# Axiomatizing probabilistic processes : ACP with generative probabilities (Extended abstract)

# Axiomatizing Probabilistic Processes: ACP with Generative Probabilities
(Extended Abstract)

J.C.M. Baeten
Dept. of Math and Computing Science, Eindhoven University of Technology
P.O. Box 513, 5600 MB Eindhoven, The Netherlands

J.A. Bergstra
Programming Research Group, University of Amsterdam
P.O. Box 41882, 1009 DB Amsterdam, The Netherlands

S.A. Smolka
Department of Computer Science, SUNY at Stony Brook
Stony Brook, NY 11794-4400, U.S.A.

**Abstract**

This paper is concerned with finding complete axiomatizations of probabilistic processes. We examine this problem within the context of the process algebra ACP and obtain as our end-result the axiom system $pr\mathrm{ACP}_I^-$, a probabilistic version of ACP which can be used to reason algebraically about the reliability and performance of concurrent systems. Our goal was to introduce probability into ACP in as simple a fashion as possible. Optimally, ACP should be the homomorphic image of the probabilistic version in which the probabilities are forgotten.

We begin by weakening slightly ACP to obtain the axiom system $\mathrm{ACP}_I^-$. The main difference between ACP and $\mathrm{ACP}_I^-$ is that the axiom $x+\delta = x$, which does not yield a plausible interpretation in the generative model of probabilistic computation, is rejected in $\mathrm{ACP}_I^-$. We argue that this does not affect the usefulness of $\mathrm{ACP}_I^-$ in practice, and show how ACP can be reconstructed from $\mathrm{ACP}_I^-$ with a minimal amount of technical machinery.

$pr\mathrm{ACP}_I^-$ is obtained from $\mathrm{ACP}_I^-$ through the introduction of probabilistic alternative and parallel composition operators, and a process graph model for $pr\mathrm{ACP}_I^-$ based on *probabilistic bisimulation* is developed. We show that $pr\mathrm{ACP}_I^-$ is a sound and complete axiomatization of probabilistic bisimulation for finite processes, and that $pr\mathrm{ACP}_I^-$ can be homomorphically embedded in $\mathrm{ACP}_I^-$ as desired.

Our results for $\mathrm{ACP}_I^-$ and $pr\mathrm{ACP}_I^-$ are presented in a modular fashion by first considering several subsets of the signatures. We conclude with a discussion about the suitability of an internal probabilistic choice operator in the context of $pr\mathrm{ACP}_I^-$.

## 1 Introduction

It is intriguing to consider the notion of probability (or probabilistic behavior) within the context of process algebra: a formal system of algebraic, equational, and operational techniques for the specification and verification of concurrent systems. Through the introduction of probabilistic measures, one can begin to analyze — in an algebraic fashion — "quantitative" aspects of concurrency such as reliability, performance, and fault tolerance.

In this paper, we address this problem in terms of complete axiomatizations of probabilistic processes within the context of the axiom system ACP [BK84]. ACP models an asynchronous merge, with synchronous communication, by means of arbitrary interleaving. It uses an additional constant $\delta$, which plays the role of *NIL* from CCS [Mil80] (CCS is a predecessor of ACP). The key axioms for $\delta$ are:

| | |
|---|---|
| $x + \delta = x$ | A6 |
| $\delta \cdot x = \delta$ | A7 |

The process $\delta$ represents an unfeasible option; i.e. a task that cannot be performed and therefore will be postponed indefinitely. The interaction with merge (parallel composition) is as follows:

$$x \parallel \delta = x \cdot \delta$$

(This is not provable from ACP but for each closed process expression $p$ we find that ACP $\vdash p \parallel \delta = p \cdot \delta$.) Now $\delta$ represents deadlock according to the explanation of [BK84].

Our goal is to introduce probability into ACP in as simple a fashion as possible. Optimally we would like ACP to be the homomorphic image of the probabilistic version in which the probabilities are forgotten. To this end, we develop a weaker version of ACP called $\text{ACP}_I^-$. This axiom system is just a minor alteration expressing almost the same process identities on finite processes. The virtues of this weaker axiom system are as follows:

(i) $\text{ACP}_I^-$ does not imply $x + \delta = x$. In fact, this axiom has often been criticized as being non-obvious for the interpretation $\delta$=deadlock=inaction.

(ii) $\text{ACP}_I^- + \{x + \delta = x\}$ implies the same identities on finite processes as ACP (but it is slightly weaker on identities between open processes).

(iii) $\text{ACP}_I^-$ has for all practical purposes the same expressiveness as ACP. I.e., if one can specify a protocol in ACP, this can be done just as well in $\text{ACP}_I^-$.

(iv) $\text{ACP}_I^-$ allows a probabilistic interpretation of $+$, and for this reason we need it as a point of departure for the development of a probabilistic version of ACP.

We introduce probability into $\text{ACP}_I^-$ by replacing the operators for alternative and parallel composition with probabilistic counterparts to obtain the axiom system $pr\text{ACP}_I^-$. Probabilistic choice in $pr\text{ACP}_I^-$ is of the *generative* variety, as defined in [vGSST90], in that a single probability distribution is ascribed to all alternatives. Consequently, choices involving possibly *different* actions are resolved probabilistically. In contrast, in the *reactive* model of probabilistic computation [LS89, vGSST90], a separate distribution is associated with each action, and choices involving different actions are resolved nondeterministically.

A property of the generative model of probabilistic computation is that, unlike the reactive model, the probabilities of alternatives are conditional with respect to the set of actions offered by the environment. A more detailed comparison of the reactive and generative models can be found in [vGSST90]. There the *stratified* model is also considered and it is shown that the generative model is an abstraction of the stratified model and the reactive model is an abstraction of the generative model.

Previous work on probabilistic process algebra [LS89, GJS90, vGSST90, Chr90, BM89, JL91, CSZ92] has been primarily of an operational/behavioral nature. Three exceptions, however, are [JS90, Tof90, LS92]. In [JS90], a complete axiomatization of generative probabilistic processes built from a limited set of operators ($NIL$, action prefix, probabilistic alternative composition, and tail recursion) are provided, while in [Tof90], axioms for synchronously composed "weighted processes" are given. A complete axiomatization of an SCCS-like calculus with reactive probabilities is presented in [LS92].

## Summary of Technical Results

We have obtained the following results toward our goal of finding complete axiomatizations of probabilistic processes.

- We first present the axiom system $\text{ACP}_I^-$, our point of departure from ACP. Its development is modular beginning with BPA (consisting of process constants, alternative composition, and sequential composition), to which we add a merge operator to obtain PA. Finally, a communication merge operator, the constant $\delta$, and an auxiliary *initials* operator $I$ are added to PA to obtain $\mathrm{ACP}_I^-$. In each case, we present a process graph model based on bisimulation and prove that the system is a sound and complete axiomatization of bisimulation for finite processes.

- We show in a technical sense, how ACP can be reconstructed from $\mathrm{ACP}_I^-$ through the reintroduction of the axiom A6.
- The axiom systems *pr*BPA, *pr*PA, and *pr*$\mathrm{ACP}_I^-$ for probabilistic processes are considered next. In each case, we present a process graph model based on *probabilistic bisimulation*, Larsen and Skou's [LS89] probabilistic extension of strong bisimulation, and prove that the system is a sound and complete axiomatization of probabilistic bisimulation for finite probabilistic processes.
- Connections between $\mathrm{ACP}_I^-$ and its probabilistic counterpart are then explored. We show that $\mathrm{ACP}_I^-$ is the homomorphic image of *pr*$\mathrm{ACP}_I^-$ in which the probabilities are forgotten. This result is obtained for both the graph model — the homomorphism preserves the structure of the bisimulation congruence classes, and the proof theory — the homomorphic image of a valid proof in *pr*$\mathrm{ACP}_I^-$ is a valid proof in $\mathrm{ACP}_I^-$.
- We show that certain technical problems arise when a probabilistic internal choice operator is added to *pr*$\mathrm{ACP}_I^-$, and argue that a state operator should be introduced to remedy the situation.

The structure of the rest of this paper is as follows. Section 2 presents the equational specifications BPA and $\mathrm{ACP}_I^-$, and their accompanying process graph models and completeness results. Section 3 treats the probabilistic versions of these axiom systems, namely, *pr*BPA and *pr*$\mathrm{ACP}_I^-$. The homomorphic derivability of $\mathrm{ACP}_I^-$ from *pr*$\mathrm{ACP}_I^-$ is the subject of Section 4, and, finally, Section 5 concludes. Note that we do not treat internal or $\tau$-moves in this paper, so we stay within the setting of concrete process algebra.

Due to space limitations, all proofs of results are either omitted or sketched; the full proofs appear in [BBS92]. Also, we have eliminated from this extended abstract the sections on the axiom system PA and its probabilistic counterpart *pr*PA, and the section concerning probabilistic internal choice.

## 2 A Weaker Version of ACP

In this section we present the equational theory $\mathrm{ACP}_I^-$, which, as described in Section 1, will be our point of departure for a probabilistic version of ACP. The main difference between ACP and $\mathrm{ACP}_I^-$ is that the axiom $x + \delta = x$, which does not yield a plausible interpretation in the generative model of probabilistic computation, is rejected in $\mathrm{ACP}_I^-$. We begin with the theory BPA (Basic Process Algebra).

### 2.1 BPA

The signature $\Sigma(\mathrm{BPA}(A))$ consists of one sort **P** (for processes) and three types of operators: constant processes $a$, for each atomic action $a$, the sequential composition (or sequencing) operator '$\cdot$', and the alternative composition (or nondeterministic choice) operator '$+$'. The set of all constants is denoted by $A$, and is considered a parameter to the theory.

$$\Sigma(\mathrm{BPA}(A)) = \{a : \to \mathbf{P} | a \in A\} \cup \{+ : \mathbf{P} \times \mathbf{P} \to \mathbf{P}\} \cup \{\cdot : \mathbf{P} \times \mathbf{P} \to \mathbf{P}\}$$

The axiom system $\mathrm{BPA}(A)$ is given by:

| | |
|---|---|
| $x + y = y + x$ | A1 |
| $(x + y) + z = x + (y + z)$ | A2 |
| $x + x = x$ | A3 |
| $(x + y) \cdot z = x \cdot z + y \cdot z$ | A4 |
| $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ | A5 |

Note the absence of the axiom $x \cdot (y + z) = x \cdot y + x \cdot z$ which does not hold in our process graph model.

**Definition 2.1** *A* process graph *$g$ is a triple $< V, r, \longrightarrow >$ such that*

- *$V$ is the set of* nodes *(vertices) of $g$*
- *$r \in V$ is the* root *of $g$*
- *$\longrightarrow \subseteq V \times A \times V$ is the* transition relation *of $g$*

The *endpoints* of $g$ are those nodes devoid of outgoing transitions and represent successful termination. We often write $v \xrightarrow{a} v'$ to denote the fact that $(v, a, v') \in \longrightarrow$. We denote by $\mathcal{G}$ the family of all process graphs. Bisimulation, due to Milner and Park, is the primary equivalence relation we consider on process graphs.

**Definition 2.2** *Let $g_1 =< V_1, r_1, \longrightarrow_1 >$, $g_2 =< V_2, r_2, \longrightarrow_2 >$ be two process graphs. A* bisimulation *between $g_1$ and $g_2$ is a relation $\mathcal{R} \subseteq V_1 \times V_2$ with the following properties:*

- $\mathcal{R}(r_1, r_2)$
- *$\forall v \in V_1$, $w \in V_2$ with $\mathcal{R}(v, w)$:*
  *$\forall a \in A$ and $v' \in V_1$,*
  *if $v \xrightarrow{a}_1 v'$ then $\exists w' \in V_2$ with $\mathcal{R}(v', w')$ and $w \xrightarrow{a}_2 w'$*
- *and* vice versa *with the roles of $v$ and $w$ reversed.*

*Graphs $g_1$ and $g_2$ are said to be* bisimilar, *written $g_1 \leftrightarroweq g_2$, if there exists a bisimulation between $g_1$ and $g_2$.*

The operators from $\Sigma(\mathrm{BPA}(A))$ are defined on the domain of (root-unwound) process graphs in the standard way (e.g., [BW90]). For example, letting $g_1 = < V_1, r_1, \longrightarrow_1 >$, $g_2 = < V_2, r_2, \longrightarrow_2 >$, we have that $g_1 \cdot g_2$ is obtained by appending a copy of $g_2$ at each endpoint of $g_1$. In detail, $g_1 \cdot g_2$ is given by $< V_1 \times V_2, (r_1, r_2), \longrightarrow >$ where $(q_1, q_2) \xrightarrow{a} (q_1', q_2')$ if either

- $q_1 \xrightarrow{a}_1 q_1'$ and $q_2 = q_2' = r_2$
- $q_2 \xrightarrow{a}_2 q_2'$ and $q_1 = q_1'$ is an endpoint

In the setting of BPA, $\leftrightarroweq$ is a congruence and BPA($A$) constitutes a sound and complete axiomatization of process equivalence in $\mathcal{G}/\leftrightarroweq$ for finite processes.

**Theorem 2.1** ([BW90])

1. $\mathcal{G}/\leftrightarroweq \models \mathrm{BPA}(A)$
2. *For all closed expressions $p, q$ over $\Sigma(\mathrm{BPA}(A))$:*
   $$\mathcal{G}/\leftrightarroweq \models p = q \implies \mathrm{BPA}(A) \vdash p = q.$$

## 2.2 ACP without A6

The equational system $\mathrm{ACP}_I^-(A)$ treats the operators of BPA($A$) as well as the new constant $\delta$, representing deadlock; a *communication merge* operator $|$ describing the result of a communication between any two atomic actions; a *merge* operator $\|$ representing the interleaved composition of two process which additionally admits the possibility of communication; a *left merge* operator $\lfloor\!\lfloor$ which is the same as $\|$ but always starts with the "left" process; and a family of restriction operators $\partial_H$, $H \subseteq A$. We will also need an auxiliary operator $I$ that defines the initial actions (the *initials*) that a process can perform.

Letting $A_\delta = A \cup \{\delta\}$, the signature of $\mathrm{ACP}_I^-(A)$ extends that of BPA($A$) as follows:

$$\Sigma(\mathrm{ACP}_I^-(A)) = \Sigma(\mathrm{BPA}(A)) \cup \{\delta :\to \mathbf{P}\} \cup \{\|: \mathbf{P}\times\mathbf{P}\to\mathbf{P}\} \cup \{⌊\!⌊: \mathbf{P}\times\mathbf{P}\to\mathbf{P}\} \cup$$
$$\{| : \mathbf{P}\times\mathbf{P}\to\mathbf{P}\} \cup \{\partial_H : \mathbf{P}\to\mathbf{P} \mid H\subseteq A\} \cup \{I : \mathbf{P}\to 2^{A_\delta}\}$$

It is convenient to define the communication merge operator as a binary commutative and associative function on atomic actions; i.e., $| : A_\delta \times A_\delta \to A_\delta$,. In order to axiomatize $|$ as a function on processes (rather than on elements of $A_\delta$) we define the characteristic predicate $\overline{A_\delta}$ of $A_\delta$ in the usual way:

$$\overline{A_\delta}(x) = \bigvee_{a\in A_\delta} (x = a)$$

We require $|$ to be total and this is captured by the following axiom:[1]

| | |
|---|---|
| $\forall a,b \in \mathbf{P}\ \overline{A_\delta}(a) \wedge \overline{A_\delta}(b) \implies \exists c \in \mathbf{P}\ \overline{A_\delta}(c) \wedge a\|b = c$ | C0 |

The axioms of $\mathrm{ACP}_I^-(A)$ are now given. In this system, $a$,$b$,$c$ range over$A_\delta$, and $\cap$,$\cup$ are used on $2^{A_\delta}$ without further specification.

BPA($A$) +

| | |
|---|---|
| $\delta \cdot x = \delta$ | A7 |

+

C0 +

| | |
|---|---|
| $a\|b = b\|a$ | C1 |
| $(a\|b)\|c = a\|(b\|c)$ | C2 |
| $\delta\|a = \delta$ | C3 |

+

| | |
|---|---|
| $x \parallel y = x ⌊\!⌊ y + y ⌊\!⌊ x + x\|y$ | CM1 |
| $a ⌊\!⌊ x = a \cdot x$ | CM2 |
| $(a\cdot x) ⌊\!⌊ y = a(x \parallel y)$ | CM3 |
| $(x+y) ⌊\!⌊ z = (x ⌊\!⌊ z) + (y ⌊\!⌊ z)$ | CM4 |
| $a\|(b\cdot x) = (a\|b)\cdot x$ | CM5 |
| $(a\cdot x)\|b = (a\|b)\cdot x$ | CM6 |
| $(a\cdot x)\|(b\cdot y) = (a\|b)\cdot(x \parallel y)$ | CM7 |
| $(x+y)\|z = x\|z + y\|z$ | CM8 |
| $x\|(y+z) = x\|y + x\|z$ | CM9 |

+

| | |
|---|---|
| $I(a) = \{a\}$ | I1 |
| $I(x\cdot y) = I(x)$ | I2 |
| $I(x+y) = I(x)\cup I(y)$ | I3 |

[1]Axiom C0 is often replaced by choosing a total function $\gamma : A_\delta \times A_\delta \to A_\delta$ and having all identities of the graph of $\gamma$ as axioms: $a|b = \gamma(a,b)$. In this way, $\gamma$ becomes a parameter to the theory (see, e.g., [BW90]).

| | | |
|---|---|---|
| $a \in H \implies \partial_H(a) = \delta$ | | D1 |
| $a \notin H \implies \partial_H(a) = a$ | | D2 |
| $I(x) \subseteq H \cup \{\delta\} \implies \partial_H(x+y) = \partial_H(y)$ | | D3.1 |
| $I(x+y) \cap (H \cup \{\delta\}) = \emptyset \implies \partial_H(x+y) = \partial_H(x) + \partial_H(y)$ | | D3.2 |
| $\partial_H(x \cdot y) = \partial_H(x) \cdot \partial_H(y)$ | | D4 |

*Comments:* $\mathrm{ACP}_I^-(A)$ differs from ACP by the absence of A6 and the presence of the weaker axioms D3.1-2 instead of D3: $\partial_H(x+y) = \partial_H(x) + \partial_H(y)$. Note that it is within axioms D3.1-2 where the auxiliary operator $I$ comes into play. We give an example to illustrate the new axiom system.

$$\begin{aligned}
\partial_{\{c\}}(a + (b + c)) &= \partial_{\{c\}}(c + (a + b)) && \text{(by A1 and A2)}\\
&= \partial_{\{c\}}(a + b) && \text{(by D3.1)}\\
&= \partial_{\{c\}}(a) + \partial_{\{c\}}(b) && \text{(by D3.2)}\\
&= a + b && \text{(by D2 twice)}
\end{aligned}$$

Our graph model for $\mathrm{ACP}_I^-(A)$ is standard (see, e.g., [BW90]) with the exception of the restriction operator. This operator removes all edges labeled with actions from the set of restricted actions $H$. It also removes $\delta$-edges, which it must do to ensure the soundness of D3.1. In case a node with at least one outgoing edge has all its edges removed, a new $\delta$-edge, to the "dead" state $v_\delta$, is added. Formally, $\partial_H(g_1)$ is given by $< V_1 \cup \{v_\delta\}, r_1, \longrightarrow >$ where $v_\delta \notin V_1$ and

$$\longrightarrow \; = \; \{(v, a, v') \in \longrightarrow_1 \mid a \notin H \cup \{\delta\}\} \; \cup$$

$$\{(v, \delta, v_\delta) \mid \#(\{(v, a, v') \in \longrightarrow_1 \mid a \in H \cup \{\delta\}\}) \; = \; \#(\{(v, a, v') \in \longrightarrow_1 \mid a \in A_\delta\}) \geq 1\}$$

Here $\#(S)$ is equivalent notation for $|S|$, for $S$ a set; i.e. $\#$ is the cardinality function on sets.

The interpretation of $\delta$ as deadlock requires a new definition of bisimulation in which a weaker condition is imposed on $\delta$-edges. The resulting relation, which we call a *$\delta$-bisimulation*, is the same as in Definition 2.2 on non-$\delta$ edges. Otherwise, if $\mathcal{R}$ is a $\delta$-bisimulation and $\mathcal{R}(v, w)$, then:

if $v \xrightarrow{\delta}_1 v'$, for some $v'$, then $w \xrightarrow{\delta}_2 w'$, for some $w'$

and *vice versa* with the roles of $v$ and $w$ reversed. The resulting equivalence is denoted $\leftrightarrows_\delta$ and can be shown to be a congruence in the context of $\mathrm{ACP}_I^-(A)$. That $\mathrm{ACP}_I^-(A)$ is a sound and complete axiomatization of $\leftrightarrows_\delta$ for finite processes is given by the following.

**Theorem 2.2**

1. $\mathcal{G}/\leftrightarrows_\delta \models \mathrm{ACP}_I^-(A)$

2. *For all closed expressions p,q over* $\Sigma(\mathrm{ACP}_I^-(A))$*:*

$$\mathcal{G}/\leftrightarrows_\delta \models p = q \implies \mathrm{ACP}_I^-(A) \vdash p = q.$$

**Proof sketch:** The proof is by a normal form reduction and relies on the completeness of BPA (Theorem 2.1). We first define a *basic term* as one constructed from the constants $A_\delta$, alternative composition, and (non-$\delta$) action prefixing. Note that a basic term is a $\mathrm{BPA}(A_\delta)$ term. A term rewriting system, $\mathrm{RACP}_I^-(A)$, based on $\mathrm{ACP}_I^-(A)$ is introduced such that a normal form of the system is a $\mathrm{BPA}(A_\delta)$ term in which all occurrences of communication merge, merge, left-merge, and restriction have been eliminated. $\mathrm{RACP}_I^-(A)$ is shown to be *strongly normalizing* by transforming a reduction sequence $\pi$ of $\mathrm{RACP}_I^-(A)$ into a valid reduction sequence of $\mathrm{RACP}(A)$ [BK84]. Finally, a normal form of $\mathrm{RACP}_I^-(A)$ is shown to be a basic term, and by the completeness of $\mathrm{BPA}(A_\delta)$ we are done. □

#### 2.2.1 Connections Between ACP and $\text{ACP}_I^-$

Let $\mathbf{A}$ be the usual bisimulation model for ACP($A$), and let $\mathbf{A}^- = \mathcal{G}/\leftrightarrows_\delta$ be the bisimulation model for $\text{ACP}_I^-(A)$. Then for $p$,$q$ closed expressions over $\Sigma(\text{ACP}(A))$ we have the following results.

1. $\mathbf{A}^- \models p = q \implies \mathbf{A} \models p = q$. This implies that $\mathbf{A}^-$ can be homomorphically embedded in $\mathbf{A}$ using the identity mapping.

2. $\mathbf{A} \models p = q \implies \mathbf{A}^- \models \partial_\emptyset(p) = \partial_\emptyset(q)$. This implies that $\mathbf{A}$ can be homomorphically embedded in $\mathbf{A}^-$ using the homomorphism $\varphi : \mathbf{A} \longrightarrow \mathbf{A}^-$, such that $\varphi(x) = \partial_\emptyset(x)$

3. $\text{ACP}(A) \vdash p = q \implies \text{ACP}_I^-(A) + \{x + \delta = x\} \vdash p = q$

4. $\text{ACP}_I^-(A) \vdash \partial_\emptyset(x + \delta) = \partial_\emptyset(x)$

## 3 A Probabilistic Version of ACP

Our discussion of probabilistic ACP will proceed in a manner similar to before. We will present the axioms systems $pr$BPA($A$) and $pr\text{ACP}_I^-(A)$, the probabilistic counterparts of BPA($A$) and $\text{ACP}_I^-(A)$, and prove completeness in a graph model based on probabilistic bisimulation.

### 3.1 Probabilistic BPA

As usual, $(0,1)$ denotes the open interval of the real line $\{r \in \Re \mid 0 < r < 1\}$, and $[0,1]$ denotes the closed interval of the real line $\{r \in \Re \mid 0 \leq r \leq 1\}$. The signature $\Sigma(pr\text{BPA}(A))$ over the sort $pr\mathbf{P}$ (for probabilistic processes) is given by:

$$\begin{aligned}\Sigma(pr\text{BPA}(A)) \quad = \quad & \{a : \rightarrow pr\mathbf{P} | a \in A\} \cup \{+_p : pr\mathbf{P} \times pr\mathbf{P} \rightarrow pr\mathbf{P} \mid p \in (0,1)\} \cup \\ & \{\cdot : pr\mathbf{P} \times pr\mathbf{P} \rightarrow pr\mathbf{P}\}\end{aligned}$$

The operator $+$ has been replaced by the family of operators $+_p$, for each probability $p$ in the interval $(0,1)$, and is now called *probabilistic alternative composition.* Intuitively, the expression $x +_p y$ behaves like $x$ with probability $p$ and like $y$ with probability $1-p$. Probabilistic alternative composition is *generative* [vGSST90] in that a single distribution (viz. the discrete probability distribution $\{p, 1-p\}$) is associated with the two alternatives $x$ and $y$. As mentioned in Section 1, these probabilities are conditional with respect to the set of actions permitted by the environment. This will become clear in Section 3.2 with the introduction of the restriction operator $\partial_H$ in the setting of probabilistic ACP.

We have the following axioms for $pr$BPA($A$):

| | |
|---|---|
| $x +_p y = y +_{1-p} x$ | $pr$A1 |
| $x +_p (y +_q z) = (x +_{p/(p+q-pq)} y) +_{p+q-pq} z$ | $pr$A2 |
| $x +_p x = x$ | $pr$A3 |
| $(x +_p y) \cdot z = x \cdot z +_p y \cdot z$ | $pr$A4 |
| $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ | $pr$A5 |

As for BPA($A$), we consider process graphs, with labels from $A$, as a model for $pr$BPA($A$). Additionally, a probability distribution will be ascribed to each node's outgoing transitions.

**Definition 3.1** *A* probabilistic process graph $g$ *is a triple* $< V, r, \mu >$ *such that* $V$ *and* $r$ *are as in Definition 2.1 and* $\mu : (V \times A \times V) \rightarrow [0,1]$, *the* transition distribution function *of* $g$, *is a total function satisfying the following* stochasticity condition*:*

$$\forall v \in V \quad \sum_{\substack{a \in A, \\ v' \in V}} \mu(v,a,v') \in \{0,1\}$$

Intuitively, $\mu(v,a,v') = p$ means that, with probability $p$, node $v$ can perform an $a$-transition to node $v'$. A node in a stochastic probabilistic process graph performs some transition with probability 1, unless it is an endpoint. When $\mu(v,a,v') > 0$ we say that $v'$ is *reachable* from $v$ and the notion of reachability extends to sequences of transitions in the natural way. We denote by $pr\mathcal{G}$ the family of all probabilistic process graphs.

The notion of strong bisimulation for nondeterministic processes has been extended by Larsen and Skou [LS89] to reactive probabilistic processes in the form of *probabilistic bisimulation*. Here we define probabilistic bisimulation on generative processes and to do so we first need to lift the definition of the transition distribution function as follows:

$$\mu : (V \times A \times 2^V) \longrightarrow [0,1] \text{ such that } \mu(v,a,S) = \sum_{v' \in S} \mu(v,a,v')$$

Intuitively, $\mu(v,a,S) = q$ means that node $v$, with total probability $q$, can perform an $a$-transition to some node in $S$.

**Definition 3.2** ([LS89]) *Let $g_1 = <V_1, r_1, \mu_1>$, $g_2 = <V_2, r_2, \mu_2>$ be probabilistic process graphs. A* probabilistic bisimulation *between $g_1$ and $g_2$ is an equivalence relation $\mathcal{R} \subseteq V_1 \times V_2$ with the following properties:*

- $\mathcal{R}(r_1, r_2)$
- *$\forall v \in V_1$, $w \in V_2$ with $v$ reachable from $r_1$, $w$ reachable from $r_2$, and $\mathcal{R}(v,w)$:*
  $\forall a \in A,\ S \in (V_1 \cup V_2)/\mathcal{R},\ \ \mu_1(v,a,S) = \mu_2(w,a,S)$

*Graphs $g_1$ and $g_2$ are* probabilistically bisimilar, *written $g_1 \leftrightarroweq^{pr} g_2$, if there exists a probabilistic bisimulation between $g_1$ and $g_2$.*

Intuitively, two nodes are probabilistically bisimilar if, for all actions in $A$, they transit to probabilistic bisimulation classes with equal probability. Note the somewhat subtle use of recursion in the definition.

We now define the operators of $pr$BPA($A$) on the domain of probabilistic process graphs. For this purpose, it is convenient to assume that probabilistic process graphs are acyclic with respect to transitions of non-zero probability (we consider only finite processes anyway) and that the root is not an endpoint. For the remainder of Section 3, let $g_1 = <V_1, r_1, \mu_1>$, $g_2 = <V_2, r_2, \mu_2>$ be probabilistic process graphs satisfying these assumptions such that $V_1 \cap V_2 = \emptyset$.

**Definition 3.3** *The operators $a \in A$, $+_p$, and $\cdot$ are defined on $pr\mathcal{G}$ as follows:*

$a \in A$: *The process graph for each of these constants is given by $<\{r_a, v\}, r_a, \mu_a>$, where $\mu_a(r_a, a, v) = 1$ is the only transition with non-zero probability.*

$g_1 +_p g_2$: *is given by $<V_1 \cup V_2 \cup \{r\}, r, \mu>$ where $r \notin V_1 \cup V_2$ and*

| | |
|---|---|
| $\mu(r,a,v') = p \cdot \mu_1(r_1,a,v')$ | *if $v' \in V_1$* |
| $\mu(r,a,v') = (1-p) \cdot \mu_2(r_2,a,v')$ | *if $v' \in V_2$* |
| $\mu(v,a,v') = \mu_1(v,a,v')$ | *if $v, v' \in V_1$* |
| $\mu(v,a,v') = \mu_2(v,a,v')$ | *if $v, v' \in V_2$* |
| $\mu(v,a,v') = 0$ | *otherwise* |

The case for $g_1 \cdot g_2$ is analogous to the nonprobabilistic case. Note that as a consequence of this definition, and the fact that probabilistic process graphs are acyclic, transitions from $r_1$ and $r_2$ (some of which may be ascribed non-zero probabilities) are not reachable from the root $r$ of $g_1 + g_2$.

We have that $\leftrightarroweq^{pr}$ is a congruence in $pr$BPA($A$).

**Proposition 3.1** *If $g_1 \leftrightarrows^{pr} g_2$, then $g +_p g_1 \leftrightarrows^{pr} g +_p g_2$, $g \cdot g_1 \leftrightarrows^{pr} g \cdot g_2$, and $g_1 \cdot g \leftrightarrows^{pr} g_2 \cdot g$.*

The graph model for $pr$BPA($A$) is now given by $pr\mathcal{G}/\leftrightarrows^{pr}$ and we prove that $pr$BPA($A$) constitutes a sound and complete axiomatization of process equivalence in $pr\mathcal{G}/\leftrightarrows$ for finite processes.

**Theorem 3.1**

1. $pr\mathcal{G}/\leftrightarrows^{pr} \models pr\text{BPA}(A)$
2. *For all closed expressions s,t over* $\Sigma(pr\text{BPA}(A))$*:*
   $pr\mathcal{G}/\leftrightarrows^{pr} \models s = t \implies pr\text{BPA}(A) \vdash s = t.$

**Proof sketch:** The proof is again by a normal form reduction. We first introduce the notation

$$\sum_{i=1}^{n}[p_i]x_i$$

with $\sum p_i = 1$ and $p_i > 0$ for all $i$. So, in particular, when $n = 1$, $p_1 = 1$. This notation abbreviates nested probabilistic alternative composition expressions as follows:

$$\sum_{i=1}^{1}[p_i]x_i = x_1 \quad \text{and} \quad \sum_{i=1}^{n+1}[p_i]x_i = x_1 +_{p_1} \left(\sum_{i=1}^{n}\left[\frac{p_{i+1}}{1-p_1}\right]x_{i+1}\right)$$

This *summation form* notation is useful as it directly reflects the transition structure of the probabilistic process graph underlying the nested probabilistic alternative composition. That is, the process graph of the summation form $\sum[p_i]x_i$ will have a probability-$p_i$ transition from its root to the node representing the root of the process graph of $x_i$.

A *probabilistic basic term* is then defined to be a summation form whose summands are either constants from $A_\delta$ or of the form $a \cdot t$, where $a \in A$ and $t$ itself is a probabilistic basic term. Furthermore, the summands of a probabilistic basic term are required to be pairwise probabilistically bisimulation inequivalent.

We next show that the axioms of $pr$BPA($A$) are sufficient to prove a closed $pr$BPA($A$) term $t$ equal to a probabilistic basic term. The proof is in two steps. First the term rewriting system corresponding to $pr$BPA($A$) axioms $pr$A4 and $pr$A5 is used to transform $t$ into a term in which the only occurrences of sequential composition are of the action-prefixing variety. Secondly, the constraint that the summands be pairwise inequivalent is met by using axioms $pr$A1, $pr$A2, and $pr$A3 to group together and, in the process, compute the total probability assumed by a summand in a probabilistic basic term. Completeness is then proved by induction on the maximum depth of the probabilistic basic terms for the given $s$ and $t$. □

## 3.2 Probabilistic ACP

The signature of $pr\text{ACP}_I^-(A)$ extends that of $pr$BPA($A$):

$$\Sigma(pr\text{ACP}_I^-(A)) = \Sigma(pr\text{BPA}(A)) \cup \{\delta :\rightarrow pr\text{P}\} \cup \{I : pr\text{P} \rightarrow 2^{A_\delta}\} \cup$$
$$\{|_{r,s} : pr\text{P} \times pr\text{P} \rightarrow pr\text{P} \mid r,s \in (0,1)\} \cup \{\|_{r,s} : pr\text{P} \times pr\text{P} \rightarrow pr\text{P} \mid r,s \in (0,1)\} \cup$$
$$\{\lfloor\!\lfloor_{r,s} : pr\text{P} \times pr\text{P} \rightarrow pr\text{P} \mid r,s \in (0,1)\} \cup \{\partial_H : pr\text{P} \rightarrow pr\text{P} \mid H \subseteq A\}$$

Thus, for each of the operators $|$, $\|$, and $\lfloor\!\lfloor$ we have a family of operators, each indexed by two probabilities from the interval $(0,1)$. These operators work intuitively as follows. Consider for example the merge operator. In the expression $x \|_{r,s} y$, a communication between $x$ and $y$ occurs with probability $1-s$, and an autonomous move by either $x$ or $y$ occurs with probability $s$. Given that an autonomous move occurs, it comes from $x$ with probability $r$ and from $y$ with probability $1-r$.

The treatment of the communication merge is exactly analogous to the situation in the nonprobabilistic case (Section 2.2). The "totality" axiom C0 now becomes:

| | |
|---|---|
| $\forall a, b \in pr\mathbf{P}\ \overline{A_\delta}(a) \wedge \overline{A_\delta}(b) \implies \exists c \in pr\mathbf{P}\ \forall r, s \in (0,1)\ \overline{A_\delta}(c) \wedge a \mid_{r,s} b = c$ | *pr*C0 |

The axioms of $pr\text{ACP}_I^-(A)$ are as follows. In this system, $a$,$b$,$c$ range over $A_\delta$, and $I$ has functionality $I : pr\mathbf{P} \to 2^{A_\delta}$.

$pr$BPA($A$) +

| | |
|---|---|
| $\delta \cdot x = \delta$ | *pr*A7 |

+

*pr*C0 +

| | |
|---|---|
| $a \mid_{r,s} b = b \mid_{(1-r),s} a$ | *pr*C1 |
| $(a \mid_{r,s} b) \mid_{u,v} c = a \mid_{r,s} (b \mid_{u,v} c)$ | *pr*C2 |
| $\delta \mid_{r,s} a = \delta$ | *pr*C3 |

+

| | |
|---|---|
| $x \parallel_{r,s} y = ((x \mathbin{\lfloor\!\lfloor}_{r,s} y) +_r (y \mathbin{\lfloor\!\lfloor}_{(1-r),s} x)) +_s (x \mid_{r,s} y)$ | *pr*CM1 |
| $a \mathbin{\lfloor\!\lfloor}_{r,s} y = a \cdot y$ | *pr*CM2 |
| $(a \cdot x) \mathbin{\lfloor\!\lfloor}_{r,s} y = a \cdot (x \parallel_{r,s} y)$ | *pr*CM3 |
| $(x +_p y) \mathbin{\lfloor\!\lfloor}_{r,s} z = (x \mathbin{\lfloor\!\lfloor}_{r,s} z) +_p (y \mathbin{\lfloor\!\lfloor}_{r,s} z)$ | *pr*CM4 |
| $a \mid_{r,s} (b \cdot x) = (a \mid_{r,s} b) \cdot x$ | *pr*CM5 |
| $(a \cdot x) \mid_{r,s} b = (a \mid_{r,s} b) \cdot x$ | *pr*CM6 |
| $(a \cdot x) \mid_{r,s} (b \cdot y) = (a \mid_{r,s} b) \cdot (x \parallel_{r,s} y)$ | *pr*CM7 |
| $(x +_p y) \mid_{r,s} z = x \mid_{r,s} z\ +_p\ y \mid_{r,s} z$ | *pr*CM8 |
| $x \mid_{r,s} (y +_p z) = x \mid_{r,s} y\ +_p\ x \mid_{r,s} z$ | *pr*CM9 |

+

| | |
|---|---|
| $I(a) = \{a\}$ | *pr*I1 |
| $I(x \cdot y) = I(x)$ | *pr*I2 |
| $I(x +_p y) = I(x) \cup I(y)$ | *pr*I3 |

+

| | |
|---|---|
| $a \in H \implies \partial_H(a) = \delta$ | *pr*D1 |
| $a \notin H \implies \partial_H(a) = a$ | *pr*D2 |
| $I(x) \subseteq H \cup \{\delta\} \implies \partial_H(x +_p y) = \partial_H(y)$ | *pr*D3.1 |
| $I(x + y) \cap (H \cup \{\delta\}) = \emptyset \implies \partial_H(x +_p y) = \partial_H(x) +_p \partial_H(y)$ | *pr*D3.2 |
| $\partial_H(x \cdot y) = \partial_H(x) \cdot \partial_H(y)$ | *pr*D4 |

To define the graph model for $pr\text{ACP}_I^-(A)$, we need to introduce a "normalization factor" to be used in computing conditional probabilities in a restricted process.

**Definition 3.4** *Let $g = <V, r, \mu>$ be a probabilistic process graph. Then, for $v \in V$, the* normalization factor of $v$ with respect to the set of actions $H \subseteq A$ *is given by*

$$\nu_H(v) = 1 - \sum\{\mu(v, a, v') | a \in H \cup \{\delta\}, v' \in V\}$$

Intuitively, $\nu_H(v)$ is the sum of the probabilities of those transitions from $v$ that remain after restricting by the set of actions $H$.

**Definition 3.5** *The operators $\delta$, $\|_{r,s}$, $⌊⌊_{r,s}$, $|_{r,s}$, and $\partial_H$, $H \subseteq A$, are defined on $prG$ as follows:*

$\delta$: *The process graph of $\delta$ is given by Definition 3.3, treating $\delta$ as a normal atomic action; i.e., the graph of $\delta$ is $<\{r_\delta, v\}, r_\delta, \mu_\delta>$, where $\mu_\delta(r_\delta, \delta, v) = 1$ is the only transition with non-zero probability.*

$g_1 \|_{r,s} g_2$: *is given by $<V_1 \times V_2, (r_1, r_2), \mu>$ where for all $a \in A_\delta$, $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$*

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} r \cdot s \cdot \mu_1(v_1, a, v_1') & \text{if } v_2 \text{ not an endpoint} \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-r) \cdot s \cdot \mu_2(v_2, a, v_2') & \text{if } v_1 \text{ not an endpoint} \\ \mu_2(v_2, a, v_2') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1', v_2')) = (1-s) \cdot \sum_{b,c:\, b|_{r,s} c = a} \mu_1(v_1, b, v_1') \cdot \mu_2(v_2, c, v_2')$$

$g_1 ⌊⌊_{r,s} g_2$: *is given by $<V_1 \times V_2, (r_1, r_2), \mu>$ where for all $a \in A_\delta$, $v_1, v_1', \in V_1$, $v_2, v_2', \in V_2$*

- $\mu((r_1, r_2), a, (v_1', r_2)) = \mu_1(r_1, a, v_1')$
- *if* $v_1 \neq r_1$ *or* $v_2 \neq r_2$

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} r \cdot s \cdot \mu_1(v_1, a, v_1') & \text{if } v_2 \text{ not an endpoint} \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-r) \cdot s \cdot \mu_2(v_2, a, v_2') & \text{if } v_1 \text{ not an endpoint} \\ \mu_2(v_2, a, v_2') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1', v_2')) = (1-s) \cdot \sum_{b,c:\, b|_{r,s} c = a} \mu_1(v_1, b, v_1') \cdot \mu_2(v_2, c, v_2')$$

- *if* $v_2' \neq r_2$ $\mu((r_1, r_2), a, (v_1', v_2')) = 0$

$g_1 |_{r,s} g_2$: *is given by $<V_1 \times V_2, (r_1, r_2), \mu>$ where for all $a \in A_\delta$, $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$*

- $\mu((r_1, r_2), a, (v_1', v_2')) = \sum_{b,c:b|_{r,s} c=a} \mu_1(r_1, b, v_1') \cdot \mu_2(r_2, c, v_2')$
- *if* $v_1 \neq r_1$ *or* $v_2 \neq r_2$

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} r \cdot s \cdot \mu_1(v_1, a, v_1') & \text{if } v_2 \text{ not an endpoint} \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-r) \cdot s \cdot \mu_2(v_2, a, v_2') & \text{if } v_1 \text{ not an endpoint} \\ \mu_2(v_2, a, v_2') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1', v_2')) = (1-s) \cdot \sum_{b,c:\, b|_{r,s} c = a} \mu_1(v_1, b, v_1') \cdot \mu_2(v_2, c, v_2')$$

- *if* ($v_1' \neq r_1$ *and* $v_2' = r_2$) *or* ($v_1' = r_1$ *and* $v_2' \neq r_2$) $\mu((r_1, r_2), a, (v_1', v_2')) = 0$

$\partial_H(g_1)$: *is given by $<V, r, \mu>$ where $V = V_1 \cup \{v_\delta\}$, $v_\delta$ a new endpoint not in $V_1$, $r = r_1$, and for all $a \in A$, $v_1, v_1' \in V_1$*

$$\mu(v_1, a, v_1') = \begin{cases} 0 & \text{if } a \in H \\ \mu_1(v_1, a, v_1')/\nu_H(v_1) & \text{otherwise} \end{cases}$$

$$\mu(v_1, \delta, v_1') = 0$$

$$\mu(v_1, a, v_\delta) = 0 \text{ if } a \neq \delta$$

$$\mu(v_1, \delta, v_\delta) = \begin{cases} 0 & \text{if } \exists a \notin H \cup \{\delta\}, v_1' \in V : \mu_1(v_1, a, v_1') > 0 \\ 1 & \text{otherwise} \end{cases}$$

Note the careful treatment of endpoints in the above definition—e.g., in a merge, if one process terminates, the other continues with its original, unweighted probability—and of transitions from the root $(r_1, r_2)$ in $g_1 \mathbin{\|\!\!\lfloor}_{r,s} g_2$ and $g_1 |_{r,s} g_2$—e.g., in a left merge, transitions emanating from the root that start with $g_2$ are given probability 0.

As in the nonprobabilistic case, the presence of $\delta$-edges requires a new definition of probabilistic bisimulation. A *$\delta$-probabilistic bisimulation* is the same as in Definition 3.2 with the additional clause

$$\mu_1(v, \delta, V_1) = \mu_2(w, \delta, V_2)$$

That is, $\delta$-probabilistically bisimilar nodes must perform the action $\delta$ with the same total probability, without regard to where the $\delta$-transitions lead. The resulting equivalence is denoted $\leftrightarrows_\delta^{pr}$.

**Theorem 3.2**

1. *$pr\mathcal{G}/\leftrightarrows_\delta^{pr} \models pr\mathrm{ACP}_I^-(A)$*
2. *For all closed expressions p,q over $\Sigma(pr\mathrm{ACP}_I^-(A))$:*

$$pr\mathcal{G}/\leftrightarrows_\delta^{pr} \models p = q \implies pr\mathrm{ACP}_I^-(A) \vdash p = q.$$

**Proof sketch:** The proof is analogous to the completeness proof of $\mathrm{ACP}_I^-(A)$.

- The definition of a probabilistic basic term uses $+_p$ instead of $+$ and the term rewriting system $pr\mathrm{RACP}_I^-(A)$ uses the probabilistic counterparts of the rules in $\mathrm{RACP}_I^-(A)$.
- $pr\mathrm{RACP}_I^-(A)$ is strongly normalizing: take a $pr\mathrm{RACP}_I^-(A)$ reduction and erase all probability subscripts. One obtains a valid $\mathrm{RACP}_I^-(A)$ reduction.
- The proof that a probabilistic normal form is also a probabilistic basic term proceeds as before – no rule in $pr\mathrm{RACP}_I^-(A)$ is conditional with respect to any probability. By the completeness of $pr\mathrm{BPA}(A_\delta)$ we are done.

□

## 4 $\mathrm{ACP}_\mathrm{I}^-$ as an Abstraction of $pr\mathrm{ACP}_\mathrm{I}^-$

In this section we demonstrate that $\mathrm{ACP}_I^-(A)$ can be considered an abstraction of $pr\mathrm{ACP}_I^-(A)$ at both the level of the graph model and at the level of the equational theory. For the former, we exhibit a homomorphism $\phi$ from probabilistic process graphs to nonprobabilistic process graphs that preserves the structure of the bisimulation congruence classes. For the latter, we exhibit a homomorphism $\Phi$ from $pr\mathrm{ACP}_I^-(A)$ terms to $\mathrm{ACP}_I^-(A)$ terms that preserves the validity of equational reasoning.

**Definition 4.1** *Let $g = \langle V, r, \mu \rangle$ be a probabilistic process graph. Then $\phi(g) = \langle V, r, \longrightarrow \rangle$ has the same states and start state as $g$ and $\longrightarrow$ is such that*

$$v_1 \xrightarrow{a} v_2 \iff \mu(v_1, a, v_2) > 0$$

**Proposition 4.1** *Let $g_1$, $g_2$ be probabilistic process graphs.*

$$\begin{aligned}
&\phi(a) = a, a \in A_\delta \\
&\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2) \\
&\phi(g_1 +_p g_2) = \phi(g_1) + \phi(g_2) \\
&\phi(g_1 |_{r,s} g_2) = \phi(g_1) \mid \phi(g_2) \\
&\phi(g_1 \|_{r,s} g_2) = \phi(g_1) \parallel \phi(g_2) \\
&\phi(g_1 \mathbin{\|\!\!\lfloor}_{r,s} g_2) = \phi(g_1) \mathbin{\|\!\!\lfloor} \phi(g_2) \\
&\phi(\partial_H(g_1)) = \partial_H(\phi(g_1))
\end{aligned}$$

**Proposition 4.2** *The homomorphism $\phi$ preserves the structure of the bisimulation congruence classes. That is,*

$$g_1 \leftrightarrows^{pr}_{\delta} g_2 \implies \phi(g_1) \leftrightarrows_{\delta} \phi(g_2)$$

The converse of this result is clearly not true, e.g., $a + b \leftrightarrows_{\delta} b + a$ but $a +_{\frac{1}{2}} b \not\leftrightarrows^{pr}_{\delta} b +_{\frac{1}{3}} a$. Thus, the graph model $\mathcal{G}/\leftrightarrows_{\delta}$ of $\mathrm{ACP}^{-}_{I}(A)$ is strictly more abstract than the probabilistic graph model $pr\mathcal{G}/\leftrightarrows^{pr}_{\delta}$ of $pr\mathrm{ACP}^{-}_{I}(A)$.

The homomorphism $\Phi : \mathcal{L}(pr\mathrm{ACP}^{-}_{I}(A)) \longrightarrow \mathcal{L}(\mathrm{ACP}^{-}_{I}(A))$ from $pr\mathrm{ACP}^{-}_{I}(A)$ terms to $\mathrm{ACP}^{-}_{I}(A)$ terms is defined as follows:

$$
\begin{aligned}
&\Phi(a) = a, a \in A_{\delta}\\
&\Phi(x) = x\\
&\Phi(x \cdot y) = \Phi(x) \cdot \Phi(y)\\
&\Phi(x +_p y) = \Phi(x) + \Phi(y)\\
&\Phi(x \mid_{r,s} y) = \Phi(x) \mid \Phi(y)\\
&\Phi(x \parallel_{r,s} y) = \Phi(x) \parallel \Phi(y)\\
&\Phi(x ⌊\!⌊_{r,s} y) = \Phi(x) ⌊\!⌊ \Phi(y)\\
&\Phi(\partial_H(x)) = \partial_H(\Phi(x))
\end{aligned}
$$

The following proposition states that any valid proof of $pr\mathrm{ACP}^{-}_{I}(A)$ can be mapped into a valid proof of $\mathrm{ACP}^{-}_{I}(A)$ using the homomorphism $\Phi$.

**Proposition 4.3** *Let $t_1$, $t_2$ be terms of $pr\mathrm{ACP}^{-}_{I}(A)$, i.e., $t_1, t_2 \in \mathcal{L}(pr\mathrm{ACP}^{-}_{I}(A))$.*

$$\frac{pr\mathrm{ACP}^{-}_{I}(A) \vdash t_1 = t_2}{\mathrm{ACP}^{-}_{I}(A) \vdash \Phi(t_1) = \Phi(t_2)}$$

**Proof sketch:** The proof is by induction on the length of the $pr\mathrm{ACP}^{-}_{I}(A)$ proof, using the observation that, for every $pr\mathrm{ACP}^{-}_{I}(A)$ axiom of the form $c \implies t_1 = t_2$, its homomorphic image $\Phi(c) \implies \Phi(t_1) = \Phi(t_2)$ is an $\mathrm{ACP}^{-}_{I}(A)$ axiom. Here $c$ is a possibly empty condition on the validity of the $pr\mathrm{ACP}^{-}_{I}(A)$ axiom, and the fact that $\Phi(c)$ is equal to the condition of the corresponding $\mathrm{ACP}^{-}_{I}(A)$ axiom means that no axiom of $pr\mathrm{ACP}^{-}_{I}(A)$ is conditional on a probability appearing within an $pr\mathrm{ACP}^{-}_{I}(A)$ term. □

Note that the converse of the result does not hold, e.g., $a + b = b + a$ but $a +_{\frac{1}{2}} b \neq b +_{\frac{1}{3}} a$. Thus, $\mathrm{ACP}^{-}_{I}(A)$ is a strictly more abstract theory than $pr\mathrm{ACP}^{-}_{I}(A)$.

## 5 Conclusions

In this paper, we have presented complete axiomatizations of probabilistic processes within the context of the process algebra ACP. Given that axiom A6 of ACP ($x + \delta = x$) does not have a plausible interpretation in the generative model of probabilistic computation, we introduced the somewhat weaker theory $\mathrm{ACP}^{-}_{I}$, in which $A6$ is rejected. $\mathrm{ACP}^{-}_{I}$ is, in essence, a minor alteration of ACP expressing almost the same process identities on finite processes.

Our end-result is the axiom system $pr\mathrm{ACP}^{-}_{I}$, which can be seen as a probabilistic extension of $\mathrm{ACP}^{-}_{I}$ for generative probabilistic processes. In particular, $\mathrm{ACP}^{-}_{I}$ is homomorphically derivable from $pr\mathrm{ACP}^{-}_{I}$. As desired, we showed that $pr\mathrm{ACP}^{-}_{I}$ constitutes a complete axiomatization of Larsen and Skou's probabilistic bisimulation for finite processes.

Several directions for future work can be identified. First, we are interested in adding certain important features to the model, such as recursion and unobservable $\tau$ actions. Secondly, we desire also to completely axiomatize the *reactive* and *stratified* models of probabilistic processes [vGSST90]. In the stratified model, which is well-suited for reasoning about probabilistic "fair" scheduling, distinctions are made between processes based on the branching structure of their purely probabilistic choices. We conjecture that by eliminating axiom *pr*A2 (probabilistic alternative composition is not associative in the stratified model!) and slightly modifying *pr*D3.2, the desired axiomatization can be obtained.

## Acknowledgements

The authors gratefully acknowledge Rob van Glabbeek, Chi-Chiang Jou, and Bernhard Steffen for valuable discussions.

## References

[BBS92] J. C. M. Baeten, J. A. Bergstra, and S. A. Smolka. *Axiomatizing Probabilistic Processes: ACP with Generative Probabilities.* Technical Report, Dept. of Math and Computing Science, Technical University of Eindhoven, Eindhoven, The Netherlands, 1992.

[BK84] J. A. Bergstra and J. W. Klop. Process algebra for synchronous communication. *Information and Computation*, 60:109–137, 1984.

[BM89] B. Bloom and A. R. Meyer. A remark on bisimulation between probabilistic processes. In Meyer and Tsailin, editors, *Logik at Botik*, Springer-Verlag, 1989.

[BW90] J. C. M. Baeten and W. P. Weijland. *Process Algebra. Cambridge Tracts in Computer Science 18*, Cambridge University Press, 1990.

[Chr90] I. Christoff. *Testing Equivalences for Probabilistic Processes.* Technical Report DoCS 90/22, Ph.D. Thesis, Department of Computer Science, Uppsala University, Uppsala, Sweden, 1990.

[CSZ92] R. Cleaveland, S. A. Smolka, and A. E. Zwarico. Testing preorders for probabilistic processes. In *Proceedings of the 19th ICALP*, July 1992.

[GJS90] A. Giacalone, C.-C. Jou, and S. A. Smolka. Algebraic reasoning for probabilistic concurrent systems. In *Proceedings of Working Conference on Programming Concepts and Methods*, IFIP TC 2, Sea of Gallilee, Israel, April 1990.

[JL91] B. Jonsson and K. G. Larsen. Specification and refinement of probabilistic processes. In *Proceedings of the 6th IEEE Symposium on Logic in Computer Science*, Amsterdam, July 1991.

[JS90] C.-C. Jou and S. A. Smolka. Equivalences, congruences, and complete axiomatizations for probabilistic processes. In J. C. M. Baeten and J. W. Klop, editors, *Proceedings of CONCUR '90*, pages 367–383, Springer-Verlag, Berlin, 1990.

[LS89] K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. In *Proceedings of 16th Annual ACM Symposium on Principles of Programming Languages*, 1989.

[LS92] K. G. Larsen and A. Skou. Compositional verification of probabilistic processes. In *Proceedings of CONCUR '92*, Springer-Verlag Lecture Notes in Computer Science, 1992.

[Mil80] R. Milner. *A Calculus of Communicating Systems.* Volume 92 of *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, 1980.

[Tof90] C. M. N. Tofts. A synchronous calculus of relative frequency. In J. C. M. Baeten and J. W. Klop, editors, *Proceedings of CONCUR '90*, pages 467–480, Springer-Verlag, Berlin, 1990.

[vGSST90] R. J. van Glabbeek, S. A. Smolka, B. Steffen, and C. M. N. Tofts. Reactive, generative, and stratified models of probabilistic processes. In *Proceedings of the 5th IEEE Symposium on Logic in Computer Science*, pages 130–141, Philadelphia, PA, 1990.