Electronic Notes in Theoretical Computer Science 66 No. 3 (2002)
URL: http://www.elsevier.nl/locate/entcs/volume66.html 15 pages

Barbs and Congruences for Safe Mobile Ambients

M.G. Vigliotti [1,2] I.C.C. Phillips [3]

Department of Computing
Imperial College
London, UK

Abstract

The Ambient Calculus offers many ways in which processes can interact and be observed. In the context of Levi and Sangiorgi's Safe Mobile Ambients (SA), the extra *co-capabilities* required for interaction complicate the fundamental observations. We show that different formulations of barbs lead to the same barbed congruence. We prove this by following Honda and Yoshida's approach for the π-calculus by defining the insensitive terms of SA.

1 Introduction

The pervasive presence of the Internet has forced the computer science community to rethink existing assumptions about physical versus virtual boundaries and mobile code in distributed computation [1]. The Ambient Calculus (AC) has been introduced as a new model for distributed mobile computation, that takes into consideration the reality of the World Wide Web, where division into administrative domains as logical boundaries requires the handling of both *mobile code* and *authorisation*. The AC deals with mobile code via simple *movements*. Ambients, which are meant to represent administrative domains, have a tree structure possibly containing sub-ambients; the notion of access and mobility is captured by the operational semantics, where processes equipped with suitable capability can freely enter or exit an ambient or dissolve ambient boundaries. In [7] Levi and Sangiorgi argued that the basic operational semantics for AC led to the phenomenon of 'grave interference' (different from standard interference which is a common phenomenon in concurrency), where two or more redexes of different 'natures' 'destroy' each other.

[1] Fully supported by an *EPSRC* Ph.D grant.
[2] Email: mgv98@doc.ic.ac.uk
[3] Email: iccp@doc.ic.ac.uk

Grave interference makes reasoning on programming much more difficult as well stated in [7]. In order to overcome this problem, Levi and Sangiorgi proposed Safe Ambients (SA) [7] as a calculus that keeps the same computational model as AC, but enhance the ambient primitives with *co-capabilities*. In this new setting, reduction is synchronous, in the sense that it requires *two* parties to be equipped with the right capability (resp. co-capability). For SA [7] a labelled transition system has been proposed but not a labelled bisimulation. Barbed bisimulation as in [9,12] has been proposed as equivalence.

A successful definition of labelled bisimulation has been developed for a dialect of SA, Safe Ambients with passwords (SAP) [10], where primitives of the language have been modified in order to make the definitions work. The main result regards the identification of the labelled bisimulation with the contextual bisimulation. Contextual barbed bisimulation is to be distinguished from the congruence obtained from barbed bisimulation equivalence [9,12].

This former equivalence is defined in [10] in an operational way. Originally contextual barbed bisimulation was born in a π-calculus setting [6] and it was recovered via an equational approach. It is a natural question, to ask whether the equational approach would work in the SA setting just as well. The main contribution of the paper is to show that indeed this is the case.

Recovering contextual bisimulation requires the definition of a equivalence relation which goes under the name of *sound theory*. A sound theory is a non trivial relation (in the sense that does not relate all the terms) that is preserved by contexts and reductions, it contains structural congruence and identifies insignificant processes: *insensitive terms*. Insensitive terms are invisible terms, in the sense that they never interact with any context. The definition of insensitive terms in the SA setting is far from being easy or trivial, but we will show that our definition although complicated works. The definition requires an elaborate analysis of free names of a process, but at the end of this construction we will be able to prove that the union of all sound theories is sound and coincides with the contextual barbed bisimulation. One of the advantages of our approach is that we do not have to commit ourselves *a priori* to any kind of observational predicate, or *barb*. The AC offers many ways in which processes can interact (since processes are equipped with capabilities for entering, exiting, and opening ambients). This means that there can be a variety of choices for the fundamental observations (i.e. the barbs) on which equivalences are based. In [2] the choice of observing a top level ambient was made, and in [11] we were able to justify the original choice of barb by using the Honda-Yoshida technique, where barbs are *induced a posteriori*. In the case of SA, there is more uncertainty about the correct choice of barb, since the extra co-capabilities increase the number of possible barbs. This motivates more strongly the need to find an approach which does not depend on a particular form of barb, which is the advantage of the Honda-Yoshida construction. Moreover we will show that our construction with a small modification can be applied to Merro and Hennessy's Safe Ambients

$P, Q ::=$		processes	$M ::=$		capabilities
	$\mathbf{0}$	inactivity	|	$\mathrm{in}\, n$	enter n
|	$!P$	replication	|	$\mathrm{out}\, n$	exit n
|	$P \mid Q$	composition	|	$\mathrm{open}\, n$	open n
|	$(\nu\ x)P$	restriction	|	$\overline{\mathrm{in}}\, n$	be entered n
|	$n\ [P]$	ambient	|	$\overline{\mathrm{out}}\, n$	be exit n
|	$M.P$	action	|	$\overline{\mathrm{open}}\, n$	be opened

Fig. 1. Processes and Capabilities

with Passwords (SAP), and in that particular setting, where primitives for exiting an ambient are changed, we will see that there is one more barb.

The rest of the paper is organised as follows: in Section 2 we recall the syntax of Safe Ambients; in Section 3 we introduce the sound theories and construct the maximal sound theory, the main result is Theorem 3.17; in Section 4 we see that different barbs are properties of any sound theory and that there is an operational definition of maximal sound theory (Theorem 4.2); moreover we prove Theorem 2.8 which claims that different barbed equivalences coincide; in Section 5 we briefly show that the same method can be applied to SAP, and conclusions follow.

2 The syntax of Safe Ambients

In this section we recall the primitives for Safe Ambient Calculus [7]. We assume there is an infinite set of names $\mathcal{N}$, ranged over by $n, m, q, r, \ldots$.

The syntax of the calculus can be found in Figure 1. We omit the primitives of communication, since we prefer to focus on the semantic techniques. The result of this paper can be extended to the primitives of communication similarly to [11]. There follows an intuitive explanation of the syntax. $\mathbf{0}$ stands for the inactive process, $!P$ simulates recursion by spinning off copies of P, $(P \mid Q)$ is the composition of two processes, $(\nu\ x)P$ (restriction) creates a new name n in P, $n\ [P]$ is the ambient n containing the active process P and $M.P$ is the process P guarded by the capability M. The meaning of the capabilities is intuitively the following: $\mathrm{open}\, n.\mathbf{0}$ dissolves an ambient with name n; $\mathrm{in}\, n$ and $\mathrm{out}\, n.\mathbf{0}$, are primitives which can be exercised within an ambient only; $\mathrm{in}\, n.\mathbf{0}$ allows the surrounding an ambient to enter another ambient with name n; $\mathrm{out}\, n.\mathbf{0}$ allows the surrounding an ambient to leave the ambient with name n. The co-capabilities express that the ambient is actively taking part in the computation: $\overline{\mathrm{out}}\, n.\mathbf{0}$ expresses that an ambient n is willing to release

$$
\begin{aligned}
m\ [\mathrm{in}\, n.P_1 \mid P_2] \mid n\ [\overline{\mathrm{in}}\, n.Q_1 \mid Q_2] &\longrightarrow n\ [Q_1 \mid Q_2 \mid m\ [P_1 \mid P_2]] \\
n\ [m\ [\mathrm{out}\, n.Q_1 \mid Q_2] \mid \overline{\mathrm{out}}\, n.P_1 \mid P_2] &\longrightarrow n\ [P_2 \mid P_2] \mid m\ [Q_1 \mid Q_2] \\
\mathrm{open}\, n.P \mid n\ [\overline{\mathrm{open}}\, n.Q_1 \mid Q_2] &\longrightarrow P \mid Q_1 \mid Q_2 \\
P \longrightarrow Q &\implies P \mid R \longrightarrow Q \mid R \\
P \longrightarrow Q &\implies n\ [P] \longrightarrow n\ [Q] \\
P \longrightarrow Q &\implies (\nu\ n)P \longrightarrow (\nu\ n)Q \\
P \equiv P' \longrightarrow Q' \equiv Q &\implies P \longrightarrow Q
\end{aligned}
$$

Fig. 2. Reduction Relation

$$
\begin{aligned}
P \mid \mathbf{0} &\equiv P \\
P \mid Q &\equiv Q \mid P \\
(P \mid Q) \mid R &\equiv Q \mid (P \mid R) \\
(\nu\ y)\mathbf{0} &\equiv \mathbf{0} \\
(\nu\ m)(\nu\ n)P &\equiv (\nu\ n)(\nu\ m)P \\
(\nu\ n)(P \mid Q) &\equiv P \mid (\nu\ n)Q \quad \text{if } n \notin fn(P) \\
(\nu\ m)n\ [P] &\equiv n\ [(\nu\ m)P] \quad \text{if } n \neq m \\
!P &\equiv P \mid\ !P \\
!\mathbf{0} &\equiv \mathbf{0}
\end{aligned}
$$

Fig. 3. Structural Congruence

an internal one, $\overline{\mathrm{in}}\, n.\mathbf{0}$ expresses that an ambient n is willing to accept another entering ambient and $\overline{\mathrm{open}}\, n$ expresses that an ambient n can be opened. The set of free names of P is written $fn(P)$ and is defined in the standard way, taking into account that the only binding operator is restriction. We will omit the final $\mathbf{0}$, writing M rather than $M.\mathbf{0}$. Computation is formally captured by the formal definition of the *reduction relation* $P \longrightarrow P'$, which is the smallest relation as defined in Figure 2. The reflexive and transitive closure is written as $\longrightarrow\!\!\!\!\!\rightarrow$. Structural congruence $\equiv$ identifies processes that we do not want to tell apart for any semantic reason. It is the least congruence relation as defined in Figure 3.

Contextual equivalence, as given in [2], equates two processes that admit the same observation or *barb*, in any *context*. A *context* $\mathcal{C}\{\}$ is simply a process with zero or more holes $\{\}$. $\mathcal{C}\{Q\}$ denotes the result of filling the hole $\{\ \}$ in context $\mathcal{C}$ with process Q. Free variables of the process can become bound

in the context, therefore contexts are not identified up to renaming of bound variables.

We shall need the following notation.

Definition 2.1 [Barbs]

- $P \downarrow \overline{open\ n}$ iff $P \equiv (\nu\ p_1 \dots p_n)(n\ [\overline{\text{open}}\, n.P_1 \mid P_2] \mid P_3)$ and $n \notin \{p_1 \dots p_n\}$;
- $P \downarrow \overline{in\ n}$ iff $P \equiv (\nu\ p_1 \dots p_n)(n\ [\overline{\text{in}}\, n.P_1 \mid P_2] \mid P_3)$ and $n \notin \{p_1 \dots p_n\}$;
- $P \downarrow in\ n$ iff $P \equiv (\nu\ p_1 \dots p_n)(q\ [\text{in}\, n.P_1 \mid P_2] \mid P_3)$ and $n \notin \{p_1 \dots p_n\}$;
- $P \downarrow out\ n$ iff $P \equiv (\nu\ p_1 \dots p_n)(q\ [\text{out}\, n.P_1 \mid P_2] \mid P_3)$ and $n \notin \{p_1 \dots p_n\}$;
- $P \downarrow open\ n$ iff $P \equiv (\nu\ p_1 \dots p_n)(\text{open}\, n.P_1 \mid P_2)$ and $n \notin \{p_1 \dots p_n\}$;

As usual in the literature, we write $P \Downarrow b$ for the weak observational predicate, if $P \longrightarrow\!\!\!\!\!\rightarrow P' \downarrow b$, where b is metavariable referring to any of barbs defined in Definition 2.1.

In [7] the barb $P \downarrow n$ is defined in order to yield the definition of *barbed congruence*. This predicate can be defined $P \downarrow n$ iff $P \downarrow \overline{open\ n}$ or $P \downarrow \overline{in\ n}$.

Definition 2.2 [Contextual Equivalence]

Two processes P, Q are said to be *contextual equivalent* $P \simeq Q$, if for all names n and all contexts $\mathcal{C}$, $\mathcal{C}\{P\} \Downarrow n$ if and only if $\mathcal{C}\{Q\} \Downarrow n$.

Definition 2.3 [Barbed Bisimulation] A symmetric relation $\mathcal{S}$ over processes is a *weak barbed bisimulation* (WBB) if $P\ \mathcal{S}\ Q$:

- if $P \downarrow n$ then $Q \Downarrow n$;
- if $P \longrightarrow P'$ then for some Q', $Q \longrightarrow\!\!\!\!\!\rightarrow Q'$ and $P'\ \mathcal{S}\ Q'$.

Definition 2.4 Two processes P, Q are said to be *weakly barbed equivalent* $P \approx_b Q$ if there exists $\mathcal{S}$, a weak barbed bisimulation, such that $P\ \mathcal{S}\ Q$.

Two processes P, Q are said to be *barbed congruent* $P \approx_b^c Q$ iff for all contexts $\mathcal{C}$, it holds that $\mathcal{C}\{P\} \approx_b \mathcal{C}\{Q\}$.

Definition 2.5 [Contextual Barbed Bisimulation] A symmetric relation $\mathcal{S}$, is a *contextual barbed bisimulation* (CBB) if whenever $P\ \mathcal{S}\ Q$ then for any n and contexts $\mathcal{C}$:

- if $\mathcal{C}\{P\} \downarrow \overline{open\ n}$ then $\mathcal{C}\{Q\} \Downarrow \overline{open\ n}$;
- if $\mathcal{C}\{P\} \longrightarrow P'$ then for some Q', $\mathcal{C}\{Q\} \longrightarrow\!\!\!\!\!\rightarrow Q'$ and $P'\ \mathcal{S}\ Q'$

Definition 2.6 Two processes P, Q are said to be *contextual barbed equivalent* $P \approx Q$ if there exists $\mathcal{S}$, a contextual bisimulation, such that $P\ \mathcal{S}\ Q$.

The relation $\approx$ is by a standard argument the largest bisimulation. The following theorem simply firms up the hierarchy among the equivalences defined above.

Theorem 2.7 $\equiv\ \subseteq \approx \subseteq\ \approx_b^c\ \subseteq \simeq$

In the previous section we have defined the different barbs (Definition 2.1), which give different definitions of bisimulation. We write $\approx^{\overline{in}}$ for a contextual congruence whose barb is $\overline{\text{in}}\,\text{n}$, similarly for the other barbs and equivalences $\approx^{in}$,$\approx^{out}$,$\approx^{open}$(there is no need of $\approx^{\overline{open}}$ since this equal to $\approx$ as in Definition 2.5). The main task of this paper is to prove the following theorem, which essentially states that all different congruences coincide.

Theorem 2.8 $\approx = \approx^{\overline{in}} = \approx^{in} = \approx^{out} = \approx^{open}$.

The novelty of this paper is the proof methods that we are going to use for the previous result. Instead of relying on the operational definition only, we will use the Honda-Yoshida [6] framework. The proof relies on the following ingredients, that can be found later in the paper:

(i) definition of sound theory and preservation of the barb $\overline{\text{in}}\,n$, for all n, by any sound theory;

(ii) proof of the soundness of the union of all sound theories and proof of the equivalence with the contextual equivalence ;

(iii) proof that any sound theory preserves all barbs . Since the union of all sound theories is sound, it also preserves all the barbs;

(iv) the union of all sound theories with one barb is equivalent to the corresponding contextual barbed equivalence equipped with the corresponding barb ;

(v) it follows that all the contextual barbed equivalences coincide because the union of all sound theories is unique.

The details of the proof are to be found at the end of Section 4.

3 Sound theories

Following the Honda and Yoshida method [6], we are going to define the notion of *sound theory* for SA. First of all, an *ambient theory*, or simply a theory $\mathcal{T}_A$ is an equivalence relation that is closed under all contexts and contains at least structural congruence. As such an ambient theory is very weak, indeed in order to go from theory to *sound theory* we need to specify some other constraints.

Definition 3.1 An ambient theory is *sound* if:

- it contains structural congruence;
- it is consistent;
- it is reduction closed;
- it identifies all the insensitive terms.

We shall deem two processes to be equivalent if they are equated in some sound theory. We let $\mathcal{T}$ range over sound theories. We will say that $\mathcal{T} \vdash P = Q$

if $P = Q$ is derivable in $\mathcal{T}$, and $\mathcal{T} \nvdash P = Q$ otherwise. We will write $P = Q$, $P \neq Q$ when it is clear from the context which particular theory we are referring to.

3.1 Consistency and reduction closure

We continue the presentation of the sound theory. *Consistency* guarantees that the theory is not trivial, i.e. there exists a pair of terms that is not identified in the theory. *Reduction closure* preserves that equality relation through reduction.

Definition 3.2 An ambient theory is *consistent* if not all processes are identified in the theory.

Definition 3.3 An ambient theory is *reduction closed* if whenever $P = Q$ and $P \longrightarrow\!\!\!\!\!\rightarrow P'$ then there exists a Q' such that $Q \longrightarrow\!\!\!\!\!\rightarrow Q'$ and $P' = Q'$.

3.2 Insensitive terms

An insensitive process (or term) is one which can never react with its environment or the surrounding *context*. In order to define insensitive terms, we need to talk about special set of free names of a term: *active names*. To explain active names, it is necessary to specify the role of names in the reduction relation. Take the term $R = \mathrm{open}\, n.P$. R may react with a context $n\ [\overline{\mathrm{open}}\, n.Q]$ but *not* with $q\ [\overline{\mathrm{open}}\, q.Q]$. Therefore, the name n plays a fundamental role in the reduction. Following this clue, we will define *insensitive terms* according to some observations on a subset of the free names of a process: the *active names*. As in the example before, active names in a term P are the ones that allow P to immediately engage in a reduction with a context. A term is insensitive if for all of its derivatives (including itself) the set of active names (i.e. the vehicle for engaging reduction) is empty. It is important to observe that not all free names of a process are active. For instance n is active in $n\ [\overline{\mathrm{open}}\, n.P]$ but the free names of P are not active. More subtly, n is active in $\mathrm{open}\, n.P$ and $m\ [\mathrm{in}\, n.P]$, but not in $q\ [\mathrm{open}\, n]$ and not in $p\ [\overline{\mathrm{in}}\, n.]$. In order to achieve this fine distinction, we need to define first the *mobile names* (Definition 3.4). Mobile names enable an ambient to move in or out, for example the name q in $n\ [\mathrm{out}\, q.Q]$. Then we are going to define the notion of *enabling names* (Definition 3.5), which are the names that enable an ambient to be entered, opened such as n in $n\ [\overline{\mathrm{in}}\, n.P]$. On top of these two definitions, we will define the active names (Definition 3.6). Notice that $\mathrm{in}\, n.P$ is mobile as well as active unlike $\mathrm{open}\, n.P$ and that $\overline{\mathrm{open}}\, n.P$ is active and enabling unlike $\overline{\mathrm{out}}\, n.P$ which is only active.

Definition 3.4 [Mobile Names]. The set of *mobile names* of a process P is

defined as follows:

$$\begin{aligned} mn(\mathbf{0}) &= \emptyset & mn(\overline{\text{in}}\, n.P) &= \emptyset \\ mn(\text{in}\, n.P) &= \{n\} & mn(\overline{\text{out}}\, n.P) &= \emptyset \\ mn(\text{out}\, n.P) &= \{n\} & mn(\overline{\text{open}}\, n.P) &= \emptyset \\ mn(\text{open}\, n.P) &= \emptyset & mn(!P) &= mn(P) \\ mn(n\ [P]) &= \emptyset & mn((\nu\ n)P) &= mn(P) - \{n\} \\ mn(P \mid Q) &= mn(P) \cup mn(Q) \end{aligned}$$

Definition 3.5 [Enabling Names] The set of *enabling names* of a process P is defined as follows:

$$\begin{aligned} en(\mathbf{0}) &= \emptyset & en(\overline{\text{in}}\, n.P) &= \{n\} \\ en(\text{in}\, n.P) &= \emptyset & en(\overline{\text{out}}\, n.P) &= \emptyset \\ en(\text{out}\, n.P) &= \emptyset & en(\overline{\text{open}}\, n.P) &= \{n\} \\ en(\text{open}\, n.P) &= \emptyset & en(!P) &= en(P) \\ en(n\ [P]) &= \emptyset & en((\nu\ n)P) &= en(P) - \{n\} \\ en(P \mid Q) &= en(P) \cup en(Q) \end{aligned}$$

Definition 3.6 [Active Names] The set of *active names* of a process P is defined as follows:

$$\begin{aligned} an(\mathbf{0}) &= \emptyset & an(\overline{\text{in}}\, n.P) &= \{n\} \\ an(\text{in}\, n.P) &= \{n\} & an(\overline{\text{out}}\, n.P) &= \{n\} \\ an(\text{out}\, n.P) &= \{n\} & an(\overline{\text{open}}\, n.P) &= \{n\} \\ an(\text{open}\, n.P) &= \{n\} & an(!P) &= an(P) \\ an(P \mid Q) &= an(P) \cup an(P) & an((\nu\ n)P) &= an(P) - \{n\} \\ an(n\ [P]) &= (\{n\} \cap en(P)) \cup mn(P) \end{aligned}$$

It is clear that $an(P) \subseteq fn(P)$. We are now ready to give the definition of insensitive terms. A term is insensitive if it never interacts with the environment. Obviously, no active names should be present, as the following definition formalises.

Definition 3.7 [6] A process P is *insensitive* if $an(P') = \emptyset$ for all P' such that $P \longrightarrow\!\!\!\!\!\rightarrow P'$.

Example 3.8 The following are examples of insensitive terms:

- $(\nu\ p_1 \dots p_n)(P)$ where $fn(P) \subseteq \{p_1 \dots p_n\}$;
- $(\nu\ n)(\text{in}\, n.P)$;

- $w\ [\mathrm{open}\, r]$;
- $(\nu\ q)(n\ [!\mathrm{in}\, q.\mathrm{out}\, q] \mid q\ [!\overline{\mathrm{in}}\, q \mid !\overline{\mathrm{out}}\, q])$;

The following lemmas state that insensitive processes have no barbs, are closed under structural congruence, and do not interact with surrounding contexts.

Lemma 3.9

(i) *If* $P \equiv Q$ *then* $an(P) = an(Q)$.

(ii) *If* U *is insensitive and* $U \equiv P$ *then* P *is insensitive.*

(iii) *If* U *is insensitive and* $U \longrightarrow\!\!\!\!\!\rightarrow\ U'$ *then* U' *is insensitive.*

Lemma 3.10 *If* $an(P) = \emptyset$ *then* P *has no barbs.*

Lemma 3.11 ([6]) *Let* U *be insensitive and* $\mathcal{C}\{\}$ *be a context.*
If $\mathcal{C}\{U\} \longrightarrow\!\!\!\!\!\rightarrow\ R$ *then* $R \equiv \mathcal{C}'\{U'\}$ *where* $\mathcal{C} \longrightarrow\!\!\!\!\!\rightarrow\ \mathcal{C}'$ *and* $U \longrightarrow\!\!\!\!\!\rightarrow\ U'$ *and* U' *is insensitive.*

Notice that insensitive terms are not equivalent to terms without barbs. It is true, as stated above that insensitive terms have no barbs, but not all terms without barbs are insensitive, for instance take $\mathrm{in}\, q.P$. At the end of this article one could interpret our work as a deeper understanding of the nature of barb. Insensitive terms and consistency are necessary in order to fully characterise the simple notion of barb, but this will become clearer in the end of next section.

We are going to prove that there exists at least one sound theory, moreover it is the minimal sound theory.

Definition 3.12 Let $\mathcal{T}_{Ins}$ be the theory generated by $\equiv$ and identifying all the insensitive processes.

We shall see that $\mathcal{T}_{Ins}$ is sound.

Lemma 3.13 *If* $\mathcal{T}_{Ins} \vdash P = Q$ *then for all* n, *if* $P \Downarrow \overline{open\ n}$ *then* $Q \Downarrow \overline{open\ n}$.

Clearly a theory $\mathcal{T}$ that preserves (weak) barbs (as in the previous theorem) must be consistent since $\mathcal{T} \not\vdash n\ [\overline{\mathrm{open}}\, n\ ] = \mathbf{0}$.

Lemma 3.14 $\mathcal{T}_{Ins}$ *is sound.*

Proof. By construction, $\equiv$ is included and the insensitive terms are identified. Reduction closure follows from the definition of $\longrightarrow$, in the case of $\equiv$; in the case of the laws identifying the insensitive terms, suppose that $\mathcal{C}\{U\} = \mathcal{C}\{V\}$. Then by Lemma 3.11 we have that if $\mathcal{C}\{U\}$ reacts (in one step) either $C\{\ \}$ reacts in which case can be imitated by the context in $\mathcal{C}\{V\}$; or it is U which reacts, $U \longrightarrow U'$, and U' is still insensitive in which case $\mathcal{C}\{V\} \longrightarrow\!\!\!\!\!\rightarrow\ \mathcal{C}\{V\}$. By Lemma 3.13 $n\ [\overline{\mathrm{open}}\, n\ ] \neq \mathbf{0}$, therefore $\mathcal{T}_{Ins}$ is consistent. □

3.3 Observable in a sound theory

A sound theory in general may be more generous, in the sense that it may equate more processes, therefore it is not trivial or automatic that *any* sound theory $\mathcal{T}$ preserves weak barbs. Indeed this is the core of the paper, whose proof relies heavily on the fact that a sound theory is consistent, unlike the proof of Lemma 3.14 where consistency was a consequence of the preservation of the barbs. The following two results aim precisely to show that sound theories admit at least one barb $n\ [\overline{\text{in}}\, n]$, for all n. Moreover, they are not a mere adaptation of the corresponding results [6]. Indeed, the use of consistency and insensitive terms is crucial as in [6], but due to the complexity of the SA, the proofs are more delicate, in the sense that requires more detailed case analysis.

Lemma 3.15 (Incompatible pairs [6]) *Let $\mathcal{T}$ be a sound theory. Then, $n\ [\overline{\text{in}}\, n\ ] \neq\ \mathbf{0}$, for all n.*

Proof. By contradiction, assume that $m\ [\overline{\text{in}}\, m] =\ \mathbf{0}$, for some m. First we prove that for all z, $z\ [\overline{\text{in}}\, z] =\ \mathbf{0}$. Then we prove inconsistency. Assume some m, $m\ [\overline{\text{in}}\, m] = \mathbf{0}$, then without loss of generality, a context is created with $s \neq q \neq m$:

$$q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s] \mid \text{in}\, m] \mid m\ [\overline{\text{in}}\, m] =\ q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s] \mid \text{in}\, m] \mid \mathbf{0}.$$

For sake of readability we denote:

$$F = q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s] \mid \text{in}\, m] \mid m\ [\overline{\text{in}}\, m].$$
$$S = q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s] \mid \text{in}\, m] \mid \mathbf{0}.$$

By reduction closure the following hold:

$$F \longrightarrow m\ [q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s]]].$$
$$m\ [q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s]]] =\ S.$$

Considering the context $\text{open}\, q \mid \{\}$ the following holds:

$$m\ [q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s]]] \mid \text{open}\, q =\ q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s] \mid \text{in}\, m] \mid \text{open}\, q.$$

The right-hand side of the previous equation reduces as follows:

$$q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s] \mid \text{in}\, m] \mid \text{open}\, q \longrightarrow s\ [\overline{\text{in}}\, s] \mid \text{in}\, m$$

By reduction closure the following chain of equations hold:

$$\begin{aligned}
s\ [\overline{\text{in}}\, s] \mid \text{in}\, m &= m\ [q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s]]] \mid \text{open}\, q \\
(\nu\ mq)(s\ [\overline{\text{in}}\, s] \mid \text{in}\, m) &= (\nu\ mq)(m\ [q\ [\overline{\text{open}}\, q.s\ [\overline{\text{in}}\, s]]] \mid \text{open}\, q) \\
s\ [\overline{\text{in}}\, s] \mid (\nu\ mq)(\text{in}\, m) &= (\nu\ mq)(m\ [q\ [\overline{\text{open}}\, q.s\ [\text{in}\, s]]] \mid \text{open}\, q) \\
s\ [\overline{\text{in}}\, s] \mid \mathbf{0} &= \mathbf{0}.
\end{aligned}$$

This concludes the first part of the proof. Now we prove inconsistency. Since for all m, $m\ [\overline{\text{in}}\, m] = \mathbf{0}$, then take the context $q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m] \mid \{\ \}$ with

$q, m \notin fn(P)$, then the following holds:

$$q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m] \mid m\ [\overline{\text{in}}\, m] = \ q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m] \mid \mathbf{0}.$$

The left-hand side term of the previous equality reduces as follows:

$$q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m] \mid m\ [\overline{\text{in}}\, m] \longrightarrow m\ [q\ [\overline{\text{open}}\, q.P]].$$

By properties of $\mathcal{T}$ the following holds:

$$\begin{aligned} m\ [q\ [\overline{\text{open}}\, q.P]] &= q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m] \\ (\nu\ qm)(\text{open}\, q \mid m\ [q\ [\overline{\text{open}}\, q.P]]) &= (\nu\ qm)(\text{open}\, q \mid q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m]) \\ \mathbf{0} &= (\nu\ qm)(\text{open}\, q \mid q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m]). \end{aligned}$$

The right-handed side of the previous equation reduces:

$$(\nu\ qm)(\text{open}\, q \mid q\ [\overline{\text{open}}\, q.P \mid \text{in}\, m]) \longrightarrow P.$$

By reduction closure it is the case that $P = \mathbf{0}$. Contradiction!
So $m\ [\overline{\text{in}}\, m\ ] \neq \mathbf{0}$ after all, for any m.

□

The previous theorem says that in any sound theory there is at least one pairs of terms that are not derivable. This might not be surprising, because of consistency. However, the incompatible pair chosen here is necessary for deriving inconsistency in the following proof which is *very important*, because it claims that any sound theory is a posteriori equipped with observables.

Proposition 3.16 *Let $\mathcal{T}$ be a sound theory. If $\mathcal{T} \vdash P = Q$ and $P \downarrow \overline{in\ n}$ then $Q \Downarrow \overline{in\ n}$.*

Proof. If $P \downarrow \overline{in\ n}$ iff $P \equiv (\nu\ p_1 \ldots p_n)(n\ [\overline{\text{in}}\, n.P_1 \mid P_2] \mid P_3)$ and $n \notin \{p_1 \ldots p_n\}$. We write $(\nu\ \ \overline{p})$ for $(\nu\ p_1 \ldots p_n)$. Take $A = fn(P) \cup fn(Q)$ and without loss of generality we can take $q, r, z \notin A$. Consider the context $q\ [\text{in}\, n.r\ [\overline{\text{in}}\, r] \mid \overline{\text{open}}\, q] \mid \{\}$ then:
$q\ [\text{in}\, n.r\ [\overline{\text{in}}\, r] \mid \overline{\text{open}}\, q] \mid P \longrightarrow (\nu\ \overline{p})(n\ [q\ [r\ [\overline{\text{open}}\, r] \mid \overline{\text{open}}\, q] \mid P_1 \mid P_2] \mid P_3)$.

Assuming that $Q \not\Downarrow \overline{in\ n}$, then for some Q':

$$q\ [\text{in}\, n.r\ [\overline{\text{in}}\, r] \mid \overline{\text{open}}\, q] \mid Q \longrightarrow\!\!\!\!\!\rightarrow\ q\ [\text{in}\, n.r\ [\overline{\text{in}}\, r] \mid \overline{\text{open}}\, q] \mid Q'.$$

$$q\ [\text{in}\, n.r\ [\overline{\text{in}}\, r] \mid \text{open}\, q] \mid Q' = (\nu\ \overline{p})(n\ [q\ [r\ [\overline{\text{open}}\, r] \mid \overline{\text{open}}\, q] \mid P_1 \mid P_2] \mid P_3).$$

For sake of readability, M denotes $q\ [\text{in}\, n.r\ [\overline{\text{in}}\, r] \mid \overline{\text{open}}\, q] \mid Q'$ and N denotes $(\nu\ \overline{p})(n\ [q\ [r\ [\overline{\text{in}}\, r] \mid \overline{\text{open}}\, q] \mid P_1 \mid P_2] \mid P_3)$. Now consider the context $\text{open}\, q.z\ [\overline{\text{in}}\, z] \mid \{\}$.

$$\text{open}\, q.z\ [\overline{\text{in}}\, z] \mid M \longrightarrow z\ [\overline{\text{in}}\, z] \mid \text{in}\, n.r\ [\overline{\text{in}}\, r] \mid Q'.$$

$$\text{open}\, q.z\ [\overline{\text{in}}\, z] \mid N \longrightarrow\!\!\!\!\!\rightarrow\ R.$$

for some R such that:

$$z\ [\overline{\text{in}}\, z] \mid \text{in}\, n.r\ [\overline{\text{in}}\, r] \mid Q' = \ R.$$

We need to analyse R. There are two different cases to analyse :

(i) If $\mathrm{open}\, q.z\ [\overline{\mathrm{in}}\, z]$ is still present in R, then:

$$R \equiv \mathrm{open}\, q.z\ [\overline{\mathrm{in}}\, z] \mid (\nu\ \overline{p})(n\ [q\ [r\ [\overline{\mathrm{in}}\, r] \mid \overline{\mathrm{open}}\, q] \mid P_1' \mid P_2'] \mid P_3')$$

for some P_1', P_2', P_3'.

Take the context $(\nu\ Aqr) \mid \{\}$:

$$\begin{aligned} R &= z\ [\overline{\mathrm{in}}\, z] \mid \mathrm{in}\, n.r\ [\overline{\mathrm{in}}\, r] \mid Q' \\ (\nu\ Aqr)(R) &= (\nu\ Aqr)(z\ [\overline{\mathrm{in}}\, z] \mid \mathrm{in}\, n.r\ [\overline{\mathrm{in}}\, r] \mid Q') \\ \mathbf{0} &= z\ [\overline{\mathrm{in}}\, z]. \end{aligned}$$

Contradiction with Lemma 3.15. So $Q \Downarrow \overline{in\ n}$.

(ii) $\mathrm{open}\, q.z\ [\overline{\mathrm{in}}\, z]$ is not longer present in R then the boundaries of the ambients n and q have been dissolved obtaining the following:

$$R \equiv z\ [\overline{\mathrm{in}}\, z] \mid (\nu\ \overline{p})(r\ [\overline{\mathrm{in}}\, r] \mid P_1'' \mid P_2'' \mid P_3'').$$

for some P_1'', P_2'', P_3''. Considering the context $(\nu\ Aqz) \mid \{\}$ (notice that we restrict on z rather than r, differently from the previous context) then:

$$\begin{aligned} R &= z\ [\overline{\mathrm{in}}\, z] \mid \mathrm{in}\, n.r\ [\overline{\mathrm{in}}\, r] \mid Q' \\ (\nu\ Aqz)R &= (\nu\ Aqz)(z\ [\overline{\mathrm{in}}\, z] \mid \mathrm{in}\, n.r\ [\overline{\mathrm{in}}\, r] \mid Q') \\ r\ [\overline{\mathrm{in}}\, r] &= \mathbf{0}. \end{aligned}$$

Contradiction with Lemma 3.15. So $Q \Downarrow \overline{in\ n}$. □

Theorem 3.17 *Let $\mathcal{U}_T$ be the union of all sound theories. Then $\mathcal{U}_T$ is sound.*

Proof. [Sketch] By construction $\equiv$ is included and the of insensitive terms are identified. It should be not difficult to see that the union of all sound theories produces a chain of equations that by transitivity preserves the reduction closure and the barb $\overline{\mathrm{in}}\, n$ (for all n), which yields consistency since $n\ [\overline{\mathrm{in}}\, n] \neq \mathbf{0}$. The latter observation shows that $\mathcal{U}_T$ preserves the barb $\overline{\mathrm{in}}\, n$. □

This theorem is quite important since it states that the union of all sound theories inherits all the properties of any sound theory, in particular the observables (all of them, even the ones that we are going to show later). In the next section we prove that there is an operational characterisation of the maximal sound theory, indeed this coincides with *contextual barbed bisimulation* (Definition 2.5).

4 From sound theories to contextual barbed bisimulations

Contextual barbed bisimulation exhibits the barb $\overline{\mathrm{open}}\, n$, therefore it is necessary to show that a sound theory exhibits the same barb.

Proposition 4.1 *Let $\mathcal{T}$ be a sound theory. Assume $\mathcal{T} \vdash P = Q$ for all n, if $P \downarrow \overline{open\ n}$ then $Q \Downarrow \overline{open\ n}$. Moreover, let $\mathcal{U}_T$ be the union of all sound theories. If $\mathcal{U}_T \vdash P = Q$ for all n, if $P \downarrow \overline{open\ n}$ then $Q \Downarrow \overline{open\ n}$.*

Proof. The first part of the proposition can be proved in a similar way to Proposition 3.16 making us of the context: $\mathrm{open}\, n.z\ [\overline{\mathrm{in}}\, z]$, with $z \notin fn(P) \cup fn(Q)$. The second part proposition is derived from Theorem 3.17. □

Theorem 4.2 $\approx = \mathcal{U}_T$.

Proof. [Sketch] $\mathcal{U}_T \subseteq \approx$. If $\mathcal{U}_T \vdash P = Q$ then by reduction closure, if $\mathcal{C}\{P\} \longrightarrow\!\!\!\!\!\rightarrow P'$ then for some Q', $\mathcal{C}\{Q\} \longrightarrow\!\!\!\!\!\rightarrow Q'$ and $P' = Q'$. Moreover, by Proposition 4.1, if $P \downarrow \overline{open\ n}$ then $Q \Downarrow \overline{open\ n}$. Since a theory is closed under all contexts, if $\mathcal{C}\{P\} \downarrow \overline{open\ n}$ then $\mathcal{C}\{Q\} \Downarrow \overline{open\ n}$. Notice that this implies that $\equiv\ \subset \approx$.

$\approx \subseteq \mathcal{U}_T$. Conversely we must prove that $P \approx Q$ is a sound theory. It is reduction closed by definition and consistent since $n\ [\overline{\mathrm{open}}\, n\ ] \not\approx \mathbf{0}$, moreover it is a congruence by definition. It identifies the insensitive terms since they reduce only internally and never interact with any context, contains structural as we have proved in the previous part.

□

The previous theorem is an important step towards the proof of Theorem 2.8. In the previous proof, one important ingredient is the presence of the observable in any sound theory (Proposition 4.1). In fact once proved that, it follows by Theorem 3.17 that the union of all sound theories preserves the same barb. So, in Definition 2.1 there were five barbs. We have already shown that sound theories preserve two of them. It should be sufficient to show that sound theories preserve the missing three barbs from Definition 2.1.

Proposition 4.3 *Let $\mathcal{T}$ be a sound theory. Suppose $\mathcal{T} \vdash P = Q$ for all n,*

(i) *if $P \downarrow in\ n$ then $Q \Downarrow in\ n$.*

(ii) *if $P \downarrow out\ n$ then $Q \Downarrow out\ n$.*

(iii) *if $P \downarrow open\ n$ then $Q \Downarrow open\ n$.*

Proof. The proof makes use of consistency and insensitive terms as in the proof of Proposition 3.16, and of the appropriate contexts: i) $n\ [\overline{\mathrm{in}}\, n.z\ [\overline{\mathrm{in}}\, z]] \mid \{\}$; ii) $n\ [\overline{\mathrm{out}}\, n.z\ [\overline{\mathrm{in}}\, z] \mid \{\}]$; iii) $n\ [\overline{\mathrm{open}}\, n.z\ [\overline{\mathrm{in}}\, z]] \mid \{\}$, assuming throughout that $z \notin fn(P) \cup fn(Q)$. □

The following is the proof of Theorem 2.8.

Proof. The union of all sound theories $\mathcal{U}_T$ preserves all the barbs by Propositions 4.3, 4.1, 3.16 and Theorem 3.17. By reasoning in a similar way, as in the proof of Theorem 4.2, it is possible to show that the union of all sound theories, equipped with each barb is equivalent to each contextual equivalence, equipped with the corresponding barb, obtaining the following chain of equations: $\mathcal{U}_T = \approx^{\overline{in}}$, $\mathcal{U}_T = \approx^{in}$, $\mathcal{U}_T = \approx^{out}$ and $\mathcal{U}_T = \approx^{open}$.

Because the union of all sound theories is unique, all contextual equivalences coincide $\mathcal{U}_T = \approx^{\overline{in}} = \approx^{in} = \approx^{out} = \approx^{open} = \approx$. □

5 Safe Ambients with Passwords

Very briefly we show that our work can be adapted to SAP [10]. The main difference between SAP and SA is the use of passwords; capabilities have two names, like in $\langle n, h\rangle$, instead of one, where h denotes the password. The basic operational semantics is the same as in SA, with the exception of the rule for exiting an ambient, where the the co-capability is external, as it is shown by the following rule:

$$n\ [q\ [\text{out}\ \langle n, h\rangle.P_1 \mid P_2] \mid P_3] \mid \overline{\text{out}}\ \langle n, h\rangle.Q \longrightarrow q\ [P_1 \mid P_2] \mid n\ [P_3] \mid Q$$

It is possible to apply the work on sound theories to this setting taking into account that the definition of active names needs to guarantee that terms like $(\nu\ h)(\text{open}\ \langle n, h\rangle.P)$ are insensitive. This is possible by defining active names as a set of pairs, for instance: $an(\text{open}\ \langle n, h\rangle.P)) = \{\langle n, h\rangle\}$, taking care of restriction in the following way: $an((\nu\ n)P) = an(P) - \{\langle z, r\rangle\}$ for some z, r, if either $n = z$ or $n = r$. Let's denote $\approx_{SAP}$ for the contextual barbed equivalence with the barb open $\langle n, n\rangle$ and ${\mathcal{U}_T}^{SAP}$ for union of all sound theories. With a similar reasoning to Theorem 4.2 we can prove the following:

Proposition 5.1 $\approx_{SAP} = {\mathcal{U}_T}^{SAP}$.

Moreover, differently from SA, where the co-capability for the $\overline{\text{out}}$ was not observable, in the SAP setting there is a new the barb: $P \downarrow \overline{\text{out}}\langle n,h\rangle$ if and only if $P \equiv (\nu\ p_1 \ldots p_n)\overline{\text{out}}\ \langle n, h\rangle.P'$ and $n, h \notin \{p_1 \ldots p_n\}$.

Proposition 5.2 *Let $\mathcal{T}^{SAP}$ be a sound theory. Suppose $\mathcal{T}^{SAP} \vdash P = Q$ for all n, h, if $P \downarrow \overline{\text{out}}\langle n,h\rangle$ then $Q \Downarrow \overline{\text{out}}\langle n,h\rangle$.*

Finally, writing $\approx_{SAP}^{\overline{out}}$ for contextual equivalence with barb $\overline{\text{out}}$, it is possible to prove that $\approx_{SAP} = {\mathcal{U}_T}^{SAP} = \approx_{SAP}^{\overline{out}}$.

6 Conclusions

In this paper we have applied the Honda-Yoshida technique to SA, in order to obtain a canonical equivalence. We have shown that the adaptation of this technique is not trivial in SA and that contextual barbed equivalence equates the same terms regardless of the barbs observed. The main task as future work is concerned, is to prove that the barbed congruence is included in the contextual barbed congruence following the proof in [3] for the asynchronous π-calculus.

Acknowledgements

We would like to thank Kohei Honda, C. Fournet and A. Gordon for useful discussions. We are also grateful to the anonymous referees for their useful comments and suggestions.

References

[1] L. Cardelli. Abstraction for Mobile Computation. In *Secure Internet Programming: Security Issues for Mobile and Distributed Object*, volume 1603 of *LNCS* pages 51–94. Springer-Verlag, 1999.

[2] L. Cardelli and A.D. Gordon. Mobile ambient. In *Proceedings of FoSSaCS'98*, volume 1378 of *LNCS*, pages 140–155. Springer-Verlag, 1998.

[3] C. Fournet, G. Gonthier. A hierarchy of equivalences for asynchronous calculi. In *Proceedings of ICALP'98*, volume 1443 of LNCS, July 1998.

[4] A.D. Gordon and L. Cardelli. Technical annex. Available at: www.microsoft.com/ adg, 1998.

[5] A.D. Gordon and L. Cardelli. Equational properties of mobile ambients. Technical Report MSR-TR-99-11, Microsoft Research Center, April 1999.

[6] K. Honda and N. Yoshida. On reduction-based process semantics. *Theoretical Computer Science*, 151:437–486, 1995.

[7] F. Levi and D. Sangiorgi. Controlling Interference for Ambients. In *Proceedings of POPL'00*, pages 142–154, *ACM* Press, 2000.

[8] R. Milner, J. Parrow, and D. Walker. A calculus for mobile processes, (Parts I and II). *Information and Computation*, 100 (1):1–77, 1992.

[9] R. Milner and D. Sangiorgi. Barbed Bisimulation. In *Proceedings of 19th ICALP*, volume 623 of *LNCS*, 1992

[10] M. Merro and M. Hennessy. Bisimulation Congruences in Safe Ambients. In *Proceedings of POPL'02*, 2002. To appear.

[11] I.C.C. Phillips and M.G. Vigliotti. On reduction semantics for the Push and Pull Ambient Calculus. In *Proceedings of IFIP TCS 2002*, Montreal, to appear.

[12] D. Sangiorgi. *Expressing mobility in Process Algebra: First-Order and Higher-Order Paradigms*. PhD thesis, University of Edinburgh, 1993.