On Bisimilarity and Substitution in Presence of Replication

Daniel Hirschkoff, Damien Pous

On Bisimilarity and Substitution in Presence of Replication*

Daniel Hirschkoff[1] and Damien Pous[2]

[1] ENS Lyon, Université de Lyon, CNRS, INRIA
[2] CNRS, Laboratoire d'Informatique de Grenoble

Abstract. We prove a new congruence result for the π-calculus: bisimilarity is a congruence in the sub-calculus that does not include restriction nor sum, and features top-level replications. Our proof relies on algebraic properties of replication, and on a new syntactic characterisation of bisimilarity. We obtain this characterisation using a rewriting system rather than a purely equational axiomatisation. We then deduce substitution closure, and hence, congruence. Whether bisimilarity is a congruence when replications are unrestricted remains open.

1 Introduction

We study algebraic properties of behavioural equivalences, and more precisely, of strong bisimilarity ($\sim$). This has long been an important question in concurrency theory, with a particular focus on the search for axiomatisations of bisimilarity (see [1] for a survey). Our primary goal is to establish congruence results for the π-calculus [13]. At the heart of the π-calculus is the mechanism of *name-passing*, which is the source of considerable expressive power. Name-passing however introduces substitutions in the formalism, and these in turn lead to irregularities in the behavioural theory of processes: due to the input prefix, we need bisimilarity to be closed under substitutions for it to be a congruence.

To establish substitution closure, we exploit a new axiomatisation of bisimilarity. Several axiomatisation results for process calculi that feature an operator of parallel composition ($|$) have been derived by decomposing this operator using sum, and possibly left merge [4,3,1]. We, on the contrary, are interested in treating parallel composition as a primitive operator. One reason for this is that the sum operator is often absent from the π-calculus since it can be encoded [9], under certain conditions. More importantly, this operator makes substitution closure fail [13,2], so that existing axiomatisations of bisimilarity in calculi featuring sum do not help when it comes to reason about congruence in the π-calculus.

In the present paper, we focus on properties of the replication operator [8], noted ($!$). As [13,2] shows, bisimilarity is not substitution closed when both replication and name restriction are present in the calculus, and we have established

* Work partially funded by the French ANR projects "Curry-Howard pour la Concurrence" CHOCO ANR-07-BLAN-0324 and COMPLICE ANR-08-BLANC-0211-01.

in [5] that it is when we renounce to replication. To our knowledge, congruence of bisimilarity in the restriction-free π-calculus with replication is an open problem [13]; we provide here a partial answer.

Behavioural properties of replication. Replication can be seen as an "infinitary version" of parallel composition. Structural congruence traditionally contains the following *structural laws* (given here for CCS): $!a.P \mid a.P \equiv !a.P$ and $!a.P \mid !a.P \equiv !a.P$, so that a replicated process acts as an unbounded number of copies of that process in parallel. A contribution of this work is an analysis of *behavioural laws* capturing other properties of replication. For example, for any context C, we have

$$!a.P \mid C[a.P] \sim !a.P \mid C[\mathbf{0}] \qquad \text{and} \qquad !a.C[a.C[\mathbf{0}]] \sim !a.C[\mathbf{0}] \ .$$

The left-hand side law is a generalisation the first structural congruence law: a replicated process can erase one of its copies arbitrarily deep in a term. The right-hand side law is more involved: read from right to left, it shows that a replicated process is able to replicate itself. Its most trivial instance is $!a.a \sim !a$.

Although the above laws are the basic ingredients we need in order to characterise bisimilarity in our setting, they do not form a complete axiomatisation of bisimilarity, as the following example shows:

$$P_1 = !a.(b|a.c) \mid !a.(c|a.b) \ \sim \ !a.b \mid !a.c = P_2 \ .$$

P_1 can be obtained from P_2 by inserting a copy of $a.b$ inside $!a.c$, and, symmetrically, a copy of $a.c$ inside $!a.b$. It seems reasonable to consider P_2 as a kind of normal form of P_1; however, P_1 and P_2 cannot be related using the above laws. Describing this phenomenon of "mutual replication" in all its generality leads to complicated equational schemata, so that we take another approach.

Overview. Our first contribution is a syntactic characterisation of bisimilarity on a fragment of CCS with top-level replications. This characterisation relies on a rewriting system for processes (such that P_1 rewrites into P_2). An important technical notion we need to introduce is that of *seed*: a seed of P is a process bisimilar to P of minimal size; for example, P_2 is a seed of P_1. Our proof goes by characterising bisimilarity on seeds, and establishing that any process P can be rewritten into a seed of P.

Our second contribution is congruence of bisimilarity in the corresponding fragment of the π-calculus. Concretely, we prove that bisimilarity is substitution closed by considering *visible* bisimilarity (sometimes called *io*-bisimilarity [7]), the equivalence obtained by disallowing challenges along internal communications. Visible bisimilarity is inherently substitution closed, and our characterisation allows us to show that it coincides with bisimilarity.

Since the technical developments that lead to congruence in the π-calculus follow to a large extent the path of our proofs for CCS, we moved them to the appendix. On the contrary, we provide detailed proofs and present most intermediate steps for CCS. We indeed view the reasonings we use in our proofs

$$\frac{}{\alpha.F \xrightarrow{\alpha} F} \qquad \frac{}{!\alpha.F \xrightarrow{\alpha} !\alpha.F \,|\, F} \qquad \frac{P \xrightarrow{\mu} P'}{P|Q \xrightarrow{\mu} P'|Q} \qquad \frac{P \xrightarrow{\overline{a}} P' \qquad Q \xrightarrow{a} Q'}{P|Q \xrightarrow{\tau} P'|Q'}$$

Fig. 1. Labelled Transition System for mCCS.

as an important contribution of this work. In particular, we make use of both algebraic and coinductive reasoning, notably using "up-to techniques" for bisimulation [12,10,11].

Outline. We describe the subset of CCS we work with and we prove general properties of replication in Sect. 2. In Sect. 3, we introduce the notion of seed, and give a characterisation of bisimilarity on seeds. The rewriting system is defined in Sect. 4, where we show that any process can be rewritten into a seed, and where we characterise strong bisimilarity. We present our new congruence result for the π-calculus in Sect. 5. Section 6 suggests directions for future work.

2 General Setting, and Properties of Replication

We let a, b range over a countable set of *names*; we work in a fragment of CCS which we call mCCS, defined by the following grammar:

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}r} \alpha,\beta & ::= & a \mid \overline{a} & \mu & ::= & \alpha \mid \tau & \text{(actions and labels)} \\ E,F & ::= & \mathbf{0} \mid \alpha.F \mid F|F & P,Q & ::= & F \mid !\alpha.F \mid P|P & \text{(processes)} \\ D & ::= & [] \mid \alpha.D \mid D|F & C & ::= & D \mid !\alpha.D \mid C|P & \text{(contexts)} \end{array}$$

This calculus features no restriction, no sum, and allows only top-level replicated prefixes. Note that the τ prefix is not included in the syntax, and only appears in *labels* (μ); we return to this point in Sect. 6. We use P, Q to range over processes; according to the syntax, a *finite* process (F) is a process which does not contain an occurrence of the replication operator ($!\alpha.$). We omit trailing occurrences of $\mathbf{0}$, and write, e.g., $\alpha.\beta$ for $\alpha.\beta.\mathbf{0}$. We shall sometimes write $\prod_{i\in[1..k]} \alpha_i.F_i$ for $\alpha_1.F_1 \,|\, \ldots \,|\, \alpha_k.F_k$. We extend the syntactic operator of replication to a function defined over processes by letting

$$!\mathbf{0} \triangleq \mathbf{0} \qquad !(P|Q) \triangleq !P|!Q \qquad !!\alpha.F \triangleq !\alpha.F \ .$$

In particular, $!F$ will always denote a process having only replicated (parallel) components. We let C range over single-hole *contexts*, mapping finite processes to processes, and similarly for *finite contexts*, ranged over using D. Note that the hole cannot occur immediately under a replication in C.

The labelled transition system (LTS) we associate to this process calculus is standard (Fig. 1 – we omit symmetric rules for parallel composition). This LTS yields the following standard notion of *bisimilarity*, ($\sim$). We also define *visible bisimilarity* ($\dot{\sim}$), where silent transitions are not taken into account.

Definition 1 Strong bisimilarity ($\sim$) *is the largest symmetric binary relation over processes such that whenever* $P \sim Q$ *and* $P \xrightarrow{\mu} P'$*, there exists* Q' *such that* $P' \sim Q'$ *and* $Q \xrightarrow{\mu} Q'$. Visible bisimilarity ($\dot{\sim}$) *is defined similarly, by restricting challenges to the cases where* $\mu \neq \tau$.

Both bisimilarities are congruences. They are moreover preserved by the extended replication function, and we have $\sim \subseteq \dot{\sim}$. On finite processes, bisimilarity and visible bisimilarity coincide and can be characterised using the following *distribution law*, where there are as many occurrences of F on both sides [5]:

$$\alpha.(F|\alpha.F|\ldots|\alpha.F) \;\sim\; \alpha.F|\alpha.F|\ldots|\alpha.F \;. \tag{D}$$

We now present some important properties of replicated processes w.r.t. bisimilarity. The following proposition allows us to obtain the two laws from the introduction, that involve copying replicated sub-terms.

Proposition 2 *If* $C[\mathbf{0}] \sim !\alpha.F|P$*, then* $C[\mathbf{0}] \sim C[\alpha.F]$.

Proof. We show that $\mathcal{R}= \{(C[\mathbf{0}], C[\alpha.F]) \;/\; \forall C \text{ s.t. } C[\mathbf{0}] \sim !\alpha.F|P \text{ for some } P\}$ is a bisimulation up to transitivity [10,11]. There are several cases to consider:

- the hole occurs at top-level in the context ($C = []|Q$) and the right-hand side process does the following transition: $C[\alpha.F] \xrightarrow{\alpha} F|Q$. By hypothesis, $Q \sim !\alpha.F|P$ so that we find Q' such that $Q \xrightarrow{\alpha} Q'$ and $Q' \sim !\alpha.F|F|P$. Injecting the latter equality gives $Q' \sim Q|F$, so that Q' closes the diagram.
- the hole occurs under a replicated prefix of the context ($C = !\beta.D|Q$) which is fired: we have $C[\mathbf{0}] \xrightarrow{\beta} P_l = C[\mathbf{0}]|D[\mathbf{0}]$ and $C[\alpha.F] \xrightarrow{\beta} P_r = C[\alpha.F]|D[\alpha.F]$. This is where we work up to transitivity: these processes are not related by $\mathcal{R}$ (we work with single-hole contexts), but we have $P_l \;\mathcal{R}\; P_c \;\mathcal{R}\; P_r$, for $P_c = C[\mathbf{0}]|D[\alpha.F]$, using contexts $C_{lc} = C[\mathbf{0}]|D$ and $C_{cr} = C|D[\alpha.F]$.
- the hole occurs under a non-replicated prefix in the context ($C = \beta.D|Q$), or the context triggers a transition that does not involve or duplicate the hole; it suffices to play the bisimulation game.
- we are left with the cases where a synchronisation is played; they can be handled similarly (in particular because contexts have a single hole). □

As a consequence, we obtain the validity of the following laws. We shall see in the sequel that together with the distribution law (D), they capture the essence of bisimilarity in our calculus.

$$!\alpha.F \mid C[\alpha.F] \;\sim\; !\alpha.F \mid C[0] \tag{A}$$

$$!\alpha.D[\alpha.D[\mathbf{0}]] \;\sim\; !\alpha.D[\mathbf{0}] \tag{A$'$}$$

(Note that Prop. 2 and the above laws hold for full CCS and for the π-calculus, as long as the hole does not occur as argument of a sum in C and D, and C and D do not bind names occurring in $\alpha.F$.) We now give two useful cancellation properties of visible bisimilarity; they are actually also valid for bisimilarity ($\sim$).

Lemma 3 *If* $!F \dot{\sim} P|Q$*, then* $!F \dot{\sim} !F|P$*.*

Proof. We reason purely algebraically: we replicate both sides of $!F \dot{\sim} P|Q$, and add P in parallel (since $!P \dot{\sim} !P|P$): this gives $!F \dot{\sim} !P|!Q \dot{\sim} !P|!Q|P$. We deduce $!F \dot{\sim} !F|P$ by injecting the first equivalence into the second one. □

Proposition 4 *If* $!F|F_0 \dot{\sim} !E|E_0$ *with* F_0, E_0 *finite, then* $!F \dot{\sim} !E$*.*

Proof. By emptying F_0 on the left-hand side[1], we find a finite process E_1 such that $!F \dot{\sim} !E|E_1$ $(*)$. Similarly, by emptying E_0 on the right-hand side we find F_1 such that $!F|F_1 \dot{\sim} !E$ $(**)$. By injecting the former equivalence in the latter, we have $!E|E_1|F_1 \dot{\sim} !E$ $(\dagger)$. By Lemma 3, $(**)$ gives $!E \dot{\sim} !E|F_1$, that we can inject into $(*)$ to obtain $!E|E_1|F_1 \dot{\sim} !F$. We finally deduce $!E \dot{\sim} !F$ from $(\dagger)$. □

Again, these properties are not specific to the subset of CCS we focus on: Prop. 4 holds provided that both F_0 and E_0 can be reduced to the empty process using transitions (this is the case, e.g., for the *normed* processes of [6]). The counterpart of this cancellation property does not hold; the replicated parts of bisimilar processes cannot always be cancelled: we cannot deduce $a \dot{\sim} \mathbf{0}$ from $!a|a \dot{\sim} !a|\mathbf{0}$.

3 Seeds

Definition 5 (Size, seed) *The* size of P*, noted* $\sharp P$*, is the number of prefixes in* P*. A* seed of P *is a process* Q *of minimal size such that* $P \dot{\sim} Q$*, whose number of replicated components is maximal among the processes of minimal size. When* P *is a seed of* P*, we simply say that* P *is a seed.*

We show how to rewrite an arbitrary process into a seed in Sect. 4; in this section, we give a characterisation of bisimilarity on seeds (Prop. 12).

Definition 6 (Distribution congruence) *We call* distribution congruence *the smallest congruence relation* $\equiv$ *that satisfies the laws of an abelian monoid for* $(|, \mathbf{0})$ *and the distribution law* (D)*.*

Fact 7 *We have* $\equiv \subseteq \sim \subseteq \dot{\sim}$*; the latter equivalence is substitution closed; on finite processes, the three relations coincide.*

Proof. The inclusions and the substitution closure of $\dot{\sim}$ are straightforward. On finite processes, $\equiv = \sim$ was proved in in [5], and one can deduce from other results therein that $\dot{\sim} \subseteq \sim$ (a proof is given for π in appendix—Thm. B4). □

It is easy to show that distribution congruence is decidable, and only relates processes having the same size. In the sequel, we always work modulo distribution congruence. We shall prove that on seeds, bisimilarity actually coincides with

[1] In the present case, "emptying F_0" means playing all prefixes of F_0 in the bisimulation game between $!F|F_0$ and $!E|E_0$. We shall reuse this terminology in some proofs below; note that this is possible only with finite processes.

distribution congruence. Thanks to Prop. 4, the replicated parts of bisimilar seeds are necessarily bisimilar. As a consequence, in the remainder of this section, we fix a seed S having only replicated components: $S = \prod_i !\alpha_i.S_i$, and we study processes obtained by composing S with finite processes.

Definition 8 (Clean process, residual) *A finite process F is* clean w.r.t. *S, written $S\#F$, if F does not contain a sub-term of the form $\alpha_i.S_i$: for all i and finite context D, $F \not\equiv D[\alpha_i.S_i]$.*

A finite process R is a residual of *S, written $S \rightsquigarrow R$ when there exist $k > 0$, $\alpha_1, .., \alpha_k$, and $P_1, .., P_k$ such that $S \xrightarrow{\alpha_1} P_1 \ldots \xrightarrow{\alpha_k} P_k \equiv S|R$. We shall use R to range over such residual processes.*

Note that if $S \rightsquigarrow R$, then R is a parallel composition of sub-terms of the S_is. We can also remark that residuals and clean processes are stable under transitions: if $S\#F$ (resp. $S \rightsquigarrow F$) and $F \xrightarrow{\alpha} F'$, then $S\#F'$ (resp. $S \rightsquigarrow F'$). As shown by the following lemma, sub-terms of seeds are clean:

Lemma 9 *(i) If $S|F$ is a seed, then $S\#F$;*
(ii) If $S \rightsquigarrow \alpha.R$, then there exist i, D such that $S_i \equiv D[\alpha.R]$.
(iii) If $S \rightsquigarrow R$, then $S\#R$.

A seed cannot absorb its non-trivial residuals:

Lemma 10 *$S \dot{\sim} S|R$ and $S \rightsquigarrow R$ entail $R = \mathbf{0}$.*

Proof. Suppose by contradiction $R \equiv \alpha.R_0|R_1$. Lemma 3 gives $S \dot{\sim} S|\alpha.R_0$, hence $S \dot{\sim} S|!\alpha.R_0$ $(*)$ by replicating all processes. Moreover, $S \rightsquigarrow \alpha.R_0$, so that Lemma 9(ii) gives i, D such that $S_i \equiv D[\alpha.R_0]$. Therefore, by $(*)$ and law (A), we obtain $S \dot{\sim} \prod_{j\neq i} !\alpha_j.S_j|!\alpha_i.D[\mathbf{0}]|!\alpha.R_0$. The latter process has the same size as S, but it has strictly more replicated components, which is contradictory. □

More generally, the replicated part of visible bisimilar seeds can be cancelled:

Lemma 11 *If $S|F \dot{\sim} S|E$, $S\#F$, and $S\#E$, then $F \equiv E$.*

Proof. We prove the following stronger property, by induction on n: for all n, F, E such that $\sharp F, \sharp E \leq n$, $S\#F$, and $S\#E$, we have:

$$\begin{cases} (i) & \forall P, S|F \dot{\sim} S|P|E \text{ entails } \sharp E \leq \sharp F\,; \\ (ii) & S|F \dot{\sim} S|E \text{ entails } E \equiv F\,. \end{cases}$$

The case $n = 0$ is trivial; assume $n > 0$.

(i) Suppose $\sharp F < \sharp E$ by contradiction. By emptying F, we get P', E' such that $S \dot{\sim} S|P'|E'$, with $0 < \sharp E' \leq \sharp E$. Write $E' = \alpha.E_0|E_1$, then $S \dot{\sim} S|\alpha.E_0$ by Lemma 3, and $S|S_i \dot{\sim} S|E_0$ for some i with $\alpha_i = \alpha$. Necessarily, $\sharp S_i \leq \sharp E_0$: otherwise, by emptying E_0, we would obtain a non empty residual R such $S|R \dot{\sim} S$, which would contradict Lemma 10. Since $\sharp E_0 < \sharp E' \leq \sharp E \leq n$, we can use the induction hypothesis, so that $S_i \equiv E_0$, and hence $\alpha_i.S_i \equiv \alpha.E_0$, which contradicts $S\#E$.

(ii) By the above point, $\sharp F = \sharp E$. We show that $\mathcal{R} \triangleq \{(F, E)\} \cup \equiv$ is a visible bisimulation. If $F \xrightarrow{\alpha} F'$, then $S|F \xrightarrow{\alpha} S|F'$, and $S|E$ can answer this challenge: $S|E \xrightarrow{\alpha} S|E'$ with $S|F' \mathrel{\dot\sim} S|E'$. If the answer comes from E, we are done by induction: $\sharp E' = \sharp F' = \sharp F - 1 \leq n - 1$. Otherwise, i.e., if $S|F' \mathrel{\dot\sim} S|S_i|E$ for some i, we get a contradiction with (i): we would have $\sharp E \leq \sharp F' = \sharp E - 1$. Challenges of E are handled symmetrically. □

We can now characterise bisimilarity on seeds:

Proposition 12 *For all seeds P, P', $P \mathrel{\dot\sim} P'$ iff $P \sim P'$ iff $P \equiv P'$.*

Proof. By Fact 7, it suffices to show that $P \mathrel{\dot\sim} P'$ entails $P \equiv P'$. Write P and P' as $S|F$ and $S'|F'$, where S, S' are replicated processes. By Prop. 4, $S \mathrel{\dot\sim} S'$. Moreover, S and S' are necessarily seeds because P and P' are (hence the notation). Write $S \equiv \prod_{i \leq m} !\alpha_i.S_i$ and $S' \equiv \prod_{j \leq n} !\alpha'_j.S'_j$, play each prefix on the left-hand side and apply Lemma 11 to show that there exists a map $\sigma : [1..m] \to [1..n]$, such that $\alpha_i.S_i \equiv \alpha'_{\sigma i}.S'_{\sigma i}$ (recall that $S \# S_j$ by Lemma 9(iii)). This map is bijective: we could otherwise construct a smaller seed. Therefore, $S \equiv S'$. By Lemma 9(i), $S\#F$ and $S'\#F'$, which allows us to deduce $F \equiv F'$, using Lemma 11. Finally, $P \equiv P'$. □

We conclude this section by the following remark: seeds are stable under transitions, so that they actually form a proper sub-calculus of CCS.

Proposition 13 *If P is a seed and $P \xrightarrow{\mu} P'$, then P' is a seed.*

4 Rewriting Processes to Normal Forms

By Prop. 12, the seed of a process P is unique up to distribution congruence ($\equiv$); in the sequel, we denote it by $\mathsf{s}(P)$. In this section, we show that the seed of a process can be obtained using a rewriting system. This entails two important properties of mCCS: visible and strong bisimilarity coincide and bisimilarity is closed under substitutions (i.e., bisimilar processes remain bisimilar when applying an arbitrary name substitution).

Definition 14 (Rewriting) *Any process T induces a relation between processes, written $\xrightarrow{T}$, defined by the following rules, modulo $\equiv$:*

$$\frac{T \equiv !\alpha.F|Q}{C[\alpha.F] \xrightarrow{T} C[\mathbf{0}]}\ (\text{R1}) \qquad \frac{}{!\alpha.F|!\alpha.F|P \xrightarrow{T} !\alpha.F|P}\ (\text{R2})$$

The reflexive transitive closure of $\xrightarrow{T}$ is written $\xrightarrow{T}{}^*$.

We give some intuitions about how the rewriting rules work. First, only the replicated part of T matters when rewriting with $\xrightarrow{T}$. Relation $\xrightarrow{T}$ is nevertheless defined for an arbitrary process T in order to facilitate the presentation of some

results below. Then, we observe that it is only sensible to rewrite P using $\xrightarrow{T}$ when T is a seed of P. This means in particular that the rewriting system does not provide a direct way to compute the seed of a process (since the seed has to be guessed). It is rather a procedure to check that some process T is a "simplification" of P—Lemma 15 below validates this intuition. Rule (R2) is rather self-explanatory. The rewriting rule (R1) relates to laws (A) and (A′); we illustrate its use by considering the following examples:

$$!a.b \mid !b \mid b.a \xrightarrow{!a|!b} !a.b \mid !b \mid b \xrightarrow{!a|!b} !a.b \mid !b \xrightarrow{!a|!b} !a \mid !b \quad (1)$$

$$!a.(b \mid a.b) \xrightarrow{!a.b} !a.b \quad (2)$$

$$!a.b \mid !b.a \xrightarrow{!a|!b} !a.b \mid !b \xrightarrow{!a|!b} !a \mid !b \quad (3)$$

$$!a|!a.b \xrightarrow{!a|!b} !a|!a \xrightarrow{!a|!b} !a \quad (4)$$

(1) The first example shows how (R1) can be used to "implement" law (A) and erase redundant sub-terms. At each rewrite step, a copy of a component of the seed (here, $!a|!b$) is erased. In the third rewriting step, simplification occurs in a replicated component.
(2) Law (A′) is applied: a replicated component can be "simplified with itself".
(3) This example illustrates how the rewriting system solves the problem we exposed in the introduction (processes P_1 and P_2), where two replicated components have to simplify each other: by guessing the seed ($!a|!b$), we are able to apply these two simplifications in sequence.
(4) Here, we make a wrong guess about the seed: when assuming that $!b$ is part of the seed, we can erase the prefix b in $!a.b$. However, at the end, we are not able to validate this assumption: $!b$ does not appear in the normal form.

Accordingly, we obtain the following correctness criterion:

Lemma 15 (Soundness) *If $P \xrightarrow{T}{}^{*} T$, then $P \sim T$.*

Definition 16 (Joinability) *We say that processes P and Q are* joinable*, written $P \curlyvee Q$, if there exists a process T such that $P \xrightarrow{T}{}^{*} T$ and $Q \xrightarrow{T}{}^{*} T$.*

By Lemma 15, $\curlyvee \subseteq \sim$; the other property which is required in order to characterise bisimilarity is *completeness* of the rewriting system, i.e., that all bisimilar processes can be joined. For this, we show that any process can be rewritten into a seed. The proof necessitates the following technical lemma:

Lemma 17 *For all P, either P is a seed, or $P \xrightarrow{\mathsf{s}(P)} P'$ for some P' s.t. $P \sim P'$.*

Proof. Write $P \equiv !F|F^P$ and $\mathsf{s}(P) \equiv S|F^S$, with $F \equiv \prod_i \beta_i.F_i$ and $S \equiv \prod_j !\alpha_j.S_j$. By Prop. 4, and since $P \dot{\sim} \mathsf{s}(P)$, $!F \dot{\sim} S$ $(*)$.

Any transition at β_i by $!F$ is answered by S at some $\alpha_{\sigma i}$, yielding equivalence $!F|F_i \;\dot{\sim}\; S|S_{\sigma i}$, which in turn gives $S|F_i \;\dot{\sim}\; S|S_{\sigma i}$, by injecting $(*)$. By Lemma 11, either (a) $F_i \equiv S_{\sigma i}$, or (b) $\neg(S\#F_i)$. In the latter case, (b), this

means that P admits some $\alpha_j.S_j$ as a sub-term, and can be rewritten using rule (R1), the resulting process being bisimilar to P, by Prop. 2.

Suppose now that we are in case (a) for all transitions from $!F$, that is, for all i, there exists σi such that $\beta_i.F_i \equiv \alpha_{\sigma i}.S_{\sigma i}$. We observe that the converse (associating a ηj to all js) also holds, and that the number of parallel components in $!F$ is necessarily greater than the number of components in S (otherwise, we would obtain a smaller seed). In the case where this number is strictly greater, this means a replicated component appears twice in $!F$, so that P can be rewritten using rule (R2). We are left with the case where the two processes have the same number of components, which entails that they are equated by $\equiv$.

To sum up, either P can be rewritten, or $!F \equiv S$. In the latter case, we deduce $S \mid F^P \mathrel{\dot\sim} S \mid F^S$ from $(*)$, and since $S \# F^S$ by Lemma 9(i), there are two cases according to Lemma 11: either $F^P \equiv F^S$, in which case $P \equiv \mathsf{s}(P)$: P is a seed; or $\neg(S \# F^P)$, i.e., F^P admits some $\alpha_j.S_j$ as a sub-term, and we can rewrite P using (R1), getting a process bisimilar to P by Prop. 2. □

Proposition 18 (Completeness) *For all P, $P \xrightarrow{\mathsf{s}(P)}{}^* \mathsf{s}(P)$.*

Thanks to our characterisation of bisimilarity on seeds (Prop. 12), we obtain:

Theorem 19 (Characterisation) *In mCCS, visible and strong bisimilarity coincide with joinability: $P \mathrel{\dot\sim} Q$ iff $P \sim Q$ iff $P \curlyvee Q$.*

Proof. We have $\curlyvee \subseteq \sim \subseteq \mathrel{\dot\sim}$ by Lemma 15. Then, $P \mathrel{\dot\sim} Q$ entails $\mathsf{s}(P) \equiv \mathsf{s}(Q)$ by Prop. 12. Since $P \xrightarrow{\mathsf{s}(P)}{}^* \mathsf{s}(P)$ and $Q \xrightarrow{\mathsf{s}(Q)}{}^* \mathsf{s}(Q)$ by Prop. 18, we get $P \curlyvee Q$. □

This result has several consequences. First, we do not need to play silent transitions in bisimulation games. Second, bisimilarity is substitution closed in mCCS. Third, bisimilarity is decidable in mCCS: the definition of joinability is a priori not effective (we are not told how to find T); however, according to the proof of Thm. 19, it suffices to search for T among the processes whose size is smaller than both P and Q to test whether $P \curlyvee Q$.

It should be noted that Christensen et al. already proved decidability of bisimilarity in a larger subset of CCS [3], so that the latter consequence is not surprising. However, their axiomatisation exploits the sum operator and the expansion law, so that it cannot be used to establish substitution closure in our setting.

5 Congruence of Strong Bisimilarity in the π-calculus

In this section, we adapt the previous results from CCS to the π-calculus in order to obtain closure of bisimilarity under substitutions, and deduce congruence in the restriction-free π-calculus with only top-level replications.

In moving from CCS to π, some care has to be taken. The first reason for that is that "being a sub-term of" is more subtle in π than in CCS, because of issues related to binding and α-conversion. The second reason is that the LTS for the

$$\frac{}{\overline{a}\langle b\rangle.F \xrightarrow{\overline{a}\langle b\rangle} F} \qquad \frac{}{!\overline{a}\langle b\rangle.F \xrightarrow{\overline{a}\langle b\rangle} !\overline{a}\langle b\rangle.F \mid F} \qquad \frac{P \xrightarrow{\mu} P' \qquad \mathrm{bn}(\mu) \cap \mathrm{fn}(Q) = \emptyset}{P|Q \xrightarrow{\mu} P'|Q}$$

$$\frac{y \notin \mathrm{fn}(a(x).F)}{a(x).F \xrightarrow{a(y)} F\{y/x\}} \qquad \frac{y \notin \mathrm{fn}(a(x).F)}{!a(x).F \xrightarrow{a(y)} !a(x).F \mid F\{y/x\}} \qquad \frac{P \xrightarrow{\overline{a}\langle b\rangle} P' \qquad Q \xrightarrow{a(x)} Q'}{P|Q \xrightarrow{\tau} P'|Q'\{b/x\}}$$

Fig. 2. Labelled Transition System for $m\pi$.

π-calculus involves substitutions, and we must choose how to handle these in the definition of behavioural equivalence. Among the various notions of bisimilarity that exist for π, we shall actually adopt the simplest and coarsest one, namely ground bisimilarity: when ground bisimilarity is closed under substitutions, the ground, early and late versions of the equivalence coincide [13].

We let x, y, a, b range over a countable set of *names*. We work in the subset of the π-calculus, called $m\pi$, defined by replacing actions from the syntax of mCCS (Sect. 2) with the following production: $\alpha, \beta \ ::= \ a(x) \mid \overline{a}\langle b\rangle$. As usual, the operator of input prefix is binding, we write $\mathrm{fn}(P)$ for the set of free names of P, $\mathrm{bn}(\alpha)$ for the set of names bounded by α, and we let $P\{y/x\}$ stand for the capture-avoiding substitution of x with y in P. Note that contexts (C) can bind names (e.g., $a(x).[]$). The LTS for $m\pi$ is presented on Fig. 2, where symmetric rules for parallel composition are omitted. The conditions involving freshness of names ensure that $P \xrightarrow{a(x)} P'$ entails $x \notin \mathrm{fn}(P)$; this allows us to give a simple definition of ground bisimilarity:

Definition 20 Ground bisimilarity*, denoted by* $\sim$*, is the largest symmetric binary relation such that* $P \sim Q$ *entails that* $\mathrm{fn}(P) = \mathrm{fn}(Q)$ *and that whenever* $P \xrightarrow{\mu} P'$*, there exists* Q' *s.t.* $Q \xrightarrow{\mu} Q'$ *and* $P' \sim Q'$*.* Visible ground bisimilarity ($\dot{\sim}$) *is defined similarly, by restricting challenges to the cases where* $\mu \neq \tau$*.*

Since we lack the restriction operator, the condition on free names is actually enforced by standard notions of bisimilarity. In particular, this definition coincides with the standard definition of ground bisimilarity on $m\pi$ [13]: input prefixes are tested with fresh names. On finite $m\pi$-processes, ground bisimilarity is a substitution closed congruence [5], so that it coincides with early and late bisimilarities. We need to show that it also coincides with visible bisimilarity (the proof, given in appendix, exploits some technical results from [5]):

Theorem 21 *On finite* $m\pi$ *processes,* $\dot{\sim}$ *and* $\sim$ *coincide.*

As for CCS, we then establish that visible and ground bisimilarities coincide on all $m\pi$ processes. Since visible bisimilarity is easily shown to be substitution closed (Prop. 22 below, proved in the appendix), this allows us to deduce congruence and coincidence with the other notions of bisimilarity (Thm. 23).

Proposition 22 *Visible bisimilarity is a substitution closed congruence.*

The reasoning goes along the same path as for CCS, so that we only review the main differences, referring to appendix B for detailed proofs. We need to adapt the definition of distribution congruence, and we rely on Thm. 21 to prove that distribution congruence is contained in ground bisimilarity. As expected, we need to impose conditions on names when stating results involving contexts; for example, in Prop. 2, C should not bind free names of $\alpha.F$. Note moreover that we need to go against a Barendregt convention to perform some rewriting steps. For example, we want to allow $!a(x).a(x) \xrightarrow{!a(x)} !a(x)$. We finally obtain coincidence of visible and ground bisimilarities, which yields congruence:

Theorem 23 (Characterisation and congruence) *In $m\pi$, early, late, visible and ground bisimilarity coincide and define a substitution closed congruence.*

6 Conclusions and future work

We have presented a characterisation of strong bisimilarity in the restriction- and sum-free fragment of CCS, where replications are only allowed at top-level (Thm. 19). This has allowed us to put forward important algebraic properties of replication w.r.t. bisimilarity. By extending this result to the π-calculus, we have established congruence of bisimilarity in the corresponding fragment (Thm. 23).

We would like to push our results further, by finding extensions of the calculi we have studied for which bisimilarity is substitution closed. A counterexample involving the operators of restriction and replication is presented in [2] to establish non-congruence of bisimilarity. Therefore, in light of [5, Corollary 5.9] and Thm. 23, we can think of two paths to explore: either add a limited usage of restriction to the language, or study the full replication operator (allowing in particular nested replications).

Adding the restriction operator. The counterexample of [2] suggests that restrictions occurring immediately under replications are problematic. A natural extension of mCCS would therefore consist in adding restriction only to the grammar for finite processes (we indeed know from [5] that restriction does not break substitution closure on finite processes). In order to analyse this setting, it seems necessary to understand a simpler extension of mCCS, where we just add the τ prefix (which can be encoded as $(\nu c)\,(\overline{c}|c.P)$, for a fresh c). We believe that bisimilarity can then be captured using the following additional laws.

$$!a.E \mid !\overline{a}.F \;\sim\; !a.E \mid !\overline{a}.F \mid !\tau.(E|F) \qquad \frac{C[\mathbf{0}] \;\sim\; !a.E \mid !\overline{a}.F \mid P}{C[\mathbf{0}] \;\sim\; C[\tau.(E|F)]}$$

However, an important difficulty in adapting our proofs to this case is the definition and analysis of a counterpart of visible bisimilarity in presence of τ prefixes.

Beyond top-level replications. Handling unrestricted replications seems really challenging. We have started investigating the case where replication is not at top-level, but where nested replications (i.e., replications that occur under replications) are forbidden. The law

$$\alpha.C[!\alpha.C[\mathbf{0}]] \;\sim\; !\alpha.C[\mathbf{0}]$$

seems important to capture bisimilarity in this setting: it somehow generalises the distribution law (D) to replicated processes, and it allows one to equate processes like $!a$ and $a.!a$. We do not know at the moment whether this law, together with the laws presented above, is sufficient to characterise bisimilarity. One of the difficulties in studying this richer language is that seeds are no longer stable under reduction (Prop. 13): for example, $!a.b|c.!b$ is a seed while its reduct along c, $!a.b|!b$, is not, being bisimilar to $!a|!b$.

Related to this question is the work on HOcore [7], a restriction-free higher-order π-calculus where strong bisimilarity is characterised by the distribution law. In this calculus, replication can be encoded using the higher order features. The encoding is not fully abstract, however, so that it does not entail substitution closure in presence of "standard" replication.

Weak bisimilarity. Rather complex laws appear when moving from the strong to the weak case. For example, the following laws are valid for weak bisimilarity:

$$!\overline{a}.a \,|\, a.b \;\approx\; !\overline{a}.a \,|\, a \,|\, b \;, \qquad\qquad !\overline{a} \,|\, !a.b \;\approx\; !\overline{a} \,|\, !a \,|\, !b \;.$$

In both cases, although the related processes have the same size, the right-hand side process could be considered as a seed. We do not know how to generalise the first equivalence. For the second one, the following law, where $\langle P \rangle_a$ is defined homomorphically, except for $\langle a.P \rangle_a = \langle \overline{a}.P \rangle_a = \langle P \rangle_a$, is an interesting candidate:

$$!\overline{a}.P \,|\, !a.Q \;\approx\; !\overline{a} \,|\, !a \,|\, !\langle P \rangle_a \,|\, !\langle Q \rangle_a \;.$$

References

1. L. Aceto, W.J. Fokkink, A. Ingolfsdottir, and B. Luttik. Finite equational bases in process algebra: Results and open questions. In *Processes, Terms and Cycles: Steps on the Road to Infinity*, volume 3838 of *LNCS*. Springer Verlag, 2005.
2. M. Boreale and D. Sangiorgi. Some congruence properties for π-calculus bisimilarities. *Theoretical Computer Science*, 198:159–176, 1998.
3. S. Christensen, Y. Hirshfeld, and F. Moller. Decidable subsets of CCS. *Computer J.*, 37(4):233–242, 1994.
4. M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *J. of ACM*, 32(1):137–161, 1985.
5. D. Hirschkoff and D. Pous. A distribution law for CCS and a new congruence result for the pi-calculus. *LMCS*, 4(2), 2008.
6. Y. Hirshfeld and M. Jerrum. Bisimulation equivalence is decidable for normed process algebra. In *Proc. ICALP*, volume 1644 of *LNCS*, pages 412–421. Springer, 1999.

7. I. Lanese, J. A. Pérez, D. Sangiorgi, and A. Schmitt. On the expressiveness and decidability of higher-order process calculi. In *Proc. LICS '08*, pages 145–155. IEEE, 2008.
8. R. Milner. Functions as Processes. *J. of Mathematical Structures in Computer Science*, 2(2):119–141, 1992.
9. U. Nestmann and B.C. Pierce. Decoding choice encodings. In *Proc. of CONCUR'96*, volume 1119 of *LNCS*, pages 179–194. Springer Verlag, 1996.
10. D. Pous. Complete lattices and up-to techniques. In *Proc. APLAS*, volume 4807 of *LNCS*, pages 351–366. Springer, 2007.
11. D. Pous. *Techniques modulo pour les bisimulations*. PhD thesis, ENS Lyon, 2008.
12. D. Sangiorgi. On the bisimulation proof method. *J. of Mathematical Structures in Computer Science*, 8:447–479, 1998.
13. D. Sangiorgi and D. Walker. *The π-calculus: a Theory of Mobile Processes*. Cambridge University Press, 2001.

A Omitted proofs about *m*CCS

Proof (of Lemma 9).

(i) By contradiction: if $F \equiv D[\alpha_i.S_i]$, then $S|F \sim S|D[\mathbf{0}]$ by law (A), which contradicts the minimality hypothesis about $S|F$.
(ii) We show that if $S \rightsquigarrow \alpha.R_0|R_1$, then there exists i, D such that $S_i \equiv D[\alpha.R_0]$, by an induction on the transitions underlying $S \rightsquigarrow \alpha.R_0|R_1$.
(iii) By contradiction, suppose that $R \equiv D[\alpha_i.S_i]$. By emptying the prefixes of D, we find R' such that $S \rightsquigarrow R'$ and $R' \equiv \alpha_i.S_i$. By (ii), there exists j, D' such that $S_j \equiv D'[\alpha_i.S_i]$, which is contradictory with the fact that S is a seed: we have $S \sim \prod_{k\neq j} !\alpha_k.S_k|!\alpha_j.D'[\mathbf{0}]$ by law (A′) or (A), depending on whether $i = j$ or not. □

Proof (of Prop. 13). Write $P \equiv S|F$, where S is replicated. S is a seed since P is and we easily check that $P' \equiv S|F'$, with $S\#F'$. Now, let $S'|F''$ be a seed of P'. By Prop. 4, $S \dot{\sim} S'$, so that $S \equiv S'$ by Prop. 12. We conclude with Lemma 11: $F' \equiv F''$, so that P' is indeed also a seed. □

Proof (of Lemma 15). By induction over the number of rewriting steps. This is obvious if this number is zero; suppose now $P \xrightarrow{T} P' \xrightarrow{T}{}^{*} T$. The induction hypothesis gives $P' \sim T$; we reason by cases on the rule used to rewrite P:

– (R1): this means that $P \equiv C[\alpha.F]$, $P' \equiv C[\mathbf{0}]$ and $T \equiv !\alpha.F|Q$. From $!\alpha.F|Q \sim C[\mathbf{0}]$, we deduce $!\alpha.F|Q \sim C[\alpha.F]$ by Prop. 2, hence $P \sim T$.
– (R2): we easily have $P \sim P'$, hence $P \sim T$. □

Proof (of Prop. 18). By induction on the size of P. By Lemma 17, either P is a seed and we are done; or $P \xrightarrow{\mathsf{s}(P)} P'$ with $P \sim P'$. We easily check that $\sharp P' < \sharp P$ so that by induction, we have $P' \xrightarrow{\mathsf{s}(P')}{}^{*} \mathsf{s}(P')$. From $P \sim P'$, we deduce $\mathsf{s}(P) \sim \mathsf{s}(P')$, so that $\mathsf{s}(P) \equiv \mathsf{s}(P')$ by Prop. 12. This allows us to obtain $P \xrightarrow{\mathsf{s}(P)} P' \xrightarrow{\mathsf{s}(P)}{}^{*} \mathsf{s}(P)$, as the rewriting system is defined modulo $\equiv$. □

B Extension to the $m\pi$-calculus

In this appendix, we adapt the proofs from mCCS to $m\pi$, and establish the results announced in Sect. 5.

B.1 Setting and algebraic laws about replication

The results from Sect. 2 extend without difficulties to the π-calculus:

Proposition B1 (Prop. 2) *If $C[\mathbf{0}] \sim\, !\alpha.F|P$, where C does not bind any free name of $\alpha.F$, then $C[\mathbf{0}] \sim C[\alpha.F]$.*

Proof. Similar to the proof of Prop. 2, the fact that C should not bind any free name of $\alpha.F$ is used when the fired prefix is an input and guards the hole: this ensures that $\alpha.F$ is not affected by the induced substitution. □

As a consequence, we obtain the validity of laws (A) and (A′), with the extra proviso that C (resp. D) does not bind names occurring free in $\alpha.F$ (resp. $\alpha.D$):

Lemma B2 (Lemma. 3) *If $!F \mathrel{\dot\sim} P|Q$, then $!F \mathrel{\dot\sim} !F|P$.*

Proof. We rely on the same purely algebraic reasoning as for Lemma 3, since the relevant laws are valid in $m\pi$ (i.e., $!P \mathrel{\dot\sim} !P|P$ and the fact that $\mathrel{\dot\sim}$ is preserved by extended replication). □

Proposition B3 (Prop. 4) *If $!F|F_0 \mathrel{\dot\sim} !E|E_0$, then $!F \mathrel{\dot\sim} !E$.*

Proof. Working in $m\pi$ does not prevent us from emptying E_0 and F_0. The rest of the CCS proof uses algebraic arguments, and can be replayed. □

B.2 Seeds

Seeds in $m\pi$ are defined exactly like in mCCS (Def. 5). We then prove the counterpart of Fact. 7. We start with coincidence of visible and ground bisimilarity on finite processes: while this can be derived from the results in [5], visible bisimilarity is not taken into account in that paper.

Theorem B4 (Thm. 21) *On finite $m\pi$ processes, $\mathrel{\dot\sim}$ and $\sim$ coincide.*

Proof. It suffices to prove that $\mathrel{\dot\sim} \subseteq \sim$. We exploit a technical result from [5], the absence of 'mutual desynchronisation' (Lemma 4.4), i.e.,

$$\text{if } \alpha \neq \beta,\ E \xrightarrow{\alpha} E',\ F \xrightarrow{\beta} F',\ \text{then } \forall F_0,\ \beta.E \,|\, F' \,|\, F_0 \not\sim E' \,|\, \alpha.F \,|\, F_0.$$

In [5], this result is proved for the finite fragment of mCCS, and then extended to the finite sum-free fragment of the π-calculus, by considering an 'erasing' translation from π into CCS (cf. Def. 5.3, Lemma 5.4 and Prop. 5.5 in [5]—the translation transforms visible bisimilar π-calculus processes into bisimilar CCS processes, so that the absence of mutual desynchronisation can be established w.r.t. visible bisimilarity in π).

Using this property, we show that the restriction of $\dot{\sim}$ to finite processes is a ground bisimulation, i.e., that challenges along silent transitions can be answered: suppose that $E \dot{\sim} F$, and $E \xrightarrow{\tau} E'$. W.l.o.g., we can write $E = a(b).E_2|\overline{a}\langle b\rangle.E_1|E_0$. By playing the input prefix, and then the output prefix, $E \dot{\sim} F$ gives $F \xrightarrow{a(b)} \xrightarrow{\overline{a}\langle b\rangle} F_1'$ with $E' \sim F_1'$. By playing theses prefixes in reverse order, we obtain $F \xrightarrow{\overline{a}\langle b\rangle} \xrightarrow{a(b)} F_2'$ with $E' \sim F_2'$. There are two cases to consider:

- if one of these sequences of transitions emanating from F involves the firing of concurrent prefixes, then we can deduce $F \xrightarrow{\tau} F_i'$, and close the diagram;
- if both correspond to the firing of sequential prefixes, i.e., $F_1 \equiv a(b).U|\overline{a}\langle b\rangle.V|F_0$ with $U \xrightarrow{\overline{a}\langle b\rangle} U'$, $V \xrightarrow{a(b)} V'$, $F_1' \equiv U'|\overline{a}\langle b\rangle.V|F_0$, and $F_2' \equiv a(b).U|V'|F_0$, we check that F_1' and F_2' determine a mutual desynchronisation ($F_1' \dot{\sim} E' \dot{\sim} F_2'$), which is contradictory. □

We then show that visible bisimilarity is a substitution closed congruence, on all $m\pi$ processes. We let σ range over capture-avoiding name substitutions; we rely on the following lemma to reason about reducts along input transitions.

Lemma B5 *$P\sigma \xrightarrow{a_0(x)} P_0$ iff there exists z, a, P' such that $P \xrightarrow{a(z)} P'$, $a_0 = a\sigma$, and $P_0 = P'\{\sigma, z \to x\}$ (where $\{\sigma, z \to x\}$ is the parallel substitution that extends σ with the replacement of x for z).*

Proposition B6 (Prop. 22) *In $m\pi$, $\dot{\sim}$ is a substitution closed congruence.*

Proof. Using Lemma B5, we show that $\{(P\sigma, Q\sigma) \,/\, \sigma,\ P \dot{\sim} Q\}$ is a visible ground bisimulation. This is possible because $\dot{\sim}$ does not test challenges along silent transitions (however, unlike for CCS, we cannot fix the substitution). Congruence then follows: we use substitution closure in order to handle the input prefix. □

Another difficulty is that [5] does not provide an algebraic characterisation of bisimilarity on finite π-processes—while it does for finite mCCS processes, using the distribution law (D). Therefore, we can no longer work with a "structural" definition of distribution congruence: we have to use the following definition.

Definition B7 (Distribution congruence for $m\pi$—Def. 6) *We call* distribution congruence *the smallest congruence relation $\equiv$ that satisfies the laws of an abelian monoid for $(|, \mathbf{0})$ and contains the restriction of $\sim$ to finite processes.*

This definition and the above results allow us to deduce the remaining inclusions corresponding to Fact. 7, about mCCS:

Lemma B8 *In $m\pi$, we have $\equiv \subseteq \sim \subseteq \dot{\sim}$.*

Proof. The second inclusion is immediate from the definitions. For the first inclusion, we show that $\equiv$ is a ground bisimulation. We exploit the fact that $\equiv$ is substitution closed on finite processes (Prop. B6 and Thm. B4) in order to handle replicated input prefixes: if $!a(x).F \equiv !a(x).E$ because $F \equiv E$, and, if $!a(x).F \xrightarrow{a(y)} !a(x).F \mid F\{y/x\}$, then $!a(x).E$ answers with the obvious transition, and we check that $!a(x).F \mid F\{y/x\} \equiv !a(x).E \mid E\{y/x\}$: thanks to substitution closure on finite processes, we have $F\{y/x\} \equiv E\{y/x\}$. □

The notion of residual process remains unchanged; we have to adapt the notion of clean process (w.r.t. a fixed seed having only replicated components only: $S = \prod_i !\alpha_i.S_i$):

Definition B9 (Clean process, residual—counterpart of Def. 8)
F is clean w.r.t. *S, written $S\#F$, if it is not the case that for some i and finite context D, $F \equiv D[\alpha_i.S_i]$, where D does not bind any free name of $\alpha_i.S_i$.*

R is a residual of *S, written $S \rightsquigarrow R$ when there exist $k > 0$, $\alpha_1, .., \alpha_k$, and $P_1, .., P_k$ such that $S \xrightarrow{\alpha_1} P_1 \ldots \xrightarrow{\alpha_k} P_k \equiv S|R$. We shall use R to range over such residual processes.*

The second point of Lemma 9 needs to be strenghtened:

Lemma B10 (Lemma 9) *(i) If $S|F$ is a seed, then $S\#F$;*
(ii) If $S \rightsquigarrow \alpha.R$, then there exist i, D such that $S_i \equiv D[\alpha.R]$ and D does not bind free names of S.
(iii) If $S \rightsquigarrow R$, then $S\#R$.

Proof. The first two points are handled like in the CCS case; we give more details for the third one. By contradiction, suppose that $R \equiv D[\alpha_i.S_i]$, where D does not bind free names of $\alpha.S_i$. By emptying the prefixes of D, we find R' such that $S \rightsquigarrow R'$ and $R' \equiv \alpha_i.S_i$ (since D does not capture names of $\alpha_i.S_i$, $\alpha_i.S_i$ appears unchanged after the sequence of transitions). By (ii), there exists j, D' such that $S_j \equiv D'[\alpha_i.S_i]$ where D' does not bind free names of S and hence, in particular, of $\alpha_i.S_i$. Therefore, we can use laws (A′) or (A) to obtain a contradiction, like in the CCS case. □

Lemma B11 (Lemma 10) *$S \dot{\sim} S|R$ and $S \rightsquigarrow R$ entail $R = \mathbf{0}$.*

Proof. Suppose by contradiction $R = \alpha.R_0|R_1$. Lemma B2 gives $S \dot{\sim} S|\alpha.R_0$, hence $S \dot{\sim} S|!\alpha.R_0$ by replicating all processes. Moreover, $S \rightsquigarrow \alpha.R_0$, so that Lemma B10(ii) gives i, D such that $S_i \equiv D[\alpha.R_0]$ and D does not bind free names of S. Since $S \dot{\sim} S|\alpha.R_0$, the free names of $\alpha.R_0$ are contained in those of S, so that they cannot be captured by D. This allows us to use law (A) to obtain a contradiction, like in the CCS case. □

Lemma B12 (Lemma 11) *If $S|F \dot{\sim} S|E$ $S\#F$, and $S\#E$, then $F \equiv E$.*

Proof. Same proof as for Lemma 11. □

Proposition B13 (Prop. 12) *For all seeds P, P', we have $P \dot{\sim} P'$ iff $P \sim P'$ iff $P \equiv P'$.*

Proof. Same proof as for Prop. 12. □

B.3 Rewriting system

The rewriting system is extended to $m\pi$ by avoiding name captures when erasing components of the seed using rule (R1); joinability is defined as previously:

Definition B14 (counterpart of Defs. 14 and 16) *Any process T induces a relation between processes, written $\xrightarrow{T}$, defined by the following rules, modulo distribution congruence ($\equiv$):*

$$\frac{T \equiv !\alpha.F|Q \qquad \mathrm{cn}(C) \cap \mathrm{fn}(\alpha.F) = \emptyset}{C[\alpha.F] \xrightarrow{T} C[\mathbf{0}]}\ (\mathrm{R1}) \qquad \frac{}{!\alpha.F|!\alpha.F|P \xrightarrow{T} !\alpha.F|P}\ (\mathrm{R2})$$

(Where $\mathrm{cn}(C)$ denotes the set of names captured by C.) The reflexive transitive closure of $\xrightarrow{T}$ is written $\xrightarrow{T}{}^*$. We say that processes P and Q are joinable*, written $P \curlyvee Q$, whenever there exists a process T such that $P \xrightarrow{T}{}^* T$ and $Q \xrightarrow{T}{}^* T$.*

With these definitions, the proofs of Lemmas 15, 17, and Prop. 18 can be replayed without additional difficulties, so that we obtain:

Theorem B15 (Characterisation—Thm. 19) *In $m\pi$, visible and strong bisimilarity coincide with joinability: $P \dot{\sim} Q$ iff $P \sim Q$ iff $P \curlyvee Q$.*

Since visible bisimilarity is a substitution closed congruence on $m\pi$ (Prop. B6), we deduce that the same holds for ground bisimilarity. This in turn entails coincidence with early and late bisimilarities, as stated in Thm. 23.