Process algebra with interleaving probabilistic parallel composition

Eindhoven University of Technology
Department of Mathematics and Computing Science

Process Algebra with Interleaving Probabilistic Parallel Composition

by

Suzana Andova

99/04

ISSN 0926-4515

Reports are available at:
http://www.win.tue.nl/win/cs

Computing Science Reports 99/04
Eindhoven, June 1999

Process Algebra with Interleaving Probabilistic Parallel Composition

Suzana Andova

Department of Mathematics and Computing Science
Eindhoven University of Technology The Netherlands
e-mail: suzana@win.tue.nl

June 3, 1999

Table of Contents

List of Tables

List of Figures

Process Algebra with Interleaving Probabilistic Parallel Composition

Abstract. In this paper we present a probabilistic version of the axiom system *ACP* appropriate for the (algebraic) formal description of probabilistic processes. The proposed formalism is built in a modular way, first Basic Process Algebra (*prBPA*) is constructed which afterwards is extended by parallel composition (*prACP*). Probabilities are introduced by an operator for internal probabilistic choice. In this way *prACP* contains both non-deterministic and probabilistic choice operators. Combining these two operators leads to the situation where the idempotency law with respect to the alternative composition does not hold anymore, so the axiom $x+x=x$ is weakened to hold only for atomic actions. In defining the operational semantics for *prBPA* and *prACP*, we use the alternating approach, where two types of transitions are allowed, probabilistic and action transitions. In order to construct a complete term model for our process algebras we use a term deduction system over a larger signature than the signature of *prBPA* and *prACP*, respectively. We show that probabilistic (strong) bisimulation as proposed by Larsen and Skou is a congruence and prove the soundness and completeness of the presented term model.
As an example of the application of *prACP* we consider the Alternating Bit Protocol with unreliable communication channels.

1 Introduction

By the increasing complexity and the number of components of real-life parallel systems, the probability that a system or some of its components will be subject to failure during the work is increased, as well. This means that very often it is desirable or even necessary to "predict" chances of failure occurring in the system. In these cases, it is insufficient to assume that the system is reliable and to specify it under this assumption. But there is a need to describe the probabilistic behaviour of the components and the system as a whole. For the last ten years various traditional specification formalisms have been extended with a notion of probabilistic behaviour for different models of probabilistic processes.

Besides this new, probabilistic approach in modelling concurrent systems, non-determinism still has an essential role specially due to interleaving of activities of independent components of a system. In the sense of treating non-determinism mainly two different approaches have been proposed, one approach which allows both non-deterministic and probabilistic choices (e.g. concurrent Markov chain [21], the alternating model [11]), and one where only probabilistic choice is allowed ([17, 9, 10, 15, 5, 8]).

The objective of this paper is to introduce a probabilistic version of *ACP* ([6, 2]) where non-determinism and probability are combined. We bring structure in our theory in a modular way. That is, first we construct a basic theory which contains operators for sequential composition, non-deterministic choice (alternative composition) and probabilistic choice, called Basic Process Algebra with probabilistic choice, and then we add new operators for parallel composition and communication. A starting point for the construction of our probabilistic process algebras is the setting of [4]. There, the authors described a version of process algebra ($BPA_{\sqcup\!\!\!\!+}$ as well as $ACP_{\sqcup\!\!\!\!+}$) with three different forms of choice: the usual, dynamic alternative composition (+), a collecting alternative composition ($\sqcup$), and finally, the partial or static alternative composition ($\sqcup\!\!\!\!+$) in between the previous two. Also, it was noted that the partial choice operator might be a good basis for obtaining a probabilistic choice operator. Thus we introduce probability into $BPA_{\sqcup\!\!\!\!+}$ by replacing the partial choice operator with a probabilistic counterpart. In this way we have two different choices in our algebra (in contrast to [5]): the standard non-deterministic choice (+) and the probabilistic choice ($\sqcup\!\!\!\!+_{\pi}$, for each probability $\pi \in \langle 0, 1\rangle$). This combination of two different kinds of choice allows us to distinguish situations where quantitative (probabilistic) information about the outcome of the choice is known from situations where the choice is non-deterministic. For example, when specifying an unreliable communication channel preferably the probabilistic choice operator is used to express for the two possible events, a message is lost and a message is successfully transmitted, the probability of occurrence of each of these two events.

In the interleaving model which is essential to *ACP*-like process algebras, parallel composition clearly is modeled using non-deterministic choice. Preserving our intuition behind non-deterministic choice and the interleaving approach to parallel composition we propose a new model for parallel composition of probabilistic processes (Example 3, p. 42). That is, the choice of the process which executes the next action is considered to be non-deterministic choice. As communication is included in parallel composition, the non-deterministic choice occurs between three processes (axiom CM1, pg. 37).

Besides the axiom system in this paper we investigate the operational semantics of probabilistic processes, based on probabilistic bisimulation equivalence as proposed by Larsen and Skou ([17]) and the alternating model ([11]). The operational semantics consists of two types of transition rules, probabilistic transitions which are unlabelled and action transitions which are labelled with atomic actions. This will entail that each process in our model may make either a probabilistic or a non-deterministic step, but not both. Therefore, we have to distinguish processes that may execute only probabilistic steps, called static processes, from those that may execute only action transitions, called dynamic processes. We achieve this by using a term deduction system over a larger signature than the signature of *prBPA* and *prACP*, respectively. Namely, for each constant a we add a new constant $\breve{a}$ which denotes the process that can successfully terminate by executing atomic action a. For reasons of clearer representation of process behaviour we use strict alternation between these two possibilities. We give a detailed proof of the soundness and completeness properties of the proposed term models. Later, we extend the model with the projection operator and by approximation of infinite processes with their finite projections we prove that each guarded recursive specification has an unique solution in the term model (by proving that RDP and RSP hold).

As an example of the application of *prACP* we consider the Alternating Bit Protocol with unreliable communication channels. The sender sends a message to the receiver via a communication channel. After having received a message the receiver sends an acknowledgment to the sender via another channel. A channel may transmit a message correctly or it may corrupt it. Unreliability of each channel is specified by a probabilistic choice $\sqcup\!\!\!\!+_\pi$ between correct transmission of a message with probability π and corruption of a message with probability $1 - \pi$.

Moreover, using standard Markov chain analysis techniques we may prove liveness of the protocol and compute the average performance of the system, like the mean number of times a message has to be sent by the sender, needed for its correct transmission via the channel.

1.1 Related work

Vardi in [21] underlines that non-determinism is unavoidable in concurrent systems and introduces concurrent Markov chains as model for probabilistic concurrent programs. He proposes a technique to resolve non-determinism by a fair scheduler and gives an algorithm for the verification of probabilistic concurrent finite-state automata.

In his thesis [11], Hansson defines a probabilistic version PCCS of CCS with both, probabilistic and non-deterministic choice. PCCS, like CCS, does not have general multiplication $\cdot$, but only prefix multiplication which allows two types of processes in theory to be distinguished: probabilistic and non-deterministic processes (different from our theory where we have only probabilistic processes). He introduces an alternating model where each process can execute a probabilistic or an action transition, but not both.

D'Argenio, Hermanns and Katoen in [8] consider asynchronous generative processes and discuss the resolution of non-determinism in that setting. They define bundle transition systems, where a certain set of non-deterministic alternatives is chosen with certain probability.

Based on the generative model, in [5] Baeten, Bergstra and Smolka propose ACP with generative probabilities. In this process algebra only probabilistic choice is allowed and parallel composition is parametrized by two probabilistic parameters which determine the probabilistic distribution for the next action.

2 Basic Process Algebra

The signature of Basic Process Algebra with Probabilistic Choice, *prBPA*, consists of a (finite) set of constants $A = \{a, b, c, \ldots\}$, a special constant $\delta \notin A$ (we usually denote $A_\delta = A \cup \{\delta\}$)

and the binary operators: $+$ (non-deterministic choice, alternative composition), $\cdot$ (sequential composition) and $\boxplus_\pi$ (probabilistic choice) for each $\pi \in \langle 0,1\rangle$. The axioms for $+$ and $\cdot$ are standard axioms of BPA_δ ([2]) (Table 1, $a \in A$), except that axiom $A3$ ($x + x = x$) is restricted to atomic actions. $A3$ is restricted, because it does not hold anymore for processes involving the new choice operator (see Example 1).

$x + y$	$= y + x$	$A1$
$(x + y) + z$	$= x + (y + z)$	$A2$
$a + a$	$= a$	$AA3$
$(x + y) \cdot z$	$= x \cdot z + y \cdot z$	$A4$
$(x \cdot y) \cdot z$	$= x \cdot (y \cdot z)$	$A5$
$x + \delta$	$= x$	$A6$
$\delta \cdot x$	$= \delta$	$A7$

Table 1. BPA_δ with restricted $A3$.

Intuitively, process $x \boxplus_\pi y$ behaves like x with probability π and behaves like y with probability $1 - \pi$. The axioms for the new operators are shown in Table 2 ($\pi \in \langle 0,1\rangle$).

$x \boxplus_\pi y$	$= y \boxplus_{1-\pi} x$	$PrAC1$
$x \boxplus_\pi (y \boxplus_\rho z)$	$= (x \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} y) \boxplus_{\pi+\rho-\pi\rho} z$	$PrAC2$
$x \boxplus_\pi x$	$= x$	$PrAC3$
$(x \boxplus_\pi y) \cdot z$	$= x \cdot z \boxplus_\pi y \cdot z$	$PrAC4$
$(x \boxplus_\pi y) + z$	$= (x + z) \boxplus_\pi (y + z)$	$PrAC5$

Table 2. Additional axioms for $prBPA$.

Axiom $PrAC2$ also has a variant, as follows:

$$(x \boxplus_\pi y) \boxplus_\rho z = x \boxplus_{\pi\rho} (y \boxplus_{\frac{(1-\pi)\rho}{1-\pi\rho}} z) \quad PrAC2'.$$

We introduce abbreviations in order to deal with probabilistic sums of several arguments:

$$x \boxplus_\pi y \boxplus_\rho z \equiv x \boxplus_\pi (y \boxplus_{\frac{\rho}{1-\pi}} z) \qquad (\pi + \rho < 1)$$
$$x \boxplus_\pi y \boxplus_\rho z \boxplus_\sigma w \equiv x \boxplus_\pi (y \boxplus_{\frac{\rho}{1-\pi}} z \boxplus_{\frac{\sigma}{1-\pi}} w) \quad (\pi + \rho + \sigma < 1), \text{ etc.}$$

This notation clearly presents the probability that a process behaves as one of its components. For example, process $x_1 \boxplus_{\pi_1} x_2 \boxplus_{\pi_2} x_3 \boxplus_{\pi_3} x_4$ behaves as process x_i, $i = 1,2,3$ with probability π_i and as process x_4 with probability $1 - \pi_1 - \pi_2 - \pi_3$.

From now on, we have that the operators bind in the following order: $\cdot$ binds stronger than all other operators, and $\uplus_\pi$ binds the weakest.

Example 1. By this example we show the interpretation of non-determinism when it has been mixed with probabilistic choice. In Figure 1 *a*) the graph representation of the following processes are shown:

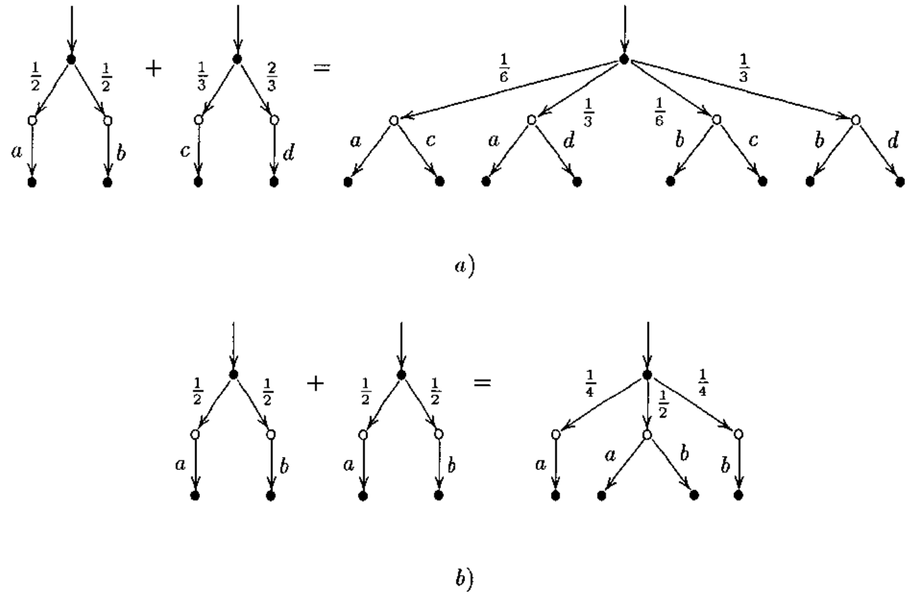
$prBPA \vdash (a \uplus_{\frac{1}{2}} b) + (c \uplus_{\frac{1}{3}} d) = (a + c) \uplus_{\frac{1}{6}} (a + d) \uplus_{\frac{1}{3}} (b + c) \uplus_{\frac{1}{6}} (b + d).$

An example in Figure 1 *b*) shows that the idempotency law with respect to alternative composition does not hold in *prBPA*. We have the equation:

$prBPA \vdash (a \uplus_{\frac{1}{2}} b) + (a \uplus_{\frac{1}{2}} b) = a \uplus_{\frac{1}{4}} (a + b) \uplus_{\frac{1}{2}} b,$

but

$prBPA \vdash a \uplus_{\frac{1}{2}} b \neq a \uplus_{\frac{1}{4}} (a + b) \uplus_{\frac{1}{2}} b.$ □



a)

b)

Fig. 1. Examples of non-deterministic choice between probabilistic processes.

Proposition 1. *If* $prBPA \vdash p = p \uplus_\pi q$ *and* $\rho > \pi$ *then* $prBPA \vdash p = p \uplus_\rho q$.

Proof. In *prBPA* the following equations hold for each $\sigma \in (0, 1)$:

$p \uplus_\rho q = (p \uplus_\sigma p) \uplus_\rho q = p \uplus_{\sigma\rho} (p \uplus_{\frac{(1-\sigma)\rho}{1-\sigma\rho}} q).$

Using the assumption $\rho > \pi$ we can choose $\sigma = \frac{\rho - \pi}{\rho(1-\pi)}$ such that $\frac{(1-\sigma)\rho}{1-\sigma\rho} = \pi$. Therefore we obtain: $p \uplus_\rho q = p \uplus_{\sigma\rho} (p \uplus_\pi q) = p \uplus_{\sigma\rho} p = p$. □

In [4] the authors propose a method for verification which is based on a partial ordering of processes. They introduce the realization axiom: $x \leq x \uplus y$, which says that x has less static non-determinism than $x \uplus y$. By the following proposition we show that this approach cannot be followed in the framework of *prBPA* because such a partial ordering cannot be defined in a non-trivial way if probabilisties are involved.

Proposition 2. *If prBPA* $\vdash p = q \uplus_\pi p$ *for some probability* $\pi \in \langle 0,1\rangle$, *then prBPA* $\vdash p \approx q$, *where* $p \approx q$ *denotes the probability of* p *being equal to* q *has a limit of* 1.

Proof. In *prBPA* the following equations hold:

$$p = q \uplus_\pi p = q \uplus_\pi (q \uplus_\pi p) = (q \uplus_{\frac{\pi}{\pi(2-\pi)}} q) \uplus_{\pi(2-\pi)} p = q \uplus_{\pi(2-\pi)} (q \uplus_{\pi(2-\pi)} p) = q \uplus_{\pi_1(2-\pi_1)} p,$$

where $\pi_1 = \pi(2-\pi)$. In such a way after n repetitions of this procedure we obtain: $p = q \uplus_{\pi_{n+1}} p$, where $\pi_{n+1} = \pi_n(2-\pi_n)$. A solution of this recurrent equation is $\pi_n = 1-(1-\pi)^{2^n}$ and as $1-\pi < 1$ we obtain $\lim_{n\to\infty} 1-(1-\pi)^{2^n} = 1$. □

Proposition 3. *The following equations hold in prBPA:*

i. $x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_i \uplus_{\pi_i} \ldots x_j \uplus_{\pi_j} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n$
$= x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_j \uplus_{\pi_j} \ldots x_i \uplus_{\pi_i} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n,$
for each i, j, $1 \leq i \leq n-1$, $1 \leq j \leq n-1$, $i < j$ *and* $n \geq 3$;

ii. $x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_i \uplus_{\pi_i} x_{i+1} \ldots \uplus_{\pi_{n-1}} x_n$
$= x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_n \uplus_{1-\sum_{j=1}^{n-1}\pi_j} x_{i+1} \ldots \uplus_{\pi_{n-1}} x_i,$
for each $1 \leq i \leq n-1$ *and* $n \geq 2$.

Proof. *i.* The proof is given by induction on n:

For $n = 3$ we have

$$x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} x_3 \equiv x_1 \uplus_{\pi_1} (x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3) = (x_1 \uplus_{\frac{\pi_1}{\pi_1+\pi_2}} x_2) \uplus_{\pi_1+\pi_2} x_3$$
$$= (x_2 \uplus_{\frac{\pi_2}{\pi_1+\pi_2}} x_1) \uplus_{\pi_1+\pi_2} x_3 = x_2 \uplus_{\pi_2} (x_1 \uplus_{\frac{\pi_1}{1-\pi_2}} x_3) \equiv x_2 \uplus_{\pi_2} x_1 \uplus_{\pi_1} x_3.$$

Suppose $n \geq 4$ and $i, j \geq 2$, $i < j$. We obtain:

$$x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_i \uplus_{\pi_i} \ldots x_j \uplus_{\pi_j} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n$$
$$\text{(let } \sigma_k = \tfrac{\pi_k}{1-\pi_1}, \text{ for } 2 \leq k \leq n-1)$$
$$= x_1 \uplus_{\pi_1} (x_2 \uplus_{\sigma_2} \ldots \uplus_{\sigma_{i-1}} x_i \uplus_{\sigma_i} \ldots x_j \uplus_{\sigma_j} x_{j+1} \ldots \uplus_{\sigma_{n-1}} x_n) \quad \text{(by IH)}$$
$$= x_1 \uplus_{\pi_1} (x_2 \uplus_{\sigma_2} \ldots \uplus_{\sigma_{i-1}} x_j \uplus_{\sigma_j} \ldots x_i \uplus_{\sigma_i} x_{j+1} \ldots \uplus_{\sigma_{n-1}} x_n)$$
$$= x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{i-1}} x_j \uplus_{\pi_j} \ldots x_i \uplus_{\pi_i} x_{j+1} \ldots \uplus_{\pi_{n-1}} x_n.$$

Now, suppose $n \geq 4$ and $i = 1, j \geq 2$. We obtain:

$$\begin{array}{l}
x_1 \boxplus_{\pi_1} x_2 \boxplus_{\pi_2} \ldots \boxplus_{\pi_{i-1}} x_i \boxplus_{\pi_i} \ldots x_j \boxplus_{\pi_j} x_{j+1} \ldots \boxplus_{\pi_{n-1}} x_n \\
(\text{let } \sigma_k = \frac{\pi_k}{1-\pi_1}, \text{ for } 2 \leq k \leq n-1) \\
= x_1 \boxplus_{\pi_1} (x_2 \boxplus_{\sigma_2} \ldots x_j \boxplus_{\sigma_j} x_{j+1} \ldots \boxplus_{\sigma_{n-1}} x_n) \text{ (by IH)} \\
= x_1 \boxplus_{\pi_1} (x_j \boxplus_{\sigma_j} \ldots \boxplus_{\sigma_{j-1}} x_2 \boxplus_{\sigma_2} x_{j+1} \ldots \boxplus_{\sigma_{n-1}} x_n) \\
= x_1 \boxplus_{\pi_1} (x_j \boxplus_{\sigma_j} (x_3 \boxplus_{\rho_3} \ldots \boxplus_{\rho_{j-1}} x_2 \boxplus_{\rho_2} x_{j+1} \ldots \boxplus_{\rho_{n-1}} x_n)) \\
(\text{ where } \rho_k = \frac{\sigma_k}{1-\sigma_j}, \text{ for } 3 \leq k \leq n-1, k \neq j) \\
= (x_1 \boxplus_{\frac{\pi_1}{\pi_1+\sigma_j-\pi_1\sigma_j}} x_j) \boxplus_{\pi_1+\sigma_j-\pi_1\sigma_j} (x_3 \boxplus_{\rho_3} \ldots \boxplus_{\rho_{j-1}} x_2 \boxplus_{\rho_2} x_{j+1} \ldots \boxplus_{\rho_{n-1}} x_n) \\
= (x_1 \boxplus_{\frac{\pi_1}{\pi_1+\pi_j}} x_j) \boxplus_{\pi_1+\pi_j} (x_3 \boxplus_{\rho_3} \ldots \boxplus_{\rho_{j-1}} x_2 \boxplus_{\rho_2} x_{j+1} \ldots \boxplus_{\rho_{n-1}} x_n) \\
= (x_j \boxplus_{1-\frac{\pi_1}{\pi_1+\pi_j}} x_1) \boxplus_{\pi_1+\pi_j} (x_3 \boxplus_{\rho_3} \ldots \boxplus_{\rho_{j-1}} x_2 \boxplus_{\rho_2} x_{j+1} \ldots \boxplus_{\rho_{n-1}} x_n) \\
= (x_j \boxplus_{\frac{\pi_j}{\pi_1+\pi_j}} x_1) \boxplus_{\pi_1+\pi_j} (x_3 \boxplus_{\rho_3} \ldots \boxplus_{\rho_{j-1}} x_2 \boxplus_{\rho_2} x_{j+1} \ldots \boxplus_{\rho_{n-1}} x_n) \\
= x_j \boxplus_{\pi_j} (x_1 \boxplus_{\frac{\pi_1}{1-\pi_j}} (x_3 \boxplus_{\rho_3} \ldots \boxplus_{\rho_{j-1}} x_2 \boxplus_{\rho_2} x_{j+1} \ldots \boxplus_{\rho_{n-1}} x_n)) \\
(\text{having } \rho_k = \frac{\sigma_k}{1-\sigma_j} = (\frac{\pi_k}{1-\pi_j})/(1 - \frac{\pi_1}{1-\pi_j})) \\
= x_j \boxplus_{\pi_j} (x_1 \boxplus_{\frac{\pi_1}{1-\pi_j}} x_3 \boxplus_{\frac{\pi_3}{1-\pi_j}} \ldots \boxplus_{\frac{\pi_{j-1}}{1-\pi_j}} x_2 \boxplus_{\frac{\pi_2}{1-\pi_j}} x_{j+1} \ldots \boxplus_{\frac{\pi_{n-1}}{1-\pi_j}} x_n) \text{ (by IH)} \\
= x_j \boxplus_{\pi_j} (x_2 \boxplus_{\frac{\pi_2}{1-\pi_j}} x_3 \boxplus_{\frac{\pi_3}{1-\pi_j}} \ldots \boxplus_{\frac{\pi_{j-1}}{1-\pi_j}} x_1 \boxplus_{\frac{\pi_1}{1-\pi_j}} x_{j+1} \ldots \boxplus_{\frac{\pi_{n-1}}{1-\pi_j}} x_n) \\
= x_j \boxplus_{\pi_j} x_2 \boxplus_{\pi_2} x_3 \boxplus_{\pi_3} \ldots \boxplus_{\pi_{j-1}} x_1 \boxplus_{\pi_1} x_{j+1} \ldots \boxplus_{\pi_{n-1}} x_n .
\end{array}$$

ii. The proof of this equation is similar to the previous one. □

2.1 Basic terms

Next, we define basic terms, which are useful for technical purposes in proofs. Because of the Elimination theorem, if we want to prove some statement valid for all closed terms, it is sufficient to prove it valid for all basic terms using structural induction as a proof method.

Definition 4. We define the set of basic terms $\mathcal{B}$ inductively, with the help of an intermediary set $\mathcal{B}_+$. In $\mathcal{B} \setminus \mathcal{B}_+$ the outermost operator is a probabilistic choice operator. Elements of $\mathcal{B}_+$ are all constants and terms that have as the outermost operator a non-deterministic choice operator or a sequential composition.

1. $A \cup \{\delta\} \subseteq \mathcal{B}_+ \subset \mathcal{B}$
2. $a \in A,\ t \in \mathcal{B} \Rightarrow a \cdot t \in \mathcal{B}_+$
3. $t, s \in \mathcal{B}_+ \Rightarrow t + s \in \mathcal{B}_+$
4. $t, s \in \mathcal{B} \Rightarrow t \boxplus_\pi s \in \mathcal{B}$ for each $\pi \in \langle 0, 1 \rangle$.

Remark. If we consider terms that only differ in the order of the summands to be identical (i.e. we work modulo axioms $A1$, $A2$, $PrAC1$ and $PrAC2$) we see that the basic terms are exactly the terms of the form

$$x \equiv x_1 \quad (x \in \mathcal{B}_+) \text{ or} \tag{1}$$

$$x \equiv x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} x_3 \ldots x_{n-1} \uplus_{\pi_{n-1}} x_n \text{ and } \ n > 1 \tag{2}$$

where $x_i \equiv \sum\limits_{j<l_i} a_{ij}t_{ij} + \sum\limits_{k<m_i} b_{ik}$ for certain atomic actions a_{ij} and b_{ik}, basic terms t_{ij} and $n, m_i, l_i \in \mathbb{N}$. We have the convention that: $\sum\limits_{j<0} s_j = \delta$.

Further, by $\mathcal{SP}$ (called the set of static processes) we will denote the set of all closed terms over the signature of *prBPA*, Σ_{prBPA}.

Definition 5. We define an auxiliary set of closed terms $\mathbf{D} \subset \mathcal{SP}$ as follows:

1. $A_\delta \subseteq \mathbf{D}$;
2. $s \in \mathbf{D}, t \in \mathcal{SP} \Rightarrow s \cdot t \in \mathbf{D}$;
3. $t, s \in \mathbf{D} \Rightarrow t + s \in \mathbf{D}$.

Remark. The closed terms from $\mathbf{D}$ are exactly of the form: $\sum\limits_{i<m} s_i \cdot t_i + \sum\limits_{j<n} a_j$ for some $n, m \in \mathbb{N}$, $a_i \in A_\delta$, closed $\mathbf{D}$ terms s_i and closed *prBPA* terms t_i. We have that $\mathcal{B}_+ \subset \mathbf{D}$.

Proposition 6. *If $s \in \mathbf{D}$ then $prBPA \vdash s = s + s$.*

Proof. We prove this result by induction of the structure of s.

1. if $s \in A_\delta$ then the result follows from axiom AA3.
2. if $s \equiv s' \cdot t$ for some $s' \in \mathbf{D}$ and $t \in \mathcal{SP}$ then by the induction hypothesis we have that $prBPA \vdash s' = s' + s'$ from which we obtain: $prBPA \vdash s + s = s' \cdot t + s' \cdot t = (s' + s') \cdot t = s' \cdot t = s$.
3. if $s \equiv s' + s''$ for some $s', s'' \in \mathbf{D}$ then by the induction hypothesis we have that $prBPA \vdash s' = s' + s'$ and $prBPA \vdash s'' = s'' + s''$ from which we obtain: $prBPA \vdash s + s = (s' + s'') + (s' + s'') = (s' + s') + (s'' + s'') = s' + s'' = s$. □

Lemma 7. *The term rewrite system shown in Table 3 ($\pi \in \langle 0, 1 \rangle$) is strongly normalizing.*

$(x + y) \cdot z$	$\to x \cdot z + y \cdot z$	*RA4*
$(x \cdot y) \cdot z$	$\to x \cdot (y \cdot z)$	*RA5*
$\delta \cdot x$	$\to \delta$	*RA7*
$(x \uplus_\pi y) \cdot z$	$\to x \cdot z \uplus_\pi y \cdot z$	*RPAC4*
$(x \uplus_\pi y) + z$	$\to (x + z) \uplus_\pi (y + z)$	*RPAC5*
$x + (y \uplus_\pi z)$	$\to (x + y) \uplus_\pi (x + z)$	*RPAC5'*

Table 3. Term rewrite system of *prBPA*.

Proof. In order to prove this proposition we use the method of the lexicographical variant of the recursive path ordering ([3]). Suppose that we have the following ordering on the signature of *prBPA*: $\cdot > + > \uplus_\pi$ and we give the symbol $\cdot$ the lexicographical status for the first argument. Then for each rewrite rule $p \to q$ in Table 3 we can easily prove that $p >_{lpo} q$. From Theorem 2.2.18 in [3] we obtain that the given term rewrite system is strongly normalizing. □

Lemma 8. *The normal forms of closed prBPA terms are basic prBPA terms.*

Proof. Suppose that p is a normal form of some closed *prBPA* term and suppose that p is not a basic term. Let p' denote the smallest sub-term of p which is not a basic term. Then we can prove that p is not a normal form. We use the fact that each sub-term of p' is a basic term. We distinguish all possible cases:

1. $p' \in A_\delta$: then p' is a basic term, which is in a contradiction with the assumption. So this case does not occur.
2. $p' \equiv p_1 \cdot p_2$ for some basic terms p_1 and p_2: by case analysis on the structure of the basic term p_1 we have:
   2.1 $p_1 \in A_\delta$: in this case p' would be a basic term, which contradicts the assumption that p' is not a basic term;
   2.2 $p_1 \equiv a \cdot p_1'$ for some $a \in A$ and some basic term p_1': then rewriting rule $RA5$ can be applied. So, p is not a normal form;
   2.3 $p_1 \equiv p_1' + p_1''$ for some basic terms p_1' and p_1'': then rewriting rule $RA4$ can be applied. So, p is not a normal form;
   2.4 $p_1 \equiv p_1' \uplus_\pi p_1''$ for some basic terms p_1' and p_1'': then rewriting rule $RPAC4$ can be applied. So, p is not a normal form.
3. $p' \equiv p_1 + p_2$ for some basic terms p_1 and p_2: by case analysis on the structure of both terms p_1 and p_2 we obtain:
   3.1 if both p_1 and p_2 are basic terms from $\mathcal{B}_+$ then p' would be a basic term, which contradicts the assumption that p' is not a basic term;
   3.2 if $p_1 \equiv p_1' \uplus_\pi p_1''$ or $p_2 \equiv p_2' \uplus_\sigma p_2''$ then rewriting rule $RPAC5$ or $RPAC5'$ is applicable. So p is not a normal form.
4. $p' \equiv p_1 \uplus_\pi p_2$ for some basic terms p_1 and p_2 and $\pi \in \langle 0, 1 \rangle$: in this case p' would be a basic term which is in contradiction with the assumption that p' is not a basic term. □

As a corollary of the previous two lemmas we obtain the following theorem:

Theorem 9. *(Elimination theorem) Let p be a closed prBPA term. Then there is a basic prBPA term q such that $prBPA \vdash p = q$.* □

Remark. If s is a closed **D** term, then the associated basic term which exists by the Elimination theorem is a term from the set $\mathcal{B}_+$.

2.2 Structured operational semantics of *prBPA*

The operational semantics consists of two types of transition rules, rules for probabilistic transitions: $\rightsquigarrow$ (which are unlabelled) and rules for action transitions: $\xrightarrow{a}$ (which are labelled with atomic actions $a \in A$). Different from other proposed operational semantics, we do not use labelled probabilistic transition and we define a probability distribution function with as domain the set of all processes, but which can easily be extended to the power set of the set of processes. Besides the fact that a function only can be considered as a probability distribution function if it is defined on the set of all processes (in other words only in that case it fulfils the conditions for probability distribution [20]), we follow this approach because it gives a easier way to work with the operational semantics.

As we have mentioned each process in our model may make either a probabilistic or an action transition, but not both. This entail that two types of processes have to be considered in the model. For this reason we consider a term deduction system with a signature different from the signature of *prBPA* by the addition of new constants. If A is the set of atomic actions of *prBPA* then we define the set of dynamic atomic actions $\breve{A}_\delta = \{\breve{a} \ : \ a \in A_\delta\}$. By a symbol $\breve{a}$, $(a \neq \delta)$ we denote a process that can successfully terminate by executing a. By $\breve{\delta}$ we denote a process that cannot execute any action.

Further we will denote $\breve{\Sigma}_{prBPA} = (A_\delta \cup \breve{A}_\delta , +, \cdot, \sqcup\!\!\!\!+_\pi)$.

Definition 10. We define the set of dynamic processes $\mathcal{DP}$ in the following way:

1. $\breve{A}_\delta \subseteq \mathcal{DP}$;
2. $s \in \mathcal{DP}, t \in \mathcal{SP} \Rightarrow s \cdot t \in \mathcal{DP}$;
3. $t, s \in \mathcal{DP} \Rightarrow t + s \in \mathcal{DP}$.

We define a map $\varphi : \mathbf{D} \rightarrow \mathcal{DP}$ as follows:

1. $\varphi(a) = \breve{a}$ for each $a \in A_\delta$;
2. $\varphi(s \cdot t) = \varphi(s) \cdot t$;
3. $\varphi(s + t) = \varphi(s) + \varphi(t)$.

If $s \in \mathbf{D}$ then $\varphi(s)$ will be denoted by $\breve{s}$.

Proposition 11. *The map φ is a bijection.* □

By $\mathcal{PR}$ we denote the set of all static and dynamic processes, that is $\mathcal{PR} = \mathcal{SP} \cup \mathcal{DP}$.

The semantics of *prBPA* is given by the term deduction system $\breve{T} = (\breve{\Sigma}_{prBPA}, D)$ induced by the deduction rules shown in Table 4. In these deduction rules a is a variable that ranges over the set A.

We use the notation $p \rightsquigarrow x$ to denote that (static) process p may execute a probabilistic step to (dynamic) process x, with other words there exists a nonzero probability with which p may behave as x. A value of this probability is defined by the probability distribution function $\mu(p,x)$ (Definition 12).

Following the notation in other *ACP*-like process algebras by $x \xrightarrow{a} p$ we denote that (dynamic) process x can do an a-transition to (static) process p and by $x \xrightarrow{a} \surd$ we denote that x can do an a-transition and then terminate.

$$
\begin{array}{ccc}
a \rightsquigarrow \breve{a} & \delta \rightsquigarrow \check{\delta} & \dfrac{p \rightsquigarrow x}{p \cdot q \rightsquigarrow x \cdot q} \\[2ex]
\dfrac{p \rightsquigarrow x,\, q \rightsquigarrow y}{p + q \rightsquigarrow x + y} & \dfrac{p \rightsquigarrow x}{p \mathbin{\sqcup\!\!\!\!+}_{\pi} q \rightsquigarrow x,\, q \mathbin{\sqcup\!\!\!\!+}_{\pi} p \rightsquigarrow x} &
\end{array}
$$

$$
\begin{array}{ccc}
\breve{a} \xrightarrow{a} \surd & \dfrac{x \xrightarrow{a} p}{x \cdot y \xrightarrow{a} p \cdot y} & \dfrac{x \xrightarrow{a} \surd}{x \cdot y \xrightarrow{a} y} \\[2ex]
\dfrac{x \xrightarrow{a} p}{x + y \xrightarrow{a} p,\, y + x \xrightarrow{a} p} & \dfrac{x \xrightarrow{a} \surd}{x + y \xrightarrow{a} \surd,\, y + x \xrightarrow{a} \surd} &
\end{array}
$$

Table 4. Deduction rules of *prBPA*.

Definition 12. (Probability distribution function) We define a probability distribution function $\mu : \mathcal{PR} \times \mathcal{PR} \rightarrow [0,1]$ inductively as follows:

$$
\begin{array}{ll}
\mu(a, \breve{a}) & = 1, \\
\mu(\delta, \check{\delta}) & = 1, \\
\mu(p \cdot q, x' \cdot q) & = \mu(p, x'), \\
\mu(p + q, x' + x'') & = \mu(p, x')\mu(q, x''), \\
\mu(p \mathbin{\sqcup\!\!\!\!+}_{\pi} q, x) & = \pi\mu(p, x) + (1 - \pi)\mu(q, x), \\
\mu(p, x) & = 0 \ \ \textit{otherwise}.
\end{array}
$$

The definition of the probability distribution function for processes containing the probabilistic choice operator as the top operator shows that the probability to behave like x depends on the probabilities of both processes in the probabilistic choice to behave like x. Namely, the probability that $p \mathbin{\sqcup\!\!\!\!+}_{\pi} q$ behaves like x is obtained as a total probability of both processes p and q to behave as x, that is, as the sum of independent probabilities for each process.

In order to have clearer presentation of probabilistic transitions we will use transition systems where each probabilistic transition $p \rightsquigarrow x$ is labelled by the associated probability $\mu(p, x)$.

Because in the construction of the term model we use the Larsen-Skou probabilistic bisimulation relation (Definition 17) we need to extend the probability distribution function to the power set of $\mathcal{PR}$.

Definition 13. We define the map $\mu^* : \mathcal{PR} \times 2^{\mathcal{PR}} \rightarrow [0, 1]$ in the following way:
$\mu^*(p, M) = \sum_{x \in M} \mu(p, x)$ for each $M \subseteq \mathcal{PR}$.

Proposition 14. *The map μ^* is well defined.*

Proof. We just need to prove that for each $p \in \mathcal{PR}$ and $M \subseteq \mathcal{PR}$, $\mu^*(p, M) \in [0, 1]$.

1. If $p \in A_\delta$ then
   $\mu^*(p, M) = \sum_{x \in M} \mu(p, x) = \begin{cases} 1, & \breve{p} \in M \\ 0, & otherwise \end{cases}$
2. If $p \equiv q \cdot s$ for some $q, s \in \mathcal{PR}$ then
   $\mu^*(q \cdot s, M) = \sum_{x \in M} \mu(q \cdot s, x) = \sum_{x : x \in M \& \exists x' : x \equiv x' \cdot s} \mu(q \cdot s, x) = \sum_{x' : x' \cdot s \in M} \mu(q, x') =$
   $\mu^*(q, \{x' \ : \ x' \cdot s \in M\}) \in [0, 1]$ by the induction hypothesis.
3. If $p \equiv q + s$ for some $q, s \in \mathcal{PR}$ then
   $\mu^*(q + s, M) = \sum_{x \in M} \mu(q + s, x) = \sum_{x : x \in M \& \exists x', x'' : x \equiv x' + x''} \mu(q, x')\mu(s, x'') \leq$
   $\mu^*(q, \{x' \ : \ \exists x'' : x' + x'' \in M\})\mu^*(s, \{x'' \ : \ \exists x' : x' + x'' \in M\}) \in [0, 1]$ by the induction hypothesis.
4. If $p \equiv q \uplus_\pi s$ for some $q, s \in \mathcal{PR}$ and $\pi \in \langle 0, 1 \rangle$ then
   $\mu^*(q \uplus_\pi s, M) = \sum_{x \in M} \mu(q \uplus_\pi s, x) = \sum_{x \in M} (\pi\mu(q, x) + (1 - \pi)\mu(s, x)) =$
   $\pi \sum_{x \in M} \mu(q, x) + (1 - \pi) \sum_{x \in M} \mu(s, x) = \pi\mu^*(q, M) + (1 - \pi)\mu^*(s, M) \in [0, 1]$ by the induction hypothesis. □

From now on we will denote $\mu^*(p, M)$ simply by $\mu(p, M)$.

Corollary 15. $\mu(p \uplus_\pi q, M) = \pi\mu(p, M) + (1 - \pi)\mu(q, M)$ □

Corollary 16. *Let us denote $M_1 \cdot M_2 = \{m_1 \cdot m_2 \ : \ m_1 \in M_1 \ \& \ m_2 \in M_2\}$. Then*
$\mu(p \cdot q, M_1 \cdot M_2) = \mu(p, M_1)$. □

Definition 17. Let R be an equivalence relation on the set of processes $\mathcal{PR}$. R is a *probabilistic bisimulation* if:

1. If pRq and $p \rightsquigarrow s$ then there is a term t such that $q \rightsquigarrow t$ and sRt;
2. If sRt and $s \xrightarrow{a} p$ for some $a \in A$, then there is a term q such that $t \xrightarrow{a} q$ and pRq;
3. If sRt and $s \xrightarrow{a} \surd$, then $t \xrightarrow{a} \surd$;

4. If pRq, then $\mu(p, M) = \mu(q, M)$ for each $M \in \mathcal{PR}/R$.

We say that p is ***probabilistically bisimilar*** to q, denote $p \mathrel{\underline{\leftrightarrow}} q$, if there is a probabilistic bisimulation R such that pRq.

From the definition of the operational semantics and the definition of the probability distribution function we obtain the following properties:

Proposition 18. *Let $p, x \in \mathcal{PR}$. Then $\mu(p, x) \neq 0$ iff $p \rightsquigarrow x$.* □

Proposition 19. *Let $p \in \mathcal{PR}$ and $M \subseteq \mathcal{PR}$. Then $\mu(p, M) \neq 0$ iff $\exists x \in M : p \rightsquigarrow x$.* □

Different from a bisimulation relation used in the construction of a term model of other *ACP*-like process algebras, here we have an extra requirement that a probabilistic bisimulation has to be an equivalence relation. This requirement is related with the fourth clause in Definition 17 which says that besides a simulation of probabilistic and action transitions between two processes considered as bisimilar, the probability of both processes to pass to elements of one equivalence class must be equal. For example, the processes presented by the transition systems $a)$ and $b)$ in Figure 2 are not bisimilar and the processes $a)$ and $c)$ are bisimilar.

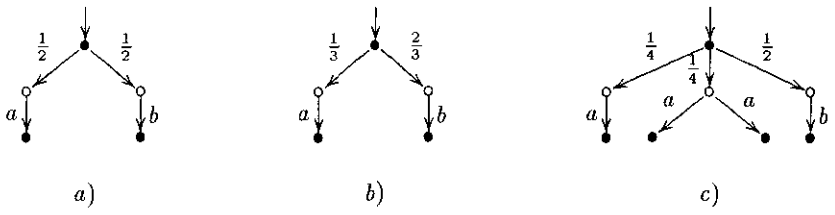


Fig. 2. An example for probabilistic bisimulation.

Next we give some properties of the probability distribution function which are used in proofs that a given equivalence relation is a probabilistic bisimulation relation.

Proposition 20. *If $p \in \mathcal{PR}$ and $M_1, M_2 \subseteq \mathcal{PR}$ such that $M_1 \cap M_2 = \emptyset$, then*

$$\mu(p, M_1 \cup M_2) = \mu(p, M_1) + \mu(p, M_2).$$

Proof. Using the properties of the sum operator (for real numbers) we obtain easily:

$$\mu(p, M_1 \cup M_2) = \sum_{x \in M_1 \cup M_2} \mu(p, x) = \sum_{x \in M_1} \mu(p, x) + \sum_{x \in M_2} \mu(p, x) = \mu(p, M_1) + \mu(p, M_2). \quad \square$$

Corollary 21. *Let $p \in \mathcal{PR}$ and $M_i \subseteq \mathcal{PR}, i \in I$ for some finite or countable infinite index set I, such that $M_i \cap M_j = \emptyset$ for each $i, j \in I, i \neq j$. Then*

$$\mu(p, \bigcup_{i\in I} M_i) = \sum_{i\in I} \mu(p, M_i).$$

□

Proposition 22. *Let $p, q \in \mathcal{PR}$ and $M \subseteq \mathcal{PR}$. If $M_1, M_2 \subseteq \mathcal{PR}$ are such that:*

$$M_1 + M_2 = \{m_1 + m_2 \ : \ m_1 \in M_1 \ \& \ m_2 \in M_2\} \subseteq M$$

then:

$$\mu(p + q, M) = \mu(p, M_1)\mu(q, M_2) + \mu(p + q, M \setminus (M_1 + M_2)).$$

Proof. It is sufficient to prove that $\mu(p + q, M_1 + M_2) = \mu(p, M_1)\mu(q, M_2)$. Using the properties of the sum operator of real numbers and the following property:

$\forall m_1 \in M_1 : \forall m_2 \in M_2 : m_1 + m_2 \in M_1 + M_2$ (∗)

we obtain:

$$\begin{aligned}\mu(p + q, M_1 + M_2) &= \sum_{x\in M_1+M_2} \mu(p + q, x) = \sum_{x\equiv m_1+m_2\in M_1+M_2} \mu(p + q, m_1 + m_2)\\ &= \sum_{m_1+m_2\in M_1+M_2} \mu(p, m_1)\mu(q, m_2) \overset{(*)}{=} \sum_{m_1\in M_1} \left(\mu(p, m_1) \sum_{m_2\in M_2} \mu(q, m_2)\right)\\ &= \left(\sum_{m_1\in M_1} \mu(p, m_1)\right)\left(\sum_{m_2\in M_2} \mu(q, m_2)\right) = \mu(p, M_1)\mu(q, M_2).\end{aligned}$$

□

One can note that in these proofs non assumption about the structure of p or the elements of equivalence classes are made and the given equalities depend on the definition of the probability distribution function. As in the following models (Section 3.2 and Section 4) we extend the probability distribution function keeping the part for the operators from *prBPA*, in the later sections we use these properties freely.

Here follow some useful properties of transitions.

Proposition 23. *If p is a $\mathcal{SP}$ term and $p \rightsquigarrow x$, then $x \in \mathcal{DP}$ (that is $x \equiv \sum_{i<m} y_i \cdot t_i + \sum_{j<n} \breve{a}_j$ for some $n, m \in \mathbb{N}$, $a_j \in A_\delta$, $\mathcal{DP}$ terms y_i and $\mathcal{SP}$ terms t_i).*

Proof. The proof is given by induction on the structure of p.

1. $p \equiv \delta$: then $\delta \rightsquigarrow \breve{\delta}$ is the only possible probabilistic transition and $\breve{\delta} \in \mathcal{DP}$;
2. $p \equiv a$: then $a \rightsquigarrow \breve{a}$ is the only possible probabilistic transition and $\breve{a} \in \mathcal{DP}$;

3. $p \equiv p_1 \cdot p_2$ for some $\mathcal{SP}$ terms p_1 and p_2: then by the assumption $p_1 \cdot p_2 \rightsquigarrow x$ we have that $p_1 \rightsquigarrow x'$ with $x \equiv x' \cdot p_2$. By the induction hypothesis we have $x' \in \mathcal{DP}$ from which we obtain $x \in \mathcal{DP}$;
4. $p \equiv p_1 + p_2$ for some $\mathcal{SP}$ terms p_1 and p_2: then by the assumption $p_1 + p_2 \rightsquigarrow x$ we have that $p_1 \rightsquigarrow x'$, $p_2 \rightsquigarrow x''$ for some x' and x'' such that $x \equiv x' + x''$. By the induction hypothesis we have $x' \in \mathcal{DP}$ and $x'' \in \mathcal{DP}$ from which we obtain $x \in \mathcal{DP}$;
5. $p \equiv p_1 \boxplus_\alpha p_2$ for some $\mathcal{SP}$ terms p_1 and p_2: then by the assumption $p_1 \boxplus_\alpha p_2 \rightsquigarrow x$ we have $p_1 \rightsquigarrow x$ or $p_2 \rightsquigarrow x$. But in both cases we have by the induction hypothesis that $x \in \mathcal{DP}$. □

Proposition 24. *If x is a $\mathcal{DP}$ term and $x \xrightarrow{a} p$ for some $a \in A$, then $p \in \mathcal{SP}$.*

Proof. It follows from the definition of the deduction rules and Definition 10. □

Remark. From Proposition 23 and 24 it follows easily that we can reduce our investigation as following:

1. $\rightsquigarrow \subseteq \mathcal{SP} \times \mathcal{DP}$,
2. $\xrightarrow{a} \subseteq \mathcal{DP} \times \mathcal{SP}$,
3. $\xrightarrow{a} \surd \subseteq \mathcal{DP}$,
4. for every probabilistic bisimulation R we have $R \subseteq \mathcal{SP} \times \mathcal{SP} \cup \mathcal{DP} \times \mathcal{DP}$.

Using this result, we consider in later proofs probabilistic transitions for static processes only and action transitions for dynamic processes only. Very often we construct a bisimulation relation as an union of relations. If one of these relations is a bisimulation relation then we do not consider transitions for pairs belonging to that relation. If one of these relations is a subset of $\mathcal{SP} \times \mathcal{SP}$, we consider only probabilistic transitions for pairs belonging to that relation. If one of these relations is a subset of $\mathcal{DP} \times \mathcal{DP}$, we consider only action transitions for pairs belonging to that relation. Moreover, in proofs concerning the fourth clause of Definition 17, we suppose that an equivalence class is a subset of $\mathcal{DP}$. And if investigate the value $\mu(p, M)$ often we assume that there is element $u \in M$ such that $p \rightsquigarrow u$, in other words we assume that M is a reachable from p. By Proposition 19 if M is an unreachable class from p we conclude that $\mu(p, M) = 0$.

Proposition 25. *If x is a* **D** *term, then the only possible probabilistic transition of x is $x \rightsquigarrow \breve{x}$ and $\mu(x, \breve{x}) = 1$.*

Proof. The proof is given by induction on the structure of x.

1. $x \in A_\delta$: then the conclusion follows from the definition of the operational rules and the distribution function μ;

2. $x \equiv y \cdot t$ for some $y \in \mathbf{D}$ and $t \in \mathcal{SP}$: then by the induction hypothesis we have that $y \rightsquigarrow \breve{y}$ is the only possible probabilistic transition of y. Using the definition of the operational rules it follows that $x \rightsquigarrow \breve{y} \cdot t$. But then we have $\breve{x} \equiv \breve{y} \cdot t$ from which we obtain that $x \rightsquigarrow \breve{x}$ is the only possible probabilistic transition of x. Moreover, $\mu(x, \breve{x}) = \mu(y \cdot t, \breve{y} \cdot t) = \mu(y, \breve{y}) = 1$;
3. $x \equiv y_1 + y_2$ for some $y_1, y_2 \in \mathbf{D}$: then by the induction hypothesis we have that $y_1 \rightsquigarrow \breve{y}_1$ is the only possible probabilistic transition of y_1 and $y_2 \rightsquigarrow \breve{y}_2$ of y_2 and $\mu(y_1, \breve{y}_1) = 1$ and $\mu(y_2, \breve{y}_2) = 1$. From the definition of the operational rules it follows that $x \rightsquigarrow \breve{y}_1 + \breve{y}_2$. But then we have $\breve{x} \equiv \breve{y}_1 + \breve{y}_2$ from which we obtain that $x \rightsquigarrow \breve{x}$ is the only possible probabilistic transition of x. Moreover, $\mu(x, \breve{x}) = \mu(y_1 + y_2, \breve{y}_1 + \breve{y}_2) = \mu(y_1, \breve{y}_1)\mu(y_2, \breve{y}_2) = 1$. □

As a corollary of the previous proposition and the definition of the operational rules we have the following results:

Corollary 26. *If x_1, x_2 are* $\mathbf{D}$ *terms then $x_1 \not\rightsquigarrow \breve{x}_2$ iff $x_1 \not\equiv x_2$.* □

Corollary 27. *If x is a basic prBPA term and $x \rightsquigarrow \breve{x}'$ for some $x' \in \mathcal{DP}$ then x' is a basic prBPA term. Moreover $x' \in \mathcal{B}_+$.* □

Proposition 28. *If R_1 and R_2 are probabilistic bisimulation relations then also $R = Eq(R_1 \circ R_2)$ is a probabilistic bisimulation relation.*

Proof. Suppose that pRr for some $p, r \in \mathcal{SP}$. It follows that there exists $q \in \mathcal{SP}$ such that pR_1q and qR_2r.

Let $p \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then there exists $v \in \mathcal{DP}$ such that $q \rightsquigarrow v$ and uR_1v from which it follows that there exists $w \in \mathcal{DP}$ such that $r \rightsquigarrow w$ and vR_2w. We obtain the following: if $p \rightsquigarrow u$ for some $u \in \mathcal{DP}$, then there exists $w \in \mathcal{DP}$ such that $r \rightsquigarrow w$ and uRw. In a similar way we can prove that if $r \rightsquigarrow w$ for some $w \in \mathcal{DP}$, then there exists $u \in \mathcal{DP}$ such that $p \rightsquigarrow u$ and wRu.

Suppose that uRw for some $u, w \in \mathcal{DP}$. It follows that there exists $v \in \mathcal{DP}$ such that uR_1v and vR_2w.

Let $u \xrightarrow{a} s$ for some $a \in A$ and $s \in \mathcal{SP}$. Then there exists $t \in \mathcal{SP}$ such that $v \xrightarrow{a} t$ and sR_1t from which it follows that there exists $o \in \mathcal{SP}$ such that $w \xrightarrow{a} o$ and tR_2o. We obtain the following: if $u \xrightarrow{a} s$ for some $a \in A$ and $s \in \mathcal{SP}$, then there exists $o \in \mathcal{SP}$ such that $w \xrightarrow{a} o$ and sRo. In a similar way we can prove that if $w \xrightarrow{a} o$ for some $o \in \mathcal{SP}$, then there exists $s \in \mathcal{SP}$ such that $u \xrightarrow{a} s$ and sRo.

If $u \xrightarrow{a} \surd$ for some $a \in A$ then $v \xrightarrow{a} \surd$ and also $w \xrightarrow{a} \surd$, and vice versa.

Suppose that pRr for some $p, r \in \mathcal{SP}$ and $M \in \mathcal{PR}/R$, $M \subseteq \mathcal{DP}$. It follows that there exists $q \in \mathcal{SP}$ such that pR_1q and qR_2r. $(\triangle)$

Moreover we have that $M = \bigcup\limits_{i \in I_1} M_{i1} = \bigcup\limits_{j \in I_2} M_{j2}$ $(I_1 \neq \emptyset, I_2 \neq \emptyset)$ for some equivalence classes $M_{i1} \in \mathcal{PR}/R_1$, $i \in I_1$ and $M_{j2} \in \mathcal{PR}/R_2$, $j \in I_2$, because R, R_1 and R_2 are equivalence relations defined on the same set and $R_1 \subseteq R$ and $R_2 \subseteq R$. From Corollary 21 and $(\triangle)$ we obtain:

$$\mu(p, M) = \mu(p, \bigcup_{i\in I_1} M_{i1}) = \sum_{i\in I_1} \mu(p, M_{i1}) = \sum_{i\in I_1} \mu(q, M_{i1}) = \mu(q, \bigcup_{i\in I_1} M_{i1}) = \mu(q, M) =$$
$$\mu(q, \bigcup_{j\in I_2} M_{j2}) = \sum_{j\in I_2} \mu(q, M_{j2}) = \sum_{j\in I_2} \mu(r, M_{j2}) = \mu(r, \bigcup_{j\in I_2} M_{j2}) = \mu(r, M). \qquad \square$$

Proposition 29. $\underline{\leftrightarrow}$ *is a probabilistic bisimulation relation.*

Proof. First, we prove that $\underline{\leftrightarrow}$ is an equivalence relation. The result that $\underline{\leftrightarrow}$ is a reflexive and symmetric relation is trivial and from Proposition 28 it follows easily that $\underline{\leftrightarrow}$ is a transitive relation.

Second, we need to prove that the four clauses from Definition 17 hold for $\underline{\leftrightarrow}$.

Suppose that $p \underline{\leftrightarrow} q$ for some $p, q \in \mathcal{SP}$. From the definition of $\underline{\leftrightarrow}$ it follows that there exists a bisimulation relation R such that pRq. If $p \rightsquigarrow u$ for some $u \in \mathcal{DP}$, then $q \rightsquigarrow v$ for some $v \in \mathcal{DP}$ such that uRv from which $u \underline{\leftrightarrow} v$.

Suppose that $u \underline{\leftrightarrow} v$ for some $u, v \in \mathcal{DP}$. From the definition of $\underline{\leftrightarrow}$ it follows that there exists a bisimulation relation R such that uRv. If $u \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$, then $v \xrightarrow{a} q$ for some $q \in \mathcal{SP}$ such that pRq which implies that $p \underline{\leftrightarrow} q$. If $u \xrightarrow{a} \surd$, then $v \xrightarrow{a} \surd$ as well.

Suppose that $p \underline{\leftrightarrow} q$ for some $p, q \in \mathcal{SP}$ and $M \in \mathcal{PR}/\underline{\leftrightarrow}$. It implies that there exists a bisimulation relation R such that pRq. Note that $R \subseteq \underline{\leftrightarrow}$. Moreover, as R and $\underline{\leftrightarrow}$ are equivalence relations defined on the same set and $R \subseteq \underline{\leftrightarrow}$ we have that $M = \bigcup_{i\in I} M_{i_R}$ for some $M_{i_R} \in \mathcal{PR}/R$, $i \in I, I \neq \emptyset$. Then we obtain:

$$\mu(p, M) = \mu(p, \bigcup_{i\in I} M_{i_R}) = \sum_{i\in I} \mu(p, M_{i_R}) = \sum_{i\in I} \mu(q, M_{i_R}) = \mu(q, \bigcup_{i\in I} M_{i_R}) = \mu(q, M). \qquad \square$$

Remark. From Definition 17 and Proposition 29 it follows that $\underline{\leftrightarrow}$ is the maximal probabilistic bisimulation relation.

Theorem 30. $\underline{\leftrightarrow}$ *is a congruence relation on prBPA.*

Proof. From Proposition 29 we have that $\underline{\leftrightarrow}$ is an equivalence relation. We only need to prove that $\underline{\leftrightarrow}$ is preserved by the operators: $+$, $\cdot$ and $+\!\!+_\pi, \pi \in \langle 0, 1]$.

With respect to $\cdot$: Let x, y, z and w be $\mathcal{PR}$ terms such that $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$. So, there exist probabilistic bisimulations R_1 and R_2 such that xR_1y and zR_2w. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup R_2)$,

where

$\alpha = \{(p \cdot s, q \cdot t) \ : \ p, q, s, t \in \mathcal{SP}, pR_1q, sR_2t\}$,

$\beta = \{(u \cdot s, v \cdot t) \ : \ u, v \in \mathcal{DP},\ s, t \in \mathcal{SP}, uR_1v, sR_2t\}$

and where Eq means the equivalence closure of the given relation.

Note that the relations α and β are equivalence relations and $\alpha \subseteq \mathcal{SP} \times \mathcal{SP}$ and $\beta \subseteq \mathcal{DP} \times \mathcal{DP}$.

Suppose $(p \cdot s)R(q \cdot t)$ for some $p, q, s, t \in \mathcal{SP}$ where pR_1q and sR_2t and $p \cdot s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $p \rightsquigarrow u'$ for some $u' \in \mathcal{DP}$

and $u \equiv u' \cdot s$. Then $q \rightsquigarrow v'$ for some $v' \in \mathcal{DP}$ such that $u'R_1v'$ and also $q \cdot t \rightsquigarrow v' \cdot t$ and by the definition of R we have that $(u' \cdot s)R(v' \cdot t)$.

Suppose $(u \cdot s)R(v \cdot t)$ for some $u, v \in \mathcal{DP}$ and $s, t \in \mathcal{SP}$, where uR_1v, sR_2t and $u \cdot s \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then from the definition of the operational rules the following two cases can occur:

1. $u \xrightarrow{a} p'$ for $p' \in \mathcal{SP}$ such that $p \equiv p' \cdot s$: then $v \xrightarrow{a} q'$ for some $q' \in \mathcal{SP}$ and $p'R_1q'$. Then $v \cdot t \xrightarrow{a} q' \cdot t$ and by the definition of R we have that $(p' \cdot s)R(q' \cdot t)$;
2. $u \xrightarrow{a} \surd$ and $p \equiv s$: then $v \xrightarrow{a} \surd$ and we obtain that $v \cdot t \xrightarrow{a} t$ and by the definition of R we have that sRt.

Transitions of the form $u \cdot s \xrightarrow{a} \surd$ cannot occur.

Suppose rRr_1 for some $r, r_1 \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, (M \subseteq \mathcal{DP})$. We have that for each class $M \in \mathcal{PR}/R$, $M = \bigcup_{i \in I} M_i$ for some $M_i \in \mathcal{PR}/R_2$ $(I \neq \emptyset)$ and also $M = \bigcup_{j \in J} K_j$ for some $K_j \in \mathcal{PR}/\beta$ $(J \neq \emptyset)$. This result follows from the fact that β and R_2 are equivalence relations defined on the same set as R, and both $R_2 \subseteq R$ and $\beta \subseteq R$. (We consider equivalence classes of β because from the previous discussion for probabilistic transitions of $p \cdot s$ and $q \cdot t$ it follows that if $p \cdot s \rightsquigarrow u$ then there exists v such that $q \cdot t \rightsquigarrow v$ and $u\beta v$.)

As R is defined as an union of three relations, but only two of them R_2 and α, contain pairs of static processes, we discuss two possibilities:

1. If rR_2r_1, then $M = \bigcup_{i \in I} M_i$ and
$$\mu(r, M) = \mu(r, \bigcup_{i \in I} M_i) = \sum_{i \in I} \mu(r, M_i) = \sum_{i \in I} \mu(r_1, M_i) = \mu(r_1, \bigcup_{i \in I} M_i) = \mu(r_1, M). \qquad (*)$$
2. If $r\alpha r_1$, then $r \equiv p \cdot s, r_1 \equiv q \cdot t$, for some $p, q, s, t \in \mathcal{SP}$ such that pR_1q and sR_2t. If K_j is an equivalence class reachable from $p \cdot s$ then it must be an element $u_j \cdot s \in K_j$ such that $p \cdot s \rightsquigarrow u_j \cdot s$ and $p \rightsquigarrow u_j$. Therefore, $K_j = [u_j \cdot s]_\beta$. Then from the definition of β we have $K_j = [u_j \cdot s]_\beta = [u_j]_{R_1} \cdot [s]_{R_2}$ and using Corollary 16 we obtain:
$\mu(p \cdot s, K_j) = \mu(p \cdot s, [u_j]_{R_1} \cdot [s]_{R_2}) = \mu(p, [u_j]_{R_1}) = \mu(q, [u_j]_{R_1}) = \mu(q \cdot t, [u_j]_{R_1} \cdot [t]_{R_2}) = \mu(q \cdot t, [u_j \cdot t]_\beta) = \mu(q \cdot t, K_j)$
and $[u_j \cdot t]_\beta = [u_j \cdot s]_\beta$ because tR_2s, which implies $(u_j \cdot t)\beta(u_j \cdot s)$.
In conclusion we obtain $\mu(r, M) = \mu(p \cdot s, M) = \mu(p \cdot s, \bigcup_{j \in J} K_j) = \sum_{j \in J} \mu(q \cdot t, K_j) = \mu(q \cdot t, \bigcup_{j \in J} K_j) = \mu(q \cdot t, M) = \mu(r_1, M)$.

With respect to $+$: Let x, y, z and w be $\mathcal{PR}$ terms such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So, there exist probabilistic bisimulations R_1 and R_2 such that xR_1y and zR_2w. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup R_1 \cup R_2)$,

where

$\alpha = \{(p + s, q + t) \; : \; p, q, s, t \in \mathcal{SP}, pR_1q, sR_2t\}$,

$\beta = \{(u+l, v+m) \ : \ u, v, l, m \in \mathcal{DP}, \ uR_1v, \ lR_2m\}$
and where Eq means the equivalence closure of the given relation.

Suppose $(p+s)R(q+t)$ for some $p, q, s, t \in \mathcal{SP}$ such that pR_1q, sR_2t and $p+s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $p \rightsquigarrow u'$ and $s \rightsquigarrow u''$ for certain $u', u'' \in \mathcal{DP}$ such that $u \equiv u' + u''$. It implies that $q \rightsquigarrow v'$ and $t \rightsquigarrow v''$ for some $v', v'' \in \mathcal{DP}$ such that $u'R_1v'$ and $u''R_2v''$. Then $q+t \rightsquigarrow v' + v''$ and by the definition of R we have that $(u' + u'')R(v' + v'')$.

Suppose $(u+l)R(v+m)$ for some $u, v, l, m \in \mathcal{DP}$ such that uR_1v, lR_2m and $u + l \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then according to the definition of the operational rules the following two cases can occur:

1. $u \xrightarrow{a} p$: then $v \xrightarrow{a} q$ for some $q \in \mathcal{SP}$ such that pR_1q. Then $v + m \xrightarrow{a} q$ and by the definition of R we have that pRq.
2. $l \xrightarrow{a} p$: this case is treated analogously to the previous case.

Suppose $(u+l)R(v+m)$ for some $u, v, l, m \in \mathcal{DP}$ such that uR_1v and lR_2m and $u + l \xrightarrow{a} \surd$ for some $a \in A$. Then from the definition of the operational rules we have $u \xrightarrow{a} \surd$ or $l \xrightarrow{a} \surd$ which implies $v \xrightarrow{a} \surd$ or $m \xrightarrow{a} \surd$. But in each of these cases it holds $v + m \xrightarrow{a} \surd$.

Suppose rRr_1 for some $r, r_1 \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, (M \subseteq \mathcal{DP})$. As R is defined as an union of relations, but only three of them, R_1, R_2 and α, contain pairs of static processes, we discuss the following possibilities:

1. If $rR_kr_1, k = 1, 2$, then because $R_1 \subseteq R$ and $R_2 \subseteq R$ we have that $M = \bigcup\limits_{i \in I_k} M_{ik}$ $(I_k \neq \emptyset)$ for some equivalence classes $M_{ik} \in \mathcal{PR}/R_k$. Then the equality $\mu(r, M) = \mu(r_1, M)$ in the both cases can be obtained easily in a similar way as in (*). (**)
2. If $r\alpha r_1$, then $r \equiv p + s$ and $r_1 \equiv q + t$ for some $p, q, s, t \in \mathcal{SP}$ such that pR_1q and sR_2t. As $\beta \subseteq R$ it follows that $M = \bigcup\limits_{i \in I} M_i$ for some $M_i \in \mathcal{PR}/\beta$ $(I \neq \emptyset)$. (We consider equivalence classes of β because from the previous discussion for probabilistic transitions of $p + s$ and $q + t$ it follows that if $p + s \rightsquigarrow u$ then there exists v such that $q + t \rightsquigarrow v$ and $u\beta v$.)
   Note that if M_i is reachable from $p + s$ then there exists an element $u_i + l_i \in M_i, u_i, l_i \in \mathcal{DP}$ such that $p \rightsquigarrow u_i$ and $s \rightsquigarrow l_i$. Moreover, from the definition of R (more precisely from the definition of β) it follows that $M_i = [u_i]_{R_1} + [l_i]_{R_2}$. Then from Proposition 22 we have:
   $\mu(p+s, M_i) = \mu(p+s, [u_i + l_i]_\beta) = \mu(p, [u_i]_{R_1})\mu(s, [l_i]_{R_2}) = \mu(q, [u_i]_{R_1})\mu(t, [l_i]_{R_2}) =$
   $\mu(q+t, [u_i + l_i]_\beta) = \mu(q+t, M_i)$
   and from Corollary 21:
   $\mu(p+s, M) = \sum\limits_{i \in I} \mu(p+s, M_i) = \sum\limits_{i \in I} \mu(q+t, M_i) = \mu(q+t, M)$.

With respect to $\uplus_\pi$: Let x, y, z and w be $\mathcal{PR}$ terms such that $x \leftrightarrow y$ and $z \leftrightarrow w$. So there exist probabilistic bisimulations R_1 and R_2 such that xR_1y and zR_2w. We define a relation R in the following way:

$R = Eq(\alpha \cup R_1 \cup R_2)$,
where

$\alpha = \{(p +\!\!\!+_{\pi} s, q +\!\!\!+_{\pi} t) \ : \ p, q, s, t \in \mathcal{SP}, pR_1q, sR_2t\}$.

Suppose $(p +\!\!\!+_{\pi} s)R(q +\!\!\!+_{\pi} t)$ for some $p, q, s, t \in \mathcal{SP}$ such that pR_1q, sR_2t and $p +\!\!\!+_{\pi} s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that either $p \rightsquigarrow u$ or $s \rightsquigarrow u$. In the first case we obtain that $q \rightsquigarrow v$ for some $v \in \mathcal{DP}$ such that uR_1v and also $q +\!\!\!+_{\pi} t \rightsquigarrow v$ and uRv. In the second case it follows that $t \rightsquigarrow v$ for some $v \in \mathcal{DP}$ such that uR_2v and also $q +\!\!\!+_{\pi} t \rightsquigarrow v$ and uRv.

We proved that whenever $p +\!\!\!+_{\pi} s \rightsquigarrow u$ for some $u \in \mathcal{DP}$ there exists $v \in \mathcal{DP}$ such that $q +\!\!\!+_{\pi} t \rightsquigarrow v$ and uRv.

Suppose rRr_1 for some $r, r_1 \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, (M \subseteq \mathcal{DP})$. We have to consider the following cases:

1. If $rR_kr_1, k = 1, 2$, then in a similar way as in (**) the property can be proved.
2. If $r\alpha r_1$, then $r \equiv p +\!\!\!+_{\pi} s$ and $r_1 \equiv q +\!\!\!+_{\pi} t$ for some $p, q, s, t \in \mathcal{SP}$ such that pR_1q and sR_2t. From Corollary 15 we have:

$$\mu(p +\!\!\!+_{\pi} s, M) = \pi\mu(p, M) + (1 - \pi)\mu(s, M) \tag{3}$$

and $M = \bigcup\limits_{i \in I_1} M_{i1} = \bigcup\limits_{j \in I_2} M_{j2}$ $(I_1 \neq \emptyset,\ I_2 \neq \emptyset)$ for some equivalence classes $M_{i1} \in \mathcal{PR}/R_1$ and $M_{j2} \in \mathcal{PR}/R_2$. Using Corollary 21 we obtain:

$$\mu(p, M) = \sum_{i \in I_1} \mu(p, M_{i1}) = \sum_{i \in I_1} \mu(q, M_{i1}) = \mu(q, M) \text{ and}$$

$$\mu(s, M) = \sum_{j \in I_2} \mu(s, M_{j2}) = \sum_{j \in I_2} \mu(t, M_{j2}) = \mu(t, M). \tag{4}$$

From (3) and (4) we get:
$\mu(r, M) = \pi\mu(p, M) + (1 - \pi)\mu(s, M) = \pi\mu(q, M) + (1 - \pi)\mu(t, M) = \mu(r_1, M)$. □

In the proof of soundness we are faced again with the problem of equal values of the distribution function for both processes occurring in an axiom (the left side process and the right side process). Considering the bisimulation relations defined for axioms we note that in most of the cases at the same time they define a bijection on the set of processes and moreover (that is very important) if M is an equivalence class and $x \in M$ then the image of x is in M, as well. The following property gives us a possibilities to deal with the distribution function considering only the existence of such a bijection.

Proposition 31. *Let $p, q \in \mathcal{SP}$ and $M \subseteq \mathcal{DP}$ and let $'\,: M \longrightarrow M$ be a bijection such that for each $m \in M$, $\mu(p, m) = \mu(q, m')$. Then $\mu(p, M) = \mu(q, M)$.*

Proof. Using the assumption that $'\ : M \to M$ is a bijection such that for each $m \in M$, $\mu(p,m) = \mu(q,m')$ we obtain:

$$\mu(p,M) = \sum_{m\in M} \mu(p,m) = \sum_{m\in M} \mu(q,m') = \mu(q, \bigcup_{m\in M} \{m'\}) = \mu(q,M).$$

□

Theorem 32. *(Soundness) Let x and y be $\mathcal{PR}$ terms. If prBPA $\vdash x = y$ then $x \leftrightarrow y$.*

Proof. A1: We define a relation R in the following way:

$$R = Eq\Big(\{(p+q,q+p)\ :\ p,q\in\mathcal{SP}\} \cup \{(u+v,v+u)\ :\ u,v\in\mathcal{DP}\}\Big).$$

Suppose $(p+q)R(q+p)$ for some $p,q \in \mathcal{SP}$ and $p+q \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $p \rightsquigarrow u'$, $q \rightsquigarrow v'$, for some $u',v' \in \mathcal{DP}$ such that $u \equiv u'+v'$. Then also $q+p \rightsquigarrow v'+u'$ and by the definition of R we have that $(u'+v')R(v'+u')$.

Suppose $(u+v)R(v+u)$ for some $u,v \in \mathcal{DP}$ and $u+v \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then from the definition of the operational rules it follows that $u \xrightarrow{a} p$ or $v \xrightarrow{a} p$. But in each of these cases we have that $v+u \xrightarrow{a} p$. Moreover pRp.

The other direction follows from symmetry.

If $(u+v)R(v+u)$ and $a \in A$ then $u+v \xrightarrow{a} \surd$ iff $u \xrightarrow{a} \surd$ or $v \xrightarrow{a} \surd$ iff $v+u \xrightarrow{a} \surd$.

Suppose $(p+q)R(q+p)$ for some $p,q \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}$. We have the following results: $\mu(p+q,u+v) = \mu(p,u)\mu(q,v) = \mu(q,v)\mu(p,u) = \mu(q+p,v+u)$ and moreover $u+v \in M$ iff $v+u \in M$. From Proposition 31 we obtain that $\mu(p+q,M) = \mu(q+p,M)$.

A2: We define a relation R in the following way:

$$R = Eq\Big(\{((p+q)+s,p+(q+s))\ :\ p,q,s\in\mathcal{SP}\} \cup\ \{((u+v)+w,u+(v+w))\ :\ u,v,w\in\mathcal{DP}\}\Big).$$

Suppose $((p+q)+s)\,R\,(p+(q+s))$ for some $p,q,s \in \mathcal{SP}$ and $(p+q)+s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that for some $u',w'' \in \mathcal{DP}$, $p+q \rightsquigarrow u'$, $s \rightsquigarrow w''$ and $u \equiv u'+w''$. It follows also that $p \rightsquigarrow u''$ and $q \rightsquigarrow v''$ for some $u'',v'' \in \mathcal{DP}$ such that $u' \equiv u''+v''$. Then $q+s \rightsquigarrow v''+w''$ and also $p+(q+s) \rightsquigarrow u''+(v''+w'')$. By the definition of R we have that $((u''+v'')+w'')R(u''+(v''+w''))$.

Suppose $((u+v)+w)R(u+(v+w))$ for some $u,v,w \in \mathcal{DP}$ and $(u+v)+w \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then from the definition of the operational rules it follows that $u \xrightarrow{a} p$ or $v \xrightarrow{a} p$ or $w \xrightarrow{a} p$. But from that it follows that $u \xrightarrow{a} p$ or $v+w \xrightarrow{a} p$ and also $u+(v+w) \xrightarrow{a} p$. Moreover pRp.

In a similar way we can prove the other direction.

For action termination for some $a \in A$ we have: $(u+v)+w \xrightarrow{a} \surd$ iff $u+v \xrightarrow{a} \surd$ or $w \xrightarrow{a} \surd$ iff $u \xrightarrow{a} \surd$ or $v \xrightarrow{a} \surd$ or $w \xrightarrow{a} \surd$ iff $u \xrightarrow{a} \surd$ or $v+w \xrightarrow{a} \surd$ iff $u+(v+w) \xrightarrow{a} \surd$.

Suppose $((p+q)+s)\,R\,(p+(q+s))$ for some $p,q,s \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}$. For the probability distribution function we have the following result: $\mu((p+q)+s,(u+v)+w) =$

$\mu(p{+}q, u{+}v)\mu(s,w) = \mu(p,u)\mu(q,v)\mu(s,w)$ and $\mu(p{+}(q{+}s), u{+}(v{+}w)) = \mu(p,u)\mu(q{+}s, v{+}w) = \mu(p,u)\mu(q,v)\mu(s,w)$ and moreover $(u+v)+w \in M$ iff $u+(v+w) \in M$. From Proposition 31 we obtain that $\mu((p+q)+s, M) = \mu(p+(q+s), M)$.

AA3: We define a relation R in the following way:

$$R = Eq\Big(\{(a+a, a), (\breve{a}+\breve{a}, \breve{a})\}\Big).$$

We look at the transitions of both sides at the same time. Observe that they can only do $a + a \rightsquigarrow \breve{a}+\breve{a}$ and $a \rightsquigarrow \breve{a}$, respectively and $(\breve{a}+\breve{a}, \breve{a}) \in R$. Furthermore, an a–transition is the only possible action transition of $\breve{a}+\breve{a}$ and $\breve{a}$.

In order to prove that $\mu(a+a, M) = \mu(a, M)$ for each $M \in \mathcal{PR}/R$ we only need to notice that $\mu(a+a, [\breve{a}]_R) = 1 = \mu(a, [\breve{a}]_R)$, and $\mu(a+a, M) = 0 = \mu(a, M)$ for any other equivalence class M.

A4: We define a relation R in the following way:

$$R = Eq\Big(\{((p{+}q)\cdot s, p\cdot s{+}q\cdot s)) \ : \ p,q,s \in \mathcal{SP}\} \cup \{((u{+}v)\cdot s, u\cdot s{+}v\cdot s)) \ : \ u,v \in \mathcal{DP}, \ s \in \mathcal{SP}\}\Big).$$

Suppose $((p+q)\cdot s)\, R\, (p\cdot s + q\cdot s)$ for $p,q,s \in \mathcal{SP}$ and $(p+q)\cdot s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that for some $u' \in \mathcal{DP}$, $p+q \rightsquigarrow u'$ and $u \equiv u' \cdot s$. It follows also that there exist $u'', v'' \in \mathcal{DP}$ such that $p \rightsquigarrow u''$, $q \rightsquigarrow v''$ and $u' \equiv u'' + v''$. Therefore, $p\cdot s \rightsquigarrow u''\cdot s$ and $q \cdot s \rightsquigarrow v'' \cdot s$ and also $p\cdot s + q\cdot s \rightsquigarrow u''\cdot s + v''\cdot s$. Moreover $((u''+v'')\cdot s) R (u''\cdot s + v''\cdot s)$.

Suppose $p\cdot s + q\cdot s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $p\cdot s \rightsquigarrow u'$, $q\cdot s \rightsquigarrow u''$ for some $u', u'' \in \mathcal{DP}$ such that $u \equiv u' + u''$. From this we obtain that $p \rightsquigarrow v'$, $q \rightsquigarrow v''$ for some $v', v'' \in \mathcal{DP}$ such that $u' \equiv v'\cdot s$ and $u'' \equiv v''\cdot s$. Then $p+q \rightsquigarrow v'+v''$ from which $(p+q)\cdot s \rightsquigarrow (v'+v'')\cdot s$. Moreover $((v'+v'')\cdot s) R (v'\cdot s + v''\cdot s)$.

Suppose $((u+v)\cdot s) R (u\cdot s + v\cdot s)$ for $u,v \in \mathcal{DP}$ and $s \in \mathcal{SP}$, and $(u+v)\cdot s \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then one of the following situations occurs:

1. $u+v \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}$ such that $p \equiv p'\cdot s$: this means that $u \xrightarrow{a} p'$ or $v \xrightarrow{a} p'$. So, $u\cdot s \xrightarrow{a} p'\cdot s$ or $v \cdot s \xrightarrow{a} p'\cdot s$. Therefore $u\cdot s + v\cdot s \xrightarrow{a} p$. Moreover pRp.
2. $u+v \xrightarrow{a} \surd$ and $p \equiv s$: this means that $u \xrightarrow{a} \surd$ or $v \xrightarrow{a} \surd$. So, $u\cdot s \xrightarrow{a} s$ or $v\cdot s \xrightarrow{a} s$. Therefore $u\cdot s + v\cdot s \xrightarrow{a} p$. Moreover pRp.

Suppose $u\cdot s + v\cdot s \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then either $u\cdot s \xrightarrow{a} p$ or $v\cdot s \xrightarrow{a} p$. In the first case the following situations can occur:

1. $u \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}$ such that $p \equiv p'\cdot s$: then $u+v \xrightarrow{a} p'$ and also $(u+v)\cdot s \xrightarrow{a} p$. Moreover pRp.
2. $u \xrightarrow{a} \surd$ and $p \equiv s$: then $u+v \xrightarrow{a} \surd$ from which $(u+v)\cdot s \xrightarrow{a} p$. Moreover pRp.

The second case can be proved in a similar way.

Transitions of the form $(u+v)\cdot s \xrightarrow{a} \surd$ and $u\cdot s + v\cdot s \xrightarrow{a} \surd$ are not possible.

Suppose $((p+q)\cdot s)R(p\cdot s + q\cdot s)$ for some $p, q, s \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}$. Then we have $\mu((p+q)\cdot s, (u+v)\cdot s) = \mu(p+q, u+v) = \mu(p,u)\mu(q,v)$ and $\mu(p\cdot s + q\cdot s, u\cdot s + v\cdot s) = \mu(p\cdot s, u\cdot s)\mu(q\cdot s, v\cdot s) = \mu(p,u)\mu(q,v)$ and moreover $(u+v)\cdot s \in M$ iff $u\cdot s + v\cdot s \in M$. From Proposition 31 we obtain that $\mu((p+q)\cdot s, M) = \mu(p\cdot s + q\cdot s, M)$.

A5: We define a relation R in the following way:

$$R = Eq\Big(\{((p\cdot q)\cdot s, p\cdot(q\cdot s)) \;:\; p,q,s \in \mathcal{SP}\} \cup \{((u\cdot q)\cdot s, u\cdot(q\cdot s)) \;:\; u \in \mathcal{DP},\; q,s \in \mathcal{SP}\}\Big).$$

Suppose $((p\cdot q)\cdot s)R(p\cdot(q\cdot s))$ for some $p,q,s \in \mathcal{SP}$ and $(p\cdot q)\cdot s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $p\cdot q \rightsquigarrow u'$ for some $u' \in \mathcal{DP}$ such that $u \equiv u'\cdot s$ and also that $p \rightsquigarrow u''$ for some $u'' \in \mathcal{DP}$ such that $u' \equiv u''\cdot q$. Then we have $p\cdot(q\cdot s) \rightsquigarrow u''\cdot(q\cdot s)$. By the definition of R we have that $((u''\cdot q)\cdot s)R(u''\cdot(q\cdot s))$.

Suppose $p\cdot(q\cdot s) \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $p \rightsquigarrow u'$ for some $u' \in \mathcal{DP}$ such that $u \equiv u'\cdot(q\cdot s)$. Then we have $p\cdot q \rightsquigarrow u'\cdot q$ and also $(p\cdot q)\cdot s \rightsquigarrow (u'\cdot q)\cdot s$. By the definition of R we have that $((u'\cdot q)\cdot s)R(u'\cdot(q\cdot s))$.

Suppose $((u\cdot q)\cdot s)R(u\cdot(q\cdot s))$ for some $u \in \mathcal{DP}$ and $q,s \in \mathcal{SP}$ and $(u\cdot q)\cdot s \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. Then from the definition of the operational rules it follows that $u\cdot q \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}$ such that $p \equiv p'\cdot s$. One of the following situations occurs:

1. $u \xrightarrow{a} p''$ for some $p'' \in \mathcal{SP}$ such that $p' \equiv p''\cdot q$. Therefore, $u\cdot(q\cdot s) \xrightarrow{a} p''\cdot(q\cdot s)$. Moreover $((p''\cdot q)\cdot s)R(p''\cdot(q\cdot s))$.
2. $u \xrightarrow{a} \surd$, then $p' \equiv q$ and $p \equiv q\cdot s$. We have $u\cdot(q\cdot s) \xrightarrow{a} p$ and moreover pRp.

Suppose $u\cdot(q\cdot s) \xrightarrow{a} p$, for some $a \in A$ and $p \in \mathcal{SP}$. One of the following situations occurs:

1. $u \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}$ such that $p \equiv p'\cdot(q\cdot s)$. Then $u\cdot q \xrightarrow{a} p'\cdot q$ and also $(u\cdot q)\cdot s \xrightarrow{a} (p'\cdot q)\cdot s$. Moreover $((p'\cdot q)\cdot s)R(p'\cdot(q\cdot s))$.
2. $u \xrightarrow{a} \surd$, then $p \equiv q\cdot s$. We have $u\cdot q \xrightarrow{a} q$ and also $(u\cdot q)\cdot s \xrightarrow{a} p$. Moreover pRp.

Transitions of the form $(u\cdot q)\cdot s \xrightarrow{a} \surd$ and $u\cdot(q\cdot s) \xrightarrow{a} \surd$ cannot occur.

Suppose $((p\cdot q)\cdot s)R(p\cdot(q\cdot s))$ for some $p,q,s \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}$. Then we have $\mu((p\cdot q)\cdot s, (u\cdot q)\cdot s) = \mu(p\cdot q, u\cdot q) = \mu(p,u)$ and $\mu(p\cdot(q\cdot s), u\cdot(q\cdot s)) = \mu(p,u)$ and moreover $(u\cdot q)\cdot s \in M$ iff $u\cdot(q\cdot s) \in M$. From Proposition 31 we obtain that $\mu((p\cdot q)\cdot s, M) = \mu(p\cdot(q\cdot s), M)$.

A6: We define a relation R in the following way:

$$R = Eq\Big(\{(p+\delta, p) \;:\; p \in \mathcal{SP}\} \;\cup\; \{(u+\breve{\delta}, u) \;:\; u \in \mathcal{DP}\}\Big).$$

We look at the transitions of the both sides at the same time using the fact that the only possible transition of δ is $\delta \rightsquigarrow \breve{\delta}$. From the definition of the operational semantics we obtain $p+\delta \rightsquigarrow u+\breve{\delta}$ iff $p \rightsquigarrow u$ and moreover $(u+\breve{\delta})Ru$.

And also $\mu(p+\delta, u+\breve{\delta}) = \mu(p,u)\mu(\delta,\breve{\delta}) = \mu(p,u)$ and as $u+\breve{\delta} \in M$ iff $u \in M$ from Proposition 31 it follows that $\mu(p+\delta, M) = \mu(p, M)$ for each $M \in \mathcal{PR}/R$.

A7: We define a relation R in the following way:

$$R = Eq\Big(\{(\delta \cdot p, \delta) \ : \ p \in \mathcal{SP}\} \ \cup \ \{(\breve{\delta} \cdot p, \breve{\delta}) \ : \ p \in \mathcal{SP}\}\Big).$$

We look at the transitions of the both sides at the same time. Observe that $\delta \cdot p$ and δ can only do a probabilistic transition to $\breve{\delta} \cdot p$ and $\breve{\delta}$, respectively, and $(\breve{\delta} \cdot p, \breve{\delta}) \in R$. Moreover, $\mu(\delta \cdot p, \breve{\delta} \cdot p) = \mu(\delta, \breve{\delta}) = 1$. Then we obtain $\mu(\delta \cdot p, [\breve{\delta}]_R) = \mu(\delta, [\breve{\delta}]_R) = 1$ and for any other $M \in \mathcal{PR}/R$ $\mu(\delta \cdot p, M) = \mu(\delta, M) = 0$.

PrAC1: We define a relation R in the following way:

$$R = Eq\Big(\{(p \boxplus_\pi q, q \boxplus_{1-\pi} p) \ : \ p, q \in \mathcal{SP}\}\Big).$$

Suppose $(p \boxplus_\pi q)\, R\, (q \boxplus_{1-\pi} p)$ for some $p, q \in \mathcal{SP}$ and $p \boxplus_\pi q \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that either $p \rightsquigarrow u$ or $q \rightsquigarrow u$. In each of these cases we have $q \boxplus_{1-\pi} p \rightsquigarrow u$ and moreover uRu.

Suppose $(p \boxplus_\pi q) R (q \boxplus_{1-\pi} p)$ for some $p, q \in \mathcal{SP}$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}$. From Corollary 15 we obtain $\mu(p \boxplus_\pi q, M) = \pi\mu(p, M) + (1-\pi)\mu(q, M) = (1-\pi)\mu(q, M) + (1-(1-\pi))\mu(p, M) = \mu(q \boxplus_{1-\pi} p, M)$.

PrAC2: We define a relation R in the following way:

$$R = Eq\Big(\{(p \boxplus_\pi (q \boxplus_\rho s), (p \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} q) \boxplus_{\pi+\rho-\pi\rho} s) \ : \ p, q, s \in \mathcal{SP}\}\Big).$$

Suppose $(p \boxplus_\pi (q \boxplus_\rho s))\, R \left((p \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} q) \boxplus_{\pi+\rho-\pi\rho} s\right)$ for some $p, q, s \in \mathcal{SP}$ and $p \boxplus_\pi (q \boxplus_\rho s) \rightsquigarrow u$ for some $u \in \mathcal{DP}$. From the definition of the operational semantics it follows that $p \rightsquigarrow u$ or $q \boxplus_\rho s \rightsquigarrow u$ and also $p \rightsquigarrow u$ or $q \rightsquigarrow u$ or $s \rightsquigarrow u$. In each of these cases we have that $\left((p \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} q) \boxplus_{\pi+\rho-\pi\rho} s\right) \rightsquigarrow u$.

In a similar way it can be proved that if $(p \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} q) \boxplus_{\pi+\rho-\pi\rho} s \rightsquigarrow u$ for some $u \in \mathcal{DP}$ then $p \boxplus_\pi (q \boxplus_\rho s) \rightsquigarrow u$.

Suppose $M \in \mathcal{PR}/R$, $M \subseteq \mathcal{DP}$. From Corollary 15 we obtain:

$$\begin{aligned}
\mu(p \boxplus_\pi (q \boxplus_\rho s), M) &= \pi\mu(p, M) + (1-\pi)\mu(q \boxplus_\rho s, M) \\
&= \pi\mu(p, M) + (1-\pi)(\rho\mu(q, M) + (1-\rho)\mu(s, M)) \\
&= \pi\mu(p, M) + (1-\pi)\rho\mu(q, M) + (1-\pi)(1-\rho)\mu(s, M)
\end{aligned}$$

and

$$\begin{aligned}
\mu\left(\left(p \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} q\right) \boxplus_{\pi+\rho-\pi\rho} s, M\right) &= (\pi+\rho-\pi\rho)\mu\left(p \boxplus_{\frac{\pi}{\pi+\rho-\pi\rho}} q, M\right) + (1-(\pi+\rho-\pi\rho))\mu(s, M) \\
&= \pi\mu(p, M) + (1-\pi)\rho\mu(q, M) + (1-\pi)(1-\rho)\mu(s, M).
\end{aligned}$$

PrAC3: We define a relation R in the following way:

$$R = Eq\Big(\{(p \boxplus_\pi p, p) \ : \ p \in \mathcal{SP}\}\Big).$$

From the definition of the deduction rules it follows that $p \uplus_\pi p \rightsquigarrow u$ for some $u \in \mathcal{DP}$ iff $p \rightsquigarrow u$. Moreover uRu.

From Corollary 15 for each $M \in \mathcal{PR}/R$, $M \subseteq \mathcal{DP}$ we obtain
$\mu(p \uplus_\pi p, M) = \pi\mu(p, M) + (1-\pi)\mu(p, M) = \mu(p, M)$.

PrAC4: We define a relation R in the following way:

$$R = Eq\Big(\{((p \uplus_\pi q)\cdot s, p\cdot s \uplus_\pi q \cdot s) \ : \ p, q, s \in \mathcal{SP}\}\Big).$$

Suppose $((p \uplus_\pi q)\cdot s)\, R\, (p \cdot s \uplus_\pi q \cdot s)$ for some $p, q, s \in \mathcal{SP}$ and $(p \uplus_\pi q)\cdot s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules we have $p \uplus_\pi q \rightsquigarrow u'$ for some $u' \in \mathcal{DP}$ such that $u \equiv u' \cdot s$ which implies either $p \rightsquigarrow u'$ or $q \rightsquigarrow u'$. In the first case it follows $p \cdot s \rightsquigarrow u$, in the second $q \cdot s \rightsquigarrow u$, and in both cases we obtain that $p \cdot s \uplus_\pi q \cdot s \rightsquigarrow u$.

Suppose $p \cdot s \uplus_\pi q \cdot s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then either $p \cdot s \rightsquigarrow u$ or $q \cdot s \rightsquigarrow u$. From the definition of the operational rules it follows that for some $u' \in \mathcal{DP}$ such that $u \equiv u' \cdot s$, $p \rightsquigarrow u'$ or $q \rightsquigarrow u'$. In each of these cases using the deduction rules we obtain $(p \uplus_\pi q) \cdot s \rightsquigarrow u$.

Suppose $M \in \mathcal{PR}/R$, $M \subseteq \mathcal{DP}$. From the definition of the probability distribution function we obtain:

$\mu((p \uplus_\pi q)\cdot s, u' \cdot s) = \mu(p \uplus_\pi q, u') = \pi\mu(p, u') + (1-\pi)\mu(q, u')$ and
$\mu(p \cdot s \uplus_\pi q \cdot s, u' \cdot s) = \pi\mu(p \cdot s, u' \cdot s) + (1-\pi)\mu(q \cdot s, u' \cdot s) = \pi\mu(p, u') + (1-\pi)\mu(q, u')$.
Then from Proposition 31 we obtain $\mu((p \uplus_\pi q)\cdot s, M) = \mu(p \cdot s \uplus_\pi q \cdot s, M)$.

PrAC5: We define a relation R in the following way:

$$R = Eq\Big(\{((p \uplus_\pi q) + s, p + s \uplus_\pi q + s) \ : \ p, q, s \in \mathcal{SP}\}\Big).$$

Suppose $((p \uplus_\pi q) + s)\, R\, (p + s \uplus_\pi q + s)$ for some $p, q, s \in \mathcal{SP}$ and $(p \uplus_\pi q) + s \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules we have $p \uplus_\pi q \rightsquigarrow u'$ and $s \rightsquigarrow u''$ for some $u', u'' \in \mathcal{DP}$ such that $u \equiv u' + u''$ and also $p \rightsquigarrow u'$ or $q \rightsquigarrow u'$. Then we obtain $p + s \rightsquigarrow u' + u''$ or $q + s \rightsquigarrow u' + u''$ from which using the definition of the operational semantics we obtain $p + s \uplus_\pi q + s \rightsquigarrow u$.

Suppose $(p + s) \uplus_\pi (q + s) \rightsquigarrow u$ for some $u \in \mathcal{DP}$. From the definition of the operational semantics we have that either $p + s \rightsquigarrow u$ or $q + s \rightsquigarrow u$. In the first case it follows that $p \rightsquigarrow u'$ and $s \rightsquigarrow u''$ for some $u', u'' \in \mathcal{DP}$ such that $u \equiv u' + u''$. Then $p \uplus_\pi q \rightsquigarrow u'$ and $(p \uplus_\pi q) + s \rightsquigarrow u$. Moreover uRu. In the second case we obtain $q \rightsquigarrow u'$ and $s \rightsquigarrow u''$ for some $u', u'' \in \mathcal{DP}$ such that $u \equiv u' + u''$. Then $p \uplus_\pi q \rightsquigarrow u'$ and $(p \uplus_\pi q) + s \rightsquigarrow u$ and uRu.

Suppose $M \in \mathcal{PR}/R$, $M \subseteq \mathcal{DP}$. Then from the definition of the probability distribution function we obtain:

$\mu((p \uplus_\pi q) + s, u + w) = \mu(p \uplus_\pi q, u)\mu(s, w) = (\pi\mu(p, u) + (1-\pi)\mu(q, u))\mu(s, w)$ and

$$\begin{aligned}\mu(p + s \uplus_\pi q + s, u + w) &= \pi\mu(p + s, u + w) + (1-\pi)\mu(q + s, u + w)\\ &= \pi\mu(p, u)\mu(s, w) + (1-\pi)\mu(q, u)\mu(s, w).\end{aligned}$$

From Proposition 31 we obtain $\mu((p \uplus_\pi q) + s, M) = \mu(p + s \uplus_\pi q + s, M)$. □

2.3 Completeness of *prBPA*

To prove completeness for *prBPA* with respect to presented term model, we use the direct method. In order to do this, we first derive some results which relate a certain transition in the model with a certain equality in the algebra. As the Completeness theorem is proved by induction on the number of symbols in closed terms, the following propositions give a way of handling it. Further by $op(x)$ we denote the number of operators of closed term x, defined in the standard way.

Proposition33: *Let x be a closed prBPA term and $a \in A$. Then:*

i. if $x \rightsquigarrow \breve{x}'$ and $\pi = \mu(x, \breve{x}')$ then $\pi = 1$ and $x = x'$ and $op(x') \leq op(x)$ or $\pi < 1$ and $x = x' \uplus_{\pi} y$ for some $y \in \mathcal{SP}$;

ii. if $\breve{x} \xrightarrow{a} \surd$ then $x = a + x$;

iii. if $\breve{x} \xrightarrow{a} x'$ then $x = a \cdot x' + x$.

Proof. i. Let x be a closed *prBPA* term and $x \rightsquigarrow \breve{x}'$ for some $\breve{x}' \in \mathcal{DP}$ and $\pi = \mu(x, \breve{x}')$. The proof is given by case distinction on the structure of x.

1. $x \equiv \delta$ or $x \equiv a$: then $x \rightsquigarrow \breve{x}$ is the only possible transition and $\mu(x, \breve{x}) = 1$. Therefore the conclusion holds;
2. $x \equiv y \cdot z$ for some closed terms y and z: the assumption $y \cdot z \rightsquigarrow \breve{x}'$ implies $y \rightsquigarrow \breve{y}'$ for some $\breve{y}' \in \mathcal{DP}$ such that $x' \equiv y' \cdot z$. By the induction hypothesis we have either:

   2.1 $y = y'$ and $\mu(y, \breve{y}') = 1$ and $op(y') \leq op(y)$ from which $x = y \cdot z = y' \cdot z = x'$ and $\mu(x, \breve{x}') = \mu(y \cdot z, \breve{y}' \cdot z) = \mu(y, \breve{y}') = 1$ and $op(x') = op(y') + op(z) + 1 \leq op(y) + op(z) + 1 = op(x)$, or

   2.2 $\mu(y, \breve{y}') < 1$ and $y = y' \uplus_{\mu(y, \breve{y}')} y''$ for some $y'' \in \mathcal{SP}$ from which $\mu(x, \breve{x}') = \mu(y, \breve{y}') < 1$ and $x = y \cdot z = (y' \uplus_{\mu(y, \breve{y}')} y'') \cdot z = y' \cdot z \uplus_{\mu(y, \breve{y}')} y'' \cdot z = x' \uplus_{\mu(x, \breve{x}')} x''$;
3. $x \equiv y + z$ for certain closed terms y and z: by the assumption $y + z \rightsquigarrow \breve{x}'$ we have $y \rightsquigarrow \breve{y}'$, $z \rightsquigarrow \breve{z}'$ for some $\breve{y}', \breve{z}' \in \mathcal{DP}$ such that $x' \equiv y' + z'$. From the definition of the probability distribution function we obtain $\mu(x, \breve{x}') = \mu(y + z, \breve{y}' + \breve{z}') = \mu(y, \breve{y}')\mu(z, \breve{z}')$. (*)
   By the induction hypothesis we have:

   3.1 $y = y'$, $\mu(y, \breve{y}') = 1$ and $op(y') \leq op(y)$ and $z = z'$ and $\mu(z, \breve{z}') = 1$ and $op(z') \leq op(z)$: then from (*) we have $\mu(x, \breve{x}') = 1$ and $op(x') = op(y') + op(z') + 1 \leq op(y) + op(z) + 1 = op(x)$ and $x = y + z = y' + z' = x'$, or

   3.2 $y = y'$, $\mu(y, \breve{y}') = 1$, $op(y') \leq op(y)$ and $\mu(z, \breve{z}') < 1$ and $z = z' \uplus_{\mu(z, \breve{z}')} z''$ for some $z'' \in \mathcal{SP}$: then from (*) we obtain $\mu(x, \breve{x}') = \mu(z, \breve{z}') < 1$ and
   $x = y + z = y' + (z' \uplus_{\mu(z, \breve{z}')} z'') = (y' + z') \uplus_{\mu(z, \breve{z}')} (y' + z'') = x' \uplus_{\mu(z, \breve{z}')} (y' + z'') = x' \uplus_{\mu(x, \breve{x}')} (y' + z'')$, or

   3.3 $\mu(y, \breve{y}') < 1$ and $y = y' \uplus_{\mu(y, \breve{y}')} y''$ and $z = z'$, $\mu(z, \breve{z}') = 1$ and $op(z') \leq op(z)$ for some $y'' \in \mathcal{SP}$: this case is similar to the previous one, or

3.4 $\mu(y,\breve{y}') < 1$ and $y = y' \uplus_{\mu(y,\breve{y}')} y''$ and $\mu(z,\breve{z}') < 1$ and $z = z' \uplus_{\mu(z,\breve{z}')} z''$ for some $y'', z'' \in \mathcal{SP}$: then $\mu(x,\breve{x}') = \mu(y,\breve{y}')\mu(z,\breve{z}') < 1$ and

$$\begin{aligned} x = y + z &= (y' \uplus_{\mu(y,\breve{y}')} y'') + (z' \uplus_{\mu(z,\breve{z}')} z'') \\ &= (y' + (z' \uplus_{\mu(z,\breve{z}')} z'')) \uplus_{\mu(y,\breve{y}')} (y'' + (z' \uplus_{\mu(z,\breve{z}')} z'')) \\ &= ((y' + z') \uplus_{\mu(z,\breve{z}')} (y' + z'')) \uplus_{\mu(y,\breve{y}')} (y'' + (z' \uplus_{\mu(z,\breve{z}')} z'')) \\ &= (y' + z') \uplus_{\mu(y,\breve{y}')\mu(z,\breve{z}')} ((y' + z'') \uplus_{\alpha} (y'' + (z' \uplus_{\mu(z,\breve{z}')} z''))) = x' \uplus_{\mu(x,\breve{x}')} x'' \end{aligned}$$

with $\alpha \in \langle 0,1 \rangle$ determined by axiom $PrAC2'$ and $x'' \equiv (y' + z'') \uplus_{\alpha} (y'' + (z' \uplus_{\mu(z,\breve{z}')} z''))$;

4. $x \equiv y \uplus_{\alpha} z$ for certain closed terms y and z and $\alpha \in \langle 0,1 \rangle$: for the probability distribution function we have $\mu(x,\breve{x}') = \alpha\mu(y,\breve{x}') + (1-\alpha)\mu(z,\breve{x}')$. (Δ)

From the assumption $y \uplus_{\alpha} z \rightsquigarrow \breve{x}'$ using the definition of the operational semantics we obtain that one of the following cases can occur:

4.1 $y \rightsquigarrow \breve{x}'$ and $\neg(z \rightsquigarrow \breve{x}')$ which implies $\mu(z,\breve{x}') = 0$. Then by the induction hypothesis we have:

(a) $y = x'$ and $\mu(y,\breve{x}') = 1$ and $op(x') \leq op(y)$: then from (Δ) we have $\mu(x,\breve{x}') = \alpha < 1$ and $x = y \uplus_{\alpha} z = x' \uplus_{\mu(x,\breve{x}')} z$ and $op(x') \leq op(y) < op(x)$, or

(b) $\mu(y,\breve{x}') < 1$ and $y = x' \uplus_{\mu(y,\breve{x}')} y'$ for some $y' \in \mathcal{SP}$: then $\mu(x,\breve{x}') = \alpha\mu(y,\breve{x}') < 1$ and $x = y \uplus_{\alpha} z = (x' \uplus_{\mu(y,\breve{x}')} y') \uplus_{\alpha} z = x' \uplus_{\alpha\mu(y,\breve{x}')} (y' \uplus_{\zeta} z) = x' \uplus_{\mu(x,\breve{x}')} x''$ where $x'' \equiv y' \uplus_{\zeta} z$ and ζ is determined by axiom $\vec{P}rAC2'$;

4.2 $z \rightsquigarrow \breve{x}'$ and $\neg(y \rightsquigarrow \breve{x}')$. This case is similar to the previous one;

4.3 $y \rightsquigarrow \breve{x}'$ and $z \rightsquigarrow \breve{x}'$. Then by the induction hypothesis we have:

(a) $y = x'$, $\mu(y,\breve{x}') = 1$ and $op(x') \leq op(y)$ and $z = x'$ and $\mu(z,\breve{x}') = 1$ and $op(x') \leq op(z)$: then from (Δ) it follows $\mu(x,\breve{x}') = 1$ and $op(x') \leq op(y) + op(z) + 1 = op(x)$ and $x = y \uplus_{\alpha} z = x' \uplus_{\alpha} x' = x'$, or

(b) $y = x'$, $\mu(y,\breve{x}') = 1$ and $op(x') \leq op(y)$ and $\mu(z,\breve{x}') < 1$ and $z = x' \uplus_{\mu(z,\breve{x}')} z'$ for some $z' \in \mathcal{SP}$: then from (Δ) we have $\mu(x,\breve{x}') = \alpha + (1-\alpha)\mu(z,\breve{x}') < 1$ and $x = y \uplus_{\alpha} z = x' \uplus_{\alpha} (x' \uplus_{\mu(z,\breve{x}')} z') = (x' \uplus_{\frac{\alpha}{\alpha+\mu(z,\breve{x}')-\alpha\mu(z,\breve{x}')}} x') \uplus_{\alpha+\mu(z,\breve{x}')-\alpha\mu(z,\breve{x}')} z' = x' \uplus_{\mu(x,\breve{x}')} z'$, or

(c) $\mu(y,\breve{x}') < 1$ and $y = x' \uplus_{\mu(y,\breve{x}')} y'$ for some $y' \in \mathcal{SP}$ and $z = x'$ and $\mu(z,\breve{x}') = 1$ and $op(x') \leq op(z)$: then from (Δ) we obtain $\mu(x,\breve{x}') = \alpha\mu(y,\breve{x}') + (1-\alpha) < 1$ and if we denote shortly $\beta = \mu(y,\breve{x}')$ we have
$x = y \uplus_{\alpha} z = (x' \uplus_{\beta} y') \uplus_{\alpha} x' = x' \uplus_{\alpha\beta} \left(x' \uplus_{\frac{1-\alpha}{1-\alpha\beta}} y'\right) =$
$x' \uplus_{(\alpha\beta + \frac{1-\alpha}{1-\alpha\beta} - \alpha\beta\frac{1-\alpha}{1-\alpha\beta})} y' = x' \uplus_{\alpha\beta+(1-\alpha)} y' = x' \uplus_{\mu(x,\breve{x}')} y'$, or

(d) $\mu(y,\breve{x}') < 1$ and $y = x' \uplus_{\mu(y,\breve{x}')} y'$ and $\mu(z,\breve{x}') < 1$ and $z = x' \uplus_{\mu(z,\breve{x}')} z'$ for some $y', z' \in \mathcal{SP}$: then we have $\mu(x,\breve{x}') = \alpha\mu(y,\breve{x}') + (1-\alpha)\mu(z,\breve{x}') < 1$ and if we denote shortly $\beta = \mu(y,\breve{x}')$ and $\zeta = \mu(z,\breve{x}')$ we obtain
$x = y \uplus_{\alpha} z = (x' \uplus_{\beta} y') \uplus_{\alpha} (x' \uplus_{\zeta} z') = x' \uplus_{\alpha\beta} \left[y' \uplus_{\frac{(1-\beta)\alpha}{1-\alpha\beta}} (x' \uplus_{\zeta} z')\right] =$

$$x' \boxplus_{\alpha\beta} \left[\left(x' \boxplus_{\frac{(1-\alpha)\zeta}{\alpha(1-\beta)+\zeta(1-\alpha)}} y' \right) \boxplus_{\frac{(1-\beta)\alpha+(1-\alpha)\zeta}{1-\alpha\beta}} z' \right] = x' \boxplus_{\eta} (y' \boxplus_{\tau} z')$$

for some $\tau \in \langle 0, 1 \rangle$ and where $\eta = \alpha\mu(y, \breve{x}') + \frac{\mu(z,\breve{x}')(1-\alpha)}{1-\alpha\mu(y,\breve{x}')} - \frac{\alpha\mu(y,\breve{x}')\mu(z,\breve{x}')(1-\alpha)}{1-\alpha\mu(y,\breve{x}')} = \alpha\mu(y, \breve{x}') + (1-\alpha)\mu(z, \breve{x}')$. So, we have:

$$x = x' \boxplus_{\eta} (y' \boxplus_{\tau} z') = x' \boxplus_{(\alpha\mu(y,\breve{x}')+\mu(z,\breve{x}')(1-\alpha))} (y' \boxplus_{\tau} z') = x' \boxplus_{\mu(x,\breve{x}')} (y' \boxplus_{\tau} z').$$

ii. Let us suppose that $\breve{x} \xrightarrow{a} \surd$. The proof is given by induction on x.

1. $x \equiv \delta$: this case is not possible;
2. $x \equiv a$: then $x = a + a = a + x$;
3. $x \equiv x' \cdot x''$ for some closed *prBPA* terms x' and x'': then an a−transition to $\surd$ is not possible;
4. $x \equiv x' + x''$ for some closed *prBPA* terms x' and x'': then from the assumption $\breve{x} \xrightarrow{a} \surd$ we have that $\breve{x}' \xrightarrow{a} \surd$ or $\breve{x}'' \xrightarrow{a} \surd$. By the induction hypothesis we have that $x' = a + x'$ or $x'' = a + x''$ but in each of these cases we have $x = x' + x'' = a + x' + x'' = a + x$.

iii. Let us suppose that $\breve{x} \xrightarrow{a} y$ for some $y \in \mathcal{SP}$. The proof is given by induction on x.

1. $x \equiv \delta$ or $x \equiv a$: these cases are not possible;
2. $x \equiv x' \cdot x''$ for some closed *prBPA* terms x' and x'': then one of the following situations is possible:
   2.1 $\breve{x}' \xrightarrow{a} y'$ for some $y' \in \mathcal{SP}$ such that $y \equiv y' \cdot x''$: then by the induction hypothesis we have that $x' = a \cdot y' + x'$ from which $x = (a \cdot y' + x') \cdot x'' = a \cdot y' \cdot x'' + x' \cdot x'' = a \cdot y + x$;
   2.2 $\breve{x}' \xrightarrow{a} \surd$ and $y \equiv x''$: then by *ii.* we have that $x' = a + x'$ from which we obtain: $x = (a + x') \cdot x'' = a \cdot x'' + x' \cdot x'' = a \cdot y + x$;
3. $x \equiv x' + x''$ for some closed *prBPA* terms x' and x'': then from the assumption $\breve{x} \xrightarrow{a} y$ we have that $\breve{x}' \xrightarrow{a} y$ or $\breve{x}'' \xrightarrow{a} y$. By the induction hypothesis we have that $x' = a \cdot y + x'$ or $x'' = a \cdot y + x''$ but in each case we have $x = x' + x'' = a \cdot y + x' + x'' = a \cdot y + x$. □

Proposition 34. *Let x and y be* **D** *terms. Then the following equivalence holds:*

$$x \leftrightarroweq y \Leftrightarrow \breve{x} \leftrightarroweq \breve{y}.$$

Proof. This result follows from Proposition 25. □

The next proposition particularises a relation between a probabilistic transitions of a basic term and its form as it was considered in Section 2.1. Here we are faced with the following situation. If a process, say p, can do a probabilistic transition to a dynamic process $\breve{x}$ with certain probability $\mu(p, \breve{x}) = \pi$, then the associated process term x may appear more than once as a sub-term of process term p in such a way that the sum of all probabilities related to x is equal to π. According to the forms of basic terms in the remark on p. 8 we use an auxiliary set Q_x which contains all indexes of sub-terms of p that are syntactically equal to x. It is clear that the set $\{Q_x \ : \ x \text{ is a sub-term of } p\}$ is a partition of the set $\{1, 2, \ldots, n\}$ as it is given in that remark.

Proposition 35. *If p is a basic prBPA term in the form (2) (Remark p. 8), then $p \rightsquigarrow x$ with $\mu(p,x) = \rho$ iff $x \equiv x_i$ and $\rho = \sum_{j \in Q_{x_i}} \pi_j$ for some i, $1 \leq i \leq n$, where $Q_{x_i} = \{j \ : \ 1 \leq j \leq n, x_i \equiv x_j\}$ and $\pi_n = 1 - \sum_{j=1}^{n-1} \pi_j$.*

Proof. Let p be a basic term in the form $p \equiv x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} x_3 \ldots x_{n-1} \uplus_{\pi_{n-1}} x_n$, for $n \geq 2$. The proof is given by induction on n. Instead of Q_{x_i} we shortly write Q_i.

($\Leftarrow$) Let $n = 2$, that is $p \equiv x_1 \uplus_{\pi_1} x_2$. Then by Proposition 25 we have that the only possible probabilistic transition of x_1 and x_2 is $x_1 \rightsquigarrow \breve{x}_1$ and $x_2 \rightsquigarrow \breve{x}_2$, respectively, with $\mu(x_1, \breve{x}_1) = 1$ and $\mu(x_2, \breve{x}_2) = 1$. From Corollary 26 and the definition of the operational rules we obtain

1. if $x_1 \not\equiv x_2$ then $p \rightsquigarrow \breve{x}_1$ and $p \rightsquigarrow \breve{x}_2$ with $\mu(p, \breve{x}_1) = \pi_1$ and $\mu(p, \breve{x}_2) = 1 - \pi_1$ and the result holds because $Q_1 = \{1\}$ and $Q_2 = \{2\}$;
2. if $x_1 \equiv x_2$ then $Q_1 = Q_2 = \{1, 2\}$ and $\sum_{j \in Q_1} \pi_j = 1$ and we obtain $p \rightsquigarrow \breve{x}_1$ with $\mu(p, \breve{x}_1) = \pi + (1 - \pi) = 1$.

Let $p \equiv x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{n-1}} x_n \equiv x_1 \uplus_{\pi_1} (x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n)$ for $n \geq 3$. From Proposition 25 it follows that the only possible probabilistic transition of x_1 is $x_1 \rightsquigarrow \breve{x}_1$ and $\mu(x_1, \breve{x}_1) = 1$ and from the induction hypothesis we have that for k, $2 \leq k \leq n$, $q \rightsquigarrow \breve{x}_k$ and $\mu(q, \breve{x}_k) = \rho'_k$ where $\rho'_k = \sum_{j \in Q'_k} \frac{\pi_j}{1-\pi_1}$ and $Q'_k = \{j \ : \ 2 \leq j \leq n, x_k \equiv x_j\}$ and $q \equiv x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n$. Combining these two results we obtain the following:

1. if there exists k, $2 \leq k \leq n$, such that $x_1 \equiv x_k$ then $Q_1 = Q'_k \cup \{1\}$ and $p \rightsquigarrow \breve{x}_1$ and $\mu(p, \breve{x}_1) = \pi_1 + (1 - \pi_1)\rho'_k = \rho_k$, where $\rho_k = \sum_{j \in Q_1} \pi_j$. Moreover for all l, $2 \leq l \leq n$, such that $x_1 \not\equiv x_l$ we have that $Q_l = Q'_l$ and from the definition of the operational rules we obtain $p \rightsquigarrow \breve{x}_l$ and $\mu(p, \breve{x}_l) = (1 - \pi_1)\rho'_l = \rho_l$ where $\rho_l = \sum_{j \in Q_l} \pi_j$;
2. if $x_1 \not\equiv x_k$ for each k, $2 \leq k \leq n$, then $Q'_k = Q_k$ and $Q_1 = \{1\}$. From the definition of the operational rules we have $p \rightsquigarrow \breve{x}_1$ and $p \rightsquigarrow \breve{x}_k$ with $\mu(p, \breve{x}_1) = \pi_1$ and $\mu(p, \breve{x}_k) = (1 - \pi_1)\rho'_k = \rho_k$ where $\rho_k = \sum_{j \in Q_k} \pi_j$.

($\Rightarrow$) Let $n = 2$, that is $p \equiv x_1 \uplus_{\pi_1} x_2$ and $p \rightsquigarrow \breve{x}$ for some $\breve{x} \in \mathcal{DP}$ which implies $\mu(p, \breve{x}) \in (0, 1]$. From the definition of the operational rules we have that one of the following cases occurs:

1. $x_1 \rightsquigarrow \breve{x}$ and $\neg(x_2 \rightsquigarrow \breve{x})$ which implies $\mu(x_2, \breve{x}) = 0$ and $\mu(p, \breve{x}) = \pi_1 \mu(x_1, \breve{x})$. Then by Proposition 25 we have that $\mu(x_1, \breve{x}) = 1$ and $x_1 \equiv x$. Using Corollary 26 we obtain $x_1 \not\equiv x_2$. This means that $Q_1 = \{1\}$ and $\mu(p, \breve{x}) = \sum_{j \in Q_1} \pi_j$;
2. $x_2 \rightsquigarrow \breve{x}$ and $\neg(x_1 \rightsquigarrow \breve{x})$ which implies $\mu(x_1, \breve{x}) = 0$ and $\mu(p, \breve{x}) = (1 - \pi_1)\mu(x_2, \breve{x})$. In a similar way as in the first case we obtain that $\mu(x_2, \breve{x}) = 1$ and $x_2 \equiv x$ and $\mu(p, \breve{x}) = \sum_{j \in Q_2} \pi_j$.

3. $x_1 \rightsquigarrow \breve{x}$ and $x_2 \rightsquigarrow \breve{x}$ and then $\mu(p,\breve{x}) = \pi_1\mu(x_1,\breve{x}) + (1-\pi_1)\mu(x_2,\breve{x})$. By Proposition 25 it follows $\mu(x_1,\breve{x}) = 1$, $x \equiv x_1$ and $\mu(x_2,\breve{x}) = 1$ and $x \equiv x_2$ from which we obtain $Q_1 = Q_2 = \{1,2\}$ and $\mu(p,\breve{x}) = \sum\limits_{j\in Q_1} \pi_j = 1$.

Let $p \equiv x_1 \uplus_{\pi_1} x_2 \uplus_{\pi_2} \ldots \uplus_{\pi_{n-1}} x_n \equiv x_1 \uplus_{\pi_1} (x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n)$ for $n \geq 3$ and $p \rightsquigarrow \breve{x}$ for some $\breve{x} \in \mathcal{DP}$ which implies $\mu(p,\breve{x}) \in \langle 0,1]$. From the definition of operational rules one of the following situations can occur:

1. $x_1 \rightsquigarrow \breve{x}$ and $\neg(x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n \rightsquigarrow \breve{x})$ which implies $\mu(p,\breve{x}) = \pi_1\mu(x_1,\breve{y})$. Then from Proposition 25 it follows that $\mu(x_1,\breve{x}) = 1$ and $x \equiv x_1$. Moreover from the definition of the deduction rules it follows easily that $\neg(x_k \rightsquigarrow \breve{x})$ which implies $x_1 \not\equiv x_k$, for each k, $2 \leq k \leq n$. Then we obtain that $Q_1 = \{1\}$ and $\mu(p,\breve{x}) = \sum\limits_{j\in Q_1} \pi_j$.
2. $x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n \rightsquigarrow \breve{x}$ and $\neg(x_1 \rightsquigarrow \breve{x})$ which implies $\mu(x_1,\breve{x}) = 0$ and $\mu(p,\breve{x}) = (1-\pi_1)\mu(y,\breve{x})$ where $y \equiv x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n$. By the induction hypothesis it follows that there exists k, $2 \leq k \leq n$ such that $x \equiv x_k$ and $\mu(y,\breve{x}) = \sum\limits_{j\in Q'_k} \frac{\pi_j}{1-\pi_1}$ where $Q'_k = \{j \ : \ 2 \leq j \leq n, x_k \equiv x_j\}$. From $\neg(x_1 \rightsquigarrow \breve{x})$ using Corollary 26 we have that $x_1 \not\equiv x_k$, which implies $Q_k = \{j \ : \ 1 \leq j \leq n, x_k \equiv x_j\} = Q'_k$ and $\mu(p,\breve{x}) = (1-\pi_1)\mu(y,\breve{x}) = (1-\pi_1)\sum\limits_{j\in Q'_k} \frac{\pi_j}{1-\pi_1} = \sum\limits_{j\in Q_k} \pi_j$;
3. $x_1 \rightsquigarrow \breve{x}$ and $x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n \rightsquigarrow \breve{x}$ and $\mu(p,\breve{x}) = \pi_1\mu(x_1,\breve{x}) + (1-\pi_1)\mu(y,\breve{x})$, where $y \equiv x_2 \uplus_{\frac{\pi_2}{1-\pi_1}} x_3 \ldots x_{n-1} \uplus_{\frac{\pi_{n-1}}{1-\pi_1}} x_n$. From Proposition 25 it follows that $\mu(x_1,\breve{x}) = 1$ and $x \equiv x_1$. Moreover from the induction hypothesis it follows that there exists k, $2 \leq k \leq n$ such that $x \equiv x_k$ and $\mu(y,\breve{x}) = \sum\limits_{j\in Q'_k} \frac{\pi_j}{1-\pi_1}$, where $Q'_k = \{j \ : \ 2 \leq j \leq n, x_k \equiv x_j\}$. Then we obtain $x_1 \equiv x_k$ and also $Q_k = \{j \ : \ 1 \leq j \leq n, x_k \equiv x_j\} = Q'_k \cup \{1\}$ and $\mu(p,\breve{x}) = \pi_1\mu(x_1,\breve{x}) + (1-\pi_1)\mu(y,\breve{x}) = \pi_1 + (1-\pi_1)\sum\limits_{j\in Q'_k} \frac{\pi_j}{1-\pi_1} = \pi_1 + \sum\limits_{j\in Q'_k} \pi_j = \sum\limits_{j\in Q_k} \pi_j$. □

Corollary 36. *Let x be a basic prBPA term and $M \in \mathcal{PR}/\leftrightarrow$. If $x \rightsquigarrow \breve{x}_i$, $1 \leq i \leq n$, are all possible probabilistic transitions of x to elements of the equivalence class M with $\mu(x,\breve{x}_i) = \sigma_i$, for some $n \in \mathbb{N}$, $\sigma_i \in \langle 0,1]$, then either $n \geq 2$ and*

$$x \equiv x'_1 \uplus_{\rho_1} x'_2 \uplus_{\rho_2} x'_3 \ldots \uplus_{\rho_{m-1}} x'_m,$$

for some $m \in \mathbb{N}, m \geq n$ and $\rho_k \in \langle 0,1\rangle$, $1 \leq k \leq m$, ($\rho_m = 1 - \sum\limits_{j=1}^{m-1} \rho_j$), and for some partition $Q_1, Q_2, \ldots, Q_n$ of the set $\{1,2,\ldots,m\}$ such that $Q_i = \{j \ : \ 1 \leq j \leq m, x_i \equiv x'_j\}$ and $\sum\limits_{j\in Q_i} \rho_j = \sigma_i$, or

$$x \equiv x'_1 \uplus_{\rho_1} x'_2 \uplus_{\rho_2} x'_3 \ldots \uplus_{\rho_{m-1}} x'_m \uplus_{\rho_m} y$$

for some $m \in \mathbb{N}$, $m \geq 1$ and $\rho_k \in \langle 0,1\rangle$, $1 \leq k \leq m$ and for some partition $Q_1, Q_2, \ldots, Q_n$ of the set $\{1,2,\ldots,m\}$ such that $Q_i = \{j \ : \ 1 \leq j \leq m, x_i \equiv x'_j\}$ and $\sum\limits_{j\in Q_i} \rho_j = \sigma_i$ and for some *basic term y, $y \notin M$*

or

$n = 1$ and $\sigma_1 = 1$ and

$$x \equiv x_1 \sqcup\!\!\!\!+_{\rho_1} x_1 \sqcup\!\!\!\!+_{\rho_2} x_1 \ldots \sqcup\!\!\!\!+_{\rho_{m-1}} x_1,$$

for some $m \in \mathbb{N}$, $m \geq 1$ and $\rho_k \in \langle 0, 1]$, $1 \leq k \leq m$, $(\rho_m = 1 - \sum\limits_{j=1}^{m-1} \rho_j)$.

Lemma 37. *If p, q and r are $\mathcal{PR}$ terms and $\pi \in \langle 0, 1\rangle$ such that $p \sqcup\!\!\!\!+_\pi q \underline{\leftrightarrow} p \sqcup\!\!\!\!+_\pi r$, then $q \underline{\leftrightarrow} r$.*

Proof. Suppose $p \sqcup\!\!\!\!+_\pi q \underline{\leftrightarrow} p \sqcup\!\!\!\!+_\pi r$. Then there exists a bisimulation R such that $(p \sqcup\!\!\!\!+_\pi q) R (p \sqcup\!\!\!\!+_\pi r)$. We consider the following relation:

$$R' = Eq(R \cup \{(q, r)\}).$$

In order to prove that R' is a bisimulation we only need to prove that the four clauses in Definition 17 are satisfied by the pair (q, r).

At first we have the following property: for each equivalent class $M \in \mathcal{PR}/R$, $\mu(q, M) = \mu(r, M)$. It follows from the fact: $\mu(p \sqcup\!\!\!\!+_\pi q, M) = \mu(p \sqcup\!\!\!\!+_\pi r, M)$, that is $\pi\mu(p, M) + (1-\pi)\mu(q, M) = \pi\mu(p, M) + (1 - \pi)\mu(r, M)$. It implies that

$$\mu(q, M) \neq 0 \text{ iff } \mu(r, M) \neq 0. \tag{5}$$

Suppose $q \rightsquigarrow x$ for some $x \in \mathcal{DP}$, which means that $\mu(q, [x]_R) \neq 0$. By (5) we have that $\mu(r, [x]_R) \neq 0$, that is there exists $y \in \mathcal{DP}$ such that $r \rightsquigarrow y$ and xRy, which implies $xR'y$. In a similar way we obtain that if $r \rightsquigarrow y$ for some $y \in \mathcal{DP}$ then there exists $x \in \mathcal{DP}$ such that $q \rightsquigarrow x$ and $xR'y$. Moreover, for the relation R' we have that $(R' \setminus R) \cap (\mathcal{DP} \times \mathcal{DP}) = \emptyset$ which implies $\mathcal{DP}/R' = \mathcal{DP}/R$. As we only consider equivalence classes $M \subseteq \mathcal{DP}$ from these results we obtain that if $M' \in \mathcal{DP}/R'$ then $M' \in \mathcal{DP}/R$ which implies $\mu(q, M') = \mu(r, M')$. □

Lemma 38. *Let y be a $\mathbf{D}$ term and $a \in A$. Then we have:*

i. $y \underline{\leftrightarrow} \delta \Rightarrow y = \delta$;
ii. $y \underline{\leftrightarrow} a \Rightarrow y = a$.

Proof. *i.* The proof is given by induction on the structure of y.

1. $y \equiv \delta$: this case is trivial;
2. $y \equiv a$ for some $a \in A$: then $a \not\underline{\leftrightarrow} \delta$ and this case cannot occur;
3. $y \equiv y_1 \cdot y_2$ for terms $y_1 \in \mathbf{D}$ and $y_2 \in \mathcal{SP}$: then we have that $y_1 \underline{\leftrightarrow} \delta$ (this can be proved by showing that the relation $R' = Eq(R \cup \{(y_1, \delta), (\breve{y}_1, \breve{\delta})\})$ is a bisimulation, where R is a bisimulation between y and δ). Then by the induction hypothesis we have that $y_1 = \delta$ from which we obtain: $y = y_1 \cdot y_2 = \delta \cdot y_2 = \delta$;

4. $y \equiv y_1 + y_2$ for some terms $y_1, y_2 \in \mathbf{D}$: then we have that $y_1 \underline{\leftrightarrow} \delta$ and $y_2 \underline{\leftrightarrow} \delta$ (these can be proved by showing that the relation $R' = Eq(R \cup \{(y_1, \delta), (y_2, \delta), (\breve{y}_1, \breve{\delta}), (\breve{y}_2, \breve{\delta})\})$ is a bisimulation, where R is a bisimulation between y and δ). Then by the induction hypothesis we have that $y_1 = \delta$ and $y_2 = \delta$ from which we obtain: $y = y_1 + y_2 = \delta + \delta = \delta$.

ii. The proof is given by induction on the structure of y.

1. $y \equiv \delta$: then $\delta \not\underline{\leftrightarrow} a$ and this case cannot occur;
2. $y \equiv b$ for some $b \in A$: it is clear that $b \equiv a$;
3. $y \equiv y_1 \cdot y_2$ for some terms $y_1 \in \mathbf{D}$ and $y_2 \in \mathcal{SP}$: this case cannot occur;
4. $y \equiv y_1 + y_2$ for some terms $y_1, y_2 \in \mathbf{D}$: then we have that $y_1 \underline{\leftrightarrow} a$ and $y_2 \underline{\leftrightarrow} a$ (these can be proved by showing that the relation $R' = Eq(R \cup \{(y_1, a), (y_2, a), (\breve{y}_1, \breve{a}), (\breve{y}_2, \breve{a})\})$ is a bisimulation, where R is a bisimulation between y and a). Then by the induction hypothesis we have that $y_1 = a$ and $y_2 = a$ from which we obtain: $y = y_1 + y_2 = a + a = a$.

□

Theorem 39. *(Completeness) If z and u are closed prBPA terms, then $z \underline{\leftrightarrow} u \Rightarrow prBPA \vdash z = u$.*

Proof. Let us suppose that z and u are basic *prBPA* terms such that $z \underline{\leftrightarrow} u$. We give the proof using induction on the structure of z.

1. $z \equiv \delta$: then from the assumption $z \underline{\leftrightarrow} u$ it follows that there exists $\breve{u}' \in \mathcal{DP}$ such that $u \rightsquigarrow \breve{u}'$ and $\breve{u}' \underline{\leftrightarrow} \breve{\delta}$. According to Proposition 33 we have to consider two possible situations:

   1.1 $\mu(u, \breve{u}') = 1$ and $u = u'$ and $op(u') \leq op(u)$: then as $u' \in \mathbf{D}$ by Proposition 34 and Lemma 38 we have that $u' = \delta$, from which it follows that $u = \delta = z$;

   1.2 $\mu(u, \breve{u}') < 1$ and $u = u' \mathbin{+\!\!\!\!\sqcup}_{\mu(u,\breve{u}')} u''$ for some $u'' \in \mathcal{SP}$: as $\mu(u, \breve{u}') < 1$ we obtain that u can make more than one probabilistic transitions. Then by Corollary 36 we have that

   $$u \equiv u'_1 \mathbin{+\!\!\!\!\sqcup}_{\sigma_1} u'_2 \mathbin{+\!\!\!\!\sqcup}_{\sigma_2} u'_3 \ldots \mathbin{+\!\!\!\!\sqcup}_{\sigma_{n-1}} u'_n$$

   for some $n \in \mathbb{N}$, $n \geq 2$, $\sigma_i \in \langle 0, 1 \rangle$ and $u_i \in \mathcal{B}_+$ and where for each i, $1 \leq i \leq n$, $\breve{u}'_i \underline{\leftrightarrow} \breve{\delta}$. If we suppose that there exists $j, 1 \leq j \leq n$, such that $\breve{u}'_j \not\underline{\leftrightarrow} \breve{\delta}$, then it implies $u \not\underline{\leftrightarrow} \delta$ which contradicts the given assumption. This provides us with considering one form only from Corollary 36. From Proposition 34 and Lemma 38 we have that for each i, $1 \leq i \leq n$, $u'_i = \delta$ from which we obtain $u = \delta = z$.

2. $z \equiv a$: then from the assumption $z \underline{\leftrightarrow} u$ it follows that there exists $\breve{u}' \in \mathcal{DP}$ such that $u \rightsquigarrow \breve{u}'$ and $\breve{u}' \underline{\leftrightarrow} \breve{a}$. According to Proposition 33 we have to distinguish two possible situations:

   2.1 $\mu(u, \breve{u}') = 1$ and $u = u'$ and $op(u') \leq op(u)$: then as $u' \in \mathbf{D}$ from Proposition 34 and Lemma 38 we have that $u' = a$ from which it follows $u = a = z$;

   2.2 $\mu(u, \breve{u}') < 1$ and $u = u' \mathbin{+\!\!\!\!\sqcup}_{\mu(u,\breve{u}')} u''$ for some $u'' \in \mathcal{SP}$: as $\mu(u, \breve{u}') < 1$ we obtain that u can make more than one probabilistic transitions. Then from Corollary 36 we have

   $$u \equiv u'_1 \mathbin{+\!\!\!\!\sqcup}_{\sigma_1} u'_2 \mathbin{+\!\!\!\!\sqcup}_{\sigma_2} u'_3 \ldots \mathbin{+\!\!\!\!\sqcup}_{\sigma_{n-1}} u'_n$$

for some $n \geq 2$, $\sigma_i \in \langle 0,1 \rangle$ and $u'_i \in \mathcal{B}_+$ and where for each i, $1 \leq i \leq n$, $\breve{u}'_i \,\underline{\leftrightarrow}\, \breve{a}$. If we suppose that there exists $j, 1 \leq j \leq n$, such that $\breve{u}'_j \,\not\underline{\leftrightarrow}\, \breve{a}$, then it implies $u \,\not\underline{\leftrightarrow}\, a$ which contradicts the given assumption. This provides us with considering one form only from Corollary 36. From Proposition 34 and Lemma 38 we have that for each i, $1 \leq i \leq n$, $u'_i = a$ from which we obtain $u = a = z$.

3. $z \equiv a \cdot t$ for some basic term t: then from the assumption $u \,\underline{\leftrightarrow}\, a \cdot t$ it follows that there exists $\breve{u}' \in \mathcal{DP}$ such that $u \rightsquigarrow \breve{u}'$ and $\breve{u}' \,\underline{\leftrightarrow}\, \breve{a} \cdot t$. According to Proposition 33 we have to consider two possible situations:

   3.1 $\mu(u, \breve{u}') = 1$ and $u = u'$ and $op(u') \leq op(u)$: then from Corollary 27 we have that $u' \in \mathcal{B}_+$. By case distinction on the structure of u' we prove that $u' = z$. By the assumption $a \cdot t \,\underline{\leftrightarrow}\, u'$ it is clear that $u' \notin A_\delta$. If $u' \equiv a \cdot s$ for a basic term s, we obtain $t \,\underline{\leftrightarrow}\, s$, from which by the induction hypothesis (which is applicable because $op(t) < z$ and $op(s) < op(u)$) we have $t = s$. Therefore we have $u' = a \cdot s = a \cdot t = z$, from which it follows $u = u' = z$.

   If $u' \equiv u_1 + u_2$ for some terms $u_1, u_2 \in \mathcal{B}_+$, we can prove that either

   (a) $u_1 \,\underline{\leftrightarrow}\, \delta$ and $u_2 \,\underline{\leftrightarrow}\, a \cdot t$ or

   (b) $u_2 \,\underline{\leftrightarrow}\, \delta$ and $u_1 \,\underline{\leftrightarrow}\, a \cdot t$ or

   (c) $u_1 \,\underline{\leftrightarrow}\, a \cdot t$ and $u_2 \,\underline{\leftrightarrow}\, a \cdot t$.

   Suppose that $u_1 \,\not\underline{\leftrightarrow}\, a \cdot t$. From Proposition 34 we have that $\breve{u}_1 \,\not\underline{\leftrightarrow}\, \breve{a} \cdot t$, which implies $\breve{u}_1 \not\xrightarrow{a}$ or $\breve{u}_1 \xrightarrow{a} v$, but $v \,\not\underline{\leftrightarrow}\, t$ for some $v \in \mathcal{SP}$.

   In the second case we have that $\breve{u}' \xrightarrow{a} v$ and by assumption $\breve{u}' \,\underline{\leftrightarrow}\, \breve{u}_1 + \breve{u}_2$ we obtain that $v \,\underline{\leftrightarrow}\, t$, which is a contradiction.

   In the first case we obtain that $\breve{u}_2 \xrightarrow{a} w$, for some $w \in \mathcal{SP}$, because by the assumption it has to be that $\breve{u}' \xrightarrow{a} w$. Moreover $w \,\underline{\leftrightarrow}\, t$. By this we proved that $\breve{u}_2 \,\underline{\leftrightarrow}\, \breve{a} \cdot t$ from which, using Proposition 34 we have $u_2 \,\underline{\leftrightarrow}\, a \cdot t$. Then from the induction hypothesis we obtain $u_2 = a \cdot t$. Moreover, if we suppose that there exist $b \in A, b \not\equiv a$ and $v \in \mathcal{SP}$ such that $\breve{u}_1 \xrightarrow{b} v$ then this implies that $\breve{u}' \xrightarrow{b} v$, as well, but $\breve{a} \cdot t \not\xrightarrow{b}$ which contradicts to the assumption $u' \,\underline{\leftrightarrow}\, a \cdot t$. So, we get that $\breve{u}_1$ can not perform any action transition, which implies that $\breve{u}_1 \,\underline{\leftrightarrow}\, \breve{\delta}$. Because $u_1 \in \mathcal{B}_+ \subseteq \mathbf{D}$ using Proposition 34 and Lemma 38 we obtain that $u_1 = \delta$.

   In a similar way we prove the case where $u_2 \,\not\underline{\leftrightarrow}\, a \cdot t$.

   In the third case $u_1 \,\underline{\leftrightarrow}\, a \cdot t$ and $u_2 \,\underline{\leftrightarrow}\, a \cdot t$ by the induction hypothesis we have $u_1 = a \cdot t$ and $u_2 = a \cdot t$.

   The assumption $u_1 \,\not\underline{\leftrightarrow}\, a \cdot t$ and $u_2 \,\not\underline{\leftrightarrow}\, a \cdot t$ leads to a contradiction with the assumption that $u_1 + u_2 \,\underline{\leftrightarrow}\, a \cdot t$.

   With this we prove that exactly one of the cases (a), (b) or (c) is possible.

   In each of these cases we obtain $u' = u_1 + u_2 = a \cdot t = z$, from which it follows $u = u' = z$;

3.2 $\mu(u, \breve{u}') < 1$ and $u = u' \uplus_{\mu(u,\breve{u}')} u''$ for some $u'' \in \mathcal{SP}$: as $\mu(u, \breve{u}') < 1$ it implies that u can make more than one probabilistic transitions. Then using Corollary 36 we have that

$$u \equiv u_1' \uplus_{\sigma_1} u_2' \uplus_{\sigma_2} u_3' \ldots \uplus_{\sigma_{n-1}} u_n'$$

for some $n \geq 2$, $\sigma_i \in \langle 0, 1 \rangle$ and $u_i' \in \mathcal{B}_+$ and where for each $i,\ 1 \leq i \leq n,\ \breve{u}_i' \underline{\leftrightarrow} \breve{a} \cdot t$. If we suppose that there exists $j, 1 \leq j \leq n$, such that $\breve{u}_j' \not\underline{\leftrightarrow} \breve{a} \cdot t$, then it implies $u \not\underline{\leftrightarrow} a \cdot t$ which contradicts the given assumption. This provides us with considering one form only from Corollary 36. By Proposition 34 and the induction hypothesis we have that for each $i,\ 1 \leq i \leq n,\ u_i' = a \cdot t$ from which we obtain $u = a \cdot t = z$.

4. $z \equiv z_1 + z_2$ for some basic terms $z_1, z_2 \in \mathcal{B}_+$: then from the assumption $z \underline{\leftrightarrow} u$ it follows that there exists $\breve{u}' \in \mathcal{DP}$ such that $u \rightsquigarrow \breve{u}'$ and $\breve{u}' \underline{\leftrightarrow} \breve{z}_1 + \breve{z}_2$. By Proposition 33 we have to consider two possible situations:

4.1 $\mu(u, \breve{u}') = 1$ and $u = u'$ and $op(u') \leq op(u)$: then by Corollary 27 we have that $u' \in \mathcal{B}_+$. By case distinction on the structure of u' we prove that $u' = z$. If u' is a basic $\mathcal{B}_+$ term of the form a or $a \cdot t$ for some $a \in A_\delta$ and $t \in \mathcal{B}$, then the result follows from cases 1, 2 and 3. So, we only need to consider the case where $u' \equiv u_1 + u_2$ for some basic $\mathcal{B}_+$ terms u_1 and u_2. From Theorem 30 (Congruence theorem) and the assumption $z \underline{\leftrightarrow} u'$ we obtain: $z \underline{\leftrightarrow} u' + z$ and $u' \underline{\leftrightarrow} u' + z$. We will prove that assumption $z \underline{\leftrightarrow} u_1 + u_2 + z$ implies $z \underline{\leftrightarrow} u_1 + z$ and $z \underline{\leftrightarrow} u_2 + z$. In order to prove the first property we consider the following relation:

$$R' = Eq(R \cup \{(z, u_1 + z), (\breve{z}, \breve{u}_1 + \breve{z})\}),$$

where R is a bisimulation relation such that $zR(u_1 + u_2)$.

As $z, u_1 \in \mathcal{B}_+ \subset \mathbf{D}$ we obtain from Proposition 25 that $z \rightsquigarrow \breve{z}$ and $u_1 \rightsquigarrow \breve{u}_1$ is the only possible probabilistic transition of z and u_1, respectively, with $\mu(z, \breve{z}) = 1$ and $\mu(u_1, \breve{u}_1) = 1$, from which we have that the only possible probabilistic transition of $u_1 + z$ is $u_1 + z \rightsquigarrow \breve{u}_1 + \breve{z}$ and $\mu(u_1 + z, \breve{u}_1 + \breve{z}) = 1$. Moreover by the definition of R' we have $(\breve{z}, \breve{u}_1 + \breve{z}) \in R'$.

Let $\breve{z} \xrightarrow{a} x$ for some $a \in A$ and $x \in \mathcal{SP}$. Then also $\breve{u}_1 + \breve{z} \xrightarrow{a} x$ and moreover $xR'x$.

Let $\breve{u}_1 \xrightarrow{a} y$ for some $a \in A$ and $y \in \mathcal{SP}$. Then from $u' \equiv u_1 + u_2$ and $\breve{u}' \equiv \breve{u}_1 + \breve{u}_2$ it follows that $\breve{u}' \xrightarrow{a} y$ and using the assumption $\breve{u}' \underline{\leftrightarrow} z$ we obtain there exists $x \in \mathcal{SP}$ such that $\breve{z} \xrightarrow{a} x$ and xRy which implies $xR'y$.

By this we prove that R' is a bisimulation relation such that $(z, u_1 + z) \in R'$ which means that $z \underline{\leftrightarrow} u_1 + z$. In a similar way we can prove the relation between z and $u_2 + z$.

In conclusion we have: $z \underline{\leftrightarrow} u' + z \Leftrightarrow z \underline{\leftrightarrow} u_1 + u_2 + z \Leftrightarrow z \underline{\leftrightarrow} u_1 + z$ and $z \underline{\leftrightarrow} u_2 + z$. By the induction hypothesis we have that $z = u_1 + z$ and $z = u_2 + z$, and using Proposition 6 we obtain

$$z = z + z = u_1 + u_2 + z = u' + z. \tag{6}$$

Moreover $u' \underline{\leftrightarrow} z + u' \Leftrightarrow u' \underline{\leftrightarrow} z_1 + z_2 + u' \Leftrightarrow u' \underline{\leftrightarrow} z_1 + u'$ and $u' \underline{\leftrightarrow} z_2 + u'$ which can be proved as the case above. By the induction hypothesis we have that $u' = z_1 + u'$ and $u' = z_2 + u'$, from which using Proposition 6 we obtain

$$u' = u' + u' = z_1 + z_2 + u' = z + u'. \tag{7}$$

Finally, from (6) and (7) we obtain $z = u'$, from which it follows $u = z$.

4.2 $\mu(u_1, \breve{u}_1) < 1$ and $u = u' \boxplus_\rho u''$ for some $u'' \in \mathcal{SP}$: as $\mu(u_1, \breve{u}_1) < 1$ we obtain that u can make more than one probabilistic transitions. Then using Corollary 36 we have that

$$u \equiv u'_1 \boxplus_{\sigma_1} u'_2 \boxplus_{\sigma_2} u'_3 \ldots \boxplus_{\sigma_{n-1}} u'_n$$

for some $n \geq 2$ and $\sigma_i \in \langle 0, 1\rangle$, $u'_i \in \mathcal{B}_+$ and where for each i, $1 \leq i \leq n$, $\breve{u}'_i \underline{\leftrightarrow} \breve{z}_1 + \breve{z}_2$. Suppose that there exists $j, 1 \leq j \leq n$, for which $\breve{u}'_j \underline{\not\leftrightarrow} \breve{z}_1 + \breve{z}_2$ (*). Then we have $\mu(z, [\breve{z}_1 + \breve{z}_2]_{\underline{\leftrightarrow}}) = 1$ but $\mu(u, [\breve{z}_1 + \breve{z}_2]_{\underline{\leftrightarrow}}) = 1 - \sum\limits_{\breve{u}_j \notin [\breve{z}_1 + \breve{z}_2]_{\underline{\leftrightarrow}}} \mu(u, [\breve{u}_j]_{\underline{\leftrightarrow}})$. From the assumption (*) we have that $\sum\limits_{\breve{u}_j \notin [\breve{z}_1 + \breve{z}_2]_{\underline{\leftrightarrow}}} \mu(u, [\breve{u}_j]_{\underline{\leftrightarrow}}) > 0$, which implies $\mu(u, [\breve{z}_1 + \breve{z}_2]_{\underline{\leftrightarrow}}) < 1$. This is a contradiction with the assumption that $z \underline{\leftrightarrow} u$. This provides us with considering one form only from Corollary 36.

Finally, by Proposition 34 and the induction hypothesis we have that for each i, $1 \leq i \leq n$, $u'_i = z_1 + z_2$ from which we obtain $u = z$.

5. $z \equiv z_1 \boxplus_\pi z_2$ for some basic *prBPA* terms z_1 and z_2: because there exists a equivalence class $K \in \mathcal{PR}/\underline{\leftrightarrow}$, $K \subseteq \mathcal{DP}$, such that $\mu(z, K) \neq 0$ we suppose $z \rightsquigarrow \breve{z}'_i$, $1 \leq i \leq p$, are all possible probabilistic transitions to elements of K, for some $p \in \mathbb{N}, p \geq 1$. From Corollary 36, because $z \notin \mathcal{B}_+$, we have that

$$z \equiv z'_1 \boxplus_{\sigma_1} z'_2 \boxplus_{\sigma_2} z'_3 \ldots \boxplus_{\sigma_{n-1}} z'_n, n \geq 2$$

or

$$z \equiv z'_1 \boxplus_{\sigma_1} z'_2 \boxplus_{\sigma_2} z'_3 \ldots \boxplus_{\sigma_{n-1}} z'_n \boxplus_{\sigma_n} y, n \geq 1$$

for some $n \in \mathbb{N}$, $\sigma_j \in \langle 0, 1\rangle$, $1 \leq j \leq n$, such that for each i, $1 \leq i \leq p$, $\mu(z, \breve{z}'_i) = \sum\limits_{j \in Q_i} \sigma_j$, $Q_i = \{j \ : \ z_j \equiv z_i\}$, and for some basic term y, $y \notin K$. (The case $n = 1$ is not possible because it contradicts the assumption $z \equiv z_1 \boxplus_\pi z_2$.)

The assumption $z \underline{\leftrightarrow} u$ and the previous assumption about probabilistic transitions of z determine the probabilistic transitions of u and from Proposition 35 we obtain:

$$u \equiv u'_1 \boxplus_{\rho_1} u'_2 \boxplus_{\rho_2} u'_3 \ldots \boxplus_{\rho_{m-1}} u'_m$$

in the first case or

$$u \equiv u'_1 \boxplus_{\rho_1} u'_2 \boxplus_{\rho_2} u'_3 \ldots \boxplus_{\rho_{m-1}} u'_m \boxplus_{\rho_m} w,$$

in the second case, for some $m \in \mathbb{N}$, basic term w, such that $w \notin K$ and $\rho_j \in \langle 0, 1]$ for each j, $1 \leq j \leq m$. (One can note that here we allow m to be 1 which covers the case where

$u \equiv u'_1$). This means that $u \rightsquigarrow \breve{u}_j$, $1 \leq j \leq m$, are all possible probabilistic transitions of u to elements of the class K and $\mu(u, \breve{u}'_j) = \sum_{l \in Q'_j} \rho_l$, where $Q'_j = \{l \ : \ u'_l \equiv u'_j\}$. Moreover we have $\breve{z}'_i \underline{\leftrightarrow} \breve{u}'_j$ for each i, j.

In the first case by Proposition 34 and the induction hypothesis we obtain that $z'_i = u'_j$ for each i, j, $1 \leq i \leq n$, $1 \leq j \leq m$, and $z'_i = z'_k$ for each i, k, $1 \leq i \leq n$, $1 \leq k \leq n$, and $u'_j = u'_l$ for each j, l, $1 \leq j \leq m$, $1 \leq l \leq m$. Then we easily obtain:

$$z \equiv z'_1 \boxplus_{\sigma_1} z'_2 \boxplus_{\sigma_2} z'_3 \ldots \boxplus_{\sigma_{n-1}} z'_n = z'_1 \boxplus_{\sigma_1} z'_1 \boxplus_{\sigma_2} z'_1 \ldots \boxplus_{\sigma_{n-1}} z'_1 = z'_1$$

and

$$u \equiv u'_1 \boxplus_{\rho_1} u'_2 \boxplus_{\rho_2} u'_3 \ldots \boxplus_{\rho_{m-1}} u'_m = u'_1 \boxplus_{\rho_1} u'_1 \boxplus_{\rho_2} u'_1 \ldots \boxplus_{\rho_{m-1}} u'_1 = u'_1$$

from which we obtain $z = u$.

In the second case we also have the results: $z'_i = u'_j$ for each i, j, $1 \leq i \leq n$, $1 \leq j \leq m$ and $z'_i = z'_k$ for each i, k, $1 \leq i \leq n$, $1 \leq k \leq n$, and $u'_j = u'_l$ for each j, l, $1 \leq j \leq m$, $1 \leq j \leq m$. Then we have

$$\begin{aligned} z &\equiv z'_1 \boxplus_{\sigma_1} z'_2 \boxplus_{\sigma_2} z'_3 \ldots \boxplus_{\sigma_{n-1}} z'_n \boxplus_{\sigma_n} y = z'_1 \boxplus_{\sigma_1} z'_1 \boxplus_{\sigma_2} z'_1 \ldots \boxplus_{\sigma_{n-1}} z'_1 \boxplus_{\sigma_n} y \\ &= z'_1 \boxplus_{\Sigma_{i=1}^{n} \sigma_i} y \end{aligned}$$

and

$$\begin{aligned} u &\equiv u'_1 \boxplus_{\rho_1} u'_2 \boxplus_{\rho_2} u'_3 \ldots \boxplus_{\rho_{m-1}} u'_m \boxplus_{\rho_m} w = u'_1 \boxplus_{\rho_1} u'_1 \boxplus_{\rho_2} u'_1 \ldots \boxplus_{\rho_{m-1}} u'_1 \boxplus_{\rho_m} w \\ &= u'_1 \boxplus_{\Sigma_{j=1}^{m} \rho_j} w. \end{aligned}$$

Using the Soundness theorem we have: $z \underline{\leftrightarrow} z'_1 \boxplus_{\Sigma_{i=1}^{n} \sigma_i} y$ and $u \underline{\leftrightarrow} u'_1 \boxplus_{\Sigma_{j=1}^{m} \rho_j} w$ and also from the assumption $z \underline{\leftrightarrow} u$ it follows that $z'_1 \boxplus_{\Sigma_{i=1}^{n} \sigma_i} y \underline{\leftrightarrow} z \underline{\leftrightarrow} u \underline{\leftrightarrow} u'_1 \boxplus_{\Sigma_{j=1}^{m} \rho_j} w$. Moreover $\mu(y, K) = 0 = \mu(w, K)$ from which $\mu(z'_1 \boxplus_{\Sigma_{i=1}^{n} \sigma_i} y, K) = \sum_{i=1}^{n} \sigma_i$ and $\mu(u'_1 \boxplus_{\Sigma_{j=1}^{m} \rho_j} w, K) = \sum_{j=1}^{m} \rho_j$ and also $\sum_{i=1}^{n} \sigma_i = \sum_{j=1}^{m} \rho_j$. Let us denote this sum by α.

We have $z'_1 \boxplus_{\alpha} y \underline{\leftrightarrow} u'_1 \boxplus_{\alpha} w$ and $z'_1 \underline{\leftrightarrow} u'_1$ and by Theorem 30 we obtain $z'_1 \boxplus_{\alpha} w \underline{\leftrightarrow} u'_1 \boxplus_{\alpha} w$ and $z'_1 \boxplus_{\alpha} y \underline{\leftrightarrow} z'_1 \boxplus_{\alpha} w$. Using Lemma 37 we have $y \underline{\leftrightarrow} w$.

Finally, we have $z'_1 \underline{\leftrightarrow} u'_1$ and $y \underline{\leftrightarrow} w$ and by the induction hypothesis we get $z'_1 = u'_1$ and $y = w$ from which it follows that $z = u$. □

3 Extension with merge and communication

3.1 Axiom system

Next, we extend *prBPA* with additional operators. The signature of *prACP* consists of the operators from *prBPA*, three new binary operators: $\|$ (merge), $|\!\lfloor$ (left merge) and $|$ (communication merge) and encapsulation ∂_H with $H \subseteq A$. *prACP* is parametrized by a communication function $\gamma : A_\delta \times A_\delta \longrightarrow A_\delta$ ([2]). Notice that we use non-deterministic choice, not probabilistic choice, in the expansion of the merge operator, contrary to [5]. The axiom of new operators are given in Table 5 with $a, b \in A_\delta$ and $\pi \in \langle 0, 1\rangle$.

$a \mid b$	$= \gamma(a, b)$		CF
$x \parallel y$	$= x |\!\lfloor y + y |\!\lfloor x + x \mid y$		$CM1$
$a |\!\lfloor x$	$= a \cdot x$		$CM2$
$a \cdot x |\!\lfloor y$	$= a \cdot (x \parallel y)$		$CM3$
$(x + y) |\!\lfloor z$	$= x |\!\lfloor z + y |\!\lfloor z$		$CM4$
$(x \sqcup\!\!\sqcup_\pi y) |\!\lfloor z$	$= x |\!\lfloor z \sqcup\!\!\sqcup_\pi y |\!\lfloor z$		$PrCM1$
$a \mid b \cdot x$	$= (a \mid b) \cdot x$		$CM5$
$a \cdot x \mid b$	$= (a \mid b) \cdot x$		$CM6$
$a \cdot x \mid b \cdot y$	$= (a \mid b) \cdot (x \parallel y)$		$CM7$
$(x \sqcup\!\!\sqcup_\pi y) \mid z$	$= x \mid z \sqcup\!\!\sqcup_\pi y \mid z$		$PrCM2$
$x \mid (y \sqcup\!\!\sqcup_\pi z)$	$= x \mid y \sqcup\!\!\sqcup_\pi x \mid z$		$PrCM3$
$\partial_H(a)$	$= a$	if $a \notin H$	$D1$
$\partial_H(a)$	$= \delta$	if $a \in H$	$D2$
$\partial_H(x + y)$	$= \partial_H(x) + \partial_H(y)$		$D3$
$\partial_H(x \cdot y)$	$= \partial_H(x) \cdot \partial_H(y)$		$D4$
$\partial_H(x \sqcup\!\!\sqcup_\pi y)$	$= \partial_H(x) \sqcup\!\!\sqcup_\pi \partial_H(y)$		$PrD1$

Table 5. Additional axioms for *prACP*.

We can note that the distribution laws of alternative composition w.r.t. communication merge are not included in this axiom system. Instead of these laws we add the rules in Table 6.

By the following example we show the reasons why we have this restriction in DyPR.

$$z = z + z \Rightarrow (x + y) \mid z = x \mid z + y \mid z$$
$$z = z + z \Rightarrow z \mid (x + y) = z \mid x + z \mid y$$

Table 6. Dynamic Processes Rule (DyPR)

Example 2. Let us assume that the distribution laws of alternative composition w.r.t. communication merge hold and let us compare two processes: $(a+b) \mid (c \sqcup\!\!\!\!+_{\pi} d)$ and $a \mid (c \sqcup\!\!\!\!+_{\pi} d) + b \mid (c \sqcup\!\!\!\!+_{\pi} d)$.

For the first of them by *PrCM3* we have:

$(a + b) \mid (c \sqcup\!\!\!\!+_{\pi} d) = ((a + b) \mid c) \sqcup\!\!\!\!+_{\pi} ((a + b) \mid d) = (a \mid c + b \mid c) \sqcup\!\!\!\!+_{\pi} (a \mid d + b \mid d)$.

For the later one by the assumed distribution laws we have:

$a \mid (c \sqcup\!\!\!\!+_{\pi} d) + b \mid (c \sqcup\!\!\!\!+_{\pi} d) = (a \mid c \sqcup\!\!\!\!+_{\pi} a \mid d) + (b \mid c \sqcup\!\!\!\!+_{\pi} b \mid d) =$

$(a \mid c + b \mid c) \sqcup\!\!\!\!+_{\pi^2} (a \mid d + b \mid c) \sqcup\!\!\!\!+_{\pi(1-\pi)} (a \mid c + b \mid d) \sqcup\!\!\!\!+_{\pi(1-\pi)} (a \mid d + b \mid d)$.

It is easy to conclude that these two processes are different. The second process has two summands which are the alternative composition of two processes each of which has been obtained by communication with a different atomic action in the probabilistic choice $c \sqcup\!\!\!\!+_{\pi} d$. Such summands do not occur in the first process. □

But if a probabilistic choice occurs between equal processes (or bisimilar) then this problem does not occur. For this reason the condition $z = z + z$ is given in the rule. This condition is fulfilled by all processes which cannot do probabilistic steps to different equivalence classes.

Theorem 40. *(Elimination theorem of prACP) Let p be a closed prACP term. Then there is a closed prBPA term q such that $prACP \vdash p = q$.*

Proof. Let p be a closed *prACP* term. The theorem is proven by induction case distinction on the structure of p.

1. $p \in A_\delta$: then p is a closed *prBPA* term;
2. $p \equiv p_1 \cdot p_2$ for certain closed *prACP* terms p_1 and p_2: by the induction hypothesis there exist closed *prBPA* terms q_1 and q_2 such that $prACP \vdash p_1 = q_1$ and $prACP \vdash p_2 = q_2$. Then we have $prACP \vdash p = p_1 \cdot p_2 = q_1 \cdot q_2$ and $q_1 \cdot q_2$ is a closed *prBPA* term;
3. $p \equiv p_1 + p_2$ for certain closed *prACP* terms p_1 and p_2: this case is treated analogously to case 2;
4. $p \equiv p_1 \mathbin{|\!\!\lfloor} p_2$ for certain closed *prACP* terms p_1 and p_2: by the induction there are closed *prBPA* terms q_1 and q_2 such that $prACP \vdash p_1 = q_1$ and $prACP \vdash p_2 = q_2$. By Theorem 9 there are basic terms r_1 and r_2 such that $prBPA \vdash q_1 = r_1$ and $prBPA \vdash q_2 = r_2$. But then also, $prACP \vdash p_1 = r_1$ and $prACP \vdash p_2 = r_2$ and $prACP \vdash p_1 \mathbin{|\!\!\lfloor} p_2 = r_1 \mathbin{|\!\!\lfloor} r_2$. By induction

on the structure of basic term r_1 we prove that there is a closed *prBPA* term r such that $prACP \vdash r_1 \mathbin{\|\!\!\lfloor} r_2 = r$.

4.1 $r_1 \equiv a \in A_\delta$: then $r_1 \mathbin{\|\!\!\lfloor} r_2 = a \mathbin{\|\!\!\lfloor} r_2 = a \cdot r_2$ and $a \cdot r_2$ is a closed *prBPA* term;

4.2 $r_1 \equiv a \cdot r_1'$ for some $a \in A$ and basic term r_1': then $r_1 \mathbin{\|\!\!\lfloor} r_2 = a \cdot r_1' \mathbin{\|\!\!\lfloor} r_2 = a \cdot (r_1' \,\|\, r_2)$. By the induction hypothesis there exists a closed *prBPA* term s such that $prACP \vdash r_1' \,\|\, r_2 = s$ and $a \cdot s$ is a closed *prBPA* term;

4.3 $r_1 \equiv r_1' + r_1''$ for some basic terms r_1' and r_1'': then $r_1 \mathbin{\|\!\!\lfloor} r_2 = (r_1' + r_1'') \mathbin{\|\!\!\lfloor} r_2 = r_1' \mathbin{\|\!\!\lfloor} r_2 + r_1'' \mathbin{\|\!\!\lfloor} r_2$. By the induction hypothesis there exist closed *prBPA* terms s' and s'' such that $prACP \vdash r_1' \mathbin{\|\!\!\lfloor} r_2 = s'$ and $prACP \vdash r_1'' \mathbin{\|\!\!\lfloor} r_2 = s''$. Then $prACP \vdash r_1 \mathbin{\|\!\!\lfloor} r_2 = s' + s''$ and $s' + s''$ is a closed *prBPA* term;

4.4 $r_1 \equiv r_1' \uplus_\pi r_1''$ for some basic terms r_1' and r_1'' and $\pi \in \langle 0, 1 \rangle$: then $r_1 \mathbin{\|\!\!\lfloor} r_2 = (r_1' \uplus_\pi r_1'') \mathbin{\|\!\!\lfloor} r_2 = r_1' \mathbin{\|\!\!\lfloor} r_2 \uplus_\pi r_1'' \mathbin{\|\!\!\lfloor} r_2$. By the induction hypothesis there exist closed *prBPA* terms s' and s'' such that $prACP \vdash r_1' \mathbin{\|\!\!\lfloor} r_2 = s'$ and $prACP \vdash r_1'' \mathbin{\|\!\!\lfloor} r_2 = s''$. Then $prACP \vdash r_1 \mathbin{\|\!\!\lfloor} r_2 = s' \uplus_\pi s''$ and $s' \uplus_\pi s''$ is a closed *prBPA* term;

5. $p \equiv p_1 \,|\, p_2$ for certain closed *prACP* terms p_1 and p_2: by induction there are closed *prBPA* terms q_1 and q_2 such that $prACP \vdash p_1 = q_1$ and $prACP \vdash p_2 = q_2$. By Theorem 9 there are basic terms r_1 and r_2 such that $prBPA \vdash q_1 = r_1$ and $prBPA \vdash q_2 = r_2$. But then also, $prACP \vdash p_1 = r_1$ and $prACP \vdash p_2 = r_2$ and $prACP \vdash p_1 \,|\, p_2 = r_1 \,|\, r_2$. By induction on the structure of basic terms r_1 and r_2 we prove that there is a closed *prBPA* term r such that $prACP \vdash r_1 \,|\, r_2 = r$.

5.1 $r_1 \equiv a \in A_\delta$ and $r_2 \equiv b \in A_\delta$: then $prACP \vdash r_1 \,|\, r_2 = a \,|\, b = \gamma(a, b)$ and $\gamma(a, b)$ is a closed *prBPA* term;

5.2 $r_1 \equiv a$ and $r_2 \equiv b \cdot r_2'$ for some $a, b \in A_\delta$ and basic term r_2': then $prACP \vdash r_1 \,|\, r_2 = (a \,|\, b) \cdot r_2'$ and $(a \,|\, b) \cdot r_2'$ is a closed *prBPA* term;

5.3 $r_1 \equiv a \cdot r_1'$ and $r_2 \equiv b$ for some $a, b \in A_\delta$ and basic term r_1': this case is treated symmetrically to the previous case;

5.4 $r_1 \equiv a \cdot r_1'$ and $r_2 \equiv b \cdot r_2'$ for some $a, b \in A_\delta$ and basic terms r_1' and r_2': then $prACP \vdash r_1 \,|\, r_2 = (a \,|\, b) \cdot (r_1' \,\|\, r_2')$. By induction there is a closed *prBPA* term s such that $prACP \vdash r_1' \,\|\, r_2' = s$. So $prACP \vdash r_1 \,|\, r_2 = (a \,|\, b) \cdot (r_1' \,\|\, r_2') = (a \,|\, b) \cdot s$ and $(a \,|\, b) \cdot s$ is a closed *prBPA* term;

5.5 $r_1 \equiv r_1' + r_1''$ for some basic terms r_1' and r_1'': according to the structure of r_2 there are two cases:

(a) if $r_2 \in \mathcal{B}_+$ then $r_2 + r_2 = r_2$ (by Proposition 6) and by *DyPR* we obtain $prACP \vdash r_1 \,|\, r_2 = (r_1' + r_1'') \,|\, r_2 = r_1' \,|\, r_2 + r_1'' \,|\, r_2$. By the induction hypothesis there are closed *prBPA* terms s' and s'' such that $prACP \vdash r_1' \,|\, r_2 = s'$ and $prACP \vdash r_1'' \,|\, r_2 = s''$. So $prACP \vdash r_1 \,|\, r_2 = r_1' \,|\, r_2 + r_1'' \,|\, r_2 = s' + s''$ and $s' + s''$ is a closed *prBPA* term;

(b) if $r_2 \in \mathcal{B} \setminus \mathcal{B}_+$ then for some $n \in \mathbb{N}, n \geq 2$ there exist $u_i \in \mathcal{B}_+$ and $\pi_i \in \langle 0, 1 \rangle$, for $1 \leq i \leq n$ such that $r_2 \equiv u_1 \uplus_{\pi_1} u_2 \uplus_{\pi_2} \ldots u_{n-1} \uplus_{\pi_{n-1}} u_n$. Moreover because $u_i \in \mathcal{B}_+$

we have that $u_i + u_i = u_i$ for each $i, 1 \leq i \leq n$ from which we obtain the following:
$prACP \vdash r_1 \,|\, r_2 = (r_1' + r_1'') \,|\, (u_1 \boxplus_{\pi_1} u_2 \boxplus_{\pi_2} \ldots u_{n-1} \boxplus_{\pi_{n-1}} u_n)$
$= (r_1' + r_1'') \,|\, u_1 \boxplus_{\pi_1} (r_1' + r_1'') \,|\, u_2 \boxplus_{\pi_2} \ldots \boxplus_{\pi_{n-1}} (r_1' + r_1'') \,|\, u_n$
$= (r_1' \,|\, u_1 + r_1'' \,|\, u_1) \boxplus_{\pi_1} (r_1' \,|\, u_2 + r_1'' \,|\, u_2) \boxplus_{\pi_2} \ldots \boxplus_{\pi_{n-1}} (r_1' \,|\, u_n + r_1'' \,|\, u_n)$.
By the induction hypothesis there exist basic *prBPA* terms s_i', s_i'', $1 \leq i \leq n$ such that $prACP \vdash r_i' \,|\, u_i = s_i'$ and $prACP \vdash r_i'' \,|\, u_i = s_i''$. Then we obtain:
$prACP \vdash r_1 \,|\, r_2 = (s_1' + s_1'') \boxplus_{\pi_1} (s_2' + s_2'') \boxplus_{\pi_2} \ldots (s_{n-1}' + s_{n-1}'') \boxplus_{\pi_{n-1}} (s_n' + s_n'')$ and $(s_1' + s_1'') \boxplus_{\pi_1} (s_2' + s_2'') \boxplus_{\pi_2} \ldots (s_{n-1}' + s_{n-1}'') \boxplus_{\pi_{n-1}} (s_n' + s_n'')$ is a closed *prBPA* term;

5.6 $r_2 \equiv r_2' + r_2''$ for some basic terms r_2' and r_2'': this case is treated symmetrically to 5.5;

5.7 $r_1 \equiv r_1' \boxplus_{\pi} r_1''$ for some basic terms r_1' and r_1'' and $\pi \in \langle 0, 1\rangle$ and r_2 is of arbitrary form: then $prACP \vdash r_1 \,|\, r_2 = (r_1' \boxplus_{\pi} r_1'') \,|\, r_2 = r_1' \,|\, r_2 \boxplus_{\pi} r_1'' \,|\, r_2$. By induction there are closed *prBPA* terms s' and s'' such that $prACP \vdash r_1' \,|\, r_2 = s'$ and $prACP \vdash r_1'' \,|\, r_2 = s''$. So $prACP \vdash r_1 \,|\, r_2 = r_1' \,|\, r_2 \boxplus_{\pi} r_1'' \,|\, r_2 = s' \boxplus_{\pi} s''$ and $s' \boxplus_{\pi} s''$ is a closed *prBPA* term;

5.8 $r_2 \equiv r_2' \boxplus_{\pi} r_2''$ for some basic terms r_2' and r_2'' and $\pi \in \langle 0, 1\rangle$ and r_1 is of arbitrary form: this case is treated symmetrically to the previous one;

6. $p \equiv p_1 \| p_2$ for certain closed *prACP* terms p_1 and p_2: then the result follows from axiom *CM*1 and cases 4. and 5;

7. $p \equiv \partial_H(p_1)$ for a certain closed *prACP* term p_1 and $H \subseteq A$: by the induction hypothesis there exists a closed *prBPA* term q_1 such that $prACP \vdash p_1 = q_1$. By Theorem 9 there is a basic term r_1 such that $prBPA \vdash q_1 = r_1$ which implies $prACP \vdash p_1 = r_1$. By induction on the structure of the basic term r_1 we prove that there is a closed *prBPA* term r such that $prACP \vdash \partial_H(r_1) = r$.

7.1 $r_1 \equiv a \in A_\delta$: then if $a \in H$, $\partial_H(r_1) = \delta$ and δ is a closed *prBPA* term. If $a \notin H$ then $\partial_H(r_1) = a$ and a is a closed *prBPA* term;

7.2 $r_1 \equiv a \cdot r_1'$ for some $a \in A$ and basic term r_1': then $\partial_H(r_1) = \partial_H(a \cdot r_1') = \partial_H(a) \cdot \partial_H(r_1')$. By the induction hypothesis there exist closed *prBPA* terms s' and s'' such that $prACP \vdash \partial_H(a) = s'$ and $prACP \vdash \partial_H(r_1') = s''$. Then $prACP \vdash \partial_H(r_1) = s' \cdot s''$ and $s' \cdot s''$ is a closed *prBPA* term;

7.3 $r_1 \equiv r_1' + r_1''$ for some basic terms r_1' and r_1'': then $\partial_H(r_1) = \partial_H(r_1') + \partial_H(r_1'')$. By the induction hypothesis there exist closed *prBPA* terms s' and s'' such that $prACP \vdash \partial_H(r_1') = s'$ and $prACP \vdash \partial_H(r_1'') = s''$. Then $prACP \vdash \partial_H(r_1) = s' + s''$ and $s' + s''$ is a closed *prBPA* term;

7.4 $r_1 \equiv r_1' \boxplus_{\pi} r_1''$ for some basic terms r_1' and r_1'' and $\pi \in \langle 0, 1\rangle$: then $\partial_H(r_1) = \partial_H(r_1') \boxplus_{\pi} \partial_H(r_1'')$. By the induction hypothesis there exist closed *prBPA* terms s' and s'' such that $prACP \vdash \partial_H(r_1') = s'$ and $prACP \vdash \partial_H(r_1'') = s''$. Then $prACP \vdash \partial_H(r_1) = s' \boxplus_{\pi} s''$ and $s' \boxplus_{\pi} s''$ is a closed *prBPA* term. □

3.2 Structured operational semantics of *prACP*

In *prACP* as in *prBPA* we need to distinguish static from dynamic processes. Indeed, we obtain the term model of *prACP* as an extension of the term model of *prBPA*, that is, by extension of the signature and the set of deduction rules of the term deduction system given in Section 2.2. We consider the signature: $\breve{\Sigma}_{prACP} = (\, A_\delta \cup \breve{A}_\delta \,, +, \cdot, \uplus_\pi, \, \|\,, \mathbin{|\!\!\lfloor}\,, \,|\,, \partial_H)$.

Analogously, we extend the sets of static and dynamic processes as follows:

Definition 41. A set of static processes $\mathcal{SP}(prACP)$ in *prACP* is the set of all closed terms over the signature of *prACP*, $\Sigma_{prACP} = (\, A_\delta \,, +, \cdot, \uplus_\pi, \, \|\,, \mathbin{|\!\!\lfloor}\,, \,|\,, \partial_H)$.

An auxiliary subset of $\mathcal{SP}(prACP)$, denoted by $\mathbf{D}(prACP)$, is defined as follows:

1. $A_\delta \subseteq \mathbf{D}(prACP)$;
2. $s, t \in \mathbf{D}(prACP) \Rightarrow s + t, s \,|\, t, \partial_H(s) \in \mathbf{D}(prACP)$;
3. $s \in \mathbf{D}(prACP), t \in \mathcal{SP}(prACP) \Rightarrow s \cdot t, s \mathbin{|\!\!\lfloor} t \in \mathbf{D}(prACP)$.

A set of dynamic processes $\mathcal{DP}(prACP)$ over the signature $\breve{\Sigma}_{prACP}$ is defined inductively as follows:

1. $\breve{A}_\delta \subseteq \mathcal{DP}(prACP)$;
2. $s, t \in \mathcal{DP}(prACP) \Rightarrow s + t, s \,|\, t, \partial_H(s) \in \mathcal{DP}(prACP)$;
3. $s \in \mathcal{DP}(prACP), t \in \mathcal{SP}(prACP) \Rightarrow s \cdot t, s \mathbin{|\!\!\lfloor} t \in \mathcal{DP}(prACP)$.

By $\mathcal{PR}(prACP)$ we will denote the set of all static and dynamic processes in *prACP*, that is $\mathcal{PR}(prACP) = \mathcal{SP}(prACP) \cup \mathcal{DP}(prACP)$.

We extend the map φ in Section 2.2 to $\varphi : \mathbf{D}(prACP) \to \mathcal{DP}(prACP)$ as follows:

1. $\varphi(a) = \breve{a}$ for each $a \in A_\delta$; 2. $\varphi(s \cdot t) = \varphi(s) \cdot t$;
3. $\varphi(s + t) = \varphi(s) + \varphi(t)$; 4. $\varphi(s \mathbin{|\!\!\lfloor} t) = \varphi(s) \mathbin{|\!\!\lfloor} t$;
5. $\varphi(s \,|\, t) = \varphi(s) \,|\, \varphi(t)$; 6. $\varphi(\partial_H(s)) = \partial_H(\varphi(s))$.

The operational semantics for the new operators in *prACP* is defined by the deduction rules given in Table 7 where a, b, c range over A and $H \subseteq A$ and the definition of the probability distribution function (Definition 42) extended over the new terms containing the new operators.

Definition 42. The probability distribution function $\mu : \mathcal{PR}(prACP) \times \mathcal{PR}(prACP) \to [0, 1]$ is defined with the equalities given in Definition 12 and the following:

$$\begin{aligned}
\mu(p \,\|\, q, x' \mathbin{|\!\!\lfloor} q + y' \mathbin{|\!\!\lfloor} p + x'' \,|\, y'') &= \mu(p, x')\mu(q, y')\mu(p, x'')\mu(q, y''),\\
\mu(p \mathbin{|\!\!\lfloor} q, x' \mathbin{|\!\!\lfloor} q) &= \mu(p, x'),\\
\mu(p \,|\, q, x' \,|\, x'') &= \mu(p, x')\mu(q, x''),\\
\mu(\partial_H(p), \partial_H(x')) &= \mu(p, x').
\end{aligned}$$

$$\frac{p \rightsquigarrow x}{p \mathbin{\|\!\lfloor} q \rightsquigarrow x \mathbin{\|\!\lfloor} q} \qquad \frac{p \rightsquigarrow x, q \rightsquigarrow y}{p \mid q \rightsquigarrow x \mid y}$$

$$\frac{p \rightsquigarrow x', q \rightsquigarrow y', p \rightsquigarrow x'', q \rightsquigarrow y''}{p \parallel q \rightsquigarrow x' \mathbin{\|\!\lfloor} y + y' \mathbin{\|\!\lfloor} x + x'' \mid y''} \qquad \frac{p \rightsquigarrow x}{\partial_H(p) \rightsquigarrow \partial_H(x)}$$

$$\frac{x \xrightarrow{a} p}{x \mathbin{\|\!\lfloor} y \xrightarrow{a} p \parallel y} \qquad \frac{x \xrightarrow{a} \surd}{x \mathbin{\|\!\lfloor} y \xrightarrow{a} y}$$

$$\frac{x \xrightarrow{a} p, y \xrightarrow{b} q, \gamma(a,b) = c}{x \mid y \xrightarrow{c} p \parallel q} \qquad \frac{x \xrightarrow{a} p, y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} p}$$

$$\frac{x \xrightarrow{a} \surd, y \xrightarrow{b} q, \gamma(a,b) = c}{x \mid y \xrightarrow{c} q} \qquad \frac{x \xrightarrow{a} \surd, y \xrightarrow{b} \surd, \gamma(a,b) = c}{x \mid y \xrightarrow{c} \surd}$$

$$\frac{x \xrightarrow{a} p, a \notin H}{\partial_H(x) \xrightarrow{a} \partial_H(p)} \qquad \frac{x \xrightarrow{a} \surd, a \notin H}{\partial_H(x) \xrightarrow{a} \surd}$$

Table 7. Operational semantics of *prACP*.

Example 3. In Figure 3 we give an example of parallel composition of probabilistic processes using labelled transition systems. We denote $e = a \mid c$ and $f = b \mid c$.

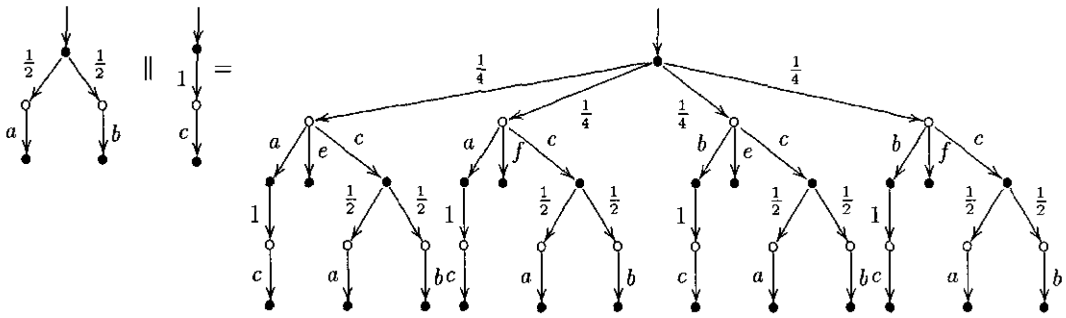


Fig. 3. Parallel composition.

Proposition 43. *Let $p, q \in \mathcal{SP}(prACP)$ and $M_i, N_i, K_i, M \subseteq \mathcal{PR}(prACP)$ for $i = 1, 2$. Then:*

1. $\mu(p \,\|\, q, M_1 \mathbin{\|\!\lfloor} M_2 + N_1 \mathbin{\|\!\lfloor} N_2 + K_1 \mid K_2) = \mu(p, M_1)\mu(q, N_1)\mu(p, K_1)\mu(q, K_2)$ *where* $M_1 \mathbin{\|\!\lfloor} M_2 + N_1 \mathbin{\|\!\lfloor} N_2 + K_1 \mid K_2 =$
   $\{m_1 \mathbin{\|\!\lfloor} m_2 + n_1 \mathbin{\|\!\lfloor} n_2 + k_1 \mid k_2 \ : \ m_1 \in M_1, m_2 \in M_2, n_1 \in N_1, n_2 \in N_2, k_1 \in K_1, k_2 \in K_2\}$;
2. $\mu(p \mathbin{\|\!\lfloor} q, M_1 \mathbin{\|\!\lfloor} M_2) = \mu(p, M_1)$ *where* $M_1 \mathbin{\|\!\lfloor} M_2 = \{m_1 \mathbin{\|\!\lfloor} m_2 \ : \ m_1 \in M_1, m_2 \in M_2\}$;
3. $\mu(p \mid q, M_1 \mid M_2) = \mu(p, M_1)\mu(q, M_2)$ *where* $M_1 \mid M_2 = \{m_1 \mid m_2 \ : \ m_1 \in M_1, m_2 \in M_2\}$;
4. $\mu(\partial_H(p), \partial_H(M)) = \mu(p, M)$ *where* $\partial_H(M) = \{\partial_H(m) \ : \ m \in M\}$.

Proof. 1. We use the abbreviations: $\bar{l}$ for $(m_1, m_2, n_1, n_2, k_1, k_2)$, $\bar{l}'$ for $(m_1, q, n_1, p, k_1, k_2)$, L for $M_1 \times M_2 \times N_1 \times N_2 \times K_1 \times K_2$ and L' for $M_1 \times \{q\} \times N_1 \times \{p\} \times K_1 \times K_2$

Then we have

$$\mu(p \,\|\, q, M_1 \mathbin{\|\!\lfloor} M_2 + N_1 \mathbin{\|\!\lfloor} N_2 + K_1 \mid K_2) =$$
$$\mu(p \,\|\, q, \{m_1 \mathbin{\|\!\lfloor} m_2 + n_1 \mathbin{\|\!\lfloor} n_2 + k_1 \mid k_2 \ : \ (m_1, m_2, n_1, n_2, k_1, k_2) \in L\}) =$$
$$\sum_{\bar{l} \in L} \mu(p \,\|\, q, m_1 \mathbin{\|\!\lfloor} m_2 + n_1 \mathbin{\|\!\lfloor} n_2 + k_1 \mid k_2) = \sum_{\bar{l}' \in L'} \mu(p \,\|\, q, m_1 \mathbin{\|\!\lfloor} q + n_1 \mathbin{\|\!\lfloor} p + k_1 \mid k_2) =$$
$$\sum_{\bar{l}' \in L'} \mu(p, m_1)\mu(q, n_2)\mu(p, k_1)\mu(q, k_2) =$$
$$\sum_{m_1 \in M_1} \sum_{n_1 \in N_1} \sum_{k_1 \in K_1} \sum_{k_2 \in K_2} \mu(p, m_1)\mu(q, n_1)\mu(p, k_1)\mu(q, k_2) =$$
$$\Big(\sum_{m_1 \in M_1} \mu(p, m_1)\Big)\Big(\sum_{n_1 \in N_1} \mu(q, n_1)\Big)\Big(\sum_{k_1 \in K_1} \mu(p, k_1)\Big)\Big(\sum_{k_2 \in K_2} \mu(q, k_2)\Big) =$$
$$\mu(p, M_1)\mu(q, N_1)\mu(p, K_1)\mu(p, K_2).$$

2. Using the definition of the probability distribution function we obtain:

$$\mu(p \mathbin{\|\!\lfloor} q, M_1 \mathbin{\|\!\lfloor} M_2) = \mu(p \mathbin{\|\!\lfloor} q, \{m_1 \mathbin{\|\!\lfloor} m_2 \ : \ m_1 \in M_1, m_2 \in M_2\}) =$$
$$\sum_{(m_1, m_2) \in M_1 \times M_2} \mu(p \mathbin{\|\!\lfloor} q, m_1 \mathbin{\|\!\lfloor} m_2) = \sum_{m_1 \in M_1, m_2 \equiv q} \mu(p \mathbin{\|\!\lfloor} q, m_1 \mathbin{\|\!\lfloor} q) =$$
$$\sum_{m_1 \in M_1} \mu(p, m_1) = \mu(p, M_1).$$

3. Using the definition of the probability distribution function we obtain:

$$\mu(p \mid q, M_1 \mid M_2) = \mu(p \mid q, \{m_1 \mid m_2 \ : \ m_1 \in M_1, m_2 \in M_2\}) =$$
$$\sum_{(m_1, m_2) \in M_1 \times M_2} \mu(p \mid q, m_1 \mid m_2) = \sum_{m_1 \in M_1} \sum_{m_2 \in M_2} \mu(p, m_1)\mu(q, m_2) =$$
$$\Big(\sum_{m_1 \in M_1} \mu(p, m_1)\Big)\Big(\sum_{m_2 \in M_2} \mu(q, m_2)\Big) = \mu(p, M_1)\mu(q, M_2).$$

4. Using the definition of the probability distribution function we obtain:

$$\mu(\partial_H(p), \partial_H(M)) = \mu(\partial_H(p), \{\partial_H(m) \ : \ m \in M\}) =$$
$$\sum_{m \in M} \mu(\partial_H(p), \partial_H(m)) = \sum_{m \in M} \mu(p, m) = \mu(p, M).$$

□

Definition 44. The probabilistic bisimulation in *prACP* is defined in the same way as in *prBPA*.

Theorem 45. $\underline{\leftrightarrow}$ *is a congruence relation on prACP.*

Proof. With respect to $\|$: Let x, y, z and w be $\mathcal{PR}(prACP)$ terms such that $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$. So, there exist probabilistic bisimulations R_1 and R_2 such that xR_1y and zR_2w. We define a relation R in the following way:

$R = Eq(\alpha_m \cup \beta_m \cup R_1 \cup R_2)$,

where

$$\alpha_m = \{(p \,\|\, q, s \,\|\, t) \ : \ p, q, s, t \in \mathcal{SP}(prACP), (p, s) \in R_1, (q, t) \in R_2\},$$

$$\begin{aligned}\beta_m = \{(u \mathbin{\|\!\lfloor} q + v \mathbin{\|\!\lfloor} p + u' \,|\, v', l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k') \ : \ & p, q, s, t \in \mathcal{SP}(prACP), \\ & u, v, l, k, u', v', l', k' \in \mathcal{DP}(prACP), \\ & (p, s),\ (u, l),\ (u', l') \in R_1, (q, t),\ (v, k),\ (v', k') \in R_2\}\end{aligned}$$

and where Eq means equivalence closure of the given relation.

Suppose $(p \,\|\, q, s \,\|\, t) \in R$ for some $p, q, s, t \in \mathcal{SP}(prACP)$ and $p \,\|\, q \rightsquigarrow m$ for some $m \in \mathcal{DP}(prACP)$. According to the definition of the operational rules it follows that for certain $u, v, u', v' \in \mathcal{DP}(prACP)$, $p \rightsquigarrow u$, $q \rightsquigarrow v$, $p \rightsquigarrow u'$ and $q \rightsquigarrow v'$ and $m \equiv u \mathbin{\|\!\lfloor} q + v \mathbin{\|\!\lfloor} p + u' \,|\, v'$. Then we have that for some $l, k, l', k' \in \mathcal{DP}(prACP)$, $s \rightsquigarrow l$, $t \rightsquigarrow k$, $s \rightsquigarrow l'$, $t \rightsquigarrow k'$ and (u, l), $(u', l') \in R_1$ and (v, k), $(v', k') \in R_2$. It follows that $s \,\|\, t \rightsquigarrow n$ where $n \equiv l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k'$ and by the definition of R we have that $(m, n) \in R$.

Suppose $(u \mathbin{\|\!\lfloor} q + v \mathbin{\|\!\lfloor} p + u' \,|\, v', l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k') \in R$ for some $u, v, u', v', l, k, l', k' \in \mathcal{DP}(prACP)$ and $u \mathbin{\|\!\lfloor} q + v \mathbin{\|\!\lfloor} p + u' \,|\, v' \xrightarrow{a} r$ for some $a \in A$ and $r \in \mathcal{SP}(prACP)$. Then from the definition of the operational rules the following cases can occur:

1. $u \mathbin{\|\!\lfloor} q \xrightarrow{a} r$: then
   1.1 $u \xrightarrow{a} r'$, for some $r' \in \mathcal{SP}(prACP)$ such that $r \equiv r' \,\|\, q$: then we have $l \xrightarrow{a} o'$ for some $o' \in \mathcal{SP}(prACP)$ such that $(r', o') \in R_1$, from which $l \mathbin{\|\!\lfloor} t \xrightarrow{a} o' \,\|\, t$. So $l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k' \xrightarrow{a} o' \,\|\, t$ and $(r' \,\|\, q, o' \,\|\, t) \in R$;
   1.2 $u \xrightarrow{a} \surd$ and $r \equiv q$: then we have $l \xrightarrow{a} \surd$ from which $l \mathbin{\|\!\lfloor} t \xrightarrow{a} t$. So $l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k' \xrightarrow{a} t$, and $(q, t) \in R$;
2. $v \mathbin{\|\!\lfloor} p \xrightarrow{a} r$: this case is similar to the previous one;
3. $u' \,|\, v' \xrightarrow{a} r$: then
   3.1 $u' \xrightarrow{b} r'$, $v' \xrightarrow{c} r''$ for some $r', r'' \in \mathcal{SP}(prACP)$, $b, c \in A$ such that $\gamma(b, c) = a$ and $r \equiv r' \,\|\, r''$: then $l' \xrightarrow{b} o'$, $k' \xrightarrow{c} o''$ for some $o', o'' \in \mathcal{SP}(prACP)$ such that $(r', o') \in R_1$ and $(r'', o'') \in R_2$. It follows that $l' \,|\, k' \xrightarrow{a} o' \,\|\, o''$, so $l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k' \xrightarrow{a} o' \,\|\, o''$ and $(r' \,\|\, r'', o' \,\|\, o'') \in R$;
   3.2 $u' \xrightarrow{b} \surd$, $v' \xrightarrow{c} r''$ for some $b, c \in A$ such that $\gamma(b, c) = a$ and $r \equiv r''$: then $l' \xrightarrow{b} \surd$, $k' \xrightarrow{c} o''$ for some $o'' \in \mathcal{SP}(prACP)$ such that $(r'', o'') \in R_2$. It follows that $l' \,|\, k' \xrightarrow{a} o''$, so $l \mathbin{\|\!\lfloor} t + k \mathbin{\|\!\lfloor} s + l' \,|\, k' \xrightarrow{a} o''$ and $(r'', o'') \in R$;
   3.3 $u' \xrightarrow{b} r'$, $v' \xrightarrow{c} \surd$ for some $b, c \in A$ such that $\gamma(b, c) = a$ and $r \equiv r'$: this case can be proved in a similar way as the previous one.

Suppose $(u \mathbin{|\!\!\lfloor} q+v \mathbin{|\!\!\lfloor} p+u' \mid v', l \mathbin{|\!\!\lfloor} t+k \mathbin{|\!\!\lfloor} s+l' \mid k') \in R$ for some $u, v, u', v', l, k, l', k' \in \mathcal{DP}(prACP)$ and $u \mathbin{|\!\!\lfloor} q+v \mathbin{|\!\!\lfloor} p+u' \mid v' \xrightarrow{a} \surd$ for some $a \in A$. This transition is possible only in the case $u' \mid v' \xrightarrow{a} \surd$, that is $u' \xrightarrow{b} \surd$, $v' \xrightarrow{c} \surd$ for some $b, c \in A$ such that $\gamma(b, c) = a$. By the assumption we have that $l' \xrightarrow{b} \surd$, $k' \xrightarrow{c} \surd$, so $l' \mid k' \xrightarrow{a} \surd$ and $l \mathbin{|\!\!\lfloor} t + k \mathbin{|\!\!\lfloor} s + l' \mid k' \xrightarrow{a} \surd$.

Suppose rRr_1 for some $r, r_1 \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}(prACP)/R, M \subsetneq \mathcal{DP}(prACP)$. We consider only the case $r\alpha_m r_1$, the cases rR_1r_1 and rR_2r_1 are trivial. From the assumption $r\alpha_m r_1$ it follows that $r \equiv p \,\|\, q$ and $r_1 \equiv s \,\|\, t$ for some $p, q, s, t \in \mathcal{SP}(prACP)$ such that pR_1s, qR_2t. Moreover, from the previous discussion about the probabilistic transitions of $p \,\|\, q$ and $s \,\|\, t$ we obtain that if $p \,\|\, q \rightsquigarrow u$ then there exists v such that $s \,\|\, t \rightsquigarrow v$ and $u\beta_m v$, and vice versa. Moreover because $M = \bigcup_{i \in I} M_i$, $I \neq \emptyset$, for some equivalence classes $M_i \in \mathcal{PR}(prACP)/\beta_m$, we are allowed to consider only β_m equivalence classes.

As we are interested in reachable classes from $p \,\|\, q$ and $s \,\|\, t$, we assume that there is an element $u_i \mathbin{|\!\!\lfloor} q + v_i \mathbin{|\!\!\lfloor} p + u'_i \mid v'_i \in M_i$ such that $p \rightsquigarrow u_i$, $q \rightsquigarrow v_i$, $p \rightsquigarrow u'_i$ and $q \rightsquigarrow v'_i$, so $M_i = [u_i \mathbin{|\!\!\lfloor} q + v_i \mathbin{|\!\!\lfloor} p + u'_i \mid v'_i]_{\beta_m}$. Moreover from the definition of β_m we get easily $M_i = [u_i]_{R_1} \mathbin{|\!\!\lfloor} [q]_{R_2} + [v_i]_{R_2} \mathbin{|\!\!\lfloor} [p]_{R_1} + [u'_i]_{R_1} \mid [v'_i]_{R_2}$. Then using Proposition 43 we obtain:

$$\begin{aligned}
\mu(p \,\|\, q, M_i) &= \mu(p \,\|\, q, [u_i]_{R_1} \mathbin{|\!\!\lfloor} [q]_{R_2} + [v_i]_{R_2} \mathbin{|\!\!\lfloor} [p]_{R_1} + [u'_i]_{R_1} \mid [v'_i]_{R_2}) \\
&= \mu(p, [u_i]_{R_1})\mu(q, [v_i]_{R_2})\mu(p, [u'_i]_{R_1})\mu(q, [v'_i]_{R_2}) \\
&= \mu(s, [u_i]_{R_1})\mu(t, [v_i]_{R_2})\mu(s, [u'_i]_{R_1})\mu(t, [v'_i]_{R_2}) \\
&= \mu(s \,\|\, t, [u_i]_{R_1} \mathbin{|\!\!\lfloor} [t]_{R_2} + [v_i]_{R_2} \mathbin{|\!\!\lfloor} [s]_{R_1} + [u'_i]_{R_1} \mid [v'_i]_{R_2}) \\
&= \mu(s \,\|\, t, [u_i \mathbin{|\!\!\lfloor} t + v_i \mathbin{|\!\!\lfloor} s + u'_i \mid v'_i]_{\beta_m}) = \mu(s \,\|\, t, M_i)
\end{aligned}$$

where the last equality holds because pR_1s and qR_2t which implies
$(u_i \mathbin{|\!\!\lfloor} t + v_i \mathbin{|\!\!\lfloor} s + u'_i \mid v'_i)\beta_m(u_i \mathbin{|\!\!\lfloor} q + v_i \mathbin{|\!\!\lfloor} p + u'_i \mid v'_i)$, and
$[u_i \mathbin{|\!\!\lfloor} t + v_i \mathbin{|\!\!\lfloor} s + u'_i \mid v'_i]_{\beta_m} = [u_i \mathbin{|\!\!\lfloor} q + v_i \mathbin{|\!\!\lfloor} p + u'_i \mid v'_i]_{\beta_m}$.

By Proposition 20 we obtain:

$$\mu(p \,\|\, q, M) = \sum_{i \in M} \mu(p \,\|\, q, M_i) = \sum_{i \in M} \mu(s \,\|\, t, M_i) = \mu(s \,\|\, t, M).$$

We proved that if $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$ then there exists a bisimulation R such that $(x \,\|\, z)R(y \,\|\, w)$, which implies $(x \,\|\, z) \underline{\leftrightarrow} (y \,\|\, w)$.

With respect to $\mathbin{|\!\!\lfloor}$: Let x, y, z and w be $\mathcal{PR}(prACP)$ terms such that $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$. So, there exist probabilistic bisimulations R_1 and R_2 such that xR_1y and zR_2w. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup \alpha_m \cup \beta_m \cup R_1 \cup R_2)$,

where

$\alpha = \{(p \mathbin{|\!\!\lfloor} q, s \mathbin{|\!\!\lfloor} t) \ : \ p, q, s, t \in \mathcal{SP}(prACP), (p, s) \in R_1, (q, t) \in R_2\}$,

$\beta = \{(u \mathbin{|\!\!\lfloor} q, v \mathbin{|\!\!\lfloor} t) \ : \ q, t \in \mathcal{SP}(prACP), \ u, v \in \mathcal{DP}(prACP), \ (u, v) \in R_1, (q, t) \in R_2\}$,

and α_m and β_m are defined as before.

Suppose $(p \mathbin{\lfloor\!\lfloor} q, s \mathbin{\lfloor\!\lfloor} t) \in R$ for some $p, q, s, t \in \mathcal{SP}(prACP)$ and $p \mathbin{\lfloor\!\lfloor} q \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that there exists $u' \in \mathcal{DP}(prACP)$ such that $p \rightsquigarrow u'$ and $u \equiv u' \mathbin{\lfloor\!\lfloor} q$. It follows that for some $v' \in \mathcal{DP}(prACP)$, $s \rightsquigarrow v'$ and $(u', v') \in R_1$ and also $s \mathbin{\lfloor\!\lfloor} t \rightsquigarrow v' \mathbin{\lfloor\!\lfloor} t$. Moreover $(u' \mathbin{\lfloor\!\lfloor} q, v' \mathbin{\lfloor\!\lfloor} t) \in R$.

Suppose $(u \mathbin{\lfloor\!\lfloor} q, v \mathbin{\lfloor\!\lfloor} t) \in R$ for some $u, v \in \mathcal{DP}(prACP)$ and $u \mathbin{\lfloor\!\lfloor} q \xrightarrow{a} r$ for some $a \in A$ and $r \in \mathcal{SP}(prACP)$. Then from the definition of the operational rules it follows that either

1. $u \xrightarrow{a} r'$ for some $r' \in \mathcal{SP}(prACP)$ such that $r \equiv r' \| q$: then $v \xrightarrow{a} o'$ for some $o' \in \mathcal{SP}(prACP)$ such that $(r', o') \in R_1$, from which $v \mathbin{\lfloor\!\lfloor} t \xrightarrow{a} o' \| t$ and $(r' \| q, o' \| t) \in R$, or
2. $u \xrightarrow{a} \surd$ and $r \equiv q$: then we have $v \xrightarrow{a} \surd$ from which $l \mathbin{\lfloor\!\lfloor} t \xrightarrow{a} t$ and $(q, t) \in R$.

The case $u \mathbin{\lfloor\!\lfloor} q \xrightarrow{a} \surd$ cannot occur.

Suppose rRr_1 for some $r, r_1 \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}(prACP)/R, M \subseteq \mathcal{DP}(prACP)$. We consider only the case $r\alpha r_1$, the cases rR_1r_1 and rR_2r_1 are trivial and the case $r\alpha_m r_1$ follows from the previous proof. From the assumption $r\alpha r_1$ it follows that $r \equiv p \mathbin{\lfloor\!\lfloor} q$ and $r_1 \equiv s \mathbin{\lfloor\!\lfloor} t$ for some $p, q, s, t \in \mathcal{SP}(prACP)$ such that pR_1s, qR_2t. Moreover, from the previous discussion about the probabilistic transitions of $p \mathbin{\lfloor\!\lfloor} q$ and $s \mathbin{\lfloor\!\lfloor} t$ we obtain that if $p \mathbin{\lfloor\!\lfloor} q \rightsquigarrow u$ then there exists v such that $s \mathbin{\lfloor\!\lfloor} t \rightsquigarrow v$ and $u\beta v$, and vice versa. Moreover because $M = \bigcup_{i \in I} M_i$, $I \neq \emptyset$, for some equivalence classes $M_i \in \mathcal{PR}(prACP)/\beta$, we consider only β equivalence classes.

As we consider reachable classes from $p \mathbin{\lfloor\!\lfloor} q$ and $s \mathbin{\lfloor\!\lfloor} t$, we assume that there is an element $u_i \mathbin{\lfloor\!\lfloor} q \in M_i$ such that $p \mathbin{\lfloor\!\lfloor} q \rightsquigarrow u_i \mathbin{\lfloor\!\lfloor} q$ and $p \rightsquigarrow u_i$. In this way we obtain that $M_i = [u_i \mathbin{\lfloor\!\lfloor} q]_\beta$. Moreover from the definition of β we get $M_i = [u_i]_{R_1} \mathbin{\lfloor\!\lfloor} [q]_{R_2}$. Then using Proposition 43 we obtain:

$\mu(p \mathbin{\lfloor\!\lfloor} q, M_i) = \mu(p \mathbin{\lfloor\!\lfloor} q, [u_i]_{R_1} \mathbin{\lfloor\!\lfloor} [q]_{R_2}) = \mu(p, [u_i]_{R_1}) = \mu(s, [u_i]_{R_1}) =$
$\mu(s \mathbin{\lfloor\!\lfloor} t, [u_i]_{R_1} \mathbin{\lfloor\!\lfloor} [t]_{R_2}) = \mu(s \mathbin{\lfloor\!\lfloor} t, M_i)$

where the last equality follows from the assumption qR_2t which implies $(u_i \mathbin{\lfloor\!\lfloor} q)\beta(u_i \mathbin{\lfloor\!\lfloor} t)$.

By Proposition 20 we obtain:

$$\mu(p \mathbin{\lfloor\!\lfloor} q, M) = \sum_{i \in M} \mu(p \mathbin{\lfloor\!\lfloor} q, M_i) = \sum_{i \in M} \mu(s \mathbin{\lfloor\!\lfloor} t, M_i) = \mu(s \mathbin{\lfloor\!\lfloor} t, M).$$

We proved that if $x \mathrel{\underline{\leftrightarrow}} y$ and $z \mathrel{\underline{\leftrightarrow}} w$ then there exists a bisimulation R such that $(x \mathbin{\lfloor\!\lfloor} z)R(y \mathbin{\lfloor\!\lfloor} w)$, which implies $(x \mathbin{\lfloor\!\lfloor} z) \mathrel{\underline{\leftrightarrow}} (y \mathbin{\lfloor\!\lfloor} w)$.

With respect to $|$: Let x, y, z and w be $\mathcal{PR}(prACP)$ terms such that $x \mathrel{\underline{\leftrightarrow}} y$ and $z \mathrel{\underline{\leftrightarrow}} w$. So, there exist probabilistic bisimulations R_1 and R_2 such that xR_1y and zR_2w. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup \alpha_m \cup \beta_m \cup R_1 \cup R_2)$,

where

$\alpha = \{(p \,|\, q, s \,|\, t) \ : \ p, q, s, t \in \mathcal{SP}(prACP), (p, s) \in R_1, (q, t) \in R_2\}$,

$\beta = \{(u \,|\, v, l \,|\, k) \ : \ u, v, l, k \in \mathcal{DP}(prACP), \ (u, l) \in R_1, (v, k) \in R_2\}$,

and α_m and β_m are defined as before.

Suppose $(p\,|\,q, s\,|\,t) \in R$ for some $p,q,s,t \in \mathcal{SP}(prACP)$ and $p\,|\,q \rightsquigarrow m$ for some $m \in \mathcal{DP}(prACP)$. According to the definition of the operational rules it follows that for certain $u,v \in \mathcal{DP}(prACP)$, $p \rightsquigarrow u$, $q \rightsquigarrow v$ and $m \equiv u\,|\,v$. Then $s \rightsquigarrow l$, $t \rightsquigarrow k$ for some $l,k \in \mathcal{DP}(prACP)$ such that $(u,l) \in R_1$ and $(v,k) \in R_2$. It follows that $s\,|\,t \rightsquigarrow l\,|\,k$ and $(u\,|\,v, l\,|\,k) \in R$.

Suppose $(u\,|\,v, l\,|\,k) \in R$ for some $u,v,l,k \in \mathcal{DP}(prACP)$ and $u\,|\,v \xrightarrow{a} r$ for some $a \in A$ and $r \in \mathcal{SP}(prACP)$. Then from the definition of the operational rules the following cases can occur:

1. $u \xrightarrow{b} r'$, $v \xrightarrow{c} r''$ for some $b,c \in A$ and $r',r'' \in \mathcal{SP}(prACP)$ such that $\gamma(b,c) = a$ and $r \equiv r' \,\|\, r''$: then $l \xrightarrow{b} o'$ and $k \xrightarrow{c} o''$ for some $o',o'' \in \mathcal{SP}(prACP)$ such that $(r',o') \in R_1$ and $(r'',o'') \in R_2$ from which $l\,|\,k \xrightarrow{a} o' \,\|\, o''$ and $(r' \,\|\, r'', o' \,\|\, o'') \in R$;
2. $u \xrightarrow{b} \surd$, $v \xrightarrow{c} r''$ for some $r'' \in \mathcal{SP}(prACP)$, $b,c \in A$ such that $\gamma(b,c) = a$ and $r \equiv r''$: then $l \xrightarrow{b} \surd$ and $k \xrightarrow{c} o''$ for some $o'' \in \mathcal{SP}(prACP)$ such that $(r'',o'') \in R_2$ from which $l\,|\,k \xrightarrow{a} o''$ and $(r'',o'') \in R$;
3. $u \xrightarrow{b} r'$, $v \xrightarrow{c} \surd$ for some $r' \in \mathcal{SP}(prACP)$, $b,c \in A$ such that $\gamma(b,c) = a$ and $r \equiv r'$: this case is similar to the previous one.

Suppose $u\,|\,v \xrightarrow{a} \surd$. It follows that $u \xrightarrow{b} \surd$ and $v \xrightarrow{c} \surd$ for some $b,c \in A$ such that $\gamma(b,c) = a$: then $l \xrightarrow{b} \surd$ and $k \xrightarrow{c} \surd$ from which $l\,|\,k \xrightarrow{a} \surd$.

Suppose rRr_1 for some $r,r_1 \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}(prACP)/R, M \subseteq \mathcal{DP}(prACP)$. We consider only the case $r\alpha r_1$, the cases rR_1r_1 and rR_2r_1 are trivial and the case $r\alpha_m r_1$ follows from the previous proof. From the assumption $r\alpha r_1$ it follows that $r \equiv p\,|\,q$ and $r_1 \equiv s\,|\,t$ for some $p,q,s,t \in \mathcal{SP}(prACP)$ such that pR_1s, qR_2t. Moreover, from the previous discussion about the probabilistic transitions of $p\,|\,q$ and $s\,|\,t$ we obtain that if $p\,|\,q \rightsquigarrow u$ then there exists v such that $s\,|\,t \rightsquigarrow v$ and $u\beta v$, and vice versa. It allows us to consider only equivalence classes of β, because $M = \bigcup\limits_{i\in I} M_i$, $I \neq \emptyset$, for some equivalence classes $M_i \in \mathcal{PR}(prACP)/\beta$.

As we consider reachable classes from $p\,|\,q$ and $s\,|\,t$, we assume that there is an element $u_i\,|\,v_i \in M_i$ such that $p\,|\,q \rightsquigarrow u_i\,|\,v_i$. In this way we obtain that $M_i = [u_i\,|\,v_i]_\beta$. Also, from the definition of β we get $M_i = [u_i]_{R_1}\,|\,[v_i]_{R_2}$. Then using Proposition 43 we obtain:

$\mu(p\,|\,q, M_i) = \mu(p\,|\,q, [u_i]_{R_1}\,|\,[v_i]_{R_2}) = \mu(p,[u_i]_{R_1})\mu(q,[v_i]_{R_2}) = \mu(s,[u_i]_{R_1})\mu(t,[v_i]_{R_2}) = \mu(s\,|\,t, [u_i]_{R_1}\,|\,[v_i]_{R_2}) = \mu(s\,|\,t, M_i)$.

By Proposition 20 we obtain:

$$\mu(p\,|\,q, M) = \sum_{i\in M} \mu(p\,|\,q, M_i) = \sum_{i\in M} \mu(s\,|\,t, M_i) = \mu(s\,|\,t, M).$$

We proved that if $x \underline{\leftrightarrow} y$ and $z \underline{\leftrightarrow} w$ then there exists a bisimulation R such that $(x\,|\,z)R(y\,|\,w)$, which implies that $(x\,|\,z) \underline{\leftrightarrow} (y\,|\,w)$.

With respect to ∂_H : Let x and y be $\mathcal{PR}(prACP)$ terms such that $x \underline{\leftrightarrow} y$. So, there exists a probabilistic bisimulations R_1 such that xR_1y. We define a relation R in the following way:

$R = Eq(\alpha \cup \beta \cup R_1)$,

where

$\alpha = \{(\partial_H(p), \partial_H(q)) \ : \ p, q \in \mathcal{SP}(prACP), (p, q) \in R_1\}$,
$\beta = \{(\partial_H(u), \partial_H(v)) \ : \ u, v \in \mathcal{DP}(prACP), \ (u, v) \in R_1\}$.

Suppose $(\partial_H(p), \partial_H(q)) \in R$ for some $p, q \in \mathcal{SP}(prACP)$ and $\partial_H(p) \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. According to the definition of the operational rules it follows that for certain $u' \in \mathcal{DP}(prACP)$, $p \rightsquigarrow u'$ and $u \equiv \partial_H(u')$. Then we have that for some $v' \in \mathcal{DP}(prACP)$, $q \rightsquigarrow v'$ and $(u', v') \in R_1$ and also $\partial_H(q) \rightsquigarrow \partial_H(v')$. Moreover, $\partial_H(u') \ \beta \ \partial_H(v')$ which implies $\partial_H(u') \ R \ \partial_H(v')$.

Suppose $(\partial_H(u), \partial_H(v)) \in R$ for some $u, v \in \mathcal{DP}(prACP)$ and $\partial_H(u) \xrightarrow{a} r$ for some $a \in A$ and $r \in \mathcal{DP}(prACP)$. From the definition of the operational rules it follows that $a \notin H$ and there exists $s \in \mathcal{SP}(prACP)$ such that $u \xrightarrow{a} s$ and $r \equiv \partial_H(s)$. Then for some $t \in \mathcal{SP}(prACP)$, $v \xrightarrow{a} t$ and $(s, t) \in R_1$ from which we have $\partial_H(v) \xrightarrow{a} \partial_H(t)$ and $\partial_H(s) \ \alpha \ \partial_H(t)$. From here we get $\partial_H(s) \ R \ \partial_H(t)$.

Suppose $\partial_H(u) \xrightarrow{a} \surd$ for some $a \in A$ which means $a \notin H$. Then it follows $u \xrightarrow{a} \surd$ and $v \xrightarrow{a} \surd$ from which $\partial_H(v) \xrightarrow{a} \surd$.

Suppose rRr_1 for some $r, r_1 \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}(prACP)/R, M \subseteq \mathcal{DP}(prACP)$. We consider only the case $r\alpha r_1$, the case rR_1r_1 is trivial. From the assumption $r\alpha r_1$ it follows that $r \equiv \partial_H(p)$ and $r_1 \equiv \partial_H(q)$ for some $p, q \in \mathcal{SP}(prACP)$ such that pR_1q. Moreover, from the previous discussion about probabilistic transitions of $\partial_H(p)$ and $\partial_H(q)$ we obtain that if $\partial_H(p) \rightsquigarrow u$, then there exists v such that $\partial_H(q) \rightsquigarrow v$ and $u\beta v$, and vice versa. It allows us to consider only equivalence classes of β, because $M = \bigcup\limits_{i \in I} M_i$, $I \neq \emptyset$, for some equivalence classes $M_i \in \mathcal{PR}(prACP)/\beta$.

As we consider reachable classes from $\partial_H(p)$ and $\partial_H(q)$, we assume that there is an element $\partial_H(u_i) \in M_i$ such that $\partial_H(p) \rightsquigarrow \partial_H(u_i)$ and so $M_i = [\partial_H(u_i)]_\beta$. Also, from the definition of β we get $M_i = \partial_H([u_i]_{R_1})$. Then using Proposition 43 we obtain:

$\mu(\partial_H(p), M_i) = \mu(\partial_H(p), \partial_H([u_i]_{R_1})) = \mu(p, [u_i]_{R_1}) = \mu(q, [u_i]_{R_1}) =$
$\mu(\partial_H(q), \partial_H([u_i]_{R_1})) = \mu(\partial_H(q), M_i)$.

By Proposition 20 we obtain:

$$\mu(\partial_H(p), M) = \sum_{i \in M} \mu(\partial_H(p), M_i) = \sum_{i \in M} \mu(\partial_H(q), M_i) = \mu(\partial_H(q), M).$$

We proved that if $x \leftrightarroweq y$ then there exists a bisimulation R such that $\partial_H(x) R \partial_H(y)$, which implies that $\partial_H(x) \leftrightarroweq \partial_H(y)$. □

Lemma 46. *If $x \in \mathcal{SP}(prACP)$ and $x \rightsquigarrow x'$, then $x' \in \mathcal{DP}(prACP)$.*

Proof. The proof is similar to the proof of Proposition 23. □

Lemma 47. *If $x \in \mathcal{DP}(prACP)$ then $x \leftrightarroweq x + x$.*

Proof. It follows directly from the definition of the operational rules of $prACP$. □

Lemma 48. *If $x, y, z \in \mathcal{DP}(prACP)$ and $x + y \leftrightarroweq z$ then $x + z \leftrightarroweq z$ and $y + z \leftrightarroweq z$.*

Proof. As $x, y, z \in \mathcal{DP}(prACP)$ we consider only the action transitions of the processes. The proof that the right side (each action transition of z) is simulated the by left side ($x + z$) is trivial. The proof that the left side ($x + z$) is simulated by the right side (z) follows from the assumption $x + y \underline{\leftrightarrow} z$ and the definition of the operational rules. □

Remark. If $x, y, z \in \mathcal{SP}(prACP)$ this property does not hold in general.

The following lemma matches probabilistic transitions of processes x and $x + x$. As we find the proof as too technical we give an example which may make the idea behind the proof more understandable.

Example 4. Let us consider process

$$x \equiv (a + b + c) \sqcup\!\!\!\!+_{\pi_1} (a + b) \sqcup\!\!\!\!+_{\pi_2} (a + c) \sqcup\!\!\!\!+_{\pi_3} a \sqcup\!\!\!\!+_{\pi_4} b$$

and we investigate possibilities of reaching a class $[y + y]_{\underline{\leftrightarrow}}$ from $x + x$ for some process y such that $x \rightsquigarrow y$. The following lemma says that always exists a process y such that $x + x \rightsquigarrow y + y$ is the only possible probabilistic transition from $x + x$ to $[y + y]_{\underline{\leftrightarrow}}$. $(\Diamond)$

In the given example one can note easily that this is true for processes $\breve{a}$, $\check{b}$ and $\breve{a} + \check{c}$. But for classes: $[\breve{a} + \check{b} + \check{c}]_{\underline{\leftrightarrow}}$ and $[\breve{a} + \check{b}]_{\underline{\leftrightarrow}}$ we have the following:
$x \rightsquigarrow \breve{a} + \check{b} + \check{c} \Rightarrow x + x \rightsquigarrow \breve{a} + \check{b} + \check{c} + \breve{a} + \check{b} + \check{c}$,
$x \rightsquigarrow \breve{a} + \check{b}, x \rightsquigarrow \breve{a} + \check{c} \Rightarrow x + x \rightsquigarrow \breve{a} + \check{b} + \breve{a} + \check{c}$ and
$\breve{a} + \check{b} + \check{c} + \breve{a} + \check{b} + \check{c} \underline{\leftrightarrow} \breve{a} + \check{b} + \breve{a} + \check{c}$,
which means that $[\breve{a} + \check{b} + \check{c}]_{\underline{\leftrightarrow}}$ is reached from $x + x$ trough different processes. A similar situation is with $[\breve{a} + \check{b}]_{\underline{\leftrightarrow}}$, that is:
$x \rightsquigarrow \breve{a} + \check{b} \Rightarrow x + x \rightsquigarrow \breve{a} + \check{b} + \breve{a} + \check{b}$,
$x \rightsquigarrow \breve{a}, x \rightsquigarrow \check{b} \Rightarrow x + x \rightsquigarrow \breve{a} + \check{b}$ and
$\breve{a} + \check{b} + \breve{a} + \check{b} \underline{\leftrightarrow} \breve{a} + \check{b}$.

In the following proof we use the iteration on the number of reachable processes from x which is a finite number. Then starting from one of them, more precisely from the index of one of these processes, in each iteration, we increase the set of indexes in the following way: if we denote $a + b + c$ as x_1, $a + b$ as x_2 and so on, b as x_5, we start from $I_1 = \{1\}$. In the next step we add to I_1 the indexes of two processes for whose non-deterministic sum is bisimilar with $\breve{a} + \check{b} + \check{c}$, for example, $2, 3 \in I_2$ because $\breve{a} + \check{b} + \breve{a} + \check{c} \underline{\leftrightarrow} \breve{a} + \check{b} + \check{c}$.

In the next step, we consider processes $\breve{a} + \check{b} (\equiv x_2)$ and $\breve{a} + \check{c} (\equiv x_3)$ and two pairs of processes whose non-deterministic sum is bisimilar to $\breve{a} + \check{b}$ and $\breve{a} + \check{c}$, respectively. In such a way we form the next set of indexes $I_3 = I_2 \cup \{4, 5\}$.

The main idea is to prove that $I_2 \setminus I_1 \neq \emptyset$ as well as $I_3 \setminus I_2 \neq \emptyset$, under the assumption that such a term y in $(\Diamond)$ does not exist (assumption (*) in the proof) and independently of the choice of a starting process. □

Lemma 49. *Let x be a closed prACP term such that $x \rightsquigarrow x_1, x \rightsquigarrow x_2, \ldots, x \rightsquigarrow x_n$, $n \geq 1$ are all possible probabilistic transitions of x and for each i, j, $1 \leq i \leq n, 1 \leq j \leq n$, if $i \neq j$ then $x_i \not\underline{\leftrightarrow} x_j$. Then there exists an $m, 1 \leq m \leq n$ such that $x + x \rightsquigarrow x_m + x_m$ is the only possible probabilistic transition of $x + x$ to equivalence class $[x_m + x_m]_{\underline{\leftrightarrow}}$.*

Proof. We start the proof from the negation of the conclusion of the lemma for which we will prove that leads to a contradiction to the assumption about probabilistic transitions of x.

Let us assume that $x \rightsquigarrow x_1, x \rightsquigarrow x_2, \ldots, x \rightsquigarrow x_n$, $n \geq 1$ are all possible probabilistic transitions of x and for each i, j, $1 \leq i \leq n, 1 \leq j \leq n$, if $i \neq j$ then $x_i \not\underline{\leftrightarrow} x_j$. It follows that $x \rightsquigarrow x_i$, $1 \leq i \leq n$, is the only possible probabilistic transition of x to equivalence class $[x_i]_{\underline{\leftrightarrow}}$ which implies that if $y \in [x_i]_{\underline{\leftrightarrow}}$ and $x \rightsquigarrow y$ then $x_i \equiv y$. $(\circ)$

Let us assume that the conclusion does not hold, that is:

$\forall i : \exists j, l : x + x \rightsquigarrow x_j + x_l \;\&\; x_j + x_l \underline{\leftrightarrow} x_i + x_i \;\&\; (x_j \not\equiv x_i \vee x_l \not\equiv x_i)$ $(*)$

First, we consider processes x_1. From $(*)$ it follows that there exist i_1, j_1 such that

$x + x \rightsquigarrow x_{i_1} + x_{j_1}$ and $x_{i_1} + x_{j_1} \underline{\leftrightarrow} x_1 + x_1$ and $(x_{i_1} \not\equiv x_1$ or $x_{j_1} \not\equiv x_1)$. $(**)$

From Proposition 48 it follows that $x_{i_1} + x_1 \underline{\leftrightarrow} x_1$ and $x_{j_1} + x_1 \underline{\leftrightarrow} x_1$ and at this point we know $\{x_1, x_{i_1} + x_1, x_{j_1} + x_1\} \subseteq [x_1]_{\underline{\leftrightarrow}}$. By I_1 we denote the set of all indexes of processes which have been already taken into consideration, that is $I_1 = \{1, i_1, j_1\}$.

Second, we consider processes x_{i_1} and x_{j_1}. From assumption $(*)$ it follows that there exist i_{11}, i_{12} such that

$x + x \rightsquigarrow x_{i_{11}} + x_{i_{12}}$ and $x_{i_{11}} + x_{i_{12}} \underline{\leftrightarrow} x_{i_1} + x_{i_1}$ and $(x_{i_{11}} \not\equiv x_{i_1}$ or $x_{i_{12}} \not\equiv x_{i_1})$ (1)

and there exist j_{11}, j_{12} such that

$x + x \rightsquigarrow x_{j_{11}} + x_{j_{12}}$ and $x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_{j_1} + x_{j_1}$ and $x_{j_{11}} \not\equiv x_{j_1}$ or $x_{j_{12}} \not\equiv x_{j_1}$. (2)

Using the Congruence theorem (Theorem 45) and Proposition 48, from (1) we obtain:

$x_{i_{1k}} + x_{i_1} + x_1 \underline{\leftrightarrow} x_{i_1} + x_1 \underline{\leftrightarrow} x_1$ which implies $x_{i_{1k}} + x_1 \underline{\leftrightarrow} x_1$ for $k = 1, 2$.

In a similar way we obtain $x_{j_{1k}} + x_1 \underline{\leftrightarrow} x_1$ for $k = 1, 2$.

In this step we have

$\{x_1, x_{i_1} + x_1, x_{j_1} + x_1, x_{i_{11}} + x_1, x_{i_{12}} + x_1, x_{j_{11}} + x_1, x_{j_{12}} + x_1\} \subseteq [x_1]_{\underline{\leftrightarrow}}$,

$\{x_{i_1}, x_{i_{11}} + x_{i_1}, x_{i_{12}} + x_{i_1}\} \subseteq [x_{i_1}]_{\underline{\leftrightarrow}}$,

$\{x_{j_1}, x_{j_{11}} + x_{j_1}, x_{j_{12}} + x_{j_1}\} \subseteq [x_{j_1}]_{\underline{\leftrightarrow}}$,

and we form the new set of indexes I_2 as $I_2 = I_1 \cup \{i_{11}, i_{12}, j_{11}, j_{12}\}$.

Next, we will prove that $\neg(\{i_{11}, i_{12}, j_{11}, j_{12}\} \subseteq \{1, i_1, j_1\})$, that is $I_2 \setminus I_1 \neq \emptyset$, which means that in the second step at least one new process has been taken into consideration. Investigating the various cases can occur, we will prove that assumption $\{i_{11}, i_{12}, j_{11}, j_{12}\} \subseteq \{1, i_1, j_1\}$ leads to a contradiction. Moreover, taking into account that:

(a) if we assume that $x_{i_{11}} \equiv x_{i_{12}} \equiv x_{j_1}$ then we obtain: $x_{i_1} \underline{\leftrightarrow} x_{i_{11}} + x_{i_{12}} \underline{\leftrightarrow} x_{j_1} + x_{j_1} \underline{\leftrightarrow} x_{j_1}$ which implies $x_{i_1} \equiv x_{j_1}$ and also, $x_1 \underline{\leftrightarrow} x_{i_1} + x_{j_1} \underline{\leftrightarrow} x_{j_1} + x_{j_1} \underline{\leftrightarrow} x_{j_1}$ which implies $x_1 \equiv x_{j_1}$ and this contradicts $(**)$

(b) in the assumptions we have $\neg(x_{i_{11}} \equiv x_{i_{12}} \equiv x_{i_1})$ and $\neg(x_{j_{11}} \equiv x_{j_{12}} \equiv x_{j_1})$,

we make the following restriction:

(a) $x_{i_{11}} \not\equiv x_{j_1}$ or $x_{i_{12}} \not\equiv x_{j_1}$;

(b) $x_{i_{11}} \not\equiv x_{i_1}$ or $x_{i_{12}} \equiv x_{i_1}$ and $x_{j_{11}} \not\equiv x_{j_1}$ or $x_{j_{12}} \not\equiv x_{j_1}$;

(c) we do not consider symmetrical cases, their correctness may be proved in a similar way as the presented one.

We have to consider the following cases:

1. if $x_{i_{11}} \equiv x_{i_{12}} \equiv x_1$, then $x_{i_1} \underline{\leftrightarrow} x_{i_{11}} + x_{i_{12}} \underline{\leftrightarrow} x_1 + x_1 \underline{\leftrightarrow} x_1$ which implies $x_{i_1} \equiv x_1$. (3)

   1.1 If $x_{j_{11}} \equiv x_1$ (independently of $x_{j_{12}}$), then $x_{j_1} \underline{\leftrightarrow} x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_1 + x_{j_{12}} \underline{\leftrightarrow} x_1$ which implies $x_{j_1} \equiv x_1$ and from (3) it follows $x_{i_1} \equiv x_1 \equiv x_{j_1}$ which contradicts $(**)$.

   1.2 If $x_{j_{11}} \equiv x_{i_1}$ and $x_{j_{12}} \equiv x_{j_1}$, then it is case 1.1 because of (3).

   For all cases left we have that $x_{i_{11}} \not\equiv x_{i_{12}}$ and $x_{j_{11}} \not\equiv x_{j_{12}}$.

2. if $x_{i_{11}} \equiv x_1$ and $x_{i_{12}} \equiv x_{i_1}$, then $x_{i_1} \underline{\leftrightarrow} x_{i_{11}} + x_{i_{12}} \underline{\leftrightarrow} x_1 + x_{i_1} \underline{\leftrightarrow} x_1$ which implies $x_{i_1} \equiv x_1$. (4)

   2.1 If $x_{j_{11}} \equiv x_1$ (independently of $x_{j_{12}}$) we obtain $x_{j_1} \underline{\leftrightarrow} x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_1 + x_{j_{12}} \underline{\leftrightarrow} x_1$ which implies $x_{j_1} \equiv x_1$ and from (4) it follows $x_{i_1} \equiv x_1 \equiv x_{j_1}$ which contradicts $(**)$.

   2.2 If $x_{j_{11}} \equiv x_{i_1}$ and $x_{j_{12}} \equiv x_{j_1}$ then $x_{j_1} \underline{\leftrightarrow} x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_{i_1} + x_{j_1} \underline{\leftrightarrow} x_1$ which implies $x_{j_1} \equiv x_1$ and from (4) it follows $x_{i_1} \equiv x_1 \equiv x_{j_1}$ which contradicts $(**)$.

3. if $x_{i_{11}} \equiv x_1$ and $x_{i_{12}} \equiv x_{j_1}$, then $x_{i_1} \underline{\leftrightarrow} x_{i_{11}} + x_{i_{12}} \underline{\leftrightarrow} x_1 + x_{j_1} \underline{\leftrightarrow} x_1$ which implies $x_{i_1} \equiv x_1$. (5)

   3.1 If $x_{j_{11}} \equiv x_1$ (independently of $x_{j_{12}}$) we obtain $x_{j_1} \underline{\leftrightarrow} x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_1 + x_{j_{12}} \underline{\leftrightarrow} x_1$ which implies $x_{j_1} \equiv x_1$ and from (5) it follows $x_{i_1} \equiv x_1 \equiv x_{j_1}$ which contradicts $(**)$.

   3.2 If $x_{j_{11}} \equiv x_{i_1}$ and $x_{j_{12}} \equiv x_{j_1}$ then $x_{j_1} \underline{\leftrightarrow} x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_{i_1} + x_{j_1} \underline{\leftrightarrow} x_1$ which implies $x_{j_1} \equiv x_1$ and from (5) it follows $x_{i_1} \equiv x_1 \equiv x_{j_1}$ which contradicts $(**)$.

   The next case covers all situations where $\{x_{i_{11}}, x_{i_{12}}, x_{j_{11}}, x_{j_{12}}\} \subseteq \{x_{i_1}, x_{j_1}\}$.

4. if $x_{i_{11}} \equiv x_{i_1}$ and $x_{i_{12}} \equiv x_{j_1}$, then $x_{i_1} \underline{\leftrightarrow} x_{i_{11}} + x_{i_{12}} \underline{\leftrightarrow} x_{i_1} + x_{j_1} \underline{\leftrightarrow} x_1$ which implies $x_{i_1} \equiv x_1$. (6)

   The only possible case is the following: if $x_{j_{11}} \equiv x_{i_1}$ (independently of $x_{j_{12}}$) then $x_{j_1} \underline{\leftrightarrow} x_{j_{11}} + x_{j_{12}} \underline{\leftrightarrow} x_{i_1} + x_{j_{12}} \underline{\leftrightarrow} x_1 + x_{j_{12}} \underline{\leftrightarrow} x_1$ which implies $x_{j_1} \equiv x_1$ and from (6) it follows $x_{i_1} \equiv x_1 \equiv x_{j_1}$ which contradicts $(**)$.

We point out that in cases 1.1, 2.1, 3.1 and 4. where process $x_{j_{11}} \equiv x_1$, results do not depend on process $x_{j_{12}}$ and for that reason we do not take alternatives of this process into account.

By this we proved that at least one of processes $x_{i_{11}}$, $x_{i_{12}}$, $x_{j_{11}}$ and $x_{j_{12}}$ is different from x_1, x_{i_1} and x_{j_1}, that is $I_2 \setminus I_1 \neq \emptyset$.

In the third step we consider $x_{i_{11}}$, $x_{i_{12}}$, $x_{j_{11}}$ and $x_{j_{12}}$ and processes that exist from $(*)$ for them. We form the set I_3 and in a similar way by case distinction we can obtain that I_3 contains at least one new index.

By repeating this procedure $n-1$ times (in the worst case) we will obtain that $|I_{n-1}| = n-1$, that is $\{1, 2, \ldots, n\} \setminus I_{n-1} \neq \emptyset$. Let $m \in \{1, 2, \ldots, n\} \setminus I_{n-1}$. Then from $(*)$ it follows that there exist m_1 and m_2 such that

$$x + x \rightsquigarrow x_{m_1} + x_{m_2} \;\&\; x_{m_1} + x_{m_2} \underline{\leftrightarrow}\, x_m + x_m \;\&\; (x_{m_1} \not\equiv x_m \vee x_{m_2} \not\equiv x_m).$$

From the previous discussion, x_{m_1} or x_{m_2} must be a new process whose index does not occur in I_{n-1}, but such a process does not exist. By this we have proved that the assumption (*) contradicts the condition of the lemma about n probabilistic transitions made by x. Thus, there is a x_m such that $x + x \rightsquigarrow x_m + x_m$ is the only possible probabilistic transition of $x + x$ to equivalence class $[x_m + x_m]_{\underline{\leftrightarrow}}$. □

Lemma 50. *Let x be a closed prACP term such that $x \underline{\leftrightarrow}\, x + x$. Then if $x \rightsquigarrow x'$ and $x \rightsquigarrow x''$ for some $x', x'' \in \mathcal{DP}(prACP)$, then $x' \underline{\leftrightarrow}\, x''$.*

Proof. Without loss of generality we can suppose that x is a term such that x does at most one probabilistic transition to an equivalence class. From Lemma 49 it follows that exists a process y such that $x \rightsquigarrow y$, and $x + x \rightsquigarrow y + y$ is the only possible probabilistic transition of $x + x$ to equivalence class $[y + y]_{\underline{\leftrightarrow}}$. We will prove the lemma by proving that $\mu(x, y) = 1$. It follows easily from the assumption $x \underline{\leftrightarrow}\, x + x$ which implies $\mu(x, [y]_{\underline{\leftrightarrow}}) = \mu(x + x, [y]_{\underline{\leftrightarrow}})$. Having that $\mu(x, [y]_{\underline{\leftrightarrow}}) = \mu(x, y)$, $\mu(x + x, [y + y]_{\underline{\leftrightarrow}}) = \mu(x + x, y + y) = \mu(x, y)^2$ and $[y]_{\underline{\leftrightarrow}} = [y + y]_{\underline{\leftrightarrow}}$ we obtain $\mu(x, y) = 1$. □

Theorem 51. *(Soundness) Let p and q be $\mathcal{PR}(prACP)$ terms. If $prACP + DyPR \vdash p = q$ then $p \underline{\leftrightarrow}\, q$.*

Proof. This theorem can be proved easily by construction of a suitable equivalence relation for each axiom which relates the left and right side of an associated axiom.

CF: We define a relation R in the following way:

$$R = Eq\Big(\{(c, a \,|\, b), (\breve{c}, \breve{a} \,|\, \breve{b})\}\Big),$$

where we denote shortly $\gamma(a, b) = c$.

We observe that the only possible probabilistic transition is $c \rightsquigarrow \breve{c}$ and $a \,|\, b \rightsquigarrow \breve{a} \,|\, \breve{b}$, respectively. An action termination for both terms, $\breve{c}$ and $\breve{a} \,|\, \breve{b}$ is possible only if $\breve{c} \not\equiv \breve{\delta}$. Then we have: $\breve{c} \xrightarrow{c} \surd$ and $\breve{a} \,|\, \breve{b} \xrightarrow{c} \surd$. For the probability distribution function we get: $\mu(c, \breve{c}) = 1$ and $\mu(a \,|\, b, \breve{a} \,|\, \breve{b}) = 1$, and the conclusion about R equivalence classes follows from the assumption $(\breve{c}, \breve{a} \,|\, \breve{b}) \in R$.

CM1: We define a relation R in the following way:

$$R = Eq\Big(\{(p \,\|\, q, p \mathbin{|\!\!\lfloor} q + q \mathbin{|\!\!\lfloor} p + p \,|\, q) \;:\; p, q \in \mathcal{SP}(prACP)\}\Big).$$

Suppose $(p \,\|\, q)R(p \mathbin{\lfloor\!\lfloor} q + q \mathbin{\lfloor\!\lfloor} p + p \,|\, q)$ for some $p, q \in \mathcal{SP}(prACP)$ and $p \,\|\, q \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that $p \rightsquigarrow u'$, $q \rightsquigarrow v'$, $p \rightsquigarrow u''$ and $q \rightsquigarrow v''$ for some $u', v', u'', v'' \in \mathcal{DP}(prACP)$ such that $u \equiv u' \mathbin{\lfloor\!\lfloor} q + v' \mathbin{\lfloor\!\lfloor} p + u'' \,|\, v''$. Then also $p \mathbin{\lfloor\!\lfloor} q \rightsquigarrow u' \mathbin{\lfloor\!\lfloor} q$, $q \mathbin{\lfloor\!\lfloor} p \rightsquigarrow v' \mathbin{\lfloor\!\lfloor} p$ and $p \,|\, q \rightsquigarrow u'' \,|\, v''$ from which we obtain that $p \mathbin{\lfloor\!\lfloor} q + q \mathbin{\lfloor\!\lfloor} p + p \,|\, q \rightsquigarrow u' \mathbin{\lfloor\!\lfloor} q + v' \mathbin{\lfloor\!\lfloor} p + u'' \,|\, v''$. Moreover $(u' \mathbin{\lfloor\!\lfloor} q + v' \mathbin{\lfloor\!\lfloor} p + u'' \,|\, v'')R(u' \mathbin{\lfloor\!\lfloor} q + v' \mathbin{\lfloor\!\lfloor} p + u'' \,|\, v'')$.

Suppose that $p \mathbin{\lfloor\!\lfloor} q + q \mathbin{\lfloor\!\lfloor} p + p \,|\, q \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules we obtain that $p \mathbin{\lfloor\!\lfloor} q \rightsquigarrow u'$, $q \mathbin{\lfloor\!\lfloor} p \rightsquigarrow v'$ and $p \,|\, q \rightsquigarrow w$ for some $u', v', w \in \mathcal{DP}(prACP)$ such that $u \equiv u' + v' + w$. It follows that $p \rightsquigarrow u''$, $q \rightsquigarrow v''$, $p \rightsquigarrow w'$ and $q \rightsquigarrow w''$ for some $u'', v'', w', w'' \in \mathcal{DP}(prACP)$ such that $u' \equiv u'' \mathbin{\lfloor\!\lfloor} q$, $v' \equiv v'' \mathbin{\lfloor\!\lfloor} p$, $w \equiv w' \,|\, w''$. Then also, $p \,\|\, q \rightsquigarrow u'' \mathbin{\lfloor\!\lfloor} q + v'' \mathbin{\lfloor\!\lfloor} p + w' \,|\, w''$. Moreover $(u'' \mathbin{\lfloor\!\lfloor} q + v'' \mathbin{\lfloor\!\lfloor} p + w' \,|\, w'')R(u'' \mathbin{\lfloor\!\lfloor} q + v'' \mathbin{\lfloor\!\lfloor} p + w' \,|\, w'')$.

Suppose $(p \,\|\, q)R(p \mathbin{\lfloor\!\lfloor} q + q \mathbin{\lfloor\!\lfloor} p + p \,|\, q)$ for some $p, q \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}(prACP)/R$, $M \subseteq \mathcal{DP}(prACP)$. From the previous discussion about the probabilistic transitions of these terms we get that if $u \in \mathcal{DP}(prACP)$, then $p \,\|\, q \rightsquigarrow u$ iff $p \mathbin{\lfloor\!\lfloor} q + q \mathbin{\lfloor\!\lfloor} p + p \,|\, q \rightsquigarrow u$. From Proposition 31 we obtain $\mu(p \,\|\, q, M) = \mu(p \mathbin{\lfloor\!\lfloor} q + q \mathbin{\lfloor\!\lfloor} p + p \,|\, q, M)$.

CM2: We define a relation R in the following way:

$$R = Eq\Big(\{(a \mathbin{\lfloor\!\lfloor} p, a \cdot p) \;:\; p \in \mathcal{SP}(prACP)\} \cup \{(\breve{a} \mathbin{\lfloor\!\lfloor} p, \breve{a} \cdot p) \;:\; p \in \mathcal{SP}(prACP)\}\Big).$$

We look at the transitions of both sides at the same time. Observe that $a \mathbin{\lfloor\!\lfloor} p$ and $a \cdot p$ can only do $a \mathbin{\lfloor\!\lfloor} p \rightsquigarrow \breve{a} \cdot p$ and $a \cdot p \rightsquigarrow \breve{a} \cdot p$, respectively, and $(\breve{a} \mathbin{\lfloor\!\lfloor} p)R(\breve{a} \cdot p)$.

Observe that $\breve{a} \mathbin{\lfloor\!\lfloor} p$ and $\breve{a} \cdot p$ for some $p \in \mathcal{SP}(prACP)$ can perform only an action transition $\breve{a} \mathbin{\lfloor\!\lfloor} p \xrightarrow{a} p$ and $\breve{a} \cdot p \xrightarrow{a} p$, respectively. Moreover pRp.

In order to prove that $\mu(a \mathbin{\lfloor\!\lfloor} p, M) = \mu(a \cdot p, M)$ for each $M \in \mathcal{PR}(prACP)/R$ we only need to notice that $\mu(a \mathbin{\lfloor\!\lfloor} p, \breve{a} \mathbin{\lfloor\!\lfloor} p) = 1$ and $\mu(a \cdot p, \breve{a} \cdot p) = 1$ and $\breve{a} \mathbin{\lfloor\!\lfloor} p \in M$ iff $\breve{a} \cdot p \in M$.

CM3: We define a relation R in the following way:

$$R = Eq\Big(\{(a \cdot p \mathbin{\lfloor\!\lfloor} q, a \cdot (p \,\|\, q)) \;:\; p, q \in \mathcal{SP}(prACP)\} \cup \{(\breve{a} \cdot p \mathbin{\lfloor\!\lfloor} q, \breve{a} \cdot (p \,\|\, q)) \;:\; p, q \in \mathcal{SP}(prACP)\}\Big).$$

Suppose $(a \cdot p \mathbin{\lfloor\!\lfloor} q)R(a \cdot (p \,\|\, q))$ for some $p, q \in \mathcal{SP}(prACP)$. Then from the definition of the operational rules it follows that the only possible probabilistic transition for each of these terms is: $a \cdot p \mathbin{\lfloor\!\lfloor} q \rightsquigarrow \breve{a} \cdot p \mathbin{\lfloor\!\lfloor} q$ and $a \cdot (p \,\|\, q) \rightsquigarrow \breve{a} \cdot (p \,\|\, q)$. Moreover by the definition of R we have that $(\breve{a} \cdot p \mathbin{\lfloor\!\lfloor} q)R(\breve{a} \cdot (p \,\|\, q))$.

Observe that $\breve{a} \cdot p \mathbin{\lfloor\!\lfloor} q$ and $\breve{a} \cdot (p \,\|\, q)$ for some $p, q \in \mathcal{SP}(prACP)$ can perform only one action transition, viz. $\breve{a} \cdot p \mathbin{\lfloor\!\lfloor} q \xrightarrow{a} p \,\|\, q$ and $\breve{a} \cdot (p \,\|\, q) \xrightarrow{a} p \,\|\, q$, respectively. Moreover $(p \,\|\, q)R(p \,\|\, q)$.

From the previous discussion about the probabilistic transitions of $a \cdot p \mathbin{\lfloor\!\lfloor} q$ and $a \cdot (p \,\|\, q)$ it follows that for each $M \in \mathcal{PR}/R$ either $\mu(a \cdot p \mathbin{\lfloor\!\lfloor} q, M) = \mu(a \cdot (p \,\|\, q), M) = 1$ or
$\mu(a \cdot p \mathbin{\lfloor\!\lfloor} q, M) = \mu(a \cdot (p \,\|\, q), M) = 0$.

CM4: We define a relation R in the following way:

$$\begin{aligned} R = Eq\Big(&\{((p + q) \mathbin{\lfloor\!\lfloor} s, p \mathbin{\lfloor\!\lfloor} s + q \mathbin{\lfloor\!\lfloor} s) \;:\; p, q, s \in \mathcal{SP}(prACP)\} \\ &\cup \{((u + v) \mathbin{\lfloor\!\lfloor} s, u \mathbin{\lfloor\!\lfloor} s + v \mathbin{\lfloor\!\lfloor} s) \;:\; u, v \in \mathcal{DP}(prACP), s \in \mathcal{SP}(prACP)\}\Big). \end{aligned}$$

Suppose $((p+q)\mathbin{\lfloor\!\lfloor} s)R(p\mathbin{\lfloor\!\lfloor} s+q\mathbin{\lfloor\!\lfloor} s)$ for some $p,q,s \in \mathcal{SP}(prACP)$ and $(p+q)\mathbin{\lfloor\!\lfloor} s \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that $(p+q) \rightsquigarrow v$ for some $v \in \mathcal{DP}(prACP)$ such that $u \equiv v\mathbin{\lfloor\!\lfloor} s$ and also $p \rightsquigarrow v'$ and $q \rightsquigarrow v''$ for some $v', v'' \in \mathcal{DP}(prACP)$ such that $v \equiv v' + v''$. Then we obtain that $p\mathbin{\lfloor\!\lfloor} s \rightsquigarrow v'\mathbin{\lfloor\!\lfloor} s$ and $q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow v''\mathbin{\lfloor\!\lfloor} s$ and also $p\mathbin{\lfloor\!\lfloor} s + q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow v'\mathbin{\lfloor\!\lfloor} s + v''\mathbin{\lfloor\!\lfloor} s$. Moreover we have that $((v'+v'')\mathbin{\lfloor\!\lfloor} s)R(v'\mathbin{\lfloor\!\lfloor} s + v''\mathbin{\lfloor\!\lfloor} s)$.

Suppose that $p\mathbin{\lfloor\!\lfloor} s + q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that $p\mathbin{\lfloor\!\lfloor} s \rightsquigarrow v$ and $q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow w$ for some $v, w \in \mathcal{DP}(prACP)$ such that $u \equiv v + w$. And also $p \rightsquigarrow v'$ and $q \rightsquigarrow w'$ for some $v', w' \in \mathcal{DP}(prACP)$ such that $v \equiv v'\mathbin{\lfloor\!\lfloor} s$ and $w \equiv w'\mathbin{\lfloor\!\lfloor} s$. Then we obtain that $p+q \rightsquigarrow v'+w'$ and also $(p+q)\mathbin{\lfloor\!\lfloor} s \rightsquigarrow (v'+w')\mathbin{\lfloor\!\lfloor} s$. Moreover we have that $((v'+w')\mathbin{\lfloor\!\lfloor} s)R(v'\mathbin{\lfloor\!\lfloor} s + w'\mathbin{\lfloor\!\lfloor} s)$.

Suppose $((u+v)\mathbin{\lfloor\!\lfloor} s)R(u\mathbin{\lfloor\!\lfloor} s + v\mathbin{\lfloor\!\lfloor} s)$ for some $u, v \in \mathcal{DP}(prACP)$, $s \in \mathcal{SP}(prACP)$ and $(u+v)\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}(prACP)$. Then from the definition of the operational rules it follows that $u+v \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}(prACP)$ such that $p \equiv p'\mathbin{\lfloor\!\lfloor} s$. Then either $u \xrightarrow{a} p'$ and in this case we obtain $u\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$, or $v \xrightarrow{a} p'$ which implies $v\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$. In each of these cases we have that $u\mathbin{\lfloor\!\lfloor} s + v\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$. Moreover pRp.

If $u\mathbin{\lfloor\!\lfloor} s + v\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}(prACP)$, then either $u\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$, from which it follows that $u \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}(prACP)$ such that $p \equiv p'\mathbin{\lfloor\!\lfloor} s$, or $v\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$, from which we obtain that $v \xrightarrow{a} p'$ for some $p' \in \mathcal{SP}(prACP)$ such that $p \equiv p'\mathbin{\lfloor\!\lfloor} s$. In each of these cases we have that $u+v \xrightarrow{a} p'$ and also $(u+v)\mathbin{\lfloor\!\lfloor} s \xrightarrow{a} p$. Moreover pRp.

Suppose $((p+q)\mathbin{\lfloor\!\lfloor} s)R(p\mathbin{\lfloor\!\lfloor} s + q\mathbin{\lfloor\!\lfloor} s)$ for some $p,q,s \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}(prACP)$. From the previous discussion about the probabilistic transitions we get that:
$(p+q)\mathbin{\lfloor\!\lfloor} s \rightsquigarrow (u+v)\mathbin{\lfloor\!\lfloor} s$ iff $p\mathbin{\lfloor\!\lfloor} s + q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow (u\mathbin{\lfloor\!\lfloor} s + v\mathbin{\lfloor\!\lfloor} s)$ for some $u, v \in \mathcal{DP}(prACP)$ such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. Moreover, using the definition of the probability distribution function we obtain:
$\mu((p+q)\mathbin{\lfloor\!\lfloor} s, (u+v)\mathbin{\lfloor\!\lfloor} s) = \mu(p+q, u+v) = \mu(p,u)\mu(q,v)$ and
$\mu(p\mathbin{\lfloor\!\lfloor} s + q\mathbin{\lfloor\!\lfloor} s, u\mathbin{\lfloor\!\lfloor} s + v\mathbin{\lfloor\!\lfloor} s) = \mu(p\mathbin{\lfloor\!\lfloor} s, u\mathbin{\lfloor\!\lfloor} s)\mu(q\mathbin{\lfloor\!\lfloor} s, v\mathbin{\lfloor\!\lfloor} s) = \mu(p,u)\mu(q,v)$.
The result $\mu((p+q)\mathbin{\lfloor\!\lfloor} s, M) = \mu(p\mathbin{\lfloor\!\lfloor} s + q\mathbin{\lfloor\!\lfloor} s, M)$ follows from Proposition 31.

PrCM1: We define a relation R in the following way:

$$R = Eq\Big(\{((p \sqcup\!\!\!\!+_{\pi} q)\mathbin{\lfloor\!\lfloor} s, p\mathbin{\lfloor\!\lfloor} s \sqcup\!\!\!\!+_{\pi} q\mathbin{\lfloor\!\lfloor} s) \ : \ p,q,s \in \mathcal{SP}(prACP)\}\Big).$$

Suppose $((p \sqcup\!\!\!\!+_{\pi} q)\mathbin{\lfloor\!\lfloor} s)R(p\mathbin{\lfloor\!\lfloor} s \sqcup\!\!\!\!+_{\pi} q\mathbin{\lfloor\!\lfloor} s)$ for some $p,q,s \in \mathcal{SP}(prACP)$ and $(p \sqcup\!\!\!\!+_{\pi} q)\mathbin{\lfloor\!\lfloor} s \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that $(p \sqcup\!\!\!\!+_{\pi} q) \rightsquigarrow v$ for some $v \in \mathcal{DP}(prACP)$ such that $u \equiv v\mathbin{\lfloor\!\lfloor} s$. Two situations can occur:

1. $p \rightsquigarrow v$: then from the definition of the operational rules it follows that $p\mathbin{\lfloor\!\lfloor} s \rightsquigarrow v\mathbin{\lfloor\!\lfloor} s$ and also $p\mathbin{\lfloor\!\lfloor} s \sqcup\!\!\!\!+_{\pi} q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow u$. Moreover uRu.
2. $q \rightsquigarrow v$: then from the definition of the operational rules it follows that $q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow v\mathbin{\lfloor\!\lfloor} s$ and also $p\mathbin{\lfloor\!\lfloor} s \sqcup\!\!\!\!+_{\pi} q\mathbin{\lfloor\!\lfloor} s \rightsquigarrow u$. Moreover uRu.

Suppose that $p \lfloor\!\lfloor s \uplus_\pi q \lfloor\!\lfloor s \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that one of the following situations is possible:

1. $p \lfloor\!\lfloor s \rightsquigarrow u$: then from the definition of the operational rules we have that $p \rightsquigarrow v$ for some $v \in \mathcal{DP}(prACP)$ such that $u \equiv v \lfloor\!\lfloor s$ and also $p \uplus_\pi q \rightsquigarrow v$. Then we have $(p \uplus_\pi q) \lfloor\!\lfloor s \rightsquigarrow v \lfloor\!\lfloor s$, that is $(p \uplus_\pi q) \lfloor\!\lfloor s \rightsquigarrow u$. Moreover uRu.
2. $q \lfloor\!\lfloor s \rightsquigarrow u$: then from the definition of the operational rules we have that $q \rightsquigarrow v$ for some $v \in \mathcal{DP}(prACP)$ such that $u \equiv v \lfloor\!\lfloor s$ and also $p \uplus_\pi q \rightsquigarrow v$. Then we have $(p \uplus_\pi q) \lfloor\!\lfloor s \rightsquigarrow v \lfloor\!\lfloor s$, that is $(p \uplus_\pi q) \lfloor\!\lfloor s \rightsquigarrow u$. Moreover uRu.

Suppose $((p \uplus_\pi q) \lfloor\!\lfloor s) R (p \lfloor\!\lfloor s \uplus_\pi q \lfloor\!\lfloor s)$ for some $p, q, s \in \mathcal{SP}(prACP)$ and $M \in \mathcal{PR}/R, M \subseteq \mathcal{DP}(prACP)$. From the previous discussion about the probabilistic transitions of $(p \uplus_\pi q) \lfloor\!\lfloor s$ and $p \lfloor\!\lfloor s \uplus_\pi q \lfloor\!\lfloor s$ we have that $(p \uplus_\pi q) \lfloor\!\lfloor s \rightsquigarrow v \lfloor\!\lfloor s$ iff $p \lfloor\!\lfloor s \uplus_\pi q \lfloor\!\lfloor s \rightsquigarrow v \lfloor\!\lfloor s$. Moreover,
$\mu((p \uplus_\pi q) \lfloor\!\lfloor s, v \lfloor\!\lfloor s) = \mu(p \uplus_\pi q, v) = \pi\mu(p, v) + (1 - \pi)\mu(q, v)$ and
$\mu(p \lfloor\!\lfloor s \uplus_\pi q \lfloor\!\lfloor s, v \lfloor\!\lfloor s) = \pi\mu(p \lfloor\!\lfloor s, v \lfloor\!\lfloor s) + (1 - \pi)\mu(q \lfloor\!\lfloor s, v \lfloor\!\lfloor s) = \pi\mu(p, v) + (1 - \pi)\mu(q, v)$.
It follows that $\mu((p \uplus_\pi q) \lfloor\!\lfloor s, M) = \mu(p \lfloor\!\lfloor s \uplus_\pi q \lfloor\!\lfloor s, M)$.

CM5: We define a relation R in the following way:

$$R = Eq\Big(\{(a \cdot p \,|\, b, (a \,|\, b) \cdot p) \ : \ p \in \mathcal{SP}(prACP)\} \cup \{(\breve{a} \cdot p \,|\, \breve{b}, \breve{c} \cdot p) \ : \ p \in \mathcal{SP}(prACP)\}\Big)$$

where we denote shortly $\gamma(a, b) = c$.

Suppose $(a \cdot p \,|\, b) R ((a \,|\, b) \cdot p)$ for some $p \in \mathcal{SP}(prACP)$. Then from the definition of the operational rules it follows that the only possible probabilistic transition for each of these terms is: $a \cdot p \,|\, b \rightsquigarrow \breve{a} \cdot p \,|\, \breve{b}$ and $(a \,|\, b) \cdot p \rightsquigarrow \breve{c} \cdot p$. Moreover by the definition of R we have that $(\breve{a} \cdot p \,|\, \breve{b}) R (\breve{c} \cdot p)$.

Suppose that $(\breve{a} \cdot p \,|\, \breve{b}) R (\breve{c} \cdot p)$. If $\breve{c} \equiv \breve{\delta}$ then both terms cannot perform any action transition. If $\breve{c} \not\equiv \breve{\delta}$, then both terms can perform only a $c-$action transition as follows: $\breve{a} \cdot p \,|\, \breve{b} \xrightarrow{c} p$ and $\breve{c} \cdot p \xrightarrow{c} p$. Moreover pRp.

From the previous discussion about the probabilistic transitions of $a \cdot p \,|\, b$ and $(a \,|\, b) \cdot p$ we have that $\mu(a \cdot p \,|\, b, \breve{a} \cdot p \,|\, \breve{b}) = 1$ and $\mu((a \,|\, b) \cdot p, \breve{c} \cdot p) = 1$ and $\breve{a} \cdot p \,|\, \breve{b} \in M$ iff $\breve{c} \cdot p \in M$. From here it follows that for each $M \in \mathcal{PR}/R$ either $\mu(a \cdot p \,|\, b, M) = \mu((a \,|\, b) \cdot p, M) = 1$ or $\mu(a \cdot p \,|\, b, M) = \mu((a \,|\, b) \cdot p, M) = 0$.

CM6: We define a relation R in the following way:

$$R = Eq\Big(\{(a \,|\, b \cdot p, (a \,|\, b) \cdot p) \ : \ p \in \mathcal{SP}(prACP)\} \cup \{(\breve{a} \,|\, \breve{b} \cdot p, \breve{c} \cdot p) \ : \ p \in \mathcal{SP}(prACP)\}\Big)$$

where we denote shortly $\gamma(a, b) = c$.

The proof that R is a bisimulation relation is similar to the proof of axiom CM5.

CM7: We define a relation R in the following way:

$$R = Eq\Big(\{(a \cdot p \,|\, b \cdot q, (a \,|\, b) \cdot (p \,\|\, q)) : p, q \in \mathcal{SP}(prACP)\} \cup \{(\breve{a} \cdot p \,|\, \breve{b} \cdot q, \breve{c} \cdot (p \,\|\, q)) : p, q \in \mathcal{SP}(prACP)\}\Big)$$

where we denote shortly $\gamma(a, b) = c$.

Suppose $(a\cdot p\,|\,b\cdot q)R((a\,|\,b)\cdot(p\,\|\,q))$ for some $p,q\in\mathcal{SP}(prACP)$. Then from the definition of the operational rules it follows that we need to consider only the following probabilistic transitions: $a\rightsquigarrow\breve{a}$ and $b\rightsquigarrow\breve{b}$ and also $a\cdot p\rightsquigarrow\breve{a}\cdot p$, $b\cdot q\rightsquigarrow\breve{b}\cdot q$. Thus, $a\cdot p\,|\,b\cdot q\rightsquigarrow\breve{a}\cdot p\,|\,\breve{b}\cdot q$ and $(a\,|\,b)\cdot(p\,\|\,q)\rightsquigarrow\breve{c}\cdot(p\,\|\,q)$. Moreover $(\breve{a}\cdot p\,|\,\breve{b}\cdot q)R(\breve{c}\cdot(p\,\|\,q))$.

Suppose that $(\breve{a}\cdot p\,|\,\breve{b}\cdot q)R(\breve{c}\cdot(p\,\|\,q))$. If $\breve{c}\equiv\breve{\delta}$ then both terms cannot perform any action transition. If $\breve{c}\not\equiv\breve{\delta}$, then both terms can perform only a $c-$action transition as follows: $\breve{a}\cdot p\,|\,\breve{b}\cdot q\xrightarrow{c}p\,\|\,q$ and $\breve{c}\cdot(p\,\|\,q)\xrightarrow{c}p\,\|\,q$. Moreover $(p\,\|\,q)R(p\,\|\,q)$.

From the previous discussion about the probabilistic transitions of $a\cdot p\,|\,b\cdot q$ and $(a\,|\,b)\cdot(p\,\|\,q)$ we have that $\mu(a\cdot p\,|\,b\cdot q,\breve{a}\cdot p\,|\,\breve{b}\cdot q)=1$ and $\mu((a\,|\,b)\cdot(p\,\|\,q),\breve{c}\cdot(p\,\|\,q))=1$ and $\breve{a}\cdot p\,|\,\breve{b}\cdot q\in M$ iff $\breve{c}\cdot(p\,\|\,q)\in M$. It follows that for each $M\in\mathcal{PR}/R$ either $\mu(a\cdot p\,|\,b\cdot q,M)=\mu((a\,|\,b)\cdot(p\,\|\,q),M)=1$ or $\mu(a\cdot p\,|\,b\cdot q,M)=\mu((a\,|\,b)\cdot(p\,\|\,q),M)=0$.

PrCM2: We define a relation R in the following way:

$$R=Eq\Big(\{((p\uplus_{\pi}q)\,|\,s,p\,|\,s\uplus_{\pi}q\,|\,s)\ :\ p,q,s\in\mathcal{SP}(prACP)\}\Big).$$

Suppose $((p\uplus_{\pi}q)\,|\,s)R(p\,|\,s\uplus_{\pi}q\,|\,s)$ for some $p,q,s\in\mathcal{SP}(prACP)$ and $(p\uplus_{\pi}q)\,|\,s\rightsquigarrow u$ for some $u\in\mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that $p\uplus_{\pi}q\rightsquigarrow v$ and $s\rightsquigarrow w$ for some $v,w\in\mathcal{DP}(prACP)$ such that $u\equiv v\,|\,w$. Two situations can occur:

1. $p\rightsquigarrow v$: then from the definition of the operational rules it follows that $p\,|\,s\rightsquigarrow v\,|\,w$ and also $p\,|\,s\uplus_{\pi}q\,|\,s\rightsquigarrow u$. Moreover uRu.
2. $q\rightsquigarrow v$: then from the definition of the operational rules it follows that $q\,|\,s\rightsquigarrow v\,|\,w$ and also $p\,|\,s\uplus_{\pi}q\,|\,s\rightsquigarrow v\,|\,w$. Moreover uRu.

Suppose that $p\,|\,s\uplus_{\pi}q\,|\,s\rightsquigarrow u$ for some $u\in\mathcal{DP}(prACP)$. Then from the definition of the operational rules it follows that either

1. $p\,|\,s\rightsquigarrow u$: then $p\rightsquigarrow v$ and $s\rightsquigarrow w$ for some $v,w\in\mathcal{DP}(prACP)$ such that $u\equiv v\,|\,w$ and $p\uplus_{\pi}q\rightsquigarrow v$ and also $(p\uplus_{\pi}q)\,|\,s\rightsquigarrow v\,|\,w$, that is $(p\uplus_{\pi}q)\,|\,s\rightsquigarrow u$. Moreover uRu.
2. $q\,|\,s\rightsquigarrow u$: then $q\rightsquigarrow v$ and $s\rightsquigarrow w$ for some $v,w\in\mathcal{DP}(prACP)$ such that $u\equiv v\,|\,w$ and $p\uplus_{\pi}q\rightsquigarrow v$ and also $(p\uplus_{\pi}q)\,|\,s\rightsquigarrow v\,|\,w$, that is $(p\uplus_{\pi}q)\,|\,s\rightsquigarrow u$. Moreover uRu.

Suppose $((p\uplus_{\pi}q)\,|\,s)R(p\,|\,s\uplus_{\pi}q\,|\,s)$ for some $p,q,s\in\mathcal{SP}(prACP)$ and $M\in\mathcal{PR}/R$, $M\subseteq\mathcal{DP}(prACP)$. From the previous discussion about the probabilistic transitions we get that: $(p\uplus_{\pi}q)\,|\,s\rightsquigarrow v\,|\,w$ iff $p\,|\,s\uplus_{\pi}q\,|\,s\rightsquigarrow v\,|\,w$. Moreover
$\mu((p\uplus_{\pi}q)\,|\,s,v\,|\,w)=\mu(p\uplus_{\pi}q,v)\mu(s,w)=(\pi\mu(p,v)+(1-\pi)\mu(q,v))\mu(s,w)$ and
$\mu(p\,|\,s\uplus_{\pi}q\,|\,s,v\,|\,w)=\pi\mu(p\,|\,s,v\,|\,w)+(1-\pi)\mu(q\,|\,s,v\,|\,w)=\pi\mu(p,v)\mu(s,w)+(1-\pi)\mu(q,v)\mu(s,w)$.
It follows that $\mu((p\uplus_{\pi}q)\,|\,s,M)=\mu(p\,|\,s\uplus_{\pi}q\,|\,s,M)$.

PrCM3: We define a relation R in the following way:

$$R=Eq\Big(\{(p\,|\,(q\uplus_{\pi}s),p\,|\,s\uplus_{\pi}p\,|\,s)\ :\ p,q,s\in\mathcal{SP}(prACP)\}\Big).$$

In a similar way as in the proof of axiom PrCM2 we can prove that R is a bisimulation relation.

Further, we give the proof of soundness of DyPR rule. In contrast to previous proofs, in which we construct a relation for which we prove that it is a bisimulation relation, in this proof we use as a bisimulation relation $\underline{\leftrightarrow}$.

Let $s \in \mathcal{SP}(prACP)$ such that $s \underline{\leftrightarrow} s + s$ and $W = \{w_i : w_i \in \mathcal{DP}(prACP), s \rightsquigarrow w_i\}$. By Lemma 50 we have that for each $w, w' \in W$, $w \underline{\leftrightarrow} w'$. Moreover $\mu(s, W) = 1$.

We will prove that for arbitrary $p, q \in \mathcal{SP}(prACP)$, $(p + q) \,|\, s \underline{\leftrightarrow} p \,|\, s + q \,|\, s$.

Let us suppose that $(p+q) \,|\, s \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. We have that $p+q \rightsquigarrow u', s \rightsquigarrow w$ for some $u' \in \mathcal{DP}(prACP), w \in W$ such that $u \equiv u' \,|\, w$ and also there exist $v, v' \in \mathcal{SP}(prACP)$ such that $p \rightsquigarrow v, q \rightsquigarrow v', u' \equiv v + v'$. Then we obtain $p \,|\, s \rightsquigarrow v \,|\, w$ and $q \,|\, s \rightsquigarrow v' \,|\, w$ and also $p \,|\, s+q \,|\, s \rightsquigarrow v \,|\, w+v' \,|\, w$. We proved that if $(p+q) \,|\, s \rightsquigarrow (v+v') \,|\, w$ then $p \,|\, s+q \,|\, s \rightsquigarrow v \,|\, w+v' \,|\, w$. According to the definition of bisimulation relation we need to prove

$(v + v') \,|\, w \underline{\leftrightarrow} v \,|\, w + v' \,|\, w.$ (1)

Let us suppose that $p \,|\, s + q \,|\, s \rightsquigarrow u$ for some $u \in \mathcal{DP}(prACP)$. It follows that there exist $u', u'' \in \mathcal{SP}(prACP)$ such that $p \,|\, s \rightsquigarrow u', q \,|\, s \rightsquigarrow u''$ and $u \equiv u' + u''$. Then it follows that there exist $v, v' \in \mathcal{SP}(prACP)$, $w, w' \in W$ such that $p \rightsquigarrow v, s \rightsquigarrow w, q \rightsquigarrow v', s \rightsquigarrow w'$ and $u' \equiv v \,|\, w, u'' \equiv v' \,|\, w'$. Thus, $p + q \rightsquigarrow v + v'$ from which $(p + q) \,|\, s \rightsquigarrow (v + v') \,|\, w$. With this we proved that if $p \,|\, s + q \,|\, s \rightsquigarrow v \,|\, w + v' \,|\, w'$ then $(p + q) \,|\, s \rightsquigarrow (v + v') \,|\, w$. Moreover we need to prove that $(v + v') \,|\, w \underline{\leftrightarrow} v \,|\, w + v' \,|\, w'$. (2)

One can see that (1) is a special case of (2). According to this it is sufficient to prove case (2).

Suppose that $(v + v') \,|\, w \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}(prACP)$. It implies that there exist $b, c \in A$ and $p', p'' \in \mathcal{SP}(prACP)$ such that $v + v' \xrightarrow{b} p'$, $w \xrightarrow{c} p''$ and $\gamma(b, c) = a$ and $p \equiv p' \,\|\, p''$. Then either $v \xrightarrow{b} p'$ or $v' \xrightarrow{b} p'$. In the first case we obtain that $v \,|\, w \xrightarrow{a} p' \,\|\, p''$ and also $v \,|\, w+v' \,|\, w' \xrightarrow{a} p' \,\|\, p''$ and $p' \,\|\, p'' \underline{\leftrightarrow} p' \,\|\, p''$. In the second case by the fact that $w \underline{\leftrightarrow} w'$ we obtain that $w' \xrightarrow{c} p''_1$ for some $p''_1 \in \mathcal{SP}(prACP)$ such that $p'' \underline{\leftrightarrow} p''_1$. Then we obtain $v' \,|\, w' \xrightarrow{a} p' \,\|\, p''_1$ and also $v \,|\, w + v' \,|\, w' \xrightarrow{a} p' \,\|\, p''_1$. By the Congruence theorem (Theorem 45) we obtain that $p' \,\|\, p'' \underline{\leftrightarrow} p' \,\|\, p''_1$.

Suppose that $v \,|\, w + v' \,|\, w' \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}(prACP)$. It follows that $v \,|\, w \xrightarrow{a} p$ or $v' \,|\, w' \xrightarrow{a} p$. In the first case we have that there exist $b, c \in A$ and $p', p'' \in \mathcal{SP}(prACP)$ such that $v \xrightarrow{b} p'$, $w \xrightarrow{c} p''$ and $\gamma(b, c) = a$ and $p \equiv p' \,\|\, p''$. Then we have that $v + v' \xrightarrow{b} p'$ and also $(v + v') \,|\, w \xrightarrow{a} p' \,\|\, p''$. Moreover $p' \,\|\, p'' \underline{\leftrightarrow} p' \,\|\, p''$. In the second case we have that there exist $b, c \in A$ and $p', p''_1 \in \mathcal{SP}(prACP)$ such that $v \xrightarrow{b} p'$, $w' \xrightarrow{c} p''_1$, $\gamma(b, c) = a$ and $p \equiv p' \,\|\, p''_1$. By the fact that $w \underline{\leftrightarrow} w'$ we obtain that $w \xrightarrow{c} p''$ for some $p'' \in \mathcal{SP}(prACP)$ and $p'' \underline{\leftrightarrow} p''_1$. Then we obtain $v + v' \xrightarrow{b} p'$ and also $(v + v') \,|\, w \xrightarrow{a} p' \,\|\, p''$. Moreover by Theorem 45 we have $p' \,\|\, p'' \underline{\leftrightarrow} p' \,\|\, p''_1$.

Herewith we proved (1) and (2) are valid.

Let us consider the value of $\mu((p + q) \,|\, s, M)$ and $\mu(p \,|\, s + q \,|\, s, M)$ for $M \in \mathcal{PR}(prACP)/\underline{\leftrightarrow}$,

$M \subseteq \mathcal{DP}(prACP)$. From the previous discussion about the probabilistic transitions of $(p+q)\,|\,s$ and $p\,|\,s+q\,|\,s$ we have that:

1. if $(p+q)\,|\,s \rightsquigarrow u$ then $u \equiv (v+v')\,|\,w$ for some $v, v' \in \mathcal{DP}(prACP)$ and $w \in W$. Then $p\,|\,s+q\,|\,s \rightsquigarrow v\,|\,w+v'\,|\,w$ and $(v+v')\,|\,w \underline{\leftrightarrow} v\,|\,w+v'\,|\,w$;
2. if $p\,|\,s+q\,|\,s \rightsquigarrow v\,|\,w+v'\,|\,w$ then $p\,|\,s+q\,|\,s \rightsquigarrow v\,|\,w+v'\,|\,w'$ as well and moreover $v\,|\,w+v'\,|\,w \underline{\leftrightarrow} v\,|\,w+v'\,|\,w'$ for each $w' \in W$.

It follows that $(v+v')\,|\,w \in M$ iff $v\,|\,w+v'\,|\,w \in M$ iff $v\,|\,w+v'\,|\,w' \in M$ for $w' \in W$. (3)

Under the assumption that M is a reachable class from $(p+q)\,|\,s$ and $p\,|\,s+q\,|\,s$ we define the following subsets of M:

$$M_w = \{(v+v')\,|\,w \;:\; v,v' \in \mathcal{DP}(prACP)\} \cup \{v\,|\,w+v'\,|\,w' \;:\; w' \in W, v, v' \in \mathcal{DP}(prACP)\},$$

for each $w \in W$. It is obviously that if $m \in M \setminus (\bigcup_{w \in W} M_w)$ then both $\neg((p+q)\,|\,s \rightsquigarrow m)$ and $\neg(p\,|\,s+q\,|\,s \rightsquigarrow m)$ and moreover if $w \not\equiv w'$ then $M_w \cap M_{w'} = \emptyset$. Then for each $w \in W$ we have:

$$\mu((p+q)\,|\,s, M_w) = \mu((p+q)\,|\,s, \{(v+v')\,|\,w \;:\; v,v' \in \mathcal{DP}(prACP)\}) =$$
$$\sum_{v,v'} \mu((p+q)\,|\,s, (v+v')\,|\,w) = \sum_{v,v'} \mu(p,v)\mu(q,v')\mu(s,w) \tag{4}$$

and

$$\mu(p\,|\,s+q\,|\,s, M_w) = \mu(p\,|\,s+q\,|\,s, \{v\,|\,w+v'\,|\,w' \;:\; w' \in W, v, v' \in \mathcal{DP}(prACP)\}) =$$
$$\sum_{v,v',w'} \mu(p\,|\,s+q\,|\,s, v\,|\,w+v'\,|\,w') = \sum_{v,v',w'} \mu(p,v)\mu(q,v')\mu(s,w)\mu(s,w') =$$
$$\sum_{v,v'} \mu(p,v)\mu(q,v')\mu(s,w)(\sum_{w'} \mu(s,w')) = \sum_{v,v'} \mu(p,v)\mu(q,v')\mu(s,w)\mu(s,W) =$$
$$\sum_{v,v'} \mu(p,v)\mu(q,v')\mu(s,w). \tag{5}$$

From (4) and (5) we obtain that for each $w \in W$, $\mu((p+q)\,|\,s, M_w) = \mu(p\,|\,s+q\,|\,s, M_w)$ and using Propsition 21 we obtain:

$$\mu((p+q)\,|\,s, M) = \mu((p+q)\,|\,s, \bigcup_{w \in W} M_w) = \sum_{w \in W} \mu((p+q)\,|\,s, M_w) = \sum_{w \in W} \mu(p\,|\,s+q\,|\,s, M_w) =$$
$$\mu(p\,|\,s+q\,|\,s, \bigcup_{w \in W} M_w) = \mu(p\,|\,s+q\,|\,s, M). \qquad \Box$$

3.3 Conservative extension theorem. Completeness of *prACP*

In order to prove the Completeness theorem of *prACP* we use the method proposed in [22, 3, 7] which is based on an analysis of the operational semantics of both, *prBPA* and *prACP*. More precisely this method is based on an analysis of the form of the deduction rules which built the operational semantics, and the operationally conservative extension property as well as the equational conservative extension property which says that the added operators $\|$, $\lfloor\!\lfloor$, $|$ and ∂ do not yield any new identities between *prBPA* terms. Briefly, we will give the basic concepts of this approach and some necessary definitions and theorems which are taken from [3] and adapted to the presented problem.

Let Σ be a signature, V an infinite set of variables, T_r a set of relation symbols and T_p a set of predicate symbols. We denote the set of closed terms over Σ by $C(\Sigma)$ and the set of (open) terms by $O(\Sigma)$. If $P \in T_p$, $R \in T_r$ and $s, t, u \in O(\Sigma)$ then we call the expressions Ps, tRu (positive) formulas.

As in our operational semantics negative premises do not appear, we consider only positive formulas.

Definition52. A term deduction system is a structure (Σ, D, T_p, T_r) with Σ a signature and D a set of deduction rules. A deduction rule $d \in D$ has the form $\dfrac{H}{C}$ with H a set of formulas and C a formula. The formulas from H are called hypotheses of d and C is called the conclusion of d. If the set of hypotheses of a deduction rule is empty we call such a rule an axiom.

Often instead (Σ, D, T_p, T_r) we will write shortly (Σ, D).

Definition53. Let $T = (\Sigma, D, T_p, T_r)$ be a term deduction system. Let I and J be index sets of arbitrary cardinality, let $t_i, s_j, t \in O(\Sigma)$ for all $i \in I$ and $j \in J$, let $P_j, P \in T_p$ be predicate symbols for all $j \in J$, and let $R_i, R \in T_r$ be relation symbols for all $i \in I$. A deduction rule $d \in D$ is in *path* format if it has one of the following four forms:

$$\frac{\{P_j s_j \ : \ j \in J\} \cup \{t_i R_i y_i \ : \ i \in I\}}{f(x_1, \ldots, x_n) R t},$$

with $f \in \Sigma$ an $n-$ary function symbol, $X = \{x_1, \ldots, x_n\}$, $Y = \{y_i \ : \ i \in I\}$ and $X \cup Y \subseteq V$ a set of distinct variables;

$$\frac{\{P_j s_j \ : \ j \in J\} \cup \{t_i R_i y_i \ : \ i \in I\}}{x R t},$$

with $X = \{x\}$, $Y = \{y_i \ : \ i \in I\}$ and $X \cup Y \subseteq V$ a set of distinct variables;

$$\frac{\{P_j s_j \ : \ j \in J\} \cup \{t_i R_i y_i \ : \ i \in I\}}{P f(x_1, \ldots, x_n)},$$

with $f \in \Sigma$ an $n-$ary function symbol, $X = \{x_1, \ldots, x_n\}$, $Y = \{y_i \ : \ i \in I\}$ and $X \cup Y \subseteq V$ a set of distinct variables or

$$\frac{\{P_j s_j \ : \ j \in J\} \cup \{t_i R_i y_i \ : \ i \in I\}}{P x},$$

with $X = \{x\}$, $Y = \{y_i \ : \ i \in I\}$ and $X \cup Y \subseteq V$ a set of distinct variables.

If in the above four cases $var(d) = X \cup Y$ we say that the deduction rule d is pure.

We say that a term deduction system is in *path* format if all its deduction rules are in *path* format. We say that a term deduction system is pure if all its deduction rules are pure.

Definition 54. Let Σ_0 and Σ_1 be two signatures. If for all operators $f \in \Sigma_0 \cap \Sigma_1$ the arity of f in Σ_0 is the same as its arity in Σ_1, then the sum of Σ_0 and Σ_1, notation $\Sigma_0 \oplus \Sigma_1$, is defined and is equal to the signature $\Sigma_0 \cup \Sigma_1$.

Definition 55. Let $T_0 = (\Sigma_0, D_0)$ and $T_1 = (\Sigma_1, D_1)$ be two term deduction systems with predicate and relation symbol T_p^i and T_r^i respectively ($i = 0, 1$). Let $\Sigma_0 \oplus \Sigma_1$ be defined. The sum of T_0 and T_1, notation $T_0 \oplus T_1$, is the term deduction system $(\Sigma_0 \oplus \Sigma_1, D_0 \cup D_1)$ with predicate and relation symbols $T_p^0 \cup T_p^1$ and $T_r^0 \cup T_r^1$, respectively.

According to this concept and the problem we are faced with, in the following we consider the term deduction system $T(prBPA) = (\check{\Sigma}_{prBPA}, D_{prBPA})$ with the term deduction rules given in Table 4, the term deduction system $T_{ex} = (\check{\Sigma}_{prACP}, D_{ex})$ with the term deduction rules given in Table 7 and the sum of these systems, the term deduction system $T = (\check{\Sigma}_{prACP}, D_{prACP})$ with the term deduction rules given in Table 4 and Table 7.

Definition 56. Let $T = (\Sigma, D)$ be a term deduction system and let F be a set of formulas. The variable dependency graph of F is a directed graph with variables occurring in F as its nodes. The edge $x \longrightarrow y$ is an edge of the variable dependency graph if and only if there is a relation $tRs \in F$ with $x \in var(t)$ and $y \in var(s)$.

The set F is well-founded if any backward chain of edges in its variable dependency graph is finite. A deduction rule is called well-founded if its set of hypothesis is so. A term deduction system is called well-founded if all its rules are well-founded.

It is not hard to verify that the following lemmas are valid.

Lemma 57. *The term deduction system $T(prBPA)$ is a pure well-founded term deduction system in path format.* □

Lemma 58. *The term deduction system T_{ex} is a pure well-founded term deduction system in path format.* □

Definition 59. Let $T_0 = (\Sigma_0, D_0)$ and $T_1 = (\Sigma_1, D_1)$ be two term deduction systems with $T(\Sigma, D) = T_0 \oplus T_1$ defined. Let $D = D(T_p, T_r)$. The term deduction system T is called an operationally conservative extension of T_0 if for all $s, u \in C(\Sigma_0)$, for all relation symbols $R \in T_r$ and predicate symbols $P \in T_p$, and for all $t \in C(\Sigma)$ we have

$$T \vdash sRt \Leftrightarrow T_0 \vdash sRt$$

and

$$T \vdash Pu \Leftrightarrow T_0 \vdash Pu.$$

Now we give a theorem providing us with sufficient conditions so that a term deduction system is an operationally conservative extension of another one. This is a restricted version of the theorem (Theorem 2.4.15) formulated in [3].

Theorem 60. *Let $T_0 = (\Sigma_0, D_0)$ be a pure well-founded term deduction system in path format. Let $T_1 = (\Sigma_1, D_1)$ be a term deduction system in path format. Then if $T = T_0 \oplus T_1$ is defined then T is an operationally conservative extension of T_0.* □

As a conclusion of Lemma 57, Lemma 58 and 60 we obtain the following result:

Lemma 61. *The term deduction system T(prACP) is an operationally conservative extension of the term deduction system T(prBPA).* □

As the main aim is to prove the equational conservativity of two theories, it is needed to connect this property with the notion of operationally conservative extension proved above. And this method provides this relation using as an intermediate step, the notion of operational conservativity up to an equivalence relation φ. Here, φ equivalence is some semantical equivalence that is defined in terms of relation and predicate symbols only.

Definition 62. Let $T_0 = (\Sigma_0, D_0)$ and $T_1 = (\Sigma_1, D_1)$ be two term deduction systems with $T(\Sigma, D) = T_0 \oplus T_1$ defined. If we have for all $s, t \in C(\Sigma_0)$

$$s =_{\varphi}^{\oplus} t \Leftrightarrow s =_{\varphi}^{0} t$$

we say that T is an operationally conservative extension of T_0 up to φ equivalence, where φ is some semantical equivalence relation that is defined in terms of relation and predicate symbols only. By $s =_{\varphi} t$ we mean that s and t are in the same φ equivalence class. The superscripts $\oplus$ and 0 are to express the system in which this holds.

As we need to get an operationally conservative extension up to the probabilistic bisimulation, we need to check if this relation is defined "in terms of predicate and relations symbols". Besides the fourth clause in Definition 17, the probabilistic bisimulation is defined obviously in terms of predicate and relation symbols. Then from the previous theorem for operationally conservative extension we obtain that for each closed *prBPA* term s, its term-relation-predicate diagrams in both *T(prBPA)* and *T(prACP)* are the same. And also for these terms the probability distribution function is defined in the same way in both *T(prBPA)* and *T(prACP)*, which provides us with a conclusion that the fourth clause in Definition 17 does not disturb the notion of the probabilistic bisimulation in terms of predicate and relation symbols only.

Next, we give few results more which finally lead to the completeness property.

Theorem 63. *Let $T_0 = (\Sigma_0, D_0)$ and $T_1 = (\Sigma_1, D_1)$ be two term deduction systems and let $T(\Sigma, D) = T_0 \oplus T_1$ be defined. If T is an operationally conservative extension of T_0 then it is also* *an operationally conservative extension up to φ equivalence, where φ is an equivalence relation defined exclusively in terms of predicate and relation symbols.* □

Lemma 64. *Term deduction system $T(prACP)$ is an operationally conservative extension up to the probabilistic bisimulation of term deduction system $T(prBPA)$.* □

Definition 65. Let $L_0 = (\Sigma_0, E_0)$ and $L_1 = (\Sigma_1, E_1)$ be two equational specifications and let $\Sigma_0 \oplus \Sigma_1$ be defined. The sum $L_0 \oplus L_1$ of L_0 and L_1 is the equational specification $(\Sigma_0 \oplus \Sigma_1, E_0 \cup E_1)$.

Definition 66. Let $L_0 = (\Sigma_0, E_0)$ and $L_1 = (\Sigma_1, E_1)$ be two equational specifications and let $\Sigma_0 \oplus \Sigma_1$ be defined. We say that L is an equationally conservative extension of L_0 if for all $s, t \in C(\Sigma_0)$

$$L \vdash s = t \Leftrightarrow L_0 \vdash s = t.$$

Theorem 67. *Let $L_0 = (\Sigma_0, E_0)$ and $L_1 = (\Sigma_1, E_1)$ be equational specification and let $L = (\Sigma, E) = L_0 \oplus L_1$ be defined. Let $T_0 = (\Sigma_0, D_0)$ and $T_1 = (\Sigma_1, D_1)$ be term deduction systems and let $T = T_0 \oplus T_1$. Let φ be an equivalence relation that is definable in terms of predicate and relation symbols only. Let L_0 be a complete axiomatization with respect to the φ equivalence model induces by T_0 and let L be a sound axiomatization with respect to the φ equivalence model induced by T. If T is an operationally conservative extension of T_0 up to φ equivalence then L is an equationally conservative extension of L_0.* □

Lemma 68. *prACP is an equationally conservative extension of prBPA, that is, if t and s are closed prBPA terms, then*

$$prBPA \vdash t = s \Leftrightarrow prACP \vdash t = s.$$

□

Theorem 69. *If in addition to the conditions of Theorem 67 the equational specification L has the elimination property for L_0, the we have that E is a complete axiomatization with respect to the φ equivalence model induced by the term deduction system T.* □

Now from the previous results and from Theorem 39, Theorem 40 and Theorem 51 we obtain:

Theorem 70. *(Completeness) If t and s are closed prACP terms, then*
$t \mathrel{\underline{\leftrightarrow}} s \Rightarrow prACP + DyPR \vdash t = s.$ □

4 Extension with infinite processes

In this section we extend the theory by the notion of infinite processes. First, we give a definition of recursive specification and guarded recursive specification. A standard way to treat infinite processes is dealing with their finite projections. For that reason, secondly, we extend *prBPA* by the projection operator and then in the term model, in an appropriate way, we match infinite processes and their finite projections. This concept of recursive specification is taken from [2] and omitted proofs may be found there.

Definition 71. A recursive equation over *prBPA* is an equation of the form

$$X = s(X)$$

where $s(X)$ is a term over *prBPA* containing variable X, but no other variables.

A recursive specification E over *prBPA* is a set of recursion equations over *prBPA*. By this we mean that we have a set of variables V and an equation of the form

$$X = s_X(V)$$

for each $X \in V$, where $s_X(V)$ is a term over *prBPA* containing variables from the set V.

V contains one distinguished variable called the root variable.

Definition 72. A solution of a recursive equation $X = s(X)$ in some model of *prBPA* is a process p by which the equation is satisfied, that is $p = s(p)$ holds in the model.

A process p is a solution of a recursive specification E in some model of *prBPA* if after substituting p for the root variable of E, there exist other processes for the other variables of E such that all equations of E are satisfied.

If E is a recursive specification with root variable X, then $\langle X|E\rangle$ denotes a solution of this specification.

Definition 73. Let s be a term over *prBPA* containing variable X. We call an occurrence of X in s guarded if s has a sub-term of the form $a \cdot t$, where $a \in A$ and t a term containing this occurrence of X; otherwise we call the occurrence of X in s unguarded.

We call a term s completely guarded if all occurrence of all variables in s are guarded and we call a recursive specification E completely guarded if all right hand sides of all equations of E are completely guarded terms.

A term s is a guarded, if there exists completely guarded term t such that *prBPA* $\vdash s = t$.

A recursive specification E is guarded, if we can rewrite E to a completely guarded specification, by use of the axioms of *prBPA* and by repeatedly replacing variables by the right-hand side of their equations. Otherwise, E is called unguarded.

4.1 Projection

Next, we extend *prBPA* with projection operator Π_n, which helps in an approximation of infinite processes. The axioms of the projection operator are given in Table 8 with $n \in \mathbf{N}, n \geq 1$, $a \in A_\delta$ and $\rho \in \langle 0, 1 \rangle$. The new process algebra is called *prBPA* with projection, $prBPA_{pro}$.

$\Pi_n(a)$	$= a$	$PR1$
$\Pi_1(a \cdot x)$	$= a$	$PR2$
$\Pi_{n+1}(a \cdot x)$	$= a \cdot \Pi_n(x)$	$PR3$
$\Pi_n(x + y)$	$= \Pi_n(x) + \Pi_n(y)$	$PR4$
$\Pi_n(x \uplus_\rho y)$	$= \Pi_n(x) \uplus_\rho \Pi_n(y)$	$prPR$

Table 8. Axioms for projection operator

Lemma 74. *If s is a basic term and $n \in \mathbf{N}$, $n \geq 1$, then there exists a closed prBPA term t such that $prBPA_{pro} \vdash \Pi_n(s) = t$.*

Proof. The proof is given by the double induction on n and the structure of s.

For $n = 1$ we have the following:

1. if $s \equiv a \in A_\delta$ then the conclusion follows from axiom $PR1$;
2. if $s \equiv a \cdot s_1$ for $a \in A_\delta$ and some basic term s_1: then $prBPA_{pro} \vdash \Pi_1(s) = a$ and a is a closed *prBPA* term;
3. if $s \equiv s_1 \Box s_2$ some basic terms s_1 and s_2 with $\Box \in \{+, \uplus_\rho\}$: then $prBPA_{pro} \vdash \Pi_1(s) = \Pi_1(s_1) \Box \Pi_1(s_2)$ and from the induction hypothesis there are closed *prBPA* terms t_1 and t_2 such that $prBPA_{pro} \vdash \Pi_1(s_1) = t_1$ and $prBPA_{pro} \vdash \Pi_1(s_2) = t_2$. Thus, we obtain $prBPA_{pro} \vdash \Pi_1(s) = t_1 \Box t_2$ and $t_1 \Box t_2$ is a closed *prBPA* term.

For $n > 1$ we have the following:

1. if $s \equiv a \in A_\delta$ then the conclusion follows from axiom $PR1$;
2. if $s \equiv a \cdot s_1$ for $a \in A_\delta$ and some basic term s_1: then $prBPA_{pro} \vdash \Pi_n(s) = a \cdot \Pi_{n-1}(s_1)$ and by the induction hypothesis there exists a closed *prBPA* term t_1 such that $prBPA_{pro} \vdash \Pi_{n-1}(s_1) = t_1$. Thus, we obtain: $prBPA_{pro} \vdash \Pi_n(s) = a \cdot t_1$ and $a \cdot t_1$ is a closed *prBPA* term;
3. if $s \equiv s_1 \Box s_2$ for some basic terms s_1 and s_2 with $\Box \in \{+, \uplus_\rho\}$: then $prBPA_{pro} \vdash \Pi_n(s) = \Pi_n(s_1) \Box \Pi_n(s_2)$. From the induction hypothesis there are closed *prBPA* terms t_1 and t_2 such that $prBPA_{pro} \vdash \Pi_n(s_1) = t_1$ and $prBPA_{pro} \vdash \Pi_n(s_2) = t_2$. Thus, we obtain $prBPA_{pro} \vdash \Pi_n(s) = t_1 \Box t_2$ and $t_1 \Box t_2$ is a closed *prBPA* term. □

Theorem 75. *(Elimination of the projection operator) Let s be a closed term over the signature of $prBPA_{pro}$. Then there exists a closed prBPA term t such that $prBPA_{pro} \vdash s = t$.*

Proof. By the induction on the structure of s and using the Elimination theorem in *prBPA* we obtain:

1. if $s \equiv a \in A_\delta$ then the conclusion follows directly;
2. if $s \equiv s_1 \Box s_2$ for some closed $prBPA_{pro}$ terms s_1 and s_2 with $\Box \in \{\cdot, +, \uplus_\rho\}$: then by the induction hypothesis there are closed *prBPA* terms t_1 and t_2 such that $prBPA_{pro} \vdash s_1 = t_1$ and $prBPA_{pro} \vdash s_2 = t_2$. Then we obtain $prBPA_{pro} \vdash s = t_1 \Box t_2$ and $t_1 \Box t_2$ is a closed *prBPA* term.
3. if $s \equiv \Pi_n(s_1)$ for some $n \geq 1$ and closed $prBPA_{pro}$ term s_1: then by the induction hypothesis there is a closed *prBPA* term r_1 such that $prBPA_{pro} \vdash s_1 = r_1$. From the Elimination theorem in *prBPA* we have that $prBPA \vdash r_1 = t_1$ for some basic term t_1. Then, from Lemma 74, there is a closed *prBPA* term t such that $prBPA_{pro} \vdash \Pi_n(r_1) = t$. The conclusion follows since $prBPA_{pro} \vdash s = \Pi_n(s_1) = \Pi_n(r_1) = \Pi_n(t_1) = t$. □

Proposition 76. *Let s be a closed $prBPA_{pro}$ term. Then there exists $n \in \mathbf{N}$, $n \geq 1$ such that $prBPA_{pro} \vdash \Pi_k(s) = s$, for each $k \geq n$.* □

In the next subsection we will introduce infinite processes as solutions of (guarded) recursive specifications. For that reason it is necessary to establish some extra principles (rules) which relates the notion of a (guarded) recursive specification, its solution and finite projections of the solution. The main goal is to prove that each guarded recursive specification determines exactly one process, that is, it has the unique solution in the term model. Following the approach in [2] we obtain this result combining two principles given below, RDP$^-$ and AIP$^-$. We note that the definition of bounded non-determinism is not given here, it can be found in [2]. Informally, process p has bounded non-determinism if the set of all reachable processes from p in n transitions, $n \geq 1$, (including both probabilistic and action transitions, in our case) is finite. The main reason why we do not work explicitly with the bounded non-determinism is that we treat guarded recursive specifications only and, as it will be shown later, each guarded recursive specification determines a process which has bounded non-determinism. Thus, we deal with the following principles:

Definition 77. The Recursive Definition Principle (RDP) is the following assumption: every recursive specification has a solution.

Definition 78. The Approximation Induction Principle (AIP) is the following assumption: a process is determined by its finite projections, that is,

$$(\forall n \geq 1 : \Pi_n(x) = \Pi_n(y)) \Rightarrow x = y.$$

Definition 79. The Restricted Recursive Definition Principle (RDP$^-$) is the following assumption: every guarded recursive specification has a solution.

Definition 80. The Restricted Approximation Induction Principle (AIP$^-$) is the following assumption: a process is determined by its finite projections, that is,

$$(\forall n \geq 1 : \Pi_n(x) = \Pi_n(y) \ \& \ x \text{ has bounded non-determinism}) \Rightarrow x = y.$$

Definition 81. The Recursive Specification Principle (RSP) is the following assumption: every guarded recursive specification has at most one solution.

4.2 Term model with infinite processes and projection

In Section 2.2 and Section 3.2 we presented the term models of *prBPA* and *prACP*, respectively, which have the completeness property for closed term. Next, we extend the domain of these models by adding new constants which present solutions of guarded recursive specifications. We consider guarded recursive specification only because, as it will be proved later, they define a unique process. By this it has not been made a severe restriction because all real concurrent systems of interest may be described using guarded recursion only. Also, we extend the domain with finite projections and using them we approximate infinite processes. We follow the same schema as before and define a subset of the set of all processes which contains dynamic processes, that is processes which may execute action transitions only. Thus, we define the domain $\mathbf{P}$ and two auxiliary subsets in the following way:

Definition 82. The set of static processes, notation $\mathbf{P}_{\mathcal{SP}}$, is defined as:

1. $A_\delta \subseteq \mathbf{P}_{\mathcal{SP}}$;
2. If E is a guarded recursive specification and X is a variable of E, then $\langle X|E\rangle \in \mathbf{P}_{\mathcal{SP}}$;
3. If $t, s \in \mathbf{P}_{\mathcal{SP}}$ then $t \cdot s, t + s, t \mathbin{+\!\!\!+}_\rho s, \Pi_n(t) \in \mathbf{P}_{\mathcal{SP}}$ for each $\rho \in \langle 0, 1\rangle$ and $n \geq 1$.

We define the following auxiliary set $\mathbf{P_D}$:

1. $A_\delta \subseteq \mathbf{P_D}$;
2. $t \in \mathbf{P_D}, s \in \mathbf{P}_{\mathcal{SP}} \Rightarrow t \cdot s, \Pi_n(t) \in \mathbf{P_D}$ for each $n \geq 1$;
3. $t, s \in \mathbf{P_D} \Rightarrow t + s \in \mathbf{P_D}$.

Definition 83. The set of dynamic processes, notation $\mathbf{P}_{\mathcal{DP}}$, is defined in the following way:

1. $\breve{A}_\delta \subseteq \mathbf{P}_{\mathcal{DP}}$;
2. $t \in \mathbf{P}_{\mathcal{DP}}, s \in \mathbf{P}_{\mathcal{SP}} \Rightarrow t \cdot s, \Pi_n(t) \in \mathbf{P}_{\mathcal{DP}}$ for each $n \geq 1$;
3. $t, s \in \mathbf{P}_{\mathcal{DP}} \Rightarrow t + s \in \mathbf{P}_{\mathcal{DP}}$.

Definition 84. $\mathbf{P} = \mathbf{P}_{\mathcal{SP}} \cup \mathbf{P}_{\mathcal{DP}}$.

Definition 85. In a similar way as it is done in Section 2.2 we define a map $\varphi : \mathbf{P_D} \to \mathbf{P}_{\mathcal{DP}}$ as follows:

1. $\varphi(a) = \breve{a}$ for each $a \in A_\delta$; 3. $\varphi(s+t) = \varphi(s) + \varphi(t)$;
2. $\varphi(s \cdot t) = \varphi(s) \cdot t$; 4. $\varphi(\Pi_n(s)) = \Pi_n(\varphi(s))$.

Again, we denote shortly $\varphi(s) = \breve{s}$.

Definition 86. The term model with infinite processes and finite projections, denoted by $\mathbf{prP} = \mathbf{P}_{\mathcal{SP}} / \underline{\leftrightarrow}$, is defined with the operational rules in Table 4, Table 9 and Table 10 and the probability distribution function determined by Definition 87 which is an extension of Definition 12 and the bisimilation as it is defined by Definition 17. Here $\langle t_X | E \rangle$ is the right hand side of the equation for X in E, with every occurring variable Y replaced by $\langle Y | E \rangle$.

$$\frac{\langle t_X | E \rangle \rightsquigarrow u}{\langle X | E \rangle \rightsquigarrow u}$$

Table 9. Deduction rule for recursion.

$$\frac{p \rightsquigarrow x}{\Pi_n(p) \rightsquigarrow \Pi_n(x)}$$

$$\frac{x \xrightarrow{a} p}{\Pi_{n+1}(x) \xrightarrow{a} \Pi_n(p)} \qquad \frac{x \xrightarrow{a} \surd}{\Pi_n(x) \xrightarrow{a} \surd} \qquad \frac{x \xrightarrow{a} p}{\Pi_1(x) \xrightarrow{a} \surd}$$

Table 10. Deduction rules for projection

Definition 87. (Probability distribution function) The function given in Definition 12 is extended to $\mu : \mathbf{P} \times \mathbf{P} \to [0,1]$ with

$$\begin{aligned}
\mu(\langle X | E \rangle, u) &= \mu(\langle t_X | E \rangle, u) \\
\\
\mu(\Pi_1(a), \Pi_1(\breve{a})) &= 1 \\
\mu(\Pi_n(a \cdot x), \Pi_n(\breve{a} \cdot x)) &= 1 \\
\mu(\Pi_n(p + q), \Pi_n(u + v)) &= \mu(\Pi_n(p), \Pi_n(u))\mu(\Pi_n(q), \Pi_n(v)) \\
\mu(\Pi_n(p \uplus_\rho q), \Pi_n(u)) &= \rho\mu(\Pi_n(p), \Pi_n(u)) + (1-\rho)\mu(\Pi_n(q), \Pi_n(u))
\end{aligned}$$

Remark: One can see that $\mathcal{SP} \subset \mathbf{P}_{\mathcal{SP}}$, $\mathcal{DP} \subset \mathbf{P}_{\mathcal{DP}}$ and $\mathbf{D} \subset \mathbf{P}_{\mathbf{D}}$. Moreover, the form of terms belonging $\mathcal{SP}$ is the same as the form of terms in $\mathbf{P}_{\mathcal{SP}}$, and the same holds for the other sets. For these reasons, from now on, we will write $\mathcal{SP}$ instead of $\mathbf{P}_{\mathcal{SP}}$, $\mathcal{DP}$ instead of $\mathbf{P}_{\mathcal{DP}}$, $\mathcal{PR}$ instead of $\mathbf{P}$ and $\mathbf{D}$ instead of $\mathbf{P}_{\mathbf{D}}$, except in situations where the distinction between these sets is necessary. As the assumption of closed terms in proofs of properties in Section 2.2 (including the proof of the Soundness theorem as well as the Congruence theorem) has not been used at all, by this we make valid all propositions in Section 2.2 (where all properties concern closed terms only) in $\mathbf{P}$.

Theorem 88. *(Soundness theorem) Let x and y be $\mathcal{PR}$ processes. If $prBPA_{pro} \vdash x = y$ then $x \underline{\leftrightarrow} y$.*

Proof. In addition we prove the soundness of the axioms for the projection operator.

PR1: We define a relation R in the following way:

$$R = Eq\Big(\{(\Pi_1(a), a), (\Pi_1(\breve{a}), \breve{a})\}\Big).$$

From the operational rules it follows directly that $a \rightsquigarrow \breve{a}$ and $\Pi_1(a) \rightsquigarrow \Pi_1(\breve{a})$ and $(\Pi_1(\breve{a}), \breve{a}) \in R$. For action transitions $\breve{a} \xrightarrow{a} \surd$ and $\Pi_1(\breve{a}) \xrightarrow{a} \surd$.

From the definition of the probability distribution function we have: $\mu(a, \breve{a}) = 1$ and $\mu(\Pi_1(a), \Pi_1(\breve{a})) = 1$, that is $\mu(a, [\breve{a}]_R) = \mu(\Pi_1(a), [\Pi_1(\breve{a})]_R) = 1$. For any other R equivalence class M, $\mu(a, M) = \mu(\Pi_1(a), M) = 0$.

PR2: We define a relation R in the following way:

$$R = Eq\Big(\{(\Pi_1(a \cdot p), a), (\Pi_1(\breve{a} \cdot p), \breve{a}) \ : \ p \in \mathcal{SP}\}\Big).$$

For probabilistic transitions it follows from the operational rules that $\Pi_1(a \cdot p) \rightsquigarrow \Pi_1(\breve{a} \cdot p)$ and $a \rightsquigarrow \breve{a}$ and $(\Pi_1(\breve{a} \cdot p), \breve{a}) \in R$. For action transitions it follows that $\breve{a} \xrightarrow{a} \surd$ and $\Pi_1(\breve{a} \cdot p) \xrightarrow{a} \surd$.

From the definition of the probability distribution function we have: $\mu(a, \breve{a}) = 1$ and $\mu(\Pi_1(a \cdot p), \Pi_1(\breve{a} \cdot p)) = 1$, that is $\mu(a, [\breve{a}]_R) = \mu(\Pi_1(a \cdot p), [\Pi_1(\breve{a} \cdot p)]_R) = 1$. For any other R equivalence class M, $\mu(a, M) = \mu(\Pi_1(a \cdot p), M) = 0$.

PR3: We define a relation R in the following way:

$$R = Eq\Big(\{(\Pi_{n+1}(a \cdot p), a \cdot \Pi_n(p)) \ : \ p \in \mathcal{SP}\} \cup \{(\Pi_{n+1}(\breve{a} \cdot p), \breve{a} \cdot \Pi_n(p)) \ : \ p \in \mathcal{SP}\}\Big).$$

Suppose $\Pi_{n+1}(a \cdot p) \rightsquigarrow w$ for some $w \in \mathcal{DP}$. From the definition of the operational rules it follows that $w \equiv \Pi_{n+1}(u)$ for some $u \in \mathcal{DP}$ such that $a \cdot p \rightsquigarrow u$, from which $u \equiv \breve{a} \cdot p$. Then $a \cdot \Pi_n(p) \rightsquigarrow \breve{a} \cdot \Pi_n(p)$ and $(\Pi_{n+1}(\breve{a} \cdot p), \breve{a} \cdot \Pi_n(p)) \in R$.

As $a \cdot \Pi_n(p) \rightsquigarrow \breve{a} \cdot \Pi_n(p)$ it the only possible probabilistic transition of $a \cdot \Pi_n(p)$ we have that it is simulated by transition $\Pi_{n+1}(a \cdot p) \rightsquigarrow \Pi_n(\breve{a} \cdot p)$.

From the definition of the operational rules it follows that the only possible action transitions are the following: $\Pi_{n+1}(\breve{a}\cdot p) \xrightarrow{a} \Pi_n(p)$ and $\breve{a}\cdot \Pi_n(p) \xrightarrow{a} \Pi_n(p)$. Moreover, $(\Pi_n(p), \Pi_n(p)) \in R$.

Action termination is not possible for both processes (even for $n = 1$).

From the definition of the probability distribution function we have:
$\mu(\Pi_{n+1}(a\cdot p), \Pi_{n+1}(\breve{a}\cdot p)) = 1$ and $\mu(a\cdot \Pi_n(p), \breve{a}\cdot \Pi_n(p)) = 1$, that is
$\mu(\Pi_{n+1}(a\cdot p), [\Pi_{n+1}(\breve{a}\cdot p)]_R) = \mu(a\cdot \Pi_n(p), [\breve{a}\cdot \Pi_n(p)]_R) = 1$. For any other R equivalence class M, $\mu(a\cdot \Pi_n(p), M) = \mu(\Pi_{n+1}(a\cdot p), M) = 0$.

PR4: We define a relation R in the following way:

$$R = Eq\Big(\{(\Pi_n(p+q), \Pi_n(p)+\Pi_n(q)) \ : \ p,q \in \mathcal{SP}\} \cup \{(\Pi_n(u+v), \Pi_n(u)+\Pi_n(v)) \ : \ u,v \in \mathcal{DP}\}\Big).$$

Suppose $\Pi_n(p+q) \rightsquigarrow w$ for some $w \in \mathcal{DP}$. From the definition of the operational rules it follows that $w \equiv \Pi_n(u)$ for some $u \in \mathcal{DP}$ such that $p+q \rightsquigarrow u$. It follows $u \equiv u_1 + u_2$ for some $u_1, u_2 \in \mathcal{DP}$ such that $u \equiv u_1 + u_2$ and $p \rightsquigarrow u_1$ and $q \rightsquigarrow u_2$. Then $\Pi_n(p) \rightsquigarrow \Pi_n(u_1)$ and $\Pi_n(q) \rightsquigarrow \Pi_n(u_2)$ from which $\Pi_n(p) + \Pi_n(q) \rightsquigarrow \Pi_n(u_1) + \Pi_n(u_2)$. Moreover,
$(\Pi_n(u_1 + u_2), \Pi_n(u_1) + \Pi_n(u_2)) \in R$.

Suppose $\Pi_n(p) + \Pi_n(q) \rightsquigarrow z$ for some $z \in \mathcal{DP}$. From the definition of the operational rules it follows that there are $z_1, z_2 \in \mathcal{DP}$ such that $z \equiv z_1 + z_2$ and $\Pi_n(p) \rightsquigarrow z_1$ and $\Pi_n(q) \rightsquigarrow z_2$. It implies that $z_1 \equiv \Pi_n(u_1)$ and $z_2 \equiv \Pi_n(u_2)$ for some $u_1, u_2 \in \mathcal{DP}$ and also $p \rightsquigarrow u_1$ and $q \rightsquigarrow u_2$. Then, $p + q \rightsquigarrow u_1 + u_2$ and $\Pi_n(p+q) \rightsquigarrow \Pi_n(u_1 + u_2)$. Moreover,
$(\Pi_n(u_1) + \Pi_n(u_2), \Pi_n(u_1 + u_2)) \in R$.

Suppose $\Pi_n(u+v) \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. From the definition of the operational rules it follows that this transition is possible only if $n > 1$. Then $p \equiv \Pi_{n-1}(q)$ for some $q \in \mathcal{SP}$ such that $u + v \xrightarrow{a} q$. This transition implies that $u \xrightarrow{a} q$ or $v \xrightarrow{a} q$, from which $\Pi_n(u) \xrightarrow{a} \Pi_{n-1}(q)$ or $\Pi_n(v) \xrightarrow{a} \Pi_{n-1}(q)$. In both cases it is that $\Pi_n(u) + \Pi_n(v) \xrightarrow{a} \Pi_{n-1}(q)$. Moreover, $(\Pi_{n-1}(q), \Pi_{n-1}(q)) \in R$.

If $\Pi_n(u)+\Pi_n(v) \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$, then from the definition of the operational rules it follows that $\Pi_n(u) \xrightarrow{a} p$ or $\Pi_n(v) \xrightarrow{a} p$. Then following the operational rules we have that in both cases $n > 1$ and $p \equiv \Pi_{n-1}(q)$ for some $q \in \mathcal{SP}$ such that $u \xrightarrow{a} q$ in the first case and $v \xrightarrow{a} q$ in the second case. In both cases $u + v \xrightarrow{a} q$ such that $p \equiv \Pi_{n-1}(q)$, from which $\Pi_n(u+v) \xrightarrow{a} \Pi_{n-1}(q)$, and moreover $(\Pi_{n-1}(q), \Pi_{n-1}(q)) \in R$.

Suppose $\Pi_n(u+v) \xrightarrow{a} \surd$ for some $a \in A$. We investigate two possible situations:

1. if $n > 1$ then $\Pi_n(u+v) \xrightarrow{a} \surd$ iff $u+v \xrightarrow{a} \surd$ iff $u \xrightarrow{a} \surd$ or $v \xrightarrow{a} \surd$ iff $\Pi_n(u) \xrightarrow{a} \surd$ or $\Pi_n(v) \xrightarrow{a} \surd$ iff $\Pi_n(u) + \Pi_n(v) \xrightarrow{a} \surd$.
2. if $n = 1$ then from $\Pi_1(u+v) \xrightarrow{a} \surd$ one of the following follows
   2.1 $u + v \xrightarrow{a} \surd$ from which $u \xrightarrow{a} \surd$ or $v \xrightarrow{a} \surd$, and also $\Pi_1(u) \xrightarrow{a} \surd$ or $\Pi_n(v) \xrightarrow{a} \surd$. In both cases $\Pi_n(u) + \Pi_n(v) \xrightarrow{a} \surd$; or
   2.2 $u + v \xrightarrow{a} r$ for some $r \in \mathcal{SP}$, from which $u \xrightarrow{a} r$ or $v \xrightarrow{a} r$, and also $\Pi_1(u) \xrightarrow{a} \surd$ or $\Pi_n(v) \xrightarrow{a} \surd$. In both cases $\Pi_n(u) + \Pi_n(v) \xrightarrow{a} \surd$.

If $\Pi_1(u) + \Pi_1(v) \xrightarrow{a} \surd$ in a similar way we can obtain that either $u + v \xrightarrow{a} \surd$ or $u + v \xrightarrow{a} r$ for some $r \in \mathcal{SP}$ and in both cases $\Pi_1(u+v) \xrightarrow{a} \surd$.

Using the definition of the probability distribution function we obtain:
$\mu(\Pi_n(p+q), \Pi_n(u+v)) = \mu(\Pi_n(p), \Pi_n(u))\mu(\Pi_n(q), \Pi_n(v))$ and
$\mu(\Pi_n(p) + \Pi_n(q), \Pi_n(u) + \Pi_n(v)) = \mu(\Pi_n(p), \Pi_n(u))\mu(\Pi_n(q), \Pi_n(v))$. The result follows from Proposition 31.

prPR: We define a relation R in the following way:

$$R = Eq\Big(\{(\Pi_n(p \sqcup\!\!\!\!+_{\rho} q), \Pi_n(p) \sqcup\!\!\!\!+_{\rho} \Pi_n(q)) \ : \ p, q \in \mathcal{SP}\}\Big).$$

Suppose $\Pi_n(p \sqcup\!\!\!\!+_{\rho} q) \rightsquigarrow w$ for some $w \in \mathcal{DP}$. From the definition of the operational rules it follows that $w \equiv \Pi_n(u)$ for some $u \in \mathcal{DP}$ *such that* $p \sqcup\!\!\!\!+_{\rho} q \rightsquigarrow u$, *from which* $p \rightsquigarrow u$ *or* $q \rightsquigarrow u$. Then $\Pi_n(p) \rightsquigarrow \Pi_n(u)$ or $\Pi_n(q) \rightsquigarrow \Pi_n(u)$, and in both cases $\Pi_n(p) \sqcup\!\!\!\!+_{\rho} \Pi_n(q) \rightsquigarrow \Pi_n(u)$. Moreover, $(\Pi_n(u), \Pi_n(u)) \in R$.

Suppose $\Pi_n(p) \sqcup\!\!\!\!+_{\rho} \Pi_n(q) \rightsquigarrow z$ for some $z \in \mathcal{DP}$. From the definition of the operational rules it follows that $\Pi_n(p) \rightsquigarrow z$ or $\Pi_n(q) \rightsquigarrow z$. Then for some $z_1 \in \mathcal{DP}$ such that $z \equiv \Pi_n(z_1)$ either $p \rightsquigarrow z_1$ or $q \rightsquigarrow z_1$. In both cases we obtain $\Pi_n(p \sqcup\!\!\!\!+_{\rho} q) \rightsquigarrow z$.

Using the definition of the probability distribution function we obtain:
$\mu(\Pi_n(p \sqcup\!\!\!\!+_{\rho} q), \Pi_n(u)) = \rho\mu(\Pi_n(p), \Pi_n(u)) + (1-\rho)\mu(\Pi_n(q), \Pi_n(u))$ and
$\mu(\Pi_n(p) \sqcup\!\!\!\!+_{\rho} \Pi_n(q), \Pi_n(u)) = \rho\mu(\Pi_n(p), \Pi_n(u)) + (1-\rho)\mu(\Pi_n(q), \Pi_n(u))$. The result follows from Proposition 31. □

The following two propositions can be proved easily and they show that each process in our model has bounded non-determinism, with the meaning described before. This provides us with the result that in $\mathcal{PR}$ there is no difference between AIP and AIP$^-$ principles.

Proposition 89. *If* $p \in \mathcal{PR}$ *then the set* $\{u \ : \ p \rightsquigarrow u\}$ *is finite.* □

Proposition 90. *If* $u \in \mathcal{PR}$ *then the set* $\{p \ : \ u \xrightarrow{a} p, a \in A\}$ *is finite.* □

Next, we give the notion of head normal form and using the Soundness theorem we prove that each definable process has a head normal form. Having this property we may deal easily and get useful properties for infinite processes (for example, Proposition 93 which is used in the proof of the Congruence theorem).

Definition 91. We say a process p has a head normal form if there is an $n \in \mathbf{N}$, processes p_i and probabilities ρ_i, $1 \leq i \leq n$ such that

$$p = p_1 \sqcup\!\!\!\!+_{\rho_1} p_2 \ldots p_{n-1} \sqcup\!\!\!\!+_{\rho_{n-1}} p_n$$

and for each i,

$$p_i = \sum_{j < s_i} a_{ij} \cdot p_{ij} + \sum_{k < t_i} b_{ik}$$

for certain $s_i, t_i \in \mathbf{N}$ with $s_i + t_i > 0$, atomic actions a_{ij}, b_{ik} and processes p_{ij}.

A process p is definable if p can be obtained from the atomic actions from A and δ by means of the operators of *prBPA* and guarded recursion.

Lemma 92. *Each definable process has a head normal form.*

Proof. The proof is quite similar to the proof in [2]. The only difference in proof is for probabilistic choice for which the conclusion follows directly from the definition of head normal form, and for non-deterministic choice where distribution laws should be applied. □

Remark. It is easy to see that each **D** process p has a head normal form as following:

$$p = \sum_{j<s_i} a_{ij} \cdot p_{ij} + \sum_{k<t_i} b_{ik}$$

for certain $s_i, t_i \in \mathbf{N}$ with $s_i + t_i > 0$, atomic actions a_{ij}, b_{ij} and processes p_{ij}. And each dynamic process $u \in \mathcal{DP}$ has a form:

$$u = \sum_{j<s_i} \breve{a}_{ij} \cdot p_{ij} + \sum_{k<t_i} \breve{b}_{ik}$$

for certain $s_i, t_i \in \mathbf{N}$ with $s_i + t_i > 0$, atomic actions a_{ij}, b_{ij} and processes p_{ij}.

We will refer to this special head normal form as dynamic head normal form, for both.

Proposition 93. *If $p \in \mathcal{SP}$ and $u \in \mathcal{DP}$ then $\mu(p, u) = \mu(\Pi_n(p), \Pi_n(u))$ for $n \in \mathbf{N}$, $n \geq 1$.*

Proof. It follows directly from a head normal form of p, the operational rules and the definition of the probability distribution function for projection. □

Corollary 94. *For arbitrary set $M \subseteq \mathcal{PR}$ and $n \geq 1$, $\mu(p, M) = \mu(\Pi_n(p), \Pi_n(M))$.*

Next we prove the congruence property of $\leftrightarrows$ with respect to the projection operator. Later on, using the results that have been obtained we prove that AIP holds in the term model and combining this result with Lemma 101 and Lemma 96 we obtain the uniqueness of solution of a guarded recursive specification in **prP**.

In advance we will give a few remarks to make the proof more understandable. The first part, about transitions, both probabilistic and action, is given in the standard way. The last part, considering μ function and equivalence classes of the relation R which has to be proven to be a bisimulation relation, depends of the definition of relation R. We choose relation R in such a way that for each equivalence class $[x]_{R_1}$, $\Pi_n([x]_{R_1})$ is an R-equivalence class for a given bisimilation relation R_1 (see the next example and the proof of the Congruence theorem). We give an example which describes informally the results used in this part of the proof.

Example 5. Let us consider the following two processes: $p = a \boxplus_{\frac{1}{3}} a \cdot p$ and $q = a \boxplus_{\frac{1}{6}} (a + a) \boxplus_{\frac{1}{6}} a \cdot (a \boxplus_{\frac{1}{3}} a \cdot q)$. We have $p \underline{\leftrightarrow} q$ because the following relation is a bisimulation:

$$R_1 = Eq\Big(\{(a, a), (a, a + a), (a \cdot p, a \cdot (a \boxplus_{\frac{1}{3}} a \cdot q)), (a \boxplus_{\frac{1}{3}} a \cdot p, a \boxplus_{\frac{1}{6}} (a + a) \boxplus_{\frac{1}{6}} a \cdot (a \boxplus_{\frac{1}{3}} a \cdot q)),$$
$$(\breve{a}, \breve{a}), (\breve{a}, \breve{a} + \breve{a}), (\breve{a} \cdot p, \breve{a} \cdot (a \boxplus_{\frac{1}{3}} a \cdot q))\}\Big).$$

We construct relation R, as it is given later in the proof, and obtain:

$$R = Eq\Big(\{(\Pi_n(a), \Pi_n(a)), (\Pi_n(a), \Pi_n(a + a)), (\Pi_n(a \cdot p), \Pi_n(a \cdot (a \boxplus_{\frac{1}{3}} a \cdot q))),$$
$$(\Pi_n(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_n(a \boxplus_{\frac{1}{6}} (a + a) \boxplus_{\frac{1}{6}} a \cdot (a \boxplus_{\frac{1}{3}} a \cdot q))), (\Pi_n(\breve{a}), \Pi_n(\breve{a})), (\Pi_n(\breve{a}), \Pi_n(\breve{a} + \breve{a})),$$
$$(\Pi_n(\breve{a} \cdot p), \Pi_n(\breve{a} \cdot (a \boxplus_{\frac{1}{3}} a \cdot q))) \ : \ n \in \mathbf{N}, n \geq 1\}\Big).$$

We obtain easily that: $[\breve{a}]_R = \{\breve{a}\}$, $[\breve{a}]_{R_1} = \{\breve{a}, \breve{a} + \breve{a}\}$, $[\Pi_1(\breve{a})]_R = \{\Pi_1(\breve{a}), \Pi_1(\breve{a} + \breve{a})\} = \Pi_1([\breve{a}]_{R_1})$ and $[\breve{a} \cdot p]_{R_1} = \{\breve{a} \cdot p, \breve{a}(a \boxplus_{\frac{1}{3}} a \cdot q\})$,
And

$$\mu(p, [\breve{a}]_{R_1}) = \mu(p, \breve{a}) + \mu(p, \breve{a} + \breve{a}) = \mu(a \boxplus_{\frac{1}{3}} a \cdot p, \breve{a}) + \mu(a \boxplus_{\frac{1}{3}} a \cdot p, \breve{a} + \breve{a}) = \tfrac{1}{3},$$
$$\mu(\Pi_1(p), [\Pi_1(\breve{a})]_R) = \mu(\Pi_1(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_1(\breve{a})) + \mu(\Pi_1(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_1(\breve{a} + \breve{a})) = \tfrac{1}{3}.$$

In a similar way using the definition of the probability distribution function about recursion we obtain:

$$\mu(p, [\breve{a} \cdot p]_{R_1}) = \mu(p, \breve{a} \cdot p) + \mu(p, \breve{a}(a \boxplus_{\frac{1}{3}} a \cdot q)) = \mu(a \boxplus_{\frac{1}{3}} a \cdot p, \breve{a} \cdot p) + \mu(a \boxplus_{\frac{1}{3}} a \cdot p, \breve{a}(a \boxplus_{\frac{1}{3}} a \cdot q)) = \tfrac{2}{3}$$

and

$$\mu(\Pi_1(p), [\Pi_1(\breve{a} \cdot p)]_R) = \mu(\Pi_1(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_1(\breve{a} \cdot p)) + \mu(\Pi_1(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_1(\breve{a}(a \boxplus_{\frac{1}{3}} a \cdot q))) = \tfrac{2}{3}.$$

Thus for each equivalence class $M = [u]_{R_1}$ it can be proven that $\mu(p, [u]_{R_1}) = \mu(\Pi_1(p), [\Pi_1(u)]_R)$ and $\mu(q, [u]_{R_1}) = \mu(\Pi_1(q), [\Pi_1(u)]_R)$ and having $\mu(p, [u]_{R_1}) = \mu(q, [u]_{R_1})$ the result follows.

That this is not the case in general we consider relation $\underline{\leftrightarrow}$ instead of R. Thus, having that $\Pi_1(\breve{a}) \underline{\leftrightarrow} \Pi_1(\breve{a} \cdot p)$ and $\breve{a} \not\underline{\leftrightarrow} \breve{a} \cdot p$ we obtain $\mu(p, [\breve{a}]_{\underline{\leftrightarrow}}) = \mu(p, \breve{a}) = \mu(a \boxplus_{\frac{1}{3}} a \cdot p, \breve{a}) = \frac{1}{3}$, but $\mu(\Pi_1(p), [\Pi_1(\breve{a})]_{\underline{\leftrightarrow}}) = \mu(\Pi_1(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_1(\breve{a})) + \mu(\Pi_1(a \boxplus_{\frac{1}{3}} a \cdot p), \Pi_1(\breve{a} \cdot p)) = \frac{1}{3} + \frac{2}{3} = 1.$ □

Theorem 95. *(Congruence theorem) $\underline{\leftrightarrow}$ is a congruence relation on* **prP**, *that is $\underline{\leftrightarrow}$ is a congruence relation with respect to $+$, $\cdot$, $\boxplus_\rho$ and Π_n, for $\rho \in \langle 0, 1 \rangle$ and $n \in \mathbf{N}, n \geq 1$.*

Proof. Once more we emphasise that the proof of Theorem 30 (the Congruence theorem of *prBPA*) has been adapted for definable processes as described in Remark on p. 68. We just need to prove that $\underline{\leftrightarrow}$ is a congruence relation with respect to Π_n operator.

Let us suppose that $x \underline{\leftrightarrow} y$ which implies that there exists a bisimulation relation R_1 such that $x R_1 y$. We need to construct a relation R such that $\Pi_n(x) R \Pi_n(y)$ which is a bisimulation.

We consider a relation

$$\begin{aligned} R = \ & \{(\Pi_n(p), \Pi_n(q)) \ : \ p, q \in \mathcal{SP} \ \& \ (p, q) \in R_1, \ n \in \mathbf{N}, n \geq 1\} \\ \cup \ & \{(\Pi_n(u), \Pi_n(v)) \ : \ u, v \in \mathcal{DP} \ \& \ (u, v) \in R_1, \ n \in \mathbf{N}, n \geq 1\}. \end{aligned}$$

We note that R_1 is an equivalence relation implies R is an equivalence relation too.

Suppose $\Pi_n(p) R \Pi_n(q)$ for some $p, q \in \mathcal{SP}$ such that $p R_1 q$ and $\Pi_n(p) \rightsquigarrow u$ for some $u \in \mathcal{DP}$. Then from the definition of the operational rules it follows that $u \equiv \Pi_n(u')$ for some $u' \in \mathcal{DP}$

such that $p \rightsquigarrow u'$. Then $q \rightsquigarrow v'$ for some $v' \in \mathcal{DP}$ and $u'R_1v'$, from which $\Pi_n(q) \rightsquigarrow \Pi_n(v')$. Moreover because $u'R_1v'$ it follows $\Pi_n(u')R\Pi_n(v')$.

Suppose $\Pi_n(u)R\Pi_n(v)$ for some $n > 1$ and $u, v \in \mathcal{DP}$ such that uR_1v and $\Pi_n(u) \xrightarrow{a} p$ for some $a \in A$ and $p \in \mathcal{SP}$. From the definition of the operational rules it follows $p \equiv \Pi_{n-1}(p')$ for some $p' \in \mathcal{SP}$ such that $u \xrightarrow{a} p'$. Then $v \xrightarrow{a} q'$ for some $q' \in \mathcal{SP}$ such that $p'R_1q'$ from which $\Pi_n(v) \xrightarrow{a} \Pi_{n-1}(q')$ and $\Pi_{n-1}(p')R\Pi_{n-1}(q')$.

Suppose that $\Pi_n(u) \xrightarrow{a} \surd$ for some $a \in A$ and uR_1v. Dependent on n there are two possibilities:

1. For any n using the operational rules from $\Pi_n(u) \xrightarrow{a} \surd$ we obtain that $u \xrightarrow{a} \surd$ from which it follows that $v \xrightarrow{a} \surd$ and also $\Pi_n(v) \xrightarrow{a} \surd$.
2. If $n = 1$ then from $\Pi_1(u) \xrightarrow{a} \surd$ we obtain that $u \xrightarrow{a} p$ for some $p \in \mathcal{SP}$. Then as uR_1v it follows that for some $q \in \mathcal{SP}$, $v \xrightarrow{a} q$ and pR_1q from which using the operational rules we get $\Pi_1(v) \xrightarrow{a} \surd$.

Now let us assume that $(\Pi_n(p), \Pi_n(q)) \in R$ and $M \in \mathcal{DP}/R$. From the previous proof for probabilistic transitions we have that M is a reachable from $\Pi_n(p)$ iff there is a process $\Pi_n(u) \in M$ such that $\Pi_n(p) \rightsquigarrow \Pi_n(u)$. Thus, $M = [\Pi_n(u)]_R$. Moreover, there is a process $\Pi_n(v) \in M$ such that $\Pi_n(q) \rightsquigarrow \Pi_n(v)$. Also, from the definition of R we obtain that $v \in [u]_{R_1}$ iff $\Pi_n(v) \in [\Pi_n(u)]_R$, which means that there is a bijection between $[u]_{R_1}$ and $[\Pi_n(u)]_R$. Combining this result and Proposition 93 we obtain that $\mu(p, [u]_{R_1}) = \mu(\Pi_n(p), [\Pi_n(u)]_R)$ and also $\mu(q, [v]_{R_1}) = \mu(\Pi_n(q), [\Pi_n(v)]_R)$. And since $[u]_{R_1} = [v]_{R_1}$ and $[\Pi_n(u)]_R = [\Pi_n(v)]_R$ and $\mu(p, [u]_{R_1}) = \mu(q, [v]_{R_1})$ the conclusion follows. □

Let us summarize the items which have been introduced up to now. We introduced infinite processes as solutions of guarded recursive specifications. Then we gave the notion of a definable process and showed that these processes have a head normal form (Lemma 92). One can note that only definable processes have been added to the domain of the new term model. Using this property in addition we can work with the head normal form of processes, which is very suitable. Also, we explained that in this model there is no difference between AIP and AIP$^-$ because each process has bounded non-determinism. In the rest of the section we show that each guarded recursive specification has a unique solution in **prP**.

Lemma 96. *RDP$^-$ holds in* **prP**. □

Proposition 97. *Let $p \in \mathbf{P}_{\mathcal{SP}}$. All finite projections of p are bisimilar with processes from $\mathcal{SP}$.* □

Proposition 98. *Let $u \in \mathbf{P}_{\mathcal{DP}}$. All finite projections of u are bisimilar with processes from $\mathcal{DP}$.* □

Proposition 99. *Let p and q be processes such that for some $n \in \mathbf{N}$, $n \geq 1$, $\Pi_n(p) \leftrightarrow \Pi_n(q)$. Then for each $k \leq n$, $\Pi_k(p) \leftrightarrow \Pi_k(q)$.* □

Theorem 100. *(Projection theorem) Let E be a guarded recursive specification with solutions p and q. Then for all $n \geq 1$ we have $\Pi_n(p) \leftrightarrow \Pi_n(q)$.* □

Lemma 101. *AIP^- implies RSP.* □

Example 6. Before giving the next theorem we give the following example to describe the idea of the proof. Let us consider the following processes: $p = a \text{ⵣ}_{\frac{1}{2}} a \cdot p \text{ⵣ}_{\frac{1}{3}} a \cdot a \cdot p$. It is easy to check that for each $n \geq 3$ it holds:
$\mu(p, [\breve{a}]_{\leftrightarrow}) = \mu(\Pi_n(p), [\Pi_n(\breve{a})]_{\leftrightarrow}) = \frac{1}{2}$,
$\mu(p, [\breve{a} \cdot p]_{\leftrightarrow}) = \mu(\Pi_n(p), [\Pi_n(\breve{a} \cdot p)]_{\leftrightarrow}) = \frac{1}{3}$ and
$\mu(p, [\breve{a} \cdot a \cdot p]_{\leftrightarrow}) = \mu(\Pi_n(p), [\Pi_n(\breve{a} \cdot a \cdot p)]_{\leftrightarrow}) = \frac{1}{6}$, that is for each $M \in \mathcal{DP}/\leftrightarrow$

$$\mu(p, M) = \mu(\Pi_n(p), \Pi_n(M)).$$

And this result does not hold if $n = 1$ or $n = 2$.

Theorem 102. *(AIP in* **prP***) If for all $n \geq 1$, $\Pi_n(p) \leftrightarrow \Pi_n(q)$ then $p \leftrightarrow q$.*

Proof. Let us consider the following relation on $\mathcal{PR}$:

$$R = Eq\Big(\{(p,q) \;:\; p,q \in \mathcal{SP} \;\&\; \forall n \geq 1 : \Pi_n(p) \leftrightarrow \Pi_n(q)\} \\ \cup \{(u,v) \;:\; u,v \in \mathcal{DP} \;\&\; \forall n \geq 1 : \Pi_n(u) \leftrightarrow \Pi_n(v)\}\Big).$$

Let $(p,q) \in R$ for some $p, q \in \mathcal{SP}$. We have that p and q have a head normal form and let for some $n \in \mathbf{N}$, processes p_i and probabilities ρ_i, $1 \leq i \leq n$,

$$p = p_1 \text{ⵣ}_{\rho_1} p_2 \cdots p_{n-1} \text{ⵣ}_{\rho_{n-1}} p_n \tag{8}$$

where for each i,

$$p_i = \sum_{j<g_i} a_{ij} \cdot p_{ij} + \sum_{k<h_i} b_{ik}$$

for certain $g_i, h_i \in \mathbf{N}$ with $g_i + h_i > 0$, atomic actions a_{ij}, b_{ij} and processes p_{ij} and for some $s \in \mathbf{N}$, processes q_i and probabilities σ_i, $1 \leq i \leq s$,

$$q = q_1 \text{ⵣ}_{\sigma_1} q_2 \cdots q_{s-1} \text{ⵣ}_{\sigma_{s-1}} q_s \tag{9}$$

where for each i,

$$q_i = \sum_{j<e_i} c_{ij} \cdot q_{ij} + \sum_{k<f_i} d_{ik}$$

for certain $e_i, f_i \in \mathbf{N}$ with $e_i + f_i > 0$, atomic actions c_{ij}, d_{ij} and processes q_{ij}. And let us assume

$$\forall m \geq 1 : \Pi_m(p) \leftrightarrow \Pi_m(q).$$

Let us suppose that $p \rightsquigarrow u$ for some process u. From the definition of the operational rules and from (8) it follows that $u \equiv \breve{p}_i$ for some $i, 1 \leq i \leq n$. Now define, for $m \geq 1$

$$S^i_m = \{v \ : \ q \rightsquigarrow v \ \& \ \Pi_m(\breve{p}_i) \underline{\leftrightarrow} \Pi_m(v)\}.$$

We can make the following observation:

1. Because $\Pi_m(p) \underline{\leftrightarrow} \Pi_m(q)$ and $\Pi_m(p) \rightsquigarrow \Pi_m(\breve{p}_i)$ it follows that there exists a $\Pi_m(v)$ such that $\Pi_m(q) \rightsquigarrow \Pi_m(v)$ and $\Pi_m(v) \underline{\leftrightarrow} \Pi_m(\breve{p}_i)$. But from (9) we have that $\Pi_m(v) \equiv \Pi_m(\breve{q}_t)$ for certain $t, 1 \leq t \leq s$. Moreover, from (9) we also get that $q \rightsquigarrow \breve{q}_t$ and combining these results we obtain that $\breve{q}_t \in S^i_m$. By this we proved that $S^i_m \neq \emptyset$ for each $m \geq 1$.
2. For each $m \geq 1$, $S^i_m \subseteq \{q_1, \ldots, q_s\}$ from which it follows that S^i_m are finite sets.
3. $S^i_1 \supseteq S^i_2 \supseteq \ldots$, since $\Pi_{m+1}(\breve{p}_i) \underline{\leftrightarrow} \Pi_{m+1}(\breve{q}_t)$ implies $\Pi_m(\breve{p}_i) \underline{\leftrightarrow} \Pi_m(\breve{q}_t)$.

From here we obtain that there exists an $\overline{m} \in \mathbf{N}$ with

$$S^i_{\overline{m}} = \bigcap_{m \geq 1} S^i_m \neq \emptyset$$

which leads to the conclusion that there is a $v \in \bigcap\limits_{m \geq 1} S^i_m$ such that $q \rightsquigarrow v$ and $\Pi_m(v) \underline{\leftrightarrow} \Pi_m(u)$ for each $m \geq 1$, that is $q \rightsquigarrow v$ and $(u, v) \in R$.

Let $(u, v) \in R$ for some $u, v \in \mathcal{DP}$. Then u and v have a dynamic head normal form, that is

$$u = \sum_{j<g} \breve{a}_j \cdot s_j + \sum_{k<h} \breve{b}_k$$

for certain $g, h \in \mathbf{N}$ with $g + h > 0$, atomic actions a_j, b_j and processes s_j and

$$v = \sum_{j<e} \breve{c}_j \cdot r_j + \sum_{k<f} \breve{d}_k$$

for certain $e, f \in \mathbf{N}$ with $e + f > 0$, atomic actions c_j, d_j and processes r_j. And let us assume

$$\forall m \geq 1 : \Pi_m(u) \underline{\leftrightarrow} \Pi_m(v).$$

Let us suppose that $u \xrightarrow{a} p$ for some process p and atomic action a. From the definition of the operational rules and the form of u it follows that $a \equiv a_j$ and $p \equiv s_j$ for some $j, 1 \leq j \leq g$. In a similar way as before for each $m \geq 1$ we define a set:

$$S^i_m = \{q \ : \ v \xrightarrow{a} q \ \& \ \Pi_m(\breve{a}s_j) \underline{\leftrightarrow} \Pi_m(q)\}.$$

Again we obtain that:

1. $S^j_m \neq \emptyset$ for each $m \geq 1$ since $\Pi_m(u) \underline{\leftrightarrow} \Pi_m(v)$ and $\Pi_m(u) \xrightarrow{a} \Pi_{m-1}(s_j)$ and since $\Pi_m(v) \xrightarrow{a} \Pi_{m-1}(r_k)$ and $\Pi_{m-1}(r_k) \underline{\leftrightarrow} \Pi_{m-1}(s_j)$ and $v \xrightarrow{a} r_k$ for some $k < e$ (according to the form of v).
2. For each $m \geq 1$, $S^j_m \subseteq \{r_1, \ldots, r_e\}$ from which it follows that S^j_m are finite sets.

3. $S_1^j \supseteq S_2^j \supseteq \ldots$, since $\Pi_{m+1}(p) \underline{\leftrightarrow} \Pi_{m+1}(q)$ implies $\Pi_m(p) \underline{\leftrightarrow} \Pi_m(q)$.

Then we can conclude that $\bigcap\limits_{j\geq 1} S_m^j$ is a non-empty set and choose q in this intersection we obtain that $v \xrightarrow{a} q$ and $\Pi_m(p) \underline{\leftrightarrow} \Pi_m(q)$ for each $m \geq 1$, that is $(p,q) \in R$.

At last we need to prove that for an arbitrary equivalence class $M \in \mathcal{PR}/R$ and a pair $(p,q) \in R$, where $p,q \in \mathcal{SP}$, it holds $\mu(p,M) = \mu(q,M)$. Again we consider only reachable classes, that is we assume that there are elements $u,v \in M$ such that $p \rightsquigarrow u$ and $q \rightsquigarrow v$. (The previous discussion about probabilistic transitions provides that u exists if and only if v exists.) Thus, for u and v we have that $\Pi_m(u) \underline{\leftrightarrow} \Pi_m(v)$ and also $[\Pi_m(u)]_{\underline{\leftrightarrow}} = [\Pi_m(v)]_{\underline{\leftrightarrow}}$ for each $m \geq 1$.

Up to now we have
$\mu(p,[u]_R) = \mu(\Pi_m(p), \Pi_m([u]_R))$,
$\mu(q,[u]_R) = \mu(\Pi_m(q), \Pi_m([u]_R))$ and
$\mu(\Pi_m(p), \Pi_m([u]_{\underline{\leftrightarrow}})) = \mu(\Pi_m(q), \Pi_m([u]_{\underline{\leftrightarrow}}))$, for each $m \geq 1$.

Claim There is an $\overline{m} \in \mathbf{N}, \overline{m} \geq 1$ such that

$$\mu(\Pi_{\overline{m}}(p), \Pi_{\overline{m}}([u]_R)) = \mu(\Pi_{\overline{m}}(p), [\Pi_{\overline{m}}(u)]_{\underline{\leftrightarrow}}).$$

Then it follows easily that $\mu(p,M) = \mu(q,M)$. This finishes the proof of the theorem. Next we give the proof of the claim.

Proof of the Claim: It is easy to prove that $\Pi_m([u]_R) \subseteq [\Pi_m(u)]_{\underline{\leftrightarrow}}$ for each $m \geq 1$ which implies

$$\mu(\Pi_m(p), \Pi_m([u]_R)) \leq \mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}}).$$

Let us suppose that $\mu(\Pi_m(p), \Pi_m([u]_R)) < \mu(\Pi_m(p), [\Pi_m(u)]_{\underline{\leftrightarrow}})$ from which it follows: $D_m = [\Pi_m(u)]_{\underline{\leftrightarrow}} \setminus \Pi_m([u]_R) \neq \emptyset$. Then we obtain that there is $w \in D_m$, $z \in \mathcal{DP}$ and a natural number n_z such that $\Pi_m(p) \rightsquigarrow w$ and

1. $w \equiv \Pi_m(z)$ & $p \rightsquigarrow z$
2. $\Pi_m(z) \underline{\leftrightarrow} \Pi_m(u)$
3. $z \notin [u]_R$
4. $\Pi_{n_z}(z) \not\underline{\leftrightarrow} \Pi_{n_z}(u)$ (from 3.)
5. $\forall k \leq m : \Pi_k(z) \underline{\leftrightarrow} \Pi_k(u)$ (from 2. and Proposition 99)
6. $n_z > m$ & $\Pi_{n_z}(z) \notin [\Pi_{n_z}(u)]_{\underline{\leftrightarrow}}$ (from 4. and 5.)
7. $\Pi_{n_z}(z) \notin D_{n_z}$ (from 6.)

Moreover from Proposition 99 and since $\forall v : \Pi_{m+1}(v) \notin \Pi_{m+1}([u]_R) \Rightarrow \Pi_m(v) \notin \Pi_m([u]_R)$ (which follows directly from the definition of $\Pi_m([u]_R)$) we have that for each $m \geq 1$,

$$D_m \supseteq D_{m+1}. \qquad (8)$$

Thus having that the set of reachable processes from p which are in D_1, say $Z = \{z_i : p \rightsquigarrow z_i\}$, is a finite set from the previous discussion we obtain that for each $z_i \in Z$ there is a natural number n_{z_i} such that $\Pi_{n_{z_i}}(z_i) \not\underline{\leftrightarrow} \Pi_{n_{z_i}}(u)$. Let denote by $\overline{n}_{z_i}$ the least of all such numbers that exist for z_i. From the conclusion 7. we have that $\Pi_{\overline{n}_{z_i}}(z_i) \notin D_{\overline{n}_{z_i}}$ and moreover since (8) if $\overline{n}_{z_i} \leq \overline{n}_{z_j}$ then $\Pi_{\overline{n}_{z_i}}(z_i) \notin D_{\overline{n}_{z_j}}$. Now as we have that $D_1 \supseteq D_{n_{z_1}} \supseteq D_{n_{z_2}} \ldots$ is a decreasing sequence of finite sets and by taking

$$\overline{m} = max\{\overline{n}_{z_i} : \Pi_1(z_i) \in D_1 \ \& \ p \rightsquigarrow z_i\}$$

we obtain that $\forall z_i \in Z : \Pi_1(z_i) \in D_1 \ \& \ p \rightsquigarrow z_i \ \Rightarrow \ \Pi_{\overline{m}}(z_i) \notin D_{\overline{m}}$. It means that
if $\Pi_{\overline{m}}(p) \rightsquigarrow \Pi_{\overline{m}}(z)$ then $(\Pi_{\overline{m}}(z) \in [\Pi_{\overline{m}}(u)]_{\underline{\leftrightarrow}}$ iff $\Pi_{\overline{m}}(z) \in \Pi_{\overline{m}}([u]_R))$. □

An extension of *prACP* with infinite processes can be made in a similar way following the approach in [2] (Section 4.5). As non new important result is obtained in this investigation, we omit this part.

5 Alternating Bit Protocol

As an example of the application of *prACP* we consider the Alternating Bit Protocol with unreliable communication channels as it is described in [2]. We give a specification in *prACP* of the constituent processes of the protocol and of the whole system. In the theory we derive the recursive specification of the behaviour of the protocol which can be viewed (in the term model) as a Markov chain. Using standard Markov chain analysis we prove some properties and do some performance analysis of the system.

The protocol is modeled as four processes, (see Figure 4), one sender process S, one receiver R and two communication channels K and L. The sender sends a message to the receiver via the unreliable communication channel K. After having received a message the receiver sends an acknowledgment to the sender via channel L. A channel may transmit a message correctly or it may corrupt it. In order to avoid a possibility of lost a message in a channel, each message has attached a control bit b which is changed alternatingly. When S read a datum d at port 1 it passes on a sequence $d0, d0, d0 \ldots$ of copies of this datum, with a bit 0 appended, to K until an acknowledgement 0 is received at port 6. Then, the next datum is read and sent on with a bit 1 appended and so on. If a channel corrupts a message it passes on $\perp$. Unreliability of each channel is specified by the probabilistic choice operator $\sqcup\!\!\!\!+_\pi$, correct transmission of a message with probability π and corruption of a message with probability $1 - \pi$.

Let D be a finite set of data and let A be a set of standard read, send and communication actions. We use the standard read/send communication function given by $r_k(x) \mid s_k(x) = c_k(x)$ for communication port k and message x. The four processes are given by the recursive specifications in Figure 5.

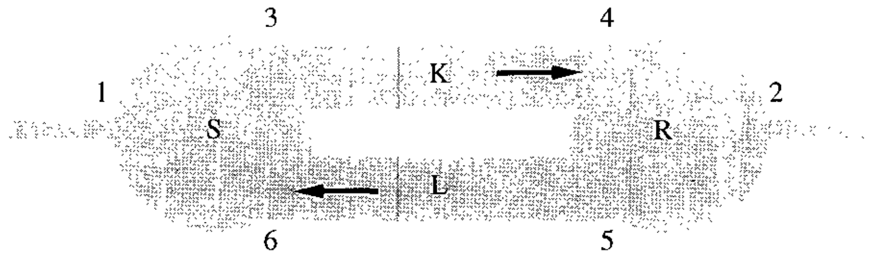


Fig. 4. Components of the protocol

Sender :

$$\begin{aligned} S\; &= S_0 \cdot S_1 \cdot S \\ S_b\; &= \sum_{d \in D} r_1(d) \cdot S_{b_d} && (b = 0, 1) \\ S_{b_d} &= s_2(db) \cdot ((r_6(1-b) + r_6(\perp)) \cdot S_{b_d} + r_6(b)) && (b = 0, 1, d \in D) \end{aligned}$$

Receiver :

$$\begin{aligned} R\; &= R_1 \cdot R_0 \cdot R \\ R_b &= (\sum_{d \in D} r_3(db) + r_3(\perp)) \cdot s_5(b) \cdot R_b + \sum_{d \in D} r_3(d(1-b)) \cdot s_4(d) \cdot s_5(1-b) && (b = 0, 1) \end{aligned}$$

Channels :

$$\begin{aligned} K &= \sum_{d \in D, b \in \{0,1\}} r_2(db) \cdot (s_3(db) \sqcup\!\!\sqcup_{\pi} s_3(\perp)) \cdot K \\ L\; &= \sum_{b \in \{0,1\}} r_5(b) \cdot (s_6(b) \sqcup\!\!\sqcup_{\rho} s_6(\perp)) \cdot L \end{aligned}$$

Fig. 5. Specification of the four components of the protocol.

The behaviour of the protocol is obtained by parallel composition of these four processes:

$$ABP = t_I \circ \partial_H(S \,\|\, K \,\|\, L \,\|\, R), \tag{10}$$

where $H = \{r_k(db), s_k(db) : k \in \{2,3,5,6\}, d \in D, b \in \{0,1\}\}$ is the set of encapsulated atomic action and t_I is the pre-abstraction operator ([1]), that renames all internal action into t.

One may notice that this specification of ABP differs from one given in *ACP* in [2], in the specification of the channels only. As *ACP* does not have a features to describe a (probability) dependent internal behaviour of systems, which is the case here, the authors use an extra i action which serves to make a choice, between the correct transmission and the corruption of a message, non-deterministicly. Moreover, using the full (fair) abstraction operator they prove that this system behaves as a one-place buffer, that is, it is a correct communication protocol. An advantage in this probabilistic approach, particularly in this protocol, is that the full abstraction is not necessary at all. Namely, the meaning of the probabilistic choice operator and its appropriate axioms cover a need of the abstraction operator in *ACP*. In this way, using the axioms of *prACP* only without any extra principles (like KFAR, CFAR) we obtain the recursive specification for

ABP, which can be considered as a Markov chain. Thus, from (10) we can derive the following recursive specification for ABP:

$$\begin{aligned} X &= \sum_{d \in D} r_1(d) \cdot Y_d \\ Y_d &= t \cdot (t \cdot s_4(d) \cdot Z \boxplus_\pi t \cdot t \cdot t \cdot Y_d) \\ Z &= t \cdot (t \cdot X \boxplus_\rho t \cdot t \cdot t \cdot Z) \end{aligned}$$

The behaviour of the whole process is depicted in Figure 6. Using the standard Markov chain techniques we may prove various properties of this system. For example, we can prove liveness for the protocol by proving that the state X is a recurrent state. Moreover, as no internal actions have got lost, we may also compute the mean number, $M(\pi)$, of sending a message from the sender needed for its correct transmission via the channels. This result is obtained by computing the mean first-passage time from the state Y_d to the state B. In Figure 7 the obtained numbers are given for different values of π. For example, if the probability of correct transmission of a message d is 0.5 then the average number of execution of the action $c_2(d)$ is 2.

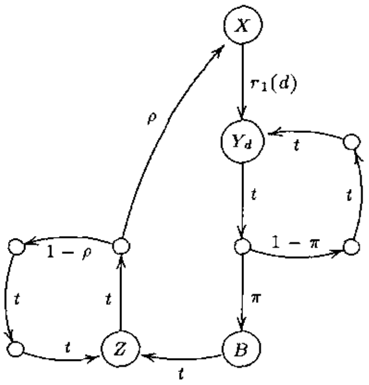


Fig. 6. The behaviour of the whole system.

π	0.1	0.15	0.2	0.25	0.3	0.35	0.4	0.45	0.5	0.55	0.6	0.65	0.7	0.75	0.8	0.85	0.9	0.95
$M(\pi)$	10.00	6.67	5.00	4.00	3.33	2.86	2.50	2.22	2.00	1.82	1.67	1.54	1.43	1.33	1.25	1.18	1.11	1.05

Fig. 7. Mean number of sending a message for different π.

6 Conclusion and Future Work

In this paper we have presented a probabilistic version of the axiom system ACP. The proposed probabilistic process algebra is based on the process algebra with partial choice, $ACP_{\boxplus}$. The main idea has been to keep the standard, non-deterministic alternative composition and to add a family of probabilistic choice operators, $\sqcup\!\!\!\!+_\pi$ for each non-zero probability π. The outcome of the probabilistic choice depends only on the internal behaviour of the system, that is, the behaviour of the system which is not influenced by the environment.

The operational semantics of *prACP* is based on the alternating model and it has been defined by a term deduction system of which the signature contains an extended set of constants (each atomic action has a dynamic counterpart) and of which the deduction rules include two transition types: probabilistic and action transition. In construction of the term models we have used probabilistic bisimulation and we have shown soundness and completeness of the term model with respect to the proposed axiom systems.

The extension with infinite processes is treated also. We have introduced infinite processes as solutions of guarded recursive specifications and using the finite projections we proved that each guarded recursive specification has unique solution in the term model.

A goal of in our work has been to find an appropriate probabilistic version of *ACP* where the interleaving axiom (CM1) is kept. It means that we followed the most direct way in the extension the non-probabilistic process algebra *ACP* with the probabilistic choice operator. Preserving our intuition behind non-deterministic choice and the interleaving approach to compositionality we proposed a new model for parallel composition of probabilistic processes. That is, the choice of the process that executes the next action is considered to be a non-deterministic choice. As communication is included in parallel composition, non-determinism occurs between three processes. By giving the specification of the Alternative Bit Protocol and obtaining some results from performance analysis of the protocol, we have shown that this model works well for certain systems. Unfortunately, we have found out that for some systems it does not give sufficient results. We have got some preliminary results of ongoing work on an improved probabilistic version of *ACP*.

Another direction in our future research is the development of algebraic verification methods in the given framework, which includes an algebraic method for resolving non-determinism in concurrent systems in order to facilitate their performance analysis. Proposition 2 says that the partial order approach, as it has been proposed in [4] for partial choice operator, cannot be applied here. We further mention as a possible option for future work the integration of a timed and probabilistic version of *ACP*.

Acknowledgments. I would like to thank Jos Baeten, Kees Middelburg and Michel Reniers for help during the work on this paper. I also thank Cris Verhoef and Pedro D'Argenio for fruitful discussions.

References

1. J.C.M. Baeten, J. A. Bergstra, *Global renaming operators in concrete process algebra*, Information

and Computation, 78: 205-245, 1988.

2. J.C.M. Baeten, W. P. Weijland, *Process algebra*, Cambridge University Press, 1990.
3. J.C.M. Baeten, C. Verhoef, *Concrete process algebra*, Handbook of Logic in Computer Science, volume 4: "Semantic Modelling", Oxford University Press, 1995.
4. J.C.M. Baeten, J.A. Bergstra, *Process algebra with partial choice*, Proc. CONCUR '94, Uppsala, B. Jonsson & J. Parrow, eds., LNCS 836, Springer Verlag, 465-480, 1994.
5. J.C.M. Baeten, J.A. Bergstra, S.A. Smolka, *Axiomatizing probabilistic processes: ACP with generative probabilities*, Information and Computation 121(2): 234-255, September 1995.
6. J.A. Bergstra, J.W. Klop, *Process algebra for synchronous communication*, Information and Control, 60: 109-137, 1984.
7. P.R. D'Argenio, C. Verhoef, *A general conservative extension theorem in process algebra with inequalities*, Theoretical Computer Science, 177: 351-380, 1997.
8. P.R. D'Argenio, H. Hermanns, J.-P. Katoen *On generative parallel composition*, Preliminary Proc. of PROBMIV'98, Indianopolis, USA, C. Baier & M. Huth & M Kwiatkowska & M. Ryan ed., 105-121, 1998.
9. A. Giacalone, C.-C. Jou, S. A. Smolka, *Algebraic reasoning for probabilistic concurrent systems*, Proc. Working Conference on Programming Concepts and Methods, IFIP TC 2, Sea of Galilee, Israel, M. Broy & C.B. Jones ed., 443-458, 1990.
10. R. J. van Glabbeek, S. A. Smolka, B. Steffen, C. M. N. Tofts, *Reactive, generative and stratified models of probabilistic processes*, Proc. of 5th Annual IEEE Symp. on Logic in Computer Science, Philadelphia, PA, 130-141, 1990.
11. H. Hansson, *Time and probability in formal design of distributed systems*, Ph.D. thesis, DoCS 91/27, University of Uppsala, 1991.
12. H. Hansson, B. Jonsson, *A calculus for communicating systems with time end probabilities*, Proc. of 11th IEEE Real-Time System Symp., Orlando, Fl., IEEE Computer Society Press, 1990.
13. S. Hart, M. Sharir, *Probabilistic temporal logic for finite and bounded models*, Proc. of 16th ACM Symp. on Theory of Computing, 1984.
14. B. Jonsson, K.G. Larsen, *Specification and refinement of probabilistic processes*, Proc. of 6th Annual IEEE Symp. on Logic in Computer Science, Amsterdam, 1991.
15. C.-C. Jou, S. A. Smolka *Equivalences, congruences and complete axiomatizations for probabilistic processes*, Proc. CONCUR '90, LNCS 458, Springer Verlag, Berlin, 367-383, 1990.
16. D. Lehmann, S. Shelah, *Reasoning with time and chance*, Information and Control, volume 53, 165-198, 1983.
17. K.G.Larsen, A.Skou, *Bisimulation through probabilistic testing*, Proc. of 16th ACM Symp. on Principles of Programming Languages, Austin, TX, 1989.
18. M.K. Molly, *Performance analysis using stochastic Petri Nets*, IEEE Transactions on Computers, volume C-31, No. 9, 913-917, 1982.
19. A. Pnueli, L. Zuck, *Verification of multiprocess probabilistic protocols*, Distributed Computing, volume 1, 53-72, 1986.
20. Y.A.Rozanov, *Introductory probability theory*, Prentice Hall, Englewood Cliffs, 1969.

21. M.Y. Vardi, *Automatic verification of probabilistic concurrent finite state programs*, Proc. of 26th Symp. on Foundations of Computer Science, IEEE Comp. Soc. Press, 327-338, 1985.

22. C. Verhoef, *A general conservative extension theorem in process algebra*, Proc. of PROCOMET'94, IFIP 2 Working Conference, San Miniato, E.-R. Olderog ed., 149-168, 1994.

This article was processed using the LaTeX macro package with LLNCS style

Computing Science Reports

Department of Mathematics and Computing Science
Eindhoven University of Technology

In this series appeared:

96/01	M. Voorhoeve and T. Basten	Process Algebra with Autonomous Actions, p. 12.
96/02	P. de Bra and A. Aerts	Multi-User Publishing in the Web: DreSS, A Document Repository Service Station, p. 12
96/03	W.M.P. van der Aalst	Parallel Computation of Reachable Dead States in a Free-choice Petri Net, p. 26.
96/04	S. Mauw	Example specifications in phi-SDL.
96/05	T. Basten and W.M.P. v.d. Aalst	A Process-Algebraic Approach to Life-Cycle Inheritance Inheritance = Encapsulation + Abstraction, p. 15.
96/06	W.M.P. van der Aalst and T. Basten	Life-Cycle Inheritance A Petri-Net-Based Approach, p. 18.
96/07	M. Voorhoeve	Structural Petri Net Equivalence, p. 16.
96/08	A.T.M. Aerts, P.M.E. De Bra, J.T. de Munk	OODB Support for WWW Applications: Disclosing the internal structure of Hyperdocuments, p. 14.
96/09	F. Dignum, H. Weigand, E. Verharen	A Formal Specification of Deadlines using Dynamic Deontic Logic, p. 18.
96/10	R. Bloo, H. Geuvers	Explicit Substitution: on the Edge of Strong Normalisation, p. 13.
96/11	T. Laan	AUTOMATH and Pure Type Systems, p. 30.
96/12	F. Kamareddine and T. Laan	A Correspondence between Nuprl and the Ramified Theory of Types, p. 12.
96/13	T. Borghuis	Priorean Tense Logics in Modal Pure Type Systems, p. 61
96/14	S.H.J. Bos and M.A. Reniers	The I^2C-bus in Discrete-Time Process Algebra, p. 25.
96/15	M.A. Reniers and J.J. Vereijken	Completeness in Discrete-Time Process Algebra, p. 139.
96/17	E. Boiten and P. Hoogendijk	Nested collections and polytypism, p. 11.
96/18	P.D.V. van der Stok	Real-Time Distributed Concurrency Control Algorithms with mixed time constraints, p. 71.
96/19	M.A. Reniers	Static Semantics of Message Sequence Charts, p. 71
96/20	L. Feijs	Algebraic Specification and Simulation of Lazy Functional Programs in a concurrent Environment, p. 27.
96/21	L. Bijlsma and R. Nederpelt	Predicate calculus: concepts and misconceptions, p. 26.
96/22	M.C.A. van de Graaf and G.J. Houben	Designing Effective Workflow Management Processes, p. 22.
96/23	W.M.P. van der Aalst	Structural Characterizations of sound workflow nets, p. 22.
96/24	M. Voorhoeve and W. van der Aalst	Conservative Adaption of Workflow, p.22
96/25	M. Vaccari and R.C. Backhouse	Deriving a systolic regular language recognizer, p. 28
97/01	B. Knaack and R. Gerth	A Discretisation Method for Asynchronous Timed Systems.
97/02	J. Hooman and O. v. Roosmalen	A Programming-Language Extension for Distributed Real-Time Systems, p. 50.
97/03	J. Blanco and A. v. Deursen	Basic Conditional Process Algebra, p. 20.
97/04	J.C.M. Baeten and J.A. Bergstra	Discrete Time Process Algebra: Absolute Time, Relative Time and Parametric Time, p. 26.
97/05	J.C.M. Baeten and J.J. Vereijken	Discrete-Time Process Algebra with Empty Process, p. 51.
97/06	M. Franssen	Tools for the Construction of Correct Programs: an Overview, p. 33.
97/07	J.C.M. Baeten and J.A. Bergstra	Bounded Stacks, Bags and Queues, p. 15.

97/08	P. Hoogendijk and R.C. Backhouse	When do datatypes commute? p. 35.
97/09	Proceedings of the Second International Workshop on Communication Modeling, Veldhoven, The Netherlands, 9-10 June, 1997.	Communication Modeling- The Language/Action Perspective, p. 147.
97/10	P.C.N. v. Gorp, E.J. Luit, D.K. Hammer E.H.L. Aarts	Distributed real-time systems: a survey of applications and a general design model, p. 31.
97/11	A. Engels, S. Mauw and M.A. Reniers	A Hierarchy of Communication Models for Message Sequence Charts, p. 30.
97/12	D. Hauschildt, E. Verbeek and W. van der Aalst	WOFLAN: A Petri-net-based Workflow Analyzer, p. 30.
97/13	W.M.P. van der Aalst	Exploring the Process Dimension of Workflow Management, p. 56.
97/14	J.F. Groote, F. Monin and J. Springintveld	A computer checked algebraic verification of a distributed summation algorithm, p. 28
97/15	M. Franssen	λP-: A Pure Type System for First Order Loginc with Automated Theorem Proving, p.35.
97/16	W.M.P. van der Aalst	On the verification of Inter-organizational workflows, p. 23
97/17	M. Vaccari and R.C. Backhouse	Calculating a Round-Robin Scheduler, p. 23.
97/18	Werkgemeenschap Informatiewetenschap redactie: P.M.E. De Bra	Informatiewetenschap 1997 Wetenschappelijke bijdragen aan de Vijfde Interdisciplinaire Conferentie Informatiewetenschap, p. 60.
98/01	W. Van der Aalst	Formalization and Verification of Event-driven Process Chains, p. 26.
98/02	M. Voorhoeve	State / Event Net Equivalence, p. 25
98/03	J.C.M. Baeten and J.A. Bergstra	Deadlock Behaviour in Split and ST Bisimulation Semantics, p. 15.
98/04	R.C. Backhouse	Pair Algebras and Galois Connections, p. 14
98/05	D. Dams	Flat Fragments of CTL and CTL*: Separating the Expressive and Distinguishing Powers. P. 22.
98/06	G. v.d. Bergen, A. Kaldewaij V.J. Dielissen	Maintenance of the Union of Intervals on a Line Revisited, p. 10.
98/07	Proceedings of the workhop on Workflow Management: Net-based Concepts, Models, Techniques and Tools (WFM'98) June 22, 1998 Lisbon, Portugal	edited by W. v.d. Aalst, p. 209
98/08	Informal proceedings of the Workshop on User Interfaces for Theorem Provers. Eindhoven University of Technology ,13-15 July 1998	edited by R.C. Backhouse, p. 180
98/09	K.M. van Hee and H.A. Reijers	An analytical method for assessing business processes, p. 29.
98/10	T. Basten and J. Hooman	Process Algebra in PVS
98/11	J. Zwanenburg	The Proof-assistemt Yarrow, p. 15
98/12	Ninth ACM Conference on Hypertext and Hypermedia Hypertext '98 Pittsburgh, USA, June 20-24, 1998 Proceedings of the second workshop on Adaptive Hypertext and Hypermedia.	Edited by P. Brusilovsky and P. De Bra, p. 95.
98/13	J.F. Groote, F. Monin and J. v.d. Pol	Checking verifications of protocols and distributed systems by computer. Extended version of a tutorial at CONCUR'98, p. 27.
98/14	T. Verhoeff (artikel volgt)	
99/01	V. Bos and J.J.T. Kleijn	Structured Operational Semantics of χ , p. 27
99/02	H.M.W. Verbeek, T. Basten and W.M.P. van der Aalst	Diagnosing Workflow Processes using Woflan, p. 44
99/03	R.C. Backhouse and P. Hoogendijk	Final Dialgebras: From Categories to Allegories, p. 26