Available online at www.sciencedirect.com
SCIENCE DIRECT®

Electronic Notes in Theoretical Computer Science 96 (2004) 7–28

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Axioms for Probability and Nondeterminism

Michael Mislove[a,1] and Joël Ouaknine[b,2] and James Worrell[a,1]

[a] *Tulane University, Department of Mathematics,*
6823 St Charles Avenue, New Orleans LA 70118, USA
[b] *Computer Science Department, Carnegie Mellon University,*
5000 Forbes Avenue, Pittsburgh PA 15213, USA

Abstract

This paper studies a simple calculus for finite-state processes featuring both nondeterministic and probabilistic choice. We present a domain model and an operational semantics for our calculus. The denotational model uses the probabilistic powerdomain of Jones and Plotkin, combined with a geometrically convex variant of the Plotkin powerdomain. The operational model defines transition rules under which a process makes transitions to probability distributions over states. We prove a full abstraction result that shows two processes have the same denotation if and only if they are probabilistically bisimilar. We also show that the expected laws for probability and nondeterminism are sound and complete with respect to the denotational model.

Keywords: Probabilistic bisimulation, nondeterministic choice, Segala-Lynch probabilistic automaton, CCS

1 Introduction

By now there is a well-established subset of the concurrency literature dealing with process algebras that feature probabilistic choice—either instead of, or in addition to, nondeterministic choice. In giving an operational semantics to such languages one must specify not only which transitions are possible, but also the probabilities with which they are taken (see, e.g., [19]). In the presence

[1] Support by the US National Science Foundation and the US Office of Naval Research is gratefully acknowledged.

[2] Support by the ONR contract N00014-95-1-0520, Defense Advanced Projects Research Agency and the Army Research Office under contract DAAD19-01-1-0485 is gratefully acknowledged.

doi:10.1016/j.entcs.2004.04.019

of unguarded recursion the resultant bookkeeping becomes quite complicated, and arguably undermines the usual advantages of an operational approach. On the other hand, in a domain model many technicalities can be hidden by importing standard constructions and results from general domain theory.

This paper gives a domain-theoretic semantics for a probabilistic process algebra. We use the probabilistic powerdomain [12] to model probabilistic choice, and we use a geometrically convex variant of the Plotkin powerdomain, independently due to Mislove [16] and Tix [20], to model nondeterministic choice. We also give an operational semantics for the process algebra, and we show that our domain model is fully abstract with respect to probabilistic bisimilarity. The relies on the main result of the paper, which presents a set of laws for probabilistic and nondeterministic choice that is sound and complete with respect to our domain model. The completeness result applies to finite-state processes; thus we restrict ourselves to a process algebra with prefixing, probabilistic choice, nondeterministic choice and recursion. However, for the completeness proof it turns out to be more convenient to work with the domain model than the operational model.

The nondeterministic sum of terms E and F is written $E + F$, while, for $0 < p < 1$, the probabilistic sum of p times E and $1 - p$ times F is written $E \oplus_p F$. The model we describe is non-alternating, that is, there is only one type of process, and the operators $+$ and $\oplus_p$ can be applied without restriction. To accommodate both types of choice, following the probabilistic automaton model of Segala and Lynch [18], we model the initial capabilities of a process as a set of probability distributions. Nondeterministic choice is modelled by union, and probabilistic choice by pointwise lifting the natural probabilistic sum operator on probability distributions to sets of such distributions. This last artifice entails that our semantics satisfies the following distributive law of probabilistic choice over nondeterministic choice

$$(E + F) \oplus_p G = (E \oplus_p F) + (F \oplus_p G)\,. \tag{1}$$

Another consequence of our interpretation of probabilistic choice is that, in order to ensure that the law $E \oplus_p E = E$ holds, we model the initial capabilities of a process as a *geometrically convex* [1] set of probability distributions. In turn this entails the following convexity law for nondeterministic choice

$$E + (E \oplus_p F) + F = E + F\,. \tag{2}$$

[1] A set S of probability distributions is *geometrically convex* if $p\sigma + (1-p)\nu \in S$ whenever $\sigma, \nu \in S$ and $0 \leqslant p \leqslant 1$. Later on we will also introduce the notion of *order convexity* for such sets.

Thus the nondeterministic choice of E and F also includes any convex combination of E and F. Operationally this corresponds to the idea of Segala and Lynch [18] that a nondeterministic choice could be resolved into a probabilistic choice by means of a randomized scheduler.

The distributive law (1) facilitates a semantics in which nondeterministic choice and probabilistic choice satisfy the expected laws. On the other hand, the dual requirement that nondeterministic choice distribute over probabilistic choice would force us to revise some of these laws. For example, an instance of this other distributive law is

$$(E \oplus_{\frac{1}{2}} F) + (E \oplus_{\frac{1}{2}} F) = E \oplus_{\frac{1}{4}} ((E + F) \oplus_{\frac{2}{3}} F) \,.$$

It would seem undesirable to retain the idempotence of $+$ in the presence of such an identity. In particular, it would imply that the simple fifty-fifty choice $E \oplus_{\frac{1}{2}} F$ is equal to various weighted combinations of E, F and $E + F$.

The dual distributive law tends to arise in those models where the guiding philosophy is that probabilistic choices should be resolved before nondeterministic choices. Examples of such models can be found in [13,17]. Analogously, the distributive law (1) implies that nondeterministic choices are resolved before probabilistic choices in our model.

1.1 Related Work

Stark and Smolka [19] and Baeten et al. [4] give complete axiomatizations of probabilistic bisimilarity for calculi featuring probabilistic choice, but without nondeterministic choice. The development in [19] closely follows the treatment of equations for bisimilarity in finite-state CCS by Milner [15]. Our completeness proof follows the same pattern, except that arguments based on operational semantics get replaced by domain theory.

Following Milner [15] and Stark and Smolka [19], we include a unique fixed point rule (cf. F4 in Table 1) for guarded recursion as part of our axiomatization. This is really a schema of conditional equations. By contrast, a purely equational axiomatization of probabilistic bisimilarity has recently been obtained by Aceto, Ésik and Ingólfsdóttir [2]. Their approach involved adding axioms for probabilistic choice to an underlying equational formulation of iteration theories.

Bandini and Segala [6] give a complete axiomatization of strong and weak probabilistic bisimilarity for an algebra including nondeterministic and probabilistic choice, but not recursion. One significant difference between their formulation and ours is that they introduce syntactic restrictions on the application of probabilistic choice and nondeterministic choice. For instance, the distributive law (1) would be ill-typed in their setting.

Baier and Kwiatkowska [5] consider the combination of probability and nondeterminism from a domain-theoretic perspective. Like us they produce a model for a process algebra by solving a domain equation involving the probabilistic powerdomain. However they use the Hoare powerdomain, rather than the geometrically convex Plotkin powerdomain. Furthermore they introduce probability via an operator of action-guarded probabilistic choice rather than the unrestricted probabilistic choice operator that we model. Finally they do not axiomatize their semantics.

A radically different way to model probability and nondeterminism in domain theory has been investigated by Varacca [21]. He models probabilistic choice using a monad of indexed valuations. This structure is more rigid than the usual probabilistic powerdomain (which is a quotient), and it supports a categorical distributive law over the Hoare powerdomain. Using this distributive law he defines a combined monad of probabilistic and nondeterministic choice. The corresponding equational theory however does not include the law $E \oplus_p E = E$.

Andova [3] considers the addition of probabilistic choice to the algebra ACP, studied extensively by de Bakker and his students. The pivotal issue in Andova's work is how to extend the parallel composition operator of ACP to the algebra extended to include probabilistic choice, an issue that requires considerable delicate reasoning to resolve.

Finally, the paper den Hartog [11] presents an extensive consideration to the interactions between differing forms of nondeterministic and probabilistic choice, called *local* and *global*, and which correspond to internal and external choice operators.

2 A Probabilistic Calculus

We begin by introducing our calculus PE of *probabilistic expressions*. This is the language of [19] augmented with a nondeterministic sum operator. The grammar for PE terms is as follows.

$$E ::= X \mid \mathbf{0} \mid aE \mid E + E \mid E \oplus_p E \mid \mu X E$$

where $a \in \mathrm{Act}$ and $0 < p < 1$.

Here X is a process variable, $\mathbf{0}$ is the inactive process, $E+F$ is the nondeterministic choice of E and F, and $E \oplus_p F$ is the probabilistic choice of E and F. While the index p is restricted to the open interval $(0,1)$, it is convenient to allow $E \oplus_1 F$ as a synonym for E and $E \oplus_0 F$ as a synonym for F. We write $\mathrm{fv}(E)$ for the set of free variables in a term E, and we write $E\{F/X\}$

to denote the term obtained by substituting F for all free occurrences of X in E. A closed term – i.e., one without free variables – is called a *probabilistic agent*.

It is convenient to have a notation for arbitrary finite nondeterministic and probabilistic sums. We write the sum $E_1 + (E_2 + (\cdots + E_n)\cdots)$ as $\sum_{i=1}^{n} E_i$. The empty summation $\sum_{i=1}^{0} E_i$ stands for $\mathbf{0}$. We also write the sum $E_1 \oplus_{p_1} (E_2 \oplus_{p_2} (\cdots \oplus_{p_{n-1}} E_n)\cdots)$ as $\sum_{i=1}^{n} r_i E_i$, where $r_i = p_i \times \prod_{j<i}(1-p_j)$ for $i<n$ and $r_n = \prod_{j<n}(1-p_j)$. Thus r_i is the probability that the i-th summand is selected.

We use Ω as an abbreviation for μXX, and we think of this as the divergent process. Intentionally this is different from [19,2] where μXX is interpreted as the inactive process, denoted $\mathbf{0}$. (Despite this difference in intentions we claim that the axioms presented in Section 7 yield a conservative extension of the theory presented in [19,2].)

Example 2.1 We give an example to illustrate some basic intuitions about the interaction between probability and nondeterminism in the presence of unguarded recursion. Consider the following two processes:

$$P \equiv \mu X(aX \oplus_{\frac{1}{2}} (X + bX))\,, \tag{3}$$

$$Q \equiv \mu X(aX + (aX \oplus_{\frac{1}{2}} bX))\,. \tag{4}$$

We first give an informal argument that $P = Q$. Each transition of P arises as the convex combination of the transitions of each summand of the probabilistic choice operator $\oplus_{\frac{1}{2}}$ after unwinding the recursion. The left-hand summand can only do an a-action and become P again. One possibility for the right-hand summand is to do a b-action and become P. We thus infer that one possible (probabilistic) transition of P is to do an a-action with probability $1/2$ and a b-action with probability $1/2$, and become P again in either case. This takes care of the right branch of the process Q.

We also can unwind the recursion, say n times, and then select a branch that results in a visible action – a or b. Because we also have the accumulated possibility of executing an a on each unwinding, the possible actions of P on such a sequence of unwindings together with their probabilities are to do a with probability $\frac{2^n-1}{2^n}$ and to do b with probability $\frac{1}{2^n}$, and in either case become P again. Since we have a continuous semantics, we infer that P can do a with probability 1 and then become P again, which takes care of the left branch of Q. This shows informally that P can do anything Q can.

The converse requires noting an important property of our semantics: a nondeterministic choice can be resolved by any probabilistic choice of the components. Since Q can either do a with probability 1, or do a and b with equal probability, and then become Q again, this property implies Q can do any convex combination of these behaviors. This implies Q can do a with probability $\frac{2^n-1}{2^n}$ or b with probability $\frac{1}{2^n}$ for each n, and then become Q again, which are the possible behaviors we deduced for P. Thus, on an informal basis, we conclude that $P = Q$.

Actually, we can provide a formal argument by anticipating the axioms in Table 1 from Section 7; here is a two line equational proof that $P = Q$:

$$\begin{aligned}\mu X(aX \oplus_{\frac{1}{2}} (X + bX)) &= \mu X((aX \oplus_{\frac{1}{2}} X) + (aX \oplus_{\frac{1}{2}} bX)) \text{ by D1}\\ &= \mu X(aX + (aX \oplus_{\frac{1}{2}} bX)) \text{ by F2}\,.\end{aligned}$$

3 Powerdomains

In this section we bring together the results from domain theory that we require to build and analyze our model. In particular, we define the combined powerdomain $\mathit{Pow}(D)$ and the attendant probabilistic and nondeterministic choice operators. The constructs themselves are what is important for understanding the paper. We carefully state some of the hypotheses required to make the constructions work (e.g., continuity and coherence), but we think that these technicalities may safely be omitted on a first reading.

For us a domain is a particular type of ordered set, specifically a continuous dcpo with a bottom element. A Scott-continuous map between domains is a monotone function that preserves directed suprema. If $(D, \sqsubseteq)$ is a domain and $L \subseteq D$, we write $\uparrow L$ for the set $\{x \in D : (\exists y \in L)\, y \sqsubseteq x\}$, and we write $\downarrow L$ for the set $\{x \in D : (\exists y \in L)\, x \sqsubseteq y\}$.

As usual, we will consider a domain D as a topological space in its Scott topology. Recall that $U \subseteq D$ is open in the Scott topology if it is an upper set ($U = \uparrow U$) and is inaccessible by directed suprema: for each directed set A, $\bigsqcup A \in U$ implies $A \cap U \neq \emptyset$. Another relevant topology for us is the Lawson topology. This is a Hausdorff refinement of the Scott topology, obtained by adding as sub-basic opens those sets of the form $D \setminus \uparrow d$, where $d \in D$. We will be particularly concerned with domains that are compact in the Lawson topology: the so-called *coherent domains*. This class is important for us in that it is closed under the probabilistic powerdomain (cf. [9] or [7]) and the Plotkin powerdomain, and because the latter admits a topological on coherent domains.

3.1 The Probabilistic Powerdomain

Next we introduce the probabilistic powerdomain $\mathbb{V}D$ of a domain D. The elements of $\mathbb{V}D$ are *valuations* on D. These are like probability measures, but can be defined using purely topological data. Technically, a *valuation* on D is a mapping $\nu\colon \Sigma D \to [0,1]$ from the lattice $(\Sigma D, \subseteq)$ of Scott open subsets of D to the unit interval satisfying the following laws.

- strictness
  $\nu\emptyset = 0$ and $\nu D = 1$
- modularity
  $\nu(U \cup V) + \nu(U \cap V) = \nu U + \nu V$ for all U, V.
- Scott continuity
  $\nu(\bigcup_{i\in I} U_i) = \sup_{i\in I} \nu U_i$ for every directed family $\{U_i\}_{i\in I}$.

The set of all valuations $\mathbb{V}D$ becomes a domain when equipped with the pointwise order: $\sigma \sqsubseteq \nu$ iff $\sigma U \leqslant \nu U$ for all $U \in \Sigma D$. Furthermore, $\mathbb{V}D$ is coherent whenever D is coherent [9,7].

The Scott topology on $\mathbb{V}D$ can be described directly in terms of the Scott topology on D using a probabilistic modality. The sub-basic opens are the sets

$$\Diamond_p U = \{\nu \in \mathbb{V}D : \nu U > p\}$$

where $0 \leqslant p \leqslant 1$ and $U \subseteq D$ is Scott open.

Each element $x \in D$ gives rise to a valuation δ_x defined by $\delta_x(U) = 1$ if $x \in U$, and $\delta_x(U) = 0$ otherwise. A *simple valuation* has the form $\sum_{a\in A} r_a\delta_a$ where $A \subseteq D$ is finite, each r_a is a non-negative real number, and $\sum_{a\in A} r_a = 1$. A central result about simple valuations is the Splitting Lemma; this will be used in the proof of completeness of our equational axiomatization.

Lemma 3.1 (Jones [12]) *Let* $\sigma = \sum_{a\in A} r_a\delta_a$ *and* $\nu = \sum_{b\in B} s_b\delta_b$ *be simple valuations on* D*. Then* $\sigma \sqsubseteq \nu$ *if and only if there exists a family of transport (or flow) numbers* $\{t_{a,b} \mid a \in A, b \in B\} \subseteq [0,1]$ *satisfying*

- *For each* $a \in A$, $\sum_{b\in B} t_{a,b} = r_a$,
- *For each* $b \in B$, $\sum_{a\in A} t_{a,b} = s_b$,
- $t_{a,b} \neq 0$ *implies* $a \sqsubseteq b$.

3.2 The Geometrically Convex Plotkin Powerdomain

Let D be a coherent domain. We say that $L \subseteq D$ is a *lens* if L is nonempty, compact in the Lawson topology and *order convex*, i.e., $L = \uparrow L \cap \downarrow L$. We let $\mathbb{P}D$ denote the set of all such lenses together with the emptyset, and we denote a typical element of $Pow(D)$ by X or Y. The set $\mathbb{P}D$ becomes a coherent domain when equipped with the *Egli-Milner order*. This is defined by

$$L \sqsubseteq L' \text{ iff } \downarrow L \subseteq \downarrow L' \text{ and } \uparrow L' \subseteq \uparrow L$$

for lenses L and L', and $\{\bot\} \sqsubseteq \emptyset$.

The Scott topology on $\mathbb{P}D$ can be described directly in terms of the Scott topology on D using 'may' and 'must' modalities. The sub-basic opens are the sets

$$\Box\, U = \{X \in \mathbb{P}D \mid X \subseteq U\}$$
$$\Diamond\, U = \{X \in \mathbb{P}D \mid X \cap U \neq \emptyset\}$$

where $U \subseteq D$ is Scott open.

Our model for probabilistic and nondeterministic choice is a retraction of $\mathbb{P}\mathbb{V}D$. In order to define this we first need to recall the concepts of order-convex closure and geometrically-convex closure. Given a Lawson compact set $S \subseteq \mathbb{V}D$, the order-convex closure of S is defined to be $\uparrow S \cap \downarrow S$. The geometrically-convex closure of S is defined to be $\{p\sigma + (1-p)\nu : \sigma, \nu \in S, 0 \leqslant p \leqslant 1\}$. An important fact is that both closure operators preserve Lawson compactness.

We now define the composite closure operator

$$\langle - \rangle : \mathbb{P}\mathbb{V}D \to \mathbb{P}\mathbb{V}D$$

by taking $\langle X \rangle$ to be the order-convex closure of the geometrically-convex closure of X. (Note that the order-convex closure of a geometrically convex set is still geometrically convex.) Then $\langle - \rangle$ is a Scott continuous idempotent map whose image, which we denote $Pow(D)$, is precisely the collection of geometrically-convex elements of $\mathbb{P}\mathbb{V}D$. It follows that $Pow(D)$ is a retraction of $\mathbb{P}\mathbb{V}D$ and is thus a coherent domain in the inherited order.

We can equip $Pow(D)$ with operations for probabilistic and nondeterministic sum as follows. Given S and S' in $Pow(D)$ the nondeterministic sum $X + Y$ is defined by

$$X + Y = \langle X \cup Y \rangle.$$

The probabilistic sum $X \oplus_p Y$ is defined by

$$X \oplus_p Y = \langle\, \{p\sigma + (1-p)\nu : \sigma \in S, \nu \in S'\}\, \rangle\,.$$

Given a finite set $F = \{\nu_1, \ldots, \nu_n\} \subseteq \mathbb{V}D$ we define $\{\!|\nu_1, \ldots, \nu_n|\!\}$ to be the element of $Pow(D)$ generated by L, that is,

$$\{\!|\nu_1, \ldots, \nu_n|\!\} = \langle \uparrow F \cap \downarrow F \rangle\,.$$

By standard arguments, both $+$ and $\oplus_p$ are Scott continuous as maps from $Pow(D) \times Pow(D)$ to $Pow(D)$. We also note that for lenses L and L', $L \oplus_p L'$ converges to L as p tends to 1 and it converges to L' as p tends to 0. Lastly we remark that the distributive law (1) holds in $Pow(D)$, essentially because the operation of probabilistic choice on $Pow(D)$ is defined pointwise. We refer the reader to Mislove [16] and Tix [20] for further explanation of these points.

3.3 Separated Sum

The remaining construction on domains that we use is *separated sum.* Let Act be a finite set of actions, which we fix once and for all. Given a domain D write $\coprod_{a\in \mathrm{Act}} D$ for the Act-fold coproduct of D with itself, with a new bottom element adjoined. Thus the elements of $\coprod_{a\in \mathrm{Act}} D$ other than $\perp$ are pairs $\langle a, d\rangle$ with $a \in$ Act and $d \in D$, and $\langle a, d\rangle \sqsubseteq \langle a', d'\rangle$ iff $a = a'$ and $d \sqsubseteq d'$.

4 The Domain Model

To find a domain model of PE we solve a probabilistic version of Abramsky's domain equation for bisimulation [1]. More precisely, we construct a domain D for which there is an isomorphism

$$\iota : D \cong Pow(\coprod_{a\in \mathrm{Act}} D\,) . \tag{5}$$

General domain theory [10] tells us that not only can we find such a domain, but there is a canonical such choice—the so-called *minimal invariant.* We think of this domain as a universal Segala-Lynch probabilistic automaton [18]. Following this intuition, if $\nu \in \iota(d)$, then we write $d \to \nu$—read d *has capability* ν.

Below we show how to interpret terms of the process algebra PE in the domain D. The semantics of a term E relative to an environment ρ (mapping variables to elements of D) is denoted $[\![E]\!]\rho$. Recursion is handled in the standard way using least fixed points. In the following definitions of the semantic map we have elided the isomorphism $\iota \colon D \to Pow(\coprod_{a\in \mathrm{Act}} D)$ for notational transparency.

$$\begin{aligned}
[\![\mathbf{0}]\!]\rho &= \emptyset \\
[\![aE]\!]\rho &= \{\!|\ \delta_{\langle a,[\![E]\!]\rho\rangle}\ |\!\} \\
[\![E+F]\!]\rho &= [\![E]\!]\rho + [\![F]\!]\rho \\
[\![E \oplus_p F]\!]\rho &= [\![E]\!]\rho \oplus_p [\![F]\!]\rho \\
[\![\mu X E]\!]\rho &= \mu\theta[\![E]\!](\rho[X \mapsto \theta]) \,.
\end{aligned}$$

These equations define a compositional map from PE to our domain model D, thus giving a denotational model for our process calculus.

4.1 A Domain Logic

Next we introduce a domain logic $\mathcal{L}$ for D. We use this logic as a tool to show that one element of D is below another. In particular, it is used in the proof of the soundness of some of the equational rules below (cf. Table 1). The logic is based on the topological description of the various functors underlying the construction of D. In order to fully capture a domain via a logic one should also give a proof system for telling when two formulas represent the same open set, cf. Abramsky [1]. For our purposes however this is unnecessary.

In the grammar for $\mathcal{L}$ there are two phrase types: state formulas and probabilistic formulas. This corresponds to the alternation of nondeterministic and probabilistic choice in the domain equation. State formulas are denoted by Roman letters and probabilistic formulas by Greek letters:

$$\begin{aligned} \text{(state formulas)}\ \ & f ::= f \wedge f \mid f \vee f \mid \Diamond\varphi \mid \Box\varphi \\ \text{(probabilistic formulas)}\ \ & \varphi ::= \top \mid \bot \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \langle a \rangle_p f \end{aligned}$$

where $a \in \mathrm{Act}$, and $p \in [0,1]$.

The modal depth of formulas is defined by

$$\begin{gathered} \mathrm{md}(\Box\varphi) = \mathrm{md}(\Diamond\varphi) = \mathrm{md}(\varphi) + 1 \\ \mathrm{md}(\langle a \rangle_p f) = \mathrm{md}(f)\,. \end{gathered}$$

As usual, the modal depth of a conjunction (disjunction) is the maximum of the modal depth of the conjuncts (disjuncts).

We define a satisfaction relation between elements of D and state formulas, and between elements of $\mathbb{V}(\coprod_{a\in\mathrm{Act}} D)$ and probabilistic formulas.

$$\begin{aligned} d \vDash \Diamond\varphi \ \ &\text{iff}\ \ (\exists\nu)(d \to \nu \ \wedge\ \nu \vDash \varphi) \\ d \vDash \Box\varphi \ \ &\text{iff}\ \ (\forall\nu)(d \to \nu \ \Rightarrow \nu \vDash \varphi) \\ \nu \vDash \langle a \rangle_p f \ \ &\text{iff}\ \ \nu\{\langle a, d\rangle : d \vDash f\} > p\,. \end{aligned}$$

Given $d, d' \in D$, we say that $d \preccurlyeq_n d'$ if $d \vDash f$ implies $d' \vDash f$ for each formula f with $\mathrm{md}(f) \leqslant n$. Similarly, given $\nu, \sigma \in \mathbb{V}(\coprod_{a\in\mathrm{Act}} D)$, we say that $\nu \preccurlyeq_n \sigma$ if $\nu \vDash \varphi$ implies $\sigma \vDash \varphi$ for each formula φ with $\mathrm{md}(\varphi) \leqslant n$.

Using the modal descriptions of the topologies on the powerdomains, and the inductive construction of the domain D, one can prove the following result.

Theorem 4.1 *Given $d, d' \in D$, $d \sqsubseteq d'$ iff $d \preccurlyeq_n d'$ for all $n \in \mathbb{N}$.*

In other words, the domain logic characterizes the order on the domain D.

5 Operational Semantics

In this section we define an operational semantics for PE. Later, in Section 6 we show that the domain-theoretic semantics from Section 4 is fully abstract with respect to a form of probabilistic bisimilarity we define below.

Let $\mathcal{PE}$ denote the set of all PE terms and $\mathcal{PA}$ the set of probabilistic agents, i.e., the closed terms. We let $\coprod_{a\in\mathrm{Act}}\mathcal{PE}$ stand for the flat poset of elements $\langle a, E\rangle$, where $a \in \mathrm{Act}$ and $E \in \mathcal{PE}$, ordered discretely, and with a bottom element $\perp$ adjoined. The operational semantics of PE can be seen as presenting a transition relation $E \to \mu$, where E is a term and $\mu \in \mathbb{V}(\coprod_{a\in\mathrm{Act}}\mathcal{PE})$ is a (necessarily simple) valuation. In actual fact we define a function $\mathrm{inits}(E)$ which gives the initial behaviours of a term E, i.e., $\mathrm{inits}(E) = \{\mu \mid E \to \mu\}$.

The set $\mathrm{inits}(E)$ is geometrically convex by definition. Since each transition $E \to \mu$ can be seen as arising from a scheduler resolving the nondeterminism in E, this last requirement corresponds to the possibility of having probabilistic schedulers. As we have explained earlier, this feature is crucial for our semantics to satisfy the distributive law (1) of probabilistic choice over nondeterministic choice. It also will be the case that $\mathrm{inits}(E)$ is order-convex; given the notion of bisimulation presented in Definition 6.2 it is harmless to identify a set with its order-convex closure in this context.

As we mentioned earlier, a complicating factor in defining an operational semantics for PE is the presence of unguarded recursion. For a simple example of this phenomenon, consider the term $P \equiv \mu X((aX \oplus_{\frac{1}{2}} X) + bX)$. It is clear that one possible transition is $P \to \delta_{\langle b,P\rangle}$. Slightly less obviously, another possible transition is $P \to \delta_{\langle a,P\rangle}$. This transition corresponds to a scheduler which always selects the left-hand summand in the body of the recursion; under such a scheduler it is guaranteed that the action a will occur eventually.

In the purely probabilistic setting, Stark and Smolka [19] handle unguarded recursion by separately calculating the possible transitions of a term and the probabilities with which they occur. These probabilities are calculated as least fixed points. Our approach is similar in spirit, but necessarily more complex in the presence of nondeterminism.

To handle unguarded recursion we introduce environments in our operational semantics. Given a set of variables $\widetilde{X} = \{X_1, \ldots, X_n\}$, an environment is a function

$$\sigma\colon \{X_1, \ldots, X_n\} \to Pow(\textstyle\coprod_{a\in\mathrm{Act}}\mathcal{PE})$$

giving the initial transitions of each variable X_i. We write $\mathrm{inits}(E, \sigma)$ for the initials of a term E in free variables $\widetilde{X}$ with respect to the environment σ; this is an element of $Pow(\coprod_{a\in\mathrm{Act}}\mathcal{PE})$. The definition of $\mathrm{inits}(E, \sigma)$ is by a nested induction: first by induction on the number of occurrences in E of a subterm of the form μXF which is *not* within the scope of a prefixing operator, and then by structural induction on E. The clauses in the definition are as follows:

- $\mathrm{inits}(\mathbf{0},\sigma)=\emptyset$
- $\mathrm{inits}(X,\sigma)=\sigma(X)$
- $\mathrm{inits}(aE,\sigma)=\{\delta_{\langle a,E\rangle}\}$
- $\mathrm{inits}(E+F,\sigma)=\mathrm{inits}(E,\sigma)+\mathrm{inits}(F,\sigma)$
- $\mathrm{inits}(E\oplus_p F,\sigma)=\mathrm{inits}(E,\sigma)\oplus_p \mathrm{inits}(F,\sigma)$
- $\mathrm{inits}(\mu XE,\sigma)=\mu\theta\,\mathrm{inits}(E',\sigma[X\mapsto\theta])$, where E' arises by substituting μXE for all *guarded* occurrences of X in E.

The last clause says that $\mathrm{inits}(\mu XE,\sigma)$ is the least solution of the equation

$$\theta=\mathrm{inits}(E',\sigma[X\mapsto\theta])$$

in the domain $Pow(\coprod_{a\in\mathrm{Act}}\mathcal{PE})$. Observe that if X is guarded in E, then E' is just $E\{\mu XE/X\}$, so X does not occur free in E' and the given fixed point is reached in one step. In fact the fixed point in this clause is solely directed toward unguarded occurrences of the variable X.

Example 5.1 Consider the agent $P\equiv\mu X((aX\oplus_{\frac{1}{2}}X)+bX)$. Then $\mathrm{inits}(P)$ is the least solution of the equation

$$\theta=\mathrm{inits}((aP\oplus_{\frac{1}{2}}X)+bP,[X\mapsto\theta])\,.$$

This can be constructed as the join in $Pow(\coprod_{a\in\mathrm{Act}}\mathcal{PA})$ of the following chain

$$\{\delta_\perp\},\{\delta_{\langle b,P\rangle},\tfrac{1}{2}\delta_{\langle a,P\rangle}+\tfrac{1}{2}\delta_\perp\},\{\delta_{\langle b,P\rangle},\tfrac{3}{4}\delta_{\langle a,P\rangle}+\tfrac{1}{4}\delta_\perp,\tfrac{1}{2}\delta_{\langle a,P\rangle}+\tfrac{1}{2}\delta_{\langle b,P\rangle}\},\cdots$$

which is equal to $\{\delta_{\langle a,P\rangle},\delta_{\langle b,P\rangle}\}$.

6 Full Abstraction

Theorem 6.1 expresses the compatibility of the operational semantics defined above with the denotational model $D\cong Pow(\coprod_{a\in\mathrm{Act}}D)$ from Section 4. Technically it says that the denotational map $[\![-]\!]\colon\mathcal{PA}\to D$ is a coalgebra homomorphism, cf. [1].

Theorem 6.1 *The following diagram commutes*

$$\begin{tikzcd}
\mathcal{PA} \arrow[r, "\mathrm{inits}"] \arrow[d, "{[\![-]\!]}"'] & Pow(\coprod_{a\in\mathrm{Act}}\mathcal{PA}) \arrow[d, "Pow(\coprod_{a\in\mathrm{Act}}{[\![-]\!]})"] \\
D \arrow[r, "\iota"'] & Pow(\coprod_{a\in\mathrm{Act}}D)
\end{tikzcd}$$

Proof. (Sketch) The proof follows the inductive structure of the definition of inits(P). The induction cases for prefixing, nondeterministic choice and probabilistic choice are immediate and exploit the similarity of the corresponding clauses in the definitions of inits and $[\![-]\!]$. The induction case for recursion relies on a compatibility between the respective fixpoint constructions in the operational and denotational semantics of recursion. $\square$

6.1 Bisimulation and Modal Logic

Our domain-theoretic semantics for probabilistic agents corresponds to a version of probabilistic bisimulation. Definitions of bisimulation for agents featuring both probabilistic choice and nondeterministic choice have appeared in [18,13]. The definition below is slightly different since we take account of divergence in our operational semantics.

Let R be a relation on $\mathcal{PA}$. We extend R to a relation on $\coprod_{a\in\mathrm{Act}}\mathcal{PA}$ by defining

$$\begin{aligned} \langle a,E\rangle\, R\, \langle b,F\rangle &\text{ iff } a=b \text{ and } E\, R\, F \\ \bot\, R\, \langle b,F\rangle &\text{ for all } b,F \\ \bot\, R\, \bot & \end{aligned}$$

Next we define the relation $\preccurlyeq_R$ on $\mathbb{V}(\coprod_{a\in\mathrm{Act}}\mathcal{PA})$ by $\mu\preccurlyeq_R\nu$ if $\mu(O)\leqslant\nu(R(O))$ for all $O\subseteq\coprod_{a\in Act}\mathcal{PA}$, where $R(O)$ is the image of O under R.

Definition 6.2 We say that a relation R on $\mathcal{PA}$ is a *partial probabilistic bisimulation* [1] if $P\,R\,Q$ implies

- $P\to\mu$ implies $(\exists\nu)(Q\to\nu$ and $\mu\preccurlyeq_R\nu)$
- $Q\to\nu$ implies $(\exists\mu)(P\to\mu$ and $\mu\preccurlyeq_R\nu)$.

If agents P and Q are related by a partial probabilistic bisimulation then we write $P\sqsubseteq Q$.

We can use the operational semantics for PE to define a satisfaction relation between probabilistic agents and formulas of the logic $\mathcal{L}$ introduced in Section 4. In fact this definition is syntactically almost identical to the corresponding definition in Section 4. The three clauses are

$$\begin{aligned} P\vDash\Diamond\varphi &\text{ iff } (\exists\nu)(P\to\nu\ \wedge\ \nu\vDash\varphi) \\ P\vDash\Box\varphi &\text{ iff } (\forall\nu)(P\to\nu\ \Rightarrow\nu\vDash\varphi) \\ \nu\vDash\langle a\rangle_p f &\text{ iff } \nu\{\langle a,P\rangle : P\vDash f\}>p\,. \end{aligned}$$

As a corollary of the compatibility of the operational and denotational semantics for PE, as expressed in Theorem 6.1, we obtain the following result relating the two semantics for the logic $\mathcal{L}$.

Corollary 6.3 *For each probabilistic agent P and formula f on $\mathcal{L}$, $P \models f$ iff $[\![P]\!] \models f$.*

Proof. By induction on the modal depth of f, using Theorem 6.1 for the induction step. □

The following result says that the logic $\mathcal{L}$ characterizes probabilistic agents up to bisimilarity. It is a slight variant of [13, Theorem 8].

Theorem 6.4 *Given probabilistic agents P and Q, $P \sqsubseteq Q$ iff $P \models f$ implies $Q \models f$ for all formulas $f \in \mathcal{L}$.*

The following theorem is the main result of this section. It says that the domain semantics for probabilistic agents is fully abstract with respect to partial probabilistic bisimilarity.

Theorem 6.5 *Given probabilistic agents P and Q, $P \sqsubseteq Q$ iff $[\![P]\!] \sqsubseteq [\![Q]\!]$.*

Proof.

$$\begin{aligned} P \sqsubseteq Q \ &\text{iff } (\forall f \in \mathcal{L})(P \models f \Rightarrow Q \models f) \quad \text{(by Theorem 6.4)} \\ &\text{iff } (\forall f \in \mathcal{L})([\![P]\!] \models f \Rightarrow [\![Q]\!] \models f) \quad \text{(by Corollary 6.3)} \\ &\text{iff } [\![P]\!] \sqsubseteq [\![Q]\!] \quad \text{(by Theorem 4.1)}\,. \end{aligned}$$

□

7 Equations

The following table gives a list of (in)equations between PE terms. These will be shown to be sound and complete with respect to the domain model D.

The semilattice equations N1–N4 are exactly the axioms for strong bisimilarity from [15]. The equations P1–P3 are the axioms for probabilistic bisimilarity from [19]. Nondeterministic choice and probabilistic choice interact via the distributive laws D1 and D2. The remaining equations concern recursion. Rule F4 implies that guarded recursions have unique fixed points. (A variable X is *guarded* in a term E if each free occurrence of X in E appears in a subterm of the form aE'.) Rules F1 and F2 show how to eliminate unguarded variables from recursive definitions.

One can think of the distributive laws D1 and D2 as saying that in an expression $E \oplus_p F$ the nondeterministic choices of E and F are resolved first, and then combined probabilistically. In particular, if F represents the empty choice, as in D2, then $E \oplus_p F$ is inert. On the other hand, if we are guided by the dual distributive law, as in [13], then $E \oplus_p \mathbf{0}$ denotes an agent which behaves like E with probability p and $\mathbf{0}$ with probability $1 - p$. We also note

Ω	$\Omega \sqsubseteq E$
N1	$E + F = F + E$
N2	$E + (F + G) = (E + F) + G$
N3	$E = E + E$
N4	$E + \mathbf{0} = E$
P1	$E \oplus_p E = E$
P2	$E \oplus_p F = F \oplus_{1-p} E$
P3	$E \oplus_p (F \oplus_q G) = (E \oplus_{\frac{p}{p+q-pq}} F) \oplus_{p+q-pq} G$
D1	$(E + F) \oplus_p G = (E \oplus_p G) + (F \oplus_p G)$
D2	$E \oplus_p \mathbf{0} = \mathbf{0}$
F1	$\mu X(E + X) = \mu X(E + \Omega)$
F2	$\mu X((E \oplus_p X) + F) = \mu X(E + F)$
F3	$\mu X E = E\{\mu X E/X\}$
F4	From $E = F\{E/X\}$ and $F\{E'/X\} \sqsubseteq E'$, X guarded in F, infer $E \sqsubseteq E'$.

Fig. 1. (In)equations for PE terms

that in the process algebras studied in [5,6] the nil process $\mathbf{0}$ cannot appear as a summand in a probabilistic choice owing to certain syntatic restrictions.

We write $\vdash E \sqsubseteq F$ to indicate that there is a deduction of $E \sqsubseteq F$. The provability relation $\vdash$ is extended pointwise to term vectors.

One straightforward but important consequence of axioms D1 and P1 is

$$\vdash E + F = E + (E \oplus_p F) + F. \tag{6}$$

A special case of this convexity equation occurs as an axiom in the presentation of Bandini and Segala [6].

Following the pattern of [15,19] the completeness of this system hinges on a couple of important transformations that can be effected by combinations of the equations. The first of these is the standard de Bakker-Bekic-Scott construction of solutions of mutually recursive definitions. This is embodied in the following proposition, which is [15, Theorem 5.7].

Proposition 7.1 (Solution Lemma) *Let $\widetilde{X} = (X_1, \ldots, X_m)$ and $\widetilde{Y} = (Y_1, \ldots, Y_n)$ be vectors of distinct variables, and $\widetilde{G} = (G_1, \ldots, G_m)$ a vector of terms with free variables in $(\widetilde{X}, \widetilde{Y})$ in which each X_i is guarded. Then there exist expressions $\widetilde{E} = (E_1, \ldots, E_m)$ with free variables in $\widetilde{Y}$ such that*

$$\vdash \widetilde{E} = \widetilde{G}\{\widetilde{E}/\widetilde{X}\}.$$

Moreover, if $\widetilde{F} = (F_1, \ldots, F_m)$ is a vector of terms with free variables in $\widetilde{Y}$ such that $\vdash \widetilde{G}\{\widetilde{F}/\widetilde{X}\} \sqsubseteq \widetilde{F}$, then $\vdash \widetilde{E} \sqsubseteq \widetilde{F}$.

Definition 7.2 A *simple term* is either Ω, a variable, or a prefix aE. A *standard form* is a term of the form

$$\sum_{i=1}^{m} \sum_{j=1}^{n(i)}\!\!\!\!\!\!\bigcirc\; r_{ij} E_{ij}$$

where each E_{ij} is a simple term.

Thus a standard form is a nondeterministic sum, with each summand being a probabilistic sum of simple terms. If a term aE occurs as one of the E_{ij} then we say that E is a *derivative* of the standard form.

The next proposition says that each PE term E is provably equal to the first coordinate of term vector $\widetilde{E}$ which is the solution of a recursive definition.

Proposition 7.3 (Standard Forms) *For any term E with free variables in $\widetilde{Y}$, there are terms $E_1, \ldots, E_k$ also with free variables in $\widetilde{Y}$ such that $\vdash E = E_1$ and each E_i is provably equal to a standard form where each derivative is taken from the set $\{E_1, \ldots, E_k\}$. Thus, for instance,*

$$\vdash E_1 = \sum_{i=1}^{m} \left(\sum_{j=1}^{n(i)}\!\!\!\!\!\!\bigcirc\; r_{ij} a_{ij} E_{f(i,j)} \oplus_{p(i)} \sum_{j=1}^{n'(i)}\!\!\!\!\!\!\bigcirc\; s_{ij} Y_{g(i,j)} \oplus_{q(i)} \Omega \right).$$

Similar equations hold for each of the E_i.

Proof. (Sketch) The proof is by structural induction on E. The distributive laws D1 and D2 are used to handle the inductive case $E \equiv F \oplus_p G$. The fixed point equations F1–F3 are used to handle the inductive case $E \equiv \mu X F$. □

8 Soundness and Completeness

The following theorem, the main result of this paper, asserts that the equations above are sound and complete for the model D.

Theorem 8.1 $\vdash E \sqsubseteq F$ *iff* $[\![E]\!] \sqsubseteq [\![F]\!]$.

The soundness of the axioms N1–N4, P1–P3, D1 and D2 follows immediately from the relevant algebraic properties of the operations $+$ and $\oplus_p$ on $Pow(D)$. We can now bootstrap the soundness of the fixed-point laws F1–F4. We explain two cases in some detail in order to show how the domain-theoretic underpinnings can be put to work.

8.1 Soundness of F2

For simplicity, to avoid mentioning environments, we assume that the only free variable occurring in E and F is X. We also omit semantic brackets, treating terms E and F directly as functions on our semantic domain D.

Suppose $d \in D$ is a fixed point of $E + F$, that is, $d = E(d) + F(d)$. Then

$$\begin{aligned}(E(d) \oplus_p d) + F(d) &= (E(d) \oplus_p (E(d) + F(d))) + F(d)\\ &= E(d) + (E(d) \oplus_p F(d)) + F(d) \quad \text{(distributivity)}\\ &= E(d) + F(d) \quad \text{(convexity)}\\ &= d\,.\end{aligned}$$

Thus d is also a fixed point of $(E \oplus_p X) + F$. Since recursion is modelled by *least* fixed points, it follows that $[\![\mu X((E \oplus_p X) + F)]\!] \sqsubseteq [\![\mu X(E + F)]\!]$.

On the other hand, suppose $d = (E(d) \oplus_p d) + F(d)$. We show that d is also a prefixed point of $E + F$ and conclude that $[\![\mu X(E + F)]\!] \sqsubseteq [\![\mu X((E \oplus_p X) + F)]\!]$. To this end, consider the following derivation.

$$\begin{aligned}d &= (E(d) \oplus_p d) + F(d)\\ &= (E(d) \oplus_p ((E(d) \oplus_p d) + F(d))) + F(d)\\ &= (E(d) \oplus_p (E(d) \oplus_p d)) + (E(d) \oplus_p F(d)) + F(d)\\ &= (E(d) \oplus_{2p-p^2} d) + (E(d) \oplus_p F(d)) + F(d)\,.\end{aligned}$$

One can further transform the last expression above by rewriting the subterm d to $(E(d) \oplus_p d) + F(d)$ and then simplifying using distributivity and convexity (2). By repeatedly performing these transformations one obtains a sequence of expressions of the form

$$(E(d) \oplus_{r_n} d) + (E(d) \oplus_{s_n} F(d)) + F(d)$$

that are all equal to d and such that r_n and s_n tend to 1. From the continuity properties of the operators $+$ and $\oplus_p$ this sequence converges in the Scott topology to $E(d) + F(d)$. It follows that $E(d) + F(d) \sqsubseteq d$. Thus d is indeed a prefixed point of $E + F$.

8.2 Soundness of F4

Suppose that F is a term in which the variable X is guarded. Furthermore suppose that E and E' are terms with $[\![E]\!] = [\![F\{E/X\}]\!]$ and $[\![F\{E'/X\}]\!] \sqsubseteq [\![E']\!]$, that is, E is a fixed point of F and E' is a prefixed point of F. To demonstrate the soundness of F4 we have to show that $[\![E]\!] \sqsubseteq [\![E']\!]$. This follows from the lemma below (by taking $G \equiv X$).

Lemma 8.2 *Let G be a term with* $\mathrm{fv}(G) \subseteq \mathrm{fv}(F)$*; then* $[\![G\{E/X\}]\!] \sqsubseteq [\![G\{E'/X\}]\!]$.

Proof. We prove by induction that $[\![G\{E/X\}]\!] \preccurlyeq_n [\![G\{E'/X\}]\!]$ for each $n \in \mathbb{N}$. By Theorem 4.1 this entails the desired result. For simplicity, to avoid mentioning environments, we suppose that X is the only variable occurring free in F.

The variable X is guarded in $G\{F/X\}$. Thus $G\{F/X\}$ has standard form

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n(i)} r_{ij} a_{ij} G_{ij} \;\; \oplus_{p(i)} \Omega \right) .$$

From the soundness of all the laws excepting F4 it follows that each term has the same denotation as its standard form. Thus

$$\begin{aligned} [\![G\{E/X\}]\!] &= [\![G\{F\{E/X\}/X\}]\!] \\ &= [\![G\{F/X\}\{E/X\}]\!] \\ &= [\![\sum_{i=1}^{m} \left(\sum_{j=1}^{n(i)} r_{ij} a_{ij} G_{ij}\{E/X\} \oplus_{p(i)} \Omega \right)]\!] . \end{aligned} \tag{7}$$

Similarly one has

$$[\![G\{E'/X\}]\!] \sqsupseteq [\![\sum_{i=1}^{m} \left(\sum_{j=1}^{n(i)} r_{ij} a_{ij} G_{ij}\{E'/X\} \oplus_{p(i)} \Omega \right)]\!] . \tag{8}$$

The induction hypothesis entails that $[\![G_{ij}\{E/X\}]\!] \preccurlyeq_n [\![G_{ij}\{E'/X\}]\!]$ for each pair i, j. The induction step relies on the structural similarities between the standard forms (7) and (8). In particular, for each capability ν of $[\![G\{E/X\}]\!]$ there is a capability σ of $[\![G\{E'/X\}]\!]$ with $\nu \preccurlyeq_n \sigma$. Conversely for each capability σ of $[\![G\{E'/X\}]\!]$ there is a capability ν of $[\![G\{E/X\}]\!]$ with $\nu \preccurlyeq_n \sigma$. It immediately follows that $[\![G\{E/X\}]\!] \preccurlyeq_{n+1} [\![G\{E'/X\}]\!]$. □

8.3 Completeness

Below we give a skeleton proof of the completeness of our axioms.

Suppose E and F are terms, which for simplicity are assumed to be closed, such that $[\![E]\!] \sqsubseteq [\![F]\!]$. By Proposition 7.3 there is a vector of closed terms $\widetilde{E} = (E_1, \ldots, E_k)$, and a vector $\widetilde{G} = (G_1, \ldots, G_k)$ of terms in free variables $\widetilde{X} = (X_1, \ldots, X_k)$, such that each G_i is a standard form, $\vdash E = E_1$, and

$$\vdash \widetilde{E} = \widetilde{G}\{\widetilde{E}/\widetilde{X}\}\,.$$

Similarly, there is a vector of closed terms $\widetilde{F} = (F_1, \ldots, F_l)$, and a vector of terms $\widetilde{H} = (H_1, \ldots, H_l)$ in variables $\widetilde{Y} = (Y_1, \ldots, Y_l)$, such that each F_j is a standard form, $\vdash F = F_1$, and

$$\vdash \widetilde{F} = \widetilde{H}\{\widetilde{F}/\widetilde{Y}\}\,.$$

Thus $\widetilde{E}$ and $\widetilde{F}$ can be seen as fixed points of two different term vectors $\widetilde{G}$ and $\widetilde{H}$. The heart of the completeness proof is to distill from $\widetilde{G}$ and $\widetilde{H}$ a 'product vector' $\widetilde{P}$, all of whose free variables are guarded, and which (roughly speaking) has $\widetilde{E}$ as a fixed point and $\widetilde{F}$ as a prefixed point. One then appeals to Proposition 7.1 to conclude that $\vdash E \sqsubseteq F$. A key technical ingredient in the construction of $\widetilde{P}$ is the Splitting Lemma. This is used to realize probability distributions occurring in $\widetilde{G}$ and $\widetilde{H}$ as marginals of joint distributions in $\widetilde{P}$.

Next we give a more detailed recipe for constructing the term vector $\widetilde{P}$. Let $R = \{(i,j) : [\![E_i]\!] \sqsubseteq [\![F_j]\!]\}$. Thus, in particular, $(1,1) \in R$. Let $\widetilde{Z}$ be a vector of variables indexed over R. We define $\widetilde{P}$ to be a vector of terms indexed over R such that each component of $\widetilde{P}$ is a term in free variables $\widetilde{Z}$ in standard form. As an example we illustrate how to construct the term $P_{(1,1)}$.

Suppose that E_1 has the following standard-form expansion

$$\vdash E_1 = \sum_{i=1}^{m} \left(\sum_{j=1}^{n(i)} r_{ij} a_{ij} E_{f(i,j)} \oplus_{p(i)} \Omega \right) . \qquad (9)$$

Also we have the standard-form expansion of F_1,

$$\vdash F_1 = \sum_{i=1}^{m'} \left(\sum_{j=1}^{n'(i)} r'_{ij} a'_{ij} F_{f'(i,j)} \oplus_{p'(i)} \Omega \right) . \qquad (10)$$

Since $[\![E_1]\!] \sqsubseteq [\![F_1]\!]$, by the definition of the order on the geometrically convex powerdomain, we have that each summand in (9) (of the outer sum) is less than some convex combination of summands in (10). By the convexity equation (6) there is no loss of generality in assuming that each summand in (9) is less than some summand in (10). For instance, suppose that the first summand in (9) is less than the first summand in (10), i.e.,

$$[\![\sum_{i=1}^{n(1)} r_{1i}a_{1i}E_{f(1,i)} \oplus_{p(1)} \Omega]\!] \sqsubseteq [\![\sum_{j=1}^{n'(1)} r'_{1j}a'_{1j}F_{f'(1,j)} \oplus_{p'(1)} \Omega]\!] \,.$$

Applying the Splitting Lemma to this inequality, there is a family s_{ij} of non-negative real numbers such that whenever $s_{ij} > 0$, then

- $a_{1i} = a'_{1j}$
- $f(1,i)Rf'(1,j)$
- $\sum_{j=1}^{n'(1)} s_{ij} = r_{1i}$
- $\sum_{i=1}^{n(1)} s_{ij} \leqslant r'_{1j}$.

We thus generate the term

$$\sum_{i,j=1}^{i=n(1),j=n'(1)} s_{ij}a_{1i}Z_{(f(1,i),f'(1,j))} \oplus_{p(1)} \Omega \,.$$

Each inequality between summands in the standard forms for E_1 and F_1 generates a term like the one above. Then $P_{(1,1)}$ is taken to be the nondeterministic sum of the terms so generated.

Finally, the conditions on s_{ij} generated by the Splitting Lemma guarantee that $\widetilde{E}$ is provably a fixed point of the term vector $\widetilde{P}$, and $\widetilde{F}$ is provably a prefixed point of the same term vector.

9 Summary

The main construction of this paper uses a powerdomain combining probabilistic choice and nondeterminism as the basis for a domain equation whose solution gives a denotational model that is sound and complete for the axioms we listed in Section 7. The other main contribution of the paper is Theorem 6.5 which asserts that the domain model is fully abstract with respect to partial probabilistic bisimilarity. These results have their inspiration in two preceding works: the development of a domain equation for bisimulation from [1], and the presentation of a powerdomain combining nondeterminism and probabilistic choice in [16,20].

Analogous results have been devised for other models for probabilistic choice, a number of which have been mentioned in Subsection 1.1. While some of these related works consider probabilistic choice and nondeterminism together, we know of no presentation of a sound and complete logic for a model combining both forms of nondeterminism with recursion. Furthermore, we use a denotational model to reason about the algebra we study. We believe that attempting to analyze our algebra directly in terms of a purely operational semantics would significantly increase the complexity of many of the proofs. A major feature of our approach is our ability to use "off-the-shelf" results from domain theory, such as the topological representation of our powerdomain model, and the Splitting Lemma, which is a central result about the probabilistic powerdomain.

There is a close link between our model and that of [19], which we have already alluded to in Subsection 1.1 and elsewhere. In [19], Stark and Smolka consider a variant of CCS in which probabilistic choice *replaces* nondeterministic choice. If we restrict attention to the subalgebra of purely probabilistic processes (i.e., those which do not employ nondeterminism), then two such processes are equivalent in our semantics if and only if they are equivalent in the Stark–Smolka semantics.

Furthermore, in the Stark–Smolka approach, the process $\mu X\, X$ has no transitions. This is reflected in their semantics by the fact that processes make transitions to subprobability distributions – ones with total mass ≤ 1. On the other hand, our semantics gives the process $\mu X\, X$ a single transition, to the probability measure $\delta_\perp$, and in our semantics, processes make transitions to probability distributions. The link between the two is that a process P in the Stark–Smolka semantics with total mass $v < 1$ corresponds to the process in our semantics that has component $(1-v)\delta_\perp$, and whose remaining distribution is the same as in the Scott–Smolka approach.

References

[1] S. Abramsky. A Domain Equation for Bisimulation. *Information and Computation* **92** (1991), pp. 161–218.

[2] L. Aceto, Z. Esik and A. Ingólfsdóttir. Equational Axioms for Probabilistic Bisimilarity. In *Proceedings of 9th AMAST*, Lecture Notes in Computer Science **2422** (2002), pp. 239–253.

[3] S. Andova, Process algebra with probabilistic choice, Proc. ARTS'99, Bamberg, Germany, J.-P. Katoen, ed., Lecture Notes in Computer Science **1601** (1999), Springer-Verlag, pp. 111-129.

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

[5] C. Baier and M. Kwiatkowska. Domain Equations for Probabilistic Processes. *Mathematical Structures in Computer Science* **10** (2000), pp. 665–717.

[6] E. Bandini and R. Segala. Axiomatizations for probabilistic bisimulation. *Proceedings of ICALP 2001*, Lecture Notes in Computer Science**2076** (2001), pp. 370–381.

[7] F. van Breugel, M. Mislove, J. Ouaknine and J. Worrell. An intrinsic characterization of approximate probabilistic bisimilarity. *Proceedings of FOSSACS 2003*, Lecture Notes in Computer Science **2620** (2003), Springer Verlag, pp. 200-215.

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

[9] A. Jung and R. Tix. The Troublesome Probabilistic Powerdomain. In *Third Workshop on Computation and Approximation, Proceedings*. Electronic Notes in Theoretical Computer Science **13** (1998), http://www.elsevier.nl/locate/entcs/volume13.html.

[10] G. Gierz, H. Hofmann, K. Keimel, J. Lawson, M. Mislove, D. Scott. *Continuous Lattices and Domains*, Cambridge, 2003.

[11] J.I. den Hartog, Probabilistic Extensions of Semantical Models, PhD thesis, Vrije Universiteit Amsterdam, 2002.

[12] C. Jones. *Probabilistic nondeterminism*, PhD Thesis, Univ. of Edinburgh, 1990.

[13] B. Jonsson, K. Larsen and W. Yi. Probabilistic Extensions of Process Algebras. In J.A. Bergstra, A. Ponse and S. Smolka, editors, *Handbook of Process Algebra*, pages 685–710, Elsevier, 2001.

[14] K.G. Larsen and A. Skou. Bisimulation through Probabilistic Testing. *Information and Computation* **94(1)** (1991), pp. 1–28.

[15] R. Milner. A complete inference system for a class of regular behaviours. *Journal of Computer and System Sciences* **28** (1984), pp. 439–466.

[16] M. Mislove. Nondeterminism and probabilistic choice: obeying the laws. In *Proceedings 11th CONCUR*, Lecture Notes in Computer Science **1877** (1999), pp. 350–364.

[17] C. Morgan, A. McIver, K. Seidel, J. Sanders. *Refinement-oriented probability for CSP*, Oxford University Computing Laboratory Technical Report TR-1294, 1994.

[18] R. Segala and N. Lynch. Probabilistic simulations for probabilistic processes. *Proceedings of CONCUR 94*, Lecture Notes in Computer Science **839** (1994), pp. 481–496.

[19] E.W. Stark and S.A. Smolka. A complete axiom system for finite-state probabilistic processes. In *Proof, Language, and Interaction: Essays in Honour of Robin Milner.* MIT Press, 2000.

[20] R. Tix. *Continuous D-cones: Convexity and Powerdomain Constructions*. PhD thesis, Technische Universität Darmstadt, 1999.

[21] D. Varacca. The Powerdomain of Indexed Valuations. In *Proceedings of 17th LICS*, IEEE Computer Society Press, 2002.