Weak Equivalences in Psi-calculi

Magnus Johansson Jesper Bengtson Joachim Parrow Björn Victor

Dept. of Information Technology, Uppsala University, Sweden

Abstract

Psi-calculi extend the pi-calculus with nominal datatypes to represent data, communication channels, and logics for facts and conditions. This general framework admits highly expressive formalisms such as concurrent higher-order constraints and advanced cryptographic primitives. We here establish the theory of weak bisimulation, where the τ actions are unobservable. In comparison to other calculi the presence of assertions poses a significant challenge in the definition of weak bisimulation, and although there appears to be a spectrum of possibilities we show that only a few are reasonable. We demonstrate that the complications mainly stem from psi-calculi where the associated logic does not satisfy weakening.

We prove that weak bisimulation equivalence has the expected algebraic properties and that the corresponding observation congruence is preserved by all operators. These proofs have been machine checked in Isabelle. The notion of weak barb is defined as the output label of a communication action, and weak barbed equivalence is bisimilarity for τ actions and preservation of barbs in all static contexts. We prove that weak barbed equivalence coincides with weak bisimulation equivalence.

1 Introduction

In our earlier work [3] we introduced psi-calculi: a framework for advanced mobile process calculi. These accommodate applications with complex data structures and their operations, and high level logics for use in conditional constructs. Extensions of the pi-calculus are not new as such, but psi-calculi provide a single general and parametric framework with a clean theory and machine-checked proofs. In [3] we presented the labelled semantics, strong bisimulation congruence and algebraic properties; its implementation in the theorem prover Isabelle was presented in [4]; a fully abstract symbolic semantics appeared in [15].

In the present paper we establish the theory of weak (or observational) equivalences for psi-calculi. These equivalences abstract from the internal behaviour of the processes and are essential for applications, e.g. in simplifying descriptions in a modular way, and in verifying implementations against more abstract specifications. Interactions between internal components are disregarded unless they affect the externally visible behaviour. If the weak equivalence is compositional then the abstract specification can also be used as a part when building even larger systems, and this facilitates modular construction and reasoning.

The canonical weak equivalence is often considered to be *barbed bisimulation congruence* [16, 19] which is defined using the possible interactions, often called barbs, and reductions, closing under all contexts to form a congruence. Although natural and easy to understand this universal quantification of contexts makes the relation hard to use in proofs. It is a known hard problem to define weak equivalences that abstract from as much detail as possible and yet are both compositional and computationally tractable. A standard approach is to use *weak bisimulations*, where a single transition $\xrightarrow{a}$ is simulated by a sequence of transitions where the internal τ actions are considered invisible, a so called *weak transition* $\stackrel{a}{\Longrightarrow}$. In the pi-calculus several alternatives have been investigated for weak bisimulation, e.g. open, late and early; the latter coincides with barbed equivalence [19].

Weak bisimulation has been studied for some extensions of the pi-calculus, but the results are not conclusive and a general framework is lacking. In the case of spi-calculus [2] the weak labelled bisimulations are rather complex and the spectrum of equivalences includes framed [2], alley [6, 7, 5], fenced [12], trellis [6], and hedged [8], where framed coincides with hedged [5, 8] and fenced with trellis [13]. For the applied pi-calculus, the weak labelled bisimulation defined in [1] does not coincide with barbed equivalence and turns out to be non-compositional unless further restrictions on the calculus are imposed (as remarked in [3]). The explicit fusion calculus [20] defines weak barbed equivalence which is compositional but computationally awkward because of a universal quantification over contexts. Extensions of the pi-calculus for constraint programming have been defined e.g. in [11] (the π^{+}-calculus) and [10] (the CC-Pi calculus). The first de-

fines only barbed equivalence; the second defines only (strong) labelled bisimulation which turns out to be non-compositional (also as remarked in [3]).

In this paper we present a labelled weak bisimulation for psi-calculi. We formally establish its algebraic properties, including compositionality. The general framework of psi-calculi allows non-monotonic logics where a formula which holds at one point may be falsified by a transition, as in e.g. the "retract" construct of CC-Pi [9]. While adding expressive power, the non-monotonicity also poses new and unexpected challenges for weak bisimulation. With the possibility of new assertions (statements about data) appearing after any transition, "obvious" laws such as $P \mathrel{\dot{\approx}} \tau.P$ become invalid. Intuitively this is because P may contain a retract that invalidates an action of its environment. As an example, consider an agent P which through a retract jams an internal communication in Q, so that $P \mid Q$ cannot progress. The agent $\tau \,.\, P$ represents a state where the jamming has not yet started. Consequently Q can progress in the constellation $\tau \,.\, P \mid Q$. In other words, P and $\tau \,.\, P$ have demonstrably different effects on their environment: the τ prefix might postpone a jamming and thereby allow other actions. This is in contrast to the situation in the standard pi-calculus where $\tau \,.\, P \mid Q$ can have no more actions than $P \mid Q$. We prove that if monotonicity is enforced, by a logical weakening law saying that whatever is true stays true, this situation cannot arise and the definition of weak bisimulation can be significantly simplified.

We finally introduce a weak barbed bisimulation where the observations, or barbs, are simply the immediately available output actions. This results in a more intuitively obvious definition. We prove that it coincides with weak labelled bisimulation. In this way the intuitively attractive barbed equivalence is given the powerful proof technique of labelled bisimulation which does not require closure under all contexts.

Overview. In the next section we review the basic definitions of syntax, semantics, and strong bisimulation of psi-calculi. In Section 3 we present the first variant of weak bisimulation. This is intended for psi-calculi where logical weakening holds, and results in a relatively traditional bisimulation definition. In Section 4 we present the second more general variant of weak bisimulation, applicable to all psi-calculi, and explain and motivate it by examples. Section 5 presents our results on algebraic properties and compositionality, and the related notion of weak congruence. In Section 6 we introduce the notions of barb and barbed bisimulation equivalences, and prove that this equivalence coincides with weak bisimilarity. Finally in Section 7 we conclude and describe ongoing and future work.

2 Psi-calculi

This section is a brief recapitulation of psi-calculi; for a more extensive treatment including motivations and examples see [3].

We assume a countably infinite set of atomic *names* $\mathcal{N}$ ranged over by $a, b, \ldots, z$. Intuitively, names will represent the symbols that can be scoped, and also represent symbols acting as variables in the sense that they can be subject to substitution. A *nominal set* [18, 14] is a set equipped with a formal notion of what it means for a name x to occur in an element A of the set, written $x \in \mathrm{n}(A)$ (often pronounced as "x is in the support of A"). We write $a\#X$, pronounced "a is fresh for X", for $a \notin \mathrm{n}(X)$, and if A is a set of names we write $A\#X$ to mean $\forall a \in A \;.\; a\#X$. A *nominal data type* is a nominal set equipped with a set of operators on it.

A psi-calculus is defined by instantiating three nominal data types and four operators:

Definition 1 (Psi-calculus parameters)**.** *A psi-calculus requires the three (not necessarily disjoint) nominal data types: the (data) terms* $\mathbf{T}$*, ranged over by* M, N*, the conditions* $\mathbf{C}$*, ranged over by* φ*, the assertions* $\mathbf{A}$*, ranged over by* Ψ*, and the four operators:*

$\leftrightarrow\colon \mathbf{T} \times \mathbf{T} \to \mathbf{C}$	*Channel Equivalence*
$\otimes : \mathbf{A} \times \mathbf{A} \to \mathbf{A}$	*Composition*
$\mathbf{1} : \mathbf{A}$	*Unit*
$\vdash \subseteq \mathbf{A} \times \mathbf{C}$	*Entailment*

We assume that there exists a simultaneous substitution function $X[\widetilde{a} := \widetilde{M}]$ for any term, assertion or condition X. The binary functions above will be written in infix. Thus, if M and N are terms then $M \leftrightarrow N$ is a condition, pronounced "M and N are channel equivalent" and if Ψ and Ψ' are assertions then so is $\Psi \otimes \Psi'$. We say that a term is a *channel* if it is channel equivalent to something. Also we write $\Psi \vdash \varphi$, "Ψ entails φ", for $(\Psi, \varphi) \in \vdash$.

We say that two assertions are equivalent, written $\Psi \simeq \Psi'$ if they entail the same conditions, i.e. for all φ we have that $\Psi \vdash \varphi \Leftrightarrow \Psi' \vdash \varphi$. We impose certain requisites on the sets and operators. In brief, channel equivalence must be symmetric and transitive, $\otimes$ must be compositional with regard to $\simeq$, and the assertions with $(\otimes, \mathbf{1})$ form an abelian monoid. For details see [3].

In the following $\tilde{a}$ means a finite (possibly empty) sequence of names, $a_1, \ldots, a_n$. The empty sequence is written ϵ and the concatenation of $\tilde{a}$ and $\tilde{b}$ is written $\tilde{a}\tilde{b}$. When occurring as an operand of a set operator, $\tilde{a}$ means the corresponding set of names $\{a_1, \ldots, a_n\}$. We also use sequences of terms, conditions, assertions, etc., in the same way.

A *frame* F can intuitively be thought of as an assertion with local names: it is of the form $(\nu\widetilde{b})\Psi$ where $\widetilde{b}$ is a sequence of names that bind into the assertion Ψ. We use F, G

to range over frames. We overload Ψ to also mean the frame $(\nu\epsilon)\Psi$ and $\otimes$ to mean composition on frames defined by $(\nu\widetilde{b_1})\Psi_1 \otimes (\nu\widetilde{b_2})\Psi_2 = (\nu\widetilde{b_1}\widetilde{b_2})(\Psi_1 \otimes \Psi_2)$ where $\widetilde{b_1}\#\widetilde{b_2}, \Psi_2$ and vice versa. We also write $(\nu c)((\nu\widetilde{b})\Psi)$ to mean $(\nu c\widetilde{b})\Psi$.

Alpha equivalent frames are identified. We define $F \vdash \varphi$ to mean that there exist an alpha variant $(\nu\widetilde{b})\Psi$ of F such that $\widetilde{b}\#\varphi$ and $\Psi \vdash \varphi$. We also define $F \simeq G$ to mean that for all φ it holds that $F \vdash \varphi$ iff $G \vdash \varphi$. Intuitively a condition is entailed by a frame if it is entailed by the assertion and does not contain any names bound by the frame. Two frames are equivalent if they entail the same conditions.

Definition 2 (Psi-calculus agents)**.** *Given valid psi-calculus parameters as in Definition 1, the psi-calculus* agents*, ranged over by $P, Q, \ldots$, are of the following forms.*

$\overline{M}\,N.P$	Output
$\underline{M}(\lambda\widetilde{x})N.P$	Input
case $\varphi_1 : P_1 \,[]\, \cdots \,[]\, \varphi_n : P_n$	Case
$(\nu a)P$	Restriction
$P \mid Q$	Parallel
$!P$	Replication
$(\!\mid \Psi \mid\!)$	Assertion

In the Input $\underline{M}(\lambda\widetilde{x})N.P$ we require that $\widetilde{x} \subseteq \mathrm{n}(N)$ is a sequence without duplicates, and the names $\widetilde{x}$ bind occurrences in both N and P. Restriction binds a in P. An assertion is guarded *if it is a subterm of an Input or Output. In a replication $!P$ there may be no unguarded assertion in P, and in* **case** $\varphi_1 : P_1 \,[]\, \cdots \,[]\, \varphi_n : P_n$ *there may be no unguarded assertion in any P_i. We identify alpha-equivalent agents.*

Some notational conventions: We define the agent $\mathbf{0}$ as $(\!\mid \mathbf{1} \mid\!)$. We sometimes abbreviate the agent **case** $\varphi_1 : P_1 \,[]\, \cdots \,[]\, \varphi_n : P_n$ as **case** $\widetilde{\varphi} : \widetilde{P}$, or if $n = 1$ as **if** φ_1 **then** P_1. In psi-calculi where a condition $\top$ exists such that $\Psi \vdash \top$ for all Ψ we write $P + Q$ to mean **case** $\top : P \,[]\, \top : Q$. In some examples where prefix objects are unimportant we elide them, writing e.g. $\overline{M}.P$ for $\overline{M}N.P$. We introduce the prefix form $\tau.P$ through a communication over a restricted channel.[1]

The *frame $\mathcal{F}(P)$ of an agent* P is defined inductively as follows:

$$\begin{aligned}
&\mathcal{F}(\underline{M}(\lambda\widetilde{x})N.P) = \mathcal{F}(\overline{M}\,N.P)\\
&\qquad = \mathcal{F}(\mathbf{case}\ \widetilde{\varphi} : \widetilde{P}) = \mathcal{F}(!P) = \mathbf{1}\\
&\mathcal{F}(\!\mid \Psi \mid\!) = (\nu\epsilon)\Psi\\
&\mathcal{F}(P \mid Q) = \mathcal{F}(P) \otimes \mathcal{F}(Q)\\
&\mathcal{F}((\nu b)P) = (\nu b)\mathcal{F}(P)
\end{aligned}$$

[1] Formally, let M_a be a term that contains the name a. Define $\tau.P = (\nu a)(\overline{M_a}.P|\underline{M_a}.\mathbf{0})$ for $a\#P$ in psi-calculi where $\forall\Psi.\Psi \vdash M_a \leftrightarrow M_a$ and for all other terms N we have that $\forall\Psi.\Psi \not\vdash M_a \leftrightarrow N$. This is the generalisation of the usual definition of τ in pi-calculus: $\tau.P = (\nu a)(\overline{a}.P|\underline{a}.\mathbf{0})$ for $a\#P$.

The *actions* ranged over by α, β are of the following three kinds: Output $\overline{M}\,(\nu\tilde{a})N$ where $\alpha \subseteq \mathrm{n}(N)$, Input $\underline{M}\,N$, and Silent τ. Here we refer to M as the *subject* and N as the *object*. We define $\mathrm{bn}(\overline{M}\,(\nu\tilde{a})N) = \tilde{a}$, and $\mathrm{bn}(\alpha) = \emptyset$ if α is an input or τ. We also define $\mathrm{n}(\tau) = \emptyset$ and $\mathrm{n}(\alpha) = \mathrm{n}(M) \cup \mathrm{n}(N)$ for the input and output actions. As in the pi-calculus, the output $\overline{M}\,(\nu\tilde{a})N$ represents an action sending N along M and opening the scopes of the names $\tilde{a}$. Note in particular that the support of this action includes $\tilde{a}$. Thus $\overline{M}\,(\nu a)a$ and $\overline{M}\,(\nu b)b$ are different actions.

Definition 3 (Transitions)**.** *A* transition *is of the kind $\Psi \rhd P \xrightarrow{\alpha} P'$, meaning that in the environment Ψ the agent P can do an α to become P'. The transitions are defined inductively in Table 1. We write $P \xrightarrow{\alpha} P'$ without an assertion to mean $\mathbf{1} \rhd P \xrightarrow{\alpha} P'$.*

Agents, frames and transitions are identified by alpha equivalence. In a transition the names in $\mathrm{bn}(\alpha)$ bind into both the action object and the derivative, therefore $\mathrm{bn}(\alpha)$ is in the support of α but not in the support of the transition. This means that the bound names can be chosen fresh, substituting each occurrence in both the object and the derivative.

Definition 4 (Strong bisimulation)**.** *A* strong bisimulation *$\mathcal{R}$ is a ternary relation between assertions and pairs of agents such that $\mathcal{R}(\Psi, P, Q)$ implies all of*

1. *Static equivalence: $\Psi \otimes \mathcal{F}(P) \simeq \Psi \otimes \mathcal{F}(Q)$*
2. *Symmetry: $\mathcal{R}(\Psi, Q, P)$*
3. *Extension of arbitrary assertion: $\forall\Psi'.\ \mathcal{R}(\Psi \otimes \Psi', P, Q)$*
4. *Simulation: for all α, P' such that $\mathrm{bn}(\alpha)\#\Psi, Q$ there exists a Q' such that*

$$\Psi \rhd P \xrightarrow{\alpha} P' \Longrightarrow \Psi \rhd Q \xrightarrow{\alpha} Q' \wedge \mathcal{R}(\Psi, P', Q')$$

We define $P \mathrel{\dot\sim_\Psi} Q$ to mean that there exists a bisimulation $\mathcal{R}$ such that $\mathcal{R}(\Psi, P, Q)$, and write $\dot\sim$ for $\dot\sim_{\mathbf{1}}$.

Definition 5 (Strong congruence)**.** *$P \sim_\Psi Q$ means that for all $\widetilde{x}, \widetilde{M}$ it holds $P[\widetilde{x} := \widetilde{M}] \mathrel{\dot\sim_\Psi} Q[\widetilde{x} := \widetilde{M}]$, and we write $P \sim Q$ for $P \sim_{\mathbf{1}} Q$.*

In [3] we explore the algebraic properties of $\sim$, in particular we prove it a congruence for any psi-calculus.

3 Weak bisimulation

We introduce weak bisimulation equivalence, $\dot\approx$, with the intuition that τ actions are invisible. This notion is standard in many variants of the pi-calculus, but in our framework it poses unexpected challenges. As an example, consider the law $P \mathrel{\dot\approx} \tau.P$. This law looks obvious and indeed

$$\textsc{In}\ \frac{\Psi \vdash M \leftrightarrow K}{\Psi \rhd \underline{M}(\lambda\widetilde{y})N.P \xrightarrow{\underline{K}\,N[\widetilde{y}:=\widetilde{L}]} P[\widetilde{y} := \widetilde{L}]} \qquad \textsc{Out}\ \frac{\Psi \vdash M \leftrightarrow K}{\Psi \rhd \overline{M}\,N.P \xrightarrow{\overline{K}\,N} P} \qquad \textsc{Case}\ \frac{\Psi \rhd P_i \xrightarrow{\alpha} P' \qquad \Psi \vdash \varphi_i}{\Psi \rhd \mathbf{case}\ \widetilde{\varphi} : \widetilde{P} \xrightarrow{\alpha} P'}$$

$$\textsc{Com}\ \frac{\Psi{\otimes}\Psi_P{\otimes}\Psi_Q \vdash M \leftrightarrow K \qquad \Psi_Q{\otimes}\Psi \rhd P \xrightarrow{\overline{M}\,(\nu\widetilde{a})N} P' \qquad \Psi_P{\otimes}\Psi \rhd Q \xrightarrow{\underline{K}\,N} Q'}{\Psi \rhd P \mid Q \xrightarrow{\tau} (\nu\widetilde{a})(P' \mid Q')}\ \widetilde{a}\#Q$$

$$\textsc{Par}\ \frac{\Psi_Q{\otimes}\Psi \rhd P \xrightarrow{\alpha} P'}{\Psi \rhd P|Q \xrightarrow{\alpha} P'|Q}\ \mathrm{bn}(\alpha)\#Q \qquad \textsc{Scope}\ \frac{\Psi \rhd P \xrightarrow{\alpha} P'}{\Psi \rhd (\nu b)P \xrightarrow{\alpha} (\nu b)P'}\ b\#\alpha, \Psi$$

$$\textsc{Open}\ \frac{\Psi \rhd P \xrightarrow{\overline{M}\,(\nu\widetilde{a})N} P'}{\Psi \rhd (\nu b)P \xrightarrow{\overline{M}\,(\nu\widetilde{a}\cup\{b\})N} P'}\ \begin{array}{l} b\#\widetilde{a}, \Psi, M \\ b \in \mathrm{n}(N) \end{array} \qquad \textsc{Rep}\ \frac{\Psi \rhd P \mid !P \xrightarrow{\alpha} P'}{\Psi \rhd !P \xrightarrow{\alpha} P'}$$

Table 1. Structured operational semantics. Symmetric versions of COM and PAR are elided. In the rule COM we assume that $\mathcal{F}(P) = (\nu\widetilde{b}_P)\Psi_P$ and $\mathcal{F}(Q) = (\nu\widetilde{b}_Q)\Psi_Q$ where $\widetilde{b}_P$ is fresh for all of $\Psi, \widetilde{b}_Q, Q, M$ and P, and that $\widetilde{b}_Q$ is similarly fresh. In the rule PAR we assume that $\mathcal{F}(Q) = (\nu\widetilde{b}_Q)\Psi_Q$ where $\widetilde{b}_Q$ is fresh for Ψ, P and α. In OPEN the expression $\tilde{a} \cup \{b\}$ means the sequence $\tilde{a}$ with b inserted anywhere.

holds for weak bisimulation in the pi-calculus. But in psi-calculi in general it would imply that parallel composition does not preserve $\dot{\approx}$. Consider a situation where it holds that $\mathbf{1} \vdash \varphi$ and $\mathcal{F}(P) \nvdash \varphi$. In other words, $\mathcal{F}(P)$ makes condition φ false. Now consider

$$P \mid \mathbf{if}\ \varphi\ \mathbf{then}\ Q \qquad \text{and} \qquad \tau.P \mid \mathbf{if}\ \varphi\ \mathbf{then}\ Q$$

Here only the right hand side has the possibility of acting like Q. Therefore the left and right hand sides are not in general equivalent. If parallel preserves $\dot{\approx}$ then it follows that P and $\tau.P$ are not always equivalent.

The root of this issue is that the frame of P can *falsify* the condition φ. There are some circumstances where this might happen; an example is if the assertions represent constraint stores and the constraint system admits retracts. Suppose that P represents a retract of φ. A system sitting in parallel with P cannot infer φ, and therefore **if** φ **then** Q will have no action. But a system in parallel with $\tau\,.\,P$ might infer φ. Only when this agent executes its action τ and asserts the retract will **if** φ **then** Q become blocked. Thus P and $\tau\,.\,P$ cannot be deemed equivalent: the parallel context of **if** φ **then** Q can tell the difference by proceeding only in company with the latter.

In many natural instances of psi-calculi this situation cannot arise. For example, if the logics involved are monotonic there can be nothing similar to a retract: formally, frame composition $\otimes$ is interpreted as conjunction of information, and a logical weakening law is assumed, saying that a conjunction cannot entail less than its conjuncts. In our framework this is represented as an extra requisite:

$$\text{weakening:} \quad \Psi \vdash \varphi \;\Rightarrow\; \Psi{\otimes}\Psi' \vdash \varphi$$

Since $(\otimes, \mathbf{1})$ is a monoid we have $\mathbf{1}{\otimes}\Psi \simeq \Psi$ for all Ψ, and with weakening this implies $\mathbf{1} \vdash \varphi \;\Rightarrow\; \Psi \vdash \varphi$, in other words, no assertion can falsify any condition. With this requisite the law $P \dot{\approx} \tau\,.\,P$ indeed holds, and it turns out that the definition of weak bisimulation is significantly simpler. We shall therefore begin by exploring weak bisimulation for psi-instances with weakening, and later generalise to the situation without weakening.

Our approach is to adjust Definition 4 (strong bisimulation) so that τ actions can be inserted or removed when simulating a transition. Clause 1 in the definition, that P and Q are statically equivalent, is adjusted so that if P can make conditions true, then Q can make them true possibly after performing some τ actions. Clauses 2 and 3 are unchanged. Clause 4 (simulation) is split in two parts. If the action α to be simulated is τ then Q should simulate by doing zero or more τs. If it is a visible (i.e. non-τ) action then Q simulates by doing an arbitrary number of τ actions before and after the α action.

We define $\Psi \rhd P \implies P'$ to mean that there exist $P_1, \ldots P_n$ where $P = P_1$, $P' = P_n$, and $\Psi \rhd P_i \xrightarrow{\tau} P_{i+1}$ for all i in $[1, n-1]$, allowing the case where $n = 1$ and $P = P'$. The weak transition $\Psi \rhd P \stackrel{\alpha}{\Longrightarrow} P'$ is defined as $\Psi \rhd P \implies P''$ and $\Psi \rhd P'' \xrightarrow{\alpha} P'''$ and $\Psi \rhd P''' \implies P'$. We also define $P \leq_\Psi Q$, pronounced P statically implies Q, to mean that $\forall\varphi.\ \Psi{\otimes}\mathcal{F}(P) \vdash \varphi \;\Rightarrow\; \Psi{\otimes}\mathcal{F}(Q) \vdash \varphi$. We write $P \leq Q$ for $P \leq_{\mathbf{1}} Q$.

Definition 6 (Simple weak bisimulation)**.** *A* simple weak bisimulation $\mathcal{R}$ *is a ternary relation between assertions and pairs of agents such that* $\mathcal{R}(\Psi, P, Q)$ *implies all of*

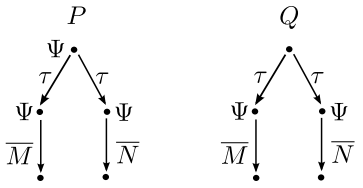
1. *Weak static implication: There exists* Q' *such that* $\Psi \rhd Q \implies Q'$ *and* $P \leq_\Psi Q'$ *and* $\mathcal{R}(\Psi, P, Q')$.
2. *Symmetry:* $\mathcal{R}(\Psi, Q, P)$
3. *Extension of arbitrary assertion:* $\forall \Psi'.\ \mathcal{R}(\Psi \otimes \Psi', P, Q)$
4. *Weak simulation: for all* α, P' *such that* $\mathrm{bn}(\alpha) \# \Psi, Q$ *and* $\Psi \rhd P \xrightarrow{\alpha} P'$ *it holds*

$$\begin{array}{ll} \text{if } \alpha = \tau: & \exists Q'.\ \Psi \rhd Q \implies Q' \ \wedge\ \mathcal{R}(\Psi, P', Q') \\ \text{if } \alpha \neq \tau: & \exists Q'.\ \Psi \rhd Q \stackrel{\alpha}{\Longrightarrow} Q' \ \wedge\ \mathcal{R}(\Psi, P', Q') \end{array}$$

We define $P \dot{\approx}^s_\Psi Q$ *to mean that there exists a simple weak bisimulation* $\mathcal{R}$ *such that* $\mathcal{R}(\Psi, P, Q)$*, and write* $P \dot{\approx}^s Q$ *for* $P \dot{\approx}^s_{\mathbf{1}} Q$.

The one point which may not be immediately obvious is Clause 1, weak static implication, where the conjunct $\mathcal{R}(\Psi, P, Q')$ may be surprising. It states that Q must evolve to a Q' that is statically implied by P, and also bisimilar to P. This last requirement may seem unnecessarily strong, but in fact without it the resulting simple weak bisimulation equivalence would not be preserved by the parallel operator. To prove this, let $\dot{\approx}'$ be defined as simple weak bisimulation above but without the conjunct $\mathcal{R}(\Psi, P, Q')$ in Clause 1. Let there be an assertion Ψ and condition φ such that $\Psi \vdash \varphi$ and $\mathbf{1} \not\vdash \varphi$, and let L, M, N be distinct terms. Consider the following agents (the diagrams illustrate agents informally):

$$\begin{array}{l} P = (\!|\Psi|\!) \mid (\tau.\overline{M}.\mathbf{0} + \tau.\overline{N}.\mathbf{0}) \\ Q = \tau.((\!|\Psi|\!)|\overline{M}.\mathbf{0}) + \tau.((\!|\Psi|\!)|\overline{N}.\mathbf{0}) \\ R = \textbf{if } \varphi \textbf{ then } \overline{L}.\mathbf{0} \end{array}$$



The transitions from P and Q are identical, only their frames differ in that $\mathcal{F}(P) = \Psi$ and $\mathcal{F}(Q) = \mathbf{1}$. With our original definition $P \dot{\approx}^s Q$, since there is no appropriate Q' for Clause 1. In contrast we have $P \dot{\approx}' Q$ since $Q \xrightarrow{\tau} Q'$ implies $\mathcal{F}(Q') = \mathcal{F}(P)$. But to simulate $P|R \xrightarrow{\overline{L}} P|\mathbf{0}$ from $Q|R$ the only possibilities are $Q|R \stackrel{\overline{L}}{\Longrightarrow} (\!|\Psi|\!)|\overline{M}.\mathbf{0}|\mathbf{0}$ and $Q|R \stackrel{\overline{L}}{\Longrightarrow} (\!|\Psi|\!)|\overline{N}.\mathbf{0}|\mathbf{0}$. Neither of these can continue to simulate $P|\mathbf{0}$ which can perform both actions $\overline{M}$ and $\overline{N}$. Therefore $P|R \not\dot{\approx}' Q|R$.

Simple weak bisimulation is the natural weak counterpart of Definition 4. For all psi-calculi that satisfy the weakening requisite it is sufficient. As we demonstrate in the following section, without weakening the simple weak bisimulation is in general not preserved by parallel composition and also not transitive; therefore a more elaborate definition is required in these cases.

4 Psi-calculi without weakening

We now generalise to psi-calculi without the weakening requisite. It turns out that the definition of weak labelled bisimulation needs to be adjusted in Clauses 1 and 4, where the interplay of assertions and transitions is quite subtle. We proceed to give the full definition of weak labelled bisimulation and a proof that it coincides with $\dot{\approx}^s$ for psi-calculi with weakening, followed by a series of examples motivating the need for the added complexities.

Definition 7 (Weak bisimulation)**.** *A* weak bisimulation $\mathcal{R}$ *is a ternary relation between assertions and pairs of agents such that* $\mathcal{R}(\Psi, P, Q)$ *implies all of*

1. *Weak static implication:*

$$\begin{array}{l} \forall \Psi' \exists Q'', Q'. \\ \quad \Psi \rhd Q \implies Q'' \quad \wedge \quad P \leq_\Psi Q'' \quad \wedge \\ \quad \Psi \otimes \Psi' \rhd Q'' \implies Q' \quad \wedge \quad \mathcal{R}(\Psi \otimes \Psi', P, Q') \end{array}$$

2. *Symmetry:* $\mathcal{R}(\Psi, Q, P)$
3. *Extension of arbitrary assertion:* $\forall \Psi'.\ \mathcal{R}(\Psi \otimes \Psi', P, Q)$
4. *Weak simulation: for all* α, P' *such that* $\mathrm{bn}(\alpha) \# \Psi, Q$ *and* $\Psi \rhd P \xrightarrow{\alpha} P'$ *it holds*

$$\begin{array}{l} \text{if } \alpha = \tau: \exists Q'. \quad \Psi \rhd Q \implies Q' \quad \wedge \quad \mathcal{R}(\Psi, P', Q') \\ \text{if } \alpha \neq \tau: \forall \Psi' \exists Q'', Q'''. \\ \quad \Psi \rhd Q \implies Q''' \quad \wedge \quad P \leq_\Psi Q''' \quad \wedge \\ \quad \Psi \rhd Q''' \xrightarrow{\alpha} Q'' \quad \wedge \\ \quad \exists Q'. \quad \Psi \otimes \Psi' \rhd Q'' \implies Q' \quad \wedge \quad \mathcal{R}(\Psi \otimes \Psi', P', Q') \end{array}$$

We define $P \dot{\approx}_\Psi Q$ *to mean that there exists a weak bisimulation* $\mathcal{R}$ *such that* $\mathcal{R}(\Psi, P, Q)$ *and write* $P \dot{\approx} Q$ *for* $P \dot{\approx}_{\mathbf{1}} Q$.

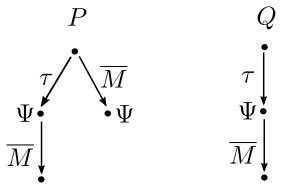
Theorem 8. *For psi-calculi that satisfy weakening,* $\dot{\approx}^s$ *and* $\dot{\approx}$ *coincide.*

The proof has been verified in Isabelle. Proof sketch for Clause 4: In one direction, every weak bisimulation with weakening is also a simple weak bisimulation (just take $\Psi' = \mathbf{1}$). For the other direction we must show that in psi-calculi that satisfy weakening, every simple weak bisimulation is a weak bisimulation. We explain how the additional requirements of clause 4 in weak bisimulation are satisfied. First, use Clause 1 to find $Q^\dagger$ such that $\Psi \rhd Q \implies Q^\dagger$ and $P \leq_\Psi Q^\dagger$ and $\mathcal{R}(\Psi, P, Q^\dagger)$. Using the latter with Clause 4 we get that $\Psi \rhd Q^\dagger \stackrel{\alpha}{\Longrightarrow} Q'$ with $\mathcal{R}(\Psi, P', Q')$, and since $\Psi \rhd Q \implies Q^\dagger$ we get a corresponding $\Psi \rhd Q \stackrel{\alpha}{\Longrightarrow} Q'$, where the first part of the weak transition passes through $Q^\dagger$. Now use the lemma (which requires weakening) $P \leq_\Psi Q$ and $\Psi \rhd Q \xrightarrow{\alpha} Q' \Rightarrow P \leq_\Psi Q'$. This gives the conjunct $P \leq_\Psi Q'''$ in Clause 4. Next use the lemma $\Psi \rhd P \xrightarrow{\alpha} P' \Rightarrow \Psi{\otimes}\Psi' \rhd P \xrightarrow{\alpha} P'$ (which also requires weakening). This means that the part "$\Psi{\otimes}\Psi' \rhd Q'' \ldots$" follows from the simpler Clause 4 (which has the same without "$\otimes\Psi'$"). Finally the last conjunct $\mathcal{R}(\Psi{\otimes}\Psi', P', Q')$ follows from $\mathcal{R}(\Psi, P', Q')$ of the simpler Clause 4, and Clause 3. □

We now proceed to motivate the added complexity of Clause 4.

Example: the use of $P \leq_\Psi Q'''$. We shall demonstrate that with a simplification omitting $P \leq_\Psi Q'''$ in Clause 4, i.e., if we do not take into account the conditions that hold at the point of executing the visible part of a simulation, then equivalence is not in general preserved by parallel. Let $\dot{\approx}'$ be defined with this simplification. Choose an instance with an assertion Ψ and condition φ such that $\Psi \not\vdash \varphi$ and $\mathbf{1} \vdash \varphi$, i.e., Ψ makes φ false. Consider the agents

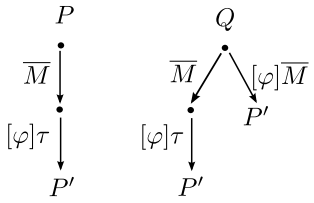
$$P = \tau.((\!|\Psi|\!) \mid \overline{M}.\mathbf{0}) + \overline{M}.(\!|\Psi|\!)$$
$$Q = \tau.((\!|\Psi|\!) \mid \overline{M}.\mathbf{0})$$
$$R = \textbf{if } \varphi \textbf{ then } \underline{M}.\overline{N}.\mathbf{0}$$



Here $P \dot{\approx}' Q$. To see this, consider the only transition that differs between the agents, namely $P \xrightarrow{\overline{M}} (\!|\Psi|\!)$. This can be simulated by $Q \xrightarrow{\tau} (\!|\Psi|\!) \mid \overline{M}.\mathbf{0} = Q'''$ and $Q''' \xrightarrow{\overline{M}} (\!|\Psi|\!)|\mathbf{0}$. But in composition with R, we have through the second branch of P that $P|R \xrightarrow{\tau} (\!|\Psi|\!)|\overline{N}.\mathbf{0}$. This cannot be weakly simulated by $Q|R$ since $Q|R \xrightarrow{\tau} (\!|\Psi|\!) \mid \overline{M}.\mathbf{0} \mid R$ which has no $\overline{N}$ transition. Therefore $P|R \not\dot{\approx}' Q|R$ and $\dot{\approx}'$ is not preserved by parallel.

Example: the quantification $\forall\Psi'$. Next we motivate the quantification of Ψ' in the subclause $\alpha \neq \tau$ of weak simulation, showing that without it, again equivalence would not be preserved by parallel. Let $\dot{\approx}'$ be defined with this simplification. Let Ψ and φ be such that $\mathbf{1} \vdash \varphi$ and $\Psi \not\vdash \varphi$ and let

$$P = \overline{M}.\,\textbf{if } \varphi \textbf{ then } \tau.P'$$
$$Q = P + \textbf{if } \varphi \textbf{ then } \overline{M}.P'$$
$$R = \underline{M}.(\!|\Psi|\!)$$



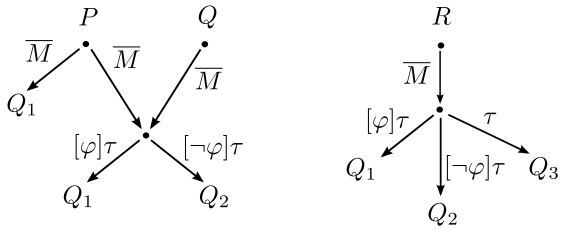
Here $P \dot{\approx}' Q$. Clearly we have $Q|R \xrightarrow{\tau} P'|(\!|\Psi|\!)$ through the second branch of Q. This cannot be weakly simulated by $P|R$. Here the only transition is $P|R \xrightarrow{\tau}$ **if** φ **then** $\tau.P' \mid (\!|\Psi|\!)$ which has no further transition. Therefore $P|R \not\dot{\approx}' Q|R$ and $\dot{\approx}'$ is not preserved by parallel.

Example: quantifier order of Ψ' and Q'. Next we motivate the order of the quantifiers, showing that if we commute the quantifiers $\forall\Psi'$ and $\exists Q'$ the resulting "equivalence" would not be transitive. Let $\dot{\approx}'$ be defined with these quantifiers commuted. Let all Q_i for $i = 1, 2, 3$ be distinct but weakly equivalent, and let $\varphi, \neg\varphi$ be two conditions that partition the assertions in two disjoint sets $\{\Psi.\ \Psi \vdash \varphi \wedge \Psi \not\vdash \neg\varphi\}$ and $\{\Psi.\ \Psi \not\vdash \varphi \wedge \Psi \vdash \neg\varphi\}$. Let $\top$ be a condition that is entailed by all assertions, and let

$$U = \textbf{case } \varphi : \tau.Q_1 \;[]\; \neg\varphi : \tau.Q_2$$
$$V = \textbf{case } \varphi : \tau.Q_1 \;[]\; \neg\varphi : \tau.Q_2 \;[]\; \top : \tau.Q_3$$

Here $U \dot{\approx} V$. The rightmost branch in $\Psi \rhd V \xrightarrow{\tau} Q_3$ is simulated by one of the two branches in U (which one depends on Ψ). Let

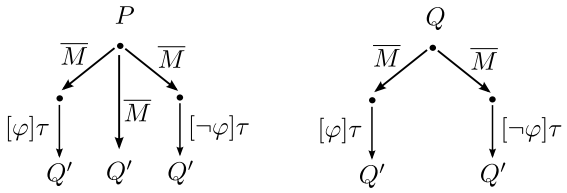
$$P = \overline{M}.Q_1 + \overline{M}.U$$
$$Q = \overline{M}.U$$
$$R = \overline{M}.V$$



Our point is that although $P \dot{\simeq} R \dot{\simeq} Q$ we have $P \dot{\simeq}' R$ and $R \dot{\simeq}' Q$, but not $P \dot{\simeq}' Q$. The crucial difference between the equivalences is explained as follows. $P \dot{\simeq} Q$ holds because the only nontrivial simulation is for Q to simulate the first branch of P. This is done by first doing $\overline{M}$ leading to U, and then for all Ψ' continuing to either Q_1 or Q_2, depending on whether $\Psi' \vdash \varphi$ or not. Here the quantification order is important. If the final bisimulation clause would read $\exists Q' \forall \Psi' \ldots$ then Q cannot simulate the first branch of P and therefore $P \dot{\not\simeq}' Q$. Note that $P \dot{\simeq}' R$ since the only nontrivial case is again for R to simulate the first branch of P. This can be done through the third branch leading to Q_3. This holds for any Ψ'.

Example: quantifier order of Ψ' and Q''. In Clause 4, the quantifier order is $\forall \Psi' \exists Q''$. Let $\dot{\simeq}'$ be defined with the alternative order $\exists Q'' \forall \Psi'$. The difference is highlighted by the following example. Let φ and $\neg\varphi$ be two conditions such that for any assertion exactly one of them is entailed, as in the previous example. Let

$$\begin{aligned} P = \;& \overline{M}.Q' + Q \\ Q = \;& \overline{M}.\textbf{if } \varphi \textbf{ then } \tau.Q' \\ & + \overline{M}.\textbf{if } \neg\varphi \textbf{ then } \tau.Q' \end{aligned}$$

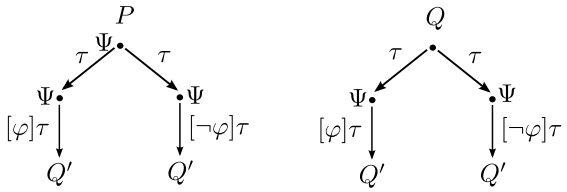


Here $P \dot{\simeq} Q$ and $P \dot{\not\simeq}' Q$. To see this consider how Q can simulate $P \xrightarrow{\overline{M}} Q'$. Using $\dot{\simeq}$, for all Ψ' we must find a Q'' such that $Q \xrightarrow{\overline{M}} Q''$ and $Q'' \implies Q'$. This holds, since the choice of Q'' may depend on Ψ'. Using $\dot{\simeq}'$ we must find one Q'' suitable for all Ψ', and there is none.

As it turns out $\dot{\simeq}'$ is a viable definition, in the sense that it is transitive and preserves parallel. But from an observational point of view it is hard to argue that P and Q should be different — in essence that would give the observer the power to observe that a conditional branch has been passed. The difference between $\dot{\simeq}$ and $\dot{\simeq}'$ is reminiscent of the difference between late and early equivalence, and as we shall see in Section 6 the weak barbed bisimulation corresponds to $\dot{\simeq}$ and not to $\dot{\simeq}'$.

Example: quantifiers in Clause 1. Keeping the simpler Clause 1 from Definition 6 will also yield an equivalence $\dot{\simeq}'$ that preserves parallel. A distinguishing example is similar to the one above. Again, let φ and $\neg\varphi$ be two conditions such that for any assertion exactly one of them is entailed. Let Ψ be an assertion such that $\mathbf{1} \leq \Psi$ and $\Psi \not\leq \mathbf{1}$ and $\Psi \otimes \Psi \simeq \mathbf{1}$.

$$\begin{aligned} P = \;& (\!|\Psi|\!) \mid (\tau \,.\, \textbf{if } \varphi \textbf{ then } \tau.Q' + \tau \,.\, \textbf{if } \neg\varphi \textbf{ then } \tau.Q' \\ Q = \;& \tau \,.\, ((\!|\Psi|\!) \mid \textbf{if } \varphi \textbf{ then } \tau.Q') \\ & + \tau \,.\, ((\!|\Psi|\!) \mid \textbf{if } \neg\varphi \textbf{ then } \tau.Q') \end{aligned}$$



Here we assume that Q' is weakly bisimilar to $(\!|\Psi|\!) \mid Q$. Then $P \dot{\simeq} Q$. The critical argument is that in Clause 1, depending on whether $\Psi' \otimes \Psi \vdash \varphi$ or not, Q can evolve to either $(\!|\Psi|\!) \mid \textbf{if } \varphi \textbf{ then } \tau.Q'$ or $(\!|\Psi|\!) \mid \textbf{if } \neg\varphi \textbf{ then } \tau.Q'$, in either case reaching an agent with a frame Ψ. It can then continue to $(\!|\Psi|\!) \mid Q' \dot{\simeq} (\!|\Psi \otimes \Psi|\!) \mid Q \dot{\simeq} Q$. In contrast $P \dot{\not\simeq}' Q$, since Q cannot evolve to an agent that both has Ψ as frame and is bisimilar to P. Again, it is hard to argue that they should be different from an observational point of view, and they are indeed weakly barbed equivalent.

5 Algebraic properties

In this section we establish results about weak bisimulation equivalence and the related congruence. First, note that weak bisimulation is not preserved by the **case** construct. The reasoning is analogous to why weak bisimulation is not preserved by the operator $+$ in CCS or the pi-calculus: $\tau \,.\, \mathbf{0} \dot{\simeq} \mathbf{0}$ but $a \,.\, \mathbf{0} + \tau \,.\, \mathbf{0} \dot{\not\simeq} a \,.\, \mathbf{0} + \mathbf{0}$. If the left-hand process does its τ action, the right-hand can only simulate by standing still. In the next step, the right-hand can do the action a which the left-hand can no longer simulate. This problem is solved in a standard way: in the simulation clause of bisimulation where $\alpha = \tau$, Q must simulate the τ action made by P with a τ chain containing at least one τ action.

Weak bisimulation is also not preserved by input prefixes, again for the same reason as in the pi-calculus. Closing the relation is under substitution in the same way as is done for strong bisimulation leads to the definition of weak congruence, denoted $\approx^c$.

Definition 9 (Weak congruence)**.** *P and Q are weakly Ψ-congruent, written $P \approx^c_\Psi Q$, if $P \dot{\simeq}_\Psi Q$ and they also satisfy* weak congruence simulation*:*

for all P' such that $\Psi \rhd P \xrightarrow{\tau} P'$ it holds:

$$\exists Q' .\; \Psi \rhd Q \stackrel{\tau}{\Longrightarrow} Q' \;\wedge\; P' \dot{\simeq}_\Psi Q'$$

and similarly with the roles of P and Q exchanged. We define $P \approx^c Q$ to mean that for all Ψ, and for all $\tilde{x}, \tilde{M}$ of equal length it holds that $P[\tilde{x} := \tilde{M}] \approx^c_\Psi Q[\tilde{x} := \tilde{M}]$.

An expected result is:

Theorem 10. *If $P \sim_\Psi Q$ then $P \approx^c_\Psi Q$.*

With this and the results in [3] it is straightforward to infer:

Theorem 11 (Structural laws)**.**

$$
\begin{array}{rcll}
P & \approx^c & P \mid \mathbf{0} & \\
P \mid (Q \mid R) & \approx^c & (P \mid Q) \mid R & \\
P \mid Q & \approx^c & Q \mid P & \\
(\nu a)\mathbf{0} & \approx^c & \mathbf{0} & \\
P \mid (\nu a)Q & \approx^c & (\nu a)(P \mid Q) & \text{if } a\#P \\
\overline{M}\,N.(\nu a)P & \approx^c & (\nu a)\overline{M}\,N.P & \text{if } a\#M,N \\
\underline{M}(\lambda\widetilde{x})N.(\nu a)P & \approx^c & (\nu a)\underline{M}(\lambda\widetilde{x})(N).P & \text{if } a\#\widetilde{x},M,N \\
\textbf{case } \widetilde{\varphi} : \widetilde{(\nu a)P} & \approx^c & (\nu a)\textbf{case } \widetilde{\varphi} : \widetilde{P} & \text{if } a\#\widetilde{\varphi} \\
(\nu a)(\nu b)P & \approx^c & (\nu b)(\nu a)P & \\
!P & \approx^c & P \mid !P &
\end{array}
$$

As noted, weak bisimilarity preserves all operators except **case** and input prefix:

Theorem 12. *For all Ψ:*

1. $P \dot{\approx}_\Psi Q \Longrightarrow P \mid R \dot{\approx}_\Psi Q \mid R$.
2. $P \dot{\approx}_\Psi Q \Longrightarrow (\nu a)P \dot{\approx}_\Psi (\nu a)Q$.
3. $P \dot{\approx}_\Psi Q \Longrightarrow !P \dot{\approx}_\Psi !Q$.
4. $P \dot{\approx}_\Psi Q \Longrightarrow \overline{M}\,N.P \dot{\approx}_\Psi \overline{M}\,N.Q$.
5. $(\forall \widetilde{L}.\, P[\widetilde{a} := \widetilde{L}] \dot{\approx}_\Psi Q[\widetilde{a} := \widetilde{L}]) \implies \underline{M}(\lambda\widetilde{a})N.P \dot{\approx}_\Psi \underline{M}(\lambda\widetilde{a})N.Q$.

Weak congruence is aptly named:

Theorem 13. *Weak congruence $\approx^c$ is preserved by all operators.*

We have also proved the usual τ laws:

Theorem 14.

1. $P \dot{\approx} \tau\,.\,P$ *in psi-calculi with weakening.*
2. $P + \tau\,.\,P \approx^c \tau\,.\,P$.
3. $\alpha\,.\,\tau\,.\,P \approx^c \alpha\,.\,P$ *in psi-calculi with weakening.*
4. $\alpha\,.\,P + \alpha\,.\,(\tau\,.\,P + Q) \approx^c \alpha\,.\,(\tau\,.\,P + Q)$.

As noted in the beginning of Section 3, Theorem 14(1) is not valid in general for psi-calculi that do not satisfy weakening. The same holds for Theorem 14(3), for a similar reason. In contrast, the remaining τ laws (2 and 4) are valid also in calculi without weakening.

The results in this section have been proved using the interactive theorem prover Isabelle.

6 Barbed equivalence

We here introduce a straightforward notion of barbed equivalence, and demonstrate that it coincides with weak labelled bisimilarity. The barbed equivalence is defined in a traditional manner [16, 19] and is more intuitively obvious than the technically intricate Definition 7. At the same time, the barbed equivalence definition is not very practical for proofs since it embodies an explicit universal quantification over contexts. The result that the equivalences coincide means that we bestow the intuitively correct notion with the practical proof method of labelled bisimulations.

Barbed equivalence is derived from a few basic principles based on an informal notion of an observer. The first is to identify what are the *barbs*, or immediate observations, of an agent. In this paper the barbs will simply be the output actions: an agent has the barb $\overline{K}\ (\nu\widetilde{a})N$ precisely if a has a transition with that label. The second is to identify what it means for an agent to reduce, or evolve, to another agent. We choose the transitions $\xrightarrow{\tau}$ to represent this. In other words, for the purpose of barbed equivalence we use the same semantics as in Table 1. Finally we identify what kind of contexts an observer may use. We here follow the work on barbed equivalence in the applied pi-calculus [1] and consider the static contexts, aka evaluation contexts, built from parallel composition and restriction. This motivates the following definitions:

Definition 15 (Barbs and reductions)**.**

1. *P has the* barb $\overline{K}\ (\nu\widetilde{a})N$*, written $P \downarrow_{\overline{K}\ (\nu\widetilde{a})N}$, if $\exists P'.\, \mathbf{1} \rhd P \xrightarrow{\overline{K}\ (\nu\widetilde{a})N} P'$. Here names in $\tilde{a}$ bind occurrences in N, and alpha equivalent barbs are identified.*
2. *P* reduces to *P', written $P \longrightarrow P'$, if $P \xrightarrow{\tau} P'$, and $P \Longrightarrow P'$ means $\mathbf{1} \rhd P \Longrightarrow P'$ (so $\Longrightarrow$ is the reflexive transitive closure of $\longrightarrow$).*
3. *P has the* weak barb $\overline{K}\ (\nu\widetilde{a})N$*, written $P \Downarrow_{\overline{K}\ (\nu\widetilde{a})N}$, if $\exists P'.\, P \Longrightarrow P'$ and $P' \downarrow_{\overline{K}\ (\nu\widetilde{a})N}$.*

Definition 16 (Weak barbed equivalence)**.** Weak barbed equivalence*, written $\dot{\approx}_b$, is the largest equivalence relation on agents satisfying:*

1. *Barb similarity: $P \downarrow_{\overline{K}\ (\nu\widetilde{a})N} \quad \Rightarrow \quad Q \Downarrow_{\overline{K}\ (\nu\widetilde{a})N}$*
2. *Reduction simulation:*
   $P \longrightarrow P' \quad \Rightarrow \quad \exists Q'.\, Q \Longrightarrow Q'$ and $P' \dot{\approx}_b Q'$.
3. *Closed under static contexts:*
   $\forall R, \tilde{a}.\ (\nu\tilde{a})(P \mid R) \dot{\approx}_b (\nu\tilde{a})(Q \mid R)$.

The main theorem of this section is :

Theorem 17. *$P \dot{\approx}_b Q$ if and only if $P \dot{\approx} Q$.*

Proof. The ($\Leftarrow$)-direction is immediate. Barb similarity and reduction simulation follow directly from Clause 4 in the definition of weak bisimulation, and closure under static contexts is proved using Theorem 12(1) and (2). The ($\Rightarrow$)-direction is more involved. The idea is to show $\dot{\approx}_b$ to be a weak bisimulation by constructing contexts which expose transitions. The proof requires a minimum of expressiveness for the psi-calculus. It uses a set of channels written M_a that do not occur in any process under consideration. In other words, $\Psi \vdash M_a \dot{\leftrightarrow} M_a$, and for all other terms N we have that $\Psi \not\vdash M_a \dot{\leftrightarrow} N$. The proof also uses conditions φ_P for agents P with the property $F \vdash \varphi_P$ if and only if $\mathcal{F}(P) \leq F$, for any frame F. In other words, φ_P is a condition that can be used to test if the environment is exactly the frame of P. If the terms M_a and conditions φ_P are not available in a psi-calculus, then they must be added for the proof of the theorem to hold. The details are outlined in Appendix A. □

We here comment briefly on alternatives for the definition of weak barbed equivalence. As far as we know, previous barbed equivalences do not include the object of an action in the barb. In contrast, we include the whole label including the object. The necessity for this is illustrated by a psi-calculus where there are no assertions except $\mathbf{1}$ and no conditions, and where both k and $\mathsf{f}(k)$ are terms but not channels, and M is a channel. Consider:

$$\begin{aligned} R &= (\nu k)\overline{M}\mathsf{f}(k) + (\nu k)\overline{M}k \\ S &= (\nu k)\overline{M}\mathsf{f}(k) \end{aligned}$$

R and S are not bisimilar since S cannot simulate $R \xrightarrow{\overline{M}\,(\nu k)k} \mathbf{0}$. But if objects are not included in the barbs they are barbed bisimilar: there is no context $C[\cdot]$ such that $C[R]$ and $C[S]$ have different barbs. The only thing a context could do is interact with R or S by performing an input of kind $\underline{M}(\lambda\tilde{x})N.T$. The only input pattern that matches $(\nu k)k$ is $(\lambda x)x$ and this also matches $(\nu k)\mathsf{f}(k)$. Observe that the pattern $(\lambda\epsilon)k$ does not match $(\nu k)k$ because of the side condition $\tilde{a}\#Q$ in the COM rule.

An alternative to including objects in the barbs could be to require a condition $\mathsf{name}(x)$ that is entailed only if x is a name. In that case a parallel composition with $M(x)\,.\,\textbf{if}\ \mathsf{name}(x)\ \textbf{then}\ \ldots$ distinguishes between P and Q.

Note that input actions are not needed as barbs. Including such barbs would not change the proof of the theorem. We conjecture that the output subjects can be excluded in barbs, but removing them complicates the proof.

A consequence of Definition 16 is that the closure under static contexts recurs: after a reduction the agents are required to be barbed bisimilar and again satisfy Clause 3. In this we have followed [1]. An alternative is to close under contexts at top level, i.e., Clause 3 is omitted from the recursive definition, and barbed congruence is defined as barbed equivalence in all contexts. This is the approach in the original work on barbs [16, 19]. The proofs become quite involved and use contexts with infinite sums. This technique is not available in psi-calculi since we require all terms to have finite support.

Finally, an alternative is to close under all contexts (and not merely static contexts). Since input contexts can be used to effect a substitution on any free name, this is akin to a recurring closure under arbitrary substitutions, and would correspond to a smaller equivalence, probably similar to the hyperequivalence of [17]. Consider an example from the polyadic pi-calculus, which as explained in [3] is a psi-calculus with $\mathbf{1}$ as the only assertion. We elide unimportant objects.

$$\begin{aligned} R &= (\nu xy)\overline{a}\langle x, y\rangle\,.\,(\overline{x} \mid y) \\ S &= (\nu xy)\overline{a}\langle x, y\rangle\,.\,(\overline{x}\,.\,y + y\,.\,\overline{x}) \end{aligned}$$

R and S are weakly bisimilar. If arbitrary substitutions recur in a barbed equivalence R and S will not be barbed equivalent. To see this consider $R \mid a(xy) \longrightarrow \overline{x} \mid y$ simulated by $S \mid a(xy) \longrightarrow \overline{x}\,.\,y + y\,.\,\overline{x}$. Closure under all contexts means that $\overline{a}y \mid a(x)\,.\,(\overline{x} \mid y)$ should be barbed bisimilar to $\overline{a}y \mid a(x)\,.\,(\overline{x}\,.\,y + y\,.\,\overline{x})$, but the former can reduce twice to reach an inert state without barbs, whereas the latter after a reduction has a barb $\overline{y}$.

7 Conclusion

We have presented two definitions of weak labelled bisimulation for psi-calculi: one is simple and traditional and the other is more involved. They coincide for calculi where the weakening assumption holds, and therefore the simpler definition is preferable in those cases. In other calculi they can be different, and the more complicated definition turns out to be necessary. Algebraic properties including compositionality have been established, and the proofs are mechanized in the interactive theorem prover Isabelle.

To strengthen the motivations of the definitions we have established the connection between weak labelled bisimulation and weak barbed bisimulation. The latter gives a more intuitive understanding of the equivalence, since it is based on observations (barbs) and closure of contexts. The result that the equivalences coincide constitutes an independent confirmation of weak labelled bisimulation.

In earlier work we presented a fully abstract symbolic version of strong bisimulation for psi-calculi with weakening [15]. In order to be practically useful this result should be extended to weak bisimulation. A more ambitious project is to extend proof mechanisation in Isabelle to include barbed equivalence.

We intend to build tools for bisimulation checking in instances of psi-calculi. For this, an algorithm for deciding weak symbolic bisimulation needs to be developed and implemented; an attractive approach would be to integrate it as an oracle in Isabelle.

References

[1] M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proceedings of POPL '01*, pages 104–115. ACM, Jan. 2001.

[2] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The Spi calculus. *Journal of Information and Computation*, 148(1):1–70, 1999.

[3] J. Bengtson, M. Johansson, J. Parrow, and B. Victor. Psi-calculi: Mobile processes, nominal data, and logic. In *Proceedings of LICS 2009*, pages 39–48. IEEE, 2009.

[4] J. Bengtson and J. Parrow. Psi-calculi in Isabelle. In S. Berghofer, T. Nipkow, C. Urban, and M. Wenzel, editors, *Proc. of TPHOLs 2009*, volume 5674 of *LNCS*, pages 99–114. Springer, Aug. 2009.

[5] M. Boreale. Erratum of Proof techniques for cryptographic processes. Unpublished manuscript, Aug. 2004.

[6] M. Boreale, R. De Nicola, and R. Pugliese. Proof techniques for cryptographic processes. In *Proceedings of LICS '99*, pages 157–166. IEEE, Computer Society Press, July 1999.

[7] M. Boreale, R. De Nicola, and R. Pugliese. Proof techniques for cryptographic processes. *SIAM Journal on Computing*, 31(3):947–986, 2002.

[8] J. Borgström. *Equivalences and Calculi for Formal Verifiation of Cryptographic Protocols*. PhD thesis, EPFL, Lausanne, 2008.

[9] M. G. Buscemi and U. Montanari. CC-Pi: A constraint-based language for specifying service level agreements. In R. De Nicola, editor, *Proceedings of ESOP 2007*, volume 4421 of *LNCS*, pages 18–32. Springer, 2007.

[10] M. G. Buscemi and U. Montanari. Open bisimulation for the concurrent constraint pi-calculus. In S. Drossopoulou, editor, *Proceedings of ESOP 2008*, volume 4960 of *LNCS*, pages 254–268. Springer, 2008.

[11] J. F. Diaz, C. Rueda, and F. D. Valencia. Pi+-calculus: A calculus for concurrent processes with constraints. *CLEI Electronic Journal*, 1(2), 1998. Proceedings of CLEI'97, Valparaiso, Chile.

[12] A. S. Elkjær, M. Höhle, H. Hüttel, and K. Overgård. Towards automatic bisimilarity checking in the spi calculus. In C. S. Calude and M. J. Dinneen, editors, *Combinatorics, Computation & Logic*, volume 21(3) of *Australian Computer Science Communications*, pages 175–189. Springer, Jan. 1999.

[13] U. Frendrup, H. Hüttel, and J. Nyholm Jensen. Two notions of environment sensitive bisimilarity for spi-calculus processes. Unpublished manuscript, 2001.

[14] M. Gabbay and A. Pitts. A new approach to abstract syntax with variable binding. *Formal Aspects of Computing*, 13:341–363, 2001.

[15] M. Johansson, B. Victor, and J. Parrow. A fully abstract symbolic semantics for psi-calculi. In *Proceedings of SOS 2009*, 2009.

[16] R. Milner and D. Sangiorgi. Barbed bisimulation. In W. Kuich, editor, *Proceedings of ICALP '92*, volume 623 of *LNCS*, pages 685–695. Springer, 1992.

[17] J. Parrow and B. Victor. The fusion calculus: Expressiveness and symmetry in mobile processes. In *Proceedings of LICS '98*, pages 176–185. IEEE, Computer Society Press, July 1998.

[18] A. M. Pitts. Nominal logic, a first order theory of names and binding. *Information and Computation*, 186:165–193, 2003.

[19] D. Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis, LFCS, University of Edinburgh, 1993. CST-99-93 (also published as ECS-LFCS-93-266).

[20] L. Wischik. *Explicit Fusions: Theory and Implementation*. PhD thesis, Computer Laboratory, University of Cambridge, 2001.

A Proof of $P \dot{\approx}_b Q$ implies $P \dot{\approx} Q$

This proof uses the result that $P \dot{\approx} Q \Rightarrow P \dot{\approx}_b Q$. In particular this allows us to use the structural laws from Section 5 also for $\dot{\approx}_b$.

As mentioned in Section 6, the idea is to show $\dot{\approx}_b$ to be a weak bisimulation by constructing elaborate contexts which expose transitions. The proof requires a minimum of expressiveness for the psi-calculus in the following three ways. Firstly, it uses a set of channels written M_a, where $a \in \mathrm{n}(M_a)$, that do not occur in any agent under consideration. In other words, $\Psi \vdash M_a \leftrightarrows M_a$, and for all other terms N we have that $\Psi \not\vdash M_a \leftrightarrows N$. Secondly, it uses conditions φ_P for agents P with the property $F \vdash \varphi_P$ if and only if $\mathcal{F}(P) \leq F$, for any frame F. In other words, φ_P is a condition that can be used to test if the environment is exactly the frame of P. Thirdly, it assumes that sequences of names, $\widetilde{a}$, are among the terms. If the terms M_a and $\widetilde{a}$, and the conditions φ_P are not available in a psi-calculus, then they must be added for the proof of the theorem to hold.

We first give a few lemmas used in the main proof.

Lemma 18 (Rewrite subject)**.**

$$\begin{array}{rl} & \Psi \rhd P \xrightarrow{\overline{M}\,(\nu\widetilde{a})N} P' \\ \wedge & \mathcal{F}(P) = (\nu\widetilde{b}_P)\Psi_P \\ \wedge & \Psi\otimes\Psi_P \vdash K \leftrightarrows M \\ \wedge & \widetilde{b}_P \# \Psi, P, K, M \\ \Longrightarrow & \Psi \rhd P \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} P' \end{array}$$

The symmetric lemma where P does an input is omitted.

Proof. A straightforward induction on the length of the derivation of the transition. □

Lemma 19. $\mathcal{F}(P) \vdash \varphi \Rightarrow \mathcal{F}(P \mid \textbf{if } \varphi \textbf{ then } R) \vdash \varphi$.

Proof. Trivial since $\mathcal{F}(\textbf{if } \varphi \textbf{ then } R) = \mathbf{1}$ and $\mathcal{F}(P)\otimes\mathbf{1} = \mathcal{F}(P)$. □

Lemma 20. *If $P \mid \underline{K}(\lambda\widetilde{a})N \,.\, \overline{M_c}\, N \Longrightarrow \xrightarrow{\overline{M_c}\,(\nu\widetilde{a})N} P'$ and $c\#P, K, N$ then $P \Longrightarrow \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} P'$.*

Proof. The only way for $P|\underline{K}(\lambda\widetilde{a})N.\overline{M_c}N$ to do the output $\overline{M_c}\,(\nu\widetilde{a})N$ is to reduce over K because of the properties of M_c. In other words there exists P' such that $P \Longrightarrow P'$ and $P' \xrightarrow{\overline{L}\,(\nu\widetilde{a})N} P''$. It must be the same N as in the input pattern since otherwise the transition $\xrightarrow{\overline{M_c}\,(\nu\widetilde{a})N} P'$ would have some other object. Let $\mathcal{F}(P') = (\nu\widetilde{b}_{P'})\Psi_{P'}$, where $\widetilde{b}_{P'}\#P, L, \underline{K}(\lambda\widetilde{a})N.\overline{M_c}\, N$. The COM rule gives us that $\mathbf{1}\otimes\Psi_{P'}\otimes\mathbf{1} \vdash L \leftrightarrows K$, and by Lemma 18 we get that $P' \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} P''$. □

Lemma 21. *If $P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$ and $P \dot{\approx}_b Q$ then $Q \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$.*

Proof. $P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$ if $P \Longrightarrow P' \downarrow_{\overline{K}\,(\nu\widetilde{a})N}$. The proof is by induction on the length of the reduction sequence $P \Longrightarrow P'$. Base case follows from barbed bisimilarity, and inductive steps from reduction simulation. □

Lemma 22. *If $(\nu b)P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$ then there exists P' such that $P \Longrightarrow P'$ and $(\nu b)P' \downarrow_{\overline{K}\,(\nu\widetilde{a})N}$.*

Proof. The only way to infer a reduction from $(\nu b)P$ is via rule SCOPE. This means that every reduction from $(\nu b)P$ to the strong observation is of form $(\nu b)P'' \longrightarrow (\nu b)P'''$. So we get that there exists P' such that $(\nu b)P' \downarrow_{\overline{K}\,(\nu\widetilde{a})N}$. Rule SCOPE gives us that $P'' \longrightarrow P'''$. This gives us that $P \Longrightarrow P'$. □

Lemma 23. *If $(\nu b)P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$ then $P \Downarrow_{\overline{K}\,(\nu\widetilde{a}\setminus\{b\})N}$.*

Proof. By Lemma 22 we get that there exists P' such that $P \Longrightarrow P'$ and $(\nu b)P' \downarrow_{\overline{K}\,(\nu\widetilde{a})N}$. If $b \in \widetilde{a}$ the transition from $(\nu b)P'$ is derived by OPEN, and this rule gives us that $P' \downarrow_{\overline{K}\,(\nu\widetilde{a}\setminus\{b\})N}$. If $b \notin \widetilde{a}$ the transition is derived by SCOPE and it holds trivially that $P' \downarrow_{\overline{K}\,(\nu\widetilde{a}\setminus\{b\})N}$. Since $P \Longrightarrow P'$ and $P' \downarrow_{\overline{K}\,(\nu\widetilde{a}\setminus b)N}$ we have that $P \Downarrow_{\overline{K}\,(\nu\widetilde{a}\setminus\{b\})N}$. □

Some of the following lemmas use a special static context which we now define:

$$E_{\widetilde{a},x}[\cdot] = (\nu\widetilde{a})([\cdot] \mid \overline{M_x}\,\widetilde{a}).$$

Lemma 24. *$P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$ if and only if $E_{\widetilde{b},x}[P] \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.\underline{K}(\lambda\widetilde{a})N.\overline{M_y}\; N \Downarrow_{\overline{M_y}\,(\nu\widetilde{a}\cup\widetilde{c})N}$ where $\widetilde{c} = (\widetilde{b} \cap \mathrm{n}(N)) \setminus \widetilde{a}$ and $x, y\#P, K, \widetilde{b}$. Here $\widetilde{a} \cup \widetilde{c}$ means the sequence $\widetilde{a}$ with the names in $\widetilde{c}$ inserted anywhere.*

Proof. For the ($\Rightarrow$)-direction, expand the definitions and follow the transitions. For the ($\Leftarrow$)-direction, we know that since $E_{\widetilde{b},x}[P] \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.\underline{K}(\lambda\widetilde{a})N.\overline{M_y}\, N \Downarrow_{\overline{M_y}\,(\nu\widetilde{a}\cup\widetilde{c})N}$ this agent must reduce over both M_x and K. Following the reduction over M_x we get to $(\nu\widetilde{b})(P \mid \underline{K}(\lambda\widetilde{a})N.\overline{M_y}\; N)$. Lemma 23 gives us that $P \mid \underline{K}(\lambda\widetilde{a})N.\overline{M_y}\; N \Downarrow_{\overline{M_y}\,(\nu\widetilde{a})N}$. By Lemma 20 we then get that $P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$. □

Lemma 25. *$P \dot{\approx}_b Q$ if and only if $E_{\widetilde{b},x}[P] \dot{\approx}_b E_{\widetilde{b},x}[Q]$ where $x\#P, Q, \widetilde{b}$.*

Proof. The ($\Rightarrow$)-direction follows directly by definition since the relation is closed under static contexts. For the ($\Leftarrow$)-direction we show that $P \dot{\approx}_b Q$ as follows:

1. Same barbs: Assume that $P \downarrow_{\overline{K}\,(\nu\widetilde{a})N}$. This implies that $P \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$. By Lemma 24 we get that

$E_{\widetilde{b},x}[P] \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.\underline{K}(\lambda\widetilde{a})N.\overline{M_y}\ N \Downarrow_{\overline{M_y}\,(\nu\widetilde{a}\cup\widetilde{c})N}$, where $\widetilde{c} = (\widetilde{b} \cap \mathrm{n}(N)) \setminus \widetilde{a}$. Since $E_{\widetilde{b},x}[P] \dot{\approx}_b E_{\widetilde{b},x}[Q]$ we get that also $E_{\widetilde{b},x}[P] | \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.\underline{K}(\lambda\widetilde{a})N.\overline{M_y}N \dot{\approx}_b E_{\widetilde{b},x}[Q] \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.\underline{K}(\lambda\widetilde{a})N.\overline{M_y}\ N$ (the relation is closed under all static contexts). By Lemma 21 we then get that $E_{\widetilde{b},x}[Q] \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.\underline{K}(\lambda\widetilde{a})N.\overline{M_y}\ N \Downarrow_{\overline{M_y}\,(\nu\widetilde{a}\cup\widetilde{c})N}$ and by Lemma 24 we get that $Q \Downarrow_{\overline{K}\,(\nu\widetilde{a})N}$.

2. Reduction simulation: This follows directly since the reductions of P and $E_{\widetilde{b},x}[P]$ coincide.

3. Closed under static contexts: We must show that $C[P] \dot{\approx}_b C[Q]$ for all contexts of form $(\nu\widetilde{c})([\cdot] \mid R)$. If we can show that $E_{\widetilde{b},y}[C[P]] \dot{\approx}_b E_{\widetilde{b},y}[C[Q]]$ we are done. We show this by finding a context $C'[\cdot]$ such that $C'[E_{\widetilde{b},x}[P]] \dot{\approx}_b E_{\widetilde{b},y}[C[P]]$. By transitivity we then get the desired result. The context to use is

$$C'[\cdot] = (\nu\widetilde{c})([\cdot] \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.(\overline{M_y}\,\widetilde{b} \mid R))$$

Putting $E_{\widetilde{b},x}[P]$ in the hole this becomes

$$C'[E_{\widetilde{b},x}[P]] = (\nu\widetilde{c})((\nu\widetilde{b})(\overline{M_x}\,\widetilde{b} \mid P) \mid \underline{M_x}(\lambda\widetilde{b})\widetilde{b}.(\overline{M_y}\,\widetilde{b} \mid R))$$

After one reduction this becomes

$$(\nu\widetilde{c})(\nu\widetilde{b})(P \mid \overline{M_y}\,\widetilde{b} \mid R)$$

which is equivalent to

$$E_{\widetilde{b},y}[C[P]] = (\nu\widetilde{b})(\overline{M_y}\,\widetilde{b} \mid (\nu\widetilde{c})(P \mid R))$$

by Theorem 11.

□

Lemma 26. *If* $(\nu b)P \implies (\nu b)P'$ *then* $P \implies P'$.

Proof. The only way to infer a reduction from $(\nu b)P$ is via rule SCOPE. This means that every reduction from $(\nu b)P$ to $(\nu b)P'$ is of form $(\nu b)P'' \longrightarrow (\nu b)P'''$. Rule SCOPE gives us that $P'' \longrightarrow P'''$ for each such reduction. This gives us that $P \implies P'$. □

Lemma 27. *If* $(\nu\widetilde{a})(P \mid \overline{M_c}\,\widetilde{a}) \implies (\nu\widetilde{a})(P' \mid \overline{M_c}\,\widetilde{a})$ *and* $c\#P$ *then* $P \implies P'$.

Proof. By repeatedly applying Lemma 26 we get that $P \mid \overline{M_c}\,\widetilde{a} \implies P' \mid \overline{M_c}\,\widetilde{a}$. Since $c\#P$ no communication between P and the agent $\overline{M_c}\widetilde{a}$ is possible, so each reduction $P'' \mid \overline{M_c}\,\widetilde{a} \longrightarrow P''' \mid \overline{M_c}\,\widetilde{a}$ in the reduction sequence must have been derived with PAR. Since $\mathcal{F}(\overline{M_c}\,\widetilde{a}) = \mathbf{1}$ this gives us that $P'' \longrightarrow P'''$. This gives us that $P \implies P'$. □

For the main proof it is easier to work with a slight variant of the definition of weak bisimulation:

Definition 28 (Weak context bisimulation)**.** *A* weak context bisimulation $\mathcal{R}$ *is a binary relation between pairs of agents such that* $\mathcal{R}(P,Q)$ *implies all of*

1. *Weak static implication:*
$$\forall\Psi\exists Q', Q'.\ Q \implies Q' \ \wedge\ P \le Q' \ \wedge\ Q' \mid (\!|\Psi|\!) \implies Q' \mid (\!|\Psi|\!) \ \wedge\ \mathcal{R}(P \mid (\!|\Psi|\!), Q' \mid (\!|\Psi|\!))$$
2. *Symmetry:* $\mathcal{R}(Q,P)$
3. *Extension of arbitrary assertion:* $\forall\Psi.\ \mathcal{R}(P \mid (\!|\Psi|\!), Q \mid (\!|\Psi|\!))$
4. *Weak simulation: for all* α, P' *such that* $\mathrm{bn}(\alpha)\#Q$ *and* $P \xrightarrow{\alpha} P'$ *it holds*
   (a) *if* $\alpha = \tau$:
   $$\exists Q'.\ Q \implies Q' \ \wedge\ \mathcal{R}(P', Q')$$
   (b) *if* $\alpha \neq \tau$: $\forall\Psi\exists Q'', Q'''$.
   $$Q \implies Q''' \ \wedge\ P \le Q''' \ \wedge\ Q''' \xrightarrow{\alpha} Q'' \ \wedge\ \exists Q'.\ Q'' \mid (\!|\Psi|\!) \implies Q' \mid (\!|\Psi|\!) \ \wedge\ \mathcal{R}(P' \mid (\!|\Psi|\!), Q' \mid (\!|\Psi|\!))$$

We define $P \dot{\approx}' Q$ *to mean that there exists a weak context bisimulation* $\mathcal{R}$ *such that* $\mathcal{R}(P,Q)$.

Lemma 29.
$\Psi \rhd P \xrightarrow{\alpha} P' \wedge \mathrm{bn}(\alpha)\#\Psi$ *iff* $P \mid (\!|\Psi|\!) \xrightarrow{\alpha} P' \mid (\!|\Psi|\!)$

Proof. The ($\Rightarrow$) direction follows directly from rule PAR. For the ($\Leftarrow$) direction we observe that the transition must be derived with rule PAR (an assertion has no transitions), and this rule gives us that $\Psi \rhd P \xrightarrow{\alpha} P' \wedge \mathrm{bn}(\alpha)\#\Psi$. □

Lemma 30. $P \le_\Psi Q$ *iff* $P \mid (\!|\Psi|\!) \le Q \mid (\!|\Psi|\!)$

Proof. Follows from the definition of $\mathcal{F}(P)$ and the definitions of $\le_\Psi$ and $\le$. □

Lemma 31. $P \dot{\approx}' Q$ *if and only if* $P \dot{\approx} Q$.

Proof. Construct the relations $\mathcal{R} = \{(\Psi, P, Q) : P|(\!|\Psi|\!) \dot{\approx}' Q \mid (\!|\Psi|\!)\}$ and $\mathcal{R}' = \{(P \mid (\!|\Psi|\!), Q \mid (\!|\Psi|\!)) : P \dot{\approx}_\Psi Q\}$ and show that they are weak and weak context bisimulations, respectively. The proof uses Lemmas 29 and 30. □

We now turn our attention to the main proof. We use the candidate relation $\mathcal{R}_l = \{(P,Q) : P \dot{\approx}_b Q\}$ and show it to be a weak context bisimulation. We must show that all clauses in Definition 28 follow from Definition 16. These clauses are Weak static implication, Symmetry, Extension of arbitrary assertion, and Weak simulation.

Weak static implication We have that $\mathcal{F}(P) \vdash \varphi_P$ by definition. Let Ψ' be an arbitrary assertion, and let $R = \overline{M_b} \mid \textbf{if } \varphi_P \textbf{ then } \tau\,.\,(\Psi' \mid \underline{M_b})$. Since $P \dot{\approx}_b Q$ we also have that $P \mid R \dot{\approx}_b Q \mid R$. Here $P \mid R$ can reduce twice:

$$P \mid R \longrightarrow\!\!\!\!\!\!\rightarrow P \mid \Psi'$$

Since $P \mid \Psi' \not\downarrow_{\overline{M_b}}$ and $P \mid R \dot{\approx}_b Q \mid R$ we know that there exists T such that $Q \mid R \implies T, T \not\downarrow_{\overline{M_b}}$, and $P \mid \Psi' \dot{\approx}_b T$, or in other words, there exists Q'' and Q' such that

$$\begin{aligned} Q \mid R &\implies Q'' \mid \overline{M_b} \mid \textbf{if } \varphi_P \textbf{ then } \tau\,.\,(\Psi' \mid \underline{M_b}) \\ &\longrightarrow Q'' \mid \overline{M_b} \mid \Psi' \mid \underline{M_b} \\ &\longrightarrow Q'' \mid \Psi' \\ &\implies Q' \mid \Psi' \end{aligned}$$

and $P \mid \Psi' \dot{\approx}_b Q' \mid \Psi'$. In other words, $\forall \Psi' \exists Q'', Q'.Q \implies Q'', P \leq Q'', Q'' \mid \Psi' \implies Q' \mid \Psi'$, and $P \mid \Psi' \dot{\approx} Q' \mid \Psi'$.

Symmetry Follows immediately since Definition 16 is symmetric.

Extension of arbitrary assertion Follows immediately since Definition 16 is closed under all evaluation contexts after each step.

Weak simulation

Case $P \xrightarrow{\tau} P'$**:** Follows immediately from Definition 16.

Case $P \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} P'$**:** We have that $\mathcal{F}(P) \vdash \varphi_P$ by definition. From Definition 16 clause 3 we get that for all static contexts $C[\cdot]$, $C[P] \dot{\approx}_b C[Q]$. Let Ψ' be an arbitrary assertion and let $R = \textbf{case } \varphi_P : \underline{K}(\lambda\widetilde{a})N.(\langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a})$, where $c\#P, Q, K, N, \widetilde{a}, \Psi'$. In particular we then have that

$$P \mid R \dot{\approx}_b Q \mid R.$$

Trivially we have that $\mathcal{F}(P) \vdash \varphi_P$ and by Lemma 19 we also have that

$$\mathcal{F}(P \mid R) \vdash \varphi_P.$$

This agent has the reduction

$$P \mid R \longrightarrow (\nu\widetilde{a})(P' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a}).$$

By Clause 2 in Definition 16 we know that $Q \mid R$ can weakly simulate this reduction. Since $(\nu\widetilde{a})(P' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a}) \downarrow_{\overline{M_c}\,(\nu\widetilde{a})\widetilde{a}}$ this simulating reduction must reduce to something that also has the barb $\overline{M_c}\,(\nu\widetilde{a})\widetilde{a}$. Since M_c does not occur in Q and is not channel equivalent to anything else, all reductions that lead to an agent with the barb M_c must reduce over K: $\exists Q''', Q''$ such that $Q \mid R \implies Q''' \mid R \longrightarrow (\nu\widetilde{a})(Q'' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a})$ (since the term M_c cannot occur in Q this also gives us that $Q \implies Q'''$). The derivation of the last reduction is:

$$\textsc{Com}\ \frac{\begin{array}{c}\mathbf{1}\otimes\Psi_{Q'''}\otimes\mathbf{1} \vdash L \leftrightarrow K \\ \mathbf{1}\otimes\mathbf{1} \rhd Q''' \xrightarrow{\overline{L}\,(\nu\widetilde{a})N} Q'' \\ \Psi_{Q'''}\otimes\mathbf{1} \rhd R \xrightarrow{\underline{K}\,N} \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a}\end{array}}{\mathbf{1} \rhd Q''' \mid R \xrightarrow{\tau} (\nu\widetilde{a})(Q'' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a})}\ \widetilde{a}\#Q$$

We here assume that $\mathcal{F}(Q''') = (\nu\widetilde{b}_{Q'''})\Psi_{Q'''}$ such that $\widetilde{b}_{Q'''}\#K, L, Q''', R$. By Lemma 18 we learn that $\mathbf{1}\otimes\mathbf{1} \rhd Q''' \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} Q''$, where the object must be $(\nu\widetilde{a})N$ since otherwise we would not have that $(\nu\widetilde{a})(Q'' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a}) \downarrow_{\overline{M_c}\,(\nu\widetilde{a})\widetilde{a}}$. We get that $\Psi_{Q'''} \vdash \varphi_P$ since otherwise R's transition would not be possible, and since $\widetilde{b}_{Q'''}\#R$ also that $\mathcal{F}(Q''') \vdash \varphi_P$. We know that $\exists Q'$ such that $(\nu\widetilde{a})(Q'' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a}) \implies (\nu\widetilde{a})(Q' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a})$ and $(\nu\widetilde{a})(P' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a}) \dot{\approx}_b (\nu\widetilde{a})(Q' \mid \langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,\widetilde{a})$.

We now turn to see how the requirements of Clause 4b in Definition 28 follow from this. We have that $P \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} P'$. Since Ψ' was arbitrarily chosen we have that $\forall \Psi' \exists Q''', Q''$ such that $Q \implies Q'''$. We also have that $\mathcal{F}(P) \vdash \varphi_P$ and $\mathcal{F}(Q''') \vdash \varphi_P$, or in other words that $P \leq Q'''$. From above we also have that $Q''' \xrightarrow{\overline{K}\,(\nu\widetilde{a})N} Q''$, and that $Q'' \mid \langle\!|\Psi'|\!\rangle \implies Q' \mid \langle\!|\Psi'|\!\rangle$ (using Lemma 27 to get rid of $\overline{M_c}\widetilde{a}$ and the restriction), and that $P' \mid \langle\!|\Psi'|\!\rangle \dot{\approx}_b Q' \mid \langle\!|\Psi'|\!\rangle$ (using Lemma 25). Finally, because of the construction of the candidate relation we have that $\mathcal{R}_l(P' \mid \langle\!|\Psi'|\!\rangle, Q' \mid \langle\!|\Psi'|\!\rangle)$.

Case $P \xrightarrow{\underline{K}\,N} P'$**:** This proof is very similar to the one for bound output, but we use the context

$$C[\cdot] = [\cdot] \mid \textbf{case } \varphi_P : \overline{K}\,N.(\langle\!|\Psi'|\!\rangle \mid \overline{M_c}\,)$$

instead. This means that there are no restrictions on the derivative of the reduction of $C[P]$, which gives us a slightly simpler problem. Apart from this the proof is the same.

□