10}] \mid c[\overline{b}.in\ b.O_2] \mid b[(c.O_1 \mid O_3) \mid \overline{in}\ c.O_4]) \\
\xrightarrow{\tau}\ & \equiv (de)(a[O_{10}] \mid c[in\ b.O_2] \mid b[(O_1 \mid O_3) \mid \overline{in}\ c.O_4]) \\
\xrightarrow{\tau}\ & \equiv (de)(a[O_{10}] \mid b[O_1 \mid O_3 \mid O_4 \mid c[O_2]]) \\
& \equiv (de)(a[O_{10}] \mid b[d[\overline{out}\ ce.O_5] \mid O_3 \mid O_4 \mid c[e[out\ d.O_6]]]) \\
\xrightarrow{\tau}\ & \equiv (de)(a[O_{10}] \mid b[d[O_5] \mid O_3 \mid O_4 \mid c[0] \mid e[O_6]]) \\
& \equiv (de)(a[O_{10}] \mid b[c[0] \mid d[\overline{e}O_7.O_8] \mid e[d(Y).O_9] \mid O_3 \mid O_4]) \\
\xrightarrow{\tau}\ & \equiv (de)(a[O_{10}] \mid b[c[0] \mid d[O_8] \mid e[O_9\{O_7/Y\}] \mid O_3 \mid O_4]) \stackrel{\text{def}}{=} P_{\text{result}}
\end{aligned}$$

If we consider the resulting process P_{result}, its components $a[O_{10}]$ and b (holding $d[O_8], e[O_9\{O_7/Y\}]$, O_3 and O_4) may continue to interact, giving rise to further details of the protocol in a potentially big picture.

The following property is a routine induction over the semantic rules. Here and henceforth, we will often omit existential statements like "for some . . ." if no confusion arises.

Lemma 2.

1. *If M is a process and $M \xrightarrow{\tau} M'$, then M' is also a process.*
2. *If M does an action, then the continual term has the form as stated below:*

   - $M \xrightarrow{in\ ab} (\widetilde{c})\langle M_1 \between M_2\rangle$ *in which* $M_1 \equiv a[M']$ *for some* M';
   - $M \xrightarrow{\overline{in}\ ab} C$ *in which* C *is a (process) context of the form* $(\widetilde{d})(b[[\cdot] \mid O] \mid O')$;
   - $M \xrightarrow{out\ ab} (\widetilde{c})\langle M_1 \between M_2\rangle$ *in which* $M_1 \equiv a[M']$ *for some* M';
   - $M \xrightarrow{out\ abc} M'$ *in which* $M' \equiv (\widetilde{d})(a[M_1] \mid b[M_2] \mid O)$ *for some* M_1, M_2 *and* O;
   - $M \xrightarrow{\overline{out}\ abc} M'$ *in which* $M' \equiv c[M'']$ *for some* M'';
   - $M \xrightarrow{ab(A)} M'$ *in which* $M' \equiv C[A]$ *for some context* $C \stackrel{\text{def}}{=} (\widetilde{d})(a[C'] \mid O)$ *s.t.* $M \xrightarrow{ab(B)} C[B]$;
   - $M \xrightarrow{\overline{ab}(A)} M'$ *in which* $M' \equiv a[M'']$ *for some* M'';
   - $M \xrightarrow{(\widetilde{d})\overline{ab}(A)} M'$ *in which* $M' \equiv a[M'']$ *for some* M''.

3. Behavioral equivalences

In this section, we examine the behavioral equivalence, in particular the bisimulation equality for FAHO. We define the notion of bisimulation and investigate its properties.

Definition 3. *A symmetric binary relation $\mathscr{R}$ on (closed) processes is a bisimulation if $P\ \mathscr{R}\ Q$ implies the following properties:*

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

- *(in-mov). If* $P \xrightarrow{in\,ab} (\widetilde{d})\langle P_1 \between P_2\rangle$, *then* $Q \Longrightarrow \xrightarrow{in\,ab} (\widetilde{e})\langle Q_1 \between Q_2\rangle$, *and for every context* $C \stackrel{\text{def}}{=} b[[\cdot] \mid O]$, *it holds that* $(\widetilde{e})(Q_2 \mid C[Q_1]) \Longrightarrow \mathscr{R}^{-1}\ (\widetilde{d})(P_2 \mid C[P_1])$.
- *(coin-mov). If* $P \xrightarrow{\overline{in}\,ab} C$, *then* $Q \Longrightarrow \xrightarrow{\overline{in}\,ab} C'$, *and for every* M, *it holds that* $C'[a[M]] \rightarrow \mathscr{R}^{-1}\ C[a[M]]$.
- *(out1-mov). If* $P \xrightarrow{out\,ab} (\widetilde{d})\langle P_1 \between P_2\rangle$, *then* $Q \Longrightarrow \xrightarrow{out\,ab} (\widetilde{e})\langle Q_1 \between Q_2\rangle$, *and for every context* $C \stackrel{\text{def}}{=} c[[\cdot] \mid O]$, *it holds that* $(\widetilde{e})(Q_1 \mid C[Q_2]) \Longrightarrow \mathscr{R}^{-1}\ (\widetilde{d})(P_1 \mid C[P_2])$.
- *(out2-mov). If* $P \xrightarrow{out\,abc} P'$, *then* $Q \xRightarrow{out\,abc} Q'$ *and* $P' \mathscr{R}\ Q'$.
- *(coout-mov). If* $P \xrightarrow{\overline{out}\,abc} P'$, *then* $Q \xRightarrow{\overline{out}\,abc} Q'$ *and* $P' \mathscr{R}\ Q'$.
- *(hocom-input). If* $P \xrightarrow{ab(A)} P'$, *then* $Q \xRightarrow{ab(A)} Q'$ *and* $P' \mathscr{R}\ Q'$.
- *(hocom-res-output). If* $P \xrightarrow{(\widetilde{d})\overline{ab}(A)} P'$, *then* $Q \xRightarrow{(\widetilde{e})\overline{ab}(B)} Q'$, *and for every context* $C \stackrel{\text{def}}{=} b[C']$, *it holds that* $(\widetilde{d})(P' \mid C[A])\ \mathscr{R}\ (\widetilde{e})(Q' \mid C[B])$.
- *(interaction). If* $P \xrightarrow{\tau} P'$, *then* $Q \Longrightarrow Q'$ *and* $P' \mathscr{R}\ Q'$.

The bisimilarity, written $\approx$, *is the union of all bisimulations (viz., the largest one).*

Remark. *In what follows, we remark on the notion of bisimulation.*

- We often use $\mathscr{R}_1\mathscr{R}_2$ to denote the composition of the two relations. For example, $P \xrightarrow{\alpha} \approx Q$ means $P \xrightarrow{\alpha} P' \approx Q$ for some P'.
- The bisimulation can be extended to (closed) terms. We note that the LTS also works on terms. This extension shall bring convenience when handling processes, for example, while discussing the closure properties. We below present the extra clauses needed to extend the definition of bisimulation. Assume $M \mathscr{R} N$ and they satisfy the follow-up two clauses in addition to those in Definition 3:
  - (prefix). If $M \xrightarrow{\vartheta} M'$ in which ϑ is not an output, then $N \xRightarrow{\vartheta} N'$ and $M' \mathscr{R}\ N'$;
  - (prefix-output). If $M \xrightarrow{(\widetilde{d})\overline{a}A} M'$, then $N \xRightarrow{(\widetilde{e})\overline{a}B} N'$, and for every context $C \stackrel{\text{def}}{=} a[C']$, every name c and O, it holds that $(\widetilde{d})(c[M' \mid O] \mid C[A])\ \mathscr{R}\ (\widetilde{e})(c[N' \mid O] \mid C[B])$.

  The second clause above adopts the style of context bisimulation (Sangiorgi, 1993), which considers the transmitted term and the residual term as a whole, except that the residual term is now tackled in an arbitrary ambient c with a parallel component. On the system level, the output action fires from the ambient, and the residual has to stay put in parallel with some within-ambient context; recall that we do not have local HO communication – that is, communications merely occur between ambients. Besides, this design brings technical convenience for the congruence properties.
- In Definition 3, the appearance of $\mathscr{R}^{-1}$ (i.e., the inverse of $\mathscr{R}$) can be replaced by $\mathscr{R}$ because $\mathscr{R}$ is symmetric. Actually, we will often write $\mathscr{R}$ instead of $\mathscr{R}^{-1}$ for the sake of clarity.
- We denote by $\sim$ the strong version of bisimilarity, which is obtained by removing the weak transitions and using strong transitions in the definition. That is, if $P \xrightarrow{\alpha} M$ and α is not τ, then one removes $\Longrightarrow$ in the clause and replaces $\xRightarrow{\alpha}$ with $\xrightarrow{\alpha}$; otherwise one replaces $\Longrightarrow$ with $\xrightarrow{\tau}$.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

- In the definition above and all the arguments in the following, we always assume no name captures concerning the contexts, with the help of necessary alpha-conversion.
- For in-movement, it should be no surprise to require that the outcome of in-movement or coin-movement (concretion or context, respectively) closes the bisimulation game in a universal way. Also we note that terms of the form $(\widetilde{d})\langle P \between P'\rangle$ or context C are not capable of actions, and the comparison of the continual pairs is deferred to the stage when processes are regained (through universal quantifications), in the way stated in the definition.
- The bisimulation is in a late fashion, meaning that the quantifiers appear after the matching action. Analogously, the early version can be defined (Sangiorgi and Walker, 2001; Fu, 2007). We stick to the late version because it is more natural and relatively easy to understand and tackle. It is also worthwhile to point out that in the first three clauses, we adopt a design similar to that of Fu (2007), which restricts the related (arbitrary) context C to certain forms directed at matching the corresponding moving actions. For example, in the first clause for moving in, since the target ambient is clear, it is good to only consider those contexts that are inside the target ambient. For the HO output action, the idea is borrowed from the HO pi-calculus (Sangiorgi and Walker, 2001) and combines with the moving primitive of ambients. So this should lend confidence to its reasonability, though the proof of its properties turns out to be more involved than the case for the HO pi-calculus. Notably, the context here is entirely different from that in the HO pi-calculus.
- The HO output clause in the bisimulation can also be defined as the delayed style (Sangiorgi, 1993; Sangiorgi and Walker, 2001). Specifically, the delay-style HO output clause is as follows:

  – (hocom-res-output-delayed). If $P \xrightarrow{(\widetilde{d})\overline{ab}(A)} P'$, then $Q \Longrightarrow \xrightarrow{(\widetilde{e})\overline{ab}(B)} Q'$, and for every context $C \stackrel{\text{def}}{=} b[C']$, it holds that $(\widetilde{e})(Q' \mid C[B]) \Longrightarrow \cdot\ \mathscr{R}^{-1}\ (\widetilde{d})(P' \mid C[A])$.

  We note that in the delayed style, the matching action by Q ends with a visible action $\xrightarrow{(\widetilde{e})\overline{ab}(B)}$, and the resulting process $(\widetilde{d})(P' \mid C[A])$ may continue to have some internal moves before fulfilling the simulation. The resulting bisimilarity, that is, the bisimilarity obtained by replacing the HO output clause in Definition 3 with the above one, is called the delayed bisimilarity and denoted by $\approx_{\text{dl}}$ (the corresponding strong version by $\sim_{\text{dl}}$). We will show below that $\approx$ and $\approx_{\text{dl}}$ actually coincide.
- The bisimulation is defined on the closed processes, that is, those that do not have free variables. It can be extended to open processes in the usual way. That is, two open processes E and F s.t. $X \in \text{fv(E,F)}$ are bisimilar, written $E \approx F$, if $E\{R/X\} \approx F\{R/X\}$ for every closed R. This can, in turn, be extended to processes containing multiple free variables.

Bisimulation up-to

Bisimulation up-to is a standard technique to build bisimulations; a bisimulation up-to, say $\sim$, is not necessarily a bisimulation itself but is assured to be contained by bisimilarity (see Sangiorgi and Walker, 2001, for a complete introduction and discussion). Below, we specify the bisimulation up-to instances for our purpose. We note that, in general, the technique of bisimulation up-to the weak bisimilarity is not necessarily sound. The failure point consists in that the simulation may be vacuous. By disallowing vacuous simulation for the up-to matching, the technique is still valid (Sangiorgi, 1993; Sangiorgi and Milner, 1992; Sangiorgi and Walker, 2001).

Definition 4. *A symmetric binary relation $\mathscr{R}$ on processes is a bisimulation up-to $\sim$ (respectively, $\equiv$) if it satisfies the conditions of Definition 3, except that every occurrence of $\mathscr{R}$ in the conditions is replaced with $\sim \mathscr{R} \sim$ (respectively, $\equiv \mathscr{R} \equiv$).*

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

A symmetric binary relation $\mathscr{R}$ on processes is a bisimulation up-to $\approx$ if it satisfies the conditions of Definition 3, except that every occurrence of $\mathscr{R}$ in the conditions is replaced with $\approx\mathscr{R}\approx$, and moreover, the last clause for interaction is replaced with the following.

- *If $P \xrightarrow{\tau} P'$, then either $Q \Longrightarrow Q'$ with $P' \mathscr{R} Q'$ or $Q \xRightarrow{\tau} Q'$ and $P' \approx \mathscr{R} \approx Q'$.*

To be useful, the bisimulation up-to technique has to be sound, as the following lemma states. See Sangiorgi and Walker (2001) and Pous and Sangiorgi (2011) for a detailed discussion.

Lemma 5. *If $\mathscr{R}$ is a bisimulation up-to $\sim$, $\equiv$, or $\approx$, then it holds that $\mathscr{R} \subseteq \approx$.*

Now we show that $\approx$ is both an equivalence relation and a congruence relation. As a prerequisite, we give a proof technique called the bisimulation lemma (Fu, 2007).

Lemma 6. *Assume that P and Q are processes.*

1. *If $P \Longrightarrow \approx Q$ and $Q \Longrightarrow \approx P$, then $P \approx Q$.*
2. *If $P \Longrightarrow \approx_{\mathrm{dl}} Q$ and $Q \Longrightarrow \approx_{\mathrm{dl}} P$, then $P \approx_{\mathrm{dl}} Q$.*

Proof. The proof is quite straightforward. In both cases, for Q to simulate P, it simply goes through some internal actions to arrive at a bisimilar state as P and then continues simulating as expected. The other direction is similar. □

The bisimulation lemma was proposed by Fu and is a general property for most well-defined bisimulations. Interested readers can refer to Fu (2007) for more details concerning this lemma. Below is another useful property whose proof exploits the bisimulation lemma.

Lemma 7. *Assume $g \notin \mathrm{fn(M,N,A,B)} \cup \widetilde{d} \cup \widetilde{e} \cup \{b\}$ and $b \notin \widetilde{d} \cup \widetilde{e}$. Then*

$$(\widetilde{d})(M \mid b[\overline{g}A]) \approx (\widetilde{e})(N \mid b[\overline{g}B])$$

implies

$$(\widetilde{d})(M \mid b[C[A]]) \approx (\widetilde{e})(N \mid b[C[B]])$$

for every context C that brings no name conflict. The result also holds for $\approx_{\mathrm{dl}}$; that is, it is still true if one replaces $\approx$ with $\approx_{\mathrm{dl}}$.

Proof. The proofs for $\approx$ and $\approx_{\mathrm{dl}}$ are similar, and we focus on $\approx$, for this case is slightly harder. Since g is fresh as described, the output action $(\widetilde{d})(M \mid b[\overline{g}A]) \xrightarrow{(\widetilde{d_1})\overline{bg}A} (\widetilde{d_2})(M \mid b[0])$, in which $\widetilde{d} = \widetilde{d_1} \cup \widetilde{d_2}$ and $\widetilde{d_1} \cap \widetilde{d_2} = \emptyset$, must be matched by

$$(\widetilde{e})(N \mid b[\overline{g}B]) \Longrightarrow (\widetilde{e})(N_1 \mid b[\overline{g}B]) \xrightarrow{(\widetilde{e_1})\overline{bg}B} (\widetilde{e_2})(N_1 \mid b[0]) \Longrightarrow (\widetilde{e_2})(N_2 \mid b[0])$$

where $\widetilde{e} = \widetilde{e_1} \cup \widetilde{e_2}$, $\widetilde{e_1} \cap \widetilde{e_2} = \emptyset$, and $N \Longrightarrow N_1 \Longrightarrow N_2$. This matching can be rewritten as

$$(\widetilde{e})(N \mid b[\overline{g}B]) \Longrightarrow (\widetilde{e})(N_2 \mid b[\overline{g}B]) \xrightarrow{(\widetilde{e_1})\overline{bg}B} (\widetilde{e_2})(N_2 \mid b[0])$$

Now, by the requirement of the bisimulation, for every context C, it holds that

$$(\widetilde{d_1})((\widetilde{d_2})(M \mid b[0]) \mid g[C[A]]) \approx (\widetilde{e_1})((\widetilde{e_2})(N_2 \mid b[0]) \mid g[C[B]])$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

which can be organized as

$$(\widetilde{d})(M \mid b[0] \mid g[C[A]]) \approx (\widetilde{e})(N_2 \mid b[0] \mid g[C[B]])$$

That is,

$$(\widetilde{d})(M \mid g[C[A]]) \approx (\widetilde{e})(N_2 \mid g[C[B]])$$

In summary, we have

$$(\widetilde{d})(M \mid g[C[A]]) \approx (\widetilde{e})(N_2 \mid g[C[B]]) \Longleftarrow (\widetilde{e})(N \mid g[C[B]])$$

Similarly, we have

$$(\widetilde{e})(M \mid g[C[A]]) \Longrightarrow \approx (\widetilde{e})(N \mid g[C[B]])$$

By the bisimulation lemma (Lemma 6), we infer

$$(\widetilde{d})(M \mid g[C[A]]) \approx (\widetilde{e})(N \mid g[C[B]]) \tag{3}$$

Taking C as $\overline{b}[\cdot]$, we have

$$(\widetilde{d})(M \mid g[\overline{b}A]) \approx (\widetilde{e})(N \mid g[\overline{b}B]) \tag{4}$$

Now we are at a position similar to the beginning of the proof of this lemma, with b and g swapped but the action $\overline{g}bA$ still fresh (i.e., g fresh). Hence through a similar argument, we can obtain the desired result, that is, equation (3) with g replaced by b.

Specifically, in (4), the action $(\widetilde{d})(M \mid g[\overline{b}A]) \xrightarrow{(\widetilde{d_1})\overline{g}bA} (\widetilde{d_2})(M \mid g[0])$ must be matched by

$$(\widetilde{e})(N \mid g[\overline{b}B]) \Longrightarrow (\widetilde{e})(N_3 \mid g[\overline{b}B]) \xrightarrow{(\widetilde{e_1})\overline{g}bB} (\widetilde{e_2})(N_3 \mid g[0]) \Longrightarrow (\widetilde{e_2})(N_4 \mid g[0])$$

where $N \Longrightarrow N_3 \Longrightarrow N_4$. Again, this matching can be rewritten as

$$(\widetilde{e})(N \mid g[\overline{b}B]) \Longrightarrow (\widetilde{e})(N_4 \mid g[\overline{b}B]) \xrightarrow{(\widetilde{e_1})\overline{g}bB} (\widetilde{e_2})(N_4 \mid g[0])$$

As regulated by the bisimulation, for every context C, it holds that

$$(\widetilde{d_1})((\widetilde{d_2})(M \mid g[0]) \mid b[C[A]]) \approx (\widetilde{e_1})((\widetilde{e_2})(N_4 \mid g[0]) \mid b[C[B]])$$

which can be organized as

$$(\widetilde{d})(M \mid g[0] \mid b[C[A]]) \approx (\widetilde{e})(N_4 \mid g[0] \mid b[C[B]])$$

That is,

$$(\widetilde{d})(M \mid b[C[A]]) \approx (\widetilde{e})(N_4 \mid b[C[B]])$$

So we have

$$(\widetilde{d})(M \mid b[C[A]]) \approx (\widetilde{e})(N_4 \mid b[C[B]]) \Longleftarrow (\widetilde{e})(N \mid b[C[B]])$$

Similarly, we have

$$(\widetilde{e})(M \mid b[C[A]]) \Longrightarrow \approx (\widetilde{e})(N \mid b[C[B]])$$

By the bisimulation lemma (Lemma 6), we derive as required

$$(\widetilde{d})(M \mid b[C[A]]) \approx (\widetilde{e})(N \mid b[C[B]]) \tag{5}$$

□

Before going ahead, we prove, as promised, that $\approx$ coincides with $\approx_{\mathrm{dl}}$. We remark that the intuition underlying this coincidence is that HO interactions are somewhat robust. That is, it does not matter if the residual processes are compared after the outgoing process gets into the target

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

context and has interactions in that context. The high control capability of HO processes renders that delay irrelevant, and no extra discriminating strength is lost or gained.

Proposition 8. *The relation* $\approx$ *coincides with the relation* $\approx_{\mathrm{dl}}$.

Proof. We focus on the HO output clause since it is the only difference between $\approx$ and $\approx_{\mathrm{dl}}$. For convenience, we first recall the two clauses. In $\approx$, it is

$\star$ If $P \xrightarrow{(\widetilde{d})\overline{a}b(A)} P'$, then $Q \xRightarrow{(\widetilde{e})\overline{a}b(B)} Q'$, and for every $C \stackrel{\mathrm{def}}{=} b[C']$, it holds that $(\widetilde{d})(P' \mid C[A]) \approx (\widetilde{e})(Q' \mid C[B])$

In $\approx_{\mathrm{dl}}$, it is

$\triangle$ If $P \xrightarrow{(\widetilde{d})\overline{a}b(A)} P'$, then $Q \Longrightarrow \xrightarrow{(\widetilde{e})\overline{a}b(B)} Q'$, and for every $C \stackrel{\mathrm{def}}{=} b[C']$, it holds that $(\widetilde{e})(Q' \mid C[B]) \Longrightarrow \cdot \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid C[A])$

To derive $\triangle$ from $\star$, we see that the weak action $Q \xRightarrow{(\widetilde{e})\overline{a}b(B)} Q'$ can be expanded as $Q \Longrightarrow \xrightarrow{(\widetilde{e})\overline{a}bB} Q'' \Longrightarrow Q'$. Now using Q'' as required by the delayed bisimulation, $\star$ can be rewritten as:

$\star'$ If $P \xrightarrow{(\widetilde{d})\overline{a}b(A)} P'$, then $Q \Longrightarrow \xrightarrow{(\widetilde{e})\overline{a}bB} Q''$, and for every $C \stackrel{\mathrm{def}}{=} b[C']$, it holds that $(\widetilde{e})(Q'' \mid C[B]) \Longrightarrow (\widetilde{e})(Q' \mid C[B]) \approx (\widetilde{d})(P' \mid C[A])$

This is exactly what $\triangle$ calls for.

To derive $\star$ from $\triangle$, we choose a special context $C_1 \stackrel{\mathrm{def}}{=} b[\overline{g}[\cdot]]$ such that g is fresh, that is, not occurring in the processes under consideration. Then we know from $\triangle$ that $(\widetilde{e})(Q' \mid C_1[B]) \Longrightarrow R \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid C_1[A])$ for some R. That is,

$$(\widetilde{e})(Q' \mid b[\overline{g}B]) \Longrightarrow R \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid b[\overline{g}A])$$

Because g is fresh, R must be of the form $(\widetilde{e})(Q'' \mid b[\overline{g}[B]])$ in which $Q' \Longrightarrow Q''$. So we have

$$(\widetilde{e})(Q' \mid b[\overline{g}B]) \Longrightarrow (\widetilde{e})(Q'' \mid b[\overline{g}B]) \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid b[\overline{g}A])$$

In summary, we have $Q \Longrightarrow \xrightarrow{(\widetilde{e})\overline{a}bB} Q' \Longrightarrow Q''$ and

$$(\widetilde{e})(Q'' \mid b[\overline{g}B]) \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid b[\overline{g}A])$$

Now by Lemma 7, we infer for every C' that

$$(\widetilde{e})(Q'' \mid b[C'[B]]) \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid b[C'[A]])$$

Hence we conclude that $\triangle$ can be rewritten as

$\triangle'$ If $P \xrightarrow{(\widetilde{d})\overline{a}b(A)} P'$, then $Q \xRightarrow{(\widetilde{e})\overline{a}bB} Q''$, and for every $C \stackrel{\mathrm{def}}{=} b[C']$, it holds that $(\widetilde{e})(Q'' \mid C[B]) \approx_{\mathrm{dl}} (\widetilde{d})(P' \mid C[A])$

This is exactly what $\star$ stipulates.

The proof is now completed. □

Now we prove that $\approx$ is an equivalence relation. In Fu (2007), the counterpart bisimilarity is declared to be an equivalence without any proof; instead, the parts (e.g., those concerning ambient movement) were assumed to meet the requirement of an equivalence automatically. Notwithstanding this, we will give full discussion to this point, because the proof technique of this kind can be of independent interest, as will become clearer.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Lemma 9. *The relation $\approx$ is an equivalence relation.*

Proof. It is clear that $\approx$ is reflexive and symmetric. Below, we show that it is transitive; that is, $P \approx Q \approx R$ implies $P \approx R$. For this purpose, we make a case analysis in proving that $\mathscr{R} \stackrel{\text{def}}{=} \{(P, R) \mid P \approx Q \approx R\} \cup \approx$ is a bisimulation. Assume $P \mathscr{R} R$. For the sake of readability, we shall attach a tip to the beginning of each case to indicate which clause of the bisimulation is being dealt with. The tips should be self-explanatory; for example, "(in-mov)" means the clause for in-movement. This convention is also used in other proofs of this paper.

- (easy-parts). $P \xrightarrow{\alpha} P'$ in which α is $out\ abc$, $\overline{out}\ abc$, $ab(A)$, τ. These cases are similar. It should be clear that $P \approx Q$ and $P \xrightarrow{\alpha} P'$ imply that $Q \Longrightarrow \stackrel{\widehat{\alpha}}{\longrightarrow} \Longrightarrow Q'$ and $P' \approx Q'$. Then from $Q \approx R$, one has $R \Longrightarrow \Longrightarrow \widehat{\alpha} \Longrightarrow R'$ and $Q' \approx R'$. So we have $P' \approx Q' \approx R$ and thus $P' \mathscr{R} R'$.
- (in-mov). $P \xrightarrow{in\ ab} (\widetilde{d})\langle P_1 \between P_2\rangle$. Since $P \approx Q$, $Q \Longrightarrow \xrightarrow{in\ ab} (\widetilde{e})\langle Q_1 \between Q_2\rangle$ (which noticeably does not have further actions), and for every context $C \stackrel{\text{def}}{=} b[[\cdot] \mid O]$, it holds that

$$(\widetilde{e})(Q_2 \mid C[Q_1]) \Longrightarrow \approx (\widetilde{d})(P_2 \mid C[P_1]) \tag{6}$$

  Because $Q \approx R$, we know that $R \rightarrow R_3 \xrightarrow{in\ ab} (\widetilde{f})\langle R_1 \between R_2\rangle$, and it holds for every context C that

$$(\widetilde{f})(R_2 \mid C[R_1]) \Longrightarrow \approx (\widetilde{e})(Q_2 \mid C[Q_1]) \tag{7}$$

  From (6) and (7), we infer
- (coin-mov). $P \xrightarrow{\overline{in}\ ab} C$. Since $P \approx Q$, $Q \Longrightarrow \xrightarrow{\overline{in}\ ab} C'$ (notice that based on the semantics, a process becomes a context after a *Mov−coin* action and is not able to move until that context is filled in), and for every M, it holds that

$$C'[a[M]] \Longrightarrow \approx C[a[M]] \tag{8}$$

  Because $Q \approx R$, we know that $R \Longrightarrow R_1 \xrightarrow{\overline{in}\ ab} C''$, and for every M, it holds that

$$C''[a[M]] \Longrightarrow \approx C'[a[M]] \tag{9}$$

  From (8) and (9), we infer $C''[a[M]] \Longrightarrow \mathscr{R} C[a[M]]$.
- (out1-mov). $P \xrightarrow{out\ ab} (\widetilde{d})\langle P_1 \between P_2\rangle$. Since $P \approx Q$, $Q \Longrightarrow \xrightarrow{out\ ab} (\widetilde{e})\langle Q_1 \between Q_2\rangle$ (which does not have further actions), and for every context $C \stackrel{\text{def}}{=} c[[\cdot] \mid O]$, it holds that

$$(\widetilde{e})(Q_1 \mid C[Q_2]) \Longrightarrow \approx (\widetilde{d})(P_1 \mid C[P_2]) \tag{10}$$

  Because $Q \approx R$, we know that $R \Longrightarrow R_3 \xrightarrow{out\ ab} (\widetilde{f})\langle R_1 \between R_2\rangle$, and it holds for every context C that

$$(\widetilde{f})(R_1 \mid C[R_2]) \Longrightarrow \approx (\widetilde{e})(Q_1 \mid C[Q_2]) \tag{11}$$

  From (10) and (11), we infer $(\widetilde{f})(R_2 \mid C[R_1]) \Longrightarrow \mathscr{R} (\widetilde{d})(P_2 \mid C[P_1])$.
- (hocom-res-output). $P \xrightarrow{(\widetilde{d})\overline{ab}A} P'$. Since $P \approx Q$, $Q \Longrightarrow Q_1 \xrightarrow{(\widetilde{e})\overline{ab}B} Q_2 \rightarrow Q'$, and for every $C_1 \stackrel{\text{def}}{=} b[C_1']$, it holds that

$$(\widetilde{d})(P' \mid C_1[A]) \approx (\widetilde{e})(Q' \mid C_1[B]) \tag{12}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Because $Q \approx R$, we know that $R \Longrightarrow R_1 \xrightarrow{(\widetilde{f})\overline{a}bB'} R_2$ with $R_1 \approx Q_1$, and for every $C_2 \stackrel{\text{def}}{=} b[C_2']$, it holds that

$$(\widetilde{e})(Q_2 \mid C_2[B]) \approx (\widetilde{f})(R_2 \mid C_2[B'])$$

Now we choose C_2' to be $\overline{g}[\cdot]$ (i.e., $\overline{g}[\cdot].0$) in which g is fresh and have

$$O_1 \stackrel{\text{def}}{=} (\widetilde{e})(Q_2 \mid b[\overline{g}B]) \approx (\widetilde{f})(R_2 \mid b[\overline{g}B']) \stackrel{\text{def}}{=} O_2$$

From $Q_2 \Longrightarrow Q'$, we know

$$O_1 \rightarrow (\widetilde{e})(Q' \mid b[\overline{g}B])$$

This must be matched by

$$O_2 \rightarrow (\widetilde{f})(R' \mid b[\overline{g}B']) \text{ caused by } R_2 \rightarrow R'$$

So we know $R \xrightarrow{(\widetilde{f})\overline{a}bB'} R'$ and

$$(\widetilde{e})(Q' \mid b[\overline{g}B]) \approx (\widetilde{f})(R' \mid b[\overline{g}B']) \tag{13}$$

From (13) and Lemma 7, we infer that for every context $C_3 \stackrel{\text{def}}{=} b[C_3']$, it holds that

$$(\widetilde{e})(Q' \mid C_3[B]) \approx (\widetilde{f})(R' \mid C_3[B']) \tag{14}$$

From (12) and (14), we finally have for every context $C \stackrel{\text{def}}{=} b[C']$ that

$$(\widetilde{d})(P' \mid C[A]) \approx (\widetilde{e})(Q' \mid C[B]) \approx (\widetilde{f})(R' \mid C[B'])$$

Hence we have, as needed

$$(\widetilde{d})(P' \mid C[A])\ \mathscr{R}\ (\widetilde{f})(R' \mid C[B'])$$

□

Remark. *As a matter of fact, the proof method for the cases of HO output, as above, may be generic in HO models (essentially, FAHO is a higher-order model). See also Sangiorgi 1993) and Fu 2005). We stress that when extended to terms, $\approx$ remains an equivalence. To see that this is true about the prefix actions, the case other than action $(\widetilde{d})\overline{a}A$ is similar and simpler; the case of $(\widetilde{d})\overline{a}A$ is similar to that for the HO pi-calculus and can be referred to Sangiorgi and Walker (2001) and Fu (2015).*

It is worth noting that $\sim$ is a congruence by the nature of strong-style bisimulations (Sangiorgi and Walker, 2001). Now we consider the congruence properties of $\approx$. These properties are divided into two parts: one for the closure under replication (Lemma 11) and the other one for the closure under the other operations (Lemma 10). The proof of Lemma 10 is placed in Appendix A.

Lemma 10. *The relation $\approx$ is closed with respect to the operations other than replication.*

Following a somewhat similar approach, we can show that $\approx$ is also closed by replication. We mention in the passing that this closure property actually makes much sense.

Lemma 11. *That $M \approx N$ implies $!M \approx !N$.*

Proof. We define $\mathscr{R}$ as follows and show that it is a bisimulation up-to $\approx$.

$$\mathscr{R} \stackrel{\text{def}}{=} \{(C[!M], C[!N]) \mid M \approx N \text{ and } C \text{ is a context}\}$$

Assume $C[!M]\mathscr{R}C[!N]$ and $C[!M] \xrightarrow{\lambda} M'$. There are several situations.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

1. The action results from the context C alone. This is a simple situation since the different parts, that is, $!M$ and $!N$, are not involved.
2. The action results from $!M$ and thus M(s) alone (intuitively some constituent M within $!M$). This can be handled by resorting to $M \approx N$ and its congruence properties (Lemma 10).
3. The action results from the entanglement (e.g., interaction) between $!M$ (intuitively some M that composes $!M$) and C. This case is based on the previous two and can be coped with in a way similar to that in Lemma 10.

So below, we focus on the second situation by case analysis (essentially of the structure of M). We take the in-movement case as the representative, for the other cases are similar. In such a case, C cannot be of the form $f[[\cdot]]$ or any form with a hole beneath an ambient. So we assume, in general, that C is of the form $(\widetilde{f})([\cdot] \mid L)$. Assume $C[!M] \xrightarrow{in\ ab} M'$, and this action stems from $!M$ and successively from M, as illustrated below.

$$\dfrac{\dfrac{\dfrac{\vdots}{M \xrightarrow{in\ ab} (\widetilde{d})\langle M_1 \between M_2\rangle \stackrel{\text{def}}{=} D_1}}{!M \xrightarrow{in\ ab} D_1 \mid !M \equiv (\widetilde{d})\langle M_1 \between M_2 \mid !M\rangle \stackrel{\text{def}}{=} D_2}}{C[!M] \xrightarrow{in\ ab} M' \equiv (\widetilde{f}\widetilde{d})\langle M_1 \between M_2 \mid !M \mid L\rangle \stackrel{\text{def}}{=} D_3}$$

Since $M \approx N$, we have the following match-up.

$$\dfrac{\dfrac{\dfrac{\vdots}{N \Longrightarrow \xrightarrow{in\ ab} (\widetilde{e})\langle N_1 \between N_2\rangle \stackrel{\text{def}}{=} D_1'}}{!N \Longrightarrow \xrightarrow{in\ ab} D_1' \mid !N \equiv (\widetilde{e})\langle N_1 \between N_2 \mid !N\rangle \stackrel{\text{def}}{=} D_2'}}{C[!N] \Longrightarrow \xrightarrow{in\ ab} N' \equiv (\widetilde{f}\widetilde{e})\langle N_1 \between N_2 \mid !N \mid L\rangle \stackrel{\text{def}}{=} D_3'}$$

Noticing that for every context $C_1 \stackrel{\text{def}}{=} b[[\cdot] \mid O]$, it holds for some L' that

$$(\widetilde{e})(N_2 \mid C_1[N_1]) \rightarrow L' \approx (\widetilde{d})(M_2 \mid C_1[M_1])$$

we have, as expected,

$$\begin{aligned}
(\widetilde{f}\widetilde{e})(N_2 \mid !N \mid L \mid C_1[N_1]) \Longrightarrow &\equiv (\widetilde{f})(!N \mid L \mid L') \\
&\approx (\widetilde{f}\widetilde{d})(M_2 \mid !N \mid L \mid C_1[M_1]) \qquad \text{by Lemma 10} \\
&\equiv C'[!N] \qquad \text{in which } C' \stackrel{\text{def}}{=} (\widetilde{f}\widetilde{d})(M_2 \mid [\cdot] \mid L \mid C_1[M_1]) \\
&\mathscr{R}\ C'[!M] \\
&\equiv (\widetilde{f}\widetilde{d})(M_2 \mid !M \mid L \mid C_1[M_1])
\end{aligned}$$

□

We are now in a good position to state the following theorem.

Theorem. *The relation $\approx$ is a congruence.*

Proof. By Lemma 9, Lemma 10, and Lemma 11. □

Remark. *We remark on several more points before ending this section.*

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

- *Proving Proposition 11 can be potentially rendered simpler using a more versatile up-to technique. That is, showing that the relation* $\mathscr{R}' \stackrel{\text{def}}{=} \{(!M, !N) \mid M \approx N\}$ *is a bisimulation up-to context and* $\approx$*; see Sangiorgi and Walker (2001) for more information on this technique.*
- *Intuitively but informally, the closure of* $\approx$ *under replication can be thought of as follows. Imagining* $!M$ *as an infinite composition of* M *(we do not have such an operation in the calculus, but it makes no difference here), that is,* $M \mid M \mid \cdots \mid M \mid \cdots$*, one can come up with some "induction"'on the size of such a composition. In other words, initially* $M \approx N$*, and assuming* $\underbrace{M \mid \cdots \mid M}_{k} \approx \underbrace{N \mid \cdots \mid N}_{k}$ *leads apparently to* $\underbrace{M \mid \cdots \mid M}_{k} \mid M \approx \underbrace{N \mid \cdots \mid N}_{k} \mid N$ *with the help of Lemma 10. Although this argument succumbs to rigor, it pins down the intuition and essence of the closure property of* $\approx$ *with regard to replication.*
- *Notice that* $a[M] \approx a[N]$ *does not imply* $M \approx N$*. Take the example* $a[b[in\, c]] \approx a[0]$ *but* $b[in\, c] \not\approx 0$*. The reason is that an ambient may bury something (deep) inside that otherwise is observable.*

4. Observational equivalences

In this section, we study the bisimulation from an observational angle, that is, the barbed bisimulation. The concept of barbed bisimulation in ambient-like calculi is somewhat different from that of traditional process calculi like the pi-calculus. That is, roughly speaking, the barbs are defined over (static) ambient names rather than action labels (Cardelli and Gordon, 2000; Sangiorgi and Walker, 2001). In this work, we stick to the traditional approach and define barbs based on actions (Sangiorgi and Walker, 2001; Fu, 2007).

Definition 12 (Barbs). *A process* P *is strongly observable for* α *(or has a barb in terms of* α*), written* $P \downarrow_\alpha$*, if* $P \xrightarrow{\alpha}$*. It is (weakly) observable for* α *(or has a weak barb in terms of* α*), written* $P \Downarrow_\alpha$*, if* $P \Longrightarrow \xrightarrow{\alpha}$*.*

Definition 13 (Barbed bisimulation/congruence). *A symmetric binary relation* $\mathscr{R}$ *is a barbed bisimulation if whenever* $P \mathscr{R} Q$*, the following properties hold:*

- *if* $P \downarrow_\alpha$*, then* $Q \Downarrow_\alpha$*;*
- *if* $P \xrightarrow{\tau} P'$*, then* $Q \rightarrow Q'$ *and* $P' \mathscr{R} Q'$*.*

We denote by $\dot{\approx}$ *the union of all barbed bisimulations, namely the largest barbed bisimulation, which is called the barbed bisimilarity. Process* P *and* Q *are barbed congruent, written* $P \simeq Q$*, if* $C[P] \;\dot{\approx}\; C[Q]$ *for all contexts* C*.*

From the definition, it is not hard to see that both $\dot{\approx}$ and $\simeq$ are equivalence relations. It is also direct to see that $\simeq$ is the largest congruence induced by $\dot{\approx}$.

Proposition 14. *Relation* $\simeq$ *is the largest congruence induced by* $\dot{\approx}$*.*

We note that $h.O$ stands for $h(X).O$ where X does not appear in O, and $\overline{h}.O$ for $\overline{h}0.O$. Sometimes we omit the trailing 0 in expressions.

Now we present the main theorem of this section.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Theorem. (Coincidence between the barbed congruence and bisimilarity). *On FAHO processes, barbed congruence coincides with bisimilarity. That is,* $\simeq = \approx$.

Proof. The inclusion $\approx \subseteq \simeq$ is not hard, by appealing to the fact that $\approx$ is a congruence. The opposite inclusion is the difficult part. In order to prove this, we show that the following relation $\mathscr{R}$ is a delayed bisimulation:

$$\mathscr{R} \stackrel{\text{def}}{=} \{(P, Q) \mid P \simeq Q\} \cup \approx_{\text{dl}}$$

Since the delayed bisimilarity coincides with bisimilarity (Proposition 8), the result of this theorem follows.

Before going further, we provide some intuition. The crux of the inclusion is that if two barbed congruent processes are not bisimilar, then they must be distinguishable after some finite steps of action matching. That is the moment the closure under contexts comes into play; that is, one can exploit some specific context to tell the two processes apart (sooner or later). One tricky part is that the bisimulation clauses are of HO nature, making the arguments much more intricate.

We expand the arguments with case analysis, focusing on processes.

- (in-mov). If $P \xrightarrow{in\,ab} (\widetilde{d})\langle P_1 \between P_2\rangle$, then for any process O and fresh name h, let C be the following context:

  $$[\cdot] \mid b[\overline{in}\, a.\overline{out}\, hh.O] \mid h[h[out\, b]]$$

  The reductions

  $$\begin{aligned} C[P] &\xrightarrow{\tau} (\widetilde{d})(P_2 \mid b[P_1 \mid \overline{out}\, hh.O]) \mid h[h[out\, b]] \\ &\xrightarrow{\tau} (\widetilde{d})(P_2 \mid b[P_1 \mid O]) \mid h[0] \mid h[0] \stackrel{\text{def}}{=} P'' \\ &\simeq (\widetilde{d})(P_2 \mid b[P_1 \mid O]) \stackrel{\text{def}}{=} P' \end{aligned}$$

  must be matched by the following sequence:

  $$\begin{aligned} C[Q] &\Longrightarrow C[Q'] \\ &\xrightarrow{\tau} (\widetilde{e})(Q_2 \mid b[Q_1 \mid \overline{out}\, hh.O]) \mid h[h[out\, b]] \\ &\xrightarrow{\tau} (\widetilde{e})(Q_2 \mid b[Q_1 \mid O]) \mid h[0] \mid h[0] \\ &\Longrightarrow Q'' \mid h[0] \mid h[0] \simeq Q'' \\ &\simeq P'' \simeq P' \end{aligned}$$

  From the matching sequence, it is clear to see that $Q \Longrightarrow \xrightarrow{in\,ab} (\widetilde{e})\langle Q_1 \between Q_2\rangle$, and

  $$(\widetilde{e})(Q_2 \mid b[Q_1 \mid O]) \Longrightarrow Q'' \simeq P'' \simeq P' \equiv (\widetilde{d})(P_2 \mid b[P_1 \mid O])$$

  That is,

  $$(\widetilde{e})(Q_2 \mid b[Q_1 \mid O]) \Longrightarrow \mathscr{R}^{-1}\, (\widetilde{d})(P_2 \mid b[P_1 \mid O])$$

- (coin-mov). If $P \xrightarrow{\overline{in}\, ab} C_1$, define context C as below for process N and fresh name h:

  $$[\cdot] \mid a[in\, b.(N \mid out\, h)]$$

  Then

  $$C[P] \xrightarrow{\tau} C_1[a[N \mid out\, h]] \stackrel{\text{def}}{=} T_1$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

We note that C_1 is of the form $(\widetilde{d})(b[[\cdot] \mid N_1] \mid P_1)$ by Lemma 2. Since h is fresh and *out bah* is observable, the action above must be matched by

$$\begin{aligned} C[Q] &\Longrightarrow C[Q_1] \\ &\xrightarrow{\tau} C_2[a[N \mid out\ h]] \\ &\Longrightarrow C_3[out\ h] \simeq T_1 \end{aligned}$$

from which we can see $Q \Longrightarrow \xrightarrow{\overline{in}\ ab} C_2$. Due to the freshness of h, we can restrict h and have

$$C_3[0] \simeq (h)C_3[out\ h] \simeq (h)T_1 \simeq C_1[a[N]]$$

Hence

$$\begin{aligned} C_2[a[N]] &\Longrightarrow C_3[0] \simeq C_1[a[N]] \\ \text{i.e., } C_2[a[N]] &\Longrightarrow \mathscr{R}^{-1}\ C_1[a[N]] \end{aligned}$$

- (out1-mov). If $P \xrightarrow{out\ ab} (\widetilde{d})\langle P_1 \between P_2\rangle$, let C be the context as follows in which f is fresh:

$$c[[\cdot] \mid \overline{out}\ bf.O] \mid b[\overline{out}\ ca.f[out\ c]]$$

Then

$$\begin{aligned} C[P] &\xrightarrow{\tau} (\widetilde{d})(P_1 \mid c[P_2 \mid \overline{out}\ bf.O]) \mid b[f[out\ c]] \\ &\xrightarrow{\tau} (\widetilde{d})(P_1 \mid c[P_2 \mid O]) \mid b[0] \mid f[0] \stackrel{\text{def}}{=} P'' \\ &\simeq (\widetilde{d})(P_1 \mid c[P_2 \mid O]) \stackrel{\text{def}}{=} P' \end{aligned}$$

The simulation of the above reduction sequence can be represented as follows:

$$\begin{aligned} C[Q] &\Longrightarrow C[Q'] \\ &\xrightarrow{\tau} (\widetilde{e})(Q_1 \mid c[Q_2 \mid \overline{out}\ bf.O]) \mid b[f[out\ c]] \\ &\xrightarrow{\tau} (\widetilde{e})(Q_1 \mid c[Q_2 \mid O]) \mid b[0] \mid f[0] \\ &\Longrightarrow Q'' \mid b[0] \mid f[0] \simeq Q'' \\ &\simeq P'' \simeq P' \end{aligned}$$

It then implies that $Q \Longrightarrow \xrightarrow{out\ ab} (\widetilde{e})\langle Q_1 \between Q_2\rangle$ and

$$(\widetilde{e})(Q_1 \mid c[Q_2 \mid O]) \Longrightarrow Q'' \simeq P'' \simeq P' \equiv (\widetilde{d})(P_1 \mid c[P_2 \mid O])$$

That is,

$$(\widetilde{e})(Q_1 \mid c[Q_2 \mid O]) \Longrightarrow \mathscr{R}^{-1}\ (\widetilde{d})(P_1 \mid c[P_2 \mid O])$$

- (out2-mov). If $P \xrightarrow{out\ abc} P'$, let C be the following context for fresh e:

$$[\cdot] \mid c[\overline{out}\ ab.in\ e] \mid e[\overline{in}\ c]$$

Then

$$\begin{aligned} C[P] &\xrightarrow{\tau} P' \mid c[in\ e] \mid e[\overline{in}\ c] \\ &\xrightarrow{\tau} P' \mid c[0] \mid e[0] \stackrel{\text{def}}{=} P'' \\ &\simeq P' \end{aligned}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

The simulation must be

$$\begin{aligned} C[Q] &\Longrightarrow C[Q_1] \\ &\xrightarrow{\tau} Q' \mid c[in\ e] \mid e[\overline{in}\ c] \\ &\xrightarrow{\tau} Q' \mid c[0] \mid e[0] \\ &\Longrightarrow Q'' \mid c[0] \mid e[0] \simeq Q'' \\ &\simeq P'' \simeq P' \end{aligned}$$

So $Q \xRightarrow{out\ abc} Q''$ and $P' \simeq Q''$, i.e., $P' \mathscr{R} Q''$.

- (coout-mov). If $P \xrightarrow{\overline{out}\ abc} P'$, let C be the following context for fresh e:

$$[\cdot] \mid a[b[out\ c.in\ e]] \mid e[\overline{in}\ b]$$

Then

$$\begin{aligned} C[P] &\xrightarrow{\tau} P' \mid a[0] \mid b[in\ e] \mid e[\overline{in}\ b] \\ &\xrightarrow{\tau} P' \mid a[0] \mid b[0] \mid e[0] \stackrel{\text{def}}{=} P'' \\ &\simeq P' \end{aligned}$$

The simulation must be

$$\begin{aligned} C[Q] &\Longrightarrow C[Q_1] \\ &\xrightarrow{\tau} Q' \mid a[0] \mid b[in\ e] \mid e[\overline{in}\ b] \\ &\xrightarrow{\tau} Q' \mid a[0] \mid b[0] \mid e[0] \\ &\Longrightarrow Q'' \mid a[0] \mid b[0] \mid e[0] \simeq Q'' \\ &\simeq P'' \simeq P' \end{aligned}$$

Thus, $Q \xRightarrow{\overline{out}\ abc} Q''$ and $P' \simeq Q''$, that is, $P' \mathscr{R} Q''$.

- (hocom-input). If $P \xrightarrow{ab(A)} P'$, we define context C for fresh d, e as below:

$$[\cdot] \mid b[\overline{a}A.\overline{out}\ de] \mid d[e[out\ b]]$$

Then

$$\begin{aligned} C[P] &\xrightarrow{\tau} P' \mid b[\overline{out}\ de] \mid d[e[out\ b]] \\ &\xrightarrow{\tau} P' \mid b[0] \mid d[0] \mid e[0] \stackrel{\text{def}}{=} P'' \\ &\simeq P' \end{aligned}$$

The simulation must be

$$\begin{aligned} C[Q] &\Longrightarrow C[Q_1] \\ &\xrightarrow{\tau} Q' \mid b[\overline{out}\ de] \mid d[e[out\ b]] \\ &\xrightarrow{\tau} Q' \mid b[0] \mid d[0] \mid e[0] \\ &\Longrightarrow Q'' \mid b[0] \mid d[0] \mid e[0] \simeq Q'' \\ &\simeq P'' \simeq P' \end{aligned}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Thus, $Q \xRightarrow{ab(A)} Q''$ and $P' \simeq Q''$, that is, $P' \mathscr{R} Q''$.

- (hocom-res-output). If $P \xrightarrow{(\widetilde{d})\overline{ab}(A)} P'$, we define context C (capture-free) for fresh d, e as below:

$$[\cdot] \mid b[a(X).(\overline{out}\ de.C'[X])] \mid d[e[out\ b]]$$

Then

$$\begin{aligned} C[P] &\xrightarrow{\tau} (\widetilde{d})(P' \mid b[\overline{out}\ de.C'[A]] \mid d[e[out\ b]]) \\ &\xrightarrow{\tau} (\widetilde{d})(P' \mid b[C'[A]] \mid d[0] \mid e[0]) \stackrel{\text{def}}{=} P'' \\ &\simeq (\widetilde{d})(P' \mid b[C'[A]]) \end{aligned}$$

The simulation must be

$$\begin{aligned} C[Q] &\Longrightarrow C[Q_1] \\ &\xrightarrow{\tau} (\widetilde{e})(Q' \mid b[\overline{out}\ de.C'[B]] \mid d[e[out\ b]]) \\ &\Longrightarrow (\widetilde{e})(Q'' \mid b[\overline{out}\ de.C'[B]] \mid d[e[out\ b]]) \qquad \text{in which } Q' \Longrightarrow Q'' \\ &\xrightarrow{\tau} (\widetilde{e})(Q'' \mid b[C'[B]] \mid d[0] \mid e[0]) \simeq (\widetilde{e})(Q'' \mid b[C'[B]]) \\ &\Longrightarrow R \simeq P'' \simeq (\widetilde{d})(P' \mid b[C'[A]]) \end{aligned}$$

Thus, we know from the simulation sequence that $Q \Longrightarrow Q_1 \xrightarrow{(\widetilde{e})\overline{ab}(B)} Q'$ and

$$(\widetilde{e})(Q' \mid b[C'[B]]) \Longrightarrow (\widetilde{e})(Q'' \mid b[C'[B]]) \Longrightarrow \simeq R \simeq (\widetilde{d})(P' \mid b[C'[A]])$$

In summary, we have $Q \Longrightarrow \xrightarrow{(\widetilde{e})\overline{ab}(B)} Q'$ and, moreover, as required (by the delayed bisimulation)

$$(\widetilde{e})(Q' \mid b[C'[B]]) \Longrightarrow \simeq (\widetilde{d})(P' \mid b[C'[A]])$$

that is,

$$(\widetilde{e})(Q' \mid b[C'[B]]) \Longrightarrow \mathscr{R}\, (\widetilde{d})(P' \mid b[C'[A]])$$

- (interaction). This is straightforward since $\approx$ and $\simeq$ share the clause in their definitions. □

5. Expressiveness

In this section, we examine the expressiveness of FAHO. We demonstrate that it can encode the minimal HO pi-calculus (Sangiorgi, 1993, 1996a,b). Since the latter is computationally complete (Lanese et al., 2011), that is, Turing complete, so is FAHO.

5.1 Calculus Π^m

We define Π^m, the basic (minimal) HO pi-calculus (or HOcore as named in the literature (Lanese et al., 2011)).

5.1.1 Syntax

We use $P, Q, R, A, B \ldots$ to range over Π^m processes, $a, b, c \ldots$ to range over names (i.e., channels), and $X, Y, Z \ldots$ to range over (process) variables. The syntax of Π^m is the following:

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

$$
\begin{array}{rll}
P, Q ::= & a(X).P & \text{input prefix} \\
\mid & \overline{a}Q.P & \text{output} \\
\mid & X & \text{process variable} \\
\mid & P \mid Q & \text{parallel composition} \\
\mid & 0 & \text{nil}
\end{array}
$$

The operators have their standard meaning (Sangiorgi, 1993; Lanese et al., 2011). An output $\overline{a}Q.P$ emits Q and continues as P. An input $a(X).P$ binds in P the free occurrences of the process variable X, which is to be instantiated by an inputted concrete process. A process variable is free otherwise. A process is closed if it has no free variables. By default, we consider closed processes. We denote by $\widetilde{\cdot}$ a tuple of objects (names, processes, and variables). Operations $\text{fpv}(\widetilde{P})$ and $\text{bpv}(\widetilde{P})$ return the free variables and bound variables in $\widetilde{P}$, respectively. A name or variable is fresh if it does not occur in the processes under examination. We write $P\{Q/X\}$ to denote the substitution of variable X with process Q. This can accordingly be generalized to the simultaneous substitution of tuples $P\{\widetilde{Q}/\widetilde{X}\}$. As usual, we often trim the trailing nil processes and have the following shortcuts of Calculus of Communicating Systems (CCS)-like (Milner 1989) processes: $a.P \stackrel{\text{def}}{=} a(X).P$ where $X \notin \text{fpv(P)}$, $a \stackrel{\text{def}}{=} a.0$, and $\overline{a} \stackrel{\text{def}}{=} \overline{a}0.0$. We note that in Π^m, one can define a loose concept of replication (since there is no restriction operation): $!P \stackrel{\text{def}}{=} \overline{c}Q_c \mid Q_c, \quad Q_c \stackrel{\text{def}}{=} c(X).(\overline{c}X \mid X \mid P)$.

5.1.2 Semantics

We now represent the LTS defined upon closed processes. The symmetric rules are skipped.

$$
(Prefix{-}Input)\ \frac{}{a(X).P \xrightarrow{a(A)} P\{A/X\}} \qquad (Prefix{-}Output)\ \frac{}{\overline{a}A.P \xrightarrow{\overline{a}A} P}
$$

$$
(Comp{-}Act)\ \frac{P \xrightarrow{\lambda} P'}{P \mid Q \xrightarrow{\lambda} P' \mid Q} \qquad (Comp{-}Tau)\ \frac{P \xrightarrow{a(A)} P' \qquad Q \xrightarrow{\overline{a}A} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'}
$$

There are three forms of actions (ranged over by α, β, λ): (1) Input action $P \xrightarrow{a(A)} P'$: P receives over a a process A that replaces X in the continuation P'. (2) Output action $P \xrightarrow{\overline{a}A} P'$: P transmits A over a and evolves to P'. For the sake of clarity, we sometimes write an output as $\overline{a}(A)$ or $\overline{a}[A]$. (3) Internal action $P \xrightarrow{\tau} P'$: the parallel components of P engage an interaction as regulated by the rule *Comp-Tau*.

The structural congruence relation is the smallest congruence generated by the following laws in addition to α-convertibility of the input-bound variables (i.e., $a(X).P \equiv a(Y).P\{Y/X\}$, in which Y is fresh):

$$
P \mid 0 \equiv P, \quad P_1 \mid P_2 \equiv P_2 \mid P_1, \quad P_1 \mid (P_2 \mid P_3) \equiv (P_1 \mid P_2) \mid P_3.
$$

By a simple induction on the rules of the structural congruence, one can derive the follow-up property concerning the synergy between the LTS and the structural congruence.

Lemma 15. *If $P \xrightarrow{\lambda} P'$ and $P \equiv Q$, then $Q \xrightarrow{\lambda} Q'$ for some Q' s.t. $P' \equiv Q'$.*

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

5.1.3 Context bisimulation

In Π^m, we have the standard behavioral equivalence, named context bisimilarity (Sangiorgi, 1993, Sangiorgi 1996). To facilitate the definition, we define the notation $E[X]$, meaning that process E has possibly the free occurrence of variable X, that is, fpv(E) $\subseteq \{X\}$, and accordingly $E[A]$, meaning $E\{A/X\}$.

Definition 16 (Context Bisimulation). *A binary relation $\mathscr{R}$ on closed Π^m processes is a context bisimulation if it satisfies the following properties whenever $P\,\mathscr{R}\,Q$:*

1. *(τ-bisimulation) If $P \xrightarrow{\tau} P'$, then $Q \Longrightarrow Q'$ for some Q' and $P'\,\mathscr{R}\,Q'$.*
2. *(input bisimulation) If $P \xrightarrow{a(A)} P'$, then $Q \xRightarrow{a(A)} Q'$ for some Q' and $P'\,\mathscr{R}\,Q'$.*
3. *(output bisimulation) If $P \xrightarrow{\overline{a}(A)} P'$, then $Q \xRightarrow{\overline{a}(B)} Q'$ for some B and Q', and for all $E[X]$, it holds that $E[A] \mid P'\ \mathscr{R}\ E[B] \mid Q'$.*

The context bisimilarity, written $\approx_{ct}$, is the union of all context bisimulations (viz., the largest one).

We denote by $\sim_{ct}$ the strong context bisimilarity in Π^m. The context bisimilarity can be extended to open processes in the standard manner: assume fpv(P,Q) $= \widetilde{X}$, then $P \approx_{ct} Q$ if and only if $P\{\widetilde{A}/\widetilde{X}\} \approx_{ct} Q\{\widetilde{A}/\widetilde{X}\}$ for all closed $\widetilde{A}$. As is well-known (Sangiorgi, 1993; Sangiorgi and Walker, 2001; Lanese et al., 2011; Lanese et al., 2011), $\approx_{ct}$ is a congruence relation.

5.2 Calculus $\Pi^m_{\mathbb{N}}$

Calculus $\Pi^m_{\mathbb{N}}$ is a parameterized variant of Π^m, in which all the names used in the processes are taken from $\mathbb{N}$, a set of names. This makes sense because we do not have the restriction operator. It is not hard to see that $\Pi^m_{\mathbb{N}}$ is also computationally complete. Actually, for $\mathbb{N}$, being finite is sufficient to attain computational completeness since in Π^m, only a finite set of names are needed to achieve such completeness (Lanese et al., 2011). Concerning expressiveness, we stress the following points before going ahead:

(1) Our main goal is to establish Turing completeness. Since the encoding in Lanese et al. (2011) only employs finitely many names to encode Minsky machines, the encoding here suffices to show the completeness.

(2) One can set $\mathbb{N}$ large enough to serve specific requirements, so the utility of the calculus is maintained at large.

(3) From a certain viewpoint, $\mathbb{N}$ can be deemed as the set of real names (verified and trusted). This corresponds well with the design idea of *FAHO*.

5.3 The encoding

The encoding borrows an idea from Fu (2007). However, since we use strict real-identity movement capabilities, the encoding strategy of Fu (2007) cannot be directly used here. We have to be more specific about the names. Consequently, we make sure to know the top-level names of the subprocess P, so as to impose out-movement from outside the surrounding ambient. In addition, we are frugal in using new names. The encoding is presented in Figure 2.

We give an example before explaining the encoding more carefully.

$$\begin{aligned}
[\![\overline{u}A.P \mid u(X).Q]\!] &\stackrel{\text{def}}{=} [\![\overline{u}A.P]\!] \mid [\![u(X).Q]\!] \\
&\equiv (\nu)(u[\overline{u}[\![A]\!]_\nu.[\![P]\!]_\nu] \mid \mathscr{E}) \mid (\nu)(u[u(X).[\![Q]\!]_\nu] \mid \mathscr{E}) \\
&\xrightarrow{\tau} (\nu)(u[[\![P]\!]_\nu] \mid \mathscr{E}) \mid (\nu)(u[[\![Q]\!]_\nu\{[\![A]\!]_\nu/X\}] \mid \mathscr{E})
\end{aligned}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

$$
\begin{array}{ll}
[\![0]\!] & \stackrel{\text{def}}{=} 0 \\
[\![X]\!] & \stackrel{\text{def}}{=} X \\
[\![P \mid P']\!] & \stackrel{\text{def}}{=} [\![P]\!] \mid [\![P']\!] \\
[\![\overline{u}A.P]\!] & \stackrel{\text{def}}{=} (\nu)(u[\overline{u}[\![A]\!]_\nu.[\![P]\!]_\nu] \mid \mathscr{E}) \\
[\![u(X).P]\!] & \stackrel{\text{def}}{=} (\nu)(u[u(X).[\![P]\!]_\nu] \mid \mathscr{E}) \\
\mathscr{E} & \stackrel{\text{def}}{=} \prod_{h\in\mathbb{N}\cup\{\nu\}} \nu[!\overline{out}\ uh.0]
\end{array}
$$

$$
\begin{array}{ll}
[\![0]\!]_\nu & \stackrel{\text{def}}{=} 0 \\
[\![X]\!]_\nu & \stackrel{\text{def}}{=} X \\
[\![P \mid P']\!]_\nu & \stackrel{\text{def}}{=} [\![P]\!]_\nu \mid [\![P']\!]_\nu \\
[\![\overline{u}A.P]\!]_\nu & \stackrel{\text{def}}{=} u[out\ \nu.\overline{u}[\![A]\!]_\nu.[\![P]\!]_\nu] \mid \mathscr{E}' \\
[\![u(X).P]\!]_\nu & \stackrel{\text{def}}{=} u[out\ \nu.u(X).[\![P]\!]_\nu] \mid \mathscr{E}' \\
\mathscr{E}' & \stackrel{\text{def}}{=} \prod_{h\in\mathbb{N}\cup\{\nu\}} \nu[out\ \nu.!\overline{out}\ uh.0]
\end{array}
$$

Figure 2. Encoding from $\Pi^m_{\mathbb{N}}$ to FAHO.

$$
\begin{aligned}
&\approx [\![P]\!] \mid (\nu)(u[0] \mid \mathscr{E}) \mid [\![Q\{A/X\}]\!] \mid (\nu)(u[0] \mid \mathscr{E}) \\
&\equiv [\![P]\!] \mid [\![Q\{A/X\}]\!] \mid (\nu)(u[0] \mid \mathscr{E}) \mid (\nu)(u[0] \mid \mathscr{E}) \\
&\equiv [\![P \mid Q\{A/X\}]\!] \mid (\nu)(u[0] \mid \mathscr{E}) \mid (\nu)(u[0] \mid \mathscr{E}) \\
&\approx [\![P \mid Q\{A/X\}]\!]
\end{aligned}
$$

In the example, the first $\approx$ is entailed by Lemma 18 and Lemma 22 to be proven shortly.

The core idea of the encoding is to interpret the HO input/output of $\Pi^m_{\mathbb{N}}$ as the same input/output within a surrounding ambient possessing the same name. So the original communication can be modeled as an ambient (HO) communication. The tricky part is to rearrange the process resulting from the communication, in order to regain the process form corresponding to the original $\Pi^m_{\mathbb{N}}$ process. To this point, we make up the apparatus $\mathscr{E}, \mathscr{E}'$, to be explained shortly. The notation $\prod_{h\in H} P_h$ abbreviates $P_{h_1} \mid P_{h_2} \mid \cdots \mid P_{h_k}$, where $H = \{h_1, h_2, \ldots, h_k\}$ is a set of names and P_{h_k} is a process containing free occurrence of h_k. Typically for the encoding's purpose, we can set H to be $\mathbb{N} \cup \{\nu\}$.

The $\mathscr{E}$ and $\mathscr{E}'$, which we call $\mathscr{E}$-blocks, play the role of getting the subprocess (e.g., P) encoding out of its surrounding ambients created by its main process (e.g., $u(X).P$), so to keep the consistency of the encoding. The special name ν ($\nu \notin \mathbb{N}$) acts as a porter; that is, it is responsible for assisting the (outer-level) $\mathscr{E}$-block to pull out the encoding of the subprocess beneath prefixes, together with its (inner-level) accompanying $\mathscr{E}$-blocks. We note that ν is shared by all processes, so it is a sole and thus very busy porter; by contrast, Fu (2007) uses possibly infinitely many such names. There may be some of them intertwined because each prefix is associated with an $\mathscr{E}$-block, and some $\mathscr{E}$-blocks help move out a subprocess coupled with another prefix, but no harm is done on the whole. That is, an encoding process can use its own repository of $\mathscr{E}$-block or those available and applicable in the system. This works since it is the very aim of the (industrial) porter to fetch out the sub-encoding once there is any. Moreover, it does not result in divergence (i.e., infinite internal action sequence). An alternative is certainly to set up separate ν for each prefix, which also entails an effective encoding, except that it may involve considerably many local names. We use a frugal way here, hopefully making the encoding more readable.

The wildcard name h stands for ν or any of the top-level names of P, which can be computed efficiently. To this end, apart from ν as explained above, we set h to include the finite name set $\mathbb{N}$,

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

so to ensure that both the subprocesses in the current setting and those (to be) received from the environment can be moved out correctly. Here one can see that $\mathbb{N}$ is necessary because we only permit real-name out-movement, so the registered names are set beforehand in $\mathbb{N}$. To be more specific, if P has some input A, then $[\![A]\!]$ will go to the surrounding ambient in $[\![P]\!]$ and thus has to be drawn out; however, A can be arbitrary and contain any name it suits, and hence, we demand that the (free) names of A (so $[\![A]\!]$ as well) must be real-name registered, that is, in the set $\mathbb{N}$. In this way, we know (the upper bound of) which ambients can be allowed to move out.

5.3.1 Properties of the encoding

In this section, we demonstrate the full abstraction property of the encoding. A simple observation is that the encoding is structural (or compositional) (Sangiorgi and Walker, 2001); that is, the encoding is defined structurally over the syntax of the $\Pi^m_{\mathbb{N}}$ processes. Also, we have another immediate property as follows.

Lemma 17. *Assume P is a closed $\Pi^m_{\mathbb{N}}$ process. Then $[\![P]\!]$ is a closed FAHO process.*

The encoding also preserves substitutions. The proof is a routine induction.

Lemma 18. *Assume P is a closed $\Pi^m_{\mathbb{N}}$ process. Then $[\![P\{A/X\}]\!]_v \equiv [\![P]\!]_v\{[\![A]\!]_v/X\}$. Moreover, we have $[\![P\{A/X\}]\!] \equiv [\![P]\!]\{[\![A]\!]/X\}$ if A appears top level (i.e., not beneath any prefix), and $[\![P\{A/X\}]\!] \equiv [\![P]\!]\{[\![A]\!]_v/X\}$ otherwise.*

The compositionality of the encoding ascertains that one can extract a subprocess and run it through the encoding separately relative to the main process, and a context of $\Pi^m_{\mathbb{N}}$ can be translated into a context of *FAHO*. This would be important when discussing the soundness and completeness of the encoding since the bisimulation requires the universality of contexts in some clauses.

5.3.1.1 Operational correspondence. The operational correspondence is a prerequisite for the full abstraction. For technical reasons, we need the notion of expansion, a preorder relation. Intuitively, Q expands P, notation $P \preccurlyeq Q$, if P and Q are bisimilar, and moreover, Q has no less internal actions while simulating P. Expansion was initially proposed to fix the problem of up-to proof technique concerning weak bisimulations (Sangiorgi and Walker, 2001). It then became a research branch in its own right. Here we use the up-to expansion technique to establish the soundness of the encoding. We note that the reason why we need the up-to expansion proof technique in establishing the soundness is that the encoding of a process usually brings about extra internal actions, so we have to leverage the weak bisimulation to obtain the operational correspondence. This will basically put us in a situation where the up-to weak bisimulation applies while proving the soundness, which does not generally work. Hence we are forced to specify the operational correspondence more delicately by means of the expansion and then use the up-to expansion technique to come by the bisimulation equivalence and, in turn, the soundness of the encoding.

Below, we define the expansion in *FAHO*, and it should be clear that it indeed refines bisimilarity. We will not discuss the expansion relation further because it is not necessary for the results here and most of its properties are nearly standard. Interested readers are referred to Sangiorgi and Walker (2001) and Sangiorgi and Rutten (2012) for a good summary of the techniques on expansion. To define the expansion relation, we need the notation $\stackrel{\widehat{\alpha}}{\rightarrow}$.

$$P \stackrel{\widehat{\alpha}}{\rightarrow} P' \quad \text{denotes} \quad \begin{cases} P \stackrel{\alpha}{\rightarrow} P' & \text{if } \alpha \text{ is not } \tau \\ P \stackrel{\tau}{\rightarrow} P' \text{ or } P \text{ is } P' & \text{if } \alpha \text{ is } \tau \end{cases}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Definition 19. *A relation $\mathscr{R}$ on FAHO processes is an expansion, if whenever $P\mathscr{R}Q$ the following properties hold:*

- *If $P \xrightarrow{\alpha} M$ and α is not τ, then Q simulates P in the same way as those for $\approx$ (Definition 3).*
- *If $P \xrightarrow{\tau} P'$, then $Q \stackrel{\tau}{\Longrightarrow} Q'$ and $P' \mathscr{R} Q'$.*
- *If $Q \xrightarrow{\alpha} N$ and α is not τ, then P simulates Q in the same way as those for $\sim$ (see the remark following Definition 3).*
- *If $Q \xrightarrow{\tau} Q'$, then $P \xrightarrow{\widehat{\tau}} P'$ and $P' \mathscr{R} Q'$.*

We say Q expands P, written $P \preccurlyeq Q$ or $Q \succcurlyeq P$, if $P\mathscr{R}Q$ for some expansion $\mathscr{R}$. We call $\preccurlyeq$ the expansion relation.

From its definition, expansion obviously refines bisimilarity; that is, we have $\sim \subseteq \preccurlyeq \subseteq \approx$. It is well-known that it is also a precongruence (Sangiorgi and Walker, 2001; Sangiorgi and Rutten, 2012). More importantly, a useful tool based on expansion is the bisimulation up-to expansion.

Definition 20. *A symmetric binary relation $\mathscr{R}$ on FAHO processes is a bisimulation up-to expansion if it satisfies the conditions of Definition 3, except that every occurrence of $\mathscr{R}$ in the conditions is replaced with $\succcurlyeq \mathscr{R} \preccurlyeq$.*

Indeed, a bisimulation up-to expansion is guaranteed to be contained by bisimilarity. See Sangiorgi and Walker (2001),Pous and Sangiorgi (2011), and Sangiorgi and Rutten (2012) for a detailed discussion. This technique will be used to prove the soundness of the encoding.

Lemma 21. *If $\mathscr{R}$ is a bisimulation up-to expansion, then it holds that $\mathscr{R} \subseteq \approx$.*

Now we move on toward the operational correspondence of the encoding. The property below will be useful in establishing the operational correspondence.

Lemma 22. *Assume P is a closed $\Pi^m_{\mathbb{N}}$ process. Then*

$$(\nu)(u[[\![P]\!]_\nu \mid O] \mid \mathscr{E}) \succcurlyeq [\![P]\!] \mid (\nu)(u[O] \mid \mathscr{E})$$

with $\mathscr{E} \stackrel{\text{def}}{=} \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, uh.0]$.

Proof. We show by induction on P that

$$(\nu)(u[[\![P]\!]_\nu \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, uh.0]) \succcurlyeq [\![P]\!] \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, uh.0])$$

- P is 0. This is straightforward since $0 \mid T \sim T$.
- P is $a(X).P_1$ ($a \in \mathbb{N}$). First, notice that

$$[\![P]\!]_\nu \equiv a[out\ \nu.a(X).[\![P_1]\!]_\nu] \mid \prod_{h\in\mathbb{N}\cup\{\nu\}} \nu[out\ \nu.!\overline{out}\, ah.0]$$

$$[\![P]\!] \equiv (\nu)(a[a(X).[\![P_1]\!]_\nu] \mid \prod_{h\in\mathbb{N}\cup\{\nu\}} \nu[!\overline{out}\, ah.0])$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

We then have

$$\begin{aligned}
&(\nu)(u[[\![P]\!]_\nu \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\equiv\ &(\nu)(u[a[out\ \nu.a(X).[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[out\ \nu.!\overline{out}\ ah.0] \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &(\nu)(a[a(X).[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ ah.0] \mid u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &(\nu)(a[a(X).[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ ah.0]) \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &[\![P]\!] \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])
\end{aligned}$$

The first expansion above results from the (silent) out-movements concerning ν, among which ambient a and those ambients ν within u are ferried out. The second expansion above is due to the fact that the separated parts, that is, $a[a(X).[\![P_1]\!]_\nu] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ ah.0]$ and $u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0]$, essentially do not have interaction with respect to ν, so the local name ν can be distributed across them. We note that the interactions concerning ν are all those about out-movement, and these movements are coupled to each prefix in the encoded process. Maybe some of them can be intertwined, but no harm is done; that is, it can use its own repository of ν-out-movement or those available in the environment.

- P is $\overline{a}A.P_1$ ($a \in \mathbb{N}$). First, notice that

$$\begin{aligned}
[\![P]\!]_\nu &\equiv a[out\ \nu.\overline{a}[\![A]\!]_\nu.[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[out\ \nu.!\overline{out}\ ah.0]\\
[\![P]\!] &\equiv (\nu)(a[\overline{a}[\![A]\!]_\nu.[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ ah.0])
\end{aligned}$$

We then have

$$\begin{aligned}
&(\nu)(u[[\![P]\!]_\nu \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\equiv\ &(\nu)(u[a[out\ \nu.\overline{a}[\![A]\!]_\nu.[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[out\ \nu.!\overline{out}\ ah.0] \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &(\nu)(a[\overline{a}[\![A]\!]_\nu.[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ ah.0] \mid u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &(\nu)(a[\overline{a}[\![A]\!]_\nu.[\![P_1]\!]_\nu] \mid \textstyle\prod_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ ah.0]) \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &[\![P]\!] \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])
\end{aligned}$$

The first and second expansions are derived for reasons similar to the previous case.

- P is $P_1 \mid P_2$. Using induction hypothesis (ind. hyp. for short) twice, we have

$$\begin{aligned}
&(\nu)(u[[\![P]\!]_\nu \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\equiv\ &(\nu)(u[[\![P_1]\!]_\nu \mid [\![P_2]\!]_\nu \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\succcurlyeq\ &[\![P_1]\!] \mid (\nu)(u[[\![P_2]\!]_\nu \mid O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0]) \qquad \text{(ind. hyp.)}\\
\succcurlyeq\ &[\![P_1]\!] \mid [\![P_2]\!] \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0]) \qquad \text{(ind. hyp.)}\\
\equiv\ &[\![P_1 \mid P_2]\!] \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])\\
\equiv\ &[\![P]\!] \mid (\nu)(u[O] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0])
\end{aligned}$$

□

As a special case of Lemma 22, we have the following corollary.

Corollary 23. *Assume P is a closed Π^m process. Then*

$$(\nu)(u[[\![P]\!]_\nu] \mid \mathscr{E}) \succcurlyeq [\![P]\!]$$

with $\mathscr{E} \stackrel{\text{def}}{=} \Pi_{h\in\mathbb{N}\cup\{\nu\}}\ \nu[!\overline{out}\ uh.0]$.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Proof. Taking O as 0 in Lemma 22 and noticing that $(\nu)(u[0] \mid \mathscr{E}) \succcurlyeq 0$, we have

$$\begin{aligned}(\nu)(u[[\![P]\!]_\nu] \mid \mathscr{E}) &\succcurlyeq (\nu)(u[[\![P]\!]_\nu \mid 0] \mid \mathscr{E}) \\ &\succcurlyeq [\![P]\!] \mid (\nu)(u[0] \mid \mathscr{E}) \qquad \text{(Lemma 22)} \\ &\succcurlyeq [\![P]\!]\end{aligned}$$

□

Lemma 24 (Operational correspondence). *Suppose that P is a closed $\Pi^m_{\mathbb{N}}$ process. The following correspondence holds:*

- *If $P \xrightarrow{a(A)} P'$, then $[\![P]\!] \xrightarrow{aa([\![A]\!]_\nu)} M \succcurlyeq [\![P']\!]$;*
- *If $P \xrightarrow{\overline{a}A} P'$, then $[\![P]\!] \xrightarrow{\overline{a}a[\![A]\!]_\nu} M \succcurlyeq [\![P']\!]$;*
- *If $P \xrightarrow{\tau} P'$, then $[\![P]\!] \xrightarrow{\tau} M \succcurlyeq [\![P']\!]$.*

Conversely,

- *If $[\![P]\!] \xrightarrow{aa([\![A]\!]_\nu)} M$, then $P \xrightarrow{a(A)} P'$ and $[\![P']\!] \preccurlyeq M$;*
- *If $[\![P]\!] \xrightarrow{\overline{a}aM'} M$, then $P \xrightarrow{\overline{a}A} P'$, and $[\![A]\!]_\nu \equiv M'$ and $[\![P']\!] \preccurlyeq M$;*
- *If $[\![P]\!] \xrightarrow{\tau} M$, then $P \xrightarrow{\tau} P'$ and $[\![P']\!] \preccurlyeq M$.*

Moreover, $[\![P]\!]$ is not capable of actions other than those above.

Proof. We only prove the forward correspondence, as the backward correspondence is similar and has nothing special. It should be clear that $[\![P]\!]$ is only capable of actions resulting from those of P (the moving actions are silent). We proceed by induction on the structure of P.

- P is 0. There is nothing to prove.
- P is $a(X).P_1$. The mere immediate action is $P \xrightarrow{a(A)} P_1\{A/X\} \equiv P'$. Then
$$[\![P]\!] \equiv (\nu)(a[a(X).[\![P_1]\!]_\nu] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, ah.0])$$
and
$$[\![P]\!] \xrightarrow{aa([\![A]\!]_\nu)} (\nu)(a[[\![P_1]\!]_\nu\{[\![A]\!]_\nu/X\}] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, ah.0])$$
By Lemma 18, we have
$$[\![P]\!] \xrightarrow{aa([\![A]\!]_\nu)} (\nu)(a[[\![P_1\{A/X\}]\!]_\nu] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, ah.0]) \stackrel{\text{def}}{=} M$$
Then by Corollary 23, we have
$$[\![P]\!] \xrightarrow{aa([\![A]\!]_\nu)} M \succcurlyeq [\![P_1\{A/X\}]\!] \equiv [\![P']\!]$$
- P is $\overline{a}A.P_1$. The only direct action is $P \xrightarrow{\overline{a}A} P_1 \equiv P'$. Then
$$[\![P]\!] \equiv (\nu)(a[\overline{a}[\![A]\!].[\![P_1]\!]_\nu] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, ah.0])$$
and
$$[\![P]\!] \xrightarrow{\overline{a}a[\![A]\!]} (\nu)(a[[\![P_1]\!]_\nu] \mid \Pi_{h\in\mathbb{N}\cup\{\nu\}}\, \nu[!\overline{out}\, ah.0]) \stackrel{\text{def}}{=} M$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Then by Corollary 23, we have

$$[\![P]\!] \xrightarrow{\overline{aa}[\![A]\!]} M \succcurlyeq [\![P_1]\!] \equiv [\![P']\!]$$

- P is $P_1 \mid P_2$. There are eight cases in total. We take one half because the other half is similar.
  - $P \xrightarrow{a(A)} P'$ due to $P_1 \xrightarrow{a(A)} P_1{}'$, and $P' \equiv P_1{}' \mid P_2$. By ind. hyp., $[\![P_1]\!] \xrightarrow{aa([\![A]\!]_v)} M_1 \succcurlyeq [\![P_1{}']\!]$. Then
  $$[\![P_1 \mid P_2]\!] \equiv [\![P_1]\!] \mid [\![P_2]\!] \xrightarrow{aa([\![A]\!]_v)} M_1 \mid [\![P_2]\!] \succcurlyeq [\![P_1{}']\!] \mid [\![P_2]\!] \equiv [\![P']\!]$$
  - $P \xrightarrow{\overline{a}A} P'$ due to $P_1 \xrightarrow{\overline{a}A} P_1{}'$, and $P' \equiv P_1{}' \mid P_2$. By ind. hyp., $[\![P_1]\!] \xrightarrow{\overline{aa}[\![A]\!]_v} M_1 \succcurlyeq [\![P_1{}']\!]$. Then
  $$[\![P_1 \mid P_2]\!] \equiv [\![P_1]\!] \mid [\![P_2]\!] \xrightarrow{\overline{aa}[\![A]\!]_v} M_1 \mid [\![P_2]\!] \succcurlyeq [\![P_1{}']\!] \mid [\![P_2]\!] \equiv [\![P']\!]$$
  - $P \xrightarrow{\tau} P'$ due to $P_1 \xrightarrow{\tau} P_1{}'$, and $P' \equiv P_1{}' \mid P_2$. By ind. hyp., $[\![P_1]\!] \xrightarrow{\tau} M_1 \succcurlyeq [\![P_1{}']\!]$. Then
  $$[\![P_1 \mid P_2]\!] \equiv [\![P_1]\!] \mid [\![P_2]\!] \xrightarrow{\tau} M_1 \mid [\![P_2]\!] \succcurlyeq [\![P_1{}']\!] \mid [\![P_2]\!] \equiv [\![P']\!]$$
  - $P \xrightarrow{\tau} P'$ due to $P_1 \xrightarrow{\overline{a}A} P_1{}'$ and $P_2 \xrightarrow{a(A)} P_2{}'$, and $P' \equiv P_1{}' \mid P_2{}'$. By ind. hyp., $[\![P_1]\!] \xrightarrow{\overline{aa}[\![A]\!]_v} M_1 \succcurlyeq [\![P_1{}']\!]$, and $[\![P_2]\!] \xrightarrow{aa([\![A]\!]_v)} M_2 \succcurlyeq [\![P_2{}']\!]$. Then
  $$[\![P_1 \mid P_2]\!] \equiv [\![P_1]\!] \mid [\![P_2]\!] \xrightarrow{\tau} M_1 \mid M_2 \succcurlyeq [\![P_1{}']\!] \mid [\![P_2{}']\!] \equiv [\![P']\!]$$

□

5.3.1.2 Soundness and completeness. This section aims to show the full abstraction of the encoding with respect to the context bisimilarity and bisimilarity. The full abstraction has two parts: soundness and completeness. That two $\Pi^m_{\mathbb{N}}$ processes are context bisimilar implies their encoding is bisimilar is called soundness, and the converse direction is called completeness. Before proceeding, however, we note that there is some incompatibility between these two bisimilarities on either side. That is, concerning the HO output, it is required to be closed under (ambient-enclosed) contexts of the form $b[C]$ in the bisimulation of FAHO, while the context bisimulation in Π^m requires the closure under all contexts. This inconsistency stands in the way, and there appears little hope of recovering the universal context from ambient-enclosed ones. Guided by this observation, we define a variant bisimulation called hov-bisimulation that tunes the original bisimulation on the HO output clause; that is, the ambient-enclosed context now becomes an arbitrary one. We stress that this variant bisimulation is not trivial, and it does not render the full abstraction trivial either. In fact, it has the analogous discriminative capacity as compared with bisimilarity defined in Section 3 (since they share the majority of the requirements). The variant bisimulation comes out of some intrinsic compatibility issue concerning the two models, and it may stand as a bisimulation equality of its own importance.

Definition 25. *A symmetric binary relation $\mathscr{R}$ on FAHO processes is a hov-bisimulation, if whenever $M \mathscr{R} N$ the properties as those of Definition 3 hold, except that the HO output clause is modified to be as below:*

- *If $P \xrightarrow{(\widetilde{d})\overline{ab}(A)} P'$, then $Q \xRightarrow{(\widetilde{e})\overline{ab}(B)} Q'$, and for every context C, it holds that*
$$(\widetilde{d})(P' \mid C[A])\, \mathscr{R}\, (\widetilde{e})(Q' \mid C[B]).$$

The hov-bisimilarity, notation $\approx_{\mathrm{hov}}$, is the union of all hov-bisimulations (viz., the largest one).

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

As can be expected, when considering terms, the bisimulation requirement on HO prefixed-output is accordingly modified as below:

- If $M \xrightarrow{(\widetilde{d})\bar{a}A} M'$, then $N \xRightarrow{(\widetilde{e})\bar{a}B} N'$, and for every context C, every name c and O, it holds that
$$(\widetilde{d})(c[M' \mid O] \mid C[A])\, \mathscr{R}\, (\widetilde{e})(c[N' \mid O] \mid C[B]).$$

We denote by $\preccurlyeq_{\text{hov}}$ the expansion of hov-bisimulation that can be defined in a way similar to that of the original bisimilarity (Definition 19).

It is noted that the properties of the original bisimilarity remain true for $\approx_{\text{hov}}$, including equivalence, (pre)congruence, and the operational correspondence. The proofs are largely the same. Furthermore, it is not hard to see that $\approx_{\text{hov}} \subseteq \approx$. We do not know if $\approx \subseteq \approx_{\text{hov}}$ is also true (though we tend to believe so). We notice that the only difference between the two bisimilarities is in the context chosen in the HO output case (see the corresponding clauses in Definition 25 and Definition 3). For $\approx_{\text{hov}}$, the context C may be supposed to take the form $(\widetilde{f})(b_1[C_1] \mid b_2[C_2] \mid \cdots \mid b_k[C_k])$. From $\approx$, we know that each $b_i[C_i]$ $(i{=}1, \ldots, k)$ meets the bisimulation requirement, that is, $(\widetilde{d})(P' \mid b_i[C_i[A]])\, \mathscr{R}\, (\widetilde{e})(Q' \mid b_i[C_i[B]])$. It can be observed that deriving $(\widetilde{d})(P' \mid C[A])\, \mathscr{R}\, (\widetilde{e})(Q' \mid C[B])$ calls for some local congruence property (i.e., within the scope of the local names $\widetilde{d}$ and $\widetilde{e}$). A similar issue was once examined in (Fu 2005, 2015).

Now, we continue with the soundness, which is always the hard part. Instead of considering "strong" soundness, we show (weak) soundness, that is, soundness in which the bisimulation equivalence in the target model, here *FAHO*, is confined to the image of the encoding, namely, those processes that are the encodings of $\Pi^m_{\mathbb{N}}$ processes. We do not know if strong soundness is true, though we very much doubt that it is false. Nevertheless, the soundness we are going to establish is sufficient to justify the encoding.

We note that it is frequent that the (weak) soundness is considered (Gorla, 2008). First, strong soundness can be far too demanding since usually, the environment in the target model may be intrinsically different and more complex, so requesting bisimulation closure under such environments does not make sense. Second, to the point of encoding, accomplishing (weak) soundness should be sufficient, because the purpose of an encoding is to realize the behavior and maintain behavioral equivalence of the source model, and taking the contexts that comprise only the encodings of the terms from the source model serves this purpose in a reasonable manner. Moreover, many behavioral properties in the source model are passed on to the encodings in the target model under (weak) soundness (Sangiorgi and Walker, 2001), for example, termination.

We denote by $\hat{\approx}_{\text{hov}}$ the $\approx_{\text{hov}}$ restricted to the image of the encoding. The proof uses the technique of up-to expansion. Assuming $\preccurlyeq_{\text{hov}}$ as the expansion for $\approx_{\text{hov}}$ (recall Definition 19), a relation $\mathscr{R}$ is a bisimulation up-to expansion, if it meets the requirements of bisimulation, except that the resulting terms of the simulation in each of the clauses are related by the relation $\succcurlyeq_{\text{hov}} \mathscr{R} \preccurlyeq_{\text{hov}}$ rather than $\mathscr{R}$ itself. Such a relation $\mathscr{R}$ is guaranteed to be subsumed by bisimilarity (see Sangiorgi and Walker, 2001, and Sangiorgi and Rutten, 2012, for more details).

Proposition 26 (Soundness). *Assume that P and Q are processes of $\Pi^m_{\mathbb{N}}$. Then it holds that $P \approx_{ct} Q$ implies $[\![P]\!] \hat{\approx}_{\text{hov}} [\![Q]\!]$.*

Proof. We show that $\mathscr{R} \stackrel{\text{def}}{=} \{([\![P]\!], [\![Q]\!]) \mid P \approx_{ct} Q\}$ is a hov-bisimulation up-to expansion. A paramount point here is that we confine to the contexts that are themselves the encoding of some $\Pi^m_{\mathbb{N}}$ processes. There are quite some cases to analyze.

- (in-mov). If $[\![P]\!] \xrightarrow{in\, ab} (\widetilde{d})\langle M_1 \between M_2 \rangle$, then by Lemma 24, we know that this is not possible.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

- (coin-mov). If $[\![P]\!] \xrightarrow{\overline{in}\,ab} C$, then by Lemma 24, we know that this is not possible.
- (out1-mov). If $[\![P]\!] \xrightarrow{out\,ab} (\widetilde{d})\langle M_1 \between M_2\rangle$, then by Lemma 24, we know that this is not possible.
- (out2-mov). If $[\![P]\!] \xrightarrow{out\,abc} M$, then by Lemma 24, we know that this is not possible.
- (coout-mov). If $[\![P]\!] \xrightarrow{\overline{out}\,abc} M$, then by Lemma 24, we know that this is not possible.
- (hocom-input). If $[\![P]\!] \xrightarrow{ab(M_1)} M_2$, then by Lemma 24, we know that it must be the case that $[\![P]\!] \xrightarrow{aa([\![A]\!]_v)} M_2$ in which $M_1 \equiv [\![A]\!]_v$, and $P \xrightarrow{a(A)} P'$ with $[\![P']\!] \preccurlyeq_{\text{hov}} M_2$. Since $P \approx_{ct} Q$, we infer that $Q \xRightarrow{a(A)} Q'$ and $P' \approx_{ct} Q'$. By Lemma 24, we have $[\![Q]\!] \xRightarrow{aa([\![A]\!]_v)} M_3 \succcurlyeq_{\text{hov}} [\![Q']\!]$. So we conclude that $M_2 \succcurlyeq_{\text{hov}} [\![P']\!]\ \mathscr{R}\ [\![Q']\!] \preccurlyeq_{\text{hov}} M_3$.
- (hocom-res-output). If $[\![P]\!] \xrightarrow{(\widetilde{d})\overline{ab}(M_1)} M_2$, then by Lemma 24, we know that it must be the case that $[\![P]\!] \xrightarrow{\overline{aa}M_1} M_2$, and $P \xrightarrow{\overline{a}A} P'$ with $[\![A]\!]_v \equiv M_1$ and $[\![P']\!] \preccurlyeq_{\text{hov}} M_2$. Since $P \approx_{ct} Q$, we infer that $Q \xRightarrow{\overline{a}B} Q'$ and for every Π^m context C, it holds that

$$P' \mid C[A] \approx_{ct} Q' \mid C[B] \tag{15}$$

  By Lemma 24, we have $[\![Q]\!] \xRightarrow{\overline{aa}[\![B]\!]_v} M_3 \succcurlyeq_{\text{hov}} [\![Q']\!]$. We need to substantiate that for every FAHO context C', it holds that

$$M_2 \mid C'[[\![A]\!]_v]) \succcurlyeq_{\text{hov}} \mathscr{R} \preccurlyeq_{\text{hov}} M_3 \mid C'[[\![B]\!]_v] \tag{16}$$

  Now because we restrict the range of the contexts to those being the encoding image of some $\Pi^m_{\mathbb{N}}$ context, it is certain that C' is of the form of $[\![C_1]\!]$ for some $\Pi^m_{\mathbb{N}}$ context C_1. Thus, (16) becomes

$$M_2 \mid [\![C_1]\!][[\![A]\!]_v]) \succcurlyeq_{\text{hov}} \mathscr{R} \preccurlyeq_{\text{hov}} M_3 \mid [\![C_1]\!][[\![B]\!]_v] \tag{17}$$

  Or equivalently, since the encoding is compositional,

$$M_2 \mid [\![C_1[A]]\!]) \succcurlyeq_{\text{hov}} \mathscr{R} \preccurlyeq_{\text{hov}} M_3 \mid [\![C_1[B]]\!] \tag{18}$$

  To reach (18), we know as a fact from (15) that

$$[\![P']\!] \mid [\![C[A]]\!]\ \mathscr{R}\ [\![Q']\!] \mid [\![C[B]]\!] \tag{19}$$

  Taking C as C_1 in (19), and noticing $[\![P']\!] \preccurlyeq_{\text{hov}} M_2$ and $[\![Q']\!] \preccurlyeq_{\text{hov}} M_3$, we have

$$M_2 \mid [\![C_1[A]]\!] \succcurlyeq_{\text{hov}} [\![P']\!] \mid [\![C_1[A]]\!]\ \mathscr{R}\ [\![Q']\!] \mid [\![C_1[B]]\!] \preccurlyeq_{\text{hov}} M_3 \mid [\![C_1[B]]\!] \tag{20}$$

  Hence we conclude that (18) follows immediately from (20).
- (interaction). If $[\![P]\!] \xrightarrow{\tau} M$, then by Lemma 24, we know that $P \xrightarrow{\tau} P'$ and $M \succcurlyeq_{\text{hov}} [\![P']\!]$. Since $P \approx_{ct} Q$, we infer that $Q \Longrightarrow Q'$ and $P' \approx_{ct} Q'$. By Lemma 24, we have $[\![Q]\!] \Longrightarrow M' \succcurlyeq_{\text{hov}} [\![Q']\!]$. So we conclude that $M \succcurlyeq_{\text{hov}} [\![P']\!]\ \mathscr{R}\ [\![Q']\!] \preccurlyeq_{\text{hov}} M'$. □

We next show the completeness of the encoding. It is worth noting that the completeness does not call for restriction to $\hat{\approx}_{\text{hov}}$ and holds for $\approx_{\text{hov}}$.

Proposition 27 (Completeness). *Assume that P and Q are processes of $\Pi^m_{\mathbb{N}}$. Then it holds that $[\![P]\!] \approx_{\text{hov}} [\![Q]\!]$ implies $P \approx_{ct} Q$.*

Proof. We show that $\mathscr{R} \stackrel{\text{def}}{=} \{(P, Q) \mid [\![P]\!] \approx_{\text{hov}} [\![Q]\!]\}$ is a context bisimulation. We make a case analysis.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

- If $P \xrightarrow{a(A)} P'$, then by Lemma 24, we know that $[\![P]\!] \xrightarrow{aa([\![A]\!]_v)} M \succcurlyeq_{\text{hov}} [\![P']\!]$. Since $[\![P]\!] \approx_{\text{hov}} [\![Q]\!]$, we infer that $[\![Q]\!] \xRightarrow{aa([\![A]\!]_v)} M'$ and $M \approx_{\text{hov}} M'$. Again by Lemma 24, we know that $Q \xRightarrow{a(A)} Q'$ and $[\![Q']\!] \preccurlyeq_{\text{hov}} M'$. Thus, we have

$$[\![P']\!] \preccurlyeq_{\text{hov}} M \approx_{\text{hov}} M' \succcurlyeq_{\text{hov}} [\![Q']\!]$$

  So we conclude $P' \mathscr{R} Q'$.

- If $P \xrightarrow{\overline{a}A} P'$, then by Lemma 24, we know that $[\![P]\!] \xrightarrow{\overline{aa}[\![A]\!]_v} M \succcurlyeq_{\text{hov}} [\![P']\!]$. Since $[\![P]\!] \approx_{\text{hov}} [\![Q]\!]$, we infer that $[\![Q]\!] \xRightarrow{\overline{aa}[\![B]\!]_v} M'$, and for every *FAHO* context C, it holds that

$$M \mid C[[\![A]\!]_v] \approx_{\text{hov}} M' \mid C[[\![B]\!]_v] \tag{21}$$

  Again by Lemma 24, we know that $Q \xRightarrow{\overline{a}B} Q'$ and $[\![Q']\!] \preccurlyeq_{\text{hov}} M'$. We need to show that for every $\Pi^m_{\mathbb{N}}$ context C_1, it holds that

$$P' \mid C_1[A] \mathscr{R} Q' \mid C_1[B]$$

  namely,

$$[\![P']\!] \mid [\![C_1[A]]\!] \approx_{\text{hov}} [\![Q']\!] \mid [\![C_1[B]]\!]$$

  that is (since the encoding is compositional),

$$[\![P']\!] \mid [\![C_1]\!][[\![A]\!]_v] \approx_{\text{hov}} [\![Q']\!] \mid [\![C_1]\!][[\![B]\!]_v] \tag{22}$$

  Due to (21) and $M \succcurlyeq_{\text{hov}} [\![P']\!]$ and $M' \succcurlyeq_{\text{hov}} [\![Q']\!]$, we have

$$[\![P']\!] \mid C[[\![A]\!]_v] \approx_{\text{hov}} [\![Q']\!] \mid C[[\![B]\!]_v] \tag{23}$$

  Now we fix C_1 and compare (22) with (23). Since the encoding is a full mapping, that is, every $\Pi^m_{\mathbb{N}}$ process has an image in the target model FAHO, when iterating all the possibilities of C, the item $[\![C_1]\!]$ must be hit somewhere sometime. So we conclude that (22) indeed is true.

- If $P \xrightarrow{\tau} P'$, then by Lemma 24, we know that $[\![P]\!] \xrightarrow{\tau} M \succcurlyeq_{\text{hov}} [\![P']\!]$. Since $[\![P]\!] \approx_{\text{hov}} [\![Q]\!]$, we infer that $[\![Q]\!] \Longrightarrow M'$ and $M \approx_{\text{hov}} M'$. Again by Lemma 24, we know that $Q \Longrightarrow Q'$ and $[\![Q']\!] \preccurlyeq_{\text{hov}} M'$. Thus, we have

$$[\![P']\!] \preccurlyeq_{\text{hov}} M \approx_{\text{hov}} M' \succcurlyeq_{\text{hov}} [\![Q']\!]$$

  So we conclude $P' \mathscr{R} Q'$.

□

5.3.2 Discussion

We provide some discussion before the end of this section. One may also consider how to encode into FAHO HO processes with the restriction operator. Such an encoding appears hard, if not impossible, strikingly different from the case for FA with FO communication. An observation is that the encoding strategy in Fu (2007) (or above) does not apply anymore. A major obstacle is that FAHO disallows anonymous movement using *in* or *out* capabilities. So apparently ambient c in

$$a[(c)c[M] \mid N]$$

finds no easy way to be called out using some proper out-movement capability. This may be the moment when the HO communication of ambients comes into play, for example, extruding the name c with the help of some small gadget that later helps to drag c out. However, one has to be very careful to keep the encoding compositional. We also notice that the HO communication

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

mechanism cannot be harnessed to realize this anonymous exit from the outmost position because HO communication only sends objects from one ambient to another, not outside. Moreover, it seems possible to design such an encoding if one looks beyond the realm of FAHO, say, allowing parent-child communication. This would be an interesting further work.

6. Conclusion

In this paper, we have put forth and examined an ambient calculus that enables built-in HO communication. In particular, the ambient calculus is capable of explicitly communicating ambients themselves between ambients in a channel-based fashion. Such communications are subject to some peer-to-peer fairness; that is, the communicating participants are equally positioned and well informed of each other's presence. Also, compared with previous works, we redesign the "exit" movement of ambients, stipulating that it should be fully real identity; that is, the ambient on the exiting movement and the ambient allowing this movement should be fairly known to each other. This stresses the equal role of ambients in interactions and brings some convenience to the behavioral theory. We present the formalism of the proposed ambients and define the bisimulation on top of it. We show that bisimilarity is both an equivalence and a congruence, which is well-known to be challenging in the HO paradigm. Moreover, the observational barbed congruence is defined and shown to coincide with bisimilarity. The related proofs are provided in detail. To evaluate the expressiveness of our calculus, we manage to encode a minimal HO pi-calculus that is Turing complete. This lends confidence to the universal computational capacity of the calculus. The HO communication mechanism of FAHO can potentially be applied to more ambient calculi, say, SA or other similar models.

There are several future works worthy of consideration. One is to compare the operations of FAHO to see if there is redundancy. We have some informal discussions about the movement capabilities below. As it appears, the in-moving and out-moving capabilities are not derivable from the HO communication mechanism because HO communications only occur between ambients. The top-level ambients' movement cannot be controlled using HO communications, unless one assumes a global ambient in which every ambient resides. To this point, let us take the in-movement as an example and look at the following possible interpretations. To interpret the following interaction,

$$a[in\ b.M \mid N] \mid c[O] \mid b[\overline{in}\ a.A \mid B] \quad \xrightarrow{\tau} \quad c[O] \mid b[A \mid B \mid a[M \mid N]]$$

we try using a HO communication to simulate the in-movement by adding a fresh restricted ambient, say, f, for ferrying ambient a into b. Assume $A' \equiv a[M \mid N]$ and $\sim$ to be any reasonable strong behavioral equivalence. We have the following:

$$\begin{aligned}(f)(f[\overline{b}A'.0] \mid c[O] \mid b[f(X).(A \mid X) \mid B]) &\xrightarrow{\tau} (f)(f[0] \mid c[O] \mid b[A \mid A' \mid B]) \\ &\sim c[O] \mid b[A \mid B \mid a[M \mid N]]\end{aligned}$$

This strategy moves the on-the-move ambient a to an object position of the output action over b. It gives rise to an immediate issue. Ambients on that position cannot fire any action, but originally process N in ambient a may have some visible action on the shoulder of a. Even if this strategy can be accepted somehow, it does not seem to apply to out-movement because one cannot write a receiving process, for example, $a(X).X$, at the top level (it must reside in some ambient). So we contend that the movement capabilities are not likely encodable using merely HO communications. That being said, it would be fairly interesting to explore a formal (and hopefully fruitful) development for the preceding discussion in future work.

Another further direction is to provide some more powerful proof techniques, like up-to context techniques, so that the burden of establishing bisimulations can be further relieved. This is, in general, not trivial for HO process models. Pertaining to this, we can endeavor to clarify the

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

relationship between bisimilarity and its variant from the last section, as mentioned in the discussion of the encoding. A third future work is to investigate whether some weaker barbs may be enough to retrieve the coincidence between bisimilarity and barbed congruence. This would make the observational characterization of bisimilarity even more enjoyable. A fourth one is to further examine the expressiveness of our ambient calculus, by comparing it with more process models, such as the FO pi-calculus (Milner et al., 1992) or the value-passing CCS (Milner, 1989). This would reveal more computational essence of the calculus, particularly the ability to control names. Also, one can attempt to apply the calculus to practical scenarios, for example, distributed systems like those of cloud/edge/pervasive computing. This can not only test the modeling capability of the calculus but also help move toward the application end.

Acknowledgments. We are grateful to the anonymous referees for their valuable comments and constructive suggestions. This work also benefits a lot from the comments by Davide Sangiorgi, Wenbo Zhang, Huan Long, Yu Long, Yin Zhang, and many other colleagues. We would also like to thank Professor Nobuko Yoshida for the time in handling the paper.

Competing interests. The authors declare none.

Funding statement. This work has been supported by project ANR 12IS02001 PACE and NSF of China (62072299, 61872142) and Shanghai "Science and Technology Innovation Action Plan" (24BC3200500,24BC3200300).

References

Bonelli, E., Compagnoni, A., Dezani-Ciancaglini, M. and Garralda, P. (2007). Boxed ambients with communication interfaces. *Mathematical Structures in Computer Science*. **17** (4) 587–645.

Bugliesi, M., Castagna, G. and Crafa, S. (2001). Boxed ambients. In: Proceedings of the 4th International Symposium on Theoretical Aspects of Computer Software (TACS 2001), LNCS, 38–63.

Cao, Z. (2011). On the operational semantics of a higher order safe ambients calculus. In: Proceedings of Theoretical and Mathematical Foundations of Computer Science(ICTMF 2011), volume **164** of CCIS, 305–312,

Cao, Z. (2012). A calculus of higher order safe ambients and its bisimulations. In: Proceedings of the Sixth International Symposium on Theoretical Aspects of Software Engineering (TASE 2012), 93–100.

Cao, Z. (2013). On the expressiveness of monadic higher order safe ambient calculus. In: Proceedings of the 2013 International Conference on Foundations of Computer Science(ICTMF 2011), 305–312.

Cardelli, L. and Gordon, A. D. (2000). Mobile ambients. *Theoretical Computer Science* **240** (1) 177–213.

Cerone, A., Hennessy, M. and Merro, M. (2012). Modelling mac-layer communications in wireless systems. In: Proceedings of the Coordination Models and Languages (COORDINATION 2013), Berlin Heidelberg: Springer, 16–30.

Charatonik, W., Zilio, S. D. and Gordon, A. (2003). Model checking mobile ambients. *Theoretical Computer Science* **308** (1-3) 277–331.

Coppo, M. and Dezani-Ciancaglini, M. (2002). A fully abstract model for higher-order mobile ambients. In: Proceedings of the 3rd International Workshop on Verification, Model Checking, and Abstract Interpretation (VMCAI 2002), volume **2294** of Lecture Notes in Computer Science, 255–271.

Coronato, A. and Pietro, G. D. (2010). Formal design of ambient intelligence applications. *Computer*. **43** (12) 60–68.

Cruz, L. R. G. and Aguirre, O. O. (2005). A virtual machine for the ambient calculus. In: Proceedings of the 2nd International Conference on Electrical and Electronics Engineering

Fournet, C. (1998). *The Join-Calculus: a calculus for distributed mobile programming*. PhD thesis, Ecole Polytechnique, Palaiseau, Nov. INRIA TU-0556. Also available from http://research.microsoft.com/∼fournet.

Fournet, C. and Gonthier, G. (1996). The reflexive chemical abstract machine and the join-calculus. In: Proceedings of the 23rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL '96), 372–385.

Fournet, C., Gonthier, G., Levy, J., Maranget, L. and Remy, D. (1996). A calculus of mobile agents, Proceedings of the 7th International Conference on Concurrency Theory (CONCUR '96), volume**1119** of Lecture Notes in Computer Science, 406–421.

Fu, Y. (2005). *Checking Equivalence for Higher Order Processes-a Progress Report*. Technical report. BASICS lab. Shanghai Jiao Tong University, Shanghai, China.

Fu, Y. (2007). Fair ambients. *Acta Informatica* **43** (8) 535–594.

Fu, Y. (2015). Theory of interaction. *Theoretical Computer Science* **611** 1–49.

Gorla, D. (2008). Comparing communication primitives via their relative expressive power. *Information and Computation* **206** (8) 931–952.

Lanese, I., Pérez, J. A., Sangiorgi, D. and Schmitt, A. (2011). On the expressiveness and decidability of higher-order process calculi. *Information and Computation* **209** (2) 198–226.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Levi, F. and Sangiorgi, D. (2003). Mobile safe ambients. *ACM Transactions on Programming Languages and Systems* **25** (1) 1–69.
Merro, M. and Hennessy, M. (2002). Bisimulation congruences in safe ambients. In: Proceedings of the 29th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 02), Portland, Oregon, 71–80.
Merro, M. and Hennessy, M. (2006). A bisimulation-based semantic theory of safe ambients. *ACM Transactions on Programming Languages and Systems* **28** (2) 290–330.
Milner, R. (1989). *Communication and Concurrency*, Prentice Hall.
Milner, R., Parrow, J. and Walker, D. (1992). A calculus of mobile processes (parts i and ii). *Information and Computation* **100** (1) 1–77.
Mylonakis, N. (2017). A graph semantics for a variant of the ambient calculus more adequate for modeling service oriented computing. In: Electronic pre-proceedings of the Eighth International Workshop on Graph Computation Models, article 7, 1–13.
Pous, D. and Sangiorgi, D. (2011). *Advanced Topics in Bisimulation and Coinduction, Chapter Enhancements of the Coinductive Proof Method*, Cambridge University Press.
Sangiorgi, D. (1993). Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms. *Phd thesis*. LFCS report ECS-LFCS-93-266. Department of Computer Science, University of Edinburgh.
Sangiorgi, D. (1996a). Bisimulation for higher-order process calculi. *Information and Computation* **131** (2) 141–178.
Sangiorgi, D. (1996b). Pi-calculus, internal mobility and agent-passing calculi. *Theoretical Computer Science* **167** (1–2) 235–274. Extracts of parts of the material contained in this paper can be found in the Proceedings of TAPSOFT'95 and ICALP'95.
Sangiorgi, D. (2011). *Introduction to Bisimulation and Coinduction*, Cambridge University Press.
Sangiorgi, D. and Milner, R. (1992). The problem of weak bisimulation up-to. In: Proceedings of CONCUR'92, volume **630** of LNCS, Springer Verlag, 32–46.
Sangiorgi, D. and Rutten, J. (2012). *Advanced Topics in Bisimulation and Coinduction*, Cambridge University Press.
Sangiorgi, D. and Walker, D. (2001). *The Pi-Calculus: A Theory of Mobile Processes*, Cambridge University Press.
Schmitt, A. and Stefani, J.-B. (2003). The m-calculus: a higher-order distributed process calculus. *ACM SIGPLAN Notices* **38** (1) 50–61.
Schmitt, A. and Stefani, J.-B. (2004). The Kell calculus: A family of higher-order distributed process calculi. In: Proceedings of the IST/FET International Workshop on Global Computing (GC2004), volume **3267** of Lecture Notes in Computer Science, 146–178.
Siewe, F., Zedan, H. and Cau, A. (2011). The calculus of context-aware ambients. *Journal of Computer and System Sciences* **77** (4) 597–620.
Sun, Y. (2015). *Toward a model checker for ambient logic using the process analysis toolkit*. Master's thesis, Department of Computer Science, Bishop's University, Sherbrooke, Quebec, Canada.
Tomásek, M. (2007). Types for calculus of mobile code applications. *Acta Electrotechnica et Informatica* (**7**) 1–6.
Xu, X. (2012). Distinguishing and relating higher-order and first-order processes by expressiveness. *Acta Informatica* **49** (7-8) 445–484.

A. Appendix Proofs for Section 3

This appendix gives the proofs for Section 3.

Proof of Lemma 10. Assume $M \approx N$. We will show that $C[M] \approx C[N]$ for every context C that is $\vartheta.[\cdot]$, $a[[\cdot]]$, $[\cdot] \mid P$, or $(c)[\cdot]$. Since it is quite straightforward to see that $\vartheta.P \approx \vartheta.Q$ (the case when ϑ is $(\widetilde{d})\overline{a}A$ is similar to that of the HO pi-calculus (Sangiorgi, 1993; Sangiorgi and Walker, 2001)), we will focus on the other contexts.

We use an inductive way to construct a relation that is a congruence in its own right. Then it is proven to be a bisimulation (over terms, so as to accommodate all possible contexts). A similar method is used in (Sangiorgi, 1993; Sangiorgi and Walker, 2001; Merro and Hennessy, 2002; Fu, 2007). We recall that $\mathfrak{N}$ denotes the set of natural numbers.

$$\begin{aligned}
\mathscr{R}_0 &\stackrel{\text{def}}{=} \approx \\
\mathscr{R}_{n+1} &\stackrel{\text{def}}{=} \{(C[M], C[N]) \mid M \,\mathscr{R}_n\, N \text{ and } C \text{ is } a[[\cdot]], [\cdot] \mid O, \text{ or } (c)[\cdot]\} \\
\mathscr{R} &\stackrel{\text{def}}{=} \bigcup_{i \in \mathfrak{N}} \mathscr{R}_i
\end{aligned}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

We now prove that $\mathscr{R}$ is a bisimulation up-to $\sim$, from which we have $\mathscr{R} \subseteq \approx$, and the congruence property follows. To the aim of this lemma, we show by induction over n that $\mathscr{R}_n$ satisfies the requirements of bisimulation up-to $\sim$ for all n. If n is 0, there is nothing to prove. Assume that for k is $0, 1, \ldots, n$, $\mathscr{R}_k$ satisfies the requirements of bisimulation up-to $\sim$. We show by a case analysis that $\mathscr{R}_{n+1}$ also does, which completes the induction. Suppose $M \mathscr{R}_n N$. We first specify the bisimulation up-to $\sim$ for convenience. We remark that $\mathscr{R}$ is (defined to be) symmetric.

- (prefix). If $M \xrightarrow{\vartheta} M'$ in which ϑ is not $(\widetilde{d})\overline{a}A$, then $N \stackrel{\vartheta}{\Longrightarrow} N'$ and $M' \sim \mathscr{R} \sim N'$.
- (prefix-output). If $M \xrightarrow{(\widetilde{d})\overline{a}A} M'$, then $N \stackrel{(\widetilde{e})\overline{a}B}{\Longrightarrow} N'$, and for every context C_1, name c and O, it holds that $(\widetilde{d})(c[M' \mid O] \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e})(c[N' \mid O] \mid C_1[B])$.
- (in-mov). If $M \xrightarrow{in\ ab} (\widetilde{d})\langle M_1 \between M_2\rangle$, then $N \Longrightarrow \xrightarrow{in\ ab} (\widetilde{e})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} b[[\cdot] \mid O]$, it holds that $(\widetilde{e})(N_2 \mid C_1[N_1]) \Longrightarrow \sim \mathscr{R} \sim (\widetilde{d})(M_2 \mid C_1[M_1])$.
- (coin-mov). If $M \xrightarrow{\overline{in}\ ab} C_1$, then $N \Longrightarrow \xrightarrow{\overline{in}\ ab} C_2$, and for every A, it holds that $C_2[a[A]] \Longrightarrow \sim \mathscr{R} \sim C_1[a[A]]$.
- (out1-mov). If $M \xrightarrow{out\ ab} (\widetilde{d})\langle M_1 \between M_2\rangle$, then $N \Longrightarrow \xrightarrow{out\ ab} (\widetilde{e})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} c[[\cdot] \mid O]$, it holds that $(\widetilde{e})(N_1 \mid C_1[N_2]) \Longrightarrow \sim \mathscr{R} \sim (\widetilde{d})(M_1 \mid C_1[M_2])$.
- (out2-mov). If $M \xrightarrow{out\ abc} M'$, then $N \stackrel{out\ abc}{\Longrightarrow} N'$ and $M' \sim \mathscr{R} \sim N'$.
- (coout-mov). If $M \xrightarrow{\overline{out}\ abc} M'$, then $N \stackrel{\overline{out}\ abc}{\Longrightarrow} N'$ and $M' \sim \mathscr{R} \sim N'$.
- (hocom-input). If $M \xrightarrow{ab(A)} M'$, then $N \stackrel{ab(A)}{\Longrightarrow} N'$ and $M' \sim \mathscr{R} \sim N'$.
- (hocom-res-output). If $M \xrightarrow{(\widetilde{d})\overline{ab}(A)} M'$, then $N \stackrel{(\widetilde{e})\overline{ab}(B)}{\Longrightarrow} N'$, and for every context $C_1 \stackrel{\text{def}}{=} b[C_1']$ that incurs no name conflict, it holds that $(\widetilde{d})(M' \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e})(N' \mid C_1[B])$.
- (interaction). If $M \xrightarrow{\tau} M'$, then $N \Longrightarrow N'$ and $M' \sim \mathscr{R} \sim N'$.

Now we have $C[M]\ \mathscr{R}_{n+1}\ C[N]$ and many cases to analyze. To be laconic, we will often omit the case that is incompatible with the corresponding action; that is in such a case (of context), some action is impossible, and we will focus on the significant cases.

- (prefix). Suppose $C[M] \xrightarrow{\vartheta} L$ in which ϑ is not $(\widetilde{d})\overline{a}A$. We expand the discussion over possible forms of C and will do the same for the rest of the cases.
  - C is $a[[\cdot]]$. This case is not possible.
  - C is $[\cdot] \mid O$. In this case, $M \mid O \xrightarrow{\vartheta} L$. Then this action must result from M or O. In the latter, we immediately know that $M \mid O \xrightarrow{\vartheta} M \mid O_1 \equiv L$ where $O \xrightarrow{\vartheta} O_1$ and also $N \mid O \xrightarrow{\vartheta} N \mid O_1$, and defining $C' \stackrel{\text{def}}{=} [\cdot] \mid O_1$ suffices to close the case. If the action comes from M, that is, $M \xrightarrow{\vartheta} M'$ and $L \equiv M' \mid O$, then by induction hypothesis (ind. hyp. for short), we know that $N \stackrel{\vartheta}{\Longrightarrow} N'$ and $M' \sim M_1\ \mathscr{R}\ N_1 \sim N'$ for some M_1 and N_1. So $M \mid O \xrightarrow{\vartheta} M' \mid O$ can be matched by $N \mid O \stackrel{\vartheta}{\Longleftarrow} N' \mid O$, and we are left with showing $M' \mid O \sim \mathscr{R} \sim N' \mid O$. This can be obtained by setting $C' \stackrel{\text{def}}{=} C$, in which case we have $C'[M'] \sim C'[M_1]$ and $C'[N'] \sim C'[N_1]$, and moreover $C'[M_1]\ \mathscr{R}\ C'[N_1]$ because of $M_1\ \mathscr{R}\ N_1$. To summarize, we have $M' \mid O \equiv C'[M'] \sim \mathscr{R} \sim C'[N'] \equiv N' \mid O$, as required.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

– C is $(c)[\cdot]$. In this case, $(c)M \xrightarrow{\vartheta} L$. Then this action must result from M and $c \notin \mathrm{n}(\vartheta)$, that is, $M \xrightarrow{\vartheta} M'$ and $L \equiv (c)M'$. By ind. hyp., we know that $N \xRightarrow{\vartheta} N'$ and $M' \sim M_1 \mathscr{R} N_1 \sim N'$ for some M_1 and N_1. So $(c)M \xrightarrow{\vartheta} L$ can be matched by $C[N] \equiv (c)N \xRightarrow{\vartheta} (c)N' \equiv C'[N']$ in which $C' \stackrel{\text{def}}{=} C$, and moreover, we have $(c)M' \equiv C'[M'] \sim (c)M_1 \mathscr{R} (c)N_1 \sim C'[N'] \equiv (c)N'$, which closes the case.

- (prefix-output). Suppose $C[M] \xrightarrow{(\widetilde{d})\bar{a}A} L$.

– C is $a[[\cdot]]$. This case is not possible, and neither is the case with other ambient names.

– C is $[\cdot] \mid O$. In this case, $M \mid O \xrightarrow{(\widetilde{d})\bar{a}A} L$. There are two subcases.

(i) If the action results from O, then $M \mid O \xrightarrow{(\widetilde{d})\bar{a}A} M \mid O_1 \equiv L$, where $O \xrightarrow{(\widetilde{d})\bar{a}A} O_1$ (we assume that $\widetilde{d}$ does not appear in M and N and will always assume no name conflict henceforth), and also $N \mid O \xrightarrow{(\widetilde{d})\bar{a}A} N \mid O_1$. Now for every context $C_1 \stackrel{\text{def}}{=} a[C_1']$, name c and O', we need to show that $(\widetilde{d})(c[M \mid O_1 \mid O'] \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{d})(c[N \mid O_1 \mid O'] \mid C_1[A])$, which follows due to $M \mathscr{R}_n N$.

(ii) If this action comes from M, that is, $M \mid O \xrightarrow{(\widetilde{d})\bar{a}A} M' \mid O \equiv L$ where $M \xrightarrow{(\widetilde{d})\bar{a}A} M'$, then by ind. hyp., we know that $N \xRightarrow{(\widetilde{e})\bar{a}B} N'$, and for every context $C_1 \stackrel{\text{def}}{=} a[C_1']$, name c_1 and O_1, it holds that

$$(\widetilde{d})(c_1[M' \mid O_1] \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e})(c_1[N' \mid O_1] \mid C_1[B]) \tag{A1}$$

So $M \mid O \xrightarrow{(\widetilde{d})\bar{a}A} M' \mid O$ can be matched by $N \mid O \xRightarrow{(\widetilde{e})\bar{a}B} N' \mid O$, and we need to show that for every $C_2 \stackrel{\text{def}}{=} a[C_2']$, c_2 and O_2, it holds that

$$(\widetilde{d})(c_2[M' \mid O \mid O_2] \mid C_2[A]) \sim \mathscr{R} \sim (\widetilde{e})(c_2[N' \mid O \mid O_2] \mid C_2[B])$$

Taking $O' \stackrel{\text{def}}{=} O \mid O_2$, this follows from (A1).

– C is $(c)[\cdot]$. In this case, $(c)M \xrightarrow{(\widetilde{d})\bar{a}A} L$. This action must result from M, that is, $M \xrightarrow{(\widetilde{e})\bar{a}A} M'$. By ind. hyp., we know that $N \xRightarrow{(\widetilde{e'})\bar{a}B} N'$, and for every $C_1 \stackrel{\text{def}}{=} a[C_1']$, f_1 and O_1, it holds that

$$(\widetilde{e})(f_1[M' \mid O_1] \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e'})(f_1[N' \mid O_1] \mid C_1[B]) \tag{A2}$$

Thus, we immediately know that $(c)N \xRightarrow{(\widetilde{d'})\bar{a}B} L'$. We need to show that for every context $C_2 \stackrel{\text{def}}{=} a[C_2']$, f_2 and O_2, it holds that

$$(\widetilde{d})(f_2[L \mid O_2] \mid C_2[A]) \sim \mathscr{R} \sim (\widetilde{d'})(f_2[L' \mid O_2] \mid C_2[B]) \tag{A3}$$

There are four subcases, depending on whether c belongs to $\widetilde{d}$ or not and whether c belongs to $\widetilde{d'}$ or not.

(i) $c \notin \widetilde{d} \cup \widetilde{d'}$, $\widetilde{d}{=}\widetilde{e}$ and $\widetilde{d'}{=}\widetilde{e'}$, and $L \equiv (c)M'$ and $L' \equiv (c)N'$. From (A2), we know that

$$(\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A]) \sim M'' \mathscr{R} N'' \sim (\widetilde{e'})(f_2[N' \mid O_2] \mid C_2[B])$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

for some M'' and N''. Assuming no name conflict and setting $C' \stackrel{\text{def}}{=} C$, we have as requested by (A3)

$$\begin{aligned}(\widetilde{d})(f_2[L \mid O_2] \mid C_2[A]) &\sim (\widetilde{e})(f_2[(c)M' \mid O_2] \mid C_2[A]) \\ &\sim (c)((\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A])) \\ &\sim C'[(\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A])] \\ &\sim C'[M''] \\ &\mathscr{R}\ C'[N''] \\ &\sim C'[(\widetilde{e'})(f_2[N' \mid O_2] \mid C_2[B])] \\ &\sim (\widetilde{d'})(f_2[(c)N' \mid O_2] \mid C_2[B]) \\ &\sim (\widetilde{d'})(f_2[L' \mid O_2] \mid C_2[B])\end{aligned}$$

(ii) $c \in \widetilde{d} \cap \widetilde{d'}$, $\widetilde{d}{=}\widetilde{e} \cup \{c\}$ and $\widetilde{d'}{=}\widetilde{e'} \cup \{c\}$, and $L \equiv M'$ and $L' \equiv N'$. From (A2), we know that

$$(\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A]) \sim M'' \mathscr{R} N'' \sim (\widetilde{e'})(f_2[N' \mid O_2] \mid C_2[B])$$

for some M'' and N''. Setting $C' \stackrel{\text{def}}{=} C$, we have as requested by (A3)

$$\begin{aligned}(\widetilde{d})(f_2[L \mid O_2] \mid C_2[A]) &\sim (\widetilde{d})(f_2[M' \mid O_2] \mid C_2[A]) \\ &\sim (c)((\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A])) \\ &\sim C'[(\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A])] \\ &\sim C'[M''] \\ &\mathscr{R}\ C'[N''] \\ &\sim C'[(\widetilde{e'})(f_2[N' \mid O_2] \mid C_2[B])] \\ &\sim (\widetilde{d'})(f_2[L' \mid O_2] \mid C_2[B])\end{aligned}$$

(iii) $c \in \widetilde{d}$, $\widetilde{d}{=}\widetilde{e} \cup \{c\}$ and $L \equiv M'$; $c \notin \widetilde{d'}$, $\widetilde{d'}{=}\widetilde{e'}$, and $L' \equiv (c)N'$. Again from (A2), we know that

$$(\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A]) \sim M'' \mathscr{R} N'' \sim (\widetilde{e'})(f_2[N' \mid O_2] \mid C_2[B])$$

for some M'' and N''. Setting $C' \stackrel{\text{def}}{=} C$, we have as requested by (A3)

$$\begin{aligned}(\widetilde{d})(f_2[L \mid O_2] \mid C_2[A]) &\sim (\widetilde{d})(f_2[M' \mid O_2] \mid C_2[A]) \\ &\sim (c)((\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A])) \\ &\sim C'[(\widetilde{e})(f_2[M' \mid O_2] \mid C_2[A])] \\ &\sim C'[M''] \\ &\mathscr{R}\ C'[N''] \\ &\sim C'[(\widetilde{e'})(f_2[N' \mid O_2] \mid C_2[B])] \\ &\sim (\widetilde{d'})(f_2[(c)N' \mid O_2] \mid C_2[B]) \\ &\sim (\widetilde{d'})(f_2[L' \mid O_2] \mid C_2[B])\end{aligned}$$

(iv) $c \notin \widetilde{d}$, $\widetilde{d}{=}\widetilde{e}$, and $L \equiv (c)M$; $c \in \widetilde{d'}$, $\widetilde{d'}{=}\widetilde{e'} \cup \{c\}$, and $L' \equiv N'$. This is similar to the last subcase.

- (in-mov). Suppose $C[M] \xrightarrow{in\ ab} (\widetilde{d})\langle L_1 \between L_2 \rangle$.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

– C is $a[[\cdot]]$. We emphasize that if the context is $b[[\cdot]]$ (b is not a), then the action *in ab* is not applicable. We will no longer comment on this kind of situation in the follow-up discussion. In this case, we know that $C[M] \equiv a[M] \xrightarrow{in\,ab} (\widetilde{d})\langle L_1 \between L_2\rangle$ comes from $M \xrightarrow{in\,b} M'$, in which $\widetilde{d}=\emptyset$, $L_1 \equiv a[M']$, and $L_2 \equiv 0$. By ind. hyp., $N \Longrightarrow N_2 \xrightarrow{in\,b} N_3 \Longrightarrow N'$ and $M' \sim M_1 \mathscr{R} N_1 \sim N'$ for some M_1 and N_1. So $C[M] \equiv a[M] \xrightarrow{in\,ab} \langle a[M'] \between 0\rangle$ can be matched by $C[N] \equiv a[N] \Longrightarrow \xrightarrow{in\,ab} \langle a[N_3] \between 0\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} b[[\cdot] \mid O]$, since $M' \sim \mathscr{R} \sim N'$, it holds that $0 \mid C_1[a[N_3]] \Longrightarrow 0 \mid C_1[a[N']] \sim \mathscr{R} \sim 0 \mid C_1[a[M']]$.
– C is $[\cdot] \mid O$. In this case, the in-movement action may come from M or O, and we analyze each case.

(i) If $M \xrightarrow{in\,ab} (\widetilde{d})\langle M_1 \between M_2\rangle$, then $M \mid O \xrightarrow{in\,ab} (\widetilde{d})\langle M_1 \between M_2 \mid O\rangle$ in which $M_1 \equiv L_1$ and $M_2 \mid O \equiv L_2$. By ind hyp., we know that $N \Longrightarrow \xrightarrow{in\,ab} (\widetilde{e})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} b[[\cdot] \mid O']$, it holds for some A_1, A_2 and A_3 that

$$(\widetilde{e})(N_2 \mid C_1[N_1]) \Longrightarrow A_1 \sim A_2 \mathscr{R} A_3 \sim (\widetilde{d})(M_2 \mid C_1[M_1])$$

So we have $N \mid O \Longrightarrow \xrightarrow{in\,ab} (\widetilde{e})\langle N_1 \between N_2 \mid O\rangle$ and

$$(\widetilde{e})(N_2 \mid O \mid C_1[N_1]) \Longrightarrow A_1 \mid O \sim A_2 \mid O \mathscr{R} A_3 \mid O \sim (\widetilde{d})(M_2 \mid O \mid C_1[M_1])$$

(ii) If $O \xrightarrow{in\,ab} (\widetilde{d})\langle O_1 \between O_2\rangle$, then $M \mid O \xrightarrow{in\,ab} (\widetilde{d})\langle O_1 \between O_2 \mid M\rangle$ in which $O_1 \equiv L_1$ and $O_2 \mid M \equiv L_2$. So $N \mid O \xrightarrow{in\,ab} (\widetilde{d})\langle O_1 \between O_2 \mid N\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} b[[\cdot] \mid O']$, it holds for $A_1 \stackrel{\text{def}}{=} (\widetilde{d})(O_2 \mid C_1[O_1])$ that

$$(\widetilde{d})(O_2 \mid N \mid C_1[O_1]) \Longrightarrow \sim N \mid A_1 \mathscr{R} M \mid A_1 \sim (\widetilde{d})(O_2 \mid M \mid C_1[O_1])$$

– C is $(c)[\cdot]$. In this case, $C[M] \equiv (c)M \xrightarrow{in\,ab} (\widetilde{d})\langle L_1 \between L_2\rangle$ due to $M \xrightarrow{in\,b} (\widetilde{d'})\langle M_1 \between M_2\rangle$ in which $\widetilde{d} = \widetilde{d'} \cup \{c\}$, $L_1 \equiv M_1$ and $L_2 \equiv M_2$. By ind. hyp., we have $N \Longrightarrow \xrightarrow{in\,ab} (\widetilde{e'})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} b[[\cdot] \mid O']$, it holds for some A_1, A_2 and A_3 that

$$(\widetilde{e'})(N_2 \mid C_1[N_1]) \Longrightarrow A_1 \sim A_2 \mathscr{R} A_3 \sim (\widetilde{d'})(M_2 \mid C_1[M_1])$$

So we have $(c)N \Longrightarrow \xrightarrow{in\,ab} (\widetilde{e})\langle N_1 \between N_2\rangle$ in which $\widetilde{e} = \widetilde{e'} \cup \{c\}$ and

$$(\widetilde{e})(N_2 \mid C_1[N_1]) \Longrightarrow (c)A_1 \sim (c)A_2 \mathscr{R} (c)A_3 \sim (\widetilde{d})(M_2 \mid C_1[M_1])$$

- (coin-mov). Suppose $C[M] \xrightarrow{\overline{in}\,ab} C_1$.

– C is $b[[\cdot]]$. In this case, we know that $C[M] \equiv b[M] \xrightarrow{\overline{in}\,ab} C_1 \equiv b[M' \mid [\cdot]]$ because of $M \xrightarrow{\overline{in}\,a} M'$. By ind. hyp., we have $N \Longrightarrow N_1 \xrightarrow{\overline{in}\,a} N_2 \Longrightarrow N' \sim \mathscr{R} \sim M'$ for some N_1, N_2, and N'. So we have $C[N] \equiv b[N] \Longrightarrow b[N_1] \xrightarrow{\overline{in}\,ab} C_2 \equiv b[N_2 \mid [\cdot]]$, and moreover for every A

$$C_2[a[A]] \equiv b[N_2 \mid a[A]] \Longrightarrow b[N' \mid a[A]] \sim \mathscr{R} \sim b[M' \mid a[A]] \equiv C_1[a[A]]$$

– C is $[\cdot] \mid O$. In this case, the coin-movement action may come from M or O, and we analyze each case.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

(i) If $M \xrightarrow{\overline{in}\,ab} C_1'$, then $C[M] \equiv M \mid O \xrightarrow{\overline{in}\,ab} C_1 \equiv C_1' \mid O$. By ind. hyp., $N \Longrightarrow \xrightarrow{\overline{in}\,ab} C_2'$, and for every A, it holds that $C_2'[a[A]] \Longrightarrow B_1 \sim B_2 \mathscr{R} B_3 \sim C_1'[a[A]]$ for some B_1, B_2, and B_3. So $C[N] \equiv N \mid O \Longrightarrow \xrightarrow{\overline{in}\,ab} C_2' \mid O \stackrel{\text{def}}{=} C_2$, and we have

$$C_2[a[A]] \equiv C_2'[a[A]] \mid O \Longrightarrow B_1 \mid O \sim B_2 \mid O \mathscr{R} B_3 \mid O \sim C_1'[a[A]] \mid O \equiv C[a[A]]$$

(ii) If $O \xrightarrow{\overline{in}\,ab} C_1'$, then $C[M] \equiv M \mid O \xrightarrow{\overline{in}\,ab} C_1 \equiv M \mid C_1'$. So $C[N] \equiv N \mid O \xrightarrow{\overline{in}\,ab} C_2 \equiv N \mid C_1'$. For every A, we have

$$C_2[a[A]] \equiv N \mid C_1'[a[A]] \sim \mathscr{R} \sim M \mid C_1'[a[A]] \equiv C_1[a[A]]$$

– C is $(c)[\cdot]$. In this case, we know that $(c)M \xrightarrow{\overline{in}\,ab} C_1$ results from $M \xrightarrow{\overline{in}\,ab} C_1'$ and $C_1 \equiv (c)C_1'$. By ind. hyp., $N \Longrightarrow \xrightarrow{\overline{in}\,ab} C_2'$, and for every A, it holds that $C_2'[a[A]] \Longrightarrow B_1 \sim B_2 \mathscr{R} B_3 \sim C_1'[a[A]]$ for some B_1, B_2, and B_3. So we have $(c)N \Longrightarrow \xrightarrow{\overline{in}\,ab} (c)C_2' \stackrel{\text{def}}{=} C_2$, and

$$C_2[a[A]] \equiv (c)C_2'[a[A]] \Longrightarrow (c)B_1 \sim (c)B_2 \mathscr{R} (c)B_3 \sim (c)C_1'[a[A]] \equiv C_1[a[A]]$$

- (out1-mov). Suppose $C[M] \xrightarrow{out\,ab} (\widetilde{d})\langle L_1 \between L_2\rangle$.

– C is $a[[\cdot]]$. In this case, we know that $C[M] \equiv a[M] \xrightarrow{out\,ab} (\widetilde{d})\langle L_1 \between L_2\rangle$ because of $M \xrightarrow{out\,b} M'$, in which $\widetilde{d} = \emptyset$, $L_1 \equiv a[M']$, and $L_2 \equiv 0$. By ind. hyp., we have $N \Longrightarrow N_1 \xrightarrow{out\,b} N_2 \Longrightarrow N' \sim \mathscr{R} \sim M'$ for some N_1, N_2, N_3, and N'. So we know that

$$C[N] \equiv a[N] \Longrightarrow a[N_1] \xrightarrow{out\,ab} \langle a[N_2] \between 0\rangle$$

and for every context $C_1 \stackrel{\text{def}}{=} c[[\cdot] \mid O]$, we have

$$a[N_2] \mid C_1[0] \Longrightarrow a[N'] \mid C_1[0] \sim \mathscr{R} \sim a[M'] \mid C_1[0] \equiv a[L_1] \mid C_1[L_2]$$

– C is $[\cdot] \mid O$. In this case, the out-movement action must come from M or O, and we analyze each case.

(i) If $M \xrightarrow{out\,ab} (\widetilde{d})\langle M_1 \between M_2\rangle$, then $M \mid O \xrightarrow{out\,ab} (\widetilde{d})\langle M_1 \between M_2 \mid O\rangle$ in which $M_1 \equiv L_1$ and $M_2 \mid O \equiv L_2$. By ind hyp., we know that $N \Longrightarrow \xrightarrow{out\,ab} (\widetilde{e})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} c[[\cdot] \mid O']$, it holds for some A_1, A_2, and A_3 that

$$(\widetilde{e})(N_1 \mid C_1[N_2]) \Longrightarrow A_1 \sim A_2 \mathscr{R} A_3 \sim (\widetilde{d})(M_1 \mid C_1[M_2])$$

So we have $N \mid O \Longrightarrow \xrightarrow{out\,ab} (\widetilde{e})\langle N_1 \between N_2 \mid O\rangle$ and

$$(\widetilde{e})(N_1 \mid O \mid C_1[N_2]) \Longrightarrow A_1 \mid O \sim A_2 \mid O \mathscr{R} A_3 \mid O \sim (\widetilde{d})(M_2 \mid O \mid C_1[M_1])$$

(ii) If $O \xrightarrow{out\,ab} (\widetilde{d})\langle O_1 \between O_2\rangle$, then $M \mid O \xrightarrow{out\,ab} (\widetilde{d})\langle O_1 \between O_2 \mid M\rangle$ in which $O_1 \equiv L_1$ and $O_2 \mid M \equiv L_2$. So $N \mid O \xrightarrow{out\,ab} (\widetilde{d})\langle O_1 \between O_2 \mid N\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} c[[\cdot] \mid O']$, it holds for $A_1 \stackrel{\text{def}}{=} (\widetilde{d})(O_2 \mid C_1[O_1])$ that

$$(\widetilde{d})(O_2 \mid N \mid C_1[O_1]) \Longrightarrow \sim N \mid A_1 \mathscr{R} M \mid A_1 \sim (\widetilde{d})(O_2 \mid M \mid C_1[O_1])$$

– C is $(c)[\cdot]$. In this case, $C[M] \equiv (c)M \xrightarrow{out\,ab} (\widetilde{d})\langle L_1 \between L_2\rangle$ due to $M \xrightarrow{out\,b} (\widetilde{d'})\langle M_1 \between M_2\rangle$ in which $\widetilde{d} = \widetilde{d'} \cup \{c\}$, $L_1 \equiv M_1$, and $L_2 \equiv M_2$. By ind. hyp., we have $N \Longrightarrow \xrightarrow{out\,ab} (\widetilde{e'})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} c[[\cdot] \mid O']$, it holds for some A_1, A_2, and A_3 that

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

$$(\widetilde{e'})(N_1 \mid C_1[N_2]) \Longrightarrow A_1 \sim A_2 \mathscr{R} A_3 \sim (\widetilde{d'})(M_1 \mid C_1[M_2])$$

So we have $(c)N \Longrightarrow \xrightarrow{out\ ab} (\widetilde{e})\langle N_1 \between N_2\rangle$ in which $\widetilde{e} = \widetilde{e'} \cup \{c\}$ and

$$(\widetilde{e})(N_1 \mid C_1[N_2]) \Longrightarrow (c)A_1 \sim (c)A_2 \mathscr{R} (c)A_3 \sim (\widetilde{d})(M_1 \mid C_1[M_2])$$

- (out2-mov). Suppose $C[M] \xrightarrow{out\ abc} L$.
  - C is $a[[\cdot]]$. The only possible situation is that $M \xrightarrow{out\ bc} (\widetilde{d})\langle M_1 \between M_2\rangle$ and $a[M] \xrightarrow{out\ abc} L \equiv (\widetilde{d})(M_1 \mid a[M_2])$. By ind. hyp. over M, we know that $N \Longrightarrow \xrightarrow{out\ bc} (\widetilde{e})\langle N_1 \between N_2\rangle$, and for every context $C_1 \stackrel{\text{def}}{=} f[[\cdot] \mid O]$, it holds that $(\widetilde{e})(N_1 \mid C_1[N_2]) \Longrightarrow \sim \mathscr{R} \sim (\widetilde{d})(M_1 \mid C_1[M_2])$. Taking C_1 as $a[[\cdot] \mid 0]$, we have
$$\begin{aligned} a[N] &\Longrightarrow \xrightarrow{out\ abc} (\widetilde{e})(N_1 \mid a[N_2]) \\ &\Longrightarrow \sim \mathscr{R} \sim (\widetilde{d})(M_1 \mid a[M_2]) \end{aligned}$$
  - C is $[\cdot] \mid O$. In this case, the action must come from M or O.

  (i) If $M \xrightarrow{out\ abc} M'$ and $M \mid O \xrightarrow{out\ abc} M' \mid O \equiv L$. Then by ind. hyp., $N \xRightarrow{out\ abc} N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $N \mid O \xRightarrow{out\ abc} N' \mid O$ and $M' \mid O \sim \mathscr{R} \sim N' \mid O$.

  (ii) If $O \xrightarrow{out\ abc} O'$ and $M \mid O \xrightarrow{out\ abc} M \mid O' \equiv L$. Then $N \mid O \xrightarrow{out\ abc} N \mid O'$, and since $M \mathscr{R} N$, we have $M \mid O' \sim \mathscr{R} \sim N \mid O'$.
  - C is $(d)[\cdot]$. In this case, $(d)M \xrightarrow{out\ abc} L$ because of $M \xrightarrow{out\ abc} M'$ and $L \equiv (d)M'$. By ind. hyp., $N \xRightarrow{out\ abc} N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $(d)N \xRightarrow{out\ abc} (d)N'$ and $(d)M' \sim \mathscr{R} \sim (d)N'$.
- (coout-mov). Suppose $C[M] \xrightarrow{\overline{out}\ abc} L$.
  - C is $c[[\cdot]]$. The only possible situation is that $M \xrightarrow{\overline{out}\ ab} M'$ and $c[M] \xrightarrow{\overline{out}\ abc} L \equiv c[M']$. Then by ind. hyp., $N \xRightarrow{\overline{out}\ ab} N'$ and $M' \sim \mathscr{R} \sim N'$. So $c[N] \xRightarrow{\overline{out}\ abc} c[N']$, and $c[M'] \sim \mathscr{R} \sim c[N']$.
  - C is $[\cdot] \mid O$. In this case, the action must come from M or O.

  (i) If $M \xrightarrow{\overline{out}\ abc} M'$ and $M \mid O \xrightarrow{\overline{out}\ abc} M' \mid O \equiv L$. Then by ind. hyp., $N \xRightarrow{\overline{out}\ abc} N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $N \mid O \xRightarrow{\overline{out}\ abc} N' \mid O$ and $M' \mid O \sim \mathscr{R} \sim N' \mid O$.

  (ii) If $O \xrightarrow{\overline{out}\ abc} O'$ and $M \mid O \xrightarrow{\overline{out}\ abc} M \mid O' \equiv L$. Then $N \mid O \xrightarrow{\overline{out}\ abc} N \mid O'$, and $M \mid O' \sim \mathscr{R} \sim N \mid O'$ since $M \mathscr{R} N$.
  - C is $(d)[\cdot]$. In this case, $(d)M \xrightarrow{\overline{out}\ abc} L$ because of $M \xrightarrow{\overline{out}\ abc} M'$ and $L \equiv (d)M'$. By ind. hyp., $N \xRightarrow{\overline{out}\ abc} N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $(d)N \xRightarrow{\overline{out}\ abc} (d)N'$ and $(d)M' \sim \mathscr{R} \sim (d)N'$.
- (hocom-input). Suppose $C[M] \xrightarrow{ab(A)} L$.
  - C is $a[[\cdot]]$. It must be the situation that $M \xrightarrow{b(A)} M'$ and $a[M] \xrightarrow{ab(A)} L \equiv a[M']$. Then by ind. hyp., $N \xRightarrow{b(A)} N'$ and $M' \sim \mathscr{R} \sim N'$. So $a[N] \xRightarrow{ab(A)} a[N']$, and $a[M'] \sim \mathscr{R} \sim a[N']$
  - C is $[\cdot] \mid O$. In this case, the action must come from M or O.

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

(i) If $M \xrightarrow{ab(A)} M'$ and $M \mid O \xrightarrow{ab(A)} M' \mid O \equiv L$. Then by ind. hyp., $N \xRightarrow{ab(A)} N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $N \mid O \xRightarrow{ab(A)} N' \mid O$ and $M' \mid O \sim \mathscr{R} \sim N' \mid O$.

(ii) If $O \xrightarrow{ab(A)} O'$ and $M \mid O \xrightarrow{ab(A)} M \mid O' \equiv L$. Then $N \mid O \xrightarrow{ab(A)} N \mid O'$, and $M \mid O' \sim \mathscr{R} \sim N \mid O'$ since $M \mathscr{R} N$.

– C is $(d)[\cdot]$. In this case, $(d)M \xrightarrow{ab(A)} L$ because of $M \xrightarrow{ab(A)} M'$ and $L \equiv (d)M'$. By ind. hyp., $N \xRightarrow{ab(A)} N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $(d)N \xRightarrow{ab(A)} (d)N'$ and $(d)M' \sim \mathscr{R} \sim (d)N'$.

- (hocom-res-output). Suppose $C[M] \xrightarrow{(\widetilde{d})\overline{ab}(A)} L$.

– C is $a[[\cdot]]$. In this case, $a[M] \xrightarrow{(\widetilde{d})\overline{ab}(A)} L$ results from $M \xrightarrow{(\widetilde{d})\overline{b}A} M'$ and $L \equiv a[M']$. By ind. hyp., $N \xRightarrow{(\widetilde{e})\overline{b}B} N'$, and for every context $C_1 \stackrel{\text{def}}{=} b[C_1{}']$, name c and O, it holds that

$$(\widetilde{d})(c[M' \mid O] \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e})(c[N' \mid O] \mid C_1[B]) \tag{A4}$$

So we have $a[N] \xRightarrow{(\widetilde{e})\overline{ab}(B)} a[N']$ and need to show that for every context $C_2 \stackrel{\text{def}}{=} b[C_2']$, it holds that

$$(\widetilde{d})(a[M'] \mid C_2[A]) \sim \mathscr{R} \sim (\widetilde{e})(a[N'] \mid C_2[B])$$

which follows from (A4) by taking c as a, O as 0, and C_1 as C_2.

– C is $[\cdot] \mid O$. In this case, the output action must come from M or O.

(i) If the action results from O, then $M \mid O \xrightarrow{(\widetilde{d})\overline{ab}(A)} M \mid O_1 \equiv L$ where $O \xrightarrow{(\widetilde{d})\overline{ab}(A)} O_1$. So we know that $N \mid O \xrightarrow{(\widetilde{d})\overline{ab}(A)} N \mid O_1$. Now for every context $C_1 \stackrel{\text{def}}{=} b[C_1{}']$, we need to show that

$$(\widetilde{d})(M \mid O_1 \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{d})(N \mid O_1 \mid C_1[A])$$

which follows by using $C' \stackrel{\text{def}}{=} [\cdot] \mid (\widetilde{d})(O_1 \mid C_1[A])$ upon $M \mathscr{R}_n N$, that is,

$$(\widetilde{d})(M \mid O_1 \mid C_1[A]) \sim C'[M] \mathscr{R} C'[N] \sim (\widetilde{d})(N \mid O_1 \mid C_1[A])$$

(ii) If this action comes from M, that is, $M \mid O \xrightarrow{(\widetilde{d})\overline{ab}(A)} M' \mid O \equiv L$ where $M \xrightarrow{(\widetilde{d})\overline{ab}(A)} M'$, then by ind. hyp., we know that $N \xRightarrow{(\widetilde{e})\overline{ab}(B)} N'$, and for every context $C_1 \stackrel{\text{def}}{=} b[C_1{}']$, it holds that

$$(\widetilde{d})(M' \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e})(N' \mid C_1[B]) \tag{A5}$$

So $M \mid O \xrightarrow{(\widetilde{d})\overline{ab}(A)} M' \mid O$ can be matched by $N \mid O \xRightarrow{(\widetilde{e})\overline{ab}(B)} N' \mid O$, and we need to show that for every context $C_2 \stackrel{\text{def}}{=} b[C_2']$, it holds that

$$(\widetilde{d})(M' \mid O \mid C_2[A]) \sim \mathscr{R} \sim (\widetilde{e})(N' \mid O \mid C_2[B])$$

From (A5), we know that

$$(\widetilde{d})(M' \mid C_2[A]) \sim M_2 \mathscr{R} N_2 \sim (\widetilde{e})(N' \mid C_2[B])$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

for some M_2 and N_2. Setting $C' \stackrel{\text{def}}{=} C$, we have as needed

$$\begin{aligned}(\widetilde{d})(M' \mid O \mid C_2[A]) &\sim C'[(\widetilde{d})(M' \mid C_2[A])] \\ &\sim C'[M_2] \\ &\mathscr{R}\ C'[N_2] \\ &\sim C'[(\widetilde{e})(N' \mid C_2[B])] \\ &\sim (\widetilde{e})(N' \mid O \mid C_2[B])\end{aligned}$$

– C is $(c)[\cdot]$. In this case, $(c)M \xrightarrow{(\widetilde{d})\overline{ab}(A)} L$ results from $M \xrightarrow{(\widetilde{e})\overline{ab}(A)} M'$. By ind. hyp., we know that $N \xRightarrow{(\widetilde{e'})\overline{ab}(B)} N'$, and for every context $C_1 \stackrel{\text{def}}{=} b[C_1{}']$, it holds that

$$(\widetilde{e})(M' \mid C_1[A]) \sim \mathscr{R} \sim (\widetilde{e'})(N' \mid C_1[B]) \tag{A6}$$

Thus, we immediately know that $(c)N \xRightarrow{(\widetilde{d'})\overline{ab}(B)} L'$. We need to show that for every context $C_2 \stackrel{\text{def}}{=} b[C_2']$, it holds that

$$(\widetilde{d})(L \mid C_2[A]) \sim \mathscr{R} \sim (\widetilde{d'})(L' \mid C_2[B]) \tag{A7}$$

There are four subcases, depending on whether c belongs to $\widetilde{d}$ or not and whether c belongs to $\widetilde{d'}$ or not.

(i) $c \notin \widetilde{d} \cup \widetilde{d'}$, $\widetilde{d}{=}\widetilde{e}$ and $\widetilde{d'}{=}\widetilde{e'}$, and $L \equiv (c)M'$ and $L' \equiv (c)N'$. From (A6), we know that

$$(\widetilde{e})(M' \mid C_2[A]) \sim M'' \mathscr{R} N'' \sim (\widetilde{e'})(N' \mid C_2[B])$$

for some M'' and N''. Assuming no name conflict and setting $C' \stackrel{\text{def}}{=} C$, we have as requested by (A7)

$$\begin{aligned}(\widetilde{d})(L \mid C_2[A]) &\sim (\widetilde{e})((c)M' \mid C_2[A]) \\ &\sim (c)((\widetilde{e})(M' \mid C_2[A])) \\ &\sim C'[(\widetilde{e})(M' \mid C_2[A])] \\ &\sim C'[M''] \\ &\mathscr{R}\ C'[N''] \\ &\sim C'[(\widetilde{e'})(N' \mid C_2[B])] \\ &\sim (\widetilde{d'})((c)N' \mid C_2[B]) \\ &\sim (\widetilde{d'})(L' \mid C_2[B])\end{aligned}$$

(ii) $c \in \widetilde{d} \cap \widetilde{d'}$, $\widetilde{d}{=}\widetilde{e} \cup \{c\}$ and $\widetilde{d'}{=}\widetilde{e'} \cup \{c\}$, and $L \equiv M'$ and $L' \equiv N'$. From (A6), we know that

$$(\widetilde{e})(M' \mid C_2[A]) \sim M'' \mathscr{R} N'' \sim (\widetilde{e'})(N' \mid C_2[B])$$

for some M'' and N''. Setting $C' \stackrel{\text{def}}{=} C$, we have, as requested by (A7)

$$\begin{aligned}(\widetilde{d})(L \mid C_2[A]) &\sim (\widetilde{d})(M' \mid C_2[A]) \\ &\sim (c)((\widetilde{e})(M' \mid C_2[A])) \\ &\sim C'[(\widetilde{e})(M' \mid C_2[A])]\end{aligned}$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

$$\begin{aligned}
&\sim C'[M''] \\
&\mathscr{R}\ C'[N''] \\
&\sim C'[(\widetilde{e'})(N' \mid C_2[B])] \\
&\sim (\widetilde{d'})(L' \mid C_2[B])
\end{aligned}$$

(iii) $c \in \widetilde{d}, \widetilde{d}{=}\widetilde{e} \cup \{c\}$ and $L \equiv M'$; $c \notin \widetilde{d'}, \widetilde{d'}{=}\widetilde{e'}$, and $L' \equiv (c)N'$. Again from (A6), we know that

$$(\widetilde{e})(M' \mid C_2[A]) \sim M'' \mathscr{R} N'' \sim (\widetilde{e'})(N' \mid C_2[B])$$

for some M'' and N''. Setting $C' \stackrel{\text{def}}{=} C$, we have, as requested by (A7)

$$\begin{aligned}
(\widetilde{d})(L \mid C_2[A]) &\sim (\widetilde{d})(M' \mid C_2[A]) \\
&\sim (c)((\widetilde{e})(M' \mid C_2[A])) \\
&\sim C'[(\widetilde{e})(M' \mid C_2[A])] \\
&\sim C'[M''] \\
&\mathscr{R}\ C'[N''] \\
&\sim C'[(\widetilde{e'})(N' \mid C_2[B])] \\
&\sim (\widetilde{d'})((c)N' \mid C_2[B]) \\
&\sim (\widetilde{d'})(L' \mid C_2[B])
\end{aligned}$$

(iv) $c \notin \widetilde{d}, \widetilde{d}{=}\widetilde{e}$, and $L \equiv (c)M$; $c \in \widetilde{d'}, \widetilde{d'}{=}\widetilde{e'} \cup \{c\}$ and $L' \equiv N'$. This is similar to the last subcase.

- (interaction). Suppose $C[M] \xrightarrow{\tau} L$.
  - C is $a[[\cdot]]$. The internal action must come from $M \xrightarrow{\tau} M'$ and $a[M] \xrightarrow{\tau} L \equiv a[M']$. Then by ind. hyp., $N \Longrightarrow N'$ and $M' \sim \mathscr{R} \sim N'$. So $a[N] \Longrightarrow a[N']$, and $a[M'] \sim \mathscr{R} \sim a[N']$.
  - C is $[\cdot] \mid O$. It is certain that the τ action results from M, O, or their interaction. There are quite a few cases depending on where the τ comes from.

(i) (From M alone). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{\tau} M'$ and $L \equiv M' \mid O$. By ind. hyp., $N \Longrightarrow N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $N \mid O \Longrightarrow N' \mid O \stackrel{\text{def}}{=} L'$ and $L \equiv M' \mid O \sim \mathscr{R} \sim N' \mid O \equiv L'$.

(ii) (From O alone). $M \mid O \xrightarrow{\tau} L$ comes from $O \xrightarrow{\tau} O'$ and $L \equiv M \mid O'$. So we have $N \mid O \xrightarrow{\tau} N \mid O' \stackrel{\text{def}}{=} L'$ and $L \equiv M \mid O' \sim \mathscr{R} \sim N \mid O' \equiv L'$ since $M \sim \mathscr{R} \sim N$.

(iii) (From in-movement interaction between M and O: M moves). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{in\ ab} (\widetilde{d})\langle M_1 \between M_2 \rangle$ and $O \xrightarrow{\overline{in}\ ab} C_1$, and $L \equiv (\widetilde{d})(M_2 \mid C_1[M_1])$. By Lemma 2, we know that C_1 is of the form $(\widetilde{f})(b[[\cdot] \mid O_1] \mid O_2)$. By ind. hyp., we have $N \Longrightarrow \xrightarrow{in\ ab} (\widetilde{e})\langle N_1 \between N_2 \rangle$, and for every context $C_2 \stackrel{\text{def}}{=} b[[\cdot] \mid O_3]$, it holds that

$$(\widetilde{e})(N_2 \mid C_2[N_1]) \Longrightarrow \sim \mathscr{R} \sim (\widetilde{d})(M_2 \mid C_2[M_1])$$

Taking O_3 as O_1, we have for some N_3, N_4 and M_3 that

$$(\widetilde{e})(N_2 \mid b[N_1 \mid O_1]) \Longrightarrow N_3 \sim N_4 \mathscr{R} M_3 \sim (\widetilde{d})(M_2 \mid b[M_1 \mid O_1])$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

So we infer that $N \mid O \Longrightarrow \xrightarrow{\tau} (\widetilde{e})(N_2 \mid C_1[N_1])$, and moreover

$$\begin{aligned}(\widetilde{e})(N_2 \mid C_1[N_1]) &\equiv (\widetilde{e})(N_2 \mid (\widetilde{f})(b[N_1 \mid O_1] \mid O_2)) \\ &\equiv (\widetilde{e})(\widetilde{f})(N_2 \mid b[N_1 \mid O_1] \mid O_2)) \\ &\Longrightarrow (\widetilde{f})(N_3 \mid O_2)) \\ &\sim (\widetilde{f})(N_4 \mid O_2)) \\ &\mathscr{R} (\widetilde{f})(M_3 \mid O_2)) \\ &\sim (\widetilde{d})(\widetilde{f})(M_2 \mid b[M_1 \mid O_1] \mid O_2) \\ &\sim (\widetilde{d})(M_2 \mid C_1[M_1]) \equiv L\end{aligned}$$

In summary, we have $N \mid O \Longrightarrow \sim \mathscr{R} \sim L$, as desired.

(iv) (From in-movement interaction between M and O: O moves). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{\overline{in}\, ab} C_1$ and $O \xrightarrow{in\, ab} (\widetilde{d})\langle O_1 \between O_2\rangle$, and $L \equiv (\widetilde{d})(O_2 \mid C_1[O_1])$. By Lemma 2, we know that O_1 is of the form $a[O_3]$ for some O_3. By ind. hyp., $N \Longrightarrow \xrightarrow{\overline{in}\, ab} C_2$, and for every A, it holds that $C_2[a[A]] \Longrightarrow \sim \mathscr{R} \sim C_1[a[A]]$. Taking A as O_3, we have for some O_4, O_5 and O_6 that

$$C_2[a[O_3]] \Longrightarrow O_4 \sim O_5 \,\mathscr{R}\, O_6 \sim C_1[a[O_3]]$$

So we know that $N \mid O \Longrightarrow \xrightarrow{\tau} (\widetilde{d})(O_2 \mid C_2[O_1])$, and moreover

$$\begin{aligned}(\widetilde{d})(O_2 \mid C_2[O_1]) &\equiv (\widetilde{d})(O_2 \mid C_2[a[O_3]]) \\ &\Longrightarrow (\widetilde{d})(O_2 \mid O_4) \\ &\sim (\widetilde{d})(O_2 \mid O_5) \\ &\mathscr{R} (\widetilde{d})(O_2 \mid O_6) \\ &\sim (\widetilde{d})(O_2 \mid C_1[a[O_3]]) \equiv L\end{aligned}$$

In summary, we have $N \mid O \Longrightarrow \sim \mathscr{R} \sim L$.

(v) (From out-movement interaction between M and O: M moves). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{out\, abc} M'$ and $O \xrightarrow{\overline{out}\, abc} O'$, and $L \equiv M' \mid O'$. By ind. hyp., $N \xrightarrow{out\, abc} N'$ and $M' \sim \mathscr{R} \sim N'$. So we infer that $N \mid O \Longrightarrow N' \mid O' \stackrel{\text{def}}{=} L'$ and $L \equiv M' \mid O' \sim \mathscr{R} \sim N' \mid O' \equiv L'$.

(vi) (From out-movement interaction between M and O: O moves). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{\overline{out}\, abc} M'$ and $O \xrightarrow{out\, abc} O'$, and $L \equiv M' \mid O'$. By ind. hyp., $N \xrightarrow{\overline{out}\, abc} N'$ and $M' \sim \mathscr{R} \sim N'$. So we infer that $N \mid O \Longrightarrow N' \mid O' \stackrel{\text{def}}{=} L'$ and $L \equiv M' \mid O' \sim \mathscr{R} \sim N' \mid O' \equiv L'$.

(vii) (From HO communication between M and O: M outputs). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{(\widetilde{d})\overline{ab}(A)} M'$ and $O \xrightarrow{ba(A)} O'$, and $L \equiv (\widetilde{d})(M' \mid O')$. By Lemma 2, $O' \equiv (\widetilde{f})(b[C_1[A]] \mid O_1)$ for some context $C_1, \widetilde{f}$ and O_1. By ind. hyp., $N \xrightarrow{(\widetilde{e})\overline{ab}(B)} N'$, and for every context $C_2 \stackrel{\text{def}}{=} b[C_2']$ that incurs no name conflict, it holds that

$$(\widetilde{d})(M' \mid C_2[A]) \sim \mathscr{R} \sim (\widetilde{e})(N' \mid C_2[B])$$

So we infer that $N \mid O \Longrightarrow (\widetilde{e})(N' \mid O'') \stackrel{\text{def}}{=} L'$ in which $O'' \equiv (\widetilde{f})(b[C_1[B]] \mid O_1)$, and taking C_2' above as C_1 leads to

$$(\widetilde{d})(M' \mid b[C_1[A]]) \sim O_2 \,\mathscr{R}\, O_3 \sim (\widetilde{e})(N' \mid b[C_1[B]])$$

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press

Thus, we have

$$\begin{aligned} L \equiv (\widetilde{d})(M' \mid (\widetilde{f})(b[C_1[A]] \mid O_1)) &\sim (\widetilde{f})((\widetilde{d})(M' \mid b[C_1[A]]) \mid O_1) \\ &\sim (\widetilde{f})(O_2 \mid O_1) \\ &\mathscr{R} (\widetilde{f})(O_3 \mid O_1) \\ &\sim (\widetilde{f})((\widetilde{e})(N' \mid b[C_1[B]]) \mid O_1) \\ &\sim (\widetilde{e})(N' \mid (\widetilde{f})(b[C_1[B]] \mid O_1)) \equiv L' \end{aligned}$$

(viii) (From HO communication between M and O: O outputs). $M \mid O \xrightarrow{\tau} L$ comes from $M \xrightarrow{ba(A)} M'$ and $O \xrightarrow{(\widetilde{d})\overline{ab}(A)} O'$, and $L \equiv (\widetilde{d})(M' \mid O')$. By ind. hyp., $N \xrightarrow{ba(A)} N'$ and $M' \sim \mathscr{R} \sim N'$. So we infer that $N \mid O \xRightarrow{\tau} (\widetilde{d})(N' \mid O') \stackrel{\text{def}}{=} L'$, and since $M' \sim \mathscr{R} \sim N'$, we have

$$L \equiv (\widetilde{d})(M' \mid O') \sim \mathscr{R} \sim (\widetilde{d})(N' \mid O') \equiv L'$$

– C is $(d)[\cdot]$. In this case, $(d)M \xrightarrow{\tau} L$ because of $M \xrightarrow{\tau} M'$ and $L \equiv (d)M'$. By ind. hyp., $N \Longrightarrow N'$ and $M' \sim \mathscr{R} \sim N'$. So we have $(d)N \Longrightarrow (d)N'$ and $(d)M' \sim \mathscr{R} \sim (d)N'$.

The proof is now completed. □

Cite this article: Xu X, Huang Y and Yao Z (2025). On higher-order communication in ambient calculi. *Mathematical Structures in Computer Science* **35**(e2), 1–55. https://doi.org/10.1017/S0960129525000015

https://doi.org/10.1017/S0960129525000015 Published online by Cambridge University Press