INFORMATION AND COMPUTATION 121, 234–255 (1995)

Axiomatizing Probabilistic Processes: ACP with Generative Probabilities*

J. C. M. BAETEN

Department of Mathematics 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, and Department of Philosophy, University of Utrecht, P.O. Box 80106, 3508 TC Utrecht, The Netherlands

AND

S. A. SMOLKA

Department of Computer Science, State University of New York at Stony Brook, Stony Brook, New York 11794-4400

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 endresult the axiom system *pr* ACP_I^-, a version of ACP whose main innovation is a probabilistic asynchronous interleaving operator. 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 ACP_I^-. The main difference between ACP and 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 ACP_I^-. We argue that this does not affect the usefulness of ACP_I^- in practice, and show how ACP can be reconstructed from ACP_I^- with a minimal amount of technical machinery. *pr* ACP_I^- is obtained from ACP_I^- through the introduction of probabilistic alternative and parallel composition operators, and a process graph model for *pr* ACP_I^- based on *probabilistic bisimulation* is developed. We show that *pr* ACP_I^- is a sound and complete axiomatization of probabilistic bisimulation for finite processes, and that *pr* ACP_I^- can be homomorphically embedded in ACP_I^- as desired. Our results for ACP_I^- and *pr* ACP_I^- are presented in a modular fashion by first considering several subsets of the signatures. We conclude with a discussion about adding an iteration operator to *pr* ACP_I^-.

1. INTRODUCTION

Real-life systems often exhibit behavior that is probabilistic or statistical in nature. For example, one may observe that a faulty communication link drops a message 2% of the time or that a site in a network is down with probability π. It is therefore 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 asynchronous, communicating systems. 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 δ, which plays the role of *NIL* from CCS [Mil80] (CCS is a predecessor of ACP). The key axioms for δ go by the names A6 and A7:

$$x+\delta=x \tag{A6}$$

$$\delta\cdot x=\delta. \tag{A7}$$

The process δ represents an unfeasible option, i.e., a task that cannot be performed and therfore 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 δ 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 first

* A preliminary version of this paper appeared in "Proceedings of CONCUR '92—Third International Conference on Concurrency Theory," Lecture Notes in Computer Science, Vol. 630, pp. 472–485, Springer-Verlag, Berlin/New York, 1992. The research of the first and second authors was supported by ESPRIT Basic Research Action 7166, CONCUR2. The second author was also supported by ESPRIT Basic Research Action 6454, CONFER. The research of the third author was supported in part by NSF Grants CCR-8704309, CCR-9120995, and CCR-9208585 and AFOSR Grant F49620-93-1-0250.

0890-5401/95 $12.00

develop a weaker version of ACP called 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) ACP_I^- does not imply $x + \delta = x$. In fact, this axiom has often been criticized as being nonobvious for the interpretation δ = deadlock = inaction.

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

(iii) ACP_I^- has for many 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 ACP_I^-.

(iv) 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 ACP_I^- by replacing the operators for alternative and parallel composition with probabilistic counterparts to obtain the axiom system *pr* ACP_I^-. The main innovation of *pr* ACP_I^- can then be seen as a probabilistic asynchronous interleaving operator. Probabilistic choice in *pr* 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 [LS92a, vGSST90], a separate distribution is associated with each action, and choices involving different actions are resolved by the environment.

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 accepted 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 [LS92a, GJS90, vGSST90, Chr90, BM89, JL91, CSZ92] has been primarily of an operational/behavioral nature. For *synchronously composed* probabilistic processes, however, various axiomatizations have been proposed. These include [GJS90, JS90, Tof90] for generative processes and [LS92b] for reactive processes. To our knowledge, *pr* ACP_I^- represents the first axiomatization of asynchronous processes to appear in the literature.

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 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 and left-merge operator to obtain PA. Finally, a communication merge operator, the constant δ, and an auxiliary *initials* operator I are added to PA to obtain 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, i.e., recursion-free processes.

- We show in a technical sense how ACP can be reconstructed from ACP_I^- through the reintroduction of the axiom (A6).

- The axiom systems *pr* BPA, *pr* PA, and *pr* 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 [LS92a] 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 ACP_I^- and its probabilistic counterpart are then explored. We show that ACP_I^- is the homomorphic image of *pr* 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* ACP_I^- is a valid proof in ACP_I^-.

The structure of the rest of this paper is as follows. Section 2 presents the equational specifications BPA, PA, and ACP_I^-, and their accompanying process graph models and completeness results. Section 3 treats the probabilistic versions of these axiom systems, namely, *pr* BPA, *pr* PA, and *pr* ACP_I^-. The homomorphic derivability of ACP_I^- from *pr* ACP_I^- is the subject of Section 4. Section 5 contains our conclusions including a discussion on adding an iteration operator to *pr* ACP_I^-. Note that we do not treat internal or τ-moves in this paper, so we stay within the setting of concrete process algebra.

2. A WEAKER VERSION OF ACP

In this section we present the equational theory 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 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 ACP_I^-.

As is the practice in ACP, we begin with the theory BPA (Basic Process Algebra) which describes processes constructed from constants, plus, and sequential composition.

We will then add to BPA a notion of parallel composition (merge and left-merge) to obtain PA (Process Algebra). Finally, the theory ACP_I^- is derived by extending BPA with the constant δ (for deadlock), a combined notion of parallel composition and communication, and a restriction operator.

2.1. BPA

2.1.1. *Equational Specification*

The signature $\Sigma(\mathrm{BPA}(A))$ consists of one sort $\mathbf{P}$ (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:

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

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

$$x + y = y + x \qquad \text{(A1)}$$

$$(x + y) + z = x + (y + z) \qquad \text{(A2)}$$

$$x + x = x \qquad \text{(A3)}$$

$$(x + y) \cdot z = x \cdot z + y \cdot z \qquad \text{(A4)}$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z). \qquad \text{(A5)}$$

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

2.1.2. *Graph Model*

We define a process graph model for $\mathrm{BPA}(A)$. The underlying notion of equivalence for process graphs is bisimulation, and we prove completeness of $\mathrm{BPA}(A)$ in this model. We will later extend our graph model to $\mathrm{PA}(A)$ and $\mathrm{ACP}_I^-(A)$. As before, let A be the set of atomic actions and now let N be a countably infinite set. We consider process graphs with labels from A and nodes from N.

DEFINITION 2.1. A *process graph* g is a triple $\langle V, r, \rightarrow \rangle$ such that

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

The *endpoints* of g are those nodes devoid of outgoing transitions representing successful termination. The major role played by endpoints is in the definition, given below, of the sequential composition of two process graphs. We often write $v \xrightarrow{a} v'$ to denote the fact that $(v, a, v') \in \rightarrow$. We denote by $\mathscr{PG}(A, N)$ the class of all process graphs over A and N. Bisimulation, due to Milner and Park [Mil80, Par81], is the primary equivalence relation we consider on such process graphs.

DEFINITION 2.2. Let $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$, $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$ be two process graphs. A *bisimulation* between g_1 and g_2 is a relation $\mathscr{R} \subseteq (V_1 \cup V_2) \times (V_1 \cup V_2)$ with the following properties:

- $\mathscr{R}(r_1, r_2)$
- $\forall v \in V_1, w \in V_2$ with $\mathscr{R}(v, w)$:

$$\forall a \in A \text{ and } v' \in V_1, \quad \text{if } v \xrightarrow{a}_1 v' \quad \text{then} \quad \exists w' \in V_2 \text{ with } \mathscr{R}(v', w') \text{ and } w \xrightarrow{a}_2 w'$$

- and *vice versa* with the roles of v and w reversed.

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

In the remainder of this paper, we will use a particular subset of $\mathscr{PG}(A, N)$, namely $\mathscr{APG}(A, N)$, the class of acyclic process graphs over A and N, the roots of which are nonendpoints. The restriction to $\mathscr{APG}(A, n)$ is motivated as follows: (i) process graphs are assumed to be acyclic in order to avoid "root unwinding" (see, e.g., [BW90]); and (ii) roots are assumed to be nonendpoints to avoid the presence of the empty process which complicates the equational theory. Both conditions only serve to simplify the presentation and are not essential.

To construct a graph model for $\mathrm{BPA}(A)$, it is convenient to work with isomorphism classes of $\mathscr{APG}(A, N)$ process graphs. Let $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$, $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$ be process graphs. We say that g_1 is *isomorphic* to g_2, written $g_1 \cong g_2$, if there exists a bijection $\psi: V_1 \rightarrow V_2$ such that $\psi(r_1) = \psi(r_2)$ and $(v, a, v') \in \rightarrow_1 \Leftrightarrow (\psi(v), a, \psi(v')) \in \rightarrow_2$. $\mathscr{PG}(A, N)/\cong$ thus denotes the set of *all* isomorphism classes of process graphs over A and N. Note that the properties of being acyclic and having a nonendpoint root are preserved under isomorphisms.

In Definitions 2.3 and 2.4, we assume that for elements G_1 and G_2 of $\mathscr{APG}(A, N)/\cong$, we can find representatives $g_1 \in G_1$ and $g_2 \in G_2$ such that g_1 and g_2 are node-disjoint. Our assumption is easily justified since we are working with isomorphism classes of $\mathscr{APG}(A, N)$.

DEFINITION 2.3. Let $G_1, G_2 \in \mathscr{APG}(A, N)/\cong$ and let $g_1 \in G_1$ and $g_2 \in G_2$ be representatives such that $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$, $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$, $V_1 \cap V_2 = \varnothing$, and $N - (V_1 \cup V_2)$ is infinite. The operators $a \in A$, $+$, and $\cdot$ are defined on $\mathscr{APG}(A, N)/\cong$ as follows:

$a \in A$: A representative process graph for a is $\langle \{r, v\}, r, \{\langle r, a, v \rangle\} \rangle$ with $r, v \in N$, $r \neq v$.

$G_1 + G_2$: A representative is $\langle (V_1 \cup V_2 \cup \{r\} - \{r_1, r_2\}), r, \rightarrow \rangle$ with $r \in N - (V_1 \cup V_2)$ and $v \xrightarrow{a} v'$ if at least one of the following holds:

- $v = r$ and $r_1 \xrightarrow{a}_1 v'$
- $v = r$ and $r_2 \xrightarrow{a}_2 v'$
- $v \xrightarrow{a}_1 v'$ and $v \neq r_1$
- $v \xrightarrow{a}_2 v'$ and $v \neq r_2$

$G_1 \cdot G_2$: A representative is $\langle (V_1 \cup V_2 - \{r_2\}), r_1, \rightarrow \rangle$ with $v \xrightarrow{a} v'$ if at least one of the following holds:

- $v \xrightarrow{a}_1 v'$ $(v, v' \in V_1)$
- $v \in V_1$, endpoint(v), and $r_2 \xrightarrow{a}_2 v'$
- $v \in V_2$, $v \neq r_2$, and $v \xrightarrow{a}_2 v'$

For $G_1, G_2 \in \mathscr{APG}(A, N)/\cong$, we define $G_1 \leftrightarrows G_2$ if for some $g_1 \in G_1$, $g_2 \in G_2$, $g_1 \leftrightarrows g_2$. Notice that $\cong \subseteq \leftrightarrows$, and it follows that we may identify $(\mathscr{APG}(A, N)/\cong)/\leftrightarrows$ with $\mathscr{APG}(A, N)/\leftrightarrows$.

For t a closed BPA(A) term, we write $Graph(t) = [\langle V_t, r_t, \rightarrow_t \rangle]_{\cong}$ to denote the isomorphism class of the process graphs obtained inductively on t using Definition 2.3. We take the liberty of writing expressions like $t \leftrightarrows t'$, instead of the more precise $Graph(t) \leftrightarrows Graph(t')$, when this is clear from the context. The definition of $Graph(t)$ and the just-mentioned notational liberty extend in the obvious way to the axiom systems PA(A) and $\mathrm{ACP}_I^-(A)$, to be considered later in this section.

In the setting of BPA(A), $\leftrightarrows$ is a congruence (see, e.g., [BW90]).

PROPOSITION 2.1. *If* $G_1 \leftrightarrows G_2$, *then* $G + G_1 \leftrightarrows G + G_2$, $G \cdot G_1 \leftrightarrows G \cdot G_2$, *and* $G_1 \cdot G \leftrightarrows G_2 \cdot G$.

We have that $\mathscr{APG}(A, N)/\leftrightarrows$, the *graph model*, is indeed a model of the axiom system BPA(A), and that BPA(A) constitutes a complete axiomatization of process equivalence in $\mathscr{APG}(A, N)/\leftrightarrows$.

THEOREM 2.1 [BW90].

1. $\mathscr{APG}(A, N)/\leftrightarrows \models \mathrm{BPA}(A)$
2. *For all closed expressions p, q over* $\Sigma(\mathrm{BPA}(A))$:

$$\mathscr{APG}(A, N)/\leftrightarrows \models p = q \Rightarrow \mathrm{BPA}(A) \vdash p = q.$$

2.2. PA

2.2.1. *Equational Specification*

The signature $\Sigma(\mathrm{PA}(A))$ is obtained from $\Sigma(\mathrm{BPA}(A))$ by adding an interleaving *merge* operator $\parallel$ and a *left-merge* operator $\lfloor\!\lfloor$:

$$\Sigma(\mathrm{PA}(A)) = \Sigma(\mathrm{BPA}(A)) \cup \{\parallel : \mathbf{P} \times \mathbf{P} \rightarrow \mathbf{P}\} \cup \{\lfloor\!\lfloor : \mathbf{P} \times \mathbf{P} \rightarrow \mathbf{P}\}.$$

Intuitively, the process $x \parallel y$ is obtained by interleaving (shuffling) the atomic actions of x and y together. Left-merge is an auxiliary operator in that it permits $\parallel$ to be specified in finitely many equations. The process $x \lfloor\!\lfloor y$ has the same meaning as $x \parallel y$, but with the restriction that the first step must come from x.

The axiom system PA(A) is given by

$$\mathrm{BPA}(A)$$
$$+$$
$$x \parallel y = x \lfloor\!\lfloor y + y \lfloor\!\lfloor x \qquad \text{(M1)}$$
$$a \lfloor\!\lfloor x = a \cdot x \qquad \text{(M2)}$$
$$(a \cdot x) \lfloor\!\lfloor y = a \cdot (x \parallel y) \qquad \text{(M3)}$$
$$(x + y) \lfloor\!\lfloor z = x \lfloor\!\lfloor z + y \lfloor\!\lfloor z. \qquad \text{(M4)}$$

2.2.2. *Graph Model*

In order to define a graph model for the two new operators of PA(A), let $\rightleftharpoons : N \times N \rightarrow N$ be an injective pairing function. For $V, W \subseteq N$, we use $V \times W$ to denote the set $\{v \rightleftharpoons w \mid v \in V, w \in W\}$ and we often write the more familiar (v, w) in place of $v \rightleftharpoons w$.

DEFINITION 2.4. Let $G_1, G_2 \in \mathscr{APG}(A, N)/\cong$ and let $g_1 \in G_1$ and $g_2 \in G_2$ be representatives such that $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$, $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$, $V_1 \cap V_2 = \emptyset$, and $N - (V_1 \cup V_2)$ is infinite. The operators $\parallel$ and $\lfloor\!\lfloor$ are defined on $\mathscr{APG}(A, N)/\cong$ as follows:

$G_1 \parallel G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \rightarrow \rangle$ where $(v_1, v_2) \xrightarrow{a} (v_1', v_2')$ if either of the following holds:

- $v_1 \xrightarrow{a}_1 v_1'$ and $v_2 = v_2'$
- $v_2 \xrightarrow{a}_2 v_2'$ and $v_1 = v_1'$

$G_1 \lfloor\!\lfloor G_2$: As $G_1 \parallel G_2$ but without transitions of the form $(r_1, r_2) \xrightarrow{a} (r_1, v)$.

Again one may notice that $\leftrightarrows$ is a congruence, $\mathscr{APG}(A, N)/\leftrightarrows \models \mathrm{PA}(A)$ and that PA(A) constitutes a complete axiomatization of process equivalence in $\mathscr{APG}(A, N)/\leftrightarrows$ [BW90].

2.3. ACP without A6

2.3.1. *Equational Specification*

The equational system $\mathrm{ACP}_I^-(A)$ treats the operators of BPA(A) as well as the new constant δ representing deadlock; a *communication merge* operator $\mid$ describing the result of a communication between any two atomic actions; a *merge* operator $\parallel$ and *left-merge* operator $\lfloor\!\lfloor$ like those of PA(A) but which additionally admit the possibility of communication; and a family of restriction operators ∂_H, $H \subseteq A$.

We will also need an auxiliary operator I that defines the initial actions that a process can perform.

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

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

It is convenient to define communication merge as the extension of a binary commutative and associative function on atomic actions (i.e., $| : A_\delta \times A_\delta \to A_\delta$) with δ acting as a multiplicative zero. This is accomplished with axioms (C1–3) below. We will later refer to the restriction of | to $A_\delta \times A_\delta$ as $\bar{\gamma}$. We further require |, restricted to $A_\delta \times A_\delta$, to be total and this is expressed by the following axiom:

$$\forall a, b \in \mathbf{P}\ \overline{A_\delta}(a) \wedge \overline{A_\delta}(b) \Rightarrow \overline{A_\delta}(a \mid b). \qquad \text{(C0)}$$

Here, $\overline{A_\delta}$ is the characteristic predicate of A_δ:

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

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

$$\mathrm{BPA}(A)$$
$$+$$
$$\delta \cdot x = \delta \qquad \text{(A7)}$$
$$+$$
$$\text{(C0)}$$
$$+$$
$$a \mid b = b \mid a \qquad \text{(C1)}$$
$$(a \mid b) \mid c = a \mid (b \mid c) \qquad \text{(C2)}$$
$$\delta \mid a = \delta \qquad \text{(C3)}$$
$$+$$
$$x \parallel y = x \mathbin{\|\!\_} y + y \mathbin{\|\!\_} x + x \mid y \qquad \text{(CM1)}$$
$$a \mathbin{\|\!\_} x = a \cdot x \qquad \text{(CM2)}$$
$$(a \cdot x) \mathbin{\|\!\_} y = a \cdot (x \parallel y) \qquad \text{(CM3)}$$
$$(x + y) \mathbin{\|\!\_} z = (x \mathbin{\|\!\_} z) + (y \mathbin{\|\!\_} z) \qquad \text{(CM4)}$$
$$a \mid (b \cdot x) = (a \mid b) \cdot x \qquad \text{(CM5)}$$
$$(a \cdot x) \mid b = (a \mid b) \cdot x \qquad \text{(CM6)}$$
$$(a \cdot x) \mid (b \cdot y) = (a \mid b) \cdot (x \parallel y) \qquad \text{(CM7)}$$
$$(x + y) \mid z = x \mid z + y \mid z \qquad \text{(CM8)}$$
$$x \mid (y + z) = x \mid y + x \mid z \qquad \text{(CM9)}$$
$$+$$
$$I(a) = \{a\} \qquad \text{(I1)}$$
$$I(x \cdot y) = I(x) \qquad \text{(I2)}$$
$$I(x + y) = I(x) \cup I(y) \qquad \text{(I3)}$$
$$+$$
$$a \in H \Rightarrow \partial_H(a) = \delta \qquad \text{(D1)}$$
$$a \notin H \Rightarrow \partial_H(a) = a \qquad \text{(D2)}$$
$$I(x) \subseteq H_\delta \Rightarrow \partial_H(x + y) = \partial_H(y) \qquad \text{(D3.1)}$$
$$I(x + y) \cap H_\delta = \varnothing \Rightarrow$$
$$\partial_H(x + y) = \partial_H(x) + \partial_H(y) \qquad \text{(D3.2)}$$
$$\partial_H(x \cdot y) = \partial_H(x) \cdot \partial_H(y). \qquad \text{(D4)}$$

Comments: $\mathrm{ACP}_I^-(A)$ differs from ACP by the absence of (A6) and the presence of (D3.1–2) instead of axiom (D3): $\partial_H(x + y) = \partial_H(x) + \partial_H(y)$. The following examples illustrate the new axiom system and, in particular, the last two examples illustrate why (D3) is no longer sound.

$\partial_{\{c\}}(a + (b + c))$	$= \partial_{\{c\}}(c + (a + b))$	(by (A1) and (A2))
	$= \partial_{\{c\}}(a + b)$	(by (D3.1))
	$= \partial_{\{c\}}(a) + \partial_{\{c\}}(b)$	(by (D3.2))
	$= a + b$	(by (D2) twice)
$\delta_{\{a\}}(a + \delta)$	$= \partial_{\{a\}}(\delta + a)$	(by (A1))
	$= \partial_{\{a\}}(a)$	(by (D3.1))
	$= \delta$	(by (D1))
$\partial_{\{a\}}(a + \delta)$	$= \partial_{\{a\}}(\delta)$	(by (D3.1))
	$= \delta$	(by (D2))
$\partial_\varnothing(a + \delta)$	$= \partial_\varnothing(\delta + a)$	(by (A1))
	$= \partial_\varnothing(a)$	(by (D3.1))
	$= a$	(by (D2))
$\partial_\varnothing(a) + \partial_\varnothing(\delta)$	$= a + \delta$	(by (D2) twice)

Axiom (C0) expresses that, for $a, b \in A_\delta$, $a \mid b \in A_\delta$. We view the restriction of | to $A_\delta \times A_\delta$ as a parameter of our graph model construction. For this purpose, we assume a partial mapping $\gamma : A \times A \to A$ which is commutative and associative. We extend γ to a total mapping $\bar{\gamma}$ over $A_\delta \times A_\delta$ as follows:

$$\bar{\gamma}(\delta, a), \bar{\gamma}(a, \delta), \bar{\gamma}(\delta, \delta) = \delta$$

$$\bar{\gamma}(a, b) = \begin{cases} \gamma(a, b) & \text{if } \gamma(a, b) \text{ defined} \\ \delta & \text{otherwise.} \end{cases}$$

Without loss of generality, γ, and thus $\bar{\gamma}$, will be fixed for the remainder of Section 2. In order to incorporate γ into the framework of $\mathrm{ACP}_I^-(A)$, we introduce the following set of axioms:

$$\mathrm{AX}(\gamma) = \{a \mid b = c : a \in A, b \in A, \gamma(a, b) = c\}$$
$$\cup \{a \mid b = \delta : a \in A, b \in A, \gamma(a, b) \text{ undefined}\}.$$

2.3.2. *Graph Model for* $\mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma)$

Our graph model for $\mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma)$ uses labels from $A_\delta = A \cup \{\delta\}$ and is additionally parameterized by γ. We will thus be working with $\mathscr{PG}(A_\delta, N, \gamma)$, $\mathscr{PG}(A_\delta, N, \gamma)/\cong$, $\mathscr{APG}(A_\delta, N, \gamma)$, and $\mathscr{APG}(A_\delta, N, \gamma)/\cong$.

Let $\mathrm{initials}(v) \subseteq A_\delta$ be the set of actions $\{a \in A_\delta \mid \exists v' \xrightarrow{a} v'\}$ v for v a process graph node. The operators of $\mathrm{ACP}_I^-(A)$, beyond those of $\mathrm{BPA}(A)$, are now defined on $\mathscr{APG}(A_\delta, N, \gamma)/\cong$.

DEFINITION 2.5. Let $G_1, G_2 \in \mathscr{APG}(A_\delta, N, \gamma)/\cong$ and let $g_1 \in G_1$ and $g_2 \in G_2$ be representatives such that $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$, $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$, $V_1 \cap V_2 = \varnothing$, and $N - (V_1 \cup V_2)$ is infinite. The $\mathrm{ACP}_I^-(A)$ operators δ, $\|$, $\lfloor\!\lfloor$, $|$, ∂_H (for $H \subseteq A$), and I are defined on $\mathscr{APG}(A_\delta, N, \gamma)/\cong$ as follows:

δ: A representative for δ is $\langle \{r, v\}, r, \{\langle r, \delta, v \rangle\} \rangle$ with $r, v \in N$, $r \neq v$.

$G_1 \| G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \rightarrow \rangle$ where $(v_1, v_2) \xrightarrow{a} (v_1', v_2')$ if at least one of the following holds:

- $v_1 \xrightarrow{a}_1 v_1'$ and $v_2 = v_2'$
- $v_2 \xrightarrow{a}_2 v_2'$ and $v_1 = v_1'$
- $v_1 \xrightarrow{b}_1 v_1'$, $v_2 \xrightarrow{c}_2 v_2'$, and $a = \bar{\gamma}(b, c)$ (for some b and c)

$G_1 \lfloor\!\lfloor G_2$: As $G_1 \| G_2$ but without transitions of the form $(r_1, r_2) \xrightarrow{a} (r_1, v)$.

$G_1 \mid G_2$: As $G_1 \| G_2$ but without transitions of the form $(r_1, r_2) \xrightarrow{a} (v, r_2)$ or $(r_1, r_2) \xrightarrow{a} (r_1, v)$.

$\partial_H(G_1)$: A representative is $\langle V_1, r_1, \rightarrow \rangle$ where

$$\rightarrow = \{(v, a, v') \in \rightarrow_1 \mid a \notin H_\delta\}$$
$$\cup \{(v, \delta, v') \mid (v, a, v') \in \rightarrow_1 \text{ and initials}(v) \subseteq H_\delta\}$$

$I(G_1)$: gives the set of actions $\mathrm{initials}(r_1)$.

Our algebra of process graphs is standard (see, e.g., [BW90]) with the exception of restriction. This operator removes all edges labeled with actions from the set of restricted actions H. It also removes δ-edges, which it must do to ensure the soundness of D3.1. In case a node in g_1 qualifies to have all its edges removed, then these edges are not removed but rather renamed into δ-transitions.

The presence of δ-transitions, which represent the capability for a process to deadlock, requires a new definition of bisimulation in which a weaker condition is imposed on δ-transitions.

DEFINITION 2.6. Let $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$, $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$ be two process graphs. A *δ-bisimulation* between g_1 and g_2 is a relation $\mathscr{R} \subseteq (V_1 \cup V_2) \times (V_1 \cup V_2)$ with the following properties:

- $\mathscr{R}(r_1, r_2)$
- $\forall v \in V_1$, $w \in V_2$ with $\mathscr{R}(v, w)$:
  - $\forall a \in A$ and $v' \in V_1$, if $v \xrightarrow{a}_1 v'$ then $\exists w' \in V_2$ with $\mathscr{R}(v', w')$ and $w \xrightarrow{a}_2 w'$
  - 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.

Graphs g_1 and g_2 are *δ-bisimilar*, written $g_1 \leftrightarrows_\delta g_2$, if there exists a δ-bisimulation between g_1 and g_2. For elements G_1 and G_2 of $\mathscr{APG}(A_\delta, N, \gamma)/\cong$, we write $G_1 \leftrightarrows_\delta G_2$ if for some $g_1 \in G_1$, $g_2 \in G_2$, we have $g_1 \leftrightarrows_\delta g_2$.

This definition is the same as Definition 2.2 with the additional stipulation that for two nodes v, w related by a δ-bisimulation, v possesses a δ-edge iff w does. We once again have that $\leftrightarrows_\delta$ is a congruence.

PROPOSITION 2.2. *If* $G_1 \leftrightarrows_\delta G_2$, *then* $G \| G_1 \leftrightarrows_\delta G \| G_2$, $G \lfloor\!\lfloor G_1 \leftrightarrows_\delta G \lfloor\!\lfloor G_2$, $G_1 \lfloor\!\lfloor G \leftrightarrows_\delta G_2 \lfloor\!\lfloor G$, $G \mid G_1 \leftrightarrows_\delta G \mid G_2$ *and* $\partial_H(G_1) \leftrightarrows_\delta \partial_H(G_2)$, *for all* $H \subseteq A$.

Proof. The proof for all operators, except ∂_H, follows the standard arguments of ACP (see, e.g., [BW90]). For ∂_H, $H \subseteq A$, the proof proceeds as follows. Suppose $G_1 \leftrightarrows_\delta G_2$ and let $g_1 = \langle V_1, r_1, \rightarrow_1 \rangle$ be a representative of G_1 and $g_2 = \langle V_2, r_2, \rightarrow_2 \rangle$ be a representative of G_2. Now let $\mathscr{R} \subseteq (V_1 \cup V_2) \times (V_1 \cup V_2)$ be a δ-bisimulation between g_1 and g_2. We show that $\mathscr{R}$ is also a δ-bisimulation between $\partial_H(g_1)$ and $\partial_H(g_2)$, $H \subseteq A$.

Let $(v_1, v_2) \in \mathscr{R}$, with $v_1 \in V_1$, $v_2 \in V_2$. There are three cases to consider:

$\mathrm{initials}(v_1) \not\subseteq H_\delta$: Then in $\partial_H(g_1)$ the transitions of v_1 are of the form $v_1 \xrightarrow{a}_1 v_1'$ with $a \notin H_\delta$. Since $g_1 \leftrightarrows_\delta g_2$, in $\partial_H(g_2)$ there exists a v_2' with $\mathscr{R}(v_1', v_2')$ and $v_2 \xrightarrow{a}_2 v_2'$.

$\mathrm{initials}(v_1) \neq \varnothing \subseteq H_\delta$: Then in $\partial_H(g_1)$ all transitions of v_1 are of the form $v_1 \xrightarrow{\delta}_1 v_1'$. Since $g_1 \leftrightarrows_\delta g_2$, in $\partial_H(g_2)$ all transitions of v_2 are likewise of the form $v_2 \xrightarrow{\delta}_2 v_2'$. By the weaker condition on δ-transitions in a δ-bisimulation, this is enough.

initials$(v_1) = \varnothing$: Then initials$(v_1) = \varnothing$ in $\partial_H(g_1)$ and, since $g_1 \leftrightarrows_\delta g_2$, initials$(v_2) = \varnothing$ in $\partial_H(g_2)$.

By considering the same three cases with the roles of v_1 and v_2 reversed, we are done. ▮

To prove the completeness of $\text{ACP}_I^-(A) \cup \text{AX}(\gamma)$ for finite processes, we first introduce the notion of a "basic term" for closed $\text{ACP}_I^-(A)$ terms. We will subsequently prove an "elimination theorem" stating that any closed $\text{ACP}_I^-(A)$ term can be reduced to a basic term using the axioms of $\text{ACP}_I^-(A) \cup \text{AX}(\gamma)$. Combined with the completeness of BPA(A), this will be enough to prove the completeness of $\text{ACP}_I^-(A) \cup \text{AX}(\gamma)$.

DEFINITION 2.7. A *basic term* is defined inductively as follows:

- $a \in A_\delta$ is a basic term.
- Let t_1, t_2 be basic and $a \in A$. Then $t_1 + t_2$ and $a \cdot t_1$ are basic.

Note that a basic term uses a restricted form of sequential composition known as action prefixing, and that a basic term is a BPA(A_δ) term, i.e., a BPA(A) term treating δ as an additional atomic action.

To prove the elimination theorem we introduce a term rewriting system based on $\text{ACP}_I^-(A)$ for which we prove a strong normalization result. The rewrite system $\text{RACP}_I^-(A)$ consists of axioms (A1–5), (A7), (C3), (CM1–9), (I1–3), and (D1–2), treated as rewrite rules with left-to-right orientation, plus the rules

$$x + (y + z) \to (x + y) + z \qquad \text{(A2')}$$

$$a \mid \delta \to \delta \qquad \text{(C3')}$$

$$c \in H_\delta \Rightarrow \partial_H(c + x) \to \partial_H(x) \qquad \text{(D3.1')}$$

$$c \in H_\delta \Rightarrow \partial_H(c \cdot x + y) \to \partial_H(y) \qquad \text{(D3.1'')}$$

$$I(x + y) \cap H_\delta = \varnothing \Rightarrow \partial_H(x + y) \to \partial_H(x) + \partial_H(y) \qquad \text{(D3.2')}$$

$$\partial_H(a \cdot x) \to \partial_H(a) \cdot \partial_H(x) \qquad \text{(D4')}$$

Note that all these rules follow easily from $\text{ACP}_I^-(A)$. We will also need the rewrite system RAX(γ), a left-to-right oriented version of AX(γ). The normal forms of $\text{RACP}_I^-(A) \cup \text{RAX}(\gamma)$ are defined as follows.

DEFINITION 2.8. A closed $\text{ACP}_I^-(A)$ term t is in *normal form* if for all $\text{RACP}_I^-(A) \cup \text{RAX}(\gamma)$ reduction paths of the form

$$t = t_0 \to t_1 \to t_2 \to \cdots$$

t_{i+1} follows from t_i through the application of either rule (A1), (A2), or (A2') (and no other), for all $i \geq 0$.

PROPOSITION 2.3. *A normal form is a basic term.*

Proof. Let t be a normal form and suppose t is not basic. Let t' be a minimal subterm of t that is not basic. Then t' has one of the forms

1. $p \parallel q$
2. $p ⌊\!⌊ q$
3. $p \mid q$
4. $\partial_H(p)$
5. $p \cdot q$ (with p not an atom or $p = \delta$),

and both p and q are basic terms due to minimality. We show that in each case a rule of $\text{RACP}_I^-(A) \cup \text{RAX}(\gamma) - \{(\text{A1}), (\text{A2}), (\text{A2'})\}$ can still be applied, thereby proving the result by contradiction. Take, for example, the second case. Since p is a basic term, there are three subcases to consider:

(a) p is of the form $p_1 + p_2$. Apply (CM4).

(b) p is an atomic action $a \in A_\delta$. Apply (CM2).

(c) p is of the form $a \cdot p_1$, $a \in A_\delta$. Apply (CM3).

The other four cases are proved similarly. ▮

Note that the converse of this result does not hold, e.g., $a + a$ is basic but not in normal from.

LEMMA 2.1. *The rewrite system* $\text{RACP}_I^-(A) \cup \text{RAX}(\gamma)$ *is strongly normalizing modulo* (A1), (A2), (A2'), *i.e., every infinite reduction path contains* (A1), (A2), (A2') *steps only from some point onwards.*

Proof. Let $\Pi = (\zeta_0, t_0) \to (\zeta_1, t_1) \to (\zeta_2, t_2) \to \cdots$ be an infinite reduction path in $\text{RACP}_I^-(A) \cup \text{RAX}(\gamma)$ where ζ_i is the (possibly empty) condition associated with rewriting t_i into t_{i+1}. We omit from Π any steps having to do with normalizing the expression $I(x + y)$ in the condition to (D3.2')-steps. We prove that only finitely many of the steps in Π can differ from (A1), (A2), (A2').

We transform the reduction sequence Π into a reduction sequence Π' of RACP(A, γ) [BK84] as follows:

- Expand each (D3.1') step of the form $(\zeta_i, t_i) \to (\zeta_{i+1}, t_{i+1})$ into a finite valid rewriting of RACP(A, γ) depending on the condition ζ_i as follows:

— $c=\delta$: $\partial_H(\delta+x) \xrightarrow{(A1)} \partial_H(x+\delta) \xrightarrow{(A6)} (\zeta_{i+1}, \partial_H(x))$
— $c\in H$: $(c\in H, \partial_H(c+x)) \xrightarrow{(D3)} (c\in H, \partial_H(c)+\partial_H(x)) \xrightarrow{(D2)} \delta+\partial_H(x) \xrightarrow{(A1)} \partial_H(x)+\delta \xrightarrow{(A6)} (\zeta_{i+1}, \partial_H(x))$

• Expand each (D3.1″) step of the form $(\zeta_i, t_i) \rightarrow (\zeta_{i+1}, t_{i+1})$ into a finite valid rewriting of (RACP)(A, γ) depending on the condition ζ_i as follows:

— $c=\delta$: $\partial_H(\delta\cdot x+y) \xrightarrow{(A7)} \partial_H(\delta+y) \xrightarrow{(A1)} \partial_H(y+\delta) \xrightarrow{(A6)} (\zeta_{i+1}, \partial_H(y))$
— $c\in H$: $(c\in H, \partial_H(c\cdot x+y)) \xrightarrow{(D3)} \partial_H(c\cdot x)+\partial_H(y) \xrightarrow{(D4)} (c\in H, \partial_H(c)\cdot\partial_H(x)+\partial_H(y)) \xrightarrow{(D2)} \delta\cdot\partial_H(x)+\partial_H(y) \xrightarrow{A7} \delta+\partial_H(y) \xrightarrow{A1} \partial_H(y)+\delta \xrightarrow{A6} (\zeta_{i+1}, \partial_H(y))$

• Transform each (D3.2′) step of the form $(\zeta_i, t_i) \rightarrow (\zeta_{i+1}, t_{i+1})$ into the conditionless step $t_i \rightarrow (\zeta_{i+1}, t_{i+1})$, as (D3.2′) is valid in RACP(A, γ) in all cases (i.e., restriction distributes over plus).[1]

Now we obtain an infinite reduction path in RACP(A, γ) and from [BW90] it follows that this reduction path contains finitely many non-(A1), (A2), (A2′) steps. But the same must hold for the original reduction sequence. ∎

Note that in the transformation of a RACP$_I^-(A)\cup$ RAX(γ) reduction sequence to a RACP(A, γ) reduction sequence, each non-(A1), (A2), (A2′) step is replaced by at most six non-(A1), (A2), (A2′) steps.

We now present the "elimination theorem" for closed ACP$_I^-(A)$ terms.

LEMMA 2.2. *Let p be a closed* ACP$_I^-(A)$ *term. Then using* RACP$_I^-(A)\cup$RAX(γ), *p can be reduced in finitely many steps to a basic term.*

Proof. If p is a basic term we are done. Otherwise, by Proposition 2.3, p is not in normal form. By Definition 2.8, there exists a reduction sequence

$$p=p_0=t_0^0\rightarrow t_1^0\rightarrow\cdots\rightarrow t_{n_0}^0=p_1$$

such that $t_{n_0-1}^0\rightarrow t_{n_0}^0$ is not an (A1), (A2), (A2)′ reduction. If p_1 is basic we are done. Otherwise there exists another reduction sequence

$$p_1=t_0^1\rightarrow t_1^1\rightarrow\cdots\rightarrow t_{n_1}^1=p_2$$

such that $t_{n_1-1}^1\rightarrow t_{n_1}^1$ is not an (A1), (A2), (A2′) reduction. This line of reasoning cannot proceed indefinitely: due to strong normalization (Lemma 2.1) p_i, for some $i\geqslant 0$, is a basic term. Otherwise, an infinite reduction with infinitely many non-(A1), (A2), (A2′) steps would have been constructed which is impossible.

THEOREM 2.2.

1. $\mathscr{APG}(A_\delta, N, \gamma)/{\leftrightarrow_\delta} \models$ ACP$_I^-(A)\cup$AX(γ)
2. *For all closed expressions p, q over* $\Sigma($ACP$_I^-(A))$:

$$\mathscr{APG}(A_\delta, N, \gamma)/{\leftrightarrow_\delta} \models p=q \Rightarrow \text{ACP}_I^-(A)\cup\text{AX}(\gamma)\vdash p=q.$$

[1] One could, of course, leave condition ζ_i intact and still have a valid reduction step in RACP(A, γ).

Proof. For part 1, we consider axioms (A7) and (D1)–(D4). The case for an axiom in AX(γ) is trivial, and the fact that $\mathscr{APG}(A_\delta, N, \gamma)/{\leftrightarrow_\delta}$ is a model of the rest of the axioms of ACP$_I^-(A)$ follows standard arguments as presented, e.g., in [BW90]. For (A7), both $\delta\cdot x$ and δ initially can perform but a single δ-transition. Since $\leftrightarrow_\delta$ matches one δ-transition with any other δ-transition (i.e., without regard to the destination states), we are done. The soundness of (D1) and (D2) is immediate since in both cases the left- and right-hand side terms represent isomorphic process graphs.

For (D3.1), the initial transitions of x will be deleted from the root of $x+y$ by the ∂_H operation, thereby again resulting in isomorphic processes. (D3.2) could fail only if $x, y\neq\delta$ and either $\partial_H(x)=\delta$ or $\partial_H(y)=\delta$. The condition to the axiom ensures against this. Note that (D3.2) is still sound under the weaker condition

$$I(x)-H_\delta\neq\varnothing \quad\text{and}\quad I(y)-H_\delta\neq\varnothing$$

but the natural probabilistic extension of the resulting axiom is not sound (see Section 3.3), and is thus rejected. Finally, (D4) also represents isomorphic processes.

For part 2, suppose $p\leftrightarrow_\delta q$. Reduce p, q to normal forms p', q' using RACP$_I^-(A)\cup$RAX(γ); by Lemma 2.2, p', q' are basic terms. By part 1, $p'\leftrightarrow_\delta p\leftrightarrow_\delta q\leftrightarrow_\delta q'$, and thus $p'\leftrightarrow_\delta q'$. There thus exists a δ-bisimulation $\mathscr{R}$ between $g_{p'}$ and $g_{q'}$, where $g_{p'}=\langle V_1, r_1, \rightarrow_1\rangle$ is a representative of *Graph*(p') and $g_{q'}=\langle V_2, r_2, \rightarrow_2\rangle$ is a representative of *Graph*(q'). Now define the relation

$$\mathscr{R}'=\mathscr{R}\cup\{(v, w)\text{: endpoint}(v)\text{ and endpoint}(w)\}.$$

We show that, given that p', q' are normal forms, $\mathscr{R}'$ is a bisimulation (of the non-δ variety) relating $g_{p'}$ and $g_{q'}$. Then, by Theorem 2.1, BPA$(A_\delta)\vdash p'=q'$ and thus ACP$_I^-(A)\cup$AX$(\gamma)\vdash p=p'=q'=q$.

Obviously $\mathscr{R}'(r_1, r_2)$, and the transfer property holds for all $a\in A$. It remains to check δ-transitions. Suppose $\mathscr{R}(v, w)$ and $v\xrightarrow{\delta}_1 v'$. Now p' is in normal form (in particular, with respect to axiom (A7)), so v' is an endpoint. By $\leftrightarrow_\delta$, there exists a w' such that $w\xrightarrow{\delta}_2 w'$. Since q' is in normal form w' is also an endpoint, and thus $\mathscr{R}'(v', w')$. ∎

2.3.3. *Connections Between* ACP *and* ACP$_I^-$

We provide some observations on the relationship between "classical" ACP and ACP$_I^-(A)$. Let ACP(A, γ) be the equational theory for ACP, parameterized by A and γ, exactly as it is presented in [BW90], and let **A** denote its bisimulation model. Also, let $\mathbf{A}^-=\mathscr{APG}(A_\delta, N, \gamma)/{\leftrightarrow_\delta}$ be the bisimulation model for ACP$_I^-(A)$. Then for p, q closed expressions over $\Sigma($ACP$(A))$ we have the following results, which we state without proof.

1. Completeness of $\mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma)$: $\mathbf{A}^- \models p = q \Rightarrow \mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma) \vdash p = q$. (This is just part 2 of Theorem 2.2.)

2. Completeness of $\mathrm{ACP}(A, \gamma)$ [BW90]: $\mathbf{A} \models p = q \Rightarrow \mathrm{ACP}(A, \gamma) \vdash p = q$.

3. $\mathbf{A}^- \models p = q \Rightarrow \mathbf{A} \models p = q$. This implies that $\mathbf{A}^-$ can be homomorphically embedded in $\mathbf{A}$.

4. $\mathbf{A} \models p = q \Rightarrow \mathbf{A}^- \models \partial_\varnothing(p) = \partial_\varnothing(q)$.

5. $\mathrm{ACP}(A, \gamma) \vdash \partial_\varnothing(p) = p$.

6. $\mathrm{ACP}(A, \gamma) \vdash p = q \Rightarrow \mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma) + \{x + \delta = x\} \vdash p = q$.

7. $\mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma) \vdash \partial_\varnothing(x + \delta) = \partial_\varnothing(x)$.

3. A PROBABILISTIC VERSION

Our discussion of probabilistic ACP will proceed in a manner similar to before. For each of the axiom systems $AX \in \{\mathrm{BPA}(A), \mathrm{PA}(A), \mathrm{ACP}_I^-(A) \cup \mathrm{AX}(\gamma)\}$, a probabilistic version $prAX$ will be introduced, along with a probabilistic version of its process graph model. Completeness in these models will also be demonstrated. The sets A of actions and N of nodes, as well as the functions γ and $\bar{\gamma}$ are exactly as before.

3.1. Probabilistic BPA

3.1.1. *Equational Specification*

Notation. 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 $\{r \in \Re \mid 0 \leqslant r \leqslant 1\}$. We let π, ρ, σ, and θ, possibly subscripted, range over these intervals.

The signature $\Sigma(pr\,\mathrm{BPA}(A))$ over the sort $pr\,\mathbf{P}$ (for probabilistic processes) is given by:

$$\Sigma(pr\,\mathrm{BPA}(A)) = \{a\colon \to pr\,\mathbf{P} \mid a \in A\}$$
$$\cup \{+_\pi\colon pr\,\mathbf{P} \times pr\,\mathbf{P} \to pr\,\mathbf{P} \mid \pi \in (0, 1)\}$$
$$\cup \{\cdot\colon pr\,\mathbf{P} \times pr\,\mathbf{P} \to pr\,\mathbf{P}\}.$$

The operator $+$ has been replaced by the family of operators $+_\pi$, for each probability π in the interval $(0, 1)$, and is now called *probabilistic alternative composition*. Intuitively, the expression $x +_\pi y$ behaves like x with probability π and like y with probability $1 - \pi$. Probabilistic alternative composition is *generative* [vGSST90] in that a single distribution (viz. the discrete probability distribution $\{\pi, 1 - \pi\}$) 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 3.3 with the introduction of the restriction operator ∂_H in the setting of probabilistic ACP.

We have the following axioms for $pr\,\mathrm{BPA}(A)$:

$$x +_\pi y = y +_{1-\pi} x \qquad (pr\ \mathrm{A1})$$
$$x +_\pi (y +_\rho z) = (x +_{\pi/(\pi + \rho - \pi\rho)} y) +_{\pi + \rho - \pi\rho} z \qquad (pr\ \mathrm{A2})$$
$$x +_\pi x = x \qquad (pr\ \mathrm{A3})$$
$$(x +_\pi y) \cdot z = x \cdot z +_\pi y \cdot z \qquad (pr\ \mathrm{A4})$$
$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \qquad (pr\ \mathrm{A5})$$

A second version of $(pr\ \mathrm{A2})$, which we call $(pr\ \mathrm{A2'})$, will be used in the proofs of Lemma 3.4 and Proposition 3.3, and is given by:

$$(x +_\pi y) +_\rho z = x +_{\pi\rho} (y +_{(1-\pi)\rho/(1-\pi\rho)} z) \qquad (pr\ \mathrm{A2'})$$

3.1.2. *Probabilistic Graph Model*

As in Section 2.1.2, we consider process graphs, with labels from A and nodes from N, as a model for $pr\,\mathrm{BPA}(A)$. Additionally, a probability distribution will be ascribed to each node's outgoing transitions.

DEFINITION 3.1. A *probabilistic process graph* g is a triple $\langle V, r, \mu \rangle$ such that

- $V \subseteq N$ is the set of *nodes* of g
- $r \in V$ is the *root* of g
- $\mu\colon (V \times A \times V) \to [0, 1]$, the *transition distribution function* of g, is a total function satisfying the following *stochasticity condition*:

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

The intended meaning of $\mu(v, a, v') = \pi$ is that node v, with probability π, can perform an a-transition to node v'. Predicate endpoint(v) is true if the above sum is zero. We denote by $pr\,\mathcal{PG}(A, N)$ the class of all probabilistic process graphs over A and N.

The notion of strong bisimulation for nondeterministic processes has been extended by Larsen and Skou [LS92a] to reactive probabilistic processes in the form of *probabilistic bisimulation*. Here we define probabilistic bisimulation on generative probabilistic processes and to do so we first need to lift the definition of the transition distribution function as follows:

$$\mu\colon (V \times A \times 2^V) \to [0, 1]$$

$$\text{such that } \mu(v, a, S) = \sum_{v' \in S} \mu(v, a, v').$$

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

DEFINITION 3.2 [LS92a]. Let $g_1 = \langle V_1, r_1, \mu_1 \rangle$, $g_2 = \langle V_2, r_2, \mu_2 \rangle$ be probabilistic process graphs. A *probabilistic bisimulation* between g_1 and g_2 is an equivalence relation $\mathscr{R} \subseteq (V_1 \cup V_2) \times (V_1 \cup V_2)$ with the following properties:

- $\mathscr{R}(r_1, r_2)$
- $\forall v \in V_1, w \in V_2$ such that $\mathscr{R}(v, w)$:

$$\forall a \in A, S \in (V_1 \cup V_2)/\mathscr{R}, \mu_1(v, a, S \cap V_1) = \mu_2(w, a, S \cap V_2).$$

Graphs g_1 and g_2 are *probabilistically bisimilar*, written $g_1 \leftrightarrow^{pr} g_2$, 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. Also, our definition differs slightly from that of [LS92a] due to the presence of $S \cap V_1$ (and $S \cap V_2$) rather than simply S in the transfer condition. The intersection with V_1 is needed since μ_1 takes as an argument triples whose third component is a subset of V_1.

Let $\phi: pr\, \mathscr{PG}(A, N) \to \mathscr{PG}(A, N)$ be a mapping from probabilistic process graphs to nonprobabilistic process graphs, defined as follows.

DEFINITION 3.3. Let $g = \langle V, r, \mu \rangle$ be a probabilistic process graph. Then $\phi(g) = \langle V, r, \to \rangle$ has the same states and start state as g and $\to$ is such that

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

We will follow several practices adopted in Section 2.1.2: (i) we restrict our attention to the subset $pr\, \mathscr{APG}(A, N)$ of $pr\, \mathscr{PG}(A, N)$ consisting of the probabilistic process graphs that are mapped by ϕ onto an element of $\mathscr{APG}(A, N)$; (ii) we work with $pr\, \mathscr{APG}(A, N)/\cong$, isomorphism classes of $pr\, \mathscr{APG}(A, N)$ (defined below in the obvious way); and (iii) for $G_1, G_2 \in pr\, \mathscr{APG}(A, N)/\cong$, we define $G_1 \leftrightarrow^{pr} G_2$ if for some $g_1 \in G_1, g_2 \in G_2, g_1 \leftrightarrow^{pr} g_2$.

For probabilistic process graphs $g_1 = \langle V_1, r_1, \mu_1 \rangle$ and $g_2 = \langle V_2, r_2, \mu_2 \rangle$, we say that g_1 is *isomorphic* to g_2, written $g_1 \cong g_2$, if there exists a bijection $\psi: V_1 \to V_2$ such that $\psi(r_1) = \psi(r_2)$ and $\mu_1(v, a, v') = \mu_2(\psi(v), a, \psi(v'))$. As in the nonprobabilistic case, $\cong\, \subseteq\, \leftrightarrow^{pr}$ so we identify $(pr\, \mathscr{APG}(A, N)/\cong)/\leftrightarrow$ with $pr\, \mathscr{APG}(A, N)/\leftrightarrow$.

DEFINITION 3.4. Let $G_1, G_2 \in pr\, \mathscr{APG}(A, N)/\cong$ and let $g_1 \in G_1$ and $g_2 \in G_2$ be representatives such that $g_1 = \langle V_1, r_1, \mu_1 \rangle$, $g_2 = \langle V_2, r_2, \mu_2 \rangle$, $V_1 \cap V_2 = \varnothing$, and $N - (V_1 \cup V_2)$ is infinite. The operators $a \in A$, $+_\pi$, and $\cdot$ are defined on $pr\, \mathscr{APG}(A, N)/\cong$ as follows:

$a \in A$: A representative probabilistic process graph for a is given by $\langle \{r, v\}, r, \mu \rangle$, where $r, v \in N$, $r \neq v$, and $\mu(r, a, v) = 1$ is the only transition with non-zero probability.

$G_1 +_\pi G_2$: A representative is $\langle (V_1 \cup V_2 \cup \{r\} - \{r_1, r_2\}), r, \mu \rangle$ with $r \in N - (V_1 \cup V_2)$ and

$$\begin{array}{ll} \mu(r, a, v') = \pi \cdot \mu_1(r_1, a, v') & \text{if } v' \in V_1 \\ \mu(r, a, v') = (1 - \pi) \cdot \mu_2(r_2, a, v') & \text{if } v' \in V_2 \\ \mu(v, a, v') = \mu_1(v, a, v') & \text{if } v, v' \in (V_1 - \{r_1\}) \\ \mu(v, a, v') = \mu_2(v, a, v') & \text{if } v, v' \in (V_2 - \{r_2\}) \\ \mu(v, a, v') = 0 & \text{otherwise.} \end{array}$$

We refer to this particular representative as $g_1 +_\pi g_2$.

$G_1 \cdot G_2$: A representative is $\langle (V_1 \cup V_2 - \{r_2\}), r_1, \mu \rangle$, where

$$\mu(v, a, v') = \begin{cases} \mu_1(v, a, v') & \text{if } v, v' \in V_1 \\ \mu_2(r_2, a, v') & \text{if } v \in V_1, \text{endpoint}(v), v' \in V_2 \\ \mu_2(v, a, v') & \text{if } v, v' \in V_2 \\ 0 & \text{otherwise.} \end{cases}$$

We refer to this particular representative as $g_1 \cdot g_2$.

So, in the definition of $G_1 +_\pi G_2$, the transitions from r_1, r_2 are now assumed by the new root r, with their probability of occurrence weighted appropriately. Similarly, the transitions of r_2 in the definition of $G_1 \cdot G_2$ are assumed by each endpoint of g_1, with their original probabilities intact.

As in the nonprobabilistic case, for t a closed pr BPA(A) term, we write $Graph(t) = [\langle V_t, r_t, \mu_t \rangle]_\cong$ to denote the isomorphism class of the probabilistic process graph obtained inductively on t using Definition 3.4. We also write $t \leftrightarrow^{pr} t'$ as shorthand for $Graph(t) \leftrightarrow^{pr} Graph(t')$. The definition of $Graph(t)$ and the just-mentioned notational shorthand extend in the obvious way to the axiom systems pr PA(A) and pr ACP$_I^-(A)$ considered later in this section.

We will subsequently prove that the axioms of pr BPA(A) are complete for finite processes in this model. To admit sound equational reasoning, in particular, the substitution of equals for equals, we first show that $\leftrightarrow^{pr}$ is a congruence in pr BPA(A). Let V be an arbitrary set with $v \in V$. For any equivalence relation $\mathscr{R}$ over V we use $[v]_\mathscr{R}$ to denote the set $\{w \in V \mid (v, w) \in \mathscr{R}\}$; i.e., $[v]_\mathscr{R}$ is the equivalence class of v induced by $\mathscr{R}$. Also, $Id_V = \{(v, v) \mid v \in V\}$ denotes the identity relation on V.

PROPOSITION 3.1. *If* $G_1 \leftrightarrow^{pr} G_2$, *then* $G +_\pi G_1 \leftrightarrow^{pr} G +_\pi G_2$, $G \cdot G_1 \leftrightarrow^{pr} G \cdot G_2$, *and* $G_1 \cdot G \leftrightarrow^{pr} G_2 \cdot G$.

Proof. Assume $G_1 \leftrightarrow^{pr} G_2$ and let $g = \langle V, r, \mu \rangle$, $g_1 = \langle V_1, r_1, \mu_1 \rangle$, and $g_2 = \langle V_2, r_2, \mu_2 \rangle$ be arbitrary representatives of G, G_1, and G_2, respectively. Further, let $\mathscr{R}$ be a probabilistic bisimulation between g_1 and g_2. We now consider each of the operators in succession. For $+_\pi$, let r_i^+ be the root and μ_i^+ be the transition distribution function of $g +_\pi g_i$, $i = 1, 2$. We show that

$$\mathscr{R}' = \{(r_1^+, r_2^+), (r_2^+, r_1^+)\} \cup \mathscr{R} \cup Id_{V \cup \{r_1^+, r_2^+\}}$$

is a probabilistic bisimulation between $g +_\pi g_1$ and $g +_\pi g_2$. First note that because $\mathscr{R}$ is an equivalence relation, so is $\mathscr{R}'$. By the nature of $\mathscr{R}'$, we are left to show that the "transfer condition" (the second condition of Definition 3.2) holds for (r_1^+, r_2^+). For $a \in A$, the only a-transitions of r_1^+ of nonzero probability are of the form:

1. $\mu_1^+(r_1^+, a, [v']_{\mathscr{R}'}) = \mu(r, a, v') \cdot \pi$, where $v' \in V$; or
2. $\mu_1^+(r_1^+, a, [v_1']_{\mathscr{R}'}) = \mu_1(r_1, a, [v_1']_{\mathscr{R}}) \cdot (1 - \pi)$, where $v_1' \in V_1$.

We also have $\mu_2^+(r_2^+, a, [v']_{\mathscr{R}'}) = \mu(r, a, v') \cdot \pi$ and, because $g_1 \leftrightarrow^{pr} g_2$, $\mu_2^+(r_2^+, a, [v_1']_{\mathscr{R}'}) = \mu_1(r_1, a, [v_1']_{\mathscr{R}}) \cdot (1 - \pi)$. This completes the case for $+_\pi$.

For both cases of sequential composition, a straightforward argument demonstrates that $\mathscr{R} \cup Id_V$ is an appropriate probabilistic bisimulation. ∎

The graph model for *pr* BPA(A) is now given by *pr* $\mathscr{APG}(A, N)/\leftrightarrow^{pr}$. To prove completeness of *pr* BPA(A) in this model, we introduce the notation

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

with $n > 0$, $\sum \pi_i = 1$, and $\pi_i > 0$ for all i. So, in particular, when $n = 1$, $\pi_1 = 1$. This notation abbreviates right-nested probabilistic alternative composition expressions as follows:

$$\sum_{i=1}^{1} [\pi_i]\, x_i = x_1 \quad \text{and}$$

$$\sum_{i=1}^{n+1} [\pi_i]\, x_i = x_1 +_{\pi_1} \left(\sum_{i=1}^{n} \left[\frac{\pi_{i+1}}{1 - \pi_1} \right] x_{i+1} \right).$$

Note that in this notation $\sum_{i=1}^{n} [\pi_i]$ is a derived n-ary operator with operands x_i. To illustrate, the left-hand side of Eq. (*pr* A2) may be written

$$\sum_{i=1}^{3} [\pi_i]\, x_i,$$

where $\pi_1 = \pi$, $\pi_2 = (1 - \pi)\rho$, $\pi_3 = (1 - \pi)(1 - \rho)$, and $x_1 = x$, $x_2 = y$, $x_3 = z$.

This *summation form* notation is useful, as it directly reflects the transition structure of a representative probabilistic process graph underlying the nested probabilistic alternative composition. That is, consider the summation form $\sum [\pi_i]\, a_i \cdot x_i$ of action-prefixed processes. A representative process graph of this summation will have, for each i, a probability-π_i a_i-transition from its root to the node representing the root of a representative of *Graph*(x_i). Thus, for example,

$$\sum_{i=1}^{3} [\pi_i]\, x_i,$$

where $\pi_i = \frac{1}{3}$, $1 \leqslant i \leqslant 3$, $x_1, x_2 = a \cdot y$, and $x_3 = b \cdot z$, has two a-transitions, each of probability $\frac{1}{3}$, to node-disjoint representatives of *Graph*(y).

The following two lemmas for manipulating summation forms, the proofs of which appear in the Appendix, will prove useful in the completeness proof for *pr* BPA(A). The first allows summands to be reordered arbitrarily, retaining their original probabilities, while the second allows two syntactically identical summands to be merged into one summand, summing the probabilities in the process.

LEMMA 3.1. *For any permutation ξ of $\{1, ..., n\}$, $n \geqslant 2$,*

$$pr\ \mathrm{BPA}(A) \vdash \sum_{i=1}^{n} [\pi_i]\, x_i = \sum_{i=1}^{n} [\pi_{\xi(i)}]\, x_{\xi(i)}.$$

LEMMA 3.2. *In the summation form $\sum_{i=1}^{n+1} [\pi_i]\, x_i$, let x_1 and x_2 be syntactically identical. Then*

$$pr\ \mathrm{BPA}(A) \vdash \sum_{i=1}^{n+1} [\pi_i]\, x_i = \sum_{i=1}^{n} [\rho_i]\, y_i,$$

where $\rho_1 = \pi_1 + \pi_2$, $y_1 = x_1$, and $\rho_i = \pi_{i+1}$, $y_i = x_{i+1}$, $2 \leqslant i \leqslant n$.

We now use summation-form notation to define a kind of normal form for closed *pr* BPA(A) terms.

DEFINITION 3.5. A *probabilistic basic term* is a summation form $\sum_{i=1}^{n} [\pi_i]\, t_i$, where t_i is either some $a \in A$ or of the form $b \cdot t_i'$, where $b \in A$ and t_i' is a probabilistic basic term. A *probabilistic head-normal form* is a probabilistic basic term $\sum_{i=1}^{n} [\pi_i]\, t_i$ such that $t_i \not\leftrightarrow^{pr} t_j$, $1 \leqslant i \neq j \leqslant n$.

Note that a probabilistic basic term, such as a basic $\mathrm{ACP}_I^-(A)$ term of Section 2.3, uses action prefixing, while a probabilistic head-normal form bears the additional constraint that its summands are pairwise inequivalent.

The *depth* of a probabilistic basic term t, denoted $d(t)$, is essentially the maximum number of nested prefixes in t. The inductive definition of d is as follows:

- $d(a) = 1$
- $d(a \cdot t) = 1 + d(t)$
- $d(\sum_i [\pi_i]\, t_i) = max_i(d(t_i))$.

The relationship observed above between a probabilistic summation form and its underlying probabilistic process graph can be strengthened in the case of probabilistic basic terms and, hence, probabilistic head-normal forms.

PROPOSITION 3.2. *Let $t = \sum_{i=1}^{n} [\pi_i]\, t_i$ be a probabilistic basic term and let $g_t = \langle V_t, r_t, \mu_t \rangle$ be a representative of Graph(t). Then one can identify nodes v_i, $1 \leqslant i \leqslant n$, in g_t such that*

- *$v_1, ..., v_n$ range over all successor nodes of r_t and are all pairwise distinct;*
- *if t_i is of the form a_i, $a_i \in A$, then endpoint(v_i) and $\pi_i = \mu_t(r_t, a_i, v_i)$;*
- *if t_i is of the form $b_i \cdot t'_i$ then $g_i \in Graph(t'_i)$, where g_i is the probabilistic process graph "rooted at v_i," and $\pi_i = \mu_t(r_t, b_i, v_i)$.*

Proposition 3.2 is an immediate consequence of the construction of *Graph(t)*, which is an element of $pr\, \mathcal{APG}(A, N)/\cong$. The formal definition of g_i is straightforward and omitted.

Below, we prove that any closed *pr* BPA(*A*) term can be reduced to a probabilistic head-normal form. We need first the following result which shows that the axioms of *pr* BPA(*A*) are complete for probabilistic head-normal forms.

LEMMA 3.3. *For probabilistic head-normal forms s, t over $\Sigma(pr\, \mathrm{BPA}(A))$:*

$$pr\, \mathcal{APG}(A, N)/\leftrightarrow^{pr} \models s = t \Rightarrow pr\, \mathrm{BPA}(A) \vdash s = t.$$

Proof. Assume $s \leftrightarrow^{pr} t$. Being a probabilistic head-normal form, s is of the form

$$s = \sum_{i=1}^{n} [\pi_i]\, s_i, \quad \text{where } s_i = a_i \text{ or } s_i = a_i \cdot s'_i$$

depending on whether or not s_i terminates after one step. Similarly, t is of the form

$$t = \sum_{j=1}^{m} [\rho_j]\, t_j, \quad \text{where } t_j = b_j \text{ or } t_j = b_j \cdot t'_j.$$

We prove the result by induction on the maximum depth of s and t. If the maximum depth is 1 then each summand s_i of s is the constant $a_i \in A$, and each summand of t_j of t is the constant $b_j \in A$. Since s and t are in probabilistic head-normal form, the a_i are pairwise distinct and the b_j are pairwise distinct. Furthermore, since $s \leftrightarrow^{pr} t$, there must exist a bijection f such that $a_i = b_{f(i)}$ and $\pi_i = \rho_{f(i)}$. By Lemma 3.1, *pr* BPA(*A*) $\vdash s = t$.

Next, assume the result for maximum depth k and let the maximum depth of s, t be $k+1$. Let $g_s = \langle V_s, r_s, \mu_s \rangle$ and $g_t = \langle V_t, r_t, \mu_t \rangle$ be representatives of *Graph(s)* and *Graph(t)*, respectively. By Proposition 3.2, we can identify $v_1, ..., v_n$ as the pairwise-distinct successors of r_s in g_s, and $u_1, ..., u_m$ as the pairwise-distinct successors of r_t in g_t. Recall that $Graph(s) \leftrightarrow^{pr} Graph(t)$ and let $\mathcal{R}$ be a probabilistic bisimulation between g_s and g_t that does not relate different endpoints among the v_i and, likewise, does not relate different endpoints among the u_j.

We prove that there exists a bijection f such that every summand s_i of s can be proven equal to summand $t_{f(i)}$ of t and $\pi_i = \rho_{f(i)}$. It then follows by n applications of substitution of equals for equals, and by using Lemma 3.1 to reorder summands as necessary, that *pr* BPA(*A*) $\vdash s = t$.

Since s is a probabilistic head-normal form, no two endpoints among the v_i are related by $\mathcal{R}$, and probabilistic bisimulation is preserved under sequential composition (Proposition 3.1), $\mu_s(r_s, a_i, v_i) = \mu_s(r_s, a_i, [v_i]_{\mathcal{R}})$, $1 \leqslant i \leqslant n$. Similarly, $\mu_t(r_t, b_j, u_j) = \mu_t(r_t, b_j, [u_j]_{\mathcal{R}})$, $1 \leqslant j \leqslant m$. $\mathcal{R}$ is a probabilistic bisimulation between g_s and g_t, so $\mathcal{R}(r_s, r_t)$ and there must exist a bijection f such that

$$\mu_s(r_s, a_i, [v_i]_{\mathcal{R}} \cap V_s) = \mu_t(r_t, b_{f(i)}, [u_{f(i)}]_{\mathcal{R}} \cap V_t),$$

with $a_i = b_{f(i)}$ and $[v_i]_{\mathcal{R}} = [u_{f(i)}]_{\mathcal{R}}$. Therefore, $\pi_i = \sigma_{f(i)}$, $1 \leqslant i \leqslant n$.

If *endpoint*(v_i), we are done; i.e., $s_i = t_{f(i)} = a_i$. Otherwise, s_i is of the form $a_i \cdot s'_i$. Since the probabilistic process graphs rooted at v_i in g_s and $u_{f(i)}$ in g_t are representatives of *Graph*(s'_i) and *Graph*($t'_{f(i)}$), respectively (Proposition 3.2), we have that $\mathcal{R}$ (restricted to the nodes in the two subtrees) is a probabilistic bisimulation witnessing $Graph(s'_i) \leftrightarrow^{pr} Graph(t'_{f(i)})$. Now, by induction, *pr* BPA(*A*) $\vdash s'_i = t'_{f(i)}$. Using substitution of equals for equals, *pr* BPA(*A*) $\vdash s_i = t_{f(i)}$. ∎

LEMMA 3.4. *For every closed pr* BPA(*A*) *term t, there is a probabilistic normal form s such that pr* BPA(*A*) $\vdash t = s$.

Proof. The proof has two parts. In the first part, we prove that a closed term t can be proven equal to a probabilistic basic term. The second part handles the constraint that the summands are pairwise inequivalent. The first part is simpler and follows the line of reasoning in [BW90]. That is, we use a term rewriting system to convert t into a term whose only instances of sequential composition are of the form $a \cdot t'$, i.e., action prefixing. The rewrite system is based on *pr* BPA(*A*) axioms *pr* A4 and *pr* A5 and is given by

$$(x +_\pi y) \cdot z \rightarrow x \cdot z +_\pi y \cdot z$$

$$(x \cdot y) \cdot z \rightarrow x \cdot (y \cdot z).$$

It is not hard to see that this term rewrite system is confluent and strongly normalizing, and that a normal form of a closed term uses only action prefixing. Therefore, given a closed *pr* BPA(A) term t, we can convert it into a probabilistic basic term as follows:

1. Reduce t until a normal form is reached.
2. Use (*pr* A2′) to rewrite all instances of left-nested summations into right-nested summations. The resulting term can then be expressed as a summation form.

By the first part of the proof, assume t is a probabilistic basic term of the form $\sum_{i=1}^{n} [\pi_i]\, t_i$ and consider the equivalence relation on $\{1, ..., n\}$ identifying i and i' iff $t_i \leftrightarrow^{pr} t_{i'}$. Suppose this gives us equivalence classes $\{B_1, ..., B_m\}$. We prove by induction on the depth of t that

$$pr\,\mathrm{BPA}(A) \vdash t = \sum_{j=1}^{m} [\rho_j]\, t'_j,$$

where $\rho_j = \sum \{\pi_i \mid i \in B_j\}$, $t'_j = t_i$ for an arbitrarily chosen $i \in B_j$. Note that the term on the right-hand-side of this equation is indeed a probabilistic normal form. If the depth of t is 1 then each t_i is a constant and the indices in a block B_j correspond to (all of the) multiple occurrences of a constant a. If $|B_j| = 1$ then we are done. Otherwise, apply the following procedure $|B_j| - 1$ times: move two instances of a to the two leftmost positions within the summation form using Lemma 3.1. Merge the two instances into one, occupying the leftmost position in the resulting summation form, using Lemma 3.2. The associated probability of this single instance of a will be the sum of the probabilities of the original two instances, as desired.

Next, assume the result for probabilistic basic terms of depth k and let $d(t) = k + 1$. There are two cases.

1. The indices in a block B_j correspond to the multiple occurrences of a constant a. The base case reasoning suffices here.
2. The indices in a block B_j correspond to probabilistically bisimilar terms of the form $a \cdot t'$, $b \cdot t''$, where t', t'' are basic. If $|B_j| = 1$ then we are done. Otherwise, apply the following procedure $|B_j| - 1$ times. Choose two instances $a \cdot t'$, $b \cdot t''$ of equivalent terms from B_j. Since $a \cdot t' \leftrightarrow^{pr} b \cdot t''$, then $a = b$ and $t' \leftrightarrow^{pr} t''$, and, by the induction hypothesis, we can assume that t' and t'' are probabilistic head-normal forms. By Lemma 3.3, *pr* BPA(A) $\vdash t' = t''$ and, by substitution of equals for equals, *pr* BPA(A) $\vdash a \cdot t' = b \cdot t''$. As in the first case, we can use Lemmas 3.1 and 3.2 to merge these two summands into a single summand, either $a \cdot t'$ or $b \cdot t''$, the choice being arbitrary. The associated probability of the merged term will be the sum of the associated probabilities of $a \cdot t'$ and $b \cdot t''$, as desired. ∎

We now prove that our algebra $pr\,\mathcal{APG}(A, N)/\leftrightarrow^{pr}$ is a model of *pr* BPA(A) and that *pr* BPA(A) constitutes a complete axiomatization of process equivalence in $pr\,\mathcal{APG}(A, N)/\leftrightarrow^{pr}$ for finite processes.

THEOREM 3.1.

1. $pr\,\mathcal{APG}(A, N)/\leftrightarrow^{pr} \models pr\,\mathrm{BPA}(A)$.
2. *For closed expressions* s, t *over* $\Sigma(pr\,\mathrm{BPA}(A))$,

$$pr\,\mathcal{APG}(A, N)/\leftrightarrow^{pr} \models s = t \Rightarrow pr\,\mathrm{BPA}(A) \vdash s = t.$$

Proof. For part 1, consider first (*pr* A1) and (*pr* A2). In both cases the left- and right-hand side terms represent isomorphic probabilistic process graphs, with the transitions from the root of x weighted by π and the transitions from the root of y weighted by $1 - \pi$, in the case of (*pr* A1); and the root transitions of x weighted by π, the root transitions of y rooted by $(1 - \pi)\,\rho$, and the root transitions of z weighted by $(1 - \pi)(1 - \rho)$, in the case of (*pr* A2).

Graph isomorphism arguments also suffice for (*pr* A4) and (*pr* A5), while the soundness of (*pr* A3) is established by the probabilistic bisimulation $\{(r_{x+_\pi x}, r_x), (r_x, r_{x+_\pi x})\} \cup Id_{V_x \cup \{r_{x+_\pi x}\}}$.

For part 2, we can apply Lemma 3.4 to find normal forms s' and t' such that *pr* BPA(A) $\vdash s = s'$ and *pr* BPA(A) $\vdash t = t'$. The result now follows by Lemma 3.3. ∎

PROPOSITION 3.3. *The various forms of* $+_\pi$ *distribute over one another*:

$$(x +_\pi y) +_\rho z = (x +_\rho z) +_\pi (y +_\rho z).$$

Proof.

$$\begin{aligned}
&(x +_\rho z) +_\pi (y +_\rho z) \\
&\quad = x +_{\rho\pi} (z +_{(1-\rho)\,p/(1-\rho\pi)} (y +_\rho z)) && (pr\ \mathrm{A2}) \\
&\quad = x +_{\rho\pi} (z +_{(1-\rho)\,p/(1-\rho\pi)} (z +_{1-\rho} y)) && (pr\ \mathrm{A1}) \\
&\quad = x +_{\rho\pi} ((z +_\pi z) +_{(1-\rho)/(1-\rho\pi)} y) && (pr\ \mathrm{A2}) \\
&\quad = x +_{\rho\pi} (z +_{(1-\rho)/(1-\rho\pi)} y) && (pr\ \mathrm{A3}) \\
&\quad = x +_{\rho\pi} (y +_{\rho(1-\pi)/(1-\rho\pi)} z) && (pr\ \mathrm{A1}) \\
&\quad = (x +_\pi y) +_\rho z && (pr\ \mathrm{A2}').
\end{aligned}$$ ∎

3.2. Probabilistic PA

3.2.1. *Equational Specification*

The signature $\Sigma(pr\,\mathrm{PA}(A))$ extends that of *pr* BPA(A).

$$\begin{aligned}
\Sigma(pr\,\mathrm{PA}(A)) = \Sigma(pr\,\mathrm{BPA}(A)) \\
\cup \{\|_\sigma : pr\,\mathbf{P} \times pr\,\mathbf{P} \to pr\,\mathbf{P} \mid \sigma \in (0, 1)\} \\
\cup \{\lfloor\!\lfloor_\sigma : pr\,\mathbf{P} \times pr\,\mathbf{P} \to pr\,\mathbf{P} \mid \sigma \in (0, 1)\}.
\end{aligned}$$

Intuitively, $\|_\sigma$ is a *probabilistic merge* operator, with the left operand receiving relative probability σ and the right operand relative probability $1 - \sigma$. As in PA(A), $\lfloor\!\lfloor_\sigma$ is a restricted version of $\|_\sigma$ in which the first step must come from the left operand.

The axiom system $pr\,\mathrm{PA}(A)$ is obtained by adding to $pr\,\mathrm{BPA}(A)$ the following axioms for probabilistic merge and left-merge:

$$x \parallel_\sigma y = x \mathbin{⌊\!⌊}_\sigma y +_\sigma y \mathbin{⌊\!⌊}_{(1-\sigma)} x \quad (pr\,\mathrm{M1})$$

$$a \mathbin{⌊\!⌊}_\sigma y = a \cdot y \quad (pr\,\mathrm{M2})$$

$$(a \cdot x) \mathbin{⌊\!⌊}_\sigma y = a \cdot (x \parallel_\sigma y) \quad (pr\,\mathrm{M3})$$

$$(x +_\pi y) \mathbin{⌊\!⌊}_\sigma z = (x \mathbin{⌊\!⌊}_\sigma z) +_\pi (y \mathbin{⌊\!⌊}_\sigma z) \quad (pr\,\mathrm{M4})$$

3.2.2. *Graph Model*

As for $pr\,\mathrm{BPA}(A)$, we provide a bisimulation model for $pr\,\mathrm{PA}(A)$, and prove the completeness of the axioms on finite probabilistic processes.

DEFINITION 3.6. Let $G_1, G_2 \in pr\,\mathcal{APG}(A, N)/\cong$ and let $g_1 \in G_1$ and $g_2 \in G_2$ be representatives such that $g_1 = \langle V_1, r_1, \mu_1 \rangle$, $g_2 = \langle V_2, r_2, \mu_2 \rangle$, $V_1 \cap V_2 = \emptyset$, and $N - (V_1 \cup V_2)$ is infinite. The operators $\|_\sigma$ and $⌊\!⌊_\sigma$ are defined on $pr\,\mathcal{APG}(A, N)/\cong$ as follows:

$G_1 \|_\sigma G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \mu \rangle$ where for all $a \in A$, $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} \sigma \cdot \mu_1(v_1, a, v_1') & \text{if } \neg\text{endpoint}(v_2) \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-\sigma) \cdot \mu_2(v_2, a, v_2') & \text{if } \neg\text{endpoint}(v_1) \\ \mu_2(v_2, a, v_2') & \text{otherwise.} \end{cases}$$

We refer to this particular representative as $g_1 \|_\sigma g_2$.

$G_1 ⌊\!⌊_\sigma G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \mu \rangle$ where for all $a \in A$, $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$

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

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} \sigma \cdot \mu_1(v_1, a, v_1') & \text{if } \neg\text{endpoint}(v_2) \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-\sigma) \cdot \mu_2(v_2, a, v_2') & \text{if } \neg\text{endpoint}(v_1) \\ \mu_2(v_2, a, v_2') & \text{otherwise} \end{cases}$$

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

We refer to this particular representative as $g_1 ⌊\!⌊_\sigma g_2$.

Note the careful treatment of endpoints in the above definition: in a merge, if one process terminates, the other continues with its original, unweighted probability. Also, in a left-merge, special attention is paid to transitions from the root (r_1, r_2) of $g_1 ⌊\!⌊_\sigma g_2$: the first and third clauses collectively define the transition distribution function μ on all transitions from (r_1, r_2), with the third clause giving probability 0 to transitions starting with g_2.

We have that probabilistic bisimulation is a congruence in $pr\,\mathrm{PA}(A)$.

PROPOSITION 3.4. *If* $G_1 \leftrightarrow^{pr} G_2$, *then* $G \|_\sigma G_1 \leftrightarrow^{pr} G \|_\sigma G_2$, $G ⌊\!⌊_\sigma G_1 \leftrightarrow^{pr} G ⌊\!⌊_\sigma G_2$, *and* $G_1 ⌊\!⌊_\sigma G \leftrightarrow^{pr} G_2 ⌊\!⌊_\sigma G$.

Proof. Assume $G_1 \leftrightarrow^{pr} G_2$ and let $g = \langle V, r, \mu \rangle$, $g_1 = \langle V_1, r_1, \mu_1 \rangle$, and $g_2 = \langle V_2, r_2, \mu_2 \rangle$ be arbitrary representatives of G, G_1, and G_2, respectively. Further, let $\mathcal{R}$ be a probabilistic bisimulation between g_1 and g_2. We first show that

$$\mathcal{R}' = \{((v, v_1), (v, v_2)) \mid v \in V, (v_1, v_2) \in \mathcal{R}\}$$

is a probabilistic bisimulation between $g \|_\sigma g_1$ and $g \|_\sigma g_2$. First note that because $\mathcal{R}$ is an equivalence relation, so is $\mathcal{R}'$. Also, for $v \in V$, $w \in (V_1 \cup V_2)$, $[(v, w)]_{\mathcal{R}'} = \{v\} \times [w]_{\mathcal{R}}$. Now consider the pair $((v, v_1), (v, v_2)) \in \mathcal{R}'$ with $v_1 \in V_1$, $v_2 \in V_2$ and let $\mu_i^{\|}$ be the transition distribution function of $g \|_\sigma g_i$, $i = 1, 2$. For $a \in A$, the only a-transitions of (v, v_1) of nonzero probability are of the form:

1. $\mu_1^{\|}((v, v_1), a, [(v', v_1)]_{\mathcal{R}'}) = \sigma \cdot \mu(v, a, v')$
2. $\mu_1^{\|}((v, v_1), a, [(v, v_1')]_{\mathcal{R}'}) = (1-\sigma) \cdot \mu_1(v_1, a, [v_1']_{\mathcal{R}} \cap V_1)$.

We also have that $\mu_2^{\|}((v, v_2), a, [(v', v_2)]_{\mathcal{R}'}) = \sigma \cdot \mu(v, a, v')$ and, because $g_1 \leftrightarrow^{pr} g_2$, $\mu_2^{\|}((v, v_2), a, [(v, v_1')]_{\mathcal{R}'}) = (1-\sigma) \cdot \mu_1(v_1, a, [v_1']_{\mathcal{R}} \cap V_1)$. The argument is similar in case (1) if v_1 is an endpoint (the value of $\mu_1^{\|}$ would not be weighted by σ), and in case (2) if v is an endpoint (the value of $\mu_1^{\|}$ would not be weighted by $1-\sigma$).

A symmetric argument, with the roles of v_1 and v_2 reversed, completes the proof that $\mathcal{R}'$ is the desired bisimulation.

An argument similar to the above can be used to show that $\mathcal{R}'$ is also a probabilistic bisimulation between $g ⌊\!⌊_\sigma g_1$ and $g ⌊\!⌊_\sigma g_2$. In particular, there are fewer transitions of non-zero probability from (r, r_1) and (r, r_2) since such transitions can come from g only. Like in the endpoint cases considered just above, the probabilities of these transitions are not weighted by σ.

A nearly symmetric argument establishes that

$$\mathcal{R}'' = \{((v_1, v), (v_2, v)) \mid (v_1, v_2) \in \mathcal{R}, v \in V\}$$

is a probabilistic bisimulation between $g_1 ⌊\!⌊_\sigma g$ and $g_2 ⌊\!⌊_\sigma g$. ∎

THEOREM 3.2.

1. $pr\ \mathcal{APG}(A, N)/\underline{\leftrightarrow}^{pr} \models pr\ \mathrm{PA}(A)$
2. *For all closed expressions s, t over* $\Sigma(pr\ \mathrm{PA}(A))$:

$$pr\ \mathcal{APG}(A, N)/\underline{\leftrightarrow}^{pr} \models s = t \Rightarrow pr\ \mathrm{PA}(A) \vdash s = t.$$

Proof. For part 1, the soundness of axioms (pr M1–4) is immediate by probabilistic process graph isomorphism arguments. The following comments, however, are in order. Axiom (pr M1) is a kind of expansion law for probabilistic merge. In (pr M2), $a \mathbin{\|\!\_}_\sigma y$ behaves like y after performing a as it will have reached a state where y is in a probabilistic merge with an endpoint. In (pr M3), $(a \cdot x) \mathbin{\|\!\_}_\sigma y$ behaves like $x \parallel_\sigma y$ after performing a since left-merge behaves like merge after its root transitions. The left-hand and right-hand side processes of (pr M4) both represent a probabilistic merge with z, the first step of which must come from x (with probability π) or y (with probability $1-\pi$).

For part 2, the proof is similar to the one given in [BW90] for the completeness of PA(A). We use the following term rewrite system, with rules corresponding to pr BPA(A) axioms (pr A3–5) and pr PA(A) axioms (pr M1–4), to eliminate all occurrences of $\parallel_\sigma$ and $\mathbin{\|\!\_}_\sigma$ in a closed pr PA(A) term:

$$x +_\pi x \to x$$
$$(x +_\pi y) \cdot z \to x \cdot z +_\pi y \cdot z$$
$$(x \cdot y) \cdot z \to x \cdot (y \cdot z)$$
$$x \parallel_\sigma y \to x \mathbin{\|\!\_}_\sigma y +_\sigma y \mathbin{\|\!\_}_{(1-\sigma)} x$$
$$a \mathbin{\|\!\_}_\sigma y \to a \cdot y$$
$$a \cdot x \mathbin{\|\!\_}_\sigma y \to a \cdot (x \parallel_\sigma y)$$
$$(x +_\pi y) \mathbin{\|\!\_}_\sigma z \to (x \mathbin{\|\!\_}_\sigma z) +_\pi (y \mathbin{\|\!\_}_\sigma z).$$

It can be proved that this term rewriting system is strongly normalizing and that a normal form of a closed term must be a probabilistic basic term. By part 1 of the theorem (the soundness of pr PA(A)) and Theorem 3.1 (the soundness and completeness of pr BPA(A)), the result is proven. ∎

3.3. Probabilistic ACP

3.3.1. *Equational Specification*

The signature of $pr\ \mathrm{ACP}_I^-(A)$ also extends that of pr BPA(A). Recalling that $A_\delta = A \cup \delta$, we have

$$\begin{aligned}
&\Sigma(pr\ \mathrm{ACP}_I^-(A))\\
&\quad = \Sigma(pr\ \mathrm{BPA}(A)) \cup \{\delta : \to pr\ \mathbf{P}\} \cup \{I\colon pr\ \mathbf{P} \to 2^{A_\delta}\}\\
&\qquad \cup \{|_{\sigma,\theta}\colon pr\ \mathbf{P} \times pr\ \mathbf{P} \to pr\ \mathbf{P} \mid \sigma, \theta \in (0,1)\}\\
&\qquad \cup \{\parallel_{\sigma,\theta}\colon pr\ \mathbf{P} \times pr\ \mathbf{P} \to pr\ \mathbf{P} \mid \sigma, \theta \in (0,1)\}\\
&\qquad \cup \{\mathbin{\|\!_}_{\sigma,\theta}\colon pr\ \mathbf{P} \times pr\ \mathbf{P} \to pr\ \mathbf{P} \mid \sigma, \theta \in (0,1)\}\\
&\qquad \cup \{\partial_H\colon pr\ \mathbf{P} \to pr\ \mathbf{P} \mid H \subseteq A\}.\\
&\qquad \cup \{I\colon pr\ \mathbf{P} \to 2^{A_\delta}\}.
\end{aligned}$$

Thus, for each of the operators $|$, $\parallel$, and $\mathbin{\|\!\_}$ we have a family of operators, each indexed by two probabilities from the interval (0, 1). These operators work intuitively as follows. Consider first the merge operator. In the expression $x \parallel_{\sigma,\theta} y$, a communication between x and y occurs with probability $1-\theta$, and an autonomous move by either x or y occurs with probability θ. Given that an autonomous move occurs, it comes from x with probability σ and from y with probability $1-\sigma$. The situation is similar for $x \mathbin{\|\!\_}_{\sigma,\theta} y$ except the first step must (with probability 1) come from x. Likewise, the first step of $x\ |_{\sigma,\theta}\ y$ must result from a communication between x and y.

The treatment of the communication merge is exactly analogous to the situation in the nonprobabilistic case (Section 2.3). The "totality" axiom (C0) now becomes

$$\begin{aligned}
&\forall a, b \in pr\ \mathbf{P} \quad \overline{A_\delta}(a) \wedge \overline{A_\delta}(b)\\
&\quad \Rightarrow \forall \sigma, \theta \in (0,1) \quad \overline{A_\delta}(a\ |_{\sigma,\theta}\ b) \quad (pr\ \mathrm{C0})
\end{aligned}$$

The axioms of $pr\ \mathrm{ACP}_I^-(A)$ are as follows. In this system, a, b, c range over A_δ, $H_\delta = H \cup \{\delta\}$, and $\{I\colon pr\ \mathbf{P} \to 2^{A_\delta}\}$. $\cap$, $\cup$ are used on 2^{A_δ} without further specification.

pr BPA(A)

+

$$\delta \cdot x = \delta \quad (pr\ \mathrm{A7})$$

+

(pr C0)

+

$$a\ |_{\sigma,\theta}\ b = b\ |_{(1-\sigma),\theta}\ a \qquad (pr\ \mathrm{C1})$$
$$(a\ |_{\sigma,\theta}\ b)\ |_{\sigma',\theta'}\ c = a\ |_{\sigma,\theta}\ (b\ |_{\sigma',\theta'}\ c) \qquad (pr\ \mathrm{C2})$$
$$\delta\ |_{\sigma,\theta}\ a = \delta \qquad (pr\ \mathrm{C3})$$

+

$$\begin{aligned}
x \parallel_{\sigma,\theta} y = {} & ((x \mathbin{\|\!_}_{\sigma,\theta} y) +_\sigma (y \mathbin{\|\!_}_{(1-\sigma),\theta} x))\\
& +_\theta (x\ |_{\sigma,\theta}\ y) && (pr\ \mathrm{CM1})\\
a \mathbin{\|\!_}_{\sigma,\theta} y = {} & a \cdot y && (pr\ \mathrm{CM2})\\
(a \cdot x) \mathbin{\|\!_}_{\sigma,\theta} y = {} & a \cdot (x \parallel_{\sigma,\theta} y) && (pr\ \mathrm{CM3})\\
(x +_\pi y) \mathbin{\|\!_}_{\sigma,\theta} z = {} & (x \mathbin{\|\!_}_{\sigma,\theta} z) +_\pi (y \mathbin{\|\!_}_{\sigma,\theta} z) && (pr\ \mathrm{CM4})\\
a\ |_{\sigma,\theta}\ (b \cdot x) = {} & (a\ |_{\sigma,\theta}\ b) \cdot x && (pr\ \mathrm{CM5})
\end{aligned}$$

$$(a \cdot x) \mid_{\sigma,\theta} b = (a \mid_{\sigma,\theta} b) \cdot x \qquad (pr\,\text{CM6})$$
$$(a \cdot x) \mid_{\sigma,\theta} (b \cdot y) = (a \mid_{\sigma,\theta} b) \cdot (x \parallel_{\sigma,\theta} y) \qquad (pr\,\text{CM7})$$
$$(x +_\pi y) \mid_{\sigma,\theta} z = x \mid_{\sigma,\theta} z +_\pi y \mid_{\sigma,\theta} z \qquad (pr\,\text{CM8})$$
$$x \mid_{\sigma,\theta} (y +_\pi z) = x \mid_{\sigma,\theta} y +_\pi x \mid_{\sigma,\theta} z \qquad (pr\,\text{CM9})$$
$$+$$
$$I(a) = \{a\} \qquad (pr\,\text{I1})$$
$$I(x \cdot y) = I(x) \qquad (pr\,\text{I2})$$
$$I(x +_\pi y) = I(x) \cup I(y) \qquad (pr\,\text{I3})$$
$$+$$
$$a \in H \Rightarrow \partial_H(a) = \delta \qquad (pr\,\text{D1})$$
$$a \notin H \Rightarrow \partial_H(a) = a \qquad (pr\,\text{D2})$$
$$I(x) \subseteq H_\delta \Rightarrow \partial_H(x +_\pi y) = \partial_H(y) \qquad (pr\,\text{D3.1})$$
$$I(x +_\pi y) \cap H_\delta = \varnothing \Rightarrow \partial_H(x +_\pi y) = \partial_H(x) +_\pi \partial_H(y) \qquad (pr\,\text{D3.2})$$
$$\partial_H(x \cdot y) = \partial_H(x) \cdot \partial_H(y) \qquad (pr\,\text{D4})$$

The axioms for γ (the restriction of $\mid_{\sigma,\theta}$ to $A \times A$) in the probabilistic setting are given by

$$pr\,\text{AX}(\gamma) = \{a \mid_{\sigma,\theta} b = c : a \in A, b \in A, \gamma(a,b) = c, \forall \sigma, \theta \in (0,1)\} \cup \{a \mid_{\sigma,\theta} b = \delta : a \in A, b \in A, \gamma(a,b) \text{ undefined}, \forall \sigma, \theta \in (0,1)\}.$$

3.3.2. *Graph Model*

As for pr BPA(A) and pr PA(A), we provide a bisimulation model for $pr\,\text{ACP}_I^-(A) \cup pr\,\text{AX}(\gamma)$ and prove completeness for finite processes. Similar to the nonprobabilistic case, our model uses labels from A_δ and is parameterized by γ. We will thus be working with $pr\,\mathcal{APG}(A_\delta, N, \gamma)$, $pr\,\mathcal{APG}(A_\delta, N, \gamma)/\cong$, and $pr\,\mathcal{APG}(A_\delta, N, \gamma)/\underline{\leftrightarrow}^{pr}_\delta$, with $\underline{\leftrightarrow}^{pr}_\delta$ defined below.

We begin with the definition of the $pr\,\text{ACP}_I^-(A)$ operators on probabilistic process graphs, and for this purpose we need to introduce a "normalization factor" to be used in computing conditional probabilities in a restricted process.

Definition 3.7. Let $g = \langle V, r, \mu \rangle$ 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

$$\nu_H(v) = 1 - \sum \{\mu(v, a, v') \mid a \in H_\delta, v' \in V\}.$$

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. In the following, let initials$(v) = \{a \in A_\delta \mid \exists v'\ \mu(v, a, v') > 0\}$ for v a probabilistic process graph node, and let the empty summation of probabilities be 0.

Definition 3.8. Let $G_1, G_2 \in pr\,\mathcal{APG}(A_\delta, N, \gamma)/\cong$ and let $g_1 \in G_1$ and $g_2 \in G_2$ be representatives such that $g_1 = \langle V_1, r_1, \mu_1 \rangle$, $g_2 = \langle V_2, r_2, \mu_2 \rangle$, $V_1 \cap V_2 = \varnothing$, and $N - (V_1 \cup V_2)$ is infinite. The operators δ, $\parallel_{\sigma,\theta}$, $⫡_{\sigma,\theta}$, $\mid_{\sigma,\theta}$, ∂_H, $H \subseteq A$, and I are defined on $pr\,\mathcal{APG}(A_\delta, N, \gamma)/\cong$ as follows:

δ: The representative probabilistic process graph for δ is given by $\langle \{r, v\}, r, \mu \rangle$, where $r, v \in N$, $r \neq v$, and $\mu(r, \delta, v) = 1$ is the only transition with nonzero probability.

$G_1 \parallel_{\sigma,\theta} G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \mu \rangle$ where for all $a \in A_\delta$, $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} \sigma \cdot \theta \cdot \mu_1(v_1, a, v_1') & \text{if } \neg\text{endpoint}(v_2) \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-\sigma) \cdot \theta \cdot \mu_2(v_2, a, v_2') & \text{if } \neg\text{endpoint}(v_1) \\ \mu_2(v_2, a, v_2') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1', v_2')) = (1-\theta) \cdot \sum_{b, c:\, \gamma(b,c) = a} \mu_1(v_1, b, v_1') \cdot \mu_2(v_2, c, v_2').$$

We refer to this particular representative as $g_1 \parallel_{\sigma,\theta} g_2$.

$G_1 ⫡_{\sigma,\theta} G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \mu \rangle$ 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 $v_2 \neq r_2$

$$\mu((v_1, v_2), a, (v_1', v_2)) = \begin{cases} \sigma \cdot \theta \cdot \mu_1(v_1, a, v_1') & \text{if } \neg\text{endpoint}(v_2) \\ \mu_1(v_1, a, v_1') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v_2')) = \begin{cases} (1-\sigma) \cdot \theta \cdot \mu_2(v_2, a, v_2') & \text{if } \neg\text{endpoint}(v_1) \\ \mu_2(v_2, a, v_2') & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1', v_2')) = (1-\theta) \cdot \sum_{b, c:\, \gamma(b,c) = a} \mu_1(v_1, b, v_1') \cdot \mu_2(v_2, c, v_2')$$

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

We refer to this particular representative as $g_1 \mathbin{\|\!\lfloor}_{\sigma,\theta} g_2$.

$G_1 \mid_{\sigma,\theta} G_2$: A representative is $\langle V_1 \times V_2, (r_1, r_2), \mu \rangle$ where for all $a \in A_\delta$, $v_1, v'_1 \in V_1$, $v_2, v'_2 \in V_2$

- $\mu((r_1, r_2), a, (v'_1, v'_2)) = \sum_{b,c:\, b \mid_{\sigma,\theta} c = a} \mu_1(r_1, b, v'_1) \cdot \mu_2(r_2, c, v'_2)$
- if $v_1 \neq r_1$ or $v_2 \neq r_2$

$$\mu((v_1, v_2), a, (v'_1, v_2)) = \begin{cases} \sigma \cdot \theta \cdot \mu_1(v_1, a, v'_1) & \text{if } \neg\text{endpoint}(v_2) \\ \mu_1(v_1, a, v'_1) & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v_1, v'_2)) = \begin{cases} (1-\sigma) \cdot \theta \cdot \mu_2(v_2, a, v'_2) & \text{if } \neg\text{endpoint}(v_1) \\ \mu_2(v_2, a, v'_2) & \text{otherwise} \end{cases}$$

$$\mu((v_1, v_2), a, (v'_1, v'_2)) = (1-\theta) \cdot \sum_{b,c:\, \gamma(b,c) = a} \mu_1(v_1, b, v'_1) \cdot \mu_2(v_2, c, v'_2)$$

- if $(v'_1 \neq r_1$ and $v'_2 = r_2)$ or $(v'_1 = r_1$ and $v'_2 \neq r_2)$ $\mu((r_1, r_2), a, (v'_1, v'_2)) = 0$.

We refer to this particular representative as $g_1 \mid_{\sigma,\theta} g_2$.

$\partial_H(G_1)$: A representative is $\langle V_1, r_1, \mu \rangle$ where, for all $a \in A$, $v, v' \in V_1$,

- if initials$(v) \subseteq H_\delta$

$$\mu(v, a, v') = 0$$
$$\mu(v, \delta, v') = \sum_{a \in A_\delta} \mu_1(v, a, v')$$

- if initials$(v) \not\subseteq H_\delta$

$$\mu(v, a, v') = \begin{cases} 0 & \text{if } a \in H_\delta \\ \mu_1(v, a, v')/\nu_H(v) & \text{otherwise.} \end{cases}$$

We refer to this particular representative as $\partial_H(g_1)$.

$I(g_1)$: gives the set of actions initials(r_1).

Similarly to the case of pr PA(A), the first and third clauses of the definitions of $g_1 \mathbin{\|\!\lfloor}_{\sigma,\theta} g_2$ and $g_1 \mid_{\sigma,\theta} g_2$ collectively define the transition distribution function μ on all transitions from the root (r_1, r_2). Also note that in the definition of $\partial_H(g_1)$, division by the normalization factor $\nu_H(v)$ occurs only when initials$(v) \not\subseteq H_\delta$, which ensures that $\nu_H(v) > 0$.

Processes are still stochastic in the graph model of pr ACP$_I^-(A) \cup pr$ AX(γ) if the probability of δ-transitions is taken into account. On the other hand, one may prefer the "substochastic" interpretation that a process like $a +_{1/2} \delta$ performs an a-transition (after which it successfully terminates) with probability $\frac{1}{2}$, but may also do nothing (deadlock) with probability $\frac{1}{2}$. However, the process $\partial_\varnothing(a +_{1/2} \delta)$ never deadlocks and is equivalent to a.

Unlike the nonprobabilistic case, the presence of δ-edges does not require a new definition of probabilistic bisimulation. This is because the second condition of Definition 3.2, which pertains to actions a in A only, implies that $\mu_1(v, \delta, V_1) = \mu_2(w, \delta, V_2)$. That is, probabilistically bisimilar nodes must perform the action δ with the same total probability, without regard to where the δ-transitions lead. This is exactly the constraint we would like to impose on δ-transitions.

To remind ourselves that we are working in a model with δ-transitions, and to maintain notational consistency with the nonprobabilistic setup, we use $\leftrightarrows_\delta^{pr}$ to denote probabilistic bisimulation in the graph model $pr\,\mathcal{APG}(A_\delta, N, \gamma)$.

In order to prove that $\leftrightarrows_\delta^{pr}$ is a congruence in pr ACP$_I^-(A)$, we need the following proposition to facilitate our reasoning that $\leftrightarrows_\delta^{pr}$ respects restriction.

PROPOSITION 3.5. *Let $g_1 = \langle V_1, r_1, \mu_1 \rangle$ and $g_2 = \langle V_2, r_2, \mu_2 \rangle$ such that $g_1 \leftrightarrows_\delta^{pr} g_2$, and let $\mathcal{R}$ be a probabilistic δ-bisimulation between g_1 and g_2 with $(v, w) \in \mathcal{R}$. Then:*

1. $\mu_1(v, a, V_1) = \mu_2(w, a, V_2)$, $a \in A_\delta$, $v \in V_1$, $w \in V_2$
2. $\mu_1(w, a, V_1) = \mu_2(v, a, V_2)$, $a \in A_\delta$, $w \in V_1$, $v \in V_2$
3. initials(v) = initials(w)
4. $\nu_H(v) = \nu_H(w)$, $H \subseteq A$.

Proof. For $a = \delta$, results (1) and (2) follow immediately from Definition 3.2. For $a \neq \delta$, (1) is easily deduced from Definition 3.2 as $\mu_1(v, a, S \cap V_1) = \mu_2(w, a, S \cap V_2)$ for all equivalence classes S of the partition of $V_1 \cup V_2$ induced by $\mathcal{R}$. Likewise for (2). Results (3) and (4) are simple consequences of (1) and (2). ∎

PROPOSITION 3.6. *If $G_1 \leftrightarrows_\delta^{pr} G_2$, then $G \|_{\sigma,\theta} G_1 \leftrightarrows_\delta^{pr} G \|_{\sigma,\theta} G_2$, $G \mathbin{\|\!\lfloor}_{\sigma,\theta} G_1 \leftrightarrows_\delta^{pr} G \mathbin{\|\!\lfloor}_{\sigma,\theta} G_2$, $G_1 \mathbin{\|\!\lfloor}_{\sigma,\theta} G \leftrightarrows_\delta^{pr} G_2 \mathbin{\|\!\lfloor}_{\sigma,\theta} G$, $G \mid_{\sigma,\theta} G_1 \leftrightarrows_\delta^{pr} G \mid_{\sigma,\theta} G_2$, $\partial_H(G_1) \leftrightarrows_\delta^{pr} \partial_H(G_2)$, for all $H \subseteq A$, and $I(G_1) = I(G_2)$.*

Proof. The proof for $\|_{\sigma,\theta}$ is similar to the proof for $\|_\sigma$ in Proposition 3.4. Let $a \neq \delta$. The a-transitions of nonzero probability stemming from (v, v_1) are now of the form:

1. $\mu_1^{\|}((v, v_1), a, [(v', v_1)]_{\mathcal{R}'}) = \sigma \cdot \theta \cdot \mu(v, a, v')$
2. $\mu_1^{\|}((v, v_1), a, [(v, v'_1)]_{\mathcal{R}'}) = (1-\sigma) \cdot \theta \cdot \mu_1(v_1, a, [v'_1]_{\mathcal{R}} \cap V_1)$
3. $\mu_1^{\|}((v, v_1), a, [(v', v'_1)]_{\mathcal{R}'}) = (1-\theta) \cdot \sum_{b,c:\, \gamma(b,c) = a} \mu(v, b, v') \cdot \mu_1(v_1, c, [v'_1]_{\mathcal{R}} \cap V_1)$
4. $\mu_1^{\|}((v, v_1), \delta, V \times V_1) = \sigma \cdot \theta \cdot \mu(v, \delta, V) + (1-\theta) \cdot \sum_{b,c:\, \gamma(b,c) = \delta} \mu(v, b, V) \cdot \mu_1(v_1, c, V_1) + (1-\sigma) \cdot \theta \cdot \mu_1(v_1, \delta, V_1)$.

The argument for the first two types of transitions is virtually identical to the argument set forth in Proposition 3.4. For the third type, since $g_1 \leftrightarrow_\delta^{pr} g_2$, $\mu_1^{\|}((v, v_1), a, [(v', v_1')]_{\mathscr{R}'}) = \mu_2^{\|}((v, v_2), a, [(v', v_1')]_{\mathscr{R}'})$. The arguments for the first three cases collectively are sufficient for the fourth case and we are done. As in Proposition 3.4, the argument is similar if v_1 or v is an endpoint.

Again, as in Proposition 3.4, the proofs for $\|\!\!\_{\sigma,\theta}$ and $|_{\sigma,\theta}$ follow reasoning similar to, if not simpler than, the proof of $\|_{\sigma,\theta}$. In particular, there are fewer transitions of nonzero probability from (r, r_1) and (r, r_2) since such transitions can come from g only, in the case of probabilistic left-merge, and from communications between g, g_1 or g, g_2 only, in the case of probabilistic communication merge.

For the case of restriction, assume $G_1 \leftrightarrow_\delta^{pr} G_2$ and let $g_1 = \langle V_1, r_1, \mu_1 \rangle$, and $g_2 = \langle V_2, r_2, \mu_2 \rangle$ be arbitrary representatives of G_1 and G_2, respectively. Further, let $\mathscr{R}$ be a probabilistic δ-bisimulation between g_1 and g_2. We show that $\mathscr{R}$ is also a probabilistic δ-bisimulation between $\partial_H(g_1)$ and $\partial_H(g_2)$, $H \subseteq A$. Let $(v_1, v_2) \in \mathscr{R}$ with $v_1 \in V_1$, $v_2 \in V_2$ and let μ_i^{∂} be the transition distribution function of $\partial_H(g_i)$, $i = 1, 2$. If initials$(v_1) \subseteq H_\delta$ then, by Proposition 3.5, initials$(v_2) \subseteq H_\delta$ and therefore $\mu_1^{\partial}(v_1, \delta, V_1)$, $\mu_2^{\partial}(v_2, \delta, V_2) = 1$. Otherwise, $\mu_1^{\partial}(v_1, a, V_1), \mu_2^{\partial}(v_2, a, V_2) = 0$, if $a \in H_\delta$; and for all $S \in (V_1 \cup V_2)/\mathscr{R}$, $\mu_1^{\partial}(v_1, a, S \cap V_1)$, $\mu_2^{\partial}(v_2, a, S \cap V_2) = \mu_1(v_1, a, S \cap V_1)/\nu_H(v_1)$, if $a \notin H_\delta$. This last step is a consequence of the fact that $(v_1, v_2) \in \mathscr{R}$ and Proposition 3.5, part (4). A symmetric argument, with the roles of v_1 and v_2 reversed, completes the proof for restriction.

That $\leftrightarrow_\delta^{pr}$ respects operator I follows directly from part (3) of Proposition 3.5. ∎

THEOREM 3.3.

1. *pr* $\mathscr{APG}(A_\delta, N, \gamma)/\leftrightarrow_\delta^{pr} \models$ *pr* $\mathrm{ACP}_I^-(A) \cup$ *pr* $\mathrm{AX}(\gamma)$
2. *For all closed expressions p, q over $\Sigma($pr $\mathrm{ACP}_I^-(A))$:*

$$pr\ \mathscr{APG}(A_\delta, N, \gamma)/\leftrightarrow_\delta^{pr} \models p = q$$
$$\Rightarrow pr\ \mathrm{ACP}_I^-(A) \cup pr\ \mathrm{AX}(\gamma) \vdash p = q.$$

Proof. For part 1, the proof of soundness of axiom (*pr* A7) is a simple extension of the soundness argument for (A7) (Theorem 2.2). Axioms (*pr* C1–3) and those of *pr* AX(γ) are merely postulated about the communication merge $|_{\sigma,\theta}$. The soundness of the rest of the axioms of *pr* $\mathrm{ACP}_I^-(A)$ rests on probabilistic process graph isomorphism arguments (the remarks given in the soundness part of the proofs of Theorems 2.2 and 3.3 are relevant with the obvious extensions).

Note that the condition to (*pr* D3.1) implies that $\nu_H(r_x) = 0$ and the condition to (*pr* D3.2) implies that $\nu_H(r_{x+_\pi y}) = 1$ and $\nu_H(r_x)$, $\nu_H(r_y) = 1$. The soundness of these axioms now easily follows. As alluded to in Section 2.3, unlike (D3.2), (*pr* D3.2) is not sound under the weaker condition

$$I(x) - H_\delta \neq \varnothing \quad \text{and} \quad I(y) - H_\delta \neq \varnothing$$

(for example, consider $x = a +_{1/2} b$, $y = c$, $H = \{a\}$, and $\pi = \frac{2}{3}$). This situation is closely related to the fact that the equivalence induced on the stratified model of probabilistic processes via abstraction to the generative model is not a congruence; in particular, it fails to respect restriction [vGSST90].

For part 2, the proof is analogous to the completeness proof of $\mathrm{ACP}_I^-(A)$.

- The definition of a probabilistic basic term uses $+_\pi$ instead of $+$.
- The term rewriting system *pr* $\mathrm{RACP}_I^-(A) \cup$ *pr* $\mathrm{RAX}(\gamma)$ uses the probabilistic counterparts of the rules in $\mathrm{RACP}_I^-(A) \cup \mathrm{RAX}(\gamma)$ and the normal form is defined analogously as well. For example, *pr* $\mathrm{RACP}_I^-(A)$ contains the rule *pr* C0′,

$$a \,|_{\sigma,\theta}\, b = c \quad \Rightarrow \quad a \,|_{\sigma,\theta}\, b \to c$$

- The proof that a probabilistic normal form is also a probabilistic basic term proceeds as before—no rule in *pr* $\mathrm{RACP}_I^-(A) \cup$ *pr* $\mathrm{RAX}(\gamma)$ is conditional with respect to any probability.
- *pr* $\mathrm{RACP}_I^-(A) \cup$ *pr* $\mathrm{RAX}(\gamma)$ is strongly normalizing modulo (*pr* A1), (*pr* A2), (*pr* A2′): take a *pr* $\mathrm{RACP}_I^-(A) \cup$ *pr* $\mathrm{RAX}(\gamma)$ reduction and erase all probability subscripts. One obtains a valid $\mathrm{RACP}_I^-(A) \cup \mathrm{RAX}(\gamma)$ reduction.
- The "elimination theorem" for closed *pr* $\mathrm{ACP}_I^-(A)$ terms is also similar. Let p be a closed *pr* $\mathrm{ACP}_I^-(A)$ term and let $\bar{p}$ be the closed $\mathrm{ACP}_I^-(A)$ term obtained by erasing all probability subscripts. Now let

$$\bar{p} = t_0 \to t_1 \to \cdots \to t_n$$

be a normalizing reduction of $\bar{p}$. This reduction can be decorated appropriately with probabilities to obtain a *pr* $\mathrm{RACP}_I^-(A) \cup$ *pr* $\mathrm{RAX}(\gamma)$ normalization of p. ∎

4. ACP_I^- AS AN ABSTRACTION OF *pr* ACP_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 ϕ from probabilistic process graphs to nonprobabilistic process graphs that preserves the structure of the bisimulation congruence classes. For the latter, we exhibit a homomorphism Φ from *pr* $\mathrm{ACP}_I^-(A)$ terms to $\mathrm{ACP}_I^-(A)$ terms that preserves the validity of equational reasoning.

4.1. Graph Model Homomorphism

Recall (Definition 3.3) the mapping $\phi: pr\ \mathscr{PG}(A, N) \to pr\ \mathscr{PG}(A, N)$ from probabilistic process graphs to nonprobabilistic ones. The defining property for ϕ is

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

and ϕ adapts to $pr\ \mathscr{APG}(A_\delta, N, \gamma)$ without modification.

PROPOSITION 4.1. *Let $g_a \in pr\ \mathscr{APG}(A_\delta, N, \gamma)$ be a representative probabilistic process graph, up to isomorphism, of $a \in A_\delta$, and similarly let $g'_a \in \mathscr{APG}(A_\delta, N, \gamma)$ be a representative (nonprobabilistic) process graph of a. Further, let g_1, g_2 be elements of $pr\ \mathscr{APG}(A_\delta, N, \gamma)$.*

$$\phi(g_a) = g'_a$$
$$\phi(g_1 \cdot g_2) = \phi(g_1) \cdot \phi(g_2)$$
$$\phi(g_1 +_\pi g_2) = \phi(g_1) + \phi(g_2)$$
$$\phi(g_1 \mid_{\sigma,\theta} g_2) = \phi(g_1) \mid \phi(g_2)$$
$$\phi(g_1 \parallel_{\sigma,\theta} g_2) = \phi(g_1) \parallel \phi(g_2)$$
$$\phi(g_1 \mathbin{\|\!\_}_{\sigma,\theta} g_2) = \phi(g_1) \mathbin{\|\!\_} \phi(g_2)$$
$$\phi(\partial_H(g_1)) = \partial_H(\phi(g_1))$$

PROPOSITION 4.2. *The mapping ϕ preserves the structure of the bisimulation congruence classes. That is,*

$$g_1 \leftrightarrows_\delta^{pr} g_2 \Rightarrow \phi(g_1) \leftrightarrows_\delta \phi(g_2).$$

Proof. Let $g_1 = \langle V_1, r_1, \mu_1 \rangle$, $g_2 = \langle V_2, r_2, \mu_2 \rangle$ be probabilistic process graphs, and let $\phi(g_1) = \langle V_1, r_1, \to_1 \rangle$ and $\phi(g_2) = \langle V_2, r_2, \to_2 \rangle$ be their homomorphic images under ϕ. Further, let $\mathscr{R} \subseteq (V_1 \cup V_2) \times (V_1 \cup V_2)$ be a probabilistic bisimulation containing (r_1, r_2). That is, $g_1 \leftrightarrows_\delta^{pr} g_2$. Now let (v, w) be an arbitrary pair in $\mathscr{R}$ such that $v \in V_1$, $w \in V_2$ and assume for some $v' \in V_1$, $a \in A$ that $\mu_1(v, a, v') > 0$. By Definition 3.3, $v \xrightarrow{a}_1 v'$. Then $\mu_1(v, a, [v']_\mathscr{R} \cap V_1) > 0$. Since $(v, w) \in \mathscr{R}$, then there exists a $w' \in [v']$ with $\mu_2(r_2, a, w') > 0$; i.e., $\mathscr{R}(v', w')$ and, by Definition 3.3 again, $r_2 \xrightarrow{a}_2 w'$. By a symmetric argument and by considering the case $a = \delta$ (which is simpler), we have as desired that $g_1 \leftrightarrows_\delta^{pr} g_2 \Rightarrow \phi(g_1) \leftrightarrows_\delta \phi(g_2)$. ∎

So it follows that ϕ induces a homomorphism $(\phi): pr\ \mathscr{APG}(A_\delta, N, \gamma)/\leftrightarrows_\delta^{pr} \to \mathscr{APG}(A_\delta, N, \gamma)/\leftrightarrows_\delta$. The converse of this result is clearly not true, e.g., $a + b \leftrightarrows_\delta b + a$ but $a +_{1/2} b \not\leftrightarrows_\delta^{pr} b +_{1/3} a$. Thus, the graph model $\mathscr{APG}(A_\delta, N, \gamma)/\leftrightarrows_\delta$ of $\text{ACP}_I^-(A)$ is strictly more abstract than the probabilistic graph model $pr\ \mathscr{APG}(A_\delta, N, \gamma)/\leftrightarrows_\delta^{pr}$ of $pr\ \text{ACP}_I^-(A)$.

4.2. Equational Theory Homomorphism

Let $\mathscr{L}(E)$ be the language of all terms, open and closed, generated by the signature of the equational specification E. The homomorphism Φ: $\mathscr{L}(pr\ \text{ACP}_I^-(A)) \to \mathscr{L}(\text{ACP}_I^-(A))$ from $pr\ \text{ACP}_I^-(A)$ terms to $\text{ACP}_I^-(A)$ terms, is defined as follows:

$$\Phi(a) = a, \quad a \in A_\delta$$
$$\Phi(x) = x$$
$$\Phi(x \cdot y) = \Phi(x) \cdot \Phi(y)$$
$$\Phi(x +_\pi y) = \Phi(x) + \Phi(y)$$
$$\Phi(x \mid_{\sigma,\theta} y) = \Phi(x) \mid \Phi(y)$$
$$\Phi(x \parallel_{\sigma,\theta} y) = \Phi(x) \parallel \Phi(y)$$
$$\Phi(x \mathbin{\|\!\_}_{\sigma,\theta} y) = \Phi(x) \mathbin{\|\!\_} \Phi(y)$$
$$\Phi(\partial_H(x)) = \partial_H(\Phi(x))$$

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

PROPOSITION 4.3. *Let t_1, t_2 be terms of $pr\ \text{ACP}_I^-(A)$, i.e., $t_1, t_2 \in \mathscr{L}(pr\ \text{ACP}_I^-(A))$.*

$$\frac{pr\ \text{ACP}_I^-(A) \cup pr\ \text{AX}(\gamma) \vdash t_1 = t_2}{\text{ACP}_I^-(A) \cup \text{AX}(\gamma) \vdash \Phi(t_1) = \Phi(t_2)}$$

Proof. The proof is by induction on the length of the $pr\ \text{ACP}_I^-(A) \cup pr\ \text{AX}(\gamma)$ proof, using the observation that, for every $pr\ \text{ACP}_I^-(A) \cup pr\ \text{AX}(\gamma)$ axiom of the form $c \Rightarrow t_1 = t_2$, its homomorphic image $\Phi(c) \Rightarrow \Phi(t_1) = \Phi(t_2)$ is an $\text{ACP}_I^-(A) \cup \text{AX}(\gamma)$ axiom. Here c is a possibly empty condition on the validity of the $pr\ \text{ACP}_I^-(A) \cup pr\ \text{AX}(\gamma)$ axiom, and the fact that $\Phi(c)$ is equal to the condition of the corresponding $\text{ACP}_I^-(A) \cup \text{AX}(\gamma)$ axiom means that no axiom of $pr\ \text{ACP}_I^-(A) \cup pr\ \text{AX}(\gamma)$ is conditional on a probability appearing within a $pr\ \text{ACP}_I^-(A)$ term. ∎

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

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 $\text{ACP}_I^-(A)$, in which A6 is rejected. $\text{ACP}_I^-(A)$ is, in essence, a minor alteration of ACP expressing almost the same process identities on finite processes.

Our end result is the axiom system $pr\ \text{ACP}_I^-(A)$, which can be seen as a probabilistic extension of $\text{ACP}_I^-(A)$ for generative processes featuring a probabilistic asynchronous interleaving operator. In particular, $\mathrm{ACP}_I^-(A)$ is homomorphically derivable from $pr\,\mathrm{ACP}_I^-(A)$. As desired, we showed that $pr\,\mathrm{ACP}_I^-(A) \cup pr\,\mathrm{AX}(\gamma)$ constitutes a complete axiomatization of Larsen and Skou's probabilistic bisimulation for finite processes.

It is easy to describe a form of iteration in our setting. The defining axiom is:

$$X^{*_\pi} \cdot Y = X \cdot (X^{*_\pi} \cdot Y) +_\pi Y$$

thus following the recursion equation for binary Kleene star [Kle56] as well as the approach put forth in [BBP94] for incorporating iteration into ACP. We remark that $*^\pi$ can be modeled in $pr\,\mathcal{APG}(A_\delta, N, \gamma)/\underline{\leftrightarrow}_\delta^{pr}$ by unfolding the recursive definition. The problem of axiomatizing $pr\,\mathrm{BPA}(A)$ plus iteration is open.

Another open problem concerns the axiomatization of the *stratified* model 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 weakening the condition to (pr D3.2) as discussed in the soundness part of the proof of Theorem 3.3, the desired axiomatization can be obtained.

APPENDIX: PROOFS OF LEMMAS 3.1 AND 3.2

LEMMA 3.1. *For any permutation ξ of $\{1, ..., n\}$, $n \geqslant 2$,*

$$pr\,\mathrm{BPA}(A) \vdash \sum_{i=1}^{n} [\pi_i]\, x_i = \sum_{i=1}^{n} [\pi_{\xi(i)}]\, x_{\xi(i)}$$

Proof. The proof is by induction on n. All nonannotated steps are assumed to follow directly from the definition of summation form notation.

- Basis: $n = 2$

We prove the nontrivial case where $\xi(1) = 2$, $\xi(2) = 1$.

$$\begin{aligned}\sum_{i=1}^{2} [\pi_i]\, x_i &= x_1 +_{\pi_1} \sum_{i=1}^{1} \left[\frac{\pi_{i+1}}{1-\pi_1}\right] x_{i+1} \\ &= x_1 +_{\pi_1} x_2 \\ &= x_2 +_{\pi_2} x_1 \qquad (pr\ \mathrm{A1}) \\ &= x_2 +_{\pi_2} \sum_{i=1}^{1} \left[\frac{\pi_i}{1-\pi_2}\right] x_i \\ &= \sum_{i=1}^{2} [\pi_{\xi(i)}]\, x_{\xi(i)}\end{aligned}$$

- Hypothesis: suppose the lemma holds for $n \leqslant k$.
- Induction: $n = k+1$

If $\xi(1) = 1$, then we have

$$\begin{aligned}\sum_{i=1}^{k+1} [\pi_i]\, x_i &= x_1 +_{\pi_1} \sum_{i=1}^{k} \left[\frac{\pi_{i+1}}{1-\pi_1}\right] x_{i+1} \\ &= x_1 +_{\pi_1} \sum_{i=1}^{k} \left[\frac{\pi_{\xi(i+1)}}{1-\pi_1}\right] x_{\xi(i+1)} \qquad \text{(induction)} \\ &= \sum_{i=1}^{k+1} [\pi_{\xi(i)}]\, x_{\xi(i)}\end{aligned}$$

If $\xi(1) = j \neq 1$, then

$$\sum_{i=1}^{k+1} [\pi_i]\, x_i$$

$$= x_1 +_{\pi_1} \sum_{i=1}^{k} \left[\frac{\pi_{i+1}}{1-\pi_1}\right] x_{i+1}$$

$$= x_1 +_{\pi_1} \sum_{i=1}^{k} \left[\frac{\pi_{\xi'(i+1)}}{1-\pi_1}\right] x_{\xi'(i+1)}$$

(induction)

where ξ' is any permutation from 2 to $n+1$ with $\xi'(2) = j$

$$= x_1 +_{\pi_1} \left(x_j +_{\pi_j/(1-\pi_1)} \sum_{i=1}^{k-1} \left[\frac{\pi_{\xi'(i+2)}}{1-\pi_1-\pi_j}\right] x_{\xi'(i+2)} \right)$$

$$= x_1 +_{\pi_1} \left(\sum_{i=1}^{k-1} \left[\frac{\pi_{\xi'(i+2)}}{1-\pi_1-\pi_j}\right] x_{\xi'(i+2)} +_{(1-\pi_1-\pi_j)/(1-\pi_1)} x_j \right)$$

(pr A1)

$$= \left(x_1 +_{\pi_1/(1-\pi_j)} \sum_{i=1}^{k-1} \left[\frac{\pi_{\xi'(i+2)}}{1-\pi_1-\pi_j}\right] x_{\xi'(i+2)} \right) +_{1-\pi_j} x_j$$

(pr A2)

$$= x_j +_{\pi_j} \left(x_1 +_{\pi_1/(1-\pi_j)} \sum_{i=1}^{k-1} \left[\frac{\pi_{\xi'(i+2)}}{1-\pi_1-\pi_j}\right] x_{\xi'(i+2)} \right)$$

(pr A1)

$$= x_j +_{\pi_j} \left(y_1 +_{\rho_1} \sum_{i=1}^{k-1} \left[\frac{\rho_{i+1}}{1-\rho_1}\right] y_{i+1} \right)$$

where $y_1 = x_1$, $\rho_1 = \dfrac{\pi_1}{1-\pi_j}$,

for $1 \leqslant i \leqslant k-1$, $y_{i+1} = x_{\xi'(i+2)}$, $\rho_{i+1} = \dfrac{\pi_{\xi'(i+2)}}{1-\pi_j}$

$$= x_j +_{\pi_j} \sum_{i=1}^{k} [\rho_i]\, y_i$$

$$= x_j +_{\pi_j} \sum_{i=1}^{k} [\rho_{\xi''(i)}]\, y_{\xi''(i)}$$

(induction)

where ξ'' is the permutation of 1 to k with

$$y_{\xi''(i)} = x_{\xi(i+1)} \text{ and } \rho_{\xi''(i)} = \frac{\pi_{\xi(i+1)}}{1-\pi_j}$$

$$= x_j +_{\pi_j} \sum_{i=1}^{k} \left[\frac{\pi_{\xi(i+1)}}{1-\pi_j}\right] x_{\xi(i+1)}$$

$$= \sum_{i=1}^{k+1} [\pi_{\xi(i)}]\, x_{\xi(i)}. \quad \blacksquare$$

LEMMA 3.2. *In the summation form* $\sum_{i=1}^{n+1} [\pi_i]\, x_i$, *let* x_1 *and* x_2 *be syntactically identical. Then*

$$pr\,\mathrm{BPA}(A) \vdash \sum_{i=1}^{n+1} [\pi_i]\, x_i = \sum_{i=1}^{n} [\rho_i]\, y_i,$$

where $\rho_1 = \pi_1 + \pi_2$, $y_1 = x_1$, *and* $\rho_i = \pi_{i+1}$, $y_i = x_{i+1}$, $2 \leqslant i \leqslant n$.

Proof. There are two cases; all nonannotated steps are assumed to follow directly from the definition of summation form notation. If $n = 1$, then we have:

$$\sum_{i=1}^{2} [\pi_i]\, x_i = x_1 +_{\pi_1} \sum_{i=1}^{1} \left[\frac{\pi_{i+1}}{1-\pi_1}\right] x_{i+1}$$

$$= x_1 +_{\pi_1} \sum_{i=1}^{1} \left[\frac{1-\pi_1}{1-\pi_1}\right] x_1$$

$$= x_1 +_{\pi_1} x_1$$

$$= x_1 \qquad (pr\ \mathrm{A3})$$

$$= \sum_{i=1}^{1} [\rho_i]\, y_i.$$

If $n \geqslant 2$, then we have:

$$\sum_{i=1}^{n+1} [\pi_i]\, x_i$$

$$= x_1 +_{\pi_1} \sum_{i=1}^{n} \left[\frac{\pi_{i+1}}{1-\pi_1}\right] x_{i+1}$$

$$= x_1 +_{\pi_1} \left(x_2 +_{\pi_2/(1-\pi_1)} \sum_{i=1}^{n-1} \left[\frac{\pi_{i+2}}{1-\pi_1-\pi_2}\right] x_{i+2} \right)$$

$$= (x_1 +_{\pi_1/(\pi_1+\pi_2)} x_1) +_{\pi_1+\pi_2} \sum_{i=1}^{n-1} \left[\frac{\pi_{i+2}}{1-\pi_1-\pi_2}\right] x_{i+2}$$

$(pr\ \mathrm{A2})$

$$= x_1 +_{\pi_1+\pi_2} \sum_{i=1}^{n-1} \left[\frac{\pi_{i+2}}{1-\pi_1-\pi_2}\right] x_{i+2}$$

$(pr\ \mathrm{A3})$

$$= y_1 +_{\rho_1} \sum_{i=1}^{n-1} \left[\frac{\rho_{i+1}}{1-\rho_1}\right] y_{i+1}$$

(given condition)

$$= \sum_{i=1}^{n} [\rho_i]\, y_i. \quad \blacksquare$$

ACKNOWLEDGMENTS

The authors gratefully acknowledge the anonymous referees and Rob van Glabbeek, Chi-Chang Jou, and Bernhard Steffen for their valuable comments.

Received September 16, 1992; final manuscript received November 29, 1994

REFERENCES

[BBP94] Bergstra, J. A., Bethke, I., and Ponse, A. (1994), "Process Algebra with Iteration and Nesting," Technical report, Programming Research Group, University of Amsterdam.

[BK84] Bergstra, J. A., and Klop, J. W. (1984), Process algebra for synchronous communication, *Inform. and Comput.* **60**, 109–137.

[BM89] Bloom, B., and Meyer, A. R. (1989), A remark on bisimulation between probabilistic processes, *in* "Logik at Botik" (Meyer and Tsailin, Eds.), Lecture Notes in Computer Science, Vol. 363, Springer-Verlag, Berlin/New York.

[BW90] Baeten, J. C. M., and Weijland, W. P. (1990), "Process Algebra" Cambridge Tracts in Computer Science, Vol. 18, Cambridge Univ. Press, London/New York.

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

[CSZ92] Cleaveland, R., Smolka, S. A., and Zwarico, A. E. (1992), Testing preorders for probabilistic processes, *in* "Proceedings of the 19th ICALP" (W. Kuich, Ed.), Lecture Notes in Computer Science, Vol. 623, Springer-Verlag, Berlin/New York.

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

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

[JS90] Jou, C.-C., and Smolka, S. A. (1990), Equivalences, congruences, and complete axiomatizations for probabilistic processes, *in* "Proceedings of CONCUR '90" (J. C. M. Baeten and J. W. Klop, Eds.), pp. 367–383, Lecture Notes in Computer Science, Vol. 458, Springer-Verlag, Berlin/New York.

[Kle56] Kleene, S. C. (1956), Representation of events in nerve nets and finite automata, *in* "Automata Studies," pp. 3–41, Princeton Univ. Press, Princeton, NJ.

[LS92a] Larsen, K. G., and Skou, A. (1992), Bisimulation through probabilistic testing, *Inform. and Comput.* **94**, 1–28; preliminary versions of this paper appeared as University of

Aalborg technical reports R 88-18 and R 88-29, and *in* "Proceedings of the 16th Annual ACM Symposium on Principles of Programming Languages, Austin, Texas, 1989."

[LS92b] Larsen, K. G., and Skou, A. (1992), Compositional verification of probabilistic processes, *in* "Proceedings of CONCUR '92," Lecture Notes in Computer Science, Springer-Verlag, Berlin/New York.

[Mil80] Milner, R. (1980), "A Calculus of Communicating Systems," Lecture Notes in Computer Science, Vol. 92, Springer-Verlag, Berlin/New York.

[Par81] Park, D. M. R. (1981), *Concurrency and automata on infinite sequences*, *in* "Proceedings of 5th G.I. Conference on Theoretical Computer Science," pp. 167–183, Lecture Notes in Computer Science, Vol. 104, Springer-Verlag, Berlin/New York.

[Tof90] Tofts, C. M. N. (1990), A synchronous calculus of relative frequency, *in* "Proceedings of CONCUR '90" (J. C. M. Baeten and J. W. Klop, Eds.), pp. 467–480, Lecture Notes in Computer Science, Vol. 458, Springer-Verlag, Berlin.

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