A Complete Axiom System for Finite-State Probabilistic Processes

Eugene W. Stark* and Scott A. Smolka†
Department of Computer Science
State University of New York at Stony Brook
Stony Brook, NY 11794-4400
USA

Abstract

A complete equational axiomatization of probabilistic bisimulation for finite-state probabilistic processes is presented. It extends Milner's complete axiomatization of regular behaviors, which appeared in Volume 28 of the *Journal of Computer and System Sciences* (1984).

1 Introduction

In [Mil84], Robin Milner presented a sound and complete equational axiomatization of strong bisimulation for a regular subset of CCS formed from the null process $\mathbf{0}$, process variables, action prefixing, process summation, and (possibly unguarded) recursion. He exhibited a close connection between such expressions and finite-state *charts*, bisimulation classes of which he referred to as *behaviors*.

In this paper, we extend Milner's results to a setting in which binary summations are of the form $E\ {}_p\!+\ E'$—meaning intuitively that expression E is chosen with probability p and expression E' with probability $1-p$—and in which probabilistic bisimulation [LS92] replaces strong bisimulation. The inference system we obtain is nearly identical to Milner's, differing only in the following two ways: axioms mentioning summation are decorated with probabilities in the appropriate way, and the unit law $E\ {}_p\!+\ \mathbf{0} = E$, which is not sound for probabilistic bisimulation, is absent.

In obtaining our complete axiomatization of probabilistic bisimulation, the following main technical contributions can be identified:

*Research supported in part by NSF grant CCR–9320846 and AFOSR grant F49620-96-1-0087.
†Research supported in part by NSF grant CCR–9505562 and AFOSR grants F49620-95-1-0508 and F49620-96-1-0087.

- Our operational semantics for probabilistic processes maintains a clear separation between the *transitions* a process may perform and the *probabilities* assigned to transitions. This is especially important in the presence of unguarded recursion, as can be seen by considering a process such as $P \stackrel{def}{=} \mathbf{fix}\ X.(a\mathbf{0}\ {}_{1/2}{+}\ X)$. Although P has only a single transition (an a-transition to $\mathbf{0}$), there are infinitely many ways to infer this transition. Moreover, each such inference is associated with its own unique probability ($1/2,\ 1/4,\ 1/8,\ \ldots$), and the probability of P's a-transition is the (infinite) sum of these probabilities. Our recursive definition of transition probabilities formally captures each of the preceding intuitions.

- We present a direct generalization of Milner's *transition induction* proof technique, which we use to prove soundness of many of our axioms for probabilistic bisimulation. A similar technique was used in [vGSS95] to show that probabilistic bisimulation is a congruence.

- We provide a succinct characterization of the consequences of the axioms for probabilistic summation, which allows us to check the provability of probabilistic summation expressions (expressions built of variables and probabilistic summation only) "by inspection." That is, we show that two probabilistic summation expressions are provably equal if and only if the versions in which the probabilities are "erased" are provable in CCS, and the total probability assigned to a summand is the same in both expressions. (More general expressions, having probabilistic summation as the top-level operator, can also be accommodated through substitution.) Using this technique, we are able to avoid much of the tedious calculation of probabilities that would otherwise be necessary in a proof "from scratch" and, in the process, obtain a completeness proof whose structure closely mimics that of the corresponding proof in [Mil84].

The axiom system we study here was proposed in [**?**], where its soundness and completeness was also announced (for the class of probabilistic agents with *rational* probabilities labeling the summation operators). However, only a proof sketch was provided there in support of these results. Jou, in his unpublished dissertation [Jou92], gave more detailed arguments in support of the soundness and completeness results, which showed that the assumption of rational probabilities was not required. Our work on the present paper began simply as an attempt to improve the presentation of the proofs in [Jou92], which seemed overly complicated. However, close scrutiny of these proofs revealed apparent subtle circularities in the proofs of soundness for the congruence laws. We were not able to untangle these circularities and maintain the overall structure of Jou's arguments, so we were forced to look for a new way of doing these proofs. The result was our discovery of the probabilistic generalization of Milner's transition induction technique, which made the soundness proofs much simpler. The presentation of this technique is one of the main contributions of the present paper. We have also improved upon Jou's presentation of the completeness proof by avoiding the explicit calculation of probabilities in the construction of a characteristic system of equations for a probabilistic expression.

As a result of these innovations, though we still use a few technical lemmas from [Jou92], most of the proof presented here is new.

In other related work, complete axiomatizations of probabilistic bisimulation were given by Baeten et al. in [BBS95] in the context of the process algebra ACP [BK84] but without recursion.

The structure of the rest of the paper is as follows. Section 2 presents the syntax and structural operational semantics of probabilistic expressions. Probabilistic bisimulation is defined in Section 3. Section 4 presents our axioms for probabilistic bisimulation and proves soundness. Section 5 gives our characterization of the consequences of the probabilistic summation laws. Section 6 establishes the completeness of our axiom system. Section 7 contains some concluding remarks.

2 Syntax and Semantics of Probabilistic Expressions

This section presents the syntax and operational semantics of probabilistic expressions, our probabilistic extension of the class of expressions Milner considered in [Mil84]. We begin by supposing an infinite set $\mathrm{Var} = \{X_1, X_2, \ldots\}$ of *agent variables*, and a set Act of *atomic actions*.

The syntax of *probabilistic expressions* (PE for short) is defined as follows:

$$E ::= X \mid aE \mid E\ {}_p\!+ E' \mid \mathbf{fix}\ X.E \qquad (X \in \mathrm{Var}, a \in \mathrm{Act}, 0 < p < 1).$$

The notions of free and bound variables are defined in the standard way, and a variable X is *guarded* in expression E if every free occurrence of X in E is contained in a subexpression of the form aE'. We regard two expressions as syntactically identical if they are equal up to change of bound variables, and we use $\equiv$ to denote this relationship. We use the term *(probabilistic) agent* to refer to a PE expression with no free variables. PA is the class of agents, with P and Q ranging over PA. We use $\mathbf{0}$ as an abbreviation for the agent $\mathbf{fix}\ X.X$. In the sequel, if $p \in [0, 1]$, then $\overline{p}$ is used as an abbreviation for $1 - p$.

To define the operational semantics of PA, we first define, using standard structural operational semantics rules, the *transitions* of agents. These are given by the following axiom and inference rules:

$$aP \xrightarrow{a} P$$

$$\frac{P_1 \xrightarrow{a} Q}{P_1\ {}_p\!+ P_2 \xrightarrow{a} Q} \qquad\qquad \frac{P_2 \xrightarrow{a} Q}{P_1\ {}_p\!+ P_2 \xrightarrow{a} Q}$$

$$\frac{E\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} Q}{\mathbf{fix}\ X.E \xrightarrow{a} Q}$$

where only X is free in E.

Except for the probabilities decorating the + signs, these are the same as Milner's rules for regular CCS agents.

We incorporate probability into the operational semantics by associating, with each triple (P, a, Q) consisting of agents P and Q and action a, a *transition probability* $\mu(P, a, Q) \in [0, 1]$. That is, $\mu : \mathrm{PA} \times \mathrm{Act} \times \mathrm{PA} \to [0, 1]$. As a more suggestive notation, we shall write $\mu(P \xrightarrow{a} Q)$ instead of $\mu(P, a, Q)$. The function μ is defined to be the least fixed point of the recursive equation:

$$\mu = \mathcal{P}(\mu),$$

where $\mathcal{P}$ is defined as follows:

$$\mathcal{P}(\mu)(aP \xrightarrow{b} Q) = \begin{cases} 1, & \text{if } b = a \text{ and } P \equiv Q \\ 0, & \text{otherwise} \end{cases}$$

$$\mathcal{P}(\mu)(P_1 \,{}_p\!+ P_2 \xrightarrow{a} Q) = p \cdot \mu(P_1 \xrightarrow{a} Q) + \overline{p} \cdot \mu(P_2 \xrightarrow{a} Q)$$

$$\mathcal{P}(\mu)(\mathbf{fix}\ X.E \xrightarrow{a} Q) = \mu(E\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} Q)$$

where, again, only X is free in E.

It is easily verified that the interval $[0, 1]$ is a CPO under the usual ordering on the real numbers. This ordering induces a pointwise ordering on the set of all functions μ taking triples (P, a, Q) to $[0, 1]$, so that this set also is a CPO. Moreover, the mapping $\mathcal{P}$ is a continuous mapping from this CPO to itself, so that the claimed least fixed point actually exists. Let μ^0 be the identically zero function, and for $i \geq 0$ define $\mu^{i+1} = \mathcal{P}(\mu^i)$. We then have the usual characterization: $\mu = \sup_{i \geq 0} \mu^i$.

To illustrate the operational semantics of PA agents, consider once again the agent $P \stackrel{def}{=} \mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X)$. As discussed in the Introduction, P has a single inferable transition $t = P \xrightarrow{a} \mathbf{0}$, and there are infinitely many ways to infer it. By definition of μ, the $(n+1)$st approximation of $\mu(t)$ is given by:

$$\begin{aligned}
\mu^{n+1}(\mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0}) &= \mathcal{P}(\mu^n)(\mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0}) \\
&= \mu^n(a\mathbf{0} \,{}_{1/2}\!+ \mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0}) \\
&= \mathcal{P}(\mu^{n-1})(a\mathbf{0} \,{}_{1/2}\!+ \mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0}) \\
&= 1/2 \cdot \mu^{n-1}(a\mathbf{0} \xrightarrow{a} \mathbf{0}) + \\
&\qquad 1/2 \cdot \mu^{n-1}(\mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0}) \\
&= 1/2 \cdot 1 + 1/2 \cdot \mathcal{P}(\mu^{n-2})(\mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0}) \\
&\;\vdots \\
&= 1/2 + 1/4 + \cdots + 1/2^k + \\
&\qquad 1/2 \cdot \mathcal{P}(\mu^{n-2k})(\mathbf{fix}\ X.(a\mathbf{0} \,{}_{1/2}\!+ X) \xrightarrow{a} \mathbf{0})
\end{aligned}$$

if $n \geq 2k$. Thus, $\mu(t)$, the probability of t, is the infinite sum $1/2 + 1/4 + 1/8 + \cdots$, whose value is 1.

Lemma 2.1 $\mu(P \xrightarrow{a} Q) > 0$ *if and only if the transition* $P \xrightarrow{a} Q$ *is inferable from the SOS rules.*

Proof – A straightforward induction on i establishes that $\mu^i(P \xrightarrow{a} Q) > 0$ if and only if transition $P \xrightarrow{a} Q$ is inferable from the SOS rules by a proof tree of depth at most i. Then, since every transition is inferable by a finite proof, it follows immediately that if $P \xrightarrow{a} Q$ is inferable then $\mu(P \xrightarrow{a} Q) > 0$. Conversely, if $\mu(P \xrightarrow{a} Q) > 0$, then since $\mu = \sup_{i \geq 0} \mu^i$, we must have $\mu^i(P \xrightarrow{a} Q) > 0$ for some $i \geq 0$, from which it follows that $P \xrightarrow{a} Q$ is inferable from the SOS rules by a proof tree of depth at most i. ∎

The next result shows that probabilistic agents P are "sub-stochastic," in the sense that the total probability assigned to all transitions of P is less than or equal to one. If the total probability is a value p strictly less than one, then we regard the value $1 - p$ as a deadlock or stopping probability.

Proposition 2.2 *For any agent* P *and* $a \in \mathrm{Act}$,

$$\sum_{Q \in \mathrm{PA}} \mu(P \xrightarrow{a} Q) \leq 1.$$

Proof – We claim that for all agents P and all $i \geq 0$,

$$\sum_{Q \in \mathrm{PA}} \mu^i(P \xrightarrow{a} Q) \leq 1.$$

The result then follows from the claim. For

$$\begin{aligned}
\sum_{P \in \mathrm{PA}} \mu(P \xrightarrow{a} Q) &= \sup_{S \in \mathcal{F}(\mathrm{PA})} \sum_{Q \in S} \sup_{i \geq 0} \mu^i(P \xrightarrow{a} Q) \\
&= \sup_{S \in \mathcal{F}(\mathrm{PA})} \sup_{i \geq 0} \sum_{Q \in S} \mu^i(P \xrightarrow{a} Q) \\
&= \sup_{i \geq 0} \sup_{S \in \mathcal{F}(\mathrm{PA})} \sum_{Q \in S} \mu^i(P \xrightarrow{a} Q) \\
&= \sup_{i \geq 0} \sum_{Q \in \mathrm{PA}} \mu^i(P \xrightarrow{a} Q) \\
&\leq 1,
\end{aligned}$$

where $\mathcal{F}(\mathrm{PA})$ denotes the collection of all finite sets of PA agents.

The proof of the claim is by induction on i, and it can be regarded as a variant of Milner's transition induction technique. We will be using this technique repeatedly throughout the paper.

1. In case $i = 0$, the result is trivial.

2. Suppose we have shown the result for some $i \geq 0$, and consider the case of $i + 1$. We consider the possible syntactic forms of P.

- If P has the form aQ, then the only transition that can be inferred for P is the transition $P \xrightarrow{a} Q$, and in this case $\mu^{i+1}(P \xrightarrow{a} Q) = 1$ by definition of μ. Note that by Lemma 2.1, $\mu(P, a, Q') = 0$ for all $Q' \not\equiv Q$, since there is no inferable transition $P \xrightarrow{a} Q'$.
- If $P \equiv P_1 \;{}_p\!+ P_2$, then

$$\begin{aligned}
\sum_{Q \in \mathrm{PA}} \mu^{i+1}(P \xrightarrow{a} Q) &= \sum_{Q \in \mathrm{PA}} p \cdot \mu^i(P_1 \xrightarrow{a} Q) + \overline{p} \cdot \mu^i(P_2 \xrightarrow{a} Q) \\
&= p \cdot \sum_{Q \in \mathrm{PA}} \mu^i(P_1 \xrightarrow{a} Q) + \overline{p} \cdot \sum_{Q \in \mathrm{PA}} \mu^i(P_2 \xrightarrow{a} Q) \\
&\leq p + \overline{p} \\
&= 1,
\end{aligned}$$

  where the induction hypothesis was used to obtain the inequality in the third line.
- Suppose $P \equiv \textbf{fix } X.E$. Then

$$\sum_{Q \in \mathrm{PA}} \mu^{i+1}(P \xrightarrow{a} Q) = \sum_{Q \in \mathrm{PA}} \mu^i(E\{P/X\} \xrightarrow{a} Q),$$

  which is ≤ 1 by induction hypothesis.

∎

In view of the previous result, for any set $\mathcal{S}$ of PA agents and any action a, the summation

$$\sum_{Q \in \mathcal{S}} \mu(P \xrightarrow{a} Q)$$

converges to a value ≤ 1. We use the notation $\mu(P \xrightarrow{a} \mathcal{S})$ to denote this value.

3 Probabilistic Bisimulation

In this section, we define probabilistic bisimulation, Larsen and Skou's [LS92] probabilistic extension of strong bisimulation. We will subsequently completely axiomatize probabilistic bisimulation equivalence for probabilistic expressions.

A (strong) *bisimulation* is a binary relation $\mathcal{R}$ on agents that satisfies the following conditions:

1. Whenever $P \mathrel{\mathcal{R}} P'$ and $P \xrightarrow{a} Q$, then there exists a transition $P' \xrightarrow{a} Q'$, such that $Q \mathrel{\mathcal{R}} Q'$.
2. Whenever $P \mathrel{\mathcal{R}} P'$ and $P' \xrightarrow{a} Q'$, then there exists a transition $P \xrightarrow{a} Q$, such that $Q \mathrel{\mathcal{R}} Q'$.

A *probabilistic bisimulation* is an equivalence relation $\mathcal{R}$ on agents that satisfies the following condition:

- Whenever $P\ \mathcal{R}\ P'$, then for all actions a and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$ we have

$$\mu(P \xrightarrow{a} \mathcal{S}) = \mu(P' \xrightarrow{a} \mathcal{S}).$$

We call agents P and P' *bisimilar*, written $P \sim P'$, if there exists a bisimulation that relates them. Likewise, agents P and P' are *probabilistically bisimilar*, written $P \overset{\mathrm{pr}}{\sim} P'$ if there exists a probabilistic bisimulation that relates them. We assume familiarity with the standard results about bisimulation and probabilistic bisimulation; in particular that bisimilarity is an equivalence relation which is the largest bisimulation, and that probabilistic bisimilarity is the largest probabilistic bisimulation.

Bisimilarity and probabilistic bisimilarity are extended to the relations *bisimulation equivalence* and *probabilistic bisimulation equivalence* on all PE expressions as follows:

- Let E and F be expressions whose free variables are contained in the set $\widetilde{X}$, and let $\# \in \{\sim, \overset{\mathrm{pr}}{\sim}\}$. Then $E \# F$ if for all sets of agents $\widetilde{P}$, $E\{\widetilde{P}/\widetilde{X}\} \# F\{\widetilde{P}/\widetilde{X}\}$.

Unlike a bisimulation, a probabilistic bisimulation is required to be an equivalence relation on agents. Intuitively, the effect of this requirement is to ensure that agents P and Q are not distinguished from each other solely because P and Q have different sets of individual transitions to a set $\mathcal{S}$ of probabilistically indistinguishable agents. Rather, only the *total* probability of the sets of transitions from P to $\mathcal{S}$ and from Q to $\mathcal{S}$ should be used as a basis for distinguishing between P and Q. Adopting this convention permits the identification of agents like $(a(b\mathbf{0}\ _{3/4}\!+ c\mathbf{0})\ _{1/2}\!+ a(c\mathbf{0}\ _{1/4}\!+ b\mathbf{0}))\ _{2/3}\!+ d\mathbf{0}$ and $a(b\mathbf{0}\ _{3/4}\!+ c\mathbf{0})\ _{2/3}\!+ d\mathbf{0}$, which would otherwise be distinguished unnecessarily. The next proposition shows that certain bisimulations are also definable starting from equivalence relations.

Proposition 3.1 *An equivalence relation $\mathcal{R}$ on agents is a bisimulation if and only if whenever $P\ \mathcal{R}\ P'$, then for all actions a and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$ we have*

$$P \xrightarrow{a} \mathcal{S} \text{ if and only if } P' \xrightarrow{a} \mathcal{S},$$

where by $P \xrightarrow{a} \mathcal{S}$ we mean that $P \xrightarrow{a} Q$ is inferable for some $Q \in \mathcal{S}$ (and similarly for $P' \xrightarrow{a} \mathcal{S}$).

Proof – Straightforward from the definition of bisimulation. ∎

Proposition 3.2 *Suppose relation $\mathcal{R}$ is a probabilistic bisimulation. Then $\mathcal{R}$ is also a bisimulation. Thus, if $E \overset{\mathrm{pr}}{\sim} F$ then $E \sim F$.*

Proof – Straightforward using Lemma 2.1 and Proposition 3.1. ∎

Corollary 3.3 *If $E \overset{\text{pr}}{\sim} F$, then E and F have the same sets of free variables, and a free variable X occurs guarded (unguarded) in E if and only if it occurs guarded (unguarded) in F.*

Proof – If E and F are probabilistically equivalent, then they are bisimulation equivalent, and the stated properties hold for bisimulation equivalence. ∎

The following lemma about probabilistic bisimulation, which appeared originally in [Jou92], will be important for us:

Lemma 3.4 *Suppose $\mathcal{P}$ is a probabilistic bisimulation, and $\mathcal{R}$ is an arbitrary equivalence relation that contains $\mathcal{P}$. Then for all pairs of agents $(P, P') \in \mathcal{P}$, all actions a, and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$:*

$$\mu(P \xrightarrow{a} \mathcal{S}) = \mu(P' \xrightarrow{a} \mathcal{S}).$$

Proof – The fact that $\mathcal{P}$ is a probabilistic bisimulation implies that

$$\mu(P \xrightarrow{a} \mathcal{S}') = \mu(P' \xrightarrow{a} \mathcal{S}')$$

whenever $(P, P') \in \mathcal{P}$ and $\mathcal{S}'$ is an equivalence class of $\mathcal{P}$. Since $\mathcal{R}$ is an equivalence relation that contains $\mathcal{P}$, every equivalence class $\mathcal{S}$ of $\mathcal{R}$ is a union of a pairwise disjoint collection of equivalence classes of $\mathcal{P}$. Thus,

$$\begin{aligned}
\mu(P \xrightarrow{a} \mathcal{S}) &= \sum_{\mathcal{S}' \subseteq \mathcal{S}} \mu(P \xrightarrow{a} \mathcal{S}') \\
&= \sum_{\mathcal{S}' \subseteq \mathcal{S}} \mu(P' \xrightarrow{a} \mathcal{S}') \\
&= \mu(P' \xrightarrow{a} \mathcal{S}).
\end{aligned}$$

∎

Following [Jou92], we now give a probabilistic version of Milner's technique of "bisimulation up to bisimulation equivalence." This technique will be useful in proving the soundness of laws for recursion.

Formally, if $\mathcal{R}$ is an equivalence relation, then define $\overline{\mathcal{R}} = (\overset{\text{pr}}{\sim} \mathcal{R} \overset{\text{pr}}{\sim})^*$. The relation $\mathcal{R}$ is called a *probabilistic bisimulation up to* $\overset{\text{pr}}{\sim}$ if whenever $P \;\mathcal{R}\; P'$, then for all actions a and all equivalence classes $\mathcal{S}$ of $\overline{\mathcal{R}}$ we have $\mu(P \xrightarrow{a} \mathcal{S}) = \mu(P' \xrightarrow{a} \mathcal{S})$.

Lemma 3.5 *If $\mathcal{R}$ is a probabilistic bisimulation up to $\overset{\text{pr}}{\sim}$, then $\overline{\mathcal{R}}$ is a probabilistic bisimulation. Moreover, $\mathcal{R} \subseteq \overset{\text{pr}}{\sim}$ and $\overline{\mathcal{R}}$ is $\overset{\text{pr}}{\sim}$.*

Proof – We have to show that whenever $P\ \overline{\mathcal{R}}\ P'$, then for all actions a and all equivalence classes $\mathcal{S}$ of $\overline{\mathcal{R}}$ we have $\mu(P \xrightarrow{a} \mathcal{S}) = \mu(P' \xrightarrow{a} \mathcal{S})$. Now, $P\ \overline{\mathcal{R}}\ P'$ precisely when there exists a finite sequence of agents $P_0, P_1, \ldots, P_n$, with $P \equiv P_0$, $P_n \equiv P'$, and such that for all i with $0 \leq i < n$ we have either $P_i \overset{\text{pr}}{\sim} P_{i+1}$ or else $P_i\ \mathcal{R}\ P_{i+1}$. But then $\mu(P_i \xrightarrow{a} \mathcal{S}) = \mu(P'_{i+1} \xrightarrow{a} \mathcal{S})$ for all $i \geq 0$, because if $P_i \overset{\text{pr}}{\sim} P_{i+1}$ it follows from Lemma 3.4 using the definition of probabilistic bisimulation, and if $P_i\ \mathcal{R}\ P_{i+1}$ it follows by hypothesis.

To prove the additional assertions, observe that $\overline{\mathcal{R}} \subseteq \overset{\text{pr}}{\sim}$ because $\overset{\text{pr}}{\sim}$ is the largest probabilistic bisimulation, and $\overset{\text{pr}}{\sim} \subseteq \overline{\mathcal{R}}$ by construction, so that $\overline{\mathcal{R}}$ is $\overset{\text{pr}}{\sim}$. It follows immediately that $\mathcal{R} \subseteq \overset{\text{pr}}{\sim}$. ∎

4 Axioms for Probabilistic Bisimulation Equivalence

In this section, we present our axiom system for probabilistic bisimulation equivalence and prove soundness. We will later show that our axioms constitute a complete equational axiomatization of probabilistic bisimulation equivalence; that is, the equation $E = F$ is deducible from the axiom system if and only if E and F are probabilistically bisimulation equivalent.

We consider the following axioms and rules for inferring assertions of the form $E = F$, where E and F are expressions:

(E1) $E = E$.

(E2) From $E = F$, infer $F = E$.

(E3) From $E = F$ and $F = G$, infer $E = G$.

(C1a) From $F = F'$ infer $F\{\widetilde{E}/\widetilde{X}\} = F'\{\widetilde{E}/\widetilde{X}\}$.

(C1b) From $\widetilde{E} = \widetilde{E}'$ infer $F\{\widetilde{E}/\widetilde{X}\} = F\{\widetilde{E}'/\widetilde{X}\}$.

(C2) From $E = E'$, infer $\mathbf{fix}\ X.E = \mathbf{fix}\ X.E'$.

(S1) $E\ {}_p{+}\ F = F\ {}_{\overline{p}}{+}\ E$.

(S2) $E\ {}_p{+}\ (F\ {}_q{+}\ G) = (E\ {}_r{+}\ F)\ {}_s{+}\ G$, whenever $p = rs$, $\overline{p}q = \overline{r}s$, and $\overline{s} = \overline{p}\,\overline{q}$.

(S3) $E\ {}_p{+}\ E = E$.

(R1) $\mathbf{fix}\ X.E = E\{\mathbf{fix}\ X.E/X\}$.

(R2) $\mathbf{fix}\ X.E\ {}_p{+}\ X = \mathbf{fix}\ X.E$.

(R3) From $E = F\{E/X\}$, where all occurrences of X in F are guarded, infer $E = \textbf{fix}\ X.F$.

We write $\vdash E = F$ to assert that an equation $E = F$ is formally provable from the above axioms and rules.

Our goal is to show that the above axioms and inference rules are sound and complete for probabilistic bisimulation equivalence. In the remainder of this section, we consider soundness.

Proposition 4.1 *The following are sound for probabilistic bisimulation equivalence.*

1. *Laws (E1)-(E3).*
2. *Laws (S1)-(S3).*
3. *Law (C1a).*

Proof – 1. Obvious from the fact that probabilistic bisimulation equivalence is an equivalence relation.

2. The obvious construction of a probabilistic bisimulation works in each case to establish these laws in the special case that the left and right-hand sides are agents. A straightforward argument using the special case and the definition of probabilistic bisimulation equivalence on expressions with free variables extends the result to all expressions.

3. An immediate consequence of the definition of probabilistic bisimulation equivalence on expressions with free variables. ∎

Proposition 4.2 *Law (R1) is sound for probabilistic bisimulation equivalence.*

Proof – Consider the least equivalence relation $\mathcal{R}$ containing all pairs either of the form $(\textbf{fix}\ X.E, E\{\textbf{fix}\ X.E/X\})$ or of the form $(E\{\textbf{fix}\ X.E/X\}, \textbf{fix}\ X.E)$. By the definition of the operational semantics, a triple $(\textbf{fix}\ X.E, a, Q)$ determines an inferable transition $\textbf{fix}\ X.E \xrightarrow{a} Q$ if and only if the triple $(E\{\textbf{fix}\ X.E/X\}, a, Q)$ determines an inferable transition $E\{\textbf{fix}\ X.E/X\} \xrightarrow{a} Q$. Thus, applying Lemma 2.1, we have that

$$\mu(\textbf{fix}\ X.E \xrightarrow{a} Q) = 0 \text{ iff } \mu(E\{\textbf{fix}\ X.E/X\} \xrightarrow{a} Q) = 0,$$

Moreover, if $\mu(\textbf{fix}\ X.E \xrightarrow{a} Q) \neq 0$, then the fixed-point property of μ guarantees that the (inferable) transition $\textbf{fix}\ X.E \xrightarrow{a} Q$ is assigned the same probability as the corresponding (inferable) transition $E\{\textbf{fix}\ X.E/X\} \xrightarrow{a} Q$. From this, it is easily verified that the relation $\mathcal{R}$ is a probabilistic bisimulation. ∎

Our soundness proofs make use of the following technical substitution lemma, which is a variant of [Mil84], Lemma 5.6.

Lemma 4.3 *Suppose G is an expression with free variables in $\langle\widetilde{X}, Z\rangle$, where Z is not among the variables $\widetilde{X}$. Suppose $\tilde{E}$ are expressions in which the variable Z does not occur free. Then*

$$G\{F/Z\}\{\tilde{E}/\widetilde{X}\} \equiv G\{\tilde{E}/\widetilde{X}\}\{F\{\tilde{E}/\widetilde{X}\}/Z\}.$$

Proof – By structural induction on G. ∎

In the next and subsequent results, we shall often have occasion to refer to a particular class of equivalence relations, for which some notation is convenient. If $\tilde{E}$ and $\tilde{F}$ are sets of expressions, and $\widetilde{X}$ is a set of variables, then define $\Omega(\tilde{E}, \tilde{F}, \widetilde{X})$ to be the reflexive, symmetric closure of the set of all pairs of expressions of the form $(G\{\tilde{E}/\widetilde{X}\}, G\{\tilde{F}/\widetilde{X}\})$, where G is an expression with no free variables other than $\widetilde{X}$. Clearly, $\Omega(\tilde{E}, \tilde{F}, \widetilde{X})$ is an equivalence relation. We will use the notation $\Omega(E, F, X)$ when $\tilde{E}$, $\tilde{F}$, and $\widetilde{X}$ are singleton sets. Note that, in this case, taking G to be X shows that $\Omega(E, F, X)$ contains the pair (E, F).

Proposition 4.4 *Law (C1b) is sound for probabilistic bisimulation equivalence.*

Proof – It suffices to prove the case in which the expressions $\tilde{E}$ and $\tilde{E}'$ are agents, and F has no free variables other than $\widetilde{X}$. The general case follows easily from this special case, using the definition of probabilistic bisimulation equivalence for expressions with free variables.

To prove the special case, we show that the relation $\mathcal{R} = \Omega(\tilde{E}, \tilde{F}, \widetilde{X})$ is a probabilistic bisimulation up to $\overset{\mathrm{pr}}{\sim}$. For this, it suffices to show that for all equivalence classes $\mathcal{S}$ of $\overline{\mathcal{R}}$, all actions a, and all expressions G with no free variables other than $\widetilde{X}$, we have

$$\mu(G\{\tilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = \mu(G\{\tilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S})$$

We actually prove the following two assertions, whose conjunction implies the desired result:

1. For all $i \geq 0$, for all expressions G with no free variables other than $\widetilde{X}$, for all equivalence classes $\mathcal{S}$ of $\overline{\mathcal{R}}$, and all actions a, we have

$$\mu^i(G\{\tilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) \leq \mu(G\{\tilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}).$$

2. The same statement with $\tilde{E}$ and $\tilde{E}'$ interchanged.

We consider only (1), as the proof of (2) is symmetric. We proceed by induction on i.

1. If $i = 0$, then we immediately have

$$\mu^i(G\{\tilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = 0 \leq \mu(G\{\tilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}).$$

2. Suppose the result has been shown for some $i \geq 0$, and consider the case of $i+1$. We consider the syntactic form of G:

   - If G is the variable X_i in $\widetilde{X}$, then $G\{\widetilde{E}/\widetilde{X}\} = E_i$ and $G\{\widetilde{E}'/\widetilde{X}\} = E'_i$. Since by hypothesis E_i and E'_i are probabilistically equivalent, we have:

     $$\begin{aligned} \mu^{i+1}(G\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}') &= \mu^{i+1}(E_i \xrightarrow{a} \mathcal{S}) \\ &\leq \mu(E_i \xrightarrow{a} \mathcal{S}) \\ &= \mu(E'_i \xrightarrow{a} \mathcal{S}) \\ &= \mu(G\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}), \end{aligned}$$

     where we have used Lemma 3.4 in replacing E_i by E'_i.

   - Suppose G is bG'. Then $G\{\widetilde{E}/\widetilde{X}\}$ is $bG'\{\widetilde{E}/\widetilde{X}\}$ and $G\{\widetilde{E}'/\widetilde{X}\}$ is $bG'\{\widetilde{E}'/\widetilde{X}\}$. If $b \neq a$, then

     $$\mu^{i+1}(G\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = 0 = \mu(G\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}).$$

     Suppose $b = a$. Then $G\{\widetilde{E}/\widetilde{X}\} \xrightarrow{b} H$ if and only if $H \equiv G'\{\widetilde{E}/\widetilde{X}\} \in \mathcal{S}$, and $G\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{b} H$ if and only if $H \equiv G'\{\widetilde{E}'/\widetilde{X}\} \in \mathcal{S}$. By definition of $\mathcal{S}$, either both $G'\{\widetilde{E}/\widetilde{X}\}$ and $G'\{\widetilde{E}'/\widetilde{X}\}$ are in $\mathcal{S}$ or both are not in $\mathcal{S}$. In the first case,

     $$\mu^{i+1}(G\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = 1 = \mu(G\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),$$

     and in the second case,

     $$\mu^{i+1}(G\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = 0 = \mu(G\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}).$$

   - Suppose G is $G_1 \,{}_p{+}\, G_2$. Then $G\{\widetilde{E}/\widetilde{X}\}$ is $G_1\{\widetilde{E}/\widetilde{X}\} \,{}_p{+}\, G_2\{\widetilde{E}/\widetilde{X}\}$ and $G\{\widetilde{E}'/\widetilde{X}\}$ is $G_1\{\widetilde{E}'/\widetilde{X}\} \,{}_p{+}\, G_2\{\widetilde{E}'/\widetilde{X}\}$. Then

     $$\mu^{i+1}(G\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = p \cdot \mu^i(G_1\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) + \overline{p} \cdot \mu^i(G_2\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),$$

     and by the fixed-point property of μ:

     $$\mu(G\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) = p \cdot \mu(G_1\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) + \overline{p} \cdot \mu(G_2\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}).$$

     By induction,

     $$\mu^i(G_1\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) \leq \mu(G_1\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),$$

     and similarly

     $$\mu^i(G_2\{\widetilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) \leq \mu(G_2\{\widetilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),$$

     from which the result follows.

- Suppose G is **fix** $Z.G'$. Then $G\{\tilde{E}/\widetilde{X}\}$ is **fix** $Z.(G'\{\tilde{E}/\widetilde{X}\})$ and $G\{\tilde{E}'/\widetilde{X}\}$ is **fix** $Z.(G'\{\tilde{E}'/\widetilde{X}\})$, because $\tilde{E}$ and $\tilde{E}'$ are agents. Then

$$\begin{aligned}\mu^{i+1}(G\{\tilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) &= \mu^{i}(G'\{\tilde{E}/\widetilde{X}\}\{G\{\tilde{E}/\widetilde{X}\}/Z\} \xrightarrow{a} \mathcal{S}) \\ &= \mu^{i}(G'\{G/Z\}\{\tilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),\end{aligned}$$

and by the fixed-point property of μ:

$$\begin{aligned}\mu(G\{\tilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) &= \mu(G'\{\tilde{E}'/\widetilde{X}\}\{G\{\tilde{E}'/\widetilde{X}\}/Z\} \xrightarrow{a} \mathcal{S}) \\ &= \mu(G'\{G/Z\}\{\tilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),\end{aligned}$$

where we have used Lemma 4.3 in each case. By induction

$$\mu^{i}(G'\{G/Z\}\{\tilde{E}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) \leq \mu(G'\{G/Z\}\{\tilde{E}'/\widetilde{X}\} \xrightarrow{a} \mathcal{S}),$$

from which the result follows.

∎

Proposition 4.5 *Law (C2) is sound for probabilistic bisimulation equivalence.*

Proof – It suffices to establish the result for the special case in which E and E' have no free variables other than X, as the general case follows easily from the special case using properties of substitution.

Suppose E and E' are probabilistically equivalent. We claim that the relation $\mathcal{R} = \Omega(\mathbf{fix}\ X.E, \mathbf{fix}\ X.E', X)$ is a probabilistic bisimulation up to $\overset{\text{pr}}{\sim}$. To prove this, it suffices to show that for all expressions G with no free variables other than X, all actions a, and all equivalence classes $\mathcal{S}$ of $(\overset{\text{pr}}{\sim} \mathcal{R} \overset{\text{pr}}{\sim})^*$ we have:

$$\mu(G\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}) = \mu(G\{\mathbf{fix}\ X.E'/X\} \xrightarrow{a} \mathcal{S}).$$

As in the proof of Proposition 4.4, we prove a stronger result consisting of the conjunction of the following two properties:

1. For all $i \geq 0$, all expressions G with no free variables other than X, all actions a, and all equivalence classes $\mathcal{S}$ of $(\overset{\text{pr}}{\sim} \mathcal{R} \overset{\text{pr}}{\sim})^*$ we have:

$$\mu^{i}(G\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}) \leq \mu(G\{\mathbf{fix}\ X.E'/X\} \xrightarrow{a} \mathcal{S}).$$

2. The same statement with E and E' interchanged.

The proof proceeds in a fashion similar to that of Proposition 4.4. The case in which G is the variable X requires an application of (C1a) and Lemma 3.4. The case in which G is **fix** $Z.G'$ uses Lemma 4.3. We omit the details. ∎

Proposition 4.6 *Law (R2) is sound for probabilistic bisimulation equivalence.*

Proof – It suffices to establish the result for the special case in which E and E' have no free variables other than X, as the general case follows easily from the special case using properties of substitution.

Suppose E and E' are probabilistically equivalent. We claim that the relation $\mathcal{R} = \Omega(\mathbf{fix}\ X.E\ {}_p{+}\ X, \mathbf{fix}\ X.E, X)$ is a probabilistic bisimulation. To prove this, it suffices to show that for all expressions G with no free variables other than X, all actions a, and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$ we have:

$$\mu(G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) = \mu(G\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}).$$

As in the previous soundness proofs, we prove a stronger result consisting of the conjunction of the following two properties:

1. For all $i \geq 0$, all expressions G with no free variables other than X, all actions a, and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$ we have:

$$\mu^i(G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) \leq \mu(G\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}).$$

2. The same statement with $\mathbf{fix}\ X.E\ {}_p{+}\ X$ and $\mathbf{fix}\ X.E$ interchanged.

Since the statements to be proved are not symmetric as in the previous cases, we consider both (1) and (2). As usual, both are proved by induction on i.

We first consider (1):

1. If $i = 0$, then

$$\mu^i(G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) = 0 \leq \mu(G\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}),$$

   and the result is immediate.

2. Suppose we have shown the result for some $i \geq 0$, and consider the case of $i+1$. Again, the only interesting cases are when G is the variable X and when G is $\mathbf{fix}\ Z.G'$.

   - If G is the variable X, then $G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} = \mathbf{fix}\ X.E\ {}_p{+}\ X$ and $G\{\mathbf{fix}\ X.E/X\} = \mathbf{fix}\ X.E$. Now,

$$\mu^{i+1}(\mathbf{fix}\ X.E\ {}_p{+}\ X \xrightarrow{a} \mathcal{S}) = \mu^i((E\ {}_p{+}\ X)\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}).$$

     By induction hypothesis

$$\mu^i((E\ {}_p{+}\ X)\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) \leq \mu((E\ {}_p{+}\ X)\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}),$$

which is just

$$\mu(E\{\mathbf{fix}\ X.E/X\}\ {}_p{+}\ \mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}).$$

By the fixed point property of μ:

$$\begin{aligned}\mu(E\{\mathbf{fix}\ X.E/X\}\ {}_p{+}\ \mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}) &= p\cdot\mu(E\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}) + \\ &\qquad \overline{p}\cdot\mu(\mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}) \\ &= p\cdot\mu(\mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}) + \\ &\qquad \overline{p}\cdot\mu(\mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}) \\ &= \mu(\mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}),\end{aligned}$$

completing the proof.

- Suppose G is $\mathbf{fix}\ Z.G'$. Then

$$G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \equiv \mathbf{fix}\ Z.(G'\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\})$$

and

$$G\{\mathbf{fix}\ X.E/X\} \equiv \mathbf{fix}\ Z.(G'\{\mathbf{fix}\ X.E/X\}),$$

because E has no free variables other than X. Thus

$$\begin{aligned}\mu^{i+1}(G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) &= \mu^{i}(G'\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \\ &\qquad \{G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\}/Z\} \xrightarrow{a} \mathcal{S}) \\ &= \mu^{i}(G'\{G/Z\}\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}),\end{aligned}$$

and by the fixed-point property of μ:

$$\begin{aligned}\mu(G\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}) &= \mu(G'\{\mathbf{fix}\ X.E/X\}\{G\{\mathbf{fix}\ X.E/X\}/Z\} \xrightarrow{a} \mathcal{S}) \\ &= \mu(G'\{G/Z\}\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}),\end{aligned}$$

where Lemma 4.3 has been applied as usual. By induction

$$\mu^{i}(G'\{G/Z\}\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) \leq \mu(G'\{G/Z\}\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}),$$

from which the result follows.

Finally, we consider (2). The proof is essentially the same as for (1), except the case in which G is the variable X. In this case $G\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} = \mathbf{fix}\ X.E\ {}_p{+}\ X$ and $G\{\mathbf{fix}\ X.E/X\} = \mathbf{fix}\ X.E$. Now,

$$\mu^{i+1}(\mathbf{fix}\ X.E \xrightarrow{a} \mathcal{S}) = \mu^{i}(E\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}).$$

By induction hypothesis

$$\mu^{i}(E\{\mathbf{fix}\ X.E/X\} \xrightarrow{a} \mathcal{S}) \leq \mu(E\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}).$$

By the fixed point property of μ:

$$\begin{aligned}\mu(E\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) &= p \cdot \mu(E\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) \\ &\qquad +\overline{p} \cdot \mu(E\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) \\ &= \mu((E\ {}_p{+}\ X)\{\mathbf{fix}\ X.E\ {}_p{+}\ X/X\} \xrightarrow{a} \mathcal{S}) \\ &= \mu(\mathbf{fix}\ X.E\ {}_p{+}\ X \xrightarrow{a} \mathcal{S}),\end{aligned}$$

completing the proof. ∎

The following result, which extends a result of Milner ([Mil89b], Lemma 13 p. 102), is needed to establish the soundness of (R3).

Lemma 4.7 *Suppose E is an expression containing no free variables other than X, such that all free occurrences of X are guarded. If $E\{P/X\} \xrightarrow{a} P'$, then P' takes the form $E'\{P/X\}$ (for some expression E'), and in addition $E\{Q/X\} \xrightarrow{a} E'\{Q/X\}$ for any Q. Moreover, for all $i \geq 0$ we have*

$$\mu(E\{P/X\} \xrightarrow{a} E'\{P/X\}) = \mu(E\{Q/X\} \xrightarrow{a} E'\{Q/X\}).$$

Proof – The proof of the first part is by transition induction, exactly as in Milner. To prove the second part, we use an induction technique similar to that used for the previous results, to prove the following assertion:

- For all $i \geq 0$ and for all expressions E with no free variables other than X, such that all free occurrences of X are guarded,

$$\mu^i(E\{P/X\} \xrightarrow{a} E'\{P/X\}) = \mu^i(E\{Q/X\} \xrightarrow{a} E'\{Q/X\}).$$

The details are straightforward, and are omitted. ∎

Proposition 4.8 *Law (R3) is sound for probabilistic bisimulation equivalence.*

Proof – Suppose $E \overset{\text{pr}}{\sim} F\{E/X\}$, where X is guarded in F. Let $\mathcal{R}$ be the relation $\Omega(E, \mathbf{fix}\ X.F, X)$. We claim that $\mathcal{R}$ is a probabilistic bisimulation. We have to show that

$$\mu(G\{E/X\} \xrightarrow{a} \mathcal{S}) = \mu(G\{\mathbf{fix}\ X.F/X\} \xrightarrow{a} \mathcal{S})$$

for all expressions G with no free variables other than X, all actions a, and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$. Once again we prove the following two statements:

1. For all $i \geq 0$, all expressions G with no free variables other than X, all actions a, and all equivalence classes $\mathcal{S}$ of $\mathcal{R}$ we have:

$$\mu^i(G\{E/X\} \xrightarrow{a} \mathcal{S}) \leq \mu(G\{\mathbf{fix}\ X.F/X\} \xrightarrow{a} \mathcal{S}).$$

2. The same statement with E and **fix** $X.F$ interchanged.

Since the statements to be proved are not symmetric as in the previous cases, we must consider both (1) and (2). These are proved, as usual, by induction on i, with the induction step containing a case analysis on the syntactic form of G. For (1), when G is the variable X, we need to use Lemma 4.7 together with the hypothesis that X is guarded in F. For (2), no new ideas are involved. The remaining details are omitted. ∎

5 Probabilistic Summation

In this section, we establish a general theorem about probabilistic summation, which will allow us to check the provability of a certain class of expressions "by inspection." That is, we show that an equation between expressions formed using only variables and probabilistic summation is provable from (S1)-(S3) if and only if the same equation, with the probabilities "erased," is provable in CCS, and the left- and right-hand sides assign the same total probabilities to variables. This result, in conjunction with law (C1a), will prove particularly useful in the completeness proof of Section 6.

Formally, to each PE expression E, we associate an *unguardedness function*

$$\mathrm{ung}_E : \mathrm{Var} \rightarrow [0,1],$$

defined to be the least solution of the following recursive conditions:

1. If E is X, then $\mathrm{ung}_E(X) = 1$ and $\mathrm{ung}_E(Y) = 0$ for all $Y \not\equiv X$.
2. If E is aF, then $\mathrm{ung}_E(X) = 0$ for all X.
3. If E is $E \;{}_p\!+\; F$, then $\mathrm{ung}_E(G) = p \cdot \mathrm{ung}_E(G) + \overline{p} \cdot \mathrm{ung}_F(G)$.
4. If E is **fix** $X.F$, then $\mathrm{ung}_E(X) = 0$, and $\mathrm{ung}_E(Y) = \mathrm{ung}_F(Y)$ for all $Y \not\equiv X$.

Intuitively, $\mathrm{ung}_E(X)$ gives the total probability assigned to unguarded occurrences of variable X in expression E. We may regard $\mathrm{ung}_E(X)$ as the "degree of unguardedness" of variable X in expression E.

Lemma 5.1 $\mathrm{ung}_E(X) = 0$ *if and only if X is guarded in E.*

Proof – Easy structural induction on E. ∎

Call a PE expression E a *summation expression* if it is formed using variables and probabilistic summation only. The laws (S1)-(S3) allow us to prove a normal-form lemma for summation expressions. For this, it is convenient to have a notation for probabilistic n-ary summation.

We define the notation $\sum_{i=1}^{n}\{(p_i, E_i) : 1 \le i \le n\}$, where $\{(p_i, E_i) : 1 \le i \le n\}$ is a nonempty set of pairs, the E_i are probabilistic expressions, and the $p_i \in (0,1)$ have the property that $\sum_{i=1}^{n} p_i = 1$, recursively as follows:

1. $\sum\{(1, E)\} = E$.
2. If $n > 1$, then

$$\sum\{(p_i, E_i) : 1 \le i \le n\} = \sum\{(p_i/\overline{p}_n, E_i) : 1 \le i \le n-1\} \;{}_{\overline{p}_n}\!+ E_n.$$

When no confusion can arise about the meaning, we often write

$$\sum_{i=1}^{n} p_i \cdot E_i$$

instead of

$$\sum\{(p_i, E_i) : 1 \le i \le n\}.$$

Lemma 5.2 *Suppose E is a summation expression. Then $\vdash E = E'$, where E' has the form $\sum_{i \in I} p_i \cdot X_i$, with the X_i distinct variables in lexicographic order.*

Proof – Easy structural induction on E, using (S1)-(S3). In essence, one simply proves the corresponding theorem about ordinary summation without the probability labels, and then one fills in the probabilities in the only way permitted by (S1)-(S3). ∎

The following proposition allows us to check the provability of probabilistic summation expressions "by inspection." To state this result, define the *erasing* of a PE expression E to be the CCS expression $\mathrm{erase}(E)$ obtained by removing all the probabilities annotating the $+$ operators.

Proposition 5.3 *Suppose E and E' are* PE *summation expressions. Then $\vdash E = E'$ if and only if the following two conditions hold:*

1. $\vdash \mathrm{erase}(E) = \mathrm{erase}(E')$ *is provable using the erasings of laws (S1)-(S3).*

2. $\mathrm{ung}_E = \mathrm{ung}_{E'}$.

Proof – Clearly, if $\vdash E_1 = E_2$ is provable using (S1)-(S3), then $\vdash \mathrm{erase}(E_1) = \mathrm{erase}(E_2)$ is provable using the erasings of (S1)-(S3). It is also easy to check that for each of the laws (S1)-(S3), if L denotes the left-hand side and R denotes the right-hand side, then $\mathrm{ung}_L = \mathrm{ung}_R$.

Conversely, suppose conditions (1) and (2) hold. By Lemma 5.2, we can use (S1)-(S3) to prove $\vdash E = \sum_{i=1}^{n} p_i \cdot X_i$, where the X_i are distinct variables in lexicographic order, and $\vdash E' = \sum_{i=1}^{n'} p'_i \cdot X'_i$, where the X'_i are distinct variables in lexicographic order.

Erasing the probabilities from these proofs, and using (1), we conclude that the erasings of (S1)-(S3) suffice to prove $\vdash E = \sum_{i=1}^{n} X_i$ and $\vdash E = \sum_{i=1}^{n'} X'_i$. It follows (standard results about the erasings of laws (S1)-(S3)) that $n = n'$ and $X_i \equiv X'_i$ for $1 \leq i \leq n$. Using (2), we conclude that $p_i = p'_i$ for $1 \leq i \leq n$, hence $\sum_{i=1}^{n} p_i \cdot X_i$ and $\sum_{i=1}^{n'} p'_i \cdot X'_i$ are identical, thus showing $\vdash E = E'$ is provable using (S1)-(S3). ∎

6 Completeness

In this section, we adapt the completeness proof of Milner for bisimulation equivalence of regular CCS expressions to a completeness proof for probabilistic bisimulation equivalence of PE expressions. The proof follows Milner in its main ideas; however some variation is required because: (1) the unit law $E \;{}_p\!+ \mathbf{0} = E$ is not sound for probabilistic bisimulation equivalence, and (2) the construction of the characteristic set of equations for $E = E'$ has to take probabilities into account.

We first restate Milner's "Unique Solution of Equations" theorem. The theorem and its proof carry over without change to the probabilistic setting.

Theorem 1 (Unique Solution of Equations) *Let $\widetilde{X} = \langle X_1, \ldots, X_m \rangle$ and $\widetilde{Y} = \langle Y_1, \ldots, Y_n \rangle$ be distinct variables, and $\widetilde{F} = \langle F_1, \ldots, F_m \rangle$ expressions with free variables in $\langle \widetilde{X}, \widetilde{Y} \rangle$ in which each X_i is guarded. Then there exist expressions $\widetilde{E} = \langle E_1, \ldots, E_m \rangle$ with free variables in $\widetilde{Y}$ such that*

$$\vdash E_i = F_i\{\widetilde{E}/\widetilde{X}\} \qquad (i \leq m).$$

Moreover, if the same property may be proved when $\widetilde{E}$ are replaced by expressions $\widetilde{E}' = \langle E'_1, \ldots, E'_m \rangle$ with free variables in $\widetilde{Y}$, then

$$\vdash E'_i = E_i \qquad (i \leq m).$$

Proof – By induction on m, exactly as in Milner. ∎

The next result is a version of Milner's "Equational Characterization" theorem. The statement is complicated somewhat by the presence of probabilities on the summations and the fact that we do not have the unit law for $\mathbf{0}$.

Theorem 2 (Equational Characterization) *For any expression E, with free variables in $\widetilde{Y}$, there exist expressions $E_1, \ldots, E_p$ $(p \geq 1)$, with free variables in $\widetilde{Y}$, satisfying p equations, each of which has one of the following three forms, where $1 \leq i \leq p$:*

1. $\vdash E_i = \sum_{j=1}^{m(i)} p_{ij} \cdot E'_{ij}$
   where each expression E'_{ij} is either $\mathbf{0}$ or has the form $a_{ij} E_{f(i,j)}$.

2. $\vdash E_i = \sum_{j=1}^{n(i)} q_{ij} \cdot Y_{g(i,j)}$
   where the variables $Y_{g(i,j)}$ are enumerated without repetition.

3. $\vdash E_i = \sum_{j=1}^{m(i)} p_{ij} \cdot E'_{ij} \;{}_r\!+\; \sum_{j=1}^{n(i)} q_{ij} \cdot Y_{g(i,j)}$
   where the first term satisfies the conditions in (1), and the second term satisfies the conditions in (2).

Moreover, $\vdash E = E_1$*.*

Proof – As in [Mil84], the proof is by induction on the structure of E. The only nontrivial case is $E \equiv \mathbf{fix}\ X.F$. In this case, by induction we have expressions $F_1, \ldots, F_p$ satisfying p equations, each of which has one of the three forms shown above, moreover $\vdash F = F_1$. Using (C2) we have $\vdash E = \mathbf{fix}\ X.F_1$.

In each of the p equations, the variable X might or might not appear as one of the $Y_{g(i,j)}$. We consider whether X appears in this way in the first equation; that is, as one of the $Y_{g(1,j)}$. If X is not one of the $Y_{g(1,j)}$, then from $\vdash E = \mathbf{fix}\ X.F_1$, using (R1) we have $\vdash E = F_1\{E/X\}$. Suppose X is one of the $Y_{g(1,j)}$. If F_1 has form (2) above with $n(1) = 1$, then we have immediately $\vdash E = \mathbf{fix}\ X.F_1 \equiv \mathbf{0}$. Otherwise, we can use (R2) and Proposition 5.3, in conjunction with (C1a), to eliminate the unguarded occurrence of X, and then use (R1) to show $\vdash E = F'_1\{E/X\}$, where F'_1 takes one of the forms (1)-(3), and X does not occur free in F'_1.

Thus, whether or not X appears in the first equation, we have

$$\vdash E = F'_1\{E/X\},$$

where either $\vdash F = F'_1$ or $\vdash F = F'_1 \;{}_s\!+ X$, where F'_1 takes one of the forms (1)-(3), and X does not occur free in F'_1.

We now proceed as in Milner, setting

$$E_i \equiv F_i\{E/X\} \qquad\qquad (1 \le i \le p),$$

and observing that by rearranging terms using Proposition 5.3 in conjunction with (C1a), we obtain equations of the desired form. Moreover, $\vdash E = E_1$ follows from $\vdash F = F_1$, and the expressions E_i are easily seen to have free variables in $\widetilde{Y}$. ∎

We now present a lemma that is useful for the completeness proof. It basically says that variables appear unguarded with equal probability in probabilistically bisimilar expressions. We first need the following cancellation rule ([Jou92], Proposition 7.5), which is not sound in the non-probabilistic case. It may be viewed as a "unique fixed point" result for a limited form of unguarded recursion. The proof given below is essentially that of Jou.

Lemma 6.1 *If* $E \overset{\mathrm{pr}}{\approx} E \;{}_p\!+ F$*, then* $E \overset{\mathrm{pr}}{\approx} F$*.*

Proof – Suppose $\widetilde{X}$ contains all the free variables of E and F. If $E \stackrel{\mathrm{pr}}{\not\sim} F$, then there exist agents $\widetilde{P}$, and action a, and a probabilistic bisimulation equivalence class $\mathcal{S}$, such that

$$\mu(E\{\widetilde{P}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}) \neq \mu(F\{\widetilde{P}/\widetilde{X}\} \xrightarrow{a} \mathcal{S}).$$

But then, letting E' and F' abbreviate $E\{\widetilde{P}/\widetilde{X}\}$ and $F\{\widetilde{P}/\widetilde{X}\}$, respectively, we have:

$$\begin{aligned}
\mu((E' \;{}_p{+}\; F') \xrightarrow{a} \mathcal{S}) - \mu(E' \xrightarrow{a} \mathcal{S}) &= p \cdot \mu(E' \xrightarrow{a} \mathcal{S}) + \overline{p} \cdot \mu(F' \xrightarrow{a} \mathcal{S}) - \mu(E' \xrightarrow{a} \mathcal{S}) \\
&= \overline{p} \cdot (\mu(F' \xrightarrow{a} \mathcal{S}) - \mu(E' \xrightarrow{a} \mathcal{S})) \\
&\neq 0.
\end{aligned}$$

It follows that $E' \stackrel{\mathrm{pr}}{\not\sim} E' \;{}_p{+}\; F'$, hence $E \stackrel{\mathrm{pr}}{\not\sim} E \;{}_p{+}\; F$. ∎

The following result is [Jou92], Proposition 7.10, only with a simpler proof.

Lemma 6.2 *Suppose $E' \;{}_p{+}\; X \stackrel{\mathrm{pr}}{\sim} F' \;{}_q{+}\; X$, where E' and F' contain no unguarded occurrences of X. Then $E' \stackrel{\mathrm{pr}}{\sim} F'$ and $p = q$.*

Proof – If $E' \;{}_p{+}\; X \stackrel{\mathrm{pr}}{\sim} F' \;{}_q{+}\; X$, then by (C1a) we have $E' \;{}_p{+}\; E' \stackrel{\mathrm{pr}}{\sim} F' \;{}_q{+}\; E'$, and hence $E' \stackrel{\mathrm{pr}}{\sim} F' \;{}_q{+}\; E'$ by (S3). It follows by Lemma 6.1 that $E' \stackrel{\mathrm{pr}}{\sim} F'$.

To show $p = q$, let a be an action not occurring in E' or F'. Since $E' \;{}_p{+}\; X \stackrel{\mathrm{pr}}{\sim} F' \;{}_q{+}\; X$, by (C1a) we have $E'\{a\mathbf{0}/X\} \;{}_p{+}\; a\mathbf{0} \stackrel{\mathrm{pr}}{\sim} F'\{a\mathbf{0}/X\} \;{}_q{+}\; a\mathbf{0} \stackrel{\mathrm{pr}}{\sim} E'\{a\mathbf{0}/X\} \;{}_q{+}\; a\mathbf{0}$. Then

$$\mu((E'\{a\mathbf{0}/X\} \;{}_p{+}\; a\mathbf{0}) \xrightarrow{a} \mathbf{0}) = p \cdot \mu(E'\{a\mathbf{0}/X\} \xrightarrow{a} \mathbf{0}) + \overline{p},$$

and

$$\mu((E'\{a\mathbf{0}/X\} \;{}_q{+}\; a\mathbf{0}) \xrightarrow{a} \mathbf{0}) = q \cdot \mu(E'\{a\mathbf{0}/X\} \xrightarrow{a} \mathbf{0}) + \overline{q}.$$

Since these two quantities must be equal, we have:

$$(p - q) \cdot \mu(E'\{a\mathbf{0}/X\} \xrightarrow{a} \mathbf{0}) = (p - q).$$

Since E' contains no unguarded occurrences of X and action a does not occur in E', we have

$$\mu(E'\{a\mathbf{0}/X\} \xrightarrow{a} \mathbf{0}) = 0.$$

It follows that $p = q$. ∎

The following completeness proof follows much the same lines as the one in [Mil84]. Given probabilistically bisimilar E and E', a "product" equational system is constructed from their respective equational characterizations. E and E' are then both shown to be solutions of this system; by uniqueness of solutions to guarded equations, completeness is established. The main technical consideration in moving to the probabilistic setting is the calculation of the probabilities for the product equational system.

Theorem 3 (Completeness) *If $E \stackrel{\mathrm{pr}}{\sim} E'$ then $\vdash E = E'$.*

Proof – Let E and E' have free variables in $\widetilde{Y}$. By Theorem 2 there are: expressions $E_1, \ldots, E_p$ satisfying p equations, each of which has one of the three forms in Theorem 2; expressions $E'_1, \ldots, E'_{p'}$ satisfying p' equations, each one of which has one of the three forms in Theorem 2; and moreover $\vdash E = E_1$ and $\vdash E' = E'_1$. For simplicity in what follows, we assume that all equations are of form (3). The argument differs only in inessential details for equations of forms (1) or (2). Thus, we suppose that

$$\vdash E_i = \sum_{j=1}^{m(i)} p_{ij} \cdot E_{ij} \;{}_{r_i}\!+ \sum_{j=1}^{n(i)} q_{ij} \cdot Y_{g(i,j)} \qquad (i \leq p)$$

where each E_{ij} is either $\mathbf{0}$ or of the form $a_{ij}E_{f(i,j)}$, and

$$\vdash E'_{i'} = \sum_{j'=1}^{m'(i')} p'_{i'j'} \cdot E'_{i'j'} \;{}_{r'_{i'}}\!+ \sum_{j'=1}^{n'(i')} q'_{i'j'} \cdot Y_{g'(i',j')} \qquad (i' \leq p').$$

where each $E'_{i'j'}$ is either $\mathbf{0}$ or of the form $a'_{i'j'}E'_{f'(i',j')}$.

Now let $I = \{\langle i, i'\rangle \mid E_i \overset{\text{pr}}{\approx} E'_{i'}\}$. Since $E \overset{\text{pr}}{\approx} E'$ by hypothesis, and in addition $\vdash E = E_1$ and $\vdash E' = E'_1$ imply by soundness that $E \overset{\text{pr}}{\approx} E_1$ and $E' \overset{\text{pr}}{\approx} E'_1$, we have $E_1 \overset{\text{pr}}{\approx} E'_1$, so that $\langle 1, 1\rangle \in I$. Moreover, the following hold for each $\langle i, i'\rangle \in I$:

1. There exists a total surjective relation $J_{ii'}$ between $\{1, \ldots, m(i)\}$ and $\{1, \ldots, m'(i')\}$, given by

   $$J_{ii'} = \{\langle j, j'\rangle \mid \text{either } E_{ij} \equiv \mathbf{0} \equiv E'_{i'j'} \text{ or else } a_{ij} = a'_{i'j'} \text{ and } \langle f(i,j), f'(i',j')\rangle \in I\}.$$

2. $r_i = r'_{i'}$.

3. $\sum\{p_{ij} \mid E_{ij} \equiv \mathbf{0}\} = \sum\{p'_{i'j'} \mid E'_{i'j'} \equiv \mathbf{0}\}$.

4. $\vdash \sum_{j=1}^{n(i)} q_{ij} \cdot Y_{g(i,j)} = \sum_{j'=1}^{n'(i')} q'_{i'j'} \cdot Y'_{g'(i',j')}$.

To prove assertion (4), observe that $E_i \overset{\text{pr}}{\approx} E'_{i'}$, in conjunction with Corollary 3.3, implies that E_i and $E'_{i'}$ have the same sets of unguarded variables, and the fact that these variables occur with the same probabilities follows from Lemma 6.2. The provability of (4) then follows from Proposition 5.3. Using Lemma 6.2 with $E_i \overset{\text{pr}}{\approx} E'_{i'}$ also yields assertion (2) and the following relation:

$$\sum_{j=1}^{m(i)} p_{ij} \cdot E_{ij} \overset{\text{pr}}{\approx} \sum_{j'=1}^{m'(i')} p'_{i'j'} \cdot E'_{i'j'}. \tag{5}$$

By the relation (5) and the definition of probabilistic bisimulation, for any given action a, the total probability associated with all summands prefixed by a on the left-hand side of relation (5) is the same as the total probability associated with all the a-prefixed summands on the right-hand side. Since the sum of all the probabilities in a summation expression must equal one, assertion (3) now follows immediately.

To prove assertion (1), let $J_{ii'}$ be defined as stated. To show that $J_{ii'}$ is total, consider an arbitrary $i \leq p$. For each $j \leq m(i)$, the term E_{ij} is either $\mathbf{0}$ or else has the form $a_{ij}E_{f(i,j)}$. In the former case, since the term E_{ij} occurs with positive probability, the total probability associated with summands in E_i of the form $a_{ij}E_{f(i,j)}$ must be less than one. Using $E_i \stackrel{\mathrm{pr}}{\approx} E'_{i'}$ together with Lemma 2.1, we conclude that the total probability associated with summands in $E'_{i'}$ of the form $a_{i'j'}E_{f'(i',j')}$ must also be less than one. This, in turn, implies that the total probability associated with summands in $E'_{i'}$ of the form $\mathbf{0}$ must be positive, thus establishing the existence of a j' such that $\langle j, j'\rangle \in J_{ii'}$ and $E_{ij} \equiv \mathbf{0} \equiv E'_{i'j'}$. In the latter case, we have $\mu(E_i \xrightarrow{a_{ij}} E_{f(i,j)}) > 0$, hence using $E_i \stackrel{\mathrm{pr}}{\approx} E'_{i'}$ together with Lemma 2.1 we conclude the existence of j' such that $\mu(E'_{i'} \xrightarrow{a} E'_{f'(i',j')}) > 0$ and $E_{f(i,j)} \stackrel{\mathrm{pr}}{\approx} E'_{f'(i',j')}$, so that $\langle f(i,j), f'(i',j')\rangle \in I$, thus completing the proof that $J_{ii'}$ is total. Symmetric reasoning establishes its surjectivity.

Now, let $J_{ii'}(j)$ denote the image of $j \in \{1, \ldots, m(i)\}$ under $J_{ii'}$ and $J_{ii'}^{-1}(j')$ the preimage of $j' \in \{1, \ldots, m'(i')\}$ under $J_{ii'}$. Let $[j]_{ii'}$ denote the set $J_{ii'}^{-1}(J_{ii'}(j))$ and let $[j']_{ii'}$ denote the set $J_{ii'}(J_{ii'}^{-1}(j'))$. It follows easily from the definitions that

1. If $\langle i, i'_1\rangle \in I$ and $\langle i, i'_2\rangle \in I$, then $[j]_{ii'_1} = [j]_{ii'_2}$ for $1 \leq j \leq m(i)$ Similarly, if $\langle i_1, i'\rangle \in I$ and $\langle i_2, i'\rangle \in I$, then $[j']_{i_1i'} = [j']_{i_2i'}$ for $1 \leq j \leq m'(i')$.

2. Note that if $k_1 \in [j]_{ii'}$ and $k_2 \in [j]_{ii'}$, then either $E_{ik_1} \equiv \mathbf{0} \equiv E_{ik_2}$ or else $E_{ik_1} \equiv a_{ik_1}E_{f(i,k_1)}$ and $E_{ik_2} \equiv a_{ik_2}E_{f(i,k_2)}$, where $a_{ik_1} = a_{ik_2}$. Similarly, if $k'_1 \in [j']_{ii'}$ and $k'_2 \in [j']_{ii'}$, then either $E'_{i'k'_1} \equiv \mathbf{0} \equiv E'_{i'k'_2}$ or else $E'_{i'k'_1} \equiv a_{i'k'_1}E'_{f'(i',k'_1)}$ and $E'_{i'k'_2} \equiv a_{i'k'_2}E'_{f'(i',k'_2)}$, where $a_{i'k'_1} = a_{i'k'_2}$.

Define

$$\nu_{ij} = \sum_{k\in[j]_{ii'}} p_{ik} \qquad\qquad (\text{any } i',\ \langle i, i'\rangle \in I)$$

and

$$\nu'_{i'j'} = \sum_{k'\in[j']_{ii'}} p'_{i'k'} \qquad\qquad (\text{any } i,\ \langle i, i'\rangle \in I)$$

From the hypothesis that E and E' are probabilistically bisimulation equivalent, it is easily seen that $\nu_{ij} = \nu'_{i'j'}$ whenever $\langle i, i'\rangle \in I$ and $\langle j, j'\rangle \in J_{ii'}$.

We now consider the formal equations, one for each $\langle i, i'\rangle \in I$:

$$X_{ii'} = \sum_{\langle j,j'\rangle\in J_{ii'}} \left(\frac{p_{ij}p'_{i'j'}}{\nu_{ij}}\right) \cdot F_{iji'j'\ r_i}\!+ \sum_{j=1}^{n(i)} q_{ij} \cdot Y_{g(i,j)}$$

where $F_{iji'j'} \equiv \mathbf{0}$ if $E_{ij} \equiv \mathbf{0} \equiv E_{i'j'}$, and otherwise $F_{iji'j'} \equiv a_{ij}X_{f(i,j),f'(i',j')}$.

First we assert that these equations are provably satisfied when each $X_{ii'}$ is instantiated to E_i. To see this, note that the typical equation becomes

$$E_i = \sum_{\langle j,j'\rangle \in J_{ii'}} \left(\frac{p_{ij}p'_{i'j'}}{\nu_{ij}}\right) \cdot F_{ij}\{E_i/X_{ii'}\} \;{}_{r_i}\!+ \sum_{j=1}^{n(i)} q_{ij} \cdot Y_{g(i,j)} \qquad (*)$$

and is provable, since—as $J_{ii'}$ is total—its right-hand side differs at most by repeated summands from that of the already proved equation for E_i. Moreover, the total probability of a repeated summand is the same as the probability associated with that summand in the already proved equation. That is, the total probability, in the first term of the equation for $X_{ii'}$, associated with all summands identical to $E_{f(i,j)}$ is

$$\frac{1}{\nu_{ij}} \cdot p_{ij} \cdot \sum_{k' \in [j']_{ii'}} p'_{i'k'} \;\; = \;\; p_{ij}.$$

Proposition 5.3 in conjunction with (C1a) thus suffice to prove $(*)$. A completely symmetric argument, relying on the surjectivity of the $J_{ii'}$, suffices to show the equations are provably satisfied when each $X_{ii'}$ is instantiated to E'_i.

Finally, we note that each $X_{ii'}$ is guarded in the right-hand sides of the formal equations. It immediately follows from Theorem 1 that $\vdash E_i = E'_{i'}$ for each $\langle i, i'\rangle \in I$, and hence $\vdash E = E'$. ∎

7 Conclusions

We have presented a complete equational axiomatization of probabilistic bisimulation for finite-state probabilistic processes. Probabilistic extensions of the transition-induction and bisimulation-up-to proof techniques [Mil89a] figured prominently in our soundness proof. Although our axiom system can be seen as a relatively minor variation of the one obtained by Milner [Mil84] for strong bisimulation, new insights and a careful accounting of probability were required to obtain the end result.

Though in the nonprobabilistic case one cannot delete the guardedness hypothesis in rule (R3), it is interesting to note that in the probabilistic case a stronger version of (R3) is in fact sound. Define variable X to be *probabilistically guarded* in expression E if $\mathrm{ung}_E(X) < 1$. By Lemma 5.1, if X is guarded, then it is probabilistically guarded. Then it can be shown that (R3) is sound for probabilistic bisimulation equivalence, even if the hypothesis that X is guarded in F is weakened to the hypothesis that X is probabilistically guarded in F. This is because, in essence, the only way that an unguarded, but probabilistically guarded variable X can appear in an expression is as a "top-level" summand with probability < 1. In the context of a recursion on X, such summands can always be eliminated using (R2).

A compelling open problem is the extension of our results to a weaker notion of probabilistic bisimulation that takes silent τ-transitions into account. Previous work by

Milner [Mil89b] is again likely to guide the choice of axioms and inference rules. One must first devise, however, an appropriate notion of "observational" probabilistic bisimulation: the absence of any such definition in the literature since probabilistic bisimulation was first proposed by Larsen and Skou around 1988, indicates that this is a nontrivial task.

References

[BBS95] J. C. M. Baeten, J. A. Bergstra, and S. A. Smolka. Axiomatizing probabilistic processes: ACP with generative probabilities. *Information and Computation*, 121(2):234–255, September 1995.

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

[Jou92] C.-C. Jou. *Aspects of Probabilistic Process Algebra.* PhD thesis, SUNY at Stony Brook, Stony Brook, New York, 1992.

[LS92] K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Information and Computation*, 94(1):1–28, September 1992.

[Mil84] R. Milner. A complete inference system for a class of regular behaviours. *J. Comput. System Sci.*, 28:439–466, 1984.

[Mil89a] R. Milner. *Communication and Concurrency.* International Series in Computer Science. Prentice Hall, 1989.

[Mil89b] R. Milner. A complete axiomatisation for observational congruence of finite-state behaviours. *Information and Computation*, 81:227–247, 1989.

[vGSS95] R. J. van Glabbeek, S. A. Smolka, and B. Steffen. Reactive, generative, and stratified models of probabilistic processes. *Information and Computation*, 121(1):59–80, August 1995.