# A Distribution Law for CCS and a New Congruence Result for the pi-calculus

Daniel Hirschkoff, Damien Pous

# A Distribution Law for CCS and a New Congruence Result for the $\pi$-calculus

Daniel Hirschkoff and Damien Pous

LIP – ENS Lyon, CNRS, INRIA, UCBL, France

**Abstract.** We give an axiomatisation of strong bisimilarity on a small fragment of CCS that does not feature the sum operator. This axiomatisation is then used to derive congruence of strong bisimilarity in the finite $\pi$-calculus in absence of sum. To our knowledge, this is the only nontrivial subcalculus of the $\pi$-calculus that includes the full output prefix and for which strong bisimilarity is a congruence.

## Introduction

In this paper, we study strong bisimilarity on two process calculi. We first focus on *microCCS* ($\mu$CCS), the very restricted fragment of CCS that only features prefix and parallel composition. Our main result on $\mu$CCS is that adding the following *distribution law*

$$\eta.(P|\eta.P|\ldots|\eta.P) \quad = \quad \eta.P|\eta.P|\ldots|\eta.P$$

to the laws of an abelian monoid for parallel composition yields a complete axiomatisation of strong bisimilarity (in the law above, $\eta$ is a CCS prefix, of the form $a$ or $\overline{a}$, and $P$ is any CCS process – the same number of copies of $P$ appear on both sides of the equation).

The distribution law is not new: it is mentioned – among other *'mixed equations'* relating prefixed terms and parallel compositions – in a study of bisimilarity on normed PA processes [4]. In our setting, this equality can be oriented from left to right to rewrite processes into normal forms, which intuitively exhibit as much concurrency as possible. Strong bisimilarity ($\sim$) between processes is then equivalent to equality of their normal forms. This rewriting phase allows us to actually compute *unique decompositions* of processes into *prime processes*, in the sense of [6]: a process $P$ is prime if $P \sim Q|R$ implies $Q \sim \mathbf{0}$ or $R \sim \mathbf{0}$.

The distribution law is an equational schema, corresponding to an infinite family of axioms, of the form $\eta.(P|(\eta.P)^k) = (\eta.P)^{k+1}$, for $k \geq 1$ (where $Q^k$ denotes the $k$-ary parallel composition of process $Q$). We show that although our setting is rather simple, there exists no finite axiomatisation of $\sim$ on $\mu$CCS.

We then move to the study of strong bisimilarity on the finite, sum-free $\pi$-calculus ($\pi$). We rely on the axiomatisation of strong bisimilarity on $\mu$CCS to prove that ground bisimilarity ($\sim_{\mathrm{g}}$) is closed under substitutions in $\pi$, i.e., that whenever $P \sim_{\mathrm{g}} Q$, then $P\sigma \sim_{\mathrm{g}} Q\sigma$ for any substitution $\sigma$. Closure under

substitution of ground bisimilarity entails that on $\pi$, ground, early, late and open bisimilarities coincide, and are congruences. The problem of congruence of $\sim_{\mathrm{g}}$ on $\pi$ is mentioned as an open question in [7, Chapter 5]. To our knowledge, this is the first congruence result for a subcalculus of the $\pi$-calculus that includes the full output prefix (see Section 5 for a discussion on this).

At the heart of our proof of congruence is a notion that we call *mutual desynchronisation*, and that corresponds to the existence of processes $T, T_{12}, T_{21}$ such that $T \xrightarrow{\eta_1}\xrightarrow{\eta_2} T_{12}$ and $T \xrightarrow{\eta_2}\xrightarrow{\eta_1} T_{21}$, for two distinct actions $\eta_1$ and $\eta_2$, and with $T_{12} \sim T_{21}$. We additionally require in the two sequences of transitions from $T$ to $T_{12}$ and $T_{21}$ respectively that the second prefix being fired should occur under the first prefix in $T$. Intuitively, in such a situation, the process behaves as if the two actions were offered concurrently, but triggers consecutive prefixes.

Using our analysis of strong bisimilarity on $\mu$CCS, we show that mutual desynchronisations do not exist in $\mu$CCS. When moving to the $\pi$-calculus, it turns out that substitution closure of $\sim_{\mathrm{g}}$ amounts to observing the same property in $\pi$. A transfer property, that extracts a bisimilarity proof in $\mu$CCS from a bisimilarity proof in $\pi$, allows us to relate the two calculi and to show that mutual desynchronisations do not exist in $\pi$, yielding congruence of $\sim_{\mathrm{g}}$.

*Paper outline.* We introduce $\mu$CCS and the distribution law in Section 1. Section 2 is devoted to the characterisation of $\sim$ on $\mu$CCS using normal forms. We prove that the distribution law yields an infinitary $\omega$-complete axiomatisation, and that no finite axiomatisation exists in Section 3. Section 4 describes the proof of our congruence result in the $\pi$-calculus, and we give concluding remarks in Section 5.

## 1 MicroCCS Processes and Normal Forms

We consider an infinite set $\mathcal{N}$ of names, ranged over with $a, b \ldots$. We define on top of $\mathcal{N}$ the set of processes of $\mu$CCS, the finite, public, sum-free CCS calculus, ranged over using $P, Q, R \ldots$, as follows:

$$\eta \quad ::= \quad a \mid \overline{a} \ , \qquad P \quad ::= \quad \mathbf{0} \mid \eta.P \mid P_1|P_2 \ .$$

$\eta$ ranges over visible actions and coactions, called *interactions*, and we let $\overline{\eta}$ stand for the coaction associated to $\eta$ (we have $\overline{\overline{\eta}} = \eta$). For $k > 0$, we write $P^k$ for the parallel composition of $k$ copies of $P$. It can be noted that our syntax does not include a construction of the form $\tau.P$ — see Remark 2.2 below.

*Structural congruence*, written $\equiv$, is defined as the smallest congruence satisfying the following laws:

$$(C_1) \quad P|Q \equiv Q|P \qquad (C_2) \quad P|(Q|R) \equiv (P|Q)|R \qquad (C_3) \quad P|\mathbf{0} \equiv P$$

We introduce a labelled transition system (LTS) for $\mu$CCS. Actions labelling transitions, ranged over with $\mu$, are either interactions, or a special silent action, written $\tau$.

**Definition 1.1 (Operational semantics and behavioural equivalence).** *The LTS for $\mu$CCS is given by the following rules:*

$$\eta.P \xrightarrow{\eta} P \qquad \frac{P \xrightarrow{\eta} P' \qquad Q \xrightarrow{\overline{\eta}} Q'}{P|Q \xrightarrow{\tau} P'|Q'} \qquad \frac{P \xrightarrow{\mu} P'}{P|Q \xrightarrow{\mu} P'|Q} \qquad \frac{P \xrightarrow{\mu} P'}{Q|P \xrightarrow{\mu} Q|P'}$$

*Bisimilarity, written $\sim$, is the largest symmetrical relation between CCS processes such that if $P \sim Q$ and $P \xrightarrow{\mu} P'$, then $Q \xrightarrow{\mu} Q'$ and $P' \sim Q'$ for some $Q'$.*

**Definition 1.2 (Size).** *Given $P$, we let $\#(P)$ (called the* size *of $P$) stand for the number of prefixes in $P$.*

**Lemma 1.3.** *$P \equiv Q$ implies $P \sim Q$ which in turn implies $\#(P) = \#(Q)$.*

*Proof.* We check that $\equiv$ is a bisimulation, so that $\equiv \subseteq \sim$.

If $P \sim Q$ and $\#(P) > \#(Q)$, we play a bisimilarity game where all challenges are interactions and are offered on $P$'s side, yielding a contradiction. □

**Definition 1.4 (Distribution law).** *The* distribution law *is given by the following equation, where the same number of copies of $P$ appears on both sides:*

$$\eta.(P\,|\eta.P|\ldots|\,\eta.P) \quad = \quad \eta.P\,|\,\eta.P\,|\ldots|\,\eta.P \ .$$

*We shall use this equality, oriented from left to right, to rewrite processes. We write $P \rightsquigarrow P'$ when there exist $P_1, P_2$ such that $P \equiv P_1$, $P_2 \equiv P'$ and $P_2$ is obtained from $P_1$ by replacing a sub-term of the form of the left-hand side process with the right-hand side process.*

*Remark 1.1 (On the distribution law and PA).* Among the studies about properties of $\sim$ in process algebras that include parallel composition (see [1] for a recent survey on axiomatisations), some works focus on calculi where parallel composition is treated as a primitive operator (as opposed to being expressible using sum or other constructs like the left merge operator). As mentioned above, particularly relevant to this work is [4], where Hirshfeld and Jerrum *"develop a structure theory for PA that completely classifies the situations in which a sequential composition of two processes can be bisimilar to a parallel composition"*. [4] establishes decidability of $\sim$ for normed PA processes: in that setting, the formal analogue of the distribution law (Def. 1.4) holds with $\eta$ and $P$ being two processes — the 'dot' operator is a general form of sequential composition. This equality is valid in [4] whenever $\eta$ is a 'monomorphic process', meaning that $\eta$ can only reduce to $\mathbf{0}$ (which corresponds to $\mu$CCS), or to $\eta$ itself. [3] presents a finite axiomatisation of PA that exploits the operators of sum and left merge.

The distribution law is an equational schema, describing an infinite family of *distribution axioms* $(D_k)$ : $\eta.(X \mid (\eta.X)^k) \ = \ (\eta.X)^{k+1}$ for $k \geq 1$.

**Lemma 1.5.** *$\rightsquigarrow$ is strongly normalising, $(\rightsquigarrow \cup \equiv)$ is confluent.*

*Proof.* If $P \rightsquigarrow P'$ then the height of $P'$ is strictly smaller than that of $P$, whence the strong normalisation. Then we check that $(\rightsquigarrow \cup \equiv)$ is locally confluent, and conclude with a variant of Newman's Lemma. □

Thus, for any process $P$, $\rightsquigarrow$ defines a normal form unique up to $\equiv$, that will be denoted by $\mathsf{n}(P)$. We let $A, B, \ldots$ range over normal forms.

## 2 Characterisation of Bisimilarity in MicroCCS

**Definition 2.1 (Components).** *We say that $\eta.Q$ is a* component *of $P$ when $P \equiv \eta.Q|R$ for some process $R$. Given a process $P$ and a natural number $i$, $P@i$ stands for the number of components of size $i$ in $P$, and $P_{|i}$ denotes the process consisting of the parallel composition of all components of size $i$ of $P$.*

For example, for $P = a|b|c.d.e$, $P@1 = 2$, $P@3 = 1$, $P@2 = P@4 = 0$, $P_{|1} = a|b$.

Normal forms enjoy the following properties:

**Lemma 2.2.** *If $A \xrightarrow{\eta} P'$, then $P'$ is a normal form, and there exists $i > 0$ s.t.:*
1. *$A \equiv \eta.A_1|A_2$, $P' \equiv A_1|A_2$ and $\#(\eta.A_1) = i$;*
2. *$P'@i = (A@i) - 1, \quad \forall n < i.\, P'@n \geq A@n, \quad \forall n > i.\, P'@n = A@n$.*

*Proof.* Straightforward. □

We now have enough technical devices to prove that equality of normal forms is equivalent to strong bisimilarity on $\mu$CCS processes.

**Proposition 2.3.** *$A \sim B$ implies $A \equiv B$.*

*Proof.* We say that a process $P$ makes a transition *at $i$* to denote the fact that $P$ makes this transition by triggering one of its components of size $i$. In this case, we can use Lemma 2.2 to reason about the shape of $P$ and of its reduct.

We reason by induction on the size of $A$. The base case is immediate: $\mathbf{0} \sim B$ implies $B \equiv \mathbf{0}$. Suppose now $A \sim B$, with $\#(A) > 0$.

We know by induction that for any $A'$ of size strictly smaller than $\#(A)$, $A' \sim B'$ implies $A' \equiv B'$, and hence in particular: $\quad \forall i,\ A'@i = B'@i. \qquad (\star)$

Based on this observation, we can remark that if $A@i < B@i$ for some $i$, we have $A@i = 0$. Indeed, by contradiction, $A@i > 0$ would allow us to trigger a component of size $i$ on $A$s side, leading (by Lemma 2.2) to a process $A'$ s.t. $A'@i = A@i - 1$. Because $A \sim B$, $B$ should be able to answer by evolving to a certain $B'$, with $A' \sim B'$, and, by $(\star)$ above, $B'@i = A'@i$, which is impossible by Lemma 2.2 since $B@i \geq A'@i + 2$.

By symmetry, we get: $\quad A@i \neq B@i \Rightarrow A@i \times B@i = 0. \qquad (\dagger)$

We are now ready to embark in the proof that $A \equiv B$. Consider for that the minimum sizes of non-nil components in $A$ and $B$, called respectively $i_0$ and $j_0$. We distinguish two cases, according to whether $i_0 = j_0$ or not.

*First case: $i_0 = j_0$.* Then by definition, and by $(\dagger)$ above, $A@i_0 = B@i_0 > 0$. We play a challenge at $i_0$ on $A$s side, say $A \xrightarrow{\eta} A'$, and we can write $A' \equiv A_1|A_2$

with $A_1@i = 0$ for $i < i_0$ and $\#(A_2) = i_0 - 1$ (that is, $A \equiv A_1|\eta.A_2$). $B$ answers the challenge offered by $A$ with $B \xrightarrow{\eta} B'$, and by $(\star)$, we can write $B' \equiv B_1|B_2$, with $A_1 \equiv B_1$ and $A_2 \equiv B_2$. Since $B \xrightarrow{\eta} B'$ and $B@i = 0$ for $i < i_0$, we can deduce $B \equiv B_1|\eta.B_2$, which gives $A \equiv B$.

*Second case:* $i_0 \neq j_0$. Wlog., we can suppose $i_0 < j_0$. We can write $A_{|i_0} \equiv \eta_1.P_1|\ldots|\eta_k.P_k$, with $\#(P_i) = i_0 - 1$ for $i = 1, \ldots, k$ (we have $A@i_0 = k$).

Consider the challenge by $A$ at $i_0$ given by $A \xrightarrow{\eta_1} A'$. We remark that by definition of $j_0$, and since $i_0 < j_0$, $B@i = 0$ for all $i \leq i_0$. Hence $B$ answers this challenge at some $j > i_0$, with $B \xrightarrow{\eta_1} B'$. By $(\star)$, $B'@j = A'@j$, and since $A@j = A'@j$, $B@j = A@j + 1$, which gives by $(\dagger)$ $A@j = 0$ and $B@j = 1$.

We know by $(\star)$ that $A' \equiv B'$: by examining these processes at components of size $\leq i_0$, we deduce $B_{|j} \equiv \eta_1.(P_1|\eta_2.P_2|\ldots|\eta_k.P_k)$.

Now consider the challenge by $A$ at $i_0$ given by $A \xrightarrow{\eta_2} A''$. Since $B@j = 1$ and $A@j = 0$, by $(\star)$ $B$ has to answer at $j$, which gives $P_1|\eta_2.P_2|\ldots|\eta_k.P_k \equiv \eta_1.P_1|P_2|\eta_3.P_3|\ldots|\eta_k.P_k$, from which we deduce $\eta_1 = \eta_2$ and $P_1 \equiv P_2$ ($\#(P_i) = i_0 - 1$). The same reasoning for $\eta_3, \ldots, \eta_k$ gives $B_{|j} \equiv \eta_1.(P_1|\eta_1.P_1|\ldots|\eta_1.P_1)$, which is contradictory with the fact that $B$ is a normal form.

Hence, $i_0 \neq j_0$ is impossible, and we have proved that $A \equiv B$. □

**Lemma 2.4.** *If $P \rightsquigarrow P'$, then $P \sim P'$. For any $P$, $P \sim \mathsf{n}(P)$.*

*Proof.* We check that the relation $(\rightsquigarrow \cup \equiv)$ is a bisimulation. □

**Theorem 2.5.** *Let $P, Q$ be two $\mu$CCS processes. Then $P \sim Q$ iff $\mathsf{n}(P) \equiv \mathsf{n}(Q)$.*

*Proof.* $\mathsf{n}(P) \equiv \mathsf{n}(Q)$ implies that $P \sim Q$ using Lemma 2.4. ($\sim$ is an equivalence relation). Conversely, if $P \sim Q$, we have that $\mathsf{n}(P) \sim \mathsf{n}(Q)$, and hence by Prop. 2.3 that $\mathsf{n}(P) \equiv \mathsf{n}(Q)$. □

**Corollary 2.6 (Cancellation).** *For all $P, Q, R$, $P|R \sim Q|R$ implies $P \sim Q$.*

*Proof.* From $\mathsf{n}(P|R) \equiv \mathsf{n}(Q|R)$ we deduce $\mathsf{n}(P) \equiv \mathsf{n}(Q)$, and hence $P \sim Q$. □

Note that this is not true in presence of replication: $a|!a \sim \mathbf{0}|!a$, but $a \not\sim \mathbf{0}$.

*Remark 2.1 (Unique decomposition of processes).* Results like Theorem 2.5 and Corollary 2.6 are related to a series of works on unique decomposition of processes, initiated in [6]. In these works, one seeks to write a term as a parallel composition of *prime* processes: $P$ is prime if $P \not\sim \mathbf{0}$ and $P \sim Q|R$ entails $Q \sim \mathbf{0}$ or $R \sim \mathbf{0}$. Unique decomposition has been established for a variety of process algebras, and used as a way to prove decidability of behavioural equivalence and to give complexity bounds for the associated decision procedure ([5,2] cite relevant references).

In the present study, more than in the existence of a unique decomposition, we are interested in a syntactic characterisation of $\sim$ (which will in particular allow us to derive Lemma 4.4 below). We therefore rely explicitly on the distribution law in order to 'extract' prime components of processes.

*Remark 2.2 ($\tau$ transitions and weak bisimilarity).* Our syntax does not include a construction of the form $\tau.P$. The results on CCS could be adapted without much difficulty to handle $\tau$ prefixes (in particular because in the bisimulation game, a $\tau$ transition resulting from a synchronisation cannot be answered by firing a $\tau$ prefix – Lemma 1.3 still holds in presence of the $\tau$ prefix). We preferred not to include $\tau$ prefixes to simplify the presentationWe preferred not to include $\tau$ prefixes to simplify the presentation, and to make the correspondence with the $\pi$-calculus (where this construction is often omitted) easier

We do not address weak bisimilarity in the present work. When including $\tau$ prefixes in the syntax, it can be proved that adding the law $\tau.P = P$ is enough to characterise weak bisimilarity. In particular, strong and weak bisimilarity coincide in $\mu$CCS.

## 3 Nonexistence of a Finite Axiomatisation

We let $M, N$ range over $\mu$CCS terms with *variables*, ranged over with $X, Y \ldots$ ($M ::= \mathbf{0} \mid \eta.M \mid M|M \mid X$). A *ground term* is a term with no occurrence of variables. *Instantiations*, ranged over using $\rho$, are mappings from variables to terms, and their domain are naturally extended to terms. Applying $\rho$ to $M$ yields a term written $M\rho$. $\rho$ is a *ground instantiation* if for all terms $M$, $M\rho$ is a ground term. Any two terms $M, N$ define an *equation*, written $M = N$.

**Definition 3.1 (Axiomatic equality).** *Given a set $\mathcal{E}$ of equations, we shall write $\mathcal{E} \vdash M = N$ whenever $M = N$ can be derived in equational logic using equations from $\mathcal{E}$.*

*We let $\mathcal{D}$ stand for the set of equations consisting of the three axioms of structural congruence $(C_1, C_2, C_3)$, and all the distribution axioms $((D_i)_{i\geq 1})$. $\mathcal{D}_k$ stands for the finite restriction of $\mathcal{D}$ where only the first $k$ distribution axioms are included $((D_i)_{1\leq i\leq k})$.*

Equations of $\mathcal{D}$ are obviously sound for $\sim$. Ground completeness is given by the following proposition, which holds by Theorem 2.5.

**Proposition 3.2 (Completeness).** *For any processes $P, Q$,*

$$P \sim Q \quad \textit{iff} \quad \mathcal{D} \vdash P = Q \ .$$

We now analyse the distribution law using a rather classical approach. We show that $\mathcal{D}$ is $\omega$-complete, that is, complete w.r.t. the extensional equality derived from strong bisimilarity. Since, by Lemma 3.8 below, $\mathcal{D}$ is *intrinsically* infinite, we derive impossibility of a finite axiomatisation of $\sim$ on $\mu$CCS, by using compactness arguments.

**Definition 3.3 (Extensional equality).** *Two terms $M$ and $N$ are* extensionally equal*, written $M \sim_\omega N$, whenever for any ground instantiation $\rho$, it holds that $M\rho \sim N\rho$. An equation $M = N$ is said to be* correct *if $M \sim_\omega N$.*

**Lemma 3.4.** *Let $M$ be a term whose variables all belong to $\{X_i\}_{i\in I}$, and let $\{a_i\}_{i\in I}$ be a collection of distinct names that do not occur in $M$.*

$$\mathsf{n}(M\{a_i.0/X_i\}) \equiv \mathsf{n}(M)\{a_i.0/X_i\}$$

*Proof.* We proceed by well founded induction over the termination of $\rightsquigarrow$.

- If $M$ is in normal form, we just have to check that $M\{a_i.0/X_i\}$ is in normal form. This is true because the $a_i$ are distinct and do not appear in $M$.
- Otherwise, if $M \rightsquigarrow N$, we check that $M\{a_i.0/X_i\} \rightsquigarrow N\{a_i.0/X_i\}$ so that:

$$\begin{aligned}
\mathsf{n}(M\{a_i.0/X_i\}) &\equiv \mathsf{n}(N\{a_i.0/X_i\}) && \text{(by confluence)}\\
&\equiv \mathsf{n}(N)\{a_i.0/X_i\} && \text{(by induction)}\\
&\equiv \mathsf{n}(M)\{a_i.0/X_i\} && \text{(by confluence)}
\end{aligned}$$

□

**Lemma 3.5.** *Let $M, N$ be two terms whose variables all belong to $\{X_i\}_{i\in I}$, and let $\{a_i\}_{i\in I}$ be a collection of distinct names that do not occur in $M$ nor in $N$.*

- *If $\mathcal{D} \vdash M = N$ then $\mathcal{D} \vdash M\rho = N\rho$ for any instantiation $\rho$;*
- *if $M\{a_i.0/X_i\} \sim N\{a_i.0/X_i\}$ then $\mathcal{D} \vdash M = N$.*

*Proof.* The first point is standard, and proved by induction over the derivation tree.

For the second property, we know by Theorem 2.5 that $\mathsf{n}(M\{a_i.0/X_i\}) \equiv \mathsf{n}(N\{a_i.0/X_i\})$. By Lemma 3.4, we have $\mathsf{n}(M\{a_i.0/X_i\}) \equiv \mathsf{n}(M)\{a_i.0/X_i\}$, and $\mathsf{n}(N\{a_i.0/X_i\}) \equiv \mathsf{n}(N)\{a_i.0/X_i\}$. Hence we have $\mathsf{n}(M) \equiv \mathsf{n}(N)$, and $\mathcal{D} \vdash M = N$ holds. □

**Theorem 3.6 ($\omega$-completeness).** *For any terms $M, N$,*

$$M \sim_\omega N \quad \textit{iff} \quad \mathcal{D} \vdash M = N \ .$$

*Proof.* Using Lemma 3.5, $\omega$-completeness boils down to the completeness of $\mathcal{D}$ for ground terms (Prop. 3.2). □

Notice that the proof of Theorem 3.6 relies on the existence of an infinite number of names. The following result is standard.

**Lemma 3.7 (Compactness).** *For any terms $M, N$,*

$$\mathcal{D} \vdash M = N \quad \textit{iff} \quad \mathcal{D}_k \vdash M = N \text{ for some } k \ .$$

*Proof.* Equational proofs are finite objects. □

**Lemma 3.8.** *Let $a$ be a name, for any number $k$, there exists $n$ such that:*

$$\mathcal{D}_k \not\vdash a.a^n = a^{n+1} \ .$$

Remember that $a^n$ stands for the $n$-ary parallel composition of $a.\mathbf{0}$, so that this equality is an instance of axiom $(D_n)$.

*Proof.* Let $n$ be a number strictly greater than $k$ such that $n+1$ is prime, and let $\theta(P,Q)$ denote the predicate: "$P \sim Q \sim a^{n+1}$, $P \equiv a.P'$, and $Q \equiv Q_1|Q_2$ with $Q_1, Q_2 \not\equiv \mathbf{0}$".

Suppose $\mathcal{D}_k \vdash a.a^n = a^{n+1}$, and consider the shortest proof of $\mathcal{D}_k \vdash P = Q$ for some processes $P, Q$ such that either $\theta(P,Q)$ or $\theta(Q,P)$. Since we have $\theta(a.a^n, a^{n+1})$, such a minimal proof does exist. We reason about the last rule used in the derivation of this proof in equational logic. For syntactic reasons, this cannot be reflexivity, a contextual rule, nor one of the structural congruence axioms. It can be neither symmetry nor transitivity, since otherwise this would give a shorter proof satisfying $\theta$. The only possibility is thus the use of one of the distribution axioms, say $D_i$ with $1 \leq i \leq k$ and $a^{n+1} \sim Q \equiv (a.Q')^{i+1}$. By Lemma 1.3, since $\#(a^{n+1}) = n+1$, $i+1$ has to divide $n+1$. This is contradictory, because we have $2 \leq i+1 \leq k+1 < n+1$, and $n+1$ is prime. □

We can finally prove the nonexistence finite axiomatisation of $\sim$ on $\mu$CCS. The proof we give corresponds to a standard application of the *Compactness Theorem*.

**Theorem 3.9 (No finite axiomatisation of $\sim$).** *For any finite set of correct equations $\mathcal{E}$, there exist processes $P$ and $Q$ such that $P \sim Q$ but $\mathcal{E} \not\vdash P = Q$.*

*Proof.* By correctness, for any equation $M = N$ in $\mathcal{E}$, $M \sim_\omega N$. Hence, by $\omega$-completeness we can prove any equation of $\mathcal{E}$ using $\mathcal{D}$. By Lemma 3.7, and since $\mathcal{E}$ is finite, there exists $k$ such that $\mathcal{D}_k \vdash \mathcal{E}$. By Lemma 3.8, there exists $n$ such that $a.a^n \sim a^{n+1}$ and $\mathcal{D}_k \not\vdash a.a^n = a^{n+1}$; and thus, $\mathcal{E} \not\vdash a.a^n = a^{n+1}$. □

# 4 A New Congruence Result for the π-calculus

## 4.1 The Finite, Sum-free π-calculus

$\pi$-calculus processes are built from an infinite set $\mathcal{N}_\pi$ of names, ranged over using $a, b \ldots, m, n \ldots, p, q \ldots, x, y \ldots$, according to the following grammar:

$$\phi \quad ::= \quad m(x) \;\big|\; \overline{m}n \;, \qquad P \quad ::= \quad \mathbf{0} \;\big|\; \phi.P \;\big|\; P_1|P_2 \;\big|\; (\boldsymbol{\nu} p)\, P \;.$$

The input prefix $m(x)$ binds name $x$ in the continuation process, and so does name restriction $(\boldsymbol{\nu} n)$ in the restricted process. A name that is not bound is said to be free, and we let $\mathrm{fn}(P)$ stand for the free names of $P$. We assume that any process that we manipulate satisfies a *Barendregt convention*: every bound name is distinct from the other bound and free names of the process. We shall use $a, b, c$ to range over free names of processes, $p, q, r$ (resp. $x, y$) to range over names bound by restriction (resp. by input), and $m, n$ to range over any name, free or bound (note that these naming conventions are used in the above grammar).

Structural congruence on $\pi$, written $\equiv$, is the smallest congruence that is an equivalence relation, contains $\alpha$-equivalence, and satisfies the following laws:

$$P|\mathbf{0} \equiv P \qquad P|(Q|R) \equiv (P|Q)|R \qquad P|Q \equiv Q|P \qquad (\boldsymbol{\nu} p)\,\mathbf{0} \equiv \mathbf{0}$$

$$(\boldsymbol{\nu} p)(\boldsymbol{\nu} q)\,P \equiv (\boldsymbol{\nu} q)(\boldsymbol{\nu} p)\,P \qquad P \,|\, (\boldsymbol{\nu} p)\,Q \equiv (\boldsymbol{\nu} p)\,(P|Q) \;\text{ if } p \notin \mathrm{fn}(P)$$

We let $P[n/x]$ stand for the capture avoiding substitution of name $x$ with name $n$ in $P$. We use $\sigma$ to range over substitutions in $\pi$ (that simultaneously replace several names).

**Definition 4.1 (Late operational semantics and ground bisimilarity).** *The late operational semantics of $\pi$ is given by a transition relation whose set of labels is defined by:*

$$\mu \quad ::= \quad a(x) \mid \overline{a}b \mid \overline{a}(p) \mid \tau\,.$$

*Names $x$ and $p$ are said to be bound in actions $a(x)$ and $\overline{a}(p)$ respectively, and we use $\mathrm{bn}(\mu)$ to denote the set of bound names of action $\mu$.*

*The late transition relation, written $\rightarrow_\pi$, is given by the following rules (symmetrical versions of the rules involving parallel composition are omitted):*

$$\phi.P \xrightarrow{\phi}_\pi P \qquad \frac{P \xrightarrow{a(x)}_\pi P' \qquad Q \xrightarrow{\overline{a}b}_\pi Q'}{P \,|\, Q \xrightarrow{\tau}_\pi P'[b/x] \,|\, Q'}$$

$$\frac{P \xrightarrow{\overline{a}b}_\pi P'}{(\boldsymbol{\nu} b)\,P \xrightarrow{\overline{a}(b)}_\pi P'}\; a \neq b \qquad \frac{P \xrightarrow{a(x)}_\pi P' \qquad Q \xrightarrow{\overline{a}(p)}_\pi Q'}{P \,|\, Q \xrightarrow{\tau}_\pi (\boldsymbol{\nu} p)\,(P'[p/x] \,|\, Q')}$$

$$\frac{P \xrightarrow{\mu}_\pi P'}{P \,|\, Q \xrightarrow{\mu}_\pi P' \,|\, Q}\; \mathrm{bn}(\mu) \cap \mathrm{fn}(Q) = \emptyset \qquad \frac{P \xrightarrow{\mu}_\pi P'}{(\boldsymbol{\nu} p)\,P \xrightarrow{\mu}_\pi (\boldsymbol{\nu} p)\,P'}\; p \notin \mathrm{fn}(\mu)$$

*Note that we do not respect the convention on names in the rule to infer a bound output, precisely because we are transforming a free name ($b$) into a bound name.*

Ground bisimilarity*, written $\sim_{\mathrm{g}}$, is the largest symmetrical relation such that whenever $P \sim_{\mathrm{g}} Q$ and $P \xrightarrow{\mu}_\pi P'$, there exists $Q'$ s.t. $Q \xrightarrow{\mu}_\pi Q'$ and $P' \sim_{\mathrm{g}} Q'$.*

**Lemma 4.2.** *1. If $P\sigma \xrightarrow{\mu}_\pi P'$ where $\mu$ is $\overline{a}b$, $\overline{a}(p)$ or $a(x)$, then $P \xrightarrow{\mu'}_\pi P''$ with $\mu'\sigma = \mu$ and $P''\sigma = P'$.*

*2. If $P\sigma \xrightarrow{\tau}_\pi P'$ then*

*(a) $P \xrightarrow{\tau}_\pi P''$ and $P''\sigma = P'$ or*

*(b) $P \xrightarrow{\overline{b}c}_\pi \xrightarrow{a(x)}_\pi P''$ where $\sigma(a) = \sigma(b)$ and $P''[c/x]\sigma \sim P'$ or*

*(c) $P \xrightarrow{\overline{b}(p)}_\pi \xrightarrow{a(x)}_\pi P''$ where $\sigma(a) = \sigma(b)$ and $((\boldsymbol{\nu} p)P''[p/x])\sigma \sim P'$.*

*In the last two cases, the input and output actions are offered concurrently by $P$.*

*Proof.* Similar to the proof of Lemma 1.4.12 in [7], where the early transition semantics is treated.

### 4.2 Mutual Desynchronisations

**Definition 4.3 (mutual desynchronisation in $\mu$CCS).** *A* mutual desynchronisation *in $\mu$CCS is given by the existence of two prefixes $\eta_1, \eta_2$, and $\mu$CCS processes $P, P', Q, Q', R$ such that $\eta_1 \neq \eta_2$, $P \xrightarrow{\eta_1} P'$, $Q \xrightarrow{\eta_2} Q'$ and $\eta_2.P|Q'|R \sim P'|\eta_1.Q|R$.*

The notion of mutual desynchronisation is not specific to $\mu$CCS. As explained in the introduction, it corresponds to a situation where three processes $T, T_{12}, T_{21}$ satisfy:

(*i*) $\eta_1 \neq \eta_2$;
(*ii*) $T \xrightarrow{\eta_1}\xrightarrow{\eta_2} T_{12}$ and $T \xrightarrow{\eta_2}\xrightarrow{\eta_1} T_{21}$, where the first prefix being triggered dominates the second in both sequences of transitions (we say that a prefix occurrence $\eta_1$ *dominates* a prefix occurrence $\eta_2$ if $\eta_2$ occurs in the term prefixed by $\eta_1$);
(*iii*) $T_{12} \sim T_{21}$.

The proof of Lemmas 4.7 and 4.8 will expose analogous situations in $\pi$.

**Lemma 4.4 (No mutual desynchronisation).** *There is no mutual desynchronisation in $\mu$CCS.*

*Proof.* We define, for any $\mu$CCS process $P$ and prefix $\eta$, the *contribution of $P$ at $\eta$*, written $s_\eta(P)$, by $s_\eta(\mathbf{0}) = 0, s_\eta(P_1|P_2) = s_\eta(P_1) + s_\eta(P_2)$ and:

$$s_\eta(\eta.P) = \#(\eta.P) \qquad s_\eta(\eta'.P) = 0 \text{ if } \eta \neq \eta'$$

Intuitively, $s_\eta(P)$ is the total size of the components of $P$ that start with $\eta$. Since the distribution law preserves this quantity, we have that $P \sim Q$ implies $s_\eta(P) = s_\eta(Q)$ for all $\eta$.

Suppose now by contradiction that there are processes s.t. $P \xrightarrow{\eta_1} P'$, $Q \xrightarrow{\eta_2} Q'$ and $\eta_2.P|Q'|R \sim P'|\eta_1.Q|R$. By the cancellation property (Corollary 2.6), we have $\eta_2.P|Q' \sim P'|\eta_1.Q$, hence for all $\eta$, $s_\eta(\eta_2.P|Q') = s_\eta(P'|\eta_1.Q)$.

Since $s_{\eta_1}(\eta_2.P|Q') = s_{\eta_1}(Q') \leq \#(Q')$ and $s_{\eta_1}(P'|\eta_1.Q)) \geq s_{\eta_1}(\eta_1.Q) = \#(Q') + 2$, by taking $\eta = \eta_1$ we finally get $\#(Q') \geq \#(Q') + 2$. □

We shall rely on the previous result to show that a situation corresponding to a mutual desynchronisation cannot arise in $\pi$ either.

In what follows, we fix two distinct names $a$ and $b$, that will occur free in the processes we shall consider. The definitions and results below will depend on $a$ and $b$, but we avoid making this dependency explicit, in order to ease readability.

**Definition 4.5 (Erasing a $\pi$ process).** *Given a $\pi$ process $P$, we define the* erasing of $P$, *written $\mathcal{E}(P)$, as follows:*

$$\mathcal{E}(a(x).P) \stackrel{\text{def}}{=} a.\mathcal{E}(P) \qquad \mathcal{E}(m(x).P) \stackrel{\text{def}}{=} \mathbf{0} \text{ if } m \neq a$$

$$\mathcal{E}(\overline{b}n.P) \stackrel{\text{def}}{=} \overline{b}.\mathcal{E}(P) \qquad \mathcal{E}(\overline{m}n.P) \stackrel{\text{def}}{=} \mathbf{0} \text{ if } m \neq b$$

$$\mathcal{E}(P_1|P_2) \stackrel{\text{def}}{=} \mathcal{E}(P_1)\,|\,\mathcal{E}(P_2) \qquad \mathcal{E}((\boldsymbol{\nu} p)\,P) \stackrel{\text{def}}{=} \mathcal{E}(P) \qquad \mathcal{E}(\mathbf{0}) \stackrel{\text{def}}{=} \mathbf{0}$$

Note that $a$ and $b$ play different roles in the definition of $\mathcal{E}(\_)$.

It is immediate from the definition that $\mathcal{E}(P)$ is a $\mu$CCS process whose only prefixes are $a$ and $\overline{b}$. Intuitively, $\mathcal{E}(P)$ only exhibits the interactions of $P$ at $a$ (in input) and $b$ (in output) that are not guarded by interactions on other names. Names $a$ and $b$ will be fixed in the proof of Lemma 4.9.

**Lemma 4.6 (Transitions of $\mathcal{E}(P)$).** *Consider a $\pi$ process $P$. We have:*

- *$P \xrightarrow{a(x)}_\pi P'$ implies $\mathcal{E}(P) \xrightarrow{a} \mathcal{E}(P')$. If $P \xrightarrow{\overline{b}c}_\pi P'$ or $P \xrightarrow{\overline{b}(p)}_\pi P'$, then $\mathcal{E}(P) \xrightarrow{\overline{b}} \mathcal{E}(P')$.*
- *Conversely, if $\mathcal{E}(P) \xrightarrow{a} P_0$, then there exist $x$ and $P'$ s.t. $P_0 = \mathcal{E}(P')$ and $P \xrightarrow{a(x)}_\pi P'$. Similarly, if $\mathcal{E}(P) \xrightarrow{\overline{b}} P_0$, there exist $c, p, P'$ s.t. $P_0 = \mathcal{E}(P')$ and either $P \xrightarrow{\overline{b}c}_\pi P'$ or $P \xrightarrow{\overline{b}(p)}_\pi P'$.*

*Proof.* Simple reasoning on the LTSs of $\mu$CCS and $\pi$.

**Proposition 4.1 (Transfer).** *If $P \sim_{\mathrm{g}} Q$ in $\pi$, then $\mathcal{E}(P) \sim \mathcal{E}(Q)$ in $\mu$CCS.*

*Proof.* We reason by induction on the size of $P$ (defined as the number of prefixes in $P$). Consider a transition of $\mathcal{E}(P)$; as observed above, it can only be a transition along $a$ or a transition along $\overline{b}$.

Suppose $\mathcal{E}(P) \xrightarrow{a} P_0$. By Lemma 4.6, $P \xrightarrow{a(x)}_\pi P'$ and $P_0 = \mathcal{E}(P')$. Since $P \sim_{\mathrm{g}} Q$, $Q \xrightarrow{a(x)}_\pi Q'$ for some $Q'$ s.t. $P' \sim_{\mathrm{g}} Q'$. By induction, the latter relation gives $\mathcal{E}(P') \sim \mathcal{E}(Q')$, and $Q \xrightarrow{a(x)}_\pi Q'$ gives by Lemma 4.6 $\mathcal{E}(Q) \xrightarrow{a} \mathcal{E}(Q')$.

The case $\mathcal{E}(P) \xrightarrow{\overline{b}} P_0$ is treated similarly: by Lemma 4.6, there are two cases, according to whether $P$ does a free output or a bound output. Reasoning like above allows us to conclude in both cases.

We can now present our central technical result about $\pi$, which comes in two lemmas.

**Lemma 4.7.** *$Q \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{p})(a(x).P_1|\overline{b}c.P_2|P_3)$ implies that for some $Q_1, Q_2, Q_3$, $Q \equiv (\boldsymbol{\nu}\widetilde{q})(a(x).Q_1|\overline{b}c.Q_2|Q_3)$ and $(\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{q})(Q_1|Q_2|Q_3)$.*

*Proof.* Let $P = (\boldsymbol{\nu}\widetilde{p})(a(x).P_1|\overline{b}c.P_2|P_3)$ and $P' = (\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3)$.

Since $Q \sim_{\mathrm{g}} P$ and $P$ can perform two transitions along $a(x)$ and $\overline{b}c$ respectively, $Q$ can also perform these transitions, which gives

$Q \equiv (\boldsymbol{\nu}\widetilde{q})(a(x).Q_1|\overline{b}c.Q_2|Q_3)$ for some $\widetilde{q}, Q_1, Q_2, Q_3$,

the first (resp. second) component exhibiting the prefix that is triggered to answer the challenge on $a(x)$ (resp. $\overline{b}$c).

Consider now the challenge $P \xrightarrow{\overline{b}c}_\pi \xrightarrow{a(x)}_\pi P'$, to which $Q$ answers by performing $Q \xrightarrow{\overline{b}c}_\pi \xrightarrow{a(x)}_\pi Q_{ba}$, with $P' \sim_{\mathrm{g}} Q_{ba}$. If $Q_{ba} = (\boldsymbol{\nu}\widetilde{q})(Q_1|Q_2|Q_3)$, that is, if $Q$ triggers the prefixes on top of its first and second components, then we are done. Similarly, if $Q$ triggers a prefix in $Q_3$ to answer the second challenge, say

$Q_3 = a(x).Q_4|Q_5$, we can set $Q'_1 = a(x).Q_4$ and $Q'_3 = Q_1|Q_5$, and the lemma is proved.

The case that remains to be analysed is when $Q_2 \xrightarrow{a(x)}_\pi Q'_2$ and $Q_{ba} = (\boldsymbol{\nu}\widetilde{q})(a(x).Q_1|Q'_2|Q_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3)$.

We consider the challenge where $P$ fires its two topmost prefixes $a(x)$ and $\overline{b}c$ in the other sequence, namely $P \xrightarrow{a(x)}_\pi \xrightarrow{\overline{b}c}_\pi P'$. By hypothesis, $Q$ triggers the prefix of its first component for the first transition. To perform the second transition, $Q$ can fire the prefix $\overline{b}c$ either in its second or third component, in which case, as above, we are done, or, and this is the last possibility, the prefix $\overline{b}c$ occurs in $Q_1$. This means $Q_{ab} = (\boldsymbol{\nu}\widetilde{q})(Q'_1|\overline{b}c.Q_2|Q_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3)$, with $Q_1 \xrightarrow{\overline{b}c}_\pi Q'_1$.

To sum up, we have $Q_{ab} = (\boldsymbol{\nu}\widetilde{q})(Q'_1|\overline{b}c.Q_2|Q_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{q})(a(x).Q_1|Q'_2|Q_3) = Q_{ba}$, with $Q_1 \xrightarrow{\overline{b}c}_\pi Q'_1$ and $Q_2 \xrightarrow{a(x)}_\pi Q'_2$: this resembles the mutual desynchronisation of Definition 4.3, translated into the $\pi$-calculus.

Indeed, we can construct a mutual desynchronisation in $\mu$CCS: $Q_{ab} \sim_{\mathrm{g}} Q_{ba}$ implies $\mathcal{E}(Q_{ab}) \sim \mathcal{E}(Q_{ba})$ by Prop. 4.1, and $Q_1 \xrightarrow{\overline{b}c}_\pi Q'_1$ (resp. $Q_2 \xrightarrow{a(x)}_\pi Q'_2$) implies by Lemma 4.6 $\mathcal{E}(Q_1) \xrightarrow{\overline{b}} \mathcal{E}(Q'_1)$ (resp. $\mathcal{E}(Q_2) \xrightarrow{a} \mathcal{E}(Q'_2)$). Finally, using Lemma 4.4, we obtain a contradiction, which concludes our proof. □

**Lemma 4.8.** *$Q \sim_{\mathrm{g}} (\boldsymbol{\nu}p, \widetilde{p})(a(x).P_1|\overline{b}p.P_2|P_3)$ implies that for some $Q_1, Q_2, Q_3$, $Q \equiv (\boldsymbol{\nu}p, \widetilde{q})(a(x).Q_1|\overline{b}p.Q_2|Q_3)$ and $(\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{q})(Q_1|Q_2|Q_3)$.*

*Proof (Hint).* The proof follows the same lines as for the previous lemma. The only difference is when analysing the transitions that lead to $Q_{ab}$: to perform the second transition, $Q$ can either extrude the name called $p$ in the equality $Q \equiv (\boldsymbol{\nu}p, \widetilde{q})(a(x).Q_1|\overline{b}p.Q_2|Q_3)$, or otherwise $Q$ can be $\alpha$-converted in order to extrude another name. In the case where $Q$ chooses to extrude a different name, we can suppose without loss of generality that the necessary $\alpha$-conversion is a swapping between name $p$ and a name $q_1 \in \widetilde{q}$. This introduces some notational complexities when expressing $Q_{ab}$, but basically it does not affect the proof w.r.t. the proof of Lemma 4.7, because the function $\mathcal{E}(\_)$ is not sensitive to name permutations that do not involve $a$ or $b$. □

### 4.3 Congruence

**Theorem 4.9 (Closure of $\sim_{\mathrm{g}}$ under substitution).** *If $P \sim_{\mathrm{g}} Q$ then for any substitution $\sigma$, $P\sigma \sim_{\mathrm{g}} Q\sigma$.*

*Proof.* We reason by induction on the size of $P$. We consider $P$, $Q$ such that $P \sim_{\mathrm{g}} Q$ and suppose $P\sigma \xrightarrow{\mu}_\pi P_0$. We examine the transitions of $P$ that make it possible for $P\sigma$ to do a $\mu$-transition to $P_0$.

According to Lemma 4.2, there are two possibilities. The first possibility corresponds to the situation where $\mu$ comes from an action that $P$ can perform,

i.e., $P \xrightarrow{\mu'}_\pi P'$ for some $\mu'$, with $P'\sigma = P_0$ (cases 1 and 2a in Lemma 4.2). Since $P \sim_{\mathrm{g}} Q$, $Q \xrightarrow{\mu'}_\pi Q'$ and $P' \sim_{\mathrm{g}} Q'$ for some $Q'$. We check that $Q\sigma \xrightarrow{\mu} Q'\sigma$, and by induction $P' \sim_{\mathrm{g}} Q'$ implies $P'\sigma \sim_{\mathrm{g}} Q'\sigma$.

The second possibility (which corresponds to the difficult case) is given by $\mu = \tau$, where the synchronisation in $P'$ has been made possible by the application of $\sigma$. There are in turn two cases, corresponding to whether the synchronisation involves a free or a bound name. In the former case, $P \xrightarrow{a(x)}_\pi P'$ and $P \xrightarrow{\overline{b}c}_\pi P''$ for some $a, x, b, c, P', P''$. This entails $P \equiv (\boldsymbol{\nu}\widetilde{p})\,(a(x).P_1|\overline{b}c.P_2|P_3)$ for some $\widetilde{p}, P_1, P_2, P_3$, and, since $P \sim_{\mathrm{g}} Q$, we conclude by Lemma 4.7 that $Q \equiv (\boldsymbol{\nu}\widetilde{q})(a(x).Q_1|\overline{b}c.Q_2|Q_3)$ and

$$(\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{q})(Q_1|Q_2|Q_3)\,.$$

Since these processes are of size smaller than $P$, we can apply any substitution to the latter relation, and in particular $[c/x]\sigma$, yielding:

$$((\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3))[c/x]\sigma \sim_{\mathrm{g}} ((\boldsymbol{\nu}\widetilde{q})(Q_1|Q_2|Q_3))[c/x]\sigma\,,$$

which, using the Barendregt convention hypothesis, amounts to

$$P_0 \equiv ((\boldsymbol{\nu}\widetilde{p})(P_1[c/x]|P_2|P_3))\sigma \sim_{\mathrm{g}} ((\boldsymbol{\nu}\widetilde{q})(Q_1[c/x]|Q_2|Q_3))\sigma \stackrel{\mathrm{def}}{=} Q_0\,.$$

We conclude by checking that $Q\sigma \xrightarrow{\tau}_\pi Q_0$.

We reason similarly for the case where the synchronisation involves the transmission of a bound name, using Lemma 4.8 instead of Lemma 4.7. We may remark that Lemma 4.8 gives $(\boldsymbol{\nu}\widetilde{p})(P_1|P_2|P_3) \sim_{\mathrm{g}} (\boldsymbol{\nu}\widetilde{q})(Q_1|Q_2|Q_3)$, and in this case $P\sigma \xrightarrow{\tau}_\pi P_0 \equiv (\boldsymbol{\nu}p, \widetilde{p})(P_1[p/x]|P_2|P_3)$ (resp. $Q\sigma \xrightarrow{\tau}_\pi (\boldsymbol{\nu}p, \widetilde{q})(Q_1[p/x]|Q_2|Q_3)$): to conclude, not only do we need closure of $\sim_{\mathrm{g}}$ (given by induction), as above, but we must also use the fact that $\sim_{\mathrm{g}}$ is preserved by restriction: $P \sim_{\mathrm{g}} Q$ implies $(\boldsymbol{\nu}p)\,P \sim_{\mathrm{g}} (\boldsymbol{\nu}p)\,Q$ for any $P, Q, p$. □

**Corollary 4.10 (Congruence of bisimilarity in $\pi$).** *In $\pi$, ground, early and late bisimilarity coincide and are congruences.*

*Proof.* By a standard argument (see [7]): since $\sim_{\mathrm{g}}$ is closed under substitution, $\sim_{\mathrm{g}}$ is an open bisimulation. □

It is known (see [7]) that adding either replication or sum to $\pi$ yields a calculus where strong bisimilarity fails to be a congruence.

## 5 Conclusion

We have presented an axiomatisation of strong bisimilarity on a small subcalculus of CCS, and a new congruence result for the $\pi$-calculus.

Technically, the notion of mutual desynchronisation is related to substitution closure of strong bisimilarity, as soon as substitutions can create new interactions

by identifying two names. We have seen in Section 4 that there exists no mutual desynchronisation in $\pi$, and that $\sim_{\mathrm{g}}$ is a congruence.

In (full) CCS, mutual desynchronisations exist, a simple example being given by $a.\overline{b} + \overline{b}.a$. The latter process is bisimilar to $a|\overline{b}$, but the equality fails to hold when $b$ is replaced with $a$. The same reasoning holds for the $\pi$-calculus with choice.

It appears that in finite calculi, mutual desynchronisations give rise to counterexamples to substitution closure of strong bisimilarity. The situation is less clear when infinite behaviours can be expressed. For instance, in the extension of $\mu$CCS with replication, the process $!a \,|\, !\overline{b}$ is bisimilar to $P \stackrel{\mathrm{def}}{=} !a.\overline{b} \,|\, !\overline{b}.a$. Process $P$ leads to a mutual desynchronisation: we have $P \xrightarrow{a}\xrightarrow{\overline{b}} \equiv P \xrightarrow{\overline{b}}\xrightarrow{a} \equiv P$. We do not know at present whether $\sim$ is substitution-closed in this extension of $\mu$CCS (we may remark that the two aforementioned processes remain bisimilar when $b$ is replaced with $a$).

Some subcalculi of the $\pi$-calculus where strong bisimilarity is a congruence are obtained by restricting the output prefix [7]. In the *asynchronous $\pi$-calculus* ($A\pi$), mutual desynchronisations do not appear, basically because the output action is not a prefix. Strong bisimilarity is a congruence on $A\pi$. In the *private $\pi$-calculus* ($P\pi$), since only private names are emitted, no substitution generated by a synchronisation can identify two previously distinct names. Strong bisimilarity is substitution closed (for the particular substitutions at work in $P\pi$), and is a congruence.

Regarding future extensions of this work, we would like to study whether our approach can be adapted to analyse weak bisimilarity in $\pi$ (as mentioned in Remark 2.2, strong and weak bisimilarity coincide in $\mu$CCS). Another interesting direction, as hinted above, would be to study strong bisimilarity on infinite, restriction-free calculi (in CCS and the $\pi$-calculus).

*Acknowledgements.* We are grateful to Arnaud Carayol for interesting discussions at early stages of this work. We benefited from support by the french initiative 'ACI GEOCAL'.

## 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. O. Burkart, D. Caucal, F. Moller, and B. Steffen. Verification over Infinite States. In *Handbook of Process Algebra*, pages 545–623. Elsevier, 2001.
3. W. Fokkink and B. Luttik. An $\omega$-complete Equational Specification of Interleaving. In *Proc. of ICALP'00*, volume 1853 of *LNCS*, pages 729–743. Springer Verlag, 2000.
4. Y. Hirshfeld and M. Jerrum. Bisimulation Equivalence is Decidable for Normed Process Algebra. In *Proc. of ICALP'99*, volume 1644 of *LNCS*, pages 412–421. Springer Verlag, 1999.

5. B. Luttik. What is Algebraic in Process Theory? *Concurrency Column, Bulletin of the EATCS*, 88, 2006.
6. R. Milner and F. Moller. Unique Decomposition of Processes. *TCS*, 107(2):357–363, 1993.
7. D. Sangiorgi and D. Walker. *The $\pi$-calculus: a Theory of Mobile Processes*. Cambridge University Press, 2001.