On barbed equivalences in π-calculus

Davide Sangiorgi[1] and David Walker[2]

[1] INRIA Sophia-Antipolis, France (davide.sangiorgi@inria.fr)
[2] Oxford University Computing Laboratory, U.K. (walker@comlab.ox.ac.uk)

Abstract. This paper presents some new results on barbed equivalences for the π-calculus. The equivalences studied are barbed congruence and a variant of it called open barbed bisimilarity. The difference between the two is that in open barbed the quantification over contexts is inside the definition of the bisimulation and is therefore recursive. It is shown that if infinite sums are admitted to the π-calculus then it is possible to give a simple proof that barbed congruence and early congruence coincide on all processes, not just on image-finite processes. It is also shown that on the π-calculus, and on the extension of it with infinite sums, open barbed bisimilarity does not correspond to any known labelled bisimilarity. It coincides with a variant of open bisimilarity in which names that have been extruded are treated in a special way, similarly to how names are treated in early bisimilarity.

1 Introduction

This paper presents some new results on barbed equivalences for the π-calculus. The equivalences studied are *barbed congruence* [9] and a variant of it [5] here called *open barbed bisimilarity*. Both equivalences are obtained via kinds of bisimulation that use reduction and a notion of observation, and both are contextual in the sense that their definitions involve quantification over contexts. Most importantly, both relations are congruences, and therefore allow compositional reasoning about processes. The difference between the two is that in open barbed the quantification over contexts is inside the definition of the bisimulation and is therefore recursive.

Equivalences whose definitions involve just notions of reduction and observation and quantification over contexts are useful because they can be applied to a wide variety of calculi and languages. This is important because it is sometimes far from clear how to define appropriate equivalences by other means, for instance based on the actions that processes can perform according to some labelled transition rules. The main difficulty with definitions that involve quantification over contexts is that they are often awkward to work with directly. It is therefore important to look for more tractable characterizations of the equivalences.

The aims of the paper are to contrast the two barbed equivalences and to show that a simple proof of a characterization theorem for barbed congruence can be given that with the addition of infinite sums applies to all processes.

State of the art Barbed congruence has been used on a variety of concurrent calculi and languages (imperative, object-oriented, functional, etc.). On languages akin to the

π-calculus, a number of results that characterize barbed congruence in terms of early congruence have been shown; examples are [3, 7, 13]. Typically, these results are for image-finite processes only. The only results we are aware of that do not assume image-finiteness are in [11] and [4]. Their proofs are complex, however, and they cover only specific dialects of the π-calculus. In [11] the π-calculus is extended with infinite sums and with infinitely many mutually recursive definitions, and moreover each recursive definition can have an infinite number of name parameters. In [4] the calculus is a form of asynchronous π-calculus.

Open barbed bisimilarity has been applied to several variants of the π-calculus and to higher-order calculi; examples are [5, 6, 1]. The main advantage of open barbed bisimilarity over barbed congruence is that a characterization result can often be proved, using an appropriate form of labelled bisimilarity, that applies to *all* processes, not just image-finite processes. We are not aware of any characterization result for open barbed bisimilarity on the standard π-calculus, however. Such a result would be useful, beyond its significance for the π-calculus, because it would shed light on the robustness of open barbed bisimilarity, and in particular on the relationship between it and barbed congruence.

Contributions The main contributions of this paper are as follows.

1. We show that if we admit infinite sums to the π-calculus, then we can give a simple proof that barbed congruence and early congruence coincide on all processes, not just on image-finite processes. (It remains an open question whether the equivalences coincide on the π-calculus.)
2. We show that, perhaps surprisingly, on the π-calculus (and on the extension of it with infinite sums) open barbed bisimilarity does not correspond to any known labelled bisimilarity. It coincides with a variant of *open bisimilarity* [12] in which names that have been extruded are treated in a special way, similarly to how names are treated in early bisimilarity.

The structure of the proof of (1) is similar to that in [13] for image-finite processes. As a corollary of (2), open barbed bisimilarity is different from barbed congruence on the π-calculus. Compared to [11], the result (1), besides having a much simpler proof, does not use infinitely many mutually recursive definitions. This is significant because infinitely many mutually recursive definitions cannot be encoded using replication; only finitely many mutually recursive definitions, each with a finite number of name parameters, can be so encoded; see [8].

The results in this paper do not tell us whether the new labelled bisimilarity introduced in (2) is interesting. Its mixture of features from open bisimilarity and early bisimilarity seems hard to justify observationally, however.

This paper treats the weak equivalences, which abstract from internal action. Analogous results for *strong* equivalences are easily obtained by simplifying the proofs. We believe that the results in the paper hold also for other dialects of the π-calculus that have the matching operator (which is fundamental to the proofs of the characterization results), for instance the Asynchronous π-calculus. The calculus we work with in this paper has guarded sums. If we were to admit unguarded sums, as in CCS, then the clause for τ transitions in the characterization of open barbed bisimilarity would have to be modified along the lines of *dynamic bisimilarity* [10].

Other related work A distinctive feature of open barbed bisimilarity is that it is both a bisimulation and a congruence. Montanari and Sassone [10] first used relations that by definition are both bisimulations and congruences, in CCS. These relations are defined like CCS bisimulation, but with an additional requirement similar to closure of an open barbed bisimulation under contexts; see Definition 2(4). On the π-calculus, the largest relation so obtained is different from (early) bisimilarity because bisimilarity is not a congruence. Honda and Yoshida [5] applied similar ideas in the setting of reduction-based bisimilarities, where τ transitions, or reductions, are the only relevant transitions of processes. The relation defined is essentially what we call *open barbed bisimilarity*, although the formulation and the calculi are rather different. In particular, a significant difference is that [5] distinguishes between names and variables, whereas this paper is about the π-calculus where there are only names.

2 Background

In this section we briefly recall some definitions and notations for the π-calculus.

We assume a countably infinite set N of *names*, ranged over by lower-case letters, $x, y, z, \ldots$. The *prefixes* are given by

$$\pi \;::=\; \overline{x}y \;\mid\; x(z) \;\mid\; \tau \;\mid\; [x = y]\pi \; .$$

Note that we take matches to be parts of prefixes. The *processes* and the *summations* of the π-calculus are given respectively by

$$\begin{array}{lcl} P & ::= & M \;\mid\; P \mid P' \;\mid\; \boldsymbol{\nu} z\, P \;\mid\; !P \\ M & ::= & \mathbf{0} \;\mid\; \pi.\, P \;\mid\; M + M' \; . \end{array}$$

We abbreviate $x(z).\,\mathbf{0}$ to x. A *context* is obtained when in some P given by the grammar above, the *hole* $[\cdot]$ replaces an occurrence of $\mathbf{0}$ that is not the left or right term in a sum $M + M'$. A *non-input context* is a context in which the hole does not occur underneath an input prefix.

In each of $x(z).\, P$ and $\boldsymbol{\nu} z\, P$, the displayed occurrence of z is binding with scope P. We write $\mathsf{fn}(E_1, E_2, \ldots)$ for the set of names that occur free in at least one of the entities $E_1, E_2, \ldots$. A *substitution* is a function σ on the set of names that has finite support, that is, is such that $\{x \mid x\sigma \neq x\}$ is finite. We write $E\sigma$ for the application of a substitution σ to an entity E.

The *actions* are given by

$$\alpha \;::=\; \overline{x}y \;\mid\; xy \;\mid\; \overline{x}(z) \;\mid\; \tau \; .$$

We write *Act* for the set of actions. We write $\mathsf{bn}(\alpha)$ for the set of names bound in α, which is $\{z\}$ if α is $\overline{x}(z)$ and $\emptyset$ otherwise, and $\mathsf{n}(\alpha)$ for the set of names that occur in α. The (*early*) *transition relations*, $\{\xrightarrow{\alpha} \mid \alpha \in \mathit{Act}\}$, are defined by the rules in Table 1. Elided from the table are four rules: the symmetric form SUM-R of SUM-L, which has

$Q + P$ in place of $P + Q$, and the symmetric forms PAR-R, COMM-R, and CLOSE-R of PAR-L, COMM-L, and CLOSE-L, in which the roles of the left and right components are swapped. We adopt rules REP-ACT, REP-COMM, and REP-CLOSE so that the transition relations are image-finite. Other rules could be used, however [8]. We write $\Longrightarrow$ for the reflexive and transitive closure of $\xrightarrow{\tau}$, and $\stackrel{\alpha}{\Longrightarrow}$ for $\Longrightarrow\xrightarrow{\alpha}\Longrightarrow$ for $\alpha \in Act$. Further, $\stackrel{\widehat{\tau}}{\Longrightarrow}$ is $\Longrightarrow$, and $\stackrel{\widehat{\alpha}}{\Longrightarrow}$ is $\stackrel{\alpha}{\Longrightarrow}$ for $\alpha \neq \tau$. We write $P \downarrow_x$ if P can perform an action of the form xy, and $P \downarrow_{\overline{x}}$ if P can perform an action of the form $\overline{x}y$ or $\overline{x}(z)$. Further, for μ a name x or a co-name $\overline{x}$, we write $P \Downarrow_\mu$ if there is Q such that $P \Longrightarrow Q$ and $Q \downarrow_\mu$.

We identify processes that are α-convertible. Moreover, in any discussion, we assume that the bound names of any processes or actions under consideration are chosen to be different from the names free in any other entities under consideration, such as processes, actions, substitutions, and sets of names. This convention is subject to the limitation that in considering a transition $P \xrightarrow{\overline{x}(z)} Q$, the name z that is bound in $\overline{x}(z)$ and in P can occur free in Q.

Definition 1 (Barbed bisimilarity and congruence).
A relation $\mathcal{S}$ is a *barbed bisimulation* if whenever $(P, Q) \in \mathcal{S}$,

1. $P \downarrow_\mu$ implies $Q \Downarrow_\mu$
2. $P \xrightarrow{\tau} P'$ implies $Q \Longrightarrow Q'$ for some Q' with $(P', Q') \in \mathcal{S}$
3. the variants of (1) and (2) with the roles of P and Q swapped.

P and Q are *barbed bisimilar*, $P \stackrel{\bullet}{\approx} Q$, if $(P, Q) \in \mathcal{S}$ for some barbed bisimulation $\mathcal{S}$. P and Q are *barbed congruent*, $P \cong^{\mathrm{c}} Q$, if $C[P] \stackrel{\bullet}{\approx} C[Q]$ for every context C. $\square$

For two processes to be barbed congruent, the systems obtained by placing them into an arbitrary context must be barbed bisimilar. In open barbed bisimilarity, on the other hand, the context enclosing the processes being tested can be changed at any point during the bisimulation game: an open barbed bisimulation is required to be closed under contexts.

Definition 2 (Open barbed bisimilarity). A relation $\mathcal{S}$ is an *open barbed bisimulation* if whenever $(P, Q) \in \mathcal{S}$,

1. $P \downarrow_\mu$ implies $Q \Downarrow_\mu$
2. $P \xrightarrow{\tau} P'$ implies $Q \Longrightarrow Q'$ for some Q' with $(P', Q') \in \mathcal{S}$
3. the variants of (1) and (2) with the roles of P and Q swapped
4. $(C[P], C[Q]) \in \mathcal{S}$ for every context C.

P and Q are *open barbed bisimilar*, $P \stackrel{\bullet}{\approx}_{\mathrm{o}} Q$, if $(P, Q) \in \mathcal{S}$ for some open barbed bisimulation $\mathcal{S}$. $\square$

Definition 3 (Early bisimilarity and congruence).
A relation $\mathcal{S}$ is an *early bisimulation* if whenever $(P, Q) \in \mathcal{S}$,

1. $P \xrightarrow{\alpha} P'$ implies $Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q'$ for some Q' with $(P', Q') \in \mathcal{S}$
2. the variant of (1) with the roles of P and Q swapped.

$$\textsc{Out}\ \frac{}{\overline{x}y.\,P \xrightarrow{\overline{x}y} P} \qquad \textsc{Inp}\ \frac{}{x(z).\,P \xrightarrow{xy} P\{y/z\}}$$

$$\textsc{Tau}\ \frac{}{\tau.\,P \xrightarrow{\tau} P} \qquad \textsc{Mat}\ \frac{\pi.\,P \xrightarrow{\alpha} P'}{[x=x]\pi.\,P \xrightarrow{\alpha} P'}$$

$$\textsc{Sum-l}\ \frac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P'}$$

$$\textsc{Par-l}\ \frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q}\quad \mathsf{bn}(\alpha)\cap\mathsf{fn}(Q)=\emptyset$$

$$\textsc{Comm-l}\ \frac{P \xrightarrow{\overline{x}y} P' \quad Q \xrightarrow{xy} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'}$$

$$\textsc{Close-l}\ \frac{P \xrightarrow{\overline{x}(z)} P' \quad Q \xrightarrow{xz} Q'}{P \mid Q \xrightarrow{\tau} \boldsymbol{\nu} z\,(P' \mid Q')}\quad z\notin\mathsf{fn}(Q)$$

$$\textsc{Res}\ \frac{P \xrightarrow{\alpha} P'}{\boldsymbol{\nu} z\,P \xrightarrow{\alpha} \boldsymbol{\nu} z\,P'}\quad z\notin\mathsf{n}(\alpha) \qquad \textsc{Open}\ \frac{P \xrightarrow{\overline{x}z} P'}{\boldsymbol{\nu} z\,P \xrightarrow{\overline{x}(z)} P'}\quad z\neq x$$

$$\textsc{Rep-act}\ \frac{P \xrightarrow{\alpha} P'}{!P \xrightarrow{\alpha} P' \mid !P}$$

$$\textsc{Rep-comm}\ \frac{P \xrightarrow{\overline{x}y} P' \quad P \xrightarrow{xy} P''}{!P \xrightarrow{\tau} (P' \mid P'') \mid !P}$$

$$\textsc{Rep-close}\ \frac{P \xrightarrow{\overline{x}(z)} P' \quad P \xrightarrow{xz} P''}{!P \xrightarrow{\tau} (\boldsymbol{\nu} z\,(P' \mid P'')) \mid !P}\quad z\notin\mathsf{fn}(P)$$

Table 1. The transition rules

P and Q are *early bisimilar*, $P \approx Q$, if $(P, Q) \in \mathcal{S}$ for some early bisimulation $\mathcal{S}$. P and Q are *early congruent*, $P \approx^{\mathrm{c}} Q$, if $P\sigma \approx Q\sigma$ for every substitution σ. □

A process P is *image-finite* if for each derivative Q of P and each action α, there are $n \geq 0$ and $Q_1, \ldots, Q_n$ such that $Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q'$ implies $Q' = Q_i$ for some i. We recall the following result for the π-calculus; see [3, 13] for proofs of closely related results.

Theorem 1 (Characterization Theorem). Suppose that P and Q are image-finite. Then $P \cong^{\mathrm{c}} Q$ iff $P \approx^{\mathrm{c}} Q$. □

3 Infinite sums

In this section we show that if we admit sums in which the number of summands is infinite, then Theorem 1 can be extended to all processes of the enriched language, that is, the assumption of image-finiteness can be removed.

The only caveat for allowing infinite sums is that the possibility of α-converting names into fresh names must be maintained. To ensure this we assume that the set of names has cardinality ω_1, the first uncountable cardinal, and require sums to have only countably many summands. (Similar results can be obtained when ω_1 is replaced by an arbitrary uncountable regular cardinal κ and sums can have only fewer than κ summands.) Accordingly, we replace the form $M + M'$ in the grammar for summations by

$$\Sigma_{i \in I} M_i$$

where I is a countable set. We write $\pi_{\infty+}$ for the resulting calculus. The modifications required to the transition rules are straightforward.

Lemma 1. The set of processes of $\pi_{\infty+}$ has cardinality ω_1.

Proof This is an instance of a standard result about inductively defined sets. See for instance Section 1.3 of [2]. □

Lemma 2. For any process P of $\pi_{\infty+}$ and action α, the set $\{P' \mid P \stackrel{\alpha}{\Longrightarrow} P'\}$ is countable.

Proof The proof uses repeatedly the fact that a countable union of countable sets is countable. First one shows that for any P and α, $\{P' \mid P \stackrel{\alpha}{\longrightarrow} P'\}$ is countable. Then one shows by induction that for $n < \omega$, $\{P' \mid P\ (\stackrel{\tau}{\longrightarrow})^n\ P'\}$ is countable. ¿From this it follows that $\{P' \mid P \Longrightarrow P'\}$ is countable, and hence that $\{P' \mid P \stackrel{\alpha}{\Longrightarrow} P'\}$ is countable. □

Definition 4 (Transfinite stratification of bisimilarity).

1. $\approx_0$ is the universal relation on $\pi_{\infty+}$.
2. For δ an ordinal, the relation $\approx_{\delta+1}$ is defined by: $P \approx_{\delta+1} Q$ if
   (a) $P \stackrel{\alpha}{\longrightarrow} P'$ implies $Q \stackrel{\widehat{\alpha}}{\Longrightarrow}\approx_\delta P'$
   (b) $Q \stackrel{\alpha}{\longrightarrow} Q'$ implies $P \stackrel{\widehat{\alpha}}{\Longrightarrow}\approx_\delta Q'$.

3. For γ a limit ordinal, $P \approx_\gamma Q$ if $P \approx_\delta Q$ for all $\delta < \gamma$. $\square$

Lemma 3. On $\pi_{\infty+}$, $P \approx Q$ iff $P \approx_\delta Q$ for every ordinal δ.

Proof First, by induction on δ we have that $P \approx Q$ implies $P \approx_\delta Q$ for every ordinal δ. For the converse first note that if $\delta < \delta'$ then $\approx_{\delta'}$ is included in $\approx_\delta$. Since by Lemma 1 the cardinality of the set of processes of $\pi_{\infty+}$ is ω_1, the universal relation $\approx_0$ has cardinality ω_1. Hence there is δ of cardinality ω_1 such that $\approx_{\delta+1}$ coincides with $\approx_\delta$. This is so because otherwise $\approx_{\delta+1}$ would be strictly included in $\approx_\delta$ for each $\delta < \omega_2$ (the second uncountable cardinal), contradicting that $\approx_0$ has cardinality ω_1. Suppose δ is the smallest ordinal such that $\approx_{\delta+1}$ coincides with $\approx_\delta$. Then $\approx_\delta$ is an early bisimulation, so $P \approx_\delta P'$ implies $P \approx P'$, and $\approx_{\delta'}$ coincides with $\approx_\delta$ for all $\delta' > \delta$. $\square$

Theorem 2 (Characterization Theorem on $\pi_{\infty+}$). Suppose P and Q are processes of $\pi_{\infty+}$. Then $P \cong^{\mathrm{c}} Q$ iff $P \approx^{\mathrm{c}} Q$.

Proof We recall that processes P and Q are *barbed equivalent*, $P \cong Q$, if $C[P] \stackrel{\cdot}{\approx} C[Q]$ for every context C of the form $[\cdot] \mid R$. We show that $P \cong Q$ iff $P \approx Q$. The conclusion $P \cong^{\mathrm{c}} Q$ iff $P \approx^{\mathrm{c}} Q$ follows since $\cong^{\mathrm{c}}$ is the largest congruence included in $\cong$ and $\approx^{\mathrm{c}}$ is the largest congruence included in $\approx$.

That $P \approx Q$ implies $P \cong Q$ follows from the facts that $\approx$ is a barbed bisimulation and a non-input congruence (that is, is preserved by all non-input contexts), and that $\cong$ is the largest non-input congruence included in $\stackrel{\cdot}{\approx}$.

The main claim needed to show that $P \cong Q$ implies $P \approx Q$ is the following.

Claim. Suppose that $P \not\approx_\delta Q$ where δ is an ordinal. Then there is a summation M such that for any $\widetilde{z} \subseteq \mathsf{fn}(P, Q)$ and any fresh name s, one of the following holds:
1. $(\boldsymbol{\nu}\widetilde{z})\,(P' \mid (M + s)) \stackrel{\cdot}{\not\approx} (\boldsymbol{\nu}\widetilde{z})\,(Q \mid (M + s))$ for all P' such that $P \Longrightarrow P'$
2. $(\boldsymbol{\nu}\widetilde{z})\,(P \mid (M + s)) \stackrel{\cdot}{\not\approx} (\boldsymbol{\nu}\widetilde{z})\,(Q' \mid (M + s))$ for all Q' such that $Q \Longrightarrow Q'$.

Proof If δ is a limit ordinal and $P \not\approx_\delta Q$, then $P \not\approx_\gamma Q$ for some $\gamma < \delta$, and the result follows immediately by induction.
Suppose $\delta = \gamma + 1$. Then there are α and P' such that $P \xrightarrow{\alpha} P'$ but $P' \not\approx_\gamma Q'$ for all Q' such that $Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q'$ (or vice versa, when the argument is the same). By Lemma 2, $\{Q' \mid Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q'\} = \{Q_i \mid i \in I\}$ for some countable set I. We prove that assertion (2) of the Claim holds (in the case when the roles of P and Q are swapped, one would prove assertion (1)).
Appealing to the induction hypothesis, for each $i \in I$ let M_i be a summation such that either (1) or (2) of the Claim holds for P', Q_i, and M_i. There are four cases, one for each form that α can take. We give the details only for the case when α is an input action. The other cases are similar, and for them we just indicate the main point in the construction.
Case 1 Suppose that α is xy. Let s_i $(i \in I)$ and s' be fresh names, and set

$$M \stackrel{\mathrm{def}}{=} \overline{x}y.\,(s' + \Sigma_{i \in I}\, \tau.\,(M_i + s_i))\ .$$

Suppose that $\widetilde{z} \subseteq \mathsf{fn}(P, Q)$ and s is fresh, and let Q' be any process such that $Q \Longrightarrow Q'$. Let $A \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(P \mid (M + s))$ and $B \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(Q' \mid (M + s))$, and suppose, for a contradiction, that $A \mathrel{\dot{\approx}} B$. We have

$$A \xrightarrow{\tau} A' \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(P' \mid (s' + \Sigma_{i\in I}\,\tau.\,(M_i + s_i)))$$

and $A' \Downarrow_{s'}$ but not $A' \Downarrow_s$. Since $A \mathrel{\dot{\approx}} B$ there is B' such that $B \Longrightarrow B' \mathrel{\dot{\approx}} A'$. In particular it must be that $B' \Downarrow_{s'}$ but not $B' \Downarrow_s$. The only way this is possible is if $I \neq \emptyset$ and

$$B' \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(Q_j \mid (s' + \Sigma_{i\in I}\,\tau.\,(M_i + s_i)))$$

for some $j \in I$ (a derivative of Q' under $\stackrel{\alpha}{\Longrightarrow}$ is also a derivative of Q).
Now either (1) or (2) of the Claim holds for P', Q_j, and M_j. Suppose that (2) holds. We have

$$A' \xrightarrow{\tau} A''_j \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(P' \mid (M_j + s_j))$$

and $A''_j \Downarrow_{s_j}$ but not $A''_j \Downarrow_{s'}$. Then $B' \Longrightarrow B''_j$ with $B''_j \mathrel{\dot{\approx}} A''_j$, and we must have

$$B''_j \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(Q'_j \mid (M_j + s_j))$$

for some Q'_j such that $Q_j \Longrightarrow Q'_j$. But $A''_j \mathrel{\dot{\approx}} B''_j$ contradicts that (2) of the Claim holds for P', Q_j, and M_j.
Dually, if (1) of the Claim holds for P', Q_j, and M_j, then we obtain a contradiction by considering how A' can match the transition

$$B' \xrightarrow{\tau} B''_j \stackrel{\text{def}}{=} (\boldsymbol{\nu}\widetilde{z})\,(Q_j \mid (M_j + s_j))\ .$$

Case 2 Suppose that α is $\overline{x}y$. Let s_i $(i \in I)$ and s' and w be fresh names, and set

$$M \stackrel{\text{def}}{=} x(w).\,(s' + \Sigma_{i\in I}\,[w = y]\tau.\,(M_i + s_i))\ .$$

Case 3 Suppose that α is $\overline{x}(z)$. Suppose that $\mathsf{fn}(P, Q) = \{a_h \mid h \in H\}$. Let s_i $(i \in I)$ and t and s' and w be fresh names, and set

$$M \stackrel{\text{def}}{=} x(w).\,(s' + \Sigma_{h\in H}[w = a_h]t + \Sigma_{i\in I}\,\tau.\,(M_i + s_i))\ .$$

Case 4 Suppose that α is τ. Let s_i $(i \in I)$ be fresh names, and set

$$M \stackrel{\text{def}}{=} \Sigma_{i\in I}\,\tau.\,(M_i + s_i)\ .$$

This completes the proof of the Claim. □

To complete the proof of the theorem, suppose that $P \not\approx Q$. Then by Lemma 3, $P \not\approx_\delta Q$ for some δ. Then let M be as given by the Claim for P and Q, let s be fresh, and set $C \stackrel{\text{def}}{=} [\cdot] \mid (M + s)$. Then $C[P] \mathrel{\dot{\not\approx}} C[Q]$, and so $P \not\cong Q$. □

4 Characterization of open barbed bisimilarity

In this section we show a characterization theorem for open barbed bisimilarity on the full π-calculus. The theorem holds both for the π-calculus and for its extension with infinite sums, $\pi_{\infty+}$. The labelled bisimilarity that characterizes open barbed bisimilarity is similar to open bisimilarity; indeed on the subcalculus without restriction it coincides with open bisimilarity. On the full calculus, however, the relations treat extruded names differently. To highlight the difference, we recall the definition of open bisimilarity.

Open bisimilarity is usually defined using the late transition relations. One of the significant features of open bisimilarity is that when comparing two processes, it suffices to consider only input actions and bound-output actions whose object is a single fresh name. This can be important in reducing the amount of work needed to determine whether processes are equivalent. Here, however, it is convenient to cast the definition using the early transition relations.

A *distinction* is a finite symmetric and irreflexive relation on names. A substitution σ *respects* a distinction D if $(x, y) \in D$ implies $x\sigma \neq y\sigma$. Given sets of names Y and Z, we write $Y \otimes Z$ for the distinction that contains all pairs (y, z) and (z, y) such that $y \in Y$, $z \in Z$, and $y \neq z$.

Definition 5 (Open bisimilarity). An *open bisimulation* is a family of relations $\{\mathcal{S}_D \mid D \text{ a distinction}\}$ such that whenever $(P, Q) \in \mathcal{S}_D$,

1. if $P \xrightarrow{\alpha} P'$ and α is not a bound output, then $Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q'$ for some Q' with $(P', Q') \in \mathcal{S}_D$
2. if $P \xrightarrow{\overline{x}(z)} P'$ then $Q \stackrel{\overline{x}(z)}{\Longrightarrow} Q'$ for some Q' with $(P', Q') \in \mathcal{S}_{D'}$ where $D' = D \cup (\{z\} \otimes \mathsf{fn}(P, Q))$
3. the variants of (1) and (2) with the roles of P and Q swapped
4. $(P\sigma, Q\sigma) \in \mathcal{S}_{D\sigma}$ for every σ that respects D.

We write $\{\approx_{\mathrm{o}}^{D} \mid D \text{ a distinction}\}$ for the pointwise union of all open bisimulations, and refer to $\approx_{\mathrm{o}}^{D}$ as *open D-bisimilarity*. In particular, we write $\approx_{\mathrm{o}}$ for $\approx_{\mathrm{o}}^{\emptyset}$, and refer to it as *open bisimilarity*. □

The definition of quasi-open bisimilarity involves a family of relations indexed by finite sets of names, rather than by distinctions. We need the analogue of the notion that a substitution respects a distinction. Suppose $\widetilde{z}$ is a finite set of names. A substitution σ *respects* $\widetilde{z}$ if whenever $z \in \widetilde{z}$ and $y \neq z$, then $y\sigma \neq z\sigma$.

Definition 6 (Quasi-open bisimilarity). A *quasi-open bisimulation* is a family of relations $\{\mathcal{S}^{\widetilde{z}} \mid \widetilde{z} \subseteq \mathsf{N} \text{ finite}\}$ such that whenever $(P, Q) \in \mathcal{S}^{\widetilde{z}}$,

1. if $P \xrightarrow{\alpha} P'$ and α is not a bound output, then $Q \stackrel{\widehat{\alpha}}{\Longrightarrow} Q'$ for some Q' with $(P', Q') \in \mathcal{S}^{\widetilde{z}}$
2. if $P \xrightarrow{\overline{x}(z)} P'$ then $Q \stackrel{\overline{x}(z)}{\Longrightarrow} Q'$ for some Q' with $(P', Q') \in \mathcal{S}^{\widetilde{z} \cup \{z\}}$
3. the variants of (1) and (2) with the roles of P and Q swapped
4. $(P\sigma, Q\sigma) \in \mathcal{S}^{\widetilde{z}\sigma}$ for every σ that respects $\widetilde{z}$.

We write $\{\approx_{\mathrm{q}}^{\tilde{z}} \mid \tilde{z} \subseteq \mathsf{N} \text{ finite}\}$ for the pointwise union of all quasi-open bisimulations, and refer to $\approx_{\mathrm{q}}^{\tilde{z}}$ as *quasi-open $\tilde{z}$-bisimilarity*. In particular, we write $\approx_{\mathrm{q}}$ for $\approx_{\mathrm{q}}^{\emptyset}$, and refer to it as *quasi-open bisimilarity*. □

In open bisimilarity, when a name z is sent in a bound-output action, the distinction is enlarged to ensure that z is never identified with any name that is free in the processes that send it. In quasi-open bisimilarity, in contrast, at no point after the scope of z is extruded can a substitution be applied that identifies z with *any* other name. Roughly, quasi-open bisimilarity treats names that are extruded in the same way that early bisimilarity treats all names.

Lemma 4. Quasi-open bisimilarity, $\approx_{\mathrm{q}}$, is a congruence.

Proof (Outline) The proof involves showing that $\approx_{\mathrm{q}}$ is preserved by each operator of the calculus. This is done by exhibiting appropriate quasi-open bisimulations. Due to the special treatment of extruded names, the case of composition needs special care. □

Quasi-open bisimilarity, like open bisimilarity, is more discriminating than early congruence: the union over $\tilde{z}$ of the relations $\approx_{\mathrm{q}}^{\tilde{z}}$ is an early bisimulation; and for instance $P \approx^{\mathrm{c}} Q$ but $P \not\approx_{\mathrm{q}} Q$ where

$$P \stackrel{\mathrm{def}}{=} x.\, x + x + x.\, [y = z]x$$
$$Q \stackrel{\mathrm{def}}{=} x.\, x + x\ .$$

The reason why $P \not\approx_{\mathrm{q}} Q$ is that $[y = z]x \not\approx_{\mathrm{q}} x$ and $[y = z]x \not\approx_{\mathrm{q}} \mathbf{0}$, as can be seen by considering the effects of applying the identity substitution and the substitution $\{y/z\}$ respectively.

Moreover, quasi-open bisimilarity is strictly weaker than open bisimilarity.

Lemma 5. $\approx_{\mathrm{o}}$ is strictly included in $\approx_{\mathrm{q}}$.

Proof For $\tilde{z}$ a finite set of names define $\mathcal{S}^{\tilde{z}}$ by setting $(P, Q) \in \mathcal{S}^{\tilde{z}}$ if there is a distinction D such that $P \approx_{\mathrm{o}}^{D} Q$ and for each pair $(x, y) \in D$, either $x \in \tilde{z}$ or $y \in \tilde{z}$. Then $\{\mathcal{S}^{\tilde{z}} \mid \tilde{z} \subseteq \mathsf{N} \text{ finite}\}$ can be shown to be a quasi-open bisimulation. So in particular, if $P \approx_{\mathrm{o}} Q$ then $(P, Q) \in \mathcal{S}^{\emptyset}$ and so $P \approx_{\mathrm{q}} Q$.

To show that the inclusion is strict we can take

$$P \stackrel{\mathrm{def}}{=} \boldsymbol{\nu} z\, \overline{x}z.\, (x(w) + x(w).\, z + x(w).\, [w = z]z)$$
$$Q \stackrel{\mathrm{def}}{=} \boldsymbol{\nu} z\, \overline{x}z.\, (x(w) + x(w).\, z)\ .$$

Then $P \xrightarrow{\overline{x}(z)} \xrightarrow{xw} P' \stackrel{\mathrm{def}}{=} [w = z]z$ and, where $D = \{(x, z), (z, x)\}$, we have $P' \not\approx_{\mathrm{o}}^{D} \mathbf{0}$ because $\{z/w\}$ respects D, while $P' \not\approx_{\mathrm{o}}^{D} z$ because the identity respects D, so $P \not\approx_{\mathrm{o}} Q$. On the other hand, $P' \approx_{\mathrm{q}}^{\{z\}} \mathbf{0}$ because $\{z/w\}$ does not respect $\{z\}$, and so $P \approx_{\mathrm{q}} Q$. □

To prove the characterization result we need that open barbed bisimilarity is preserved by arbitrary substitution.

Lemma 6. $P \stackrel{\bullet}{\approx}_{\mathrm{o}} Q$ implies $P\sigma \stackrel{\bullet}{\approx}_{\mathrm{o}} Q\sigma$, for all σ.

Proof Suppose $\sigma = \{{}^{y_1 \cdots y_n}\!/\!_{x_1 \ldots x_n}\}$ where $\{x_1, \ldots, x_n\}$ is the support of σ. Let a be a fresh name and set

$$P_1 \stackrel{\text{def}}{=} \boldsymbol{\nu} a\, (\overline{a} y_1. \ldots. \overline{a} y_n \mid a(x_1). \ldots. a(x_n). P)$$
$$Q_1 \stackrel{\text{def}}{=} \boldsymbol{\nu} a\, (\overline{a} y_1. \ldots. \overline{a} y_n \mid a(x_1). \ldots. a(x_n). Q)\ .$$

By clause (4) of Definition 2, $P_1 \stackrel{\bullet}{\approx}_{\mathrm{o}} Q_1$. Using some simple properties of $\stackrel{\bullet}{\approx}_{\mathrm{o}}$, we have

$$P_1 \stackrel{\bullet}{\approx}_{\mathrm{o}} \underbrace{\tau. \ldots. \tau.}_{n} P\sigma \stackrel{\bullet}{\approx}_{\mathrm{o}} P\sigma\ ,$$

and similarly, $Q_1 \stackrel{\bullet}{\approx}_{\mathrm{o}} Q\sigma$. Hence by transitivity, $P\sigma \stackrel{\bullet}{\approx}_{\mathrm{o}} Q\sigma$. $\Box$

The following result holds for the π-calculus and for its extension with infinite sums.

Theorem 3 (Characterization Theorem for open barbed bisimilarity). For any processes P and Q, $P \approx_{\mathrm{q}} Q$ iff $P \stackrel{\bullet}{\approx}_{\mathrm{o}} Q$.

Proof The implication from left to right holds because $\approx_{\mathrm{q}}$ is an open barbed bisimulation. This follows from the definitions and the fact that $\approx_{\mathrm{q}}$ is a congruence, by Lemma 4.

For the other implication, we define a family of relations $\{\mathcal{R}^{\widetilde{x}} \mid \widetilde{x} \subseteq \mathsf{N} \text{ finite}\}$ such that $\stackrel{\bullet}{\approx}_{\mathrm{o}}$ is included in $\mathcal{R}^{\emptyset}$, and show that it is a quasi-open bisimulation.

Suppose $\widetilde{x} = \{x_i \mid i \in I\}$. Set $(P, Q) \in \mathcal{R}^{\widetilde{x}}$ if there is $\widetilde{a} = \{a_i \mid i \in I\}$ (with $a_i \neq a_j$ for $i \neq j$) such that $\widetilde{a} \cap \mathsf{fn}(P, Q, \widetilde{x}) = \emptyset$ and

$$\boldsymbol{\nu} \widetilde{x}\, (\mathit{\Pi}_{i \in I} !\overline{a_i} x_i \mid P) \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu} \widetilde{x}\, (\mathit{\Pi}_{i \in I} !\overline{a_i} x_i \mid Q)\ . \tag{1}$$

We consider clauses (4), (1), and (2) in Definition 6; the argument for clause (3) is similar to those for (1) and (2).

Suppose $(P, Q) \in \mathcal{R}^{\widetilde{x}}$. Let $P_1 \stackrel{\text{def}}{=} \boldsymbol{\nu} \widetilde{x}\, (\mathit{\Pi}_{i \in I} !\overline{a_i} x_i \mid P)$ and $Q_1 \stackrel{\text{def}}{=} \boldsymbol{\nu} \widetilde{x}\, (\mathit{\Pi}_{i \in I} !\overline{a_i} x_i \mid Q)$ be as in equation (1).

Clause (4) Suppose σ respects $\widetilde{x}$. Choose $\widetilde{b} = \{b_i \mid i \in I\}$ such that $b_i \neq b_j$ for $i \neq j$ and $\widetilde{b} \cap \mathsf{fn}(P, Q, \widetilde{x}, P\sigma, Q\sigma, \widetilde{x}\sigma) = \emptyset$. Let $\theta = \{\widetilde{b}/\widetilde{a}\}$. Then by applying Lemma 6 to equation (1) with the substitution θ,

$$\boldsymbol{\nu} \widetilde{x}\, (\mathit{\Pi}_{i \in I} !\overline{b_i} x_i \mid P) \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu} \widetilde{x}\, (\mathit{\Pi}_{i \in I} !\overline{b_i} x_i \mid Q)\ . \tag{2}$$

Let ρ be the substitution that agrees with σ except that $b_i \rho = b_i$ for each i. Then by applying Lemma 6 to equation (2) with the substitution ρ, where $\widetilde{y} = \widetilde{x}\sigma$ we have

$$\boldsymbol{\nu} \widetilde{y}\, (\mathit{\Pi}_{i \in I} !\overline{b_i} y_i \mid P\sigma) \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu} \widetilde{y}\, (\mathit{\Pi}_{i \in I} !\overline{b_i} y_i \mid Q\sigma)\ .$$

Hence $(P\sigma, Q\sigma) \in \mathcal{R}^{\widetilde{y}}$, as required.

Clause (1) We give just the argument for input actions. Those for free-output and τ actions are of a similar nature.

Suppose $P \xrightarrow{x\,z} P'$. We have to find Q' such that $Q \xRightarrow{x\,z} Q'$ and $(P',Q') \in \mathcal{R}^{\widetilde{x}}$. There are four cases, determined by whether or not $x \in \widetilde{x}$ and whether or not $z \in \widetilde{x}$. We give just one case. The arguments for the others are variations of it.

Suppose $x \in \widetilde{x}$, say $x = x_i$, and $z \notin \widetilde{x}$. Let s, s', and u be fresh names, and consider the context

$$C \stackrel{\text{def}}{=} \Big(s + a_i(u).(s' + \overline{u}z)\Big) \mid [\cdot]\ .$$

We have

$$C[P_1] \Longrightarrow P_2 \stackrel{\text{def}}{=} \mathbf{0} \mid \boldsymbol{\nu}\widetilde{x}\,(\Pi_{i\in I}!\overline{a_i}x_i \mid P')$$

and it holds that not $P_2 \Downarrow_s$ and not $P_2 \Downarrow_{s'}$. Since $P_1 \stackrel{\bullet}{\approx}_{\mathrm{o}} Q_1$, there is Q_2 such that $C[Q_1] \Longrightarrow Q_2 \stackrel{\bullet}{\approx}_{\mathrm{o}} P_2$, so in particular it holds that not $Q_2 \Downarrow_s$ and not $Q_2 \Downarrow_{s'}$. The only possibility is that

$$Q_2 = \mathbf{0} \mid \boldsymbol{\nu}\widetilde{x}\,(\Pi_{i\in I}!\overline{a_i}x_i \mid Q')$$

for some Q' such that $Q \xRightarrow{x\,z} Q'$. Since $P_2 \stackrel{\bullet}{\approx}_{\mathrm{o}} Q_2$ we have

$$\boldsymbol{\nu}\widetilde{x}\,(\Pi_{i\in I}!\overline{a_i}x_i \mid P') \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu}\widetilde{x}\,(\Pi_{i\in I}!\overline{a_i}x_i \mid Q')$$

and so $(P',Q') \in \mathcal{R}^{\widetilde{x}}$.

Clause (2) Suppose $P \xrightarrow{\overline{x}(z)} P'$, where z is fresh. We have to find Q' such that $Q \xRightarrow{\overline{x}(z)} Q'$ and $(P',Q') \in \mathcal{R}^{\widetilde{x}\cup\{z\}}$. There are two subcases. We give one; the argument for the other is a variation of it.

Suppose $x \in \widetilde{x}$, say $x = x_i$. Let s, s', t, u, and a be fresh names, and consider the context

$$C \stackrel{\text{def}}{=} \Big(s + a_i(u).(s' + u(z).(\,!\overline{a}z \mid \Pi_{c\in\mathsf{fn}(P,Q)}[z=c]t))\Big) \mid [\cdot]\ .$$

We have

$$C[P_1] \Longrightarrow P_2 \stackrel{\text{def}}{=} \boldsymbol{\nu}z\,\Big(!\overline{a}z \mid \Pi_{c\in\mathsf{fn}(P,Q)}[z=c]t \mid \boldsymbol{\nu}\widetilde{x}\,(\Pi_{i\in I}!\overline{a_i}x_i \mid P')\Big)$$

and it holds that not $P_2 \Downarrow_s$ and not $P_2 \Downarrow_{s'}$ and not $P_2 \Downarrow t$. Since $P_1 \stackrel{\bullet}{\approx}_{\mathrm{o}} Q_1$, there is Q_2 such that $C[Q_1] \Longrightarrow Q_2 \stackrel{\bullet}{\approx}_{\mathrm{o}} P_2$, so in particular it holds that not $Q_2 \Downarrow_s$ and not $Q_2 \Downarrow_{s'}$ and not $Q_2 \Downarrow t$. The only possibility is that

$$Q_2 = \boldsymbol{\nu}z\,\Big(!\overline{a}z \mid \Pi_{c\in\mathsf{fn}(P,Q)}[z=c]t \mid \boldsymbol{\nu}\widetilde{x}\,(\Pi_{i\in I}!\overline{a_i}x_i \mid Q')\Big)$$

for some Q' such that $Q \xRightarrow{\overline{x}(z)} Q'$. Since $P_2 \stackrel{\bullet}{\approx}_{\mathrm{o}} Q_2$ we have, using axioms of structural congruence and the property

$$\boldsymbol{\nu}y\,([y=b]M \mid R) \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu}y\,R \qquad \text{if } y \neq b,$$

that

$$P_2 \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu}z\,\boldsymbol{\nu}\widetilde{x}\,\Big(!\overline{a}z \mid \Pi_{i\in I}!\overline{a_i}x_i \mid P')\Big)$$

and

$$Q_2 \stackrel{\bullet}{\approx}_{\mathrm{o}} \boldsymbol{\nu}z\,\boldsymbol{\nu}\widetilde{x}\,\Big(!\overline{a}z \mid \Pi_{i\in I}!\overline{a_i}x_i \mid Q')\Big)\ .$$

Hence $(P',Q') \in \mathcal{R}^{\widetilde{x}\cup\{z\}}$, as required.

This completes the outline of the proof of the theorem. $\square$

References

1. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *28th Annual Symposium on Principles of Programming Languages*. ACM, 2001.
2. P. Aczel. An introduction to inductive definitions. In *Handbook of Mathematical Logic*. North Holland, 1977.
3. R. Amadio, I. Castellani, and D. Sangiorgi. On bisimulations for the asynchronous π-calculus. *Theoretical Computer Science*, 195(2):291–324, 1998.
4. C. Fournet and G. Gonthier. A hierarchy of equivalences for asynchronous calculi. In *ICALP'98: Automata, Languages and Programming*, volume 1443 of *Lecture Notes in Computer Science*. Springer-Verlag, 1998.
5. K. Honda and N. Yoshida. On reduction-based process semantics. *Theoretical Computer Science*, 152(2):437–486, 1995.
6. A. Jeffrey and J. Rathke. A theory of bisimulation for a fragment of Concurrent ML with local names. In *15th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society Press, 2000.
7. M. Merro. *Locality in the π-calculus and Applications to Object-Oriented Languages*. PhD thesis, Ecole des Mines de Paris, 2000.
8. R. Milner. The polyadic π-calculus: a tutorial. In *Logic and Algebra of Specification*. Springer-Verlag, 1993.
9. R. Milner and D. Sangiorgi. Barbed bisimulation. In *ICALP'92: Automata, Languages and Programming*, volume 623 of *Lecture Notes in Computer Science*. Springer-Verlag, 1992.
10. U. Montanari and V. Sassone. Dynamic congruence vs. progressing bisimulation for CCS. *Fundamenta Informaticae*, XVI(2):171–199, 1992.
11. D. Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis, Department of Computer Science, University of Edinburgh, 1992.
12. D. Sangiorgi. A theory of bisimulation for the π-calculus. *Acta Informatica*, 33:69–97, 1996.
13. D. Sangiorgi. The name discipline of uniform receptiveness. *Theoretical Computer Science*, 221:457–493, 1999.