Probabilistic Barbed Congruence

Yuxin Deng [a], Wenjie Du [b]

[a] *Shanghai Jiao Tong University, China*
yuxindeng@sjtu.edu.cn

[b] *Shanghai Normal University, China*
wenjiedu@shnu.edu.cn

Abstract

This paper defines a *probabilistic barbed congruence* which turns out to coincide with observational equivalence in a probabilistic extension of CCS. Based on this coincidence result, we provide a sound and complete axiomatisation for the barbed congruence in a finite fragment of probabilistic CCS.

Key words: Probabilistic process calculus, Barbed congruence, Observational equivalence, Axiomatisation.

1 Introduction

Nowadays process algebras have become an important model to reason about concurrent computations. To describe the operational behaviour of a process, one can usually define two types of semantics: The *transition semantics* is given by defining appropriate equivalences (e.g. observational equivalence) based on a *labelled* transition system, while the *reduction semantics* is given by defining appropriate equivalences (e.g. barbed bisimulation) based on an *unlabelled* transition system. Reduction semantics is simpler but in some cases more enlightening than transition semantics, especially when one wants to compare two calculi which syntactically may be quite far from each other. Barbed bisimulation [14] was proposed by Milner and Sangiorgi as a tool to describe uniformly bisimulation-based equivalences which can be used in many different calculi. The idea is to equip a global observer with a minimal ability to observe actions and process states. However, barbed bisimulation is a very weak relation and it often fails to be a congruence. An easy way of inducing a congruence from barbed bisimulation is to require two processes to be barbed bisimilar under all contexts. The congruence thus obtained is called *barbed congruence*, which has the disadvantage of being difficult to use because of the quantification over all contexts.

Sangiorgi has shown in [15, Theorem 3.3.2] that weak bisimulation coincides with barbed congruence in a variant of CCS [13] with a guarded sum.

This paper is electronically published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

This characterisation result is significant because it allows us to use the coinductive proof technique offered by weak bisimulation to establish the equivalence of two processes under barbed congruence, and we do not need to consider all contexts any more.

In this paper we extend Sangiorgi's result to the probabilistic setting. More precisely, we define observational equivalence and barbed congruence in a probabilistic extension of Milner's CCS, then we show that the two equivalences coincide in this probabilistic CCS. In addition, we provide a sound and complete axiomatisation for observational equivalence in a finite fragment of the probabilistic CCS. Thanks to the above coincidence result, the axiomatisation is also sound and complete for barbed congruence.

Observational equivalence was already studied in various probabilistic process algebras [6,7,8]. However, the definitions of observational equivalence in [6,7,8] require a notion of *combined weak transitions* [17], which are formed by linear combinations of our familiar basic weak transitions. In this paper, we adopt the notion of weak transitions defined in [9], which is obtained by lifting a relation between states and distributions of states to one between distributions and distributions. Since the weak transitions of [9] have a built-in linear combination, it turns out to be equivalent to the combined weak transitions of [17]. However, the former is cleaner and more elegant than the latter because it constructs weak transitions from strong transitions simply by inserting some invisible transitions, as in the nonprobabilistic setting [13]. We no longer have to define complicated weak transition rules as in [6,7,8].

Although it is easy to show that observational equivalence is included in barbed congruence, the opposite inclusion is nontrivial. We need to build a class of contexts powerful enough to guarantee that barbed bisimulation on these contexts implies observational equivalence. The proof schema is similar to that in [15], but our construction of contexts is somewhat simpler though we are in the probabilistic setting.

The completeness proof of our axiomatisation uses the same idea as the related proof in [7]: we exploit a Promotion Lemma (Lemma 5.6) as our stepping stone to show that the axiomatisation is complete w.r.t. observational equivalence (Theorem 5.7). Although more operators such as parallel composition are considered in this paper than in [6,7], they are not difficult to deal with in axiomatisation. For example, we use a probabilistic version of the expansion law to eliminate all occurrences of parallel composition.

There is a lot of other related work about axiomatisations of probabilistic equivalences [10,4,2,18,1,3]. However, most of them is about axiomatizing probabilistic strong bisimilarity, so the interesting and subtle issue about weak transitions does not arise. Amongst those work about weak equivalences (e.g. branching bisimulation), to the best of our knowledge, none of them deals with barbed congruence.

The rest of the paper is structured as follows. In Section 2, we present the syntax and operational semantics of a probabilistic version of CCS. Next, we

define observational equivalence and show that it is a congruence in Section 3. We define barbed congruence and prove its coincidence with observational equivalence in Section 4. We provide a sound and complete axiomatisation in Section 5, restricted to a finite fragment of our calculus. Finally, we conclude in Section 6.

2 Probabilistic CCS

In this section we give a probabilistic extension of CCS [13] that allows for non-deterministic and probabilistic choice. It is similar to the calculi studied in [5,11]. We assume a countable set of atomic actions, $\mathcal{A} = \{a, b, ...\}$. Given a special action τ not in $\mathcal{A}$, we let $u, v, ...$ range over the set of *actions*, $Act = \mathcal{A} \cup \overline{\mathcal{A}} \cup \{\tau\}$, where $\overline{\mathcal{A}} = \{\bar{a} \mid a \in \mathcal{A}\}$. The class of processes $\mathcal{P}$ is defined by the following syntax:

$$P ::= u.\bigoplus_{i\in I} p_i P_i \;\Big|\; \sum_{i\in I} P_i \;\Big|\; P_1 \mid P_2 \;\Big|\; P\backslash A \;\Big|\; P[f] \;\Big|\; C\langle\widetilde{x}\rangle$$

where $A \subseteq \mathcal{A}$ and $f : Act \to Act$ is a renaming function. Here $\bigoplus_{i\in I} p_i P_i$ stands for a *probabilistic choice* operator, where the p_i's represent positive probabilities, i.e., they satisfy $p_i \in (0, 1]$ and $\sum_{i\in I} p_i = 1$. Sometimes we are interested in certain branches of the probabilistic choice; in this case we write $\bigoplus_{i\in 1..n} p_i P_i$ as $p_1 P_1 \oplus ... \oplus p_n P_n$ or $(\bigoplus_{i\in 1..(n-1)} p_i P_i) \oplus p_n P_n$ where $\bigoplus_{i\in 1..(n-1)} p_i P_i$ abbreviates (with a slight abuse of notation) $p_1 P_1 \oplus ... \oplus p_{n-1} P_{n-1}$. The second construction $\sum_{i\in I} P_i$ stands for a *nondeterministic choice*, and occasionally we may write $\sum_{i\in 1..m} P_i$ as $P_1 + ... + P_m$. When $m = 0$ we abbreviate the nondeterministic choice as $\mathbf{0}$; when $m = 1$ we abbreviate it as P_1. We also abbreviate $u.\mathbf{0}$ as u. We use $\mid$ to denote the usual *parallel composition*. The *restriction* and *renaming* operators are as in CCS: $P\backslash A$ behaves like P as long as P does not perform an action $a \in A$; $P[f]$ behaves like P where each action $a \in Act$ is replaced by $f(a)$. A constant C has a definition $C \stackrel{\text{def}}{=} (\widetilde{x})P$, where $P \in \mathcal{P}$ and the parameters $\widetilde{x}$ collect all action names which may occur in P. The intuition is that $C\langle\widetilde{y}\rangle$ behaves as P with $\widetilde{y}$ replacing $\widetilde{x}$. For simplicity, sometimes we shall put in the parameters $\widetilde{x}$ only those action names of P which are supposed to be instantiated.

Before giving the operational semantics of processes we need to introduce some notation about *probability distributions*. A (discrete) probability distribution over a set S is a mapping $\Delta : S \to [0, 1]$ with $\sum_{s\in S} \Delta(s) = 1$. The *support* of Δ is given by $\lceil\Delta\rceil := \{\, s \in S \mid \Delta(s) > 0 \,\}$. Let $\mathcal{D}(S)$, ranged over by Δ, Θ, Φ, denote the collection of all such distributions over S. We use $\overline{s}$ to denote the point distribution assigning probability 1 to state s and 0 to all others, so that $\lceil\overline{s}\rceil = \{s\}$. If $p_i \geq 0$ and Δ_i is a distribution for each i in some finite index set I, then $\sum_{i\in I} p_i \cdot \Delta_i$ is a distribution given by

$$(\sum_{i\in I} p_i \cdot \Delta_i)(s) \quad = \quad \sum_{i\in I} p_i \cdot \Delta_i(s) \tag{1}$$

where $\sum_{i\in I} p_i = 1$. We will sometimes write it as $p_1 \cdot \Delta_1 + \ldots + p_n \cdot \Delta_n$ when the index set I is $\{1, \ldots, n\}$.

Some operations on processes can be extended to distributions of processes straightforwardly. Let Δ_1, Δ_2 be two distributions on processes. We define $\Delta_1 \mid \Delta_2$, $\Delta_1\backslash A$ and $\Delta_1[f]$ as the following distributions.

$$(\Delta_1 \mid \Delta_2)(P) \stackrel{\text{def}}{=} \begin{cases} \Delta_1(P_1) \cdot \Delta_2(P_2) & \text{if } P = P_1 \mid P_2 \\ \mathbf{0} & \text{otherwise} \end{cases}$$

$$(\Delta_1\backslash A)(P) \stackrel{\text{def}}{=} \begin{cases} \Delta_1(P') & \text{if } P = P'\backslash A \\ \mathbf{0} & \text{otherwise} \end{cases}$$

$$(\Delta_1[f])(P) \stackrel{\text{def}}{=} \begin{cases} \Delta_1(P') & \text{if } P = P'[f] \\ \mathbf{0} & \text{otherwise} \end{cases}$$

The operational semantics of a process P is defined as a simple probabilistic automaton [16] whose states are the processes reachable from P and the transition relation is defined by the rules in Table 1, where $P \xrightarrow{u} \Delta$ describes a transition that, by performing an action u, leaves from P and leads to a distribution $\Delta \in \mathcal{D}(\mathcal{P})$. The meaning of the rules should be self-explanatory.

The presence of both probabilistic and non-deterministic choice in the probabilistic CCS allows us to specify systems that have both probabilistic and non-deterministic behaviour.

3 Observational equivalence

In the probabilistic setting, the definitions of bisimulation-like equivalences are somewhat complicated by the fact that transitions go from processes to distributions (see e.g. [12]). So we need to generalise relations between processes to relations between distributions. Inspired by [9], we develop the mathematical machinery below for doing this.

Let $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ be a relation from processes to processes. We lift it to a relation $\overline{\mathcal{R}} \subseteq \mathcal{D}(\mathcal{P}) \times \mathcal{D}(\mathcal{P})$ by letting $\Delta\ \overline{\mathcal{R}}\ \Theta$ whenever

(i) $\Delta = \sum_{i\in I} p_i \cdot \overline{P_i}$, where I is a finite index set and $\sum_{i\in I} p_i = 1$

(ii) For each $i \in I$ there is a process Q_i such that $P_i \mathcal{R} Q_i$

(iii) $\Theta = \sum_{i\in I} p_i \cdot \overline{Q_i}$.

An important point here is that in the decomposition (i) of Δ into $\sum_{i\in I} p_i \cdot \overline{P_i}$, the processes P_i are *not necessarily distinct*: that is, the decomposition is not in general unique.

The lifting construction satisfies the following useful properties.

Lemma 3.1 (i) *If $\mathcal{R}_1 \subseteq \mathcal{R}_2$ then $\overline{\mathcal{R}_1} \subseteq \overline{\mathcal{R}_2}$*

(ii) *If $\mathcal{R}$ is a transitive relation, then so is $\overline{\mathcal{R}}$.* □

$$u.\bigoplus_{i\in I} p_i P_i \xrightarrow{u} \Delta \text{ where } \Delta(P) = \sum\{p_i \mid i \in I, P_i = P\}$$

$$\frac{P_i \xrightarrow{u} \Delta}{\sum_{i\in I} P_i \xrightarrow{u} \Delta} \text{ for some } i \in I$$

$$\frac{P_1 \xrightarrow{u} \Delta_1}{P_1 \mid P_2 \xrightarrow{u} \Delta_1 \mid \overline{P_2}} \qquad \frac{P_2 \xrightarrow{u} \Delta_2}{P_1 \mid P_2 \xrightarrow{u} \overline{P_1} \mid \Delta_2}$$

$$\frac{P_1 \xrightarrow{a} \Delta_1 \quad P_2 \xrightarrow{\bar{a}} \Delta_2}{P_1 \mid P_2 \xrightarrow{\tau} \Delta_1 \mid \Delta_2} \qquad \frac{P_1 \xrightarrow{\bar{a}} \Delta_1 \quad P_2 \xrightarrow{a} \Delta_2}{P_1 \mid P_2 \xrightarrow{\tau} \Delta_1 \mid \Delta_2}$$

$$\frac{P \xrightarrow{u} \Delta_1 \quad u \notin A \cup \overline{A}}{P\backslash A \xrightarrow{u} \Delta_1\backslash A} \qquad \frac{P \xrightarrow{v} \Delta_1 \quad f(v) = u}{P[f] \xrightarrow{u} \Delta_1[f]}$$

$$\frac{C \stackrel{\text{def}}{=} (\widetilde{x})P \quad P\{\widetilde{y}/\widetilde{x}\} \xrightarrow{u} \Delta}{C\langle\widetilde{y}\rangle \xrightarrow{u} \Delta}$$

Table 1
Operational semantics

Proof. See Appendix A. □

The following proposition is inherited from Proposition 6.1 of [9].

Proposition 3.2 Suppose $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ and $\sum_{i\in I} p_i = 1$. Then we have

(i) $\Theta_i \; \overline{\mathcal{R}} \; \Delta_i$ implies $(\sum_{i\in I} p_i \cdot \Theta_i) \; \overline{\mathcal{R}} \; (\sum_{i\in I} p_i \cdot \Delta_i)$.

(ii) If $(\sum_{i\in I} p_i \cdot \Theta_i) \; \overline{\mathcal{R}} \; \Delta$ then $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$ for some set of distributions Δ_i such that $\Theta_i \; \overline{\mathcal{R}} \; \Delta_i$. □

We write $P \xrightarrow{\hat{\tau}} \Delta$ if either $P \xrightarrow{\tau} \Delta$ or $\Delta = \overline{P}$. We write $P \xrightarrow{\hat{u}} \Delta$ for $P \xrightarrow{u} \Delta$ if $u \neq \tau$. To define *weak transitions* we need to consider sequences of transitions, so we generalise transitions in such a way that they go from distributions to distributions. Let $\Delta \xrightarrow{\hat{u}} \Theta$ whenever

(i) $\Delta = \sum_{i\in I} p_i \cdot \overline{P_i}$, where I is a finite index set and $\sum_{i\in I} p_i = 1$

(ii) For each $i \in I$ there is a distribution Θ_i such that $P_i \xrightarrow{\hat{u}} \Theta_i$

(iii) $\Theta = \sum_{i\in I} p_i \cdot \Theta_i$.

Weak transitions are defined in the standard manner except that they now apply to distributions, and $\xrightarrow{\hat{\tau}}$ is used instead of $\xrightarrow{\tau}$. This reflects the intuition that if a distribution may perform a sequence of invisible moves before or after executing a visible action, different parts of the distribution

may perform different numbers of internal actions.

- Let $\Delta_1 \stackrel{\hat{\tau}}{\Longrightarrow} \Delta_2$ whenever $\Delta_1 (\stackrel{\hat{\tau}}{\longrightarrow})^* \Delta_2$.
- Let $\Delta_1 \stackrel{u}{\Longrightarrow} \Delta_2$ denote $\Delta_1 \stackrel{\hat{\tau}}{\Longrightarrow} \stackrel{u}{\longrightarrow} \stackrel{\hat{\tau}}{\Longrightarrow} \Delta_2$.

If $u \neq \tau$ we also write $\Delta_1 \stackrel{\hat{u}}{\Longrightarrow} \Delta_2$ for $\Delta_1 \stackrel{u}{\Longrightarrow} \Delta_2$.

Definition 3.3 An equivalence relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is a *(weak) bisimulation* if $P \mathcal{R} Q$ and $P \stackrel{u}{\longrightarrow} \Delta$ implies $Q \stackrel{\hat{u}}{\Longrightarrow} \Theta$ such that $\Delta \overline{\mathcal{R}} \Theta$.

Two processes P and Q are *bisimilar*, written $P \approx_w Q$, if there exists a bisimulation $\mathcal{R}$ s.t. $P \mathcal{R} Q$.

To see that $\approx_w$ is the biggest bisimulation, we need to establish some properties of bisimulations.

Lemma 3.4 Suppose $\sum_{i \in I} p_i = 1$ and $\Delta_i \stackrel{\hat{u}}{\Longrightarrow} \Phi_i$ for each $i \in I$, with I a finite index set. (Recall that $\sum_{i \in I} p_i \cdot \Delta_i$ is only defined for finite I.) Then

$$\sum_{i \in I} p_i \cdot \Delta_i \stackrel{\hat{u}}{\Longrightarrow} \sum_{i \in I} p_i \cdot \Phi_i$$

□

Proof. We first prove the case $u = \tau$. For each $i \in I$ there is a number k_i such that $\Delta_i = \Delta_{i0} \stackrel{\hat{\tau}}{\longrightarrow} \Delta_{i1} \stackrel{\hat{\tau}}{\longrightarrow} \Delta_{i2} \stackrel{\hat{\tau}}{\longrightarrow} \cdots \stackrel{\hat{\tau}}{\longrightarrow} \Delta_{ik_i} = \Phi_i$. Let $k = \max\{k_i \mid i \in I\}$, using that I is finite. Since we have $\Phi \stackrel{\hat{\tau}}{\longrightarrow} \Phi$ for any $\Phi \in \mathcal{D}(\mathcal{P})$, we can add spurious transitions to these sequences, until all k_i equal k. After this preparation the lemma follows by k applications of lifting transitions.

The case $u \neq \tau$ now follows by one more application of lifting transitions on $\stackrel{u}{\longrightarrow}$, preceded and followed by an application of the case $u = \tau$. □

Lemma 3.5 Let $\mathcal{R}$ be a bisimulation. Suppose $\Delta \overline{\mathcal{R}} \Phi$ and $\Delta \stackrel{u}{\longrightarrow} \Delta'$. Then $\Phi \stackrel{\hat{u}}{\Longrightarrow} \Phi'$ for some Φ' such that $\Delta' \overline{\mathcal{R}} \Phi'$.

Proof. First $\Delta \overline{\mathcal{R}} \Phi$ means that

$$\Delta = \sum_{i \in I} p_i \cdot \overline{P_i}, \qquad P_i \mathcal{R} R_i, \qquad \Phi = \sum_{i \in I} p_i \cdot \overline{R_i} \; ; \tag{2}$$

also $\Delta \stackrel{u}{\longrightarrow} \Delta'$ means

$$\Delta = \sum_{j \in J} q_j \cdot \overline{Q_j}, \qquad Q_j \stackrel{u}{\longrightarrow} \Theta_j, \qquad \Delta' = \sum_{j \in J} q_j \cdot \Theta_j \; , \tag{3}$$

and we can assume *w.l.o.g.* that all the coefficients p_i, q_j are non-zero. Now define $I_j = \{\, i \in I \mid P_i = Q_j \,\}$ and $J_i = \{\, j \in J \mid Q_j = P_i \,\}$, so that trivially

$$\{(i,j) \mid i \in I,\ j \in J_i\} \quad = \quad \{(i,j) \mid j \in J,\ i \in I_j\} \tag{4}$$

and note that

$$\Delta(P_i) = \sum_{j \in J_i} q_j \qquad \text{and} \qquad \Delta(Q_j) = \sum_{i \in I_j} p_i \tag{5}$$

Because of (5) we have

$$\begin{aligned}\Phi = \sum_{i\in I} p_i \cdot \overline{R_i} &= \sum_{i\in I} p_i \cdot \sum_{j\in J_i} \tfrac{q_j}{\Delta(P_i)} \cdot \overline{R_i} \\ &= \sum_{i\in I} \sum_{j\in J_i} \tfrac{p_i\cdot q_j}{\Delta(P_i)} \cdot \overline{R_i}\end{aligned}$$

Now for each j in J_i we know that in fact $Q_j = P_i$, and so from the middle parts of (2) and (3) we obtain $R_i \stackrel{\hat{u}}{\Longrightarrow} \Phi'_{ij}$ such that $\Theta_j \ \overline{\mathcal{R}}\ \Phi'_{ij}$. Lemma 3.4 yields

$$\Phi \stackrel{\hat{u}}{\Longrightarrow} \Phi' = \sum_{i\in I} \sum_{j\in J_i} \tfrac{p_i\cdot q_j}{\Delta(P_i)} \cdot \Phi'_{ij}$$

where within the summations $P_i = Q_j$, so that, using (4), Φ' can also be written as

$$\sum_{j\in J} \sum_{i\in I_j} \frac{p_i \cdot q_j}{\Delta(Q_j)} \cdot \Phi'_{ij} \tag{6}$$

Below we show that $\Delta' \ \overline{\mathcal{R}}\ \Phi'$, which we do by manipulating Δ' so that it takes on a form similar to that in (6):

$$\begin{aligned}\Delta' &= \sum_{j\in J} q_j \cdot \Theta_j \\ &= \sum_{j\in J} q_j \cdot \sum_{i\in I_j} \tfrac{p_i}{\Delta(Q_j)} \cdot \Theta_j \qquad \text{using (5) again} \\ &= \sum_{j\in J} \sum_{i\in I_j} \tfrac{p_i\cdot q_j}{\Delta(Q_j)} \cdot \Theta_j\end{aligned}$$

Comparing this with (6) above we see that the required result, $\Delta' \ \overline{\mathcal{R}}\ \Phi'$, follows from an application of Proposition 3.2(i). □

Lemma 3.6 Let $\mathcal{R}$ be a bisimulation. Suppose $\Delta \ \overline{\mathcal{R}}\ \Phi$ and $\Delta \stackrel{\hat{u}}{\Longrightarrow} \Delta'$. Then $\Phi \stackrel{\hat{u}}{\Longrightarrow} \Phi'$ for some Φ' such that $\Delta' \ \overline{\mathcal{R}}\ \Phi'$.

Proof. First we consider two claims

(i) If $\Delta \ \overline{\mathcal{R}}\ \Phi$ and $\Delta \stackrel{\hat{\tau}}{\longrightarrow} \Delta'$, then $\Phi \stackrel{\hat{\tau}}{\Longrightarrow} \Phi'$ for some Φ' such that $\Delta \ \overline{\mathcal{R}}\ \Phi'$

(ii) If $\Delta \ \overline{\mathcal{R}}\ \Phi$ and $\Delta \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$, then $\Phi \stackrel{\hat{\tau}}{\Longrightarrow} \Phi'$ for some Φ' such that $\Delta' \ \overline{\mathcal{R}}\ \Phi'$.

The proof of claim (i) is similar to that of Lemma 3.5. Claim (ii) follows from claim (i) by induction on the length of the derivation of $\stackrel{\hat{\tau}}{\Longrightarrow}$. By combining claim (ii) with Lemma 3.5, we obtain the required result. □

Lemma 3.7 *Let $\mathcal{R} = \bigcup_i \{\, \mathcal{R}_i \mid \mathcal{R}_i$ is a bisimulation$\,\}$. Then the equivalence closure of $\mathcal{R}$, written $\mathcal{R}^*$, is a bisimulation.*

Proof. If $P \ \mathcal{R}^*\ Q$ then there exists some bisimulations $\mathcal{R}_0, ..., \mathcal{R}_{n-1}$ and some processes $P_0, ..., P_n$ such that $P = P_0$, $Q = P_n$, and for all i with $0 \leq i < n$, we have $P_i \ \mathcal{R}_i\ P_{i+1}$. If $P \stackrel{u}{\longrightarrow} \Delta_0$ then there exist Δ'_1 such that $P_1 \stackrel{\hat{u}}{\Longrightarrow} \Delta'_1$ with $\Delta_0 \ \overline{\mathcal{R}_0}\ \Delta'_1$. For all i with $1 \leq i < n$, by Lemma 3.6 there exist Δ'_{i+1} such that $P_{i+1} \stackrel{\hat{u}}{\Longrightarrow} \Delta'_{i+1}$ with $\Delta'_i \ \overline{\mathcal{R}_i}\ \Delta'_{i+1}$. By Lemma 3.1 it holds that $\Delta_0 \ \overline{\mathcal{R}^*}\ \Delta'_n$. □

Because of the above lemma, we can equivalently express $\approx_w$ as $\mathcal{R}^*$, which

is the biggest bisimulation. As usual, observational equivalence is defined in terms of $\approx_w$.

Definition 3.8 Two processes P, Q are *observationally equivalent*, written $P \simeq_w Q$, if

(i) whenever $P \xrightarrow{u} \Delta$, there exists Θ s.t. $Q \stackrel{u}{\Longrightarrow} \Theta$ and $\Delta \,\overline{\approx_w}\, \Theta$

(ii) whenever $Q \xrightarrow{u} \Theta$, there exists Δ s.t. $P \stackrel{u}{\Longrightarrow} \Delta$ and $\Delta \,\overline{\approx_w}\, \Theta$.

The following lemma can be used to show that $\simeq_w$ is indeed an equivalence relation.

Lemma 3.9 *If $\Delta \stackrel{\tau}{\Longrightarrow} \Delta'$ then there exists Δ'' such that $\Delta \xrightarrow{\tau} \Delta'' \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$.*

Proof. Let $\lceil \Delta \rceil = \{P_i\}_{i \in I}$ for some index set I and $\Delta(P_i) = p_i$ for each $i \in I$. We first consider the special case that

$$\Delta \xrightarrow{\hat{\tau}} \Theta \xrightarrow{\tau} \Theta' \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$$

with $\Delta \neq \Theta$ and $\Delta \not\xrightarrow{\tau} \Theta$. By definition there exists Θ_i for each $i \in I$ such that $P_i \xrightarrow{\hat{\tau}} \Theta_i$ and $\Theta = \sum_{i \in I} p_i \cdot \Theta_i$. More precisely, there is a partition of I into two sets I_1, I_2 such that

$$\forall i \in I_1 : P_i \xrightarrow{\tau} \Theta_i \text{ and } \forall i \in I_2 : \Theta_i = \overline{P_i}. \tag{7}$$

That is, $\Theta = \sum_{i \in I_1} p_i \cdot \Theta_i + \sum_{i \in I_2} p_i \cdot \overline{P_i}$. By Proposition 3.2 (ii), we know from $\Theta \xrightarrow{\tau} \Theta'$ that $\Theta' = \sum_{i \in I_1} p_i \cdot \Theta'_i + \sum_{i \in I_2} p_i \cdot \Theta'_i$ and

$$\forall i \in I_1 : \Theta_i \xrightarrow{\tau} \Theta'_i \text{ and } \forall i \in I_2 : \Theta_i \xrightarrow{\tau} \Theta'_i \tag{8}$$

for some Θ'_i ($i \in I$). It follows from (7) and (8) that

$$\begin{aligned} \Delta &\xrightarrow{\tau} \textstyle\sum_{i \in I_1} p_i \cdot \Theta_i + \sum_{i \in I_2} p_i \cdot \Theta'_i \\ &\xrightarrow{\hat{\tau}} \textstyle\sum_{i \in I_1} p_i \cdot \Theta'_i + \sum_{i \in I_2} p_i \cdot \Theta'_i \\ &= \Theta' \\ &\stackrel{\hat{\tau}}{\Longrightarrow} \Delta' \end{aligned}$$

For the general case that

$$\Delta \stackrel{\hat{\tau}}{\Longrightarrow} \Theta \xrightarrow{\tau} \Theta' \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$$

we prove by induction that $\Delta \xrightarrow{\tau} \Delta'' \stackrel{\hat{\tau}}{\Longrightarrow} \Delta'$ for some Δ'', using the result for the above special case. □

Proposition 3.10 *$\simeq_w$ is an equivalence relation.*

Proof. Reflexivity and symmetry are immediate. Using Lemmas 3.9 and 3.6, transitivity is easy to show. □

In Proposition 3.12 we show that the probabilistic CCS operators are compositional for $\simeq_w$, i.e. $\simeq_w$ is a congruence. The following lemma gathers some facts we need in the proof of this proposition. Their proofs are straightforward.

Lemma 3.11 (i) *If $P \stackrel{u}{\Longrightarrow} \Delta$ then $P + Q \stackrel{u}{\Longrightarrow} \Delta$.*

(ii) *If* $\Delta_1 \stackrel{\hat{u}}{\Longrightarrow} \Delta_1'$ *then* $\Delta_1 \mid \Delta_2 \stackrel{\hat{u}}{\Longrightarrow} \Delta_1' \mid \Delta_2$ *and* $\Delta_2 \mid \Delta_1 \stackrel{\hat{u}}{\Longrightarrow} \Delta_2 \mid \Delta_1'$.

(iii) *If* $\Delta_1 \stackrel{a}{\longrightarrow} \Delta_1'$ *and* $\Delta_2 \stackrel{\bar{a}}{\longrightarrow} \Delta_2'$ *then* $\Delta_1 \mid \Delta_2 \stackrel{\tau}{\longrightarrow} \Delta_1' \mid \Delta_2'$.

(iv) *If* $P \stackrel{u}{\Longrightarrow} \Delta$ *then* $P[f] \stackrel{f(u)}{\Longrightarrow} \Delta[f]$.

(v) *If* $P \stackrel{u}{\Longrightarrow} \Delta$ *and* $u \notin A \cup \overline{A}$ *then* $P\backslash A \stackrel{u}{\Longrightarrow} \Delta\backslash A$. □

Proposition 3.12 *Suppose* $P_i \simeq_w Q_i$ *for* $i \in I$. *Then*

(i) $u.\sum_{i\in I} p_i P_i \simeq_w u.\sum_{i\in I} p_i Q_i$

(ii) $P_1 + P_2 \simeq_w Q_1 + Q_2$

(iii) $P_1 \mid P_2 \simeq_w Q_1 \mid Q_2$

(iv) $P_1\backslash A \simeq_w Q_1\backslash A$

(v) $P_1[f] \simeq_w Q_1[f]$

Proof. We consider the third item, which is the hardest. We construct the relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ as follows:

$$\mathcal{R} \stackrel{\text{def}}{=} \{(P_1 \mid P_2,\ Q_1 \mid Q_2) \mid P_1 \approx_w Q_1 \text{ and } P_2 \approx_w Q_2\}.$$

We show that $\mathcal{R}$ is a bisimulation. There are four cases to consider.

(i) Suppose $P_1 \approx_w Q_1$, $P_2 \approx_w Q_2$ and $P_1 \mid P_2 \stackrel{u}{\longrightarrow} \Delta_1 \mid \overline{P_2}$ because of the transition $P_1 \stackrel{u}{\longrightarrow} \Delta_1$. Then $Q_1 \stackrel{\hat{u}}{\Longrightarrow} \Theta_1$ for some Θ_1 with $\Delta_1 \mathrel{\overline{\approx_w}} \Theta_1$. By Lemma 3.11 we have $Q_1 \mid Q_2 \stackrel{\hat{u}}{\Longrightarrow} \Theta_1 \mid \overline{Q_2}$ and also $(\Delta_1 \mid \overline{P_2})\ \overline{\mathcal{R}}\ (\Theta_1 \mid \overline{Q_2})$.

(ii) Suppose $P_1 \mid P_2 \stackrel{\tau}{\longrightarrow} \Delta_1 \mid \Delta_2$ because of the transitions $P_1 \stackrel{a}{\longrightarrow} \Delta_1$ and $P_2 \stackrel{\bar{a}}{\longrightarrow} \Delta_2$. Then we have $Q_1 \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_1' \stackrel{a}{\longrightarrow} \Theta_1'' \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_1$ for some $\Theta_1, \Theta_1', \Theta_1''$ with $\Delta_1 \mathrel{\overline{\approx_w}} \Theta_1$, and $Q_2 \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_2' \stackrel{\bar{a}}{\longrightarrow} \Theta_2'' \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_2$ for some $\Theta_2, \Theta_2', \Theta_2''$ with $\Delta_2 \mathrel{\overline{\approx_w}} \Theta_2$. By Lemma 3.11 we have $Q_1 \mid Q_2 \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_1' \mid \Theta_2' \stackrel{\tau}{\longrightarrow} \Theta_1'' \mid \Theta_2'' \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_1 \mid \Theta_2$ and $(\Delta_1 \mid \Delta_2)\ \overline{\mathcal{R}}\ (\Theta_1 \mid \Theta_2)$.

(iii) The symmetric cases of (i) and (ii) can be similarly analysed.

So we have checked that $\mathcal{R}$ is a bisimulation. Now suppose $P_1 \simeq_w Q_1$ and $P_2 \simeq_w Q_2$. It is immediate that $(P_1 \mid P_2)\ \mathcal{R}\ (Q_1 \mid Q_2)$, thus $(P_1 \mid P_2) \approx_w (Q_1 \mid Q_2)$. Moreover, by using arguments similar to the above analysis, it can be shown that

(i) if $P_1 \mid P_2 \stackrel{\tau}{\longrightarrow} \Delta$ then $Q_1 \mid Q_2 \stackrel{\tau}{\Longrightarrow} \Theta$ for some Θ such that $\Delta\ \overline{\mathcal{R}}\ \Theta$

(ii) if $Q_1 \mid Q_2 \stackrel{\tau}{\longrightarrow} \Theta$ then $P_1 \mid P_2 \stackrel{\tau}{\Longrightarrow} \Delta$ for some Δ such that $\Delta\ \overline{\mathcal{R}}\ \Theta$.

Therefore, it holds that $P_1 \mid P_2 \simeq_w Q_1 \mid Q_2$. □

4 Barbed congruence

In this section, although we define barbed congruence in the probabilistic CCS, the definition can be given in any probabilistic process calculus that possesses a reduction relation and a predicate $\downarrow_a$ detecting the possibility of performing

action a.

We write $P \downarrow_a$ if $P \xrightarrow{a} \Delta$ for some Δ, and $\Delta \downarrow_a$ if $P \downarrow_a$ for all $P \in \lceil\Delta\rceil$. We write $P \Downarrow_a$ if $P \stackrel{\hat{\tau}}{\Longrightarrow} \Delta$ for some Δ s.t. $\Delta \downarrow_a$; similar for $\Delta \Downarrow_a$. The negation of $P \downarrow_a$ is $P \not\downarrow_a$; similar for the meaning of $\Delta \not\Downarrow_a$.

Definition 4.1 An equivalence relation $\mathcal{R} \subseteq \mathcal{P} \times \mathcal{P}$ is a *barbed bisimulation* if $P \mathcal{R} Q$ implies:

(i) whenever $P \xrightarrow{\tau} \Delta$ then $Q \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$ and $\Delta \overline{\mathcal{R}} \Theta$

(ii) for each atomic action a, if $P \downarrow_a$ then $Q \Downarrow_a$.

Two processes P and Q are *barbed-bisimilar*, written $P \approx_b Q$, if $P \mathcal{R} Q$ for some barbed bisimulation $\mathcal{R}$.

The following property is fundamental.

Lemma 4.2 *Let $\mathcal{R}$ be a barbed bisimulation. If $\Delta \overline{\mathcal{R}} \Phi$ and $\Delta \Downarrow_a$ then we have $\Phi \Downarrow_a$.* □

Proof. First we consider two claims

(i) If $\Delta \overline{\mathcal{R}} \Phi$ and $\Delta \xrightarrow{\hat{\tau}} \Delta'$, then $\Phi \stackrel{\hat{\tau}}{\Longrightarrow} \Phi'$ for some Φ' such that $\Delta' \overline{\mathcal{R}} \Phi'$;

(ii) If $\Delta \overline{\mathcal{R}} \Phi$ and $\Delta \downarrow_a$, then $\Phi \Downarrow_a$.

The proof of claim (i) is similar to that of Lemma 3.5. Claim (ii) can be easily proved by using Lemma 3.4. The required result then follows from the two claims. □

Barbed bisimilarity is too weak to be a congruence, but it induces a congruence relation by quantifying over all contexts. As usual, a context is a process expression with a hole in it. Given a context $C[\cdot]$ and a process P, we write $C[P]$ to denote the process obtained by filling in the hole of $C[\cdot]$ with P.

Definition 4.3 Two processes P and Q are *barbed-congruent*, denoted by $P \simeq_b Q$, if for each context $C[\cdot]$, it holds that $C[P] \approx_b C[Q]$.

We now characterize barbed congruence as observational equivalence. The proof schema of this characterisation is similar to that in [15], namely, to construct contexts with sufficient distinguishing power so that two processes barbed-bisimilar under these contexts must be able to strictly mimic each other's moves in the manner of observationally equivalent processes. It is interesting to see that our construction of the contexts does not involve probabilistic choice operator, and it is somewhat simpler than the construction in [15], though we are dealing with probabilistic processes.

Theorem 4.4 *$\simeq_b$ and $\simeq_w$ coincide.*

Proof. The inclusion $\simeq_w \subseteq \simeq_b$ is immediate. For the opposite direction, we need to build a class of contexts Cxt powerful enough to guarantee that

barbed bisimulation on these contexts implies observational equivalence, i.e. prove that

$$\mathcal{R} \;=\; \{(P,Q) \mid \text{for some } C[\cdot] \in Cxt : C[P] \approx_b C[Q]\}$$

is an observational equivalence.

As in [15], we use H to represent a set of pairs of action names, and let H_i denote the projection of H on the i-th component of the pairs, for $i = 1, 2$. We require that $H_1 \cap H_2 = \emptyset$ and there is a bijective function from $H_1 \times \mathbb{N}$ to H_2 that maps a pair $(a, n) \in H_1 \times \mathbb{N}$ to a name $a_n \in H_2$. Let $\{i_n, o_n, c_n \mid n \in \mathbb{N}\}$ be a set of names disjoint from names in H. We define the processes

$$\begin{aligned} V_n \stackrel{\text{def}}{=} (H)(&\textstyle\sum_{a\in H_1} \bar{a}.((a_n + i_n) \mid \overline{a_n}.V_{n+1}\langle H\rangle) \\ &+ \textstyle\sum_{a\in H_1} a.((a_n + o_n) \mid \overline{a_n}.V_{n+1}\langle H\rangle) + c_n) \end{aligned}$$

and the relation

$$\begin{aligned} \mathcal{R}_1 \stackrel{\text{def}}{=} \{(P,Q) \mid{}& n, H \text{ exist s.t. } act(P) \cup act(Q) \subseteq H_1 \text{ and} \\ & (P \mid V_n\langle H\rangle) \approx_b (Q \mid V_n\langle H\rangle)\} \end{aligned}$$

where $act(P)$ collects the set of action names appearing in P. For simplicity, in the sequel we omit the parameter H and write V_n for $V_n\langle H\rangle$.

We now prove that $\mathcal{R}_1$ is a weak bisimulation. It is straightforward that $\mathcal{R}_1$ is an equivalence relation. So let's see how two processes related by $\mathcal{R}_1$ can match each other's transitions. Suppose $P\mathcal{R}_1 Q$ and $P \xrightarrow{u} \Delta$, we need to find some Θ s.t.

$$Q \stackrel{\hat{u}}{\Longrightarrow} \Theta \text{ and } \Delta \;\overline{\mathcal{R}_1}\; \Theta. \tag{9}$$

We consider the case when u is an input, say $u = a$. The cases when u is an output can be similarly analyzed; and the case when u is τ is simpler. Process $P \mid V_n$ has the following transitions:

$$\begin{aligned} P \mid V_n \xrightarrow{\tau} \Delta \mid \overline{(a_n + i_n) \mid \overline{a_n}.V_{n+1}} &\stackrel{\text{def}}{=} \Phi_1 \\ \xrightarrow{\tau} \Delta \mid \overline{V_{n+1}} &\stackrel{\text{def}}{=} \Phi_2 \end{aligned}$$

Since $P \mid V_n \approx_b Q \mid V_n$, there exist distributions Γ_1, Γ_2 s.t.

$$\begin{aligned} Q \mid V_n &\stackrel{\hat{\tau}}{\Longrightarrow} \Gamma_1 \;\overline{\approx_b}\; \Phi_1 \\ &\stackrel{\hat{\tau}}{\Longrightarrow} \Gamma_2 \;\overline{\approx_b}\; \Phi_2 \end{aligned}$$

We shall see that $\Gamma_i's$ structure, $i = 1, 2$, strictly mirrors $\Phi_i's$.

- Γ_1: Since $(Q \mid V_n) \Downarrow_{c_n}$ and $\Phi_1 \not\Downarrow_{c_n}$, process V_n has to perform some action in $Q \mid V_n \stackrel{\hat{\tau}}{\Longrightarrow} \Gamma_1$ so as to ensure $\Gamma_1 \;\overline{\approx_b}\; \Phi_1$. However, V_n cannot perform more than one actions because $\Phi_1 \Downarrow_{i_n}$. Therefore Γ_1 must be of the form $\Theta_1 \mid \overline{(u'_n + i_n) \mid \overline{u'_n}.V_{n+1}}$ for some u' and Θ_1 s.t. $Q \stackrel{u'}{\Longrightarrow} \Theta_1$ and $V_n \xrightarrow{\overline{u'}} \overline{(u'_n + i_n) \mid \overline{u'_n}.V_{n+1}}$. Since $\Phi_1 \Downarrow_{a_n}$ and Γ_1 must be able to do the same, we deduce that $u'_n = a_n$, thus $u' = a$, i.e. $\Gamma_1 = \Theta_1 \mid \overline{(a_n + i_n) \mid \overline{a_n}.V_{n+1}}$. So the

structure of Γ_1 is very similar to that of Φ_1.

- Γ_2: Since $\Gamma_1 \Downarrow_{a_n}$ and $\Phi_2 \not\Downarrow_{a_n}$, there must be an interaction between $a_n + i_n$ and $\overline{a_n}.V_{n+1}$ so as to ensure $\Gamma_2 \mathrel{\overline{\approx_b}} \Phi_2$. However, $\overline{a_n}.V_{n+1}$ cannot perform more than one actions because $\Phi_2 \Downarrow_{c_{n+1}}$. Therefore it must be the case that $\Gamma_2 = \Theta_2 \mid \overline{V_{n+1}}$ for some Θ_2 s.t. $\Theta_1 \stackrel{\hat{\tau}}{\Longrightarrow} \Theta_2$. Now we can observe that Γ_2's structure strictly mirrors Φ_2's.

Combining the above steps gives $Q \stackrel{a}{\Longrightarrow} \Theta_2$. Moreover, we have $\Delta \mathrel{\overline{\mathcal{R}_1}} \Theta_2$ because $\Delta \mid \overline{V_{n+1}} = \Phi_2 \mathrel{\overline{\approx_b}} \Gamma_2 = \Theta_2 \mid \overline{V_{n+1}}$. Hence, for $\Theta \stackrel{\text{def}}{=} \Theta_2$, the requirements in (9) are met, this completes the proof that $\mathcal{R}_1$ is a weak bisimulation.

We now define the relation

$$\mathcal{R} = \{(P, Q) \mid P + w \approx_b Q + w \text{ and } P \mathcal{R}_1 Q\}$$

where w does not appear in P, Q. If $P \mathcal{R} Q$ then $P \approx_w Q$ since $\mathcal{R}_1$ is a weak bisimulation. Suppose $P \stackrel{\tau}{\longrightarrow} \Delta$, then $P + w \stackrel{\tau}{\longrightarrow} \Delta$. Since $P + w \approx_b Q + w$, then there is some Θ such that $Q + w \stackrel{\hat{\tau}}{\Longrightarrow} \Theta$ and $\Delta \mathrel{\overline{\approx_b}} \Theta$. It is obvious that $\Delta \not\Downarrow_w$, so $\Theta \not\Downarrow_w$, which means that $Q + w$ must be able to make some τ move and discard the summand w. In other words, $Q + w \stackrel{\tau}{\Longrightarrow} \Theta$ for some Θ with $\Delta \mathrel{\overline{\approx_b}} \Theta$. This can only happen if $Q \stackrel{\tau}{\Longrightarrow} \Theta$. Symmetrically, if $Q \stackrel{\tau}{\longrightarrow} \Theta$, we can show that there is some Δ such that $P \stackrel{\tau}{\Longrightarrow} \Delta$ and $\Delta \mathrel{\overline{\approx_b}} \Theta$. Therefore, it holds that $P \simeq_w Q$. □

5 Axiomatisation for finite processes

In this section we restrict ourselves to a finite fragment of our calculus, using all operators in Section 2 except for constants. We present the axiom system $\mathcal{A}$ for $\simeq_w$, which includes all axioms and rules displayed in Table 2, together with the usual rules for equality (reflexivity, symmetry, transitivity and substitutivity).

Remark 5.1 In fact, $\mathcal{A}$ is obtained from the axiom system $\mathcal{A}_o$ in [8] by dropping all axioms about recursion and adding **R1-2, N1-2**, the axioms about restriction and renaming operators; for a detailed account of other axioms, the reader is refered to [8], where an observational equivalence ($\simeq$) was defined and completely axiomatized by $\mathcal{A}_o$. As we shall see later, $\simeq_w$ is completely axiomatized by $\mathcal{A}$. It follows that, although formulated in different ways, $\simeq$ and $\simeq_w$ coincide, at least for finite processes without restriction and renaming operators.

The notation $\mathcal{A} \vdash P = Q$ means that the equation $P = Q$ is derivable by applying the axioms and rules from $\mathcal{A}$. The soundness of the axioms displayed in Table 2, and therefore of $\mathcal{A}$, is easy to be verified.

Theorem 5.2 (Soundness) *If $\mathcal{A} \vdash P = Q$ then $P \simeq_w Q$.* □

The remainder of the section is devoted to proving the completeness of $\mathcal{A}$.

Definition 5.3 We say that P is in *normal form* if P is of the form

$$\sum_i u_i.\bigoplus_j p_{ij}P_{ij}$$

where each P_{ij} is also in normal form.

Lemma 5.4 *For each process P, there is some P' in normal form, such that $\mathcal{A} \vdash P = P'$.*

Proof. The proof is carried out by induction on the structure of P. By using axioms **R1-2**, **N1-2** and **E**, we can eliminate all occurrences of restriction, renaming and parallel composition operators. □

Lemma 5.5 (Saturation) *If P is in normal form and $P \stackrel{u}{\Longrightarrow} \Delta$ with $\lceil\Delta\rceil = \{P_i\}_{i\in i}$ and $\Delta(P_i) = p_i$ then $\mathcal{A} \vdash P = P + u.\bigoplus_i p_iP_i$.*

Proof. By transition induction. We heavily rely on the probabilistic τ-laws **T1-3** and the axiom **C**. Details are given in Appendix B. □

The proof of completeness is established by induction on the depth, $d(P)$, of a normal form P. Its depth is defined as:

$$\begin{aligned} d(\mathbf{0}) &= 0 \\ d(u.\bigoplus_i p_iP_i) &= 1 + max\{P_i\}_i \\ d(\textstyle\sum_i P_i) &= max\{d(P_i)\} \end{aligned}$$

As in [7], we prove a Promotion Lemma and use it as a stepping stone to establish the completeness of $\mathcal{A}$.

Lemma 5.6 (Promotion) *If $P \approx_w Q$ then $\mathcal{A} \vdash \tau.P = \tau.Q$.*

Proof. We assume that P and Q are in normal form, in view of Lemma 5.4. The proof is by induction on $d = d(P) + d(Q)$. We consider the nontrivial case that $d > 0$.

Let $u.\bigoplus_{j\in J} r_jR_j$ be any summand of P. Then we have $P \xrightarrow{u} \Delta$, with $\Delta = \sum_{j\in J} r_j \cdot \overline{R_j}$. Since $P \approx_w Q$, there exists Θ such that $Q \stackrel{\hat{u}}{\Longrightarrow} \Theta$ and $\Delta \,\overline{\approx_w}\, \Theta$. Hence,

$$\Delta = \sum_{i\in I} p_i \cdot \overline{P_i}, \qquad P_i \;\approx_w\; Q_i, \qquad \Theta = \sum_{i\in I} p_i \cdot \overline{Q_i}. \tag{10}$$

It follows from induction hypothesis that $\mathcal{A} \vdash \tau.P_i = \tau.Q_i$. So we can use **T3** to derive that $\mathcal{A} \vdash u.\bigoplus_i p_iP_i = u.\bigoplus_i p_i\tau.P_i = u.\bigoplus_i p_i\tau.Q_i = u.\bigoplus_i p_iQ_i$. Since $\sum_{j\in J} r_j \cdot \overline{R_j} = \Delta = \sum_{i\in I} p_i \cdot \overline{P_i}$, it follows from **S5** that $\mathcal{A} \vdash u.\bigoplus_{j\in J} r_jR_j = u.\bigoplus_i p_iP_i$. Now observe that $\tau.Q \stackrel{u}{\Longrightarrow} \Theta$, we know from Lemma 5.5 that $\mathcal{A} \vdash \tau.Q = \tau.Q + u.\bigoplus_{i\in I} p_iQ_i = \tau.Q + u.\bigoplus_{j\in J} r_jR_j$.

In summary $\mathcal{A} \vdash \tau.Q = \tau.Q + P$. Symmetrically $\mathcal{A} \vdash \tau.P = \tau.P + Q$. Therefore, $\mathcal{A} \vdash \tau.P = \tau.Q$ by **T4**. □

S1	$P + \mathbf{0} = P$
S2	$P + P = P$
S3	$\sum_{i\in I} P_i = \sum_{i\in I} P_{\rho(i)}$ ρ is any permutation on I
S4	$u.\bigoplus_{i\in I} p_i P_i = u.\bigoplus_{i\in I} p_{\rho(i)} P_{\rho(i)}$ ρ is any permutation on I
S5	$u.((\bigoplus_i p_i P_i) \oplus pP \oplus qP) = u.((\bigoplus_i p_i P_i) \oplus (p+q)P)$
T1	$\tau.\bigoplus_i p_i(P_i + u.\bigoplus_j p_{ij}.P_{ij}) + u.\bigoplus_{i,j} p_i p_{ij}.P_{ij}$ $= \tau.\bigoplus_i p_i(P_i + u.\bigoplus_j p_{ij}.P_{ij})$
T2	$u.\bigoplus_i p_i(P_i + \tau.\bigoplus_j p_{ij}.P_{ij}) + u.\bigoplus_{i,j} p_i p_{ij}.P_{ij}$ $= u.\bigoplus_i p_i(P_i + \tau.\bigoplus_j p_{ij}.P_{ij})$
T3	$u.(p\tau.P \oplus \bigoplus_i p_i P_i) = u.(pP \oplus \bigoplus_i p_i P_i)$
T4	If $\tau.P = \tau.P + Q$ and $\tau.Q = \tau.Q + P$ then $\tau.P = \tau.Q$.
R1	$(u.\bigoplus_{i\in I} p_i P_i)\backslash A = \begin{cases} \mathbf{0} & \text{if } u \in A \cup \overline{A} \\ u.\bigoplus_{i\in I} p_i(P_i\backslash A) & \text{otherwise} \end{cases}$
R2	$(\sum_{i\in I} P_i)\backslash A = \sum_{i\in I} P_i\backslash A$
N1	$(u.\bigoplus_{i\in I} p_i P_i)[f] = f(u).\bigoplus_{i\in I} p_i P_i[f]$
N2	$(\sum_{i\in I} P_i)[f] = \sum_{i\in I} P_i[f]$
C	$\sum_{i\in 1..n} u.\bigoplus_j p_{ij} P_{ij} = \sum_{i\in 1..n} u.\bigoplus_j p_{ij} P_{ij} + u.\bigoplus_{i\in 1..n}\bigoplus_j r_i p_{ij} P_{ij}$ with $\sum_{i\in 1..n} r_i = 1$.

E Assume $P \equiv \sum_i u_i.\bigoplus_j p_{ij}P_{ij}$ and $Q \equiv \sum_k v_k.\bigoplus_l q_{kl}Q_{kl}$. Then infer:

$$P \mid Q = \sum_i u_i.\bigoplus_j p_{ij}(P_{ij} \mid Q) + \sum_k v_k.\bigoplus_l q_{kl}(P \mid Q_{kl}) + \sum_{u_i \ opp \ v_k} \tau.\bigoplus_{j,l}(p_{ij}q_{kl})(P_{ij} \mid Q_{kl})$$

where u_i *opp* v_k means that u_i and v_k are complementary actions, i.e., $\bar{u}_i = v_k$.

Table 2
The axiom system $\mathcal{A}$

Theorem 5.7 (Completeness) *If $P \simeq_w Q$ then $\mathcal{A} \vdash P = Q$.*

Proof. The proof is similar to that for Lemma 5.6.

Let $u.\bigoplus_{j\in J} r_j R_j$ be any summand of P. Then we have $P \xrightarrow{u} \Delta$, with $\Delta = \sum_{j\in J} r_j \cdot \overline{R_j}$. Since $P \simeq_w Q$, there exists Θ such that $Q \stackrel{u}{\Longrightarrow} \Theta$ and $\Delta \mathrel{\overline{\approx_w}} \Theta$. Hence,

$$\Delta = \sum_{i\in I} p_i \cdot \overline{P_i}, \qquad P_i \approx_w Q_i, \qquad \Theta = \sum_{i\in I} p_i \cdot \overline{Q_i}. \tag{11}$$

It follows from the promotion lemma that $\mathcal{A} \vdash \tau.P_i = \tau.Q_i$. So we can use **T3** to derive that $\mathcal{A} \vdash u.\bigoplus_i p_i P_i = u.\bigoplus_i p_i \tau.P_i = u.\bigoplus_i p_i \tau.Q_i = u.\bigoplus_i p_i Q_i$. Since $\sum_{j\in J} r_j \cdot \overline{R_j} = \Delta = \sum_{i\in I} p_i \cdot \overline{P_i}$, it follows from **S5** that $\mathcal{A} \vdash u.\bigoplus_{j\in J} r_j R_j = u.\bigoplus_i p_i P_i$. Now observe that $Q \stackrel{u}{\Longrightarrow} \Theta$, we know from Lemma 5.5 that $\mathcal{A} \vdash Q = Q + u.\bigoplus_{i\in I} p_i Q_i = Q + u.\bigoplus_{j\in J} r_j R_j$.

In summary $\mathcal{A} \vdash Q = Q + P$. Symmetrically $\mathcal{A} \vdash P = P + Q$. Therefore, $\mathcal{A} \vdash P = Q$. □

Corollary 5.8 *$P \simeq_b Q$ iff $\mathcal{A} \vdash P = Q$.*

Proof. A direct consequence of Theorems 4.4, 5.2 and 5.7. □

6 Concluding remarks

In this paper we have proposed a probabilistic barbed congruence and proved that it coincides with observational equivalence in a probabilistic extension of CCS. For finite processes, we have provided an axiom system which is sound and complete w.r.t. barbed congruence.

In the future it would be interesting to establish similar results in other probabilistic process calculi. It was shown in [15] that in the π-calculus barbed congruence coincides with early bisimulation congruence. We think that it might be possible to extend this result to a probabilistic π-calculus.

References

[1] L. Aceto, Z. Ésik, and A. Ingólfsdóttir. Equational axioms for probabilistic bisimilarity (preliminary report). Technical Report RS-02-6, BRICS, 2002.

[2] S. Andova. *Probabilistic Process Algebra*. PhD thesis, Eindhoven University of Technology, 2002.

[3] S. Andova, J. C. M. Baeten, and T. A. C. Willemse. A complete axiomatisation of branching bisimulation for probabilistic systems with an application in protocol verification. In *Proceedings of the 17th International Conference on Concurrency Theory*, volume 4137 of *Lecture Notes in Computer Science*, pages 327–342. Springer, 2006.

[4] J. C. M. Baeten, J. A. Bergstra, and S. A. Smolka. Axiomatizing probabilistic processes: ACP with generative probabilities. *Information and Computation*, 121(2):234–255, 1995.

[5] C. Baier and M. Z. Kwiatkowaska. Domain equations for probabilistic processes. *Mathematical Structures in Computer Science*, 10(6):665–717, 2000.

[6] E. Bandini and R. Segala. Axiomatizations for probabilistic bisimulation. In *Proceedings of the 28th International Colloquium on Automata, Languages and Programming*, volume 2076 of *Lecture Notes in Computer Science*, pages 370–381. Springer, 2001.

[7] Y. Deng and C. Palamidessi. Axiomatizations for probabilistic finite-state behaviors. *Theoretical Computer Science*, 373(1-2):92–114, 2007.

[8] Y. Deng, C. Palamidessi, and J. Pang. Compositional reasoning for probabilistic finite-state behaviors. In *Processes, Terms and Cycles: Steps on the Road to Infinity, Essays Dedicated to Jan Willem Klop, on the Occasion of His 60th Birthday*, volume 3838 of *Lecture Notes in Computer Science*, pages 309–337. Springer, 2005.

[9] Y. Deng, R. van Glabbeek, M. Hennessy, C. Morgan, and C. Zhang. Remarks on testing probabilistic processes. *Electronic Notes in Theoretical Computer Science*, 172:359–397, 2007.

[10] A. Giacalone, C.-C. Jou, and S. A. Smolka. Algebraic reasoning for probabilistic concurrent systems. In *Proceedings of IFIP WG 2.2/2.3 Working Conference on Programming Concepts and Methods*, pages 453–459, 1990.

[11] M. Z. Kwiatkowska and G. Norman. A testing equivalence for reactive probabilistic processes. *Electronic Notes in Theoretical Computer Science*, 16(2):114–132, 1998.

[12] K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, 1991.

[13] R. Milner. *Communication and Concurrency*. Prentice-Hall, 1989.

[14] R. Milner and D. Sangiorgi. Barbed bisimulation. In *Proceedings of the 19th International Colloquium on Automata, Languages and Programming*, volume 623 of *Lecture Notes in Computer Science*, pages 685–695. Springer, 1992.

[15] D. Sangiorgi. *Expressing Mobility in Process Algebras: First-Order and Higher-Order Paradigms*. PhD thesis CST–99–93, Department of Computer Science, University of Edinburgh, 1992.

[16] R. Segala. *Modeling and Verification of Randomized Distributed Real-Time Systems*. PhD thesis, MIT, Deptartment of EECS, 1995.

[17] R. Segala and N. A. Lynch. Probabilistic simulations for probabilistic processes. In *Proceedings of the 5th International Conference on Concurrency Theory*, volume 836 of *Lecture Notes in Computer Science*, pages 481–496. Springer, 1994.

[18] E. W. Stark and S. A. Smolka. A complete axiom system for finite-state probabilistic processes. In *Proof, language, and interaction: essays in honour of Robin Milner*, pages 571–595. MIT Press, 2000.

Appendix

A Proof of Lemma 3.1

Part (i) of the lemma is easy to prove because of the fact that if $\Delta_1 \ \overline{\mathcal{R}_1} \ \Delta_2$ and $\mathcal{R}_1 \subseteq \mathcal{R}_2$ then $\Delta_1 \ \overline{\mathcal{R}_2} \ \Delta_2$. We now prove part (ii). Given three distributions $\Delta_1, \Delta_2, \Delta_3$ and a transitive relation $\mathcal{R}$, we show that if $\Delta_1 \ \overline{\mathcal{R}} \ \Delta_2$ and $\Delta_2 \ \overline{\mathcal{R}} \ \Delta_3$ then $\Delta_1 \ \overline{\mathcal{R}} \ \Delta_3$.

First $\Delta_1 \ \overline{\mathcal{R}} \ \Delta_2$ means that

$$\Delta_1 = \sum_{i\in I} p_i \cdot \overline{P_i}, \qquad P_i \ \mathcal{R} \ P'_i, \qquad \Delta_2 = \sum_{i\in I} p_i \cdot \overline{P'_i} \ ; \tag{A.1}$$

also $\Delta_2 \ \overline{\mathcal{R}} \ \Delta_3$ means that

$$\Delta_2 = \sum_{j\in J} q_j \cdot \overline{Q'_j}, \qquad Q'_j \ \mathcal{R} \ Q_j, \qquad \Delta_3 = \sum_{j\in J} q_j \cdot \overline{Q_i} \ ; \tag{A.2}$$

and we can assume *w.l.o.g.* that all the coefficients p_i, q_j are non-zero. Now define $I_j = \{\, i \in I \mid P'_i = Q'_j \,\}$ and $J_i = \{\, j \in J \mid Q'_j = P'_i \,\}$, so that trivially

$$\{(i,j) \mid i \in I, \ j \in J_i\} \quad = \quad \{(i,j) \mid j \in J, \ i \in I_j\} \tag{A.3}$$

and note that

$$\Delta_2(P'_i) = \sum_{j\in J_i} q_j \qquad \text{and} \qquad \Delta_2(Q'_j) = \sum_{i\in I_j} p_i \tag{A.4}$$

Because of (A.4) we have

$$\begin{aligned} \Delta_1 = \textstyle\sum_{i\in I} p_i \cdot \overline{P_i} &= \textstyle\sum_{i\in I} p_i \cdot \sum_{j\in J_i} \frac{q_j}{\Delta_2(P'_i)} \cdot \overline{P_i} \\ &= \textstyle\sum_{i\in I} \sum_{j\in J_i} \frac{p_i \cdot q_j}{\Delta_2(P'_i)} \cdot \overline{P_i} \end{aligned}$$

Similarly

$$\begin{aligned} \Delta_3 = \textstyle\sum_{j\in J} q_j \cdot \overline{Q_j} &= \textstyle\sum_{j\in J} q_j \cdot \sum_{i\in I_j} \frac{p_i}{\Delta_2(Q'_j)} \cdot \overline{Q_j} \\ &= \textstyle\sum_{j\in J} \sum_{i\in I_j} \frac{p_i \cdot q_j}{\Delta_2(Q'_j)} \cdot \overline{Q_j} \\ &= \textstyle\sum_{i\in I} \sum_{j\in J_i} \frac{p_i \cdot q_j}{\Delta_2(Q'_j)} \cdot \overline{Q_j} \qquad \text{by (A.3)} \end{aligned}$$

Now for each j in J_i we know that in fact $Q'_j = P'_i$, and so from the middle parts of (A.1) and (A.2), together with the transitivity of $\mathcal{R}$, we obtain $\Delta_1 \ \overline{\mathcal{R}} \ \Delta_3$.□

B Proof of Lemma 5.5

We find it convenient to show the following result and consider Lemma 5.5 as a corollary.

Lemma B.1 *If P is in normal form and $\overline{P} \stackrel{u}{\Longrightarrow} \Delta$ with $\lceil \Delta \rceil = \{P_i\}_{i \in i}$ and $\Delta(P_i) = p_i$ then $\mathcal{A} \vdash P = P + u.\bigoplus_i p_i P_i$.*

Proof. We write $(\stackrel{\hat{\tau}}{\longrightarrow})^n$ for n steps of $\hat{\tau}$-transitions. First, we prove by induction on n that

$$\text{If } \overline{P}(\stackrel{\hat{\tau}}{\longrightarrow})^n \stackrel{u}{\longrightarrow} \Delta \text{ then } \mathcal{A} \vdash P = P + u.\bigoplus_{i \in I} p_i P_i \tag{B.1}$$

where $\Delta = \sum_{i \in I} p_i \cdot \overline{P_i}$.

- $n = 0$. If $\overline{P} \stackrel{u}{\longrightarrow} \Delta$ then by the definition of lifting there is a finite index set I such that $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$ and $P \stackrel{u}{\longrightarrow} \Delta_i$ for each $i \in I$. Let $\lceil \Delta_i \rceil = \{P_{ij}\}_{j \in J_i}$ and $\Delta_i(P_{ij}) = p_{ij}$. Since P is in normal form, it has the summand $u.\bigoplus_{j \in J_i} p_{ij} P_{ij}$ for each $i \in I$. So we use **S2** to derive that $\mathcal{A} \vdash P = P + u.\bigoplus_{j \in J_i} p_{ij} P_{ij}$. By repeating this procedure for all $i \in I$, we have that

$$\begin{aligned} \mathcal{A} \vdash P &= P + \textstyle\sum_{i \in I} u.\bigoplus_{j \in J_i} p_{ij} P_{ij} \\ &= P + \textstyle\sum_{i \in I} u.\bigoplus_{j \in J_i} p_{ij} P_{ij} + u.\bigoplus_{i \in I, j \in J_i} p_i p_{ij} P_{ij} && \text{by } \mathbf{C} \\ &= P + u.\textstyle\bigoplus_{i \in I, j \in J_i} p_i p_{ij} P_{ij}. \end{aligned}$$

- Suppose (B.1) holds for some $n \geq 0$ and we consider the case for $n+1$. We claim that

  $$\text{If } P \stackrel{\hat{\tau}}{\longrightarrow} \Delta'(\stackrel{\hat{\tau}}{\longrightarrow})^n \stackrel{u}{\longrightarrow} \Delta \text{ then } \mathcal{A} \vdash P = P + u.\bigoplus_{i \in I} p_i P_i \tag{B.2}$$

  where $\Delta = \sum_{i \in I} p_i \cdot \overline{P_i}$. To see this, we focus on the first step of transition $P \stackrel{\hat{\tau}}{\longrightarrow} \Delta'$. There are two cases.

(i) $\Delta' = \overline{P}$. So $\overline{P}(\stackrel{\hat{\tau}}{\longrightarrow})^n \stackrel{u}{\longrightarrow} \Delta$ and we use induction hypothesis to derive that $\mathcal{A} \vdash P = P + u.\bigoplus_i p_i P_i$.

(ii) $P \stackrel{\tau}{\longrightarrow} \Delta'$. By the definition of lifting and Proposition 3.2 (ii), there is finite index set I such that (1) $\Delta' = \sum_{i \in I} p_i \cdot \overline{P_i'}$; (2) $P_i'(\stackrel{\hat{\tau}}{\longrightarrow})^n \stackrel{u}{\longrightarrow} \Delta_i$; (3) $\Delta = \sum_{i \in I} p_i \cdot \Delta_i$. Let $\Delta_i = \sum_{j \in J_i} p_{ij} \overline{P_{ij}}$, then we know from part (2) of the above statement and induction hypothesis that

$$\mathcal{A} \vdash P_i' = P_i' + u.\bigoplus_{j \in J_i} p_{ij} P_{ij} \tag{B.3}$$

Therefore, we derive that

$$\begin{aligned} \mathcal{A} \vdash P &= P + \tau.\textstyle\bigoplus_{i \in I} p_i P_i' && \text{by } \mathbf{S2} \\ &= P + \tau.\textstyle\bigoplus_{i \in I} p_i (P_i' + u.\bigoplus_{j \in J_i} p_{ij} P_{ij}) && \text{by (B.3)} \\ &= P + \tau.\textstyle\bigoplus_{i \in I} p_i (P_i' + u.\bigoplus_{j \in J_i} p_{ij} P_{ij}) \\ &\quad + u.\textstyle\bigoplus_{i \in I, j \in J_i} p_i p_{ij} P_{ij} && \text{by } \mathbf{T1} \\ &= P + u.\textstyle\bigoplus_{i \in I, j \in J_i} p_i p_{ij} P_{ij} \end{aligned}$$

So we have proved claim (B.2).

Now suppose that $\overline{P}(\stackrel{\hat{\tau}}{\longrightarrow})^{n+1} \stackrel{u}{\longrightarrow} \Delta$. By the definition of lifting and

Proposition 3.2 (ii), there is a finite index set I such that $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$ and $P(\xrightarrow{\hat{\tau}})^{n+1} \xrightarrow{u} \Delta_i$ for each $i \in I$. Let $\Delta_i = \sum_{j\in J_i} p_{ij}\overline{P_{ij}}$. Therefore, we have that

$$\begin{aligned}\mathcal{A} \vdash P &= P + \textstyle\sum_{i\in I} u.\bigoplus_{j\in J_i} p_{ij}P_{ij} && \text{by (B.2)}\\ &= P + \textstyle\sum_{i\in I} u.\bigoplus_{j\in J_i} p_{ij}P_{ij} + u.\bigoplus_{i\in I, j\in J_i} p_i p_{ij}P_{ij} && \text{by } \mathbf{C}\\ &= P + u.\bigoplus_{i\in I, j\in J_i} p_i p_{ij}P_{ij}\end{aligned}$$

This completes the proof of (B.1).

We are now in a position to show by induction on m that

(B.4) $$\text{If } \overline{P} \stackrel{\hat{\tau}}{\Longrightarrow} \xrightarrow{u} (\xrightarrow{\hat{\tau}})^m \Delta \text{ then } \mathcal{A} \vdash P = P + u.\bigoplus_{i\in I} p_i P_i$$

where $\Delta = \sum_{i\in I} p_i \cdot \overline{P_i}$.

- $m = 0$. Then the result follows from (B.1).
- Suppose (B.4) holds for some $m \geq 0$ and we consider the case for $m+1$. Assume that $\overline{P} \stackrel{\hat{\tau}}{\Longrightarrow} \xrightarrow{u} (\xrightarrow{\hat{\tau}})^m \Delta' \xrightarrow{\hat{\tau}} \Delta$. We focus on the last step $\Delta' \xrightarrow{\hat{\tau}} \Delta$. By the definition of lifting, there is a finite index set I such that (1) $\Delta' = \sum_{i\in I} p_i \cdot \overline{P_i}$; (2) $P_i \xrightarrow{\hat{\tau}} \Delta_i$; (3) $\Delta = \sum_{i\in I} p_i \cdot \Delta_i$. From part (1) of this statement and induction hypothesis, we know that

  (B.5) $$\mathcal{A} \vdash P = P + u.\bigoplus_{i\in I} p_i P_i$$

  Part (2) of the above statement includes two cases.
  - $\Delta_i = \overline{P_i}$. By **S2**, it holds that

    (B.6) $$\mathcal{A} \vdash \tau.P_i = \tau.P_i + \tau.P_i$$
  - $P_i \xrightarrow{\tau} \Delta_i$. Let $\Delta_i = \sum_{j\in J_i} p_{ij}\overline{P_{ij}}$. It is easy to see that P_i is in normal form, so $\tau.\bigoplus_{j\in J_i} p_{ij}P_{ij}$ is a summand of P_i. It follows from **S2** that

    (B.7) $$\mathcal{A} \vdash P_i = P_i + \tau.\bigoplus_{j\in J_i} p_{ij}P_{ij}$$

  We can partition I into two disjoint sets I_1, I_2 such that (1) $\Delta_i = \overline{P_i}$ for all $i \in I_1$; (2) $P_i \xrightarrow{\tau} \Delta_i$ for all $i \in I_2$. We continue our inference from (B.5).

$$\begin{aligned}\mathcal{A} \vdash P &= P + u.(\textstyle\bigoplus_{i\in I_1} p_i P_i \oplus \bigoplus_{i\in I_2} p_i P_i)\\ &= P + u.(\textstyle\bigoplus_{i\in I_1} p_i \tau.P_i \oplus \bigoplus_{i\in I_2} p_i P_i) && \text{by } \mathbf{T3}\\ &= P + u.(\textstyle\bigoplus_{i\in I_1} p_i(\tau.P_i + \tau.P_i)\\ &\quad \oplus \bigoplus_{i\in I_2} p_i(P_i + \tau.\bigoplus_{j\in J_i} p_{ij}P_{ij})) && \text{by (B.6) and (B.7)}\\ &= P + u.(\textstyle\bigoplus_{i\in I_1} p_i(\tau.P_i + \tau.P_i)\\ &\quad \oplus \bigoplus_{i\in I_2} p_i(P_i + \tau.\bigoplus_{j\in J_i} p_{ij}P_{ij}))\\ &\quad + u.(\textstyle\bigoplus_{i\in I_1} p_i P_i \oplus \bigoplus_{i\in I_2, j\in J_i} p_i p_{ij}P_{ij}) && \text{by } \mathbf{T2}\\ &= P + u.(\textstyle\bigoplus_{i\in I_1} p_i P_i \oplus \bigoplus_{i\in I_2, j\in J_i} p_i p_{ij}P_{ij})\end{aligned}$$

This completes the proof of (B.4), from which we immediately obtain the required result that

(B.8) If $\overline{P} \stackrel{u}{\Longrightarrow} \Delta$ then $\mathcal{A} \vdash P = P + u.\bigoplus_{i\in I} p_i P_i$

where $\Delta = \sum_{i\in I} p_i \cdot \overline{P_i}$. □

Lemma 5.5 is an obvious corollary of Lemma B.1.