Basic Research in Computer Science

BRICS RS-02-38 D. Varacca: The Powerdomain of Indexed Valuations

The Powerdomain of Indexed Valuations

Daniele Varacca

BRICS Report Series **RS-02-38**

ISSN 0909-0878 **September 2002**

Copyright © 2002, Daniele Varacca.
BRICS, Department of Computer Science
University of Aarhus. All rights reserved.

Reproduction of all or part of this work
is permitted for educational or research use
on condition that this copyright notice is
included in any copy.

See back inner page for a list of recent BRICS Report Series publications.
Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/02/38/`

The powerdomain of indexed valuations

This is an extended version of a paper appearing in proceeding of LICS 02

Daniele Varacca
BRICS[*]*- University of Aarhus, Denmark*
Computer Laboratory - University of Cambridge, UK
varacca@brics.dk

September 2, 2002

Abstract

This paper is about combining nondeterminism and probabilities. We study this phenomenon from a domain theoretic point of view. In domain theory, nondeterminism is modeled using the notion of powerdomain, while probability is modeled using the powerdomain of valuations. Those two functors do not combine well, as they are. We define the notion of powerdomain of indexed valuations, which can be combined nicely with the usual nondeterministic powerdomain. We show an equational characterization of our construction. Finally we discuss the computational meaning of indexed valuations, and we show how they can be used, by giving a denotational semantics of a simple imperative language.

Contents

1 Introduction **2**

[*]Basic Research in Computer Science (www.brics.dk),
funded by the Danish National Research Foundation.

2 Indexed valuations in the category of sets **6**
2.1 Definition 6
2.2 Equational characterization 13

3 The construction of Tix and Mislove in the category of sets **17**

4 Indexed valuations in the category of continuous domains **21**
4.1 Definition 21
4.2 Equational characterization 24
4.3 A distributive law (categorically) 29
4.4 A distributive law (equationally) 35

5 The Construction of Tix and Mislove **39**

6 Semantics of programs **39**
6.1 The operational model 40
6.2 A simple imperative language 41
6.3 Denotational semantics for the finite fragment 46
6.4 Denotational semantics for the full language 48
6.5 Denotational semantics using Tix-Mislove 50

7 Future Work **53**

1 Introduction

Nondeterminism and probability are computational effects whose semantics has been thoroughly studied. The combination of the two appears to be essential in giving models for concurrent processes [Var85, Han91, SL95]. Denotationally, nondeterminism is handled by the notion of powerdomain functor in a suitable category of domains [Plo83], while probabilistic behavior is handled by the powerdomain of valuations [Jon90, Kir93]. They happen to be monads, thus fitting the general idea, introduced by Moggi, of monads as models for computational effects [Mog91].

A general way for combining two monads is by defining a *distributive law* [Bec69]. Suppose we have two monads (T, η^T, μ^T), (S, η^S, μ^S) on some category. A *distributive law* of S over T is a natural transformation $d : ST \stackrel{\cdot}{\longrightarrow} TS$ satisfying the following axioms:

- $d \circ \eta^S T = T\eta^S$
- $d \circ S\eta^T = \eta^T S$
- $d \circ \mu^S T = T\mu^S \circ dS \circ Sd$
- $d \circ S\mu^T = \mu^T S \circ Td \circ dT$

With a distributive law we can define a monad on the functor TS:
if $d : ST \dot{\longrightarrow} TS$ is a distributive law, then $\big(TS, \eta^T\eta^S, (\mu^T\mu^S) \circ TdS\big)$ is a monad.

$$TSTS \xrightarrow[TdS]{\cdot} TTSS \xrightarrow[\mu^T\mu^S]{\cdot} TS$$

Now, let (P, η^P, μ^P) be the finite nonempty powerset monad, and (V, η^V, μ^V) be the finite probability distribution monad in the category **SET**. If we want to build some kind of "combined" monad, we have to face the following obstacle:

Proposition 1.1. *There is no distributive law of V over P.*

Proof: The idea for this proof is due to Gordon Plotkin[1]. Assume that $d : VP \dot{\longrightarrow} PV$ is a distributive law. Consider the set $X := \{a, b, c, d\}$. Take $\Xi := \frac{1}{2}\delta_{\{a,b\}} + \frac{1}{2}\delta_{\{c,d\}} \in VP(X)$. We try to find out what $R := d_X(\Xi)$ is.
Let $Y := \{a, b\}$. Consider:

$$f : X \to Y \quad f : \begin{cases} a & \mapsto & a \\ b & \mapsto & b \\ c & \mapsto & a \\ d & \mapsto & b \end{cases}$$

$$f' : X \to Y \quad f' : \begin{cases} a & \mapsto & a \\ b & \mapsto & b \\ c & \mapsto & b \\ d & \mapsto & a\,. \end{cases}$$

Consider the naturality diagram for f:

$$\begin{array}{ccc} \Xi & \xmapsto{d_X} & R \\ {\scriptstyle VP(f)}\downarrow & & \downarrow{\scriptstyle PV(f)} \\ \delta_Y & \xmapsto[d_Y]{} & S. \end{array}$$

[1]Personal communication.

One of the unit laws for d tells us that $S := d_Y(\delta_Y) = \{\delta_a, \delta_b\}$. Therefore, considering the functorial action of PV, we must have that

$$\emptyset \neq R \subseteq \left\{p\delta_a + (1-p)\delta_c \mid p \in [0,1]\right\} \cup \left\{q\delta_b + (1-q)\delta_d \mid q \in [0,1]\right\}$$

Consider the same diagram for f':

$$\begin{array}{ccc} \Xi & \xrightarrow{d_X} & R \\ {\scriptstyle VP(f')}\downarrow & & \downarrow{\scriptstyle PV(f')} \\ \delta_Y & \xrightarrow[d_Y]{} & S. \end{array}$$

This tells us that

$$\emptyset \neq R \subseteq \left\{p'\delta_a + (1-p')\delta_d \mid p' \in [0,1]\right\} \cup \left\{q'\delta_b + (1-q')\delta_c \mid q \in [0,1]\right\}.$$

Combining these pieces of information we conclude that R must be a nonempty subset of $\{\delta_a, \delta_b, \delta_c, \delta_d\}$.

Now let $Z := \{a, c\}$. Consider

$$f'' : X \to Z \quad f'' : \begin{cases} a & \mapsto & a \\ b & \mapsto & a \\ c & \mapsto & c \\ d & \mapsto & c\,. \end{cases}$$

Let us look at the naturality diagram for f'':

$$\begin{array}{ccc} \Xi & \xrightarrow{d_X} & R \\ {\scriptstyle VP(f'')}\downarrow & & \downarrow{\scriptstyle PV(f'')} \\ \frac{1}{2}\delta_{\{a\}} + \frac{1}{2}\delta_{\{c\}} & \xrightarrow[d_Z]{} & T. \end{array}$$

Since $T = PV(f'')(R)$, then T must be a nonempty subset of $\{\delta_a, \delta_c\}$. But the other unit law for d tells us that $T = d(\frac{1}{2}\delta_{\{a\}} + \frac{1}{2}\delta_{\{c\}}) = \{\frac{1}{2}\delta_a + \frac{1}{2}\delta_c\}$. Contradiction. □

A very similar argument can be applied to prove the dual

Proposition 1.2. *There is no distributive law of P over V.*

Similar statements are true for the corresponding monads in the category of continuous domains and continuous functions $\mathbf{CONT}$. If $\mathcal{P}$ is some powerdomain monad and $\mathcal{V}$ is the powerdomain of valuations monad, then there is no distributive law between them.

Let us look at the reason for this phenomenon. The monads above arise as free algebras for suitable equational theories. In such cases a categorical distributive law amounts to an equational distributive law between the operators of the theories. In our case we would like to distribute the probabilistic choice over the nondeterministic one. Assume that $+_p$ is a probabilistic choice operator: $A +_p B$ is choosing A with probability p and B with probability $(1 - p)$. This operator satisfies $A +_p A = A$. Now if A, B, C are sets, we would like that:

$$A +_p (B \cup C) = (A +_p B) \cup (A +_p C) .$$

But if this law has to be true, then

$$\{x, y\} = \{x, y\} +_p \{x, y\} = \{x, y, x +_p y, y +_p x\}$$

which is a contradiction.

Morally the proof of proposition 1.1 relies on the law $A +_p A = A$. Dually the proof of proposition 1.2 relies on the law $A \cup A = A$. It would be interesting to investigate more in details the relations between categorical and equational distributive laws, although it might already have been done, and I am simply not aware of it.

The equation $\{x, y\} = \{x, y, x +_p y, y +_p x\}$ suggests a possible solution to this difficulty. Tix [Tix99] and Mislove [Mis00], independently, define the notion of geometrically convex powerdomain $\mathcal{P}_{TM}$, which cannot be applied to arbitrary continuous domains, but to continuous d-cones only. Morally, $\mathcal{P}_{TM}(X)$ is the set of all *convex* subsets of X. The binary operator $\cup$ is interpreted as union followed by convex closure. The composition $\mathcal{P}_{TM} \circ \mathcal{V}$ is proved to have the universal property that makes it a monad.

Our solution amounts to defining the notion of *indexed valuation* functor $\mathcal{IV}$. Indexed valuations are similar to usual valuations but they do not satisfy $A +_p A = A$. It is possible to define a distributive law between the usual $\mathcal{P}$ and $\mathcal{IV}$. We perform this construction both in the category of sets and in the category of continuous domains.

As in the case of $\mathcal{P}$ and $\mathcal{V}$, the functor $\mathcal{IV}$ is freely generated by an (in)equational theory.

Besides their categorical justification, indexed valuations have a computational meaning, which we present by giving semantics to an imperative language containing both random assignment and nondeterministic choice. The operational semantics is given in terms of alternating transition systems. Such systems come equipped with a notion of scheduler for resolving the nondeterminism. In the literature there are two notions of scheduler: deterministic and probabilistic. Using indexed valuations, we give a denotational semantics which is adequate with respect to deterministic schedulers. A semantics in terms of the Tix-Mislove construction, instead, is adequate with respect to probabilistic schedulers.

2 Indexed valuations in the category of sets

We perform our construction in the category of sets and functions. We define the indexed valuation functor and the distributive law. The notions introduced in this section will also be necessary when we work in the category of continuous domains.

2.1 Definition

We need some preliminary definitions.

Definition 2.1. A *discrete valuation* (DV) on a set X is a function

$$\nu : X \to \overline{\mathbb{R}^+} := [0, +\infty] \; .$$

Given a discrete valuation ν on X, we define its *norm* $|\nu|$ as

$$|\nu| := \sum_{x \in X} \nu(x) := \; sup_{F \subseteq_{fin} X} \sum_{x \in F} \nu(x) \; .$$

For $Y \subseteq X$ we also put

$$\nu(Y) := \sum_{y \in Y} \nu(y) \; .$$

The support $Supp(\nu)$ of a DV ν is defined as

$$Supp(\nu) := \nu^{-1}(]0, +\infty]) = \{x \in X \mid \nu(x) > 0\} \; .$$

As far as I know this notion, although straightforward, does not have a standard name in the literature. The name "discrete valuations" comes from the fact that they are valuations on the discrete topology (see section 4.1). In [JLY01] discrete valuations taking values in $[0, +\infty[$ are called *weightings*.

We denote the set of discrete valuations on X by $V(X)$.

Definition 2.2. A discrete valuation ν is a *discrete partial probability distribution* if $|\nu| \leq 1$. A discrete valuation ν is a *finite valuation* if $Supp(\nu)$ is finite.

Partial probability distributions are sufficient for semantics of probabilistic processes. Nevertheless, we choose to deal with the more general notion of valuation, because the corresponding equational theory is nicer while the other fundamental properties are the same [Kir93].

We now introduce the main new concept.

Definition 2.3. Let X be a set. An *indexed discrete valuation* (IDV) on X is a pair $(Ind, Prob)$ where $Ind : I \to X$ is a function and $Prob$ is a discrete valuation on I, for some set I.

Notice that we do not require that Ind be injective. This is indeed the main point of this construction: we want to divide the probability of an element among its indexes. One possible interpretation is that indexes in I represent computations, while elements of X represent observations.

We shall also write x_i for $Ind(i)$ and p_i for $Prob(i)$. An indexed discrete valuation $\xi := (Ind, Prob)$ will also be denoted as $(x_i, p_i)_{i \in I}$.

We are now going to define an equivalence relation on the class of IDV's. It is the transitive closure of two simpler equivalence relations.

Definition 2.4. We set

$$(x_i, p_i)_{i \in I} \sim_1 (y_j, q_j)_{j \in J}$$

if and only if there exists a bijection $h : I \to J$ such that

$$\forall i \in I.\ y_{h(i)} = x_i \ ,$$

$$\forall i \in I.\ q_{h(i)} = p_i \ .$$

This says that two IDV's are equivalent up to renaming of the indexes. If we interpret indexes as computations, we may say that we do not care about the identity of a single computation. We only care of how many different computations there are, and how they relate to observations.

Given an IDV $(x_i, p_i)_{i \in I}$, let $I_0 := \{i \in I \mid p_i = 0\}$.

Definition 2.5. We set

$$(x_i, p_i)_{i\in I} \sim_2 (y_j, q_j)_{j\in J}$$

if and only if

$$I \setminus I_0 = J \setminus J_0 \ ,$$
$$\forall i \in I \setminus I_0.\ x_i = y_i \ \&\ p_i = q_i \ .$$

This says that only indexes in the support matter. Intuitively, computations with probability 0 do not happen, so we may as well ignore them.

Definition 2.6. The equivalence relation $\sim$ is the transitive closure of $\sim_1 \circ \sim_2$.

¿From now on we will use the term "indexed discrete valuations" to denote equivalence classes under $\sim$.

Given a set X and an infinite cardinal number α we define the set $IV_\alpha(X)$ as follows:

$$IV_\alpha(X) := \{[(x_i, p_i)_{i\in I}]_\sim \mid Card(I) < \alpha\} \ .$$

In particular $IV_{\aleph_0}(X)$ is the set of indexed discrete valuations whose indexing set is finite. Its elements are called indexed finite valuations. For simplicity, we shall write IV for $IV_{\aleph_0}$.

The construction above can be extended to a functor $IV : \mathbf{SET} \to \mathbf{SET}$ as follows. If $f : X \to Y$ then

$$IV(f)([(x_i, p_i)_{i\in I}]_\sim) := [(f(x_i), p_i)_{i\in I}]_\sim \ .$$

It is easy to check that this construction is well defined (i.e. does not depend on the representative). The functor IV extends to a monad, with the following unit and multiplication (we drop the mention of equivalence classes to simplify the reading):

$$\eta^{IV}_X : X \to IV(X) \ ,$$
$$\eta^{IV}_X(x) := (x, 1)_{*\in\{*\}} \ ;$$
$$\mu^{IV}_X : IV(IV(X)) \to IV(X) \ ,$$
$$\mu^{IV}_X \ (((x_{i_\lambda}, p_{i_\lambda})_{i_\lambda\in I_\lambda}, \pi_\lambda)_{\lambda\in\Lambda}) := (x_j, q_j)_{j\in J}$$

where

$$J = \biguplus_{\lambda\in\Lambda} I_\lambda \ , \ \ q_j = p_j\pi_\lambda \text{ if } j \in I_\lambda \ .$$

To simplify the definition of μ, recall that an IDV is in fact an equivalence class. We can therefore assume that $I_\lambda = I$ for every $\lambda \in \Lambda$ because we can always reindex and add indexes with probability 0. Therefore

$$((x_{i_\lambda}, p_{i_\lambda})_{i_\lambda \in I_\lambda}, \pi_\lambda)_{\lambda\in\Lambda} \sim ((x_i^\lambda, p_i^\lambda)_{i\in I}, \pi_\lambda)_{\lambda\in\Lambda} \ .$$

And

$$\mu_X^{IV}\left(((x_i^\lambda, p_i^\lambda)_{i\in I}, \pi_\lambda)_{\lambda\in\Lambda}\right) := (x_i^\lambda, \pi_\lambda p_i^\lambda)_{(i,\lambda)\in I\times\Lambda} \ .$$

Proposition 2.7. *The triple $(IV, \eta^{IV}, \mu^{IV})$ defined above is a monad.*

Proof: It is easy to check that η, μ are well defined and are natural transformations. Let us now check the defining diagrams:

1.

$$\begin{array}{ccc} IV(X) & & \\ {\scriptstyle IV(\eta_X)}\downarrow & \searrow & \\ IV^2(X) & \xrightarrow[\mu_X]{} & IV(X) \end{array}$$

$$IV(\eta_X)\big((x_i, p_i)_{i\in I}\big) = ((x_i, 1)_{*\in\{*\}}, p_i)_{i\in I};$$
$$\mu_X\big(((x_i, 1)_{*\in\{*\}}, p_i)_{i\in I}\big) = (x_i, 1p_i)_{(i,*)\in I\times\{*\}} \sim (x_i, p_i)_{i\in I} \ .$$

2.

$$\begin{array}{ccc} & & IV(X) \\ & \swarrow & \downarrow{\scriptstyle \eta_{IV(X)}} \\ IV(X) & \xleftarrow[\mu_X]{} & IV^2(X) \end{array}$$

$$\eta_{IV(X)}\big((x_i, p_i)_{i\in I}\big) = ((x_i, p_i)_{i\in I}, 1)_{*\in\{*\}};$$
$$\mu_X\big(((x_i, p_i)_{i\in I}, 1)_{*\in\{*\}}\big) = (x_i, 1p_i)_{(*,i)\in\{*\}\times I} \sim (x_i, p_i)_{i\in I} \ .$$

3.

$$\begin{array}{ccc} IV^3(X) & \xrightarrow{\mu_{IV(X)}} & IV^2(X) \\ {\scriptstyle IV(\mu_X)}\downarrow & & \downarrow{\scriptstyle \mu_X} \\ IV^2(X) & \xrightarrow[\mu_X]{} & IV(X) \end{array}$$

$$
\begin{aligned}
&\mu_X \circ IV(\mu_X) \left((((x_i^{j,l}, p_i^{j,l})_{i\in I}, r_j^l)_{j\in J}, q_l)_{l\in L} \right) = \\
&= \quad \mu_X \left(((x_i^{j,l}, p_i^{j,l} r_j^l)_{(i,j)\in I\times J}, q_l)_{l\in L} \right) \\
&= \quad (x_i^{j,l}, p_i^{j,l} r_j^l q_l)_{(i,j,l)\in I\times J\times L} \\
&= \quad \mu_X \left(((x_i^{j,l}, p_i^{j,l})_{i\in I}, r_j^l q_l)_{(j,l)\in J\times L} \right) \\
&= \quad \mu_X \circ \mu_{IV(X)} \left((((x_i^{j,l}, p_i^{j,l})_{i\in I}, r_j^l)_{j\in J}, q_l)_{l\in L} \right) \ .
\end{aligned}
$$

Notice that we make essential use of the fact that indexed valuations are defined as equivalence classes.

Recall that the monad on the nonempty finite powerset functor P is defined as follows:

$$
\begin{aligned}
\eta_X^P &: X \to P(X) \ , \\
\eta^P(x) &= \{x\} \ ; \\
\mu_X^P &: P(P(X)) \to P(X) \ , \\
\mu_X^P(\mathcal{S}) &= \bigcup \mathcal{S} \ .
\end{aligned}
$$

We define a distributive law of indexed valuations over powerset.

Theorem 2.8. *Let $IV : \mathbf{SET} \to \mathbf{SET}$ be as above, and $P : \mathbf{SET} \to \mathbf{SET}$ be the covariant nonempty finite powerset monad. Then*

$$
d : IV \circ P \to P \circ IV \ ,
$$

$$
d_X(S_i, p_i)_{i\in I} := \{(h(i), p_i)_{i\in I} \mid h : I \to X,\ h(i) \in S_i\}
$$

is a distributive law.

Proof: We first notice (omitting the easy proof) that d is well defined. Then we have to show that d is a natural transformation.

$$
\begin{array}{ccc}
X & IV(P(X)) & \xrightarrow{d_X} P(IV(X)) \\
{\scriptstyle f}\downarrow & {\scriptstyle IV(P(f))}\downarrow & \downarrow{\scriptstyle P(IV(f))} \\
Y & IV(P(Y)) & \xrightarrow{d_Y} P(IV(Y))
\end{array}
$$

Take a function $f : X \to Y$. Take $\Xi \in IV(P(X))$, $\Xi = (S_i, p_i)_{i\in I}$. We have $IV(P(f))(\Xi) = (f(S_i), p_i)_{i\in I}$. Then

$$d_Y(f(S_i), p_i)_{i\in I} = \big\{(h'(i), p_i)_{i\in I} \mid h' : I \to Y,\ h'(i) \in f(S_i)\big\} =: A\ .$$

On the other hand consider

$$P(IV(f))\Big(\big\{(h(i), p_i)_{i\in I} \mid h : I \to X,\ h(i) \in S_i\big\}\Big)\ .$$

This is equal to

$$\big\{(f(h(i)), p_i)_{i\in I} \mid h : I \to X,\ h(i) \in S_i\big\} =: B\ .$$

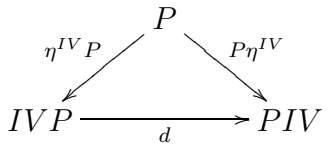
We have to show that $A = B$. Clearly $B \subseteq A$, just let $h' = f \circ h$. Take now an element $(h'(i), p_i)_{i\in I}$ of A. This means that $h'(i) = f(x_i)$ for some $x_i \in S_i$. For every S_i, we select one such x_i and then we define $h(i) = x_i$. Thus we have

$$(f(h(i)), p_i)_{i\in I} = (h'(i), p_i)_{i\in I}$$

so that $(h'(i), p_i)_{i\in I}$ belongs to B.

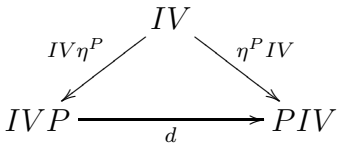
Now we have to check the four diagrams characterizing the distributive law:

1.



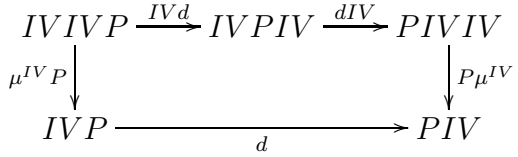
$$\begin{aligned} d_X\left((S,1)_{*\in\{*\}I}\right) &= \big\{(h(*),1)_{*\in\{*\}} \mid h : \{*\} \to X,\ h(*) \in S\big\} \\ &= \big\{(x,1)_{*\in\{*\}} \mid x \in S\big\}\ . \end{aligned}$$

2.



$$\begin{aligned} d_X\big((\{x_i\}, p_i)_{i\in I}\big) &= \big\{(h(i), p_i)_{i\in I} \mid h : I \to X,\ h(i) \in \{x_i\}\big\} \\ &= \big\{(x_i, p_i)_{i\in I}\big\}\ . \end{aligned}$$

3.



Let $\mathcal{X} := (\Xi_\lambda, \pi_\lambda)_{\lambda\in\Lambda} \in IV(IV(P(X)))$, where $\Xi_\lambda := (S_{i_\lambda}, p_{i_\lambda})_{i_\lambda\in I_\lambda}$. As before we can assume that $I_\lambda = I$ for every $\lambda \in \Lambda$. Therefore $\Xi_\lambda = (S_i^\lambda, p_i^\lambda)_{i\in I}$. We have that

$$\mu^{IV}_{P(X)}(\mathcal{X}) = (S_i^\lambda, p_i^\lambda\pi_\lambda)_{(i,\lambda)\in I\times\Lambda} .$$

If we apply d_X to this term we get

$$\left\{(h(i,\lambda), p_i^\lambda\pi_\lambda)_{(i,\lambda)\in I\times\Lambda} \mid h : I\times\Lambda \to X,\ h(i,\lambda)\in S_i^\lambda\right\} := A .$$

Consider now $IV(d_X)(\mathcal{X})$. It is

$$(d_X(\Xi_\lambda), \pi_\lambda)_{\lambda\in\Lambda}$$

where

$$d_X(\Xi_\lambda) = \left\{(h^\lambda(i), p_i^\lambda)_{i\in I} \mid h^\lambda : I \to X,\ h^\lambda(i)\in S_i^\lambda\right\} .$$

Now apply $d_{IV(X)}$. We get

$$\left\{(H(\lambda), \pi_\lambda)_{\lambda\in\Lambda} \mid H : \Lambda \to IV(X),\ H(\lambda)\in d_X(\Xi_\lambda)\right\} := B .$$

The function H is choosing an element in $d_X(\Xi_\lambda)$. We can think of H as choosing a function $h^\lambda : I \to X, h^\lambda(i) \in S_i^\lambda$. Therefore we can equivalently define B as follows:

$$B = \left\{((H(\lambda)(i), p_i^\lambda)_{i\in I}, \pi_\lambda)_{\lambda\in\Lambda} \mid H : \Lambda \to (I \to X),\ H(\lambda)(i)\in S_i^\lambda\right\} .$$

Now we have to show that the flattening (through μ^{IV}) of every valuation in B gives a valuation in A, and that every valuation in A can be obtained flattening a valuation in B. We have

$$\mu^{IV}_X\left(((H(\lambda)(i), p_i^\lambda)_{i\in I}, \pi_\lambda)_{\lambda\in\Lambda}\right) \quad = \quad (H(\lambda)(i), p_i^\lambda\pi_\lambda)_{i\in I} .$$

Now it is enough to observe that "uncurrying" H we get an $h : I\times\Lambda \to X$, satisfying $h(i,\lambda) \in S_i^\lambda$. So $P(\mu^{IV}_X)(B) \subseteq A$. The other inclusion is obtained by "currying" h to get H.

4.

$$\begin{array}{ccccc} IVPP & \xrightarrow{dP} & PIVP & \xrightarrow{Pd} & PPIV \\ {\scriptstyle IV\mu^P}\downarrow & & & & \downarrow{\scriptstyle \mu^P IV} \\ IVP & & \xrightarrow[d]{} & & PIV \end{array}$$

Remember that $\mu^P_X(\mathcal{S}) = \bigcup \mathcal{S}$. Let $\mathcal{X} := (\mathcal{S}_i, p_i)_{i\in I} \in IV(P(P(X)))$. We have that

$$IV(\mu^P_X)(\mathcal{X}) = (\bigcup \mathcal{S}_i, p_i)_{i\in I}\ .$$

If we apply d_X to this term we get

$$\left\{(h(i), p_i)_{i\in I} \mid h : I \to X,\ h(i) \in \bigcup \mathcal{S}_i\right\} := A\ .$$

Consider now $d_{P(X)}(\mathcal{X})$. It is

$$\left\{(h'(i), p_i)_{i\in I} \mid h' : I \to P(X),\ h'(i) \in \mathcal{S}_i\right\} := D\ .$$

The function h' is choosing an set in $\mathcal{S}_i$ for every i. Now two steps in one. First step: we apply $P(d_X)$ to D and we obtain a set C of sets of valuations. Second step: we flatten C to a set B of valuations defined as:

$$\left\{(h''(i), p_i)_{i\in I} \mid h'' : I \to X,\ h''(i) \in h'(i),\ h' : I \to P(X),\ h'(i) \in \mathcal{S}_i\right\}\ .$$

We claim that $A = B$. Clearly $B \subseteq A$ because $h''(i) \in \bigcup \mathcal{S}_i$. But also $A \subseteq B$. We build h' as follows: for every i we choose $S_i \in \mathcal{S}_i$ such that $h(i) \in S_i$. Then $h'' = h$ does the job.

□

It then follows that the functor $P \circ IV$ is endowed with a monad structure.

2.2 Equational characterization

We now define two operations on indexed discrete valuations, which will allow us to characterize IV as a free algebra.

Definition 2.9. Let $\nu := (Ind, Prob) = (x_i, p_i)_{i\in I}$ and $\xi := (Ind', Prob') = (y_j, q_j)_{j\in J}$ be IDV's on X. Assume that $I \cap J = \emptyset$ (this is not restrictive, because we can always reindex).

We define $\nu \oplus \xi$ to be $(Ind \cup Ind', Prob \cup Prob')$. For $p \in \overline{\mathbb{R}^+}$ we define $p\nu$ to be $(x_i, pp_i)_{i\in I}$. With $\underline{0}$ we denote the IDV whose indexing set is empty.

Note, in particular, that $p\nu \oplus (1-p)\nu \not\sim \nu$.
Consider the following equational theory:

1. $A \oplus B = B \oplus A$;
2. $A \oplus (B \oplus C) = (A \oplus B) \oplus C$;
3. $A \oplus \underline{0} = A$;
4. $0A = \underline{0}$;
5. $1A = A$;
6. $p(A \oplus B) = pA \oplus pB \;\; p \in \overline{\mathbb{R}^+}$;
7. $p(qA) = (pq)A \;\; p, q \in \overline{\mathbb{R}^+}$.

These axioms are almost the ones defining a *real cone* [Tix99]. The only difference is that we drop the axiom $(p+q)A = (pA \oplus qA)$.

Definition 2.10. A *real quasi-cone*[2] is a model for the equational theory (1)–(7).

Proposition 2.11. *The indexed finite valuations are the free real quasi-cone.*

Proof: For any set X, it is clear that $IV(X)$ with the operations defined above is a quasi-cone. Let Q be a quasi-cone and let $f : X \to Q$ a function. We have to show that there is a unique quasi-cone homomorphism $\overline{f} : IV(X) \to Q$ such that $\overline{f}(x, 1) = f(x)$. The homomorphism condition forces us to define

$$\overline{f}(x_i, p_i)_{i \in I} = \bigoplus_{i \in I} p_i f(x_i) \; .$$

Associativity, commutativity, and the two $\underline{0}$-laws guarantee that the definition does not depend on the representative for $(x_i, p_i)_{i \in I}$. The unit law guarantees that $\overline{f}(x, 1) = f(x)$. The homomorphism condition for the sum (and $\underline{0}$) is obvious, while for the scalar product we have to use the laws (6) and (7). □

Recall that a semilattice is a model of the following theory.

8. $A \uplus B = B \uplus A$;
9. $A \uplus (B \uplus C) = (A \uplus B) \uplus C$;

[2]This name is provisional: suggestions will be appreciated

10. $A \uplus A = A$.

It is well known that the finite nonempty powerset is the free semilattice.

The universality of these constructions gives rise to adjunctions, which in turn give rise to monads. It is rather straightforward to check that they are the ones defined in section 2.1.

Consider now the combined equational theory (1)–(10) augmented with the following axioms.

11. $p(A \uplus B) = pA \uplus pB$;

12. $A \oplus (B \uplus C) = (A \oplus B) \uplus (A \oplus C)$.

Notice that (11)–(12) express equationally that the probabilistic operators distribute over the nondeterministic one.

Theorem 2.12. *The monad on $P \circ IV$ obtained via the categorical distributive law defined above is the free algebra for the equational theory (1)–(12).*

Proof: First we show that $P \circ IV$ is left adjoint to the forgetful functor. Let's start by observing that $P(IV(X))$ is indeed a model of (1)–(12), where $\uplus$ is interpreted as union, addition and scalar multiplications are the standard extensions to subsets of the corresponding operations in $IV(X)$, and $\underline{0}$ is the singleton of the empty indexed valuation. Now let Q be a model of (1)–(12), and let $f : X \to Q$ be a function. We have to show that there is a unique function $\overline{f} : P(IV(X)) \to Q$ which respects the operations and such that $\overline{f}\{(x, 1)\} = f(x)$. The homomorphism condition forces us to define

$$\overline{f}\{(x_i, p_i)_{i \in I}\} = \bigoplus_{i \in I} p_i f(x_i) \; ;$$

$$\overline{f}(A) = \bigcup_{\nu \in A} \overline{f}(\{\nu\}) \; .$$

Laws (1)–(4) again guarantee that the definition in the first line does not depend on the representative for $(x_i, p_i)_{i \in I}$. Laws (8),(9) guarantee that the second line is well defined. The law (5) guarantees that $\overline{f}\{(x, 1)\} = f(x)$. The function respects the sum (and $\underline{0}$) because of law (12). It respects the product because of laws (6),(7),(11). It respects the union because of law (10).

Notice that the unit of the adjunction is just $\eta_P \eta_{IV}$.

We have to show that this monad generated by this adjunction is the same as the monad generated by the distributive law. The functor and the unit are the same. Instead of showing that the multiplication is the same, we equivalently show that the Kleisli extension operators are the same.

Let $f : X \to P(IV(Y))$ be a function. Consider a finite set of discrete valuations $A \in P(IV(X))$. Since A is finite it is not restrictive to assume that all its elements are indexed by the same set I. So we can write

$$A = \left\{ (x_i^\rho, p_i^\rho)_{i \in I} \,|\, \rho \in R \right\} ,$$

with the convention that for two different ρ, ρ' the corresponding valuations are different. Analogously, we write

$$f(x_i^\rho) = \left\{ (y_j^{\sigma^{i,\rho}}, q_j^{\sigma^{i,\rho}})_{j \in J} \,|\, \sigma^{i,\rho} \in S^{i,\rho} \right\} ,$$

with a similar convention as above for any fixed (i, ρ), and also assuming that the $S^{i,\rho}$ are all disjoint. Again it is not restrictive to assume that all the valuations are indexed by the same set J.

We want to evaluate $\overline{f}(A)$, the Kleisli extension of the monad generated by the universal property:

$$\overline{f}\Big(\left\{ (x_i^\rho, p_i^\rho)_{i \in I} \,|\, \rho \in R \right\} \Big) = \bigcup_{\rho \in R} \bigoplus_{i \in I} p_i^\rho f(x_i^\rho) .$$

Now it can be proved by induction on the size of I that

$$\begin{aligned} &\bigoplus_{i \in I} p_i^\rho \left\{ (y_j^{\sigma^{i,\rho}}, q_j^{\sigma^{i,\rho}})_{j \in J} \,|\, \sigma^{i,\rho} \in S^{i,\rho} \right\} \\ &= \left\{ (y_j^{k^\rho(i)}, p_i^\rho q_j^{k^\rho(i)})_{(j,i) \in J \times I} \,|\, k^\rho : I \to \bigcup_{i \in I} S^{i,\rho},\ k^\rho(i) \in S^{i,\rho} \right\} . \end{aligned}$$

Therefore:

$$\begin{aligned} &\overline{f}\Big(\left\{ (x_i^\rho, p_i^\rho)_{i \in I} \,|\, \rho \in R \right\} \Big) \\ &= \left\{ (y_j^{k^\rho(i)}, p_i^\rho q_j^{k^\rho(i)})_{(j,i) \in J \times I} \,|\, k^\rho : I \to \bigcup_{i \in I} S^{i,\rho},\ k^\rho(i) \in S^{i,\rho}, \rho \in R \right\} . \end{aligned}$$

Let's now look at $f^\dagger(A)$, the Kleisli extension of the monad obtained via the distributive law.

$$f^\dagger\Big(\left\{ (x_i^\rho, p_i^\rho)_{i \in I} \,|\, \rho \in R \right\} \Big)$$

$$= \mu^P \mu^{IV} \circ PdIV\Big(\big\{(f(x_i^\rho), p_i^\rho)_{i\in I} \,|\, \rho \in R\big\}\Big)$$

$$= \mu^P \mu^{IV}\Big(\Big\{\big\{(h^\rho(i), p_i^\rho)_{i\in I} \,|\, h^\rho : I \to IV(Y), h^\rho(i) \in f(x_i^\rho)\big\} | \rho \in R\Big\}\Big)$$

By the conventions we have assumed, choosing an element in $f(x_i^\rho)$ is the same as choosing a $\sigma^{i,\rho} \in S^{i,\rho}$, therefore it is equivalent to think of h^ρ as a function $h^\rho : I \to \bigcup_{i\in I} S^{i,\rho},\ h^\rho(i) \in S^{i,\rho}$. Then we can continue the chain of equalities

$$= \mu^P \mu^{IV}\Big(\Big\{\big\{((y_j^{h^\rho(i)}, q_j^{h^\rho(i)})_{j\in J}, p_i^\rho)_{i\in I} \,|\, h^\rho : I \to \bigcup_{i\in I} S^{i,\rho},\ k^\rho(i) \in S^{i,\rho}\big\} | \rho \in R\Big\}\Big)$$

$$= \mu^P\Big(\Big\{\big\{(y_j^{h^\rho(i)}, p_i^\rho q_j^{h^\rho(i)})_{(j,i)\in J\times I} \,|\, h^\rho : I \to \bigcup_{i\in I} S^{i,\rho},\ h^\rho(i) \in S^{i,\rho}\big\} \,|\, \rho \in R\Big\}\Big)$$

$$= \Big\{(y_j^{h^\rho(i)}, p_i^\rho q_j^{h^\rho(i)})_{(j,i)\in J\times I} \,|\, h^\rho : I \to \bigcup_{i\in I} S^{i,\rho},\ h^\rho(i) \in S^{i,\rho}, \rho \in R\Big\}\,.$$

□

If we see finite indexed valuations and finite sets as (equivalence classes of) terms we can give a syntactic interpretation of the categorical distributive law: it takes a term where there are no probabilistic operators inside a nondeterministic one and transforms it into a term where all the nondeterministic operators have been pushed outside. In other words we interpret the equations (11)–(12) as rewriting rules, from left to right.

3 The construction of Tix and Mislove in the category of sets

Another possibility for combining nondeterminism and probability is the one suggested in [Tix99, Mis00]. Those works are only concerned with DCPO's. In this section we perform a similar construction in the category $\mathbf{SET}$.

Definition 3.1. A *real cone*[3]

13. $(p+q)A = pA \oplus qA\ p, q \in \overline{\mathbb{R}^+}$.

We call $\mathbf{RCONE}$ the category of real cones and homomorphisms.

[3]Our definition is the one used in [Kir93]. The definition in [Tix99] is slightly different.

If X is a set, the set of finite valuations over X (denote by $V(X)$) can be endowed with a real cone structure, the operations being defined pointwise. It is easy to verify that

Proposition 3.2. *The finite valuations are the free real cone.*

Definition 3.3. A subset X of a real cone is *convex* if for every $x, y \in X, p \in [0,1]$, we have $px \oplus (1-p)y \in X$. Given a set X, its *convex closure* $\overline{X}$ is the smallest convex set containing X. A convex set X is *finitely generated* if there exists a finite set X_0 such that $X = \overline{X_0}$. Given a finite set I, elements $x_i, i \in I$ of a real cone and nonnegative real numbers $p_i, i \in I$ such that $\sum_{i\in I} p_i = 1$, the element $\bigoplus_{i\in I} p_i x_i$ is said to be a *convex combination* of the x_i.

The following result is standard.

Proposition 3.4. *For a set X, we have that $\overline{X}$ is the set of convex combinations of elements of X.*

Definition 3.5. For a real cone Z we define

$$P_{TM}(Z) = \{Y \subseteq Z \mid Y \text{ convex, finitely generated}\} .$$

We define

- $pY = \{py \mid y \in Y\}$;
- $Y \oplus Y' = \{y \oplus y' \mid y \in Y, y' \in Y'\}$;
- $\underline{0} = \{\lambda x.0\}$;
- $Y \uplus Y' = \overline{Y \cup Y'} = \{py \oplus (1-p)y' \mid p \in [0,1],\ y \in Y, y' \in Y'\}$.

Definition 3.6. A *real cone-semilattice* is a model for the theory (1)–(13). The corresponding category is called $\mathbf{RCS}$.

Proposition 3.7. *The operator P_{TM} with the operations as above defines a functor $\mathbf{RCONE} \to \mathbf{RCS}$ which is left adjoint of the forgetful functor.*

Proof: First we have to show that the operations are well defined and that satisfy the axioms. If Y, Y' are convex, it is easy to show that $pY, Y \oplus Y', Y \uplus Y$ are convex. If Y_0, Y_0' are finite generators for Y, Y' then pY_0 is a finite generator for pY, $Y_0 \oplus Y_0'$ is a finite generator for $Y \oplus Y'$ and $Y_0 \cup Y_0'$ is a finite generator for

$Y \uplus Y'$. As for the axioms the only nontrivial ones are (12)-(13): here is where convexity is needed.

Then we have to show the universal property characterizing freeness. For every real cone Z and real cone-semilattice H and real cone homomorphism $f : X \to H$, there exists a unique **RCS**-morphism $\overline{f} : P_{TM}(Z) \to H$ such that $\overline{f}(\{z\}) = f(z)$. Now for every $Y \in P_{TM}(Z)$ let Y_0 be one of its finite generators, then

$$\overline{f}(Y) = \bigUplus_{y \in Y_0} f^\sharp(y) \; .$$

The homomorphism condition implies uniqueness. We have to show that this function is well defined and that it is indeed an homomorphism. First we need to show that the definition does not depend on the chosen finite generator.

Lemma 3.8. *Let H be a real cone-semilattice, let Y_0, Z_0 be finite subsets of H. If $\overline{Y_0} = \overline{Z_0}$, then $\bigUplus Y_0 = \bigUplus Z_0$*

Proof: We prove this for the simple case where $Y_0 = \{y, y'\}, Z_0 = \{z, z'\}$. The general case can be proved in a similar way. We want to prove that $y \uplus y' = z \uplus z'$. We will prove that $y \uplus y' = y \uplus y' \uplus z \uplus z'$ (which, by symmetry, implies our result). Note that, from the assumption, z, z' must be convex combinations of y, y'. The statement is thus a consequence of the following proposition.

Proposition 3.9. *In a real cone-semilattice, if w is a convex combination of y, y' then*

$$y \uplus y' = y \uplus y' \uplus w \; .$$

Proof: Let $w = py \oplus (1-p)y'$. Then

$$y \uplus y' = p(y \uplus y') \oplus (1-p)(y \uplus y')$$

$$= y \uplus y' \uplus (py \oplus (1-p)y') \uplus (py' \oplus (1-p)y) \; .$$

The statement of the proposition follows from

Lemma 3.10. *In a semilattice, if $x = x \uplus x' \uplus x''$, then $x = x \uplus x'$.*

Proof:

$$x \uplus x' = x \uplus x' \uplus x'' \uplus x' = x \uplus x' \uplus x'' = x$$

□

The combination of the two adjunctions

$$\mathbf{SET} \underset{\longleftarrow}{\overset{\longrightarrow}{\perp}} \mathbf{RCONE} \underset{\longleftarrow}{\overset{\longrightarrow}{\perp}} \mathbf{RCS}$$

gives rise to a monad in $\mathbf{SET}$. Let's look concretely at its Kleisli extension.

Take $f : X \to P_{TM}(V(Y))$, say $f(x) = B_x$. We have that the Kleisli extension $f^\dagger : P_{TM}(V(X)) \to P_{TM}(V(Y))$ is defined as

$$f^\dagger(A) = \biguplus_{\xi \in A_0} \sum_{x \in X} \xi(x) B_x \ .$$

We will need the following

Proposition 3.11.

$$f^\dagger(A) = \bigcup_{\xi \in A} \sum_{x \in X} \xi(x) B_x = \{ \sum_{x \in X} \xi(x) h(x) \,|\, h : X \to V(Y), h(x) \in B_x,\ \xi \in A \} \ .$$

Proof: Let's call

- $V = \bigcup_{\xi \in A_0} \sum_{x \in X} \xi(x) B_x$;
- $U = \biguplus_{\xi \in A_0} \sum_{x \in X} \xi(x) B_x$;
- $W = \bigcup_{\xi \in A} \sum_{x \in X} \xi(x) B_x$.

Remember that $U = \overline{V}$.

Clearly $V \subseteq W$. Moreover W is convex:

$$\begin{aligned} & p \sum_{x \in X} \xi(x) h(x) + (1-p) \sum_{x \in X} \xi'(x) h'(x) \\ & = \sum_{x \in X} p\xi(x) h(x) + (1-p) \xi'(x) h'(x) \ . \end{aligned}$$

Define $\xi'' = p\xi + (1-p)\xi' \in A$, and $h''(x) = \frac{p\xi(x)}{\xi''(x)} h(x) + \frac{(1-p)\xi'(x)}{\xi''(x)} h'(x)$. Since B_x is convex , then $h''(x) \in B_x$. (If $\xi''(x) = 0$ then $h''(x)$ can be set equal to any element of B_x.) We have

$$\xi''(x) h''(x) = p\xi(x) h(x) + (1-p) \xi'(x) h'(x) \ .$$

Therefore $U \subseteq W$.

For the other direction take $\sum_{x \in X} \xi(x) h(x)$. We know that $\xi = \sum_i p_i \xi_i$ with $\xi_i \in A_0$. So

$$\sum_{x \in X} \xi(x) h(x) = \sum_{x \in X} \sum_i p_i \xi_i(x) h(x) = \sum_i p_i \sum_{x \in X} \xi_i(x) h(x)$$

which is a convex combination of elements of V. □

4 Indexed valuations in the category of continuous domains

4.1 Definition

To give semantics to languages with recursion we work in a category of domains. We shall recall briefly the domain theoretic notions we need. For a more detailed treatment, the suggested reference is [AJ94].

In every DCPO an *approximation* relation $\ll$ is definable (also known as *way-below* relation). We say that $x \ll y$ if $y \sqsubseteq \bigsqcup^{\uparrow} Z \Longrightarrow \exists z \in Z. x \sqsubseteq z$. A subset B of a DCPO D is a *basis* if every $x \in D$ is the directed lub of the elements of B that are way-below x. A DCPO with a basis is called a *continuous domain*.

An example of a continuous domain is $(\overline{\mathbb{R}^+}, \leq)$. Its way-below relation is

$$p \ll q \text{ iff } (p < q \text{ or } p = 0) .$$

A basis of $\overline{\mathbb{R}^+}$ is $\mathbb{Q}^+$.

The properties of the way-below relation on B suggest the following definition.

Definition 4.1. A relation $<$ on a set X is an *AB-relation* if it is transitive and satisfies the finite interpolation property: for every $F \subseteq_{fin} X$ and for every $x \in X$, $F < x \Longrightarrow \exists y \in X.\ F < y < x$. The structure $(X, <)$ is called an *abstract basis*.

A preorder is also an abstract basis. For AB-relations we shall use the same terminology as for preorders. We therefore speak of monotonic functions, lower sets, directed sets, and so on. In particular we recall that an *ideal* is a lower directed set. The set of ideals of X is called $Idl(X)$. For any $x \in X$ the set $\iota(x) := x\downarrow := \{y \mid y < x\}$ is an ideal. The structure $(Idl(X), \subseteq)$ is a continuous domain with basis $\iota(X)$. It is called the *ideal completion* of X. Conversely if D is a continuous domain with basis B, then $(B, \ll)$ is an abstract basis whose ideal completion is isomorphic to D. Notice that directedness implies the following property, that we call *roundedness*: if $\mathcal{I}$ is and ideal of $(X, <)$, then for every $x \in \mathcal{I}$ there exists $x' \in \mathcal{I}$ such that $x < x'$.

Let $(X, <)$ be an abstract basis, $(D, \sqsubseteq)$ be a (not necessarily continuous) DCPO, and $f : X \to D$ be a function mapping $<$ to $\sqsubseteq$ ("monotonic"). The function $f^\sharp : Idl(X) \to D$ defined as

$$f^\sharp(I) = \bigsqcup_{x \in I}^{\uparrow} f(x)$$

is continuous. Notice that in general $f^\sharp(\iota(x)) \neq f(x)$. If $(X, <)$, $(Y, <)$ are two abstract bases and if $f : X \to Y$ is a monotonic function, we define the *extension* $ext(f)$ to be the continuous function $(\iota \circ f)^\sharp : Idl(X) \to Idl(Y)$.

We conclude this quick introductory part with the definition of the powerdomain of valuations.

Definition 4.2. A *continuous valuation* on a topological space (X, τ) is a function $\nu : \tau \to \overline{\mathbb{R}^+}$ satisfying:

- (Strictness)
  $\nu(\emptyset) = 0$;
- (Monotonicity)
  $U \subseteq V \Longrightarrow \nu(U) \leq \nu(V)$;
- (Modularity)
  $\nu(U) + \nu(V) = \nu(U \cup V) + \nu(U \cap V)$;
- (Continuity) whenever $\mathcal{J}$ is a directed subset of τ

$$\nu\big(\bigcup \mathcal{J}\big) = \sup_{U \in \mathcal{J}} \nu(U) \ .$$

For each $x \in X$, the function η_x such that

$$\eta_x(U) = \begin{cases} 1 & x \in U \\ 0 & x \notin U \end{cases}$$

is a continuous valuation and it is called *point* valuation. A *simple* valuation is a linear combination of point valuations (the addition and scalar multiplication being defined pointwise). A continuous valuation on a DCPO D is a continuous valuation on its Scott topology. The set $\mathcal{V}(D)$ of continuous valuations on D ordered pointwise is again a DCPO. If D is a continuous domain, $\mathcal{V}(D)$ is a continuous domain with basis the set of simple valuations.

Now we introduce the new concepts. If $(X, <)$ is an abstract basis then we can define a relation $\prec$ on $IV(X)$ in such a way that $(IV(X), \prec)$ is an abstract basis:

Definition 4.3. For $(x_i, p_i)_{i \in I}, (y_j, q_j)_{j \in J} \in IV(X)$

$$(x_i, p_i)_{i \in I} \prec (y_j, q_j)_{j \in J}$$

if and only if there exists a partial surjective function $f : J \to I$, s.t.:

$$x_{f(j)} < y_j \ ,$$

$$p_i \ll \sum_{f(j)=i} q_j \ .$$

We call such an f a *witness* for the relation.

There are three reasons for this choice. Firstly, this definition is an "indexed" version of the splitting lemma of [Jon90]. Secondly, it has an interesting computational interpretation. To explain this we need the notion of scheduler for a probabilistic-nondeterministic operational model, which we shall present in section 6.1. Finally, this definition corresponds to an inequational theory that allows us to match equational and categorical distributive laws, as we did in the category of sets.

Proposition 4.4. *$(IV(X), \prec)$ is an abstract basis.*

Proof: To show transitivity we show that if f is a witness for $(x_i, p_i)_{i\in I} \prec (y_j, q_j)_{j\in J}$ and g is a witness for $(y_j, q_j)_{j\in J} \prec (z_l, r_l)_{l\in L}$ then $f \circ g$ is a witness for $(x_i, p_i)_{i\in I} \prec (z_l, r_l)_{l\in L}$. Clearly it is surjective.

- $x_{f(g(l))} < y_{g(l)} < z_l$. And $<$ is transitive.
- $p_i \ll \sum_{f(j)=i} q_j \ll \sum_{f(j)=i} \sum_{g(l)=j} r_l = \sum_{(f(g(l))=i} r_l$.

We have now to show the finite interpolation property. It is enough to consider the cases for which $|F| = 0, 2$. We leave to the reader the case $|F| = 0$. Let $(x_i, p_i)_{i\in I}, (y_j, q_j)_{j\in J} \prec (z_l, r_l)_{l\in L}$ with witnesses f and g. For every $l \in L$ consider the set $Z_l := \{x_f(l) \mid l \in L\} \cup \{y_g(l) \mid l \in L\}$. It is finite. Since f, g are witnessing functions, we have $Z_l < z_l$. Since $(X, <)$ is an abstract basis, there exists a z'_l such that $Z_l < z'_l < z_l$

Let $s := \sum_{l\in L} r_l$. Suppose first $s < +\infty$. Let $2s\epsilon$ be the minimum among all the numbers

$$\left(\sum_{f(l)=i} r_l\right) - p_i, \quad \left(\sum_{g(l)=j} r_l\right) - q_j \ .$$

Consider $(z'_l, (1-\epsilon)r_l)_{l\in L}$. The identity function on L is a witness for $(z'_l, (1-\epsilon)r_l)_{l\in L} \prec (z_l, r_l)_{l\in L}$ while f, g are witnesses for $(x_i, p_i)_{i\in I}, (y_j, q_j)_{j\in J} \prec (z'_l, (1-$

$\epsilon) r_l)_{l \in L}$:

$$\begin{aligned}
\left(\sum_{f(l)=i} (1-\epsilon) r_l \right) - p_i &= \left(\sum_{f(l)=i} r_l \right) - \epsilon \left(\sum_{f(l)=i} r_l \right) - p_i \\
&\geq \left(\sum_{f(l)=i} r_l \right) - \epsilon \left(\sum_{l \in L} r_l \right) - p_i \\
&= \left(\sum_{f(l)=i} r_l \right) - s\epsilon - p_i \\
&\gg \left(\sum_{f(l)=i} r_l \right) - 2s\epsilon - p_i \geq 0 \, .
\end{aligned}$$

The case $s = +\infty$ is similar. □

Definition 4.5. If D is a continuous domain with basis B, let $\mathcal{IV}(D)$ be the ideal completion of $(IV(B), \prec)$. Its elements are called *indexed valuations*.

For every indexed finite valuation $\nu := (b_i, p_i)_{i \in I}$ over B, we can define a simple valuation ν^* as follows. Consider $X := \{b_i \mid i \in I\}$. Then define $\nu^* := \sum_{i \in I} p_i \eta_{b_i}$. For every open subset U of D we define $\nu(U) := \nu^*(U)$

Every indexed valuation $\nu \in \mathcal{IV}(D)$ defines a continuous valuation ν^*: if L is a directed set of indexed finite valuations, and if $\nu = \bigsqcup^{\uparrow} L$, then for every open $O \subseteq D$, we define $\nu^*(O) := \sup_{\nu' \in L} \nu'(O)$.

Moreover, all valuations can be obtained this way.

Proposition 4.6. *[Var01] Let $\mathcal{V}$ be Jones' powerdomain of valuations functor. The function $(-)^* : \mathcal{IV}(D) \to \mathcal{V}(D)$ is a continuous surjection, natural in D.*

4.2 Equational characterization

We are going to characterize indexed valuations as a free construction. Recall the equational theory (1)–(7) of section 2.2. We add only one more axiom, which corresponds to definition 4.3 of the AB-relation on indexed finite valuations.

- HV: $(p+q)A \sqsubseteq (pA \oplus qA)$

Definition 4.7. A *continuous quasi-cone* is a structure $(D, \sqsubseteq, \oplus, \odot)$ such that

- $(D, \sqsubseteq)$ is a continuous domain;
- $\oplus : D \times D \to D$ is continuous;
- $\odot : [0, +\infty] \times D \to D$ is continuous[4];
- axioms (1)–(7) + (HV) are satisfied.

Let $\mathbf{CONT}$ be the category of continuous domains, and $\mathbf{QCONT}$ be the category of continuous quasi-cones and continuous homomorphisms. (In fact, in what follows, we will always mention bases. Therefore $\mathbf{CONT}$ will be the category of abstract bases and continuous functions between their completions. This is clearly equivalent to the category as defined above. Similar considerations apply to all the other categories we will define.)

Proposition 4.8. *The operator $\mathcal{IV}$ defined in the previous section extends to a functor $\mathbf{CONT} \to \mathbf{QCONT}$ which is left adjoint to the forgetful functor.*

Proof: First we show that when D is in $\mathbf{CONT}$ then $\mathcal{IV}(D)$ is indeed in $\mathbf{QCONT}$. By construction $\mathcal{IV}(D)$ is a continuous domain. We have to define the operations. We put

- $\mathcal{I} \oplus \mathcal{J} = \{x \oplus y \,|\, x \in \mathcal{I}, y \in \mathcal{J}\}\downarrow$;
- $p\mathcal{I} = \{px \,|\, x \in \mathcal{I}\}$;
- $\underline{0} = \{(\ ,\ )_{i \in \emptyset}\}$.

Such operations are well defined and they satisfy the axioms. In particular (HV) follows from the roundedness of the ideals and the following lemma.

Lemma 4.9. *If $\nu \prec \xi$ and $p \ll q_1 + q_2$ then $p\nu \prec q_1\xi \oplus q_2\xi$.*

Proof: Let $\nu := (a_i, p_i)_{i \in I}, \xi := (b_j, r_j)_{j \in J}$. Since $\nu \prec \xi$, by definition there exists $f : J \twoheadrightarrow I$, s.t.:

$$a_{f(j)} \ll_B b_j \ ;$$

$$p_i \ll \sum_{f(j)=i} r_j \ .$$

[4]The symbol $\odot$ is used here for clarity. Everywhere else the scalar multiplication is denoted simply by juxtaposition of its arguments.

We want to prove that $p\nu \prec q_1\xi \oplus q_2\xi$, i.e. that.

$$(a_i, pp_i)_{i\in I} \prec (b_j, q_k r_j)_{(j,k)\in J\times\{1,2\}} \ .$$

We need a function $f' : J \times \{1, 2\} \twoheadrightarrow I$, s.t.:

1. $a_{f'(j,k)} \ll_B b_j$;
2. $pp_i \ll \sum_{f'(j,k)=i} q_k r_j$.

Define f' as follows: $f'(j, k) := f(j)$. First f' is clearly surjective. Secondly, the expression (1) is obviously satisfied. As for (2) notice first that $pp_i \ll (q_1 + q_2)p_i$; since $p_i \ll \sum_{f(j)=i} r_j$, then for $k = 1, 2$ $q_k p_i \ll \sum_{f(j)=i} q_k r_j$. So $(q_1 + q_2)p_i \ll \sum_{f(j)=i} q_1 r_j + \sum_{f(j)=i} q_2 r_j = \sum_{f'(j,1)=i} q_1 r_j + \sum_{f'(j,2)=i} q_2 r_j = \sum_{f'(j,k)=i} q_k r_j$. □Lemma

The operations are continuous. The scalar multiplication is also continuous in the first argument. To prove that, take an ideal $\mathcal{I} \in \mathcal{IV}(D)$. We want to prove that

$$\bigcup_{p<q} p\mathcal{I} = q\mathcal{I} \ ,$$

that is for every ν, we have $\nu \in q\mathcal{I}$ if and only if there exist $p \ll q$ s.t. $\nu \in p\mathcal{I}$. The "if" direction follows from monotonicity of the scalar multiplication, which in turn follows from the fact that $pY \prec qY \oplus 0Y = qY$. It remains the other inclusion.

Consider the case $q < \infty$ (the other being similar). Take $\nu \in q\mathcal{I}$. By roundedness there is $\nu' \in q\mathcal{I}$ s.t. $\nu \prec \nu'$. We leave to the reader to prove that there exists ϵ such that $\nu \prec (1 - \epsilon)\xi_\nu$. But $\nu' \in q\mathcal{I}$, therefore $\nu \in (1 - \epsilon)q\mathcal{I}$.

The nature of the AB-relation allows us to observe

Lemma 4.10. *With the definitions above we have*

- $p[(b_i, p_i)_{i\in I} \downarrow] = (b_i, pp_i)_{i\in I} \downarrow$;
- $(b_i, p_i)_{i\in I} \downarrow \oplus (b'_j, p'_j)_{j\in J} \downarrow = [(b_i, p_i)_{i\in I} \oplus (b'_j, p'_j)_{j\in J}] \downarrow$.

To prove this the key observation is the following:

Proposition 4.11. *If*

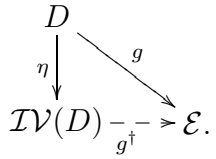
$$(b_i, p_i)_{i\in I} \prec (c_j, q_j)_{j\in J} \ ,$$

then for every j there exist $c'_j \ll c_j$ and $q'_j \ll q_j$ such that

$$(b_i, p_i)_{i\in I} \prec (c'_j, q'_j)_{j\in J} \prec (c_j, q_j)_{j\in J} \ .$$

The proof of this proposition is already contained in the proof of proposition 4.4.

Now we show the universal property, which proves both that $\mathcal{IV}$ is a functor and that is left adjoint: for every continuous function $g : D \to \mathcal{E}$ where $\mathcal{E} \in \mathbf{QCONT}$ there is a unique $g^\dagger : \mathcal{IV}(D) \to \mathcal{E}$ (in the category $\mathbf{QCONT}$) s.t.



where $\eta(d) = \{(b,p)_{*\in\{*\}} \mid b \ll d,\ p < 1\}$. (The assignment $g \mapsto g^\dagger$ is continuous.)

Take the restriction of g to B_D. It has a unique homomorphic extension $\overline{g} : IV(B_D) \to \mathcal{E}$. Defined by

$$\begin{aligned} \overline{g}\left((b,1)_{*\in\{*\}}\right) &:= g(b)\ ; \\ \overline{g}\left((b_i,p_i)_{i\in I}\right) &:= \bigoplus_{i\in I} p_i g(b_i)\ . \end{aligned}$$

We claim that $\overline{g}$ is monotonic, in the sense that,

Lemma 4.12. *if $\nu \prec \xi$, then $\overline{g}(\nu) \sqsubseteq \overline{g}(\xi)$.*

Proof: (of the lemma) First suppose that $(b,p)_{*\in\{*\}} \prec (c_j,q_j)_{j\in J}$, and the the witness f for this is total. Then $p \ll \sum_{j\in J} q_i =: q$ and for every j, $b \ll c_j$. Notice also that $p = \sum_{j\in J} \frac{q_j}{q} p$. Applying iteratively the inequation (HV), we can show that:

$$\overline{g}\left((b,p)_{*\in\{*\}}\right) = pg(b) \sqsubseteq \bigoplus_{j\in J} \frac{q_j}{q} pg(b)\ .$$

Then, by monotonicity of the operations and of g,

$$\bigoplus_{j\in J} \frac{q_j}{q} pg(b) \sqsubseteq \bigoplus_{j\in J} q_j g(c_j) = \overline{g}\left((c_j,q_j)_{j\in J}\right)\ .$$

Now suppose $(b_i,p_i)_{i\in I} \prec (c_j,q_j)_{j\in J}$ with again a total witness f. Let $J_i = f^{-1}(i)$. Clearly $(b_i,p_i)_{*\in\{*\}} \prec (c_j,q_j)_{j\in J_i}$ for every $i \in I$. Therefore

$$\overline{g}\left((b_i,p_i)_{*\in\{*\}}\right) \sqsubseteq \overline{g}\left((c_j,q_j)_{j\in J_i}\right)\ .$$

Notice that $(b_i, p_i)_{i\in I} = \bigoplus_{i\in I}(b_i, p_i)_{*\in\{*\}}$ and $(c_j, q_j)_{j\in J} = \bigoplus_{i\in I}(c_j, q_j)_{j\in J_i}$. Monotonicity of the sum, and the homomorphism condition on $\overline{g}$ imply that

$$\overline{g}\left((b_i, p_i)_{i\in I}\right) \sqsubseteq \overline{g}\left((c_j, q_j)_{j\in J}\right) \ .$$

Finally, for the case where f is not total, let J_0 be the domain of f and J_1 be its complement. Clearly $(c_j, q_j)_{j\in J} = (c_j, q_j)_{j\in J_0} \oplus (c_j, q_j)_{j\in J_1}$. Moreover.

$$\overline{g}\left((b_i, p_i)_{i\in I}\right) \sqsubseteq \overline{g}\left((c_j, q_j)_{j\in J_0}\right) \ .$$

Equations (4)-(5) together with the monotonicity of the scalar multiplication imply $\underline{0} \sqsubseteq A$. Therefore

$$\underline{0} = \overline{g}\left((\ , \ )\right) \sqsubseteq \overline{g}\left((c_j, q_j)_{j\in J_1}\right) \ .$$

And finally

$$\overline{g}\left((b_i, p_i)_{i\in I}\right) = \overline{g}\left((b_i, p_i)_{i\in I} \oplus (\ , \ )\right) \sqsubseteq \overline{g}\left((c_j, q_j)_{j\in J}\right) \ .$$

□(lemma)

Let us call $g^\dagger$ the extension of $\overline{g}$ to $\mathcal{IV}(D)$ (the ideal completion of $(IV(B_D)$.) We recall that $g^\dagger(\mathcal{I}) := \bigsqcup^{\uparrow}_{X\in\mathcal{I}} \overline{g}(X)$. We know that the function $g^\dagger$ is continuous. The continuity of the operations implies that $g^\dagger$ is also an homomorphism. Thus it is a morphism of the category. It remains to show that $g^\dagger\big(\{(b, p)_{*\in\{*\}} \mid b \ll d,\ p < 1\}\big) = g(d)$

Now

$$g^\dagger\big(\{(b, p)_{*\in\{*\}} \mid b \ll d,\ p < 1\}\big) = \bigsqcup_{b\ll d,\, p<1}{}^{\uparrow}\, \overline{g}((b, p)_{*\in\{*\}})$$

$$= \bigsqcup_{b\ll d,\, p<1}{}^{\uparrow}\, pg(b) = \bigsqcup_{p<1}{}^{\uparrow}\, pg(d) = g(d) \ .$$

The last two equalities being a consequence of the continuity of g and of the scalar multiplication.

In a similar way, using lemma 4.10, one can prove that in fact for every $\nu \in IV(B_D)$, $\overline{g}(\nu) = g^\dagger(\nu\downarrow)$.

$$\begin{array}{ccc} IV(B_D) & & \\ {\scriptstyle\iota}\downarrow & \searrow^{\overline{g}} & \\ \mathcal{IV}(D) & \xrightarrow[g^\dagger]{} & \mathcal{E}. \end{array}$$

To prove uniqueness, let $h : \mathcal{IV}(D) \to \mathcal{E}$ be a continuous homomorphism such that for every $d \in D$, $h(\eta(d)) = g(d)$. Since h is an homomorphism, we have that when for every $(b_i, p_i)_{i\in I} \in IV(B_D)$

$$h\big((b_i, p_i)_{i\in I} \downarrow\big) = \bigoplus_{i\in I} p_i h(\eta(b_i)) = \bigoplus_{i\in I} p_i g(b_i)$$

$$= \overline{g}\big((b_i, p_i)_{i\in I}\big) = g^\dagger\big((b_i, p_i)_{i\in I} \downarrow\big)$$

Since h and $g^\dagger$ coincide on the basis, they are equal.

We omit the straightforward proof that the assignment $g \mapsto g^\dagger$ is continuous. □

Omitting the mention of the forgetful functor, we can say that $\mathcal{IV}$ is a monad in $\mathbf{CONT}$. The unit $\eta^{\mathcal{IV}}_D : D \to \mathcal{IV}(D)$ is defined as

$$\eta^{\mathcal{IV}}_D(d) = (d, 1)_{*\in\{*\}} \downarrow = \{(b, p)_{*\in\{*\}} \mid b \ll d,\ p < 1\} .$$

The multiplication $\mu^{\mathcal{IV}}_D : \mathcal{IV}^2(D) \to \mathcal{IV}(D)$ is just the extension of $\mu^{IV}_B : IV^2(B) \to IV(B)$ defined as in the category $\mathbf{SET}$.

Notice that the universal property of this construction shows also that it is independent of the choice of the basis B of D.

4.3 A distributive law (categorically)

Given a continuous domain D with basis B, consider the set $P(B)$ of nonempty finite subsets of B, endowed with the Hoare order:

$$X \prec Y \iff \forall x \in X.\exists y \in Y.x \ll y .$$

It is known that $(P(B), \prec)$ is a basis for the Hoare powerdomain $\mathcal{P}_H(D)$.

With the usual abuse of notation, we say that $\mathcal{P}_H$ has a monad structure in the category $\mathbf{CONT}$ (in the sequel we write $\mathcal{P}$ for $\mathcal{P}_H$).

To define a distributive law we need to give a family α_D of continuous functions $\mathcal{IV} \circ \mathcal{P}(D) \to \mathcal{P} \circ \mathcal{IV}(D)$. Remember that these functors are defined as ideal completions of some abstract bases. Our approach is to define a (monotonic) function between the bases and take the extension as our candidate. Consider the function $a_B : IV(P(B)) \to P(IV(B))$:

$$a_B\big((S_i, p_i)_{i\in I}\big) = \big\{(h(i), p_i)_{i\in I} \mid h : I \to B,\ h(i) \in S_i\big\} .$$

Lemma 4.13. *The function a_B preserves the abstract basis relation.*

Proof: Take $(S_i, p_i)_{i\in I} \prec (T_j, q_j)_{j\in J}$. Let $f : J \twoheadrightarrow I$ be a witness for that. Therefore:

- $p_i \ll \sum_{f(j)=i} q(j)$;
- $S_{f(j)} \prec T_j$.

The second formula is by definition equivalent to saying that for every $b \in S_{f(j)}$ there exists $c \in T_j$ such that $b \ll c$.

We have to prove that

$$\left\{(h(i), p_i)_{i\in I} \middle|\, h : I \to B,\ h(i) \in S_i\right\} \prec \left\{(k(j), q_j)_{j\in J} \middle|\, k : J \to B,\ k(j) \in T_j\right\}.$$

We have to show that for every $h : I \to B, h(i) \in S_i$ there exist a $k : J \to B, k(j) \in T_j$ such that $(h(i), p_i)_{i\in I} \prec (k(j), q_j)_{j\in J}$. How is k defined? For every j, consider $h(f(j))$. It is an element of $S_{f(j)}$. Therefore there exist some $c \in T_j$ with $h(f(j)) \ll c$. Let $k(j)$ be one of such c's [5]. Now we claim that f is a witness of $(h(i), p_i)_{i\in I} \prec (k(j), q_j)_{j\in J}$. We have already $p_i \ll \sum_{f(j)=i} q(j)$. And by construction $h(f(j)) \ll k(j)$, so we are done. □

Notice that it is essential the way the AB-relation is defined. Had we used Egli-Milner or Smyth AB-relation on finite sets, the statement of the lemma would not be true.

Define α_D to be the extension of a_B.

Theorem 4.14. *The family $\alpha_D : \mathcal{IV}(\mathcal{P}(D)) \to \mathcal{P}(\mathcal{IV}(D))$ defined above is a distributive law.*

We prove naturality directly, relying on the naturality of a_B in the category of sets. The proof is rather simple, but nevertheless we need some special notation.

Let $\mathcal{D}$ be a continuous domain with basis B_D. If $Y \in P(B_D)$ and if $X \subseteq D$, we write $Y \ll X$ to mean $\forall b \in Y.\exists d \in X$ such that $b \ll d$. If $X \subseteq D$ we will write $X\downarrow$ to mean $\left\{Y \in P(B_D) \,|\, Y \ll X\right\}$.

If I is a finite set and for every $i \in I$, $d_i \in D, p_i \in \overline{\mathbb{R}^+}$, and $b_i \in B_D, q_i \in \overline{\mathbb{R}^+}$ then we write $(b_i, q_i)_{i\in I} \ll (d_i, p_i)_{i\in I}$ to mean $\forall i \in I.b_i \ll d_i, q_i \ll p_i$. If J is any finite set, possibly different from I, and if for every $j \in J$, $b'_j \in B_D, q'_j \in \overline{\mathbb{R}^+}$, then we write $(b'_j, q'_j)_{j\in J} \ll (d_i, p_i)_{i\in I}$ to mean that there is $(b_i, q_i)_{i\in I} \in IV(B_D)$

[5] Since everything is finite, we do not even invoke the axiom of choice, take that, Zorn!

such that $(b'_j, q'_j)_{j\in J} \prec (b_i, q_i)_{i\in I} \ll (d_i, p_i)_{i\in I}$. We also write $(d_i, p_i)_{i\in I} \downarrow$ to mean $\big\{(b_i, q_i)_{i\in I} \in IV(B_D) \,|\, \forall i \in I. b_i \ll d_i, q_i \ll p_i\big\} \downarrow \in \mathcal{IV}(D)$.

Consistently we write

$$(X_i, p_i)_{i\in I} \downarrow$$

to mean

$$\big\{(Y_i, q_i)_{i\in I} \in IV(P(B_D)) \,|\, Y_i \ll X_i, q_i \ll p_i\big\} \downarrow \in \mathcal{IV}(\mathcal{P}(D))$$

and we write

$$\big\{(d^\rho_i, p^\rho_i)_{i\in I} \,|\, \rho \in R\big\} \downarrow$$

(assuming finiteness of R) to mean

$$\big\{\{(b^\rho_i, q^\rho_i)_{i\in I} \,|\, \rho \in R\} \downarrow, \,|\, \forall \rho \in R. b^\rho_i \ll d^\rho_i, q^\rho_i \ll p^\rho_i\big\} \downarrow \in \mathcal{P}(\mathcal{IV}(D)) \,.$$

We can extend proposition 4.11 and lemma 4.10 to this new notation.

Proposition 4.15. *If*

$$(b_i, p_i)_{i\in I} \ll (d_j, q_j)_{j\in J} \,,$$

then for every j there exist $c'_j \in B_D$, $c'_j \ll c_j$ and $q'_j \ll q_j$ such that

$$(b_i, p_i)_{i\in I} \prec (c'_j, q'_j)_{j\in J} \ll (c_j, q_j)_{j\in J} \,.$$

Lemma 4.16. *If $d_i, d'_j \in D$ for every $i \in I, j \in J$ then:*

$p[(d_i, p_i)_{i\in I} \downarrow] = (d_i, pp_i)_{i\in I} \downarrow$ *;*

- $(d_i, p_i)_{i\in I} \downarrow \oplus (d'_j, p'_j)_{j\in J} \downarrow = [(b_i, p_i)_{i\in I} \oplus (b'_j, p'_j)_{j\in J}] \downarrow$ *;*

If Y, Y' are finite subsets of D then

- $Y \downarrow \uplus Y' \downarrow = (Y \cup Y') \downarrow$.

Using lemma 4.16 we prove the following.

Lemma 4.17. *If Z is any set and $f : Z \to D$ is a function, then the homomorphic extension $\overline{f} : IV(P(Z)) \to \mathcal{IV}(\mathcal{P}(D))$ is defined as*

$$\overline{f}\big((Y_i, p_i)_{i\in I}\big) = (f[Y_i], p_i)_{i\in I} \downarrow \,;$$

and $\overline{f} : P(IV(Z)) \to \mathcal{P}(\mathcal{IV}(D))$ is defined as

$$\overline{f}\big(\{(z^\rho_i, p^\rho_i)_{i\in I} \,|\, \rho \in R\}\big) = \big\{(f(z^\rho_i), p^\rho_i)_{i\in I} \,|\, \rho \in R\big\} \downarrow \,.$$

Now, let $f : D \to D'$ be a continuous function. Consider the restriction of f to B_D. First we prove that

Lemma 4.18. $\alpha\big((f[Y_i], p_i)_{i\in I} \downarrow\big) = \overline{f}(a\big((Y_i, p_i)_{i\in I}\big))$.

$$\begin{array}{ccc} B_D & & IV(P(B)) \xrightarrow{a} P(IV(B)) \\ {\scriptstyle f}\downarrow & & \quad\overline{f}\downarrow \qquad\qquad \downarrow\overline{f} \\ \mathcal{D} & & \mathcal{IV}(\mathcal{P}(D)) \xrightarrow[\alpha]{} \mathcal{P}(\mathcal{IV}(D)). \end{array}$$

Now

$$\alpha\big((f[Y_i], p_i)_{i\in I} \downarrow\big) = \Big\{a\big((Z_i, q_i)_{i\in I}\big) \mid Z_i \ll f[Y_i], q_i \ll p_i\Big\} \downarrow$$

$$= \Big\{\big\{(h(i), q_i)_{i\in I} \mid h : I \to B_{D'}, h(i) \in Z_i\big\} \mid Z_i \ll f[Y_i], q_i \ll p_i\Big\} \downarrow$$

$$= \big\{(h(i), p_i)_{i\in I} \mid h' : I \to D', h(i) \in f[Y_i]\big\} \downarrow \ .$$

The first two equalities are true by definition. As for the last, let $\mathcal{A}$ be

$$\Big\{\big\{(h(i), q_i)_{i\in I} \mid h : I \to B_{D'}, h(i) \in Z_i\big\} \mid Z_i \ll f[Y_i], q_i \ll p_i\Big\} \downarrow$$

and let $\mathcal{B}$ be

$$\big\{(h(i), p_i)_{i\in I} \mid h' : I \to D', h(i) \in f[Y_i]\big\} \downarrow \ .$$

Take $X \in \mathcal{B}$. This means that for every $\nu \in X$ there exists $h\nu : I \to D', h_\nu(i) \in f[Y_i]$ such that $\nu \prec (h_\nu(i), p_i)_{i\in I}$. We want to prove that $X \in \mathcal{A}$. So we want to prove that there exists a family (Z_i) and a family (q_i) such that $Z_i \ll f[Y_i], q_i \ll p_i$ and for every $\nu \in X$ there exists $k_\nu : I \to B_{D'}, k_\nu(i) \in Z_i$ for which $\nu \prec (k_\nu(i), q_i)_{i\in I}$. By proposition 4.15 we can find $q_i^\nu \ll p_i$ and $z_i^\nu \in B_{D'}$ with $z_i^\nu \ll h_\nu(i)$ such that $\nu \prec (z_i^\nu, q_i^\nu)_{i\in I} \ll (h_\nu(i), p_i)_{i\in I}$. Let $Z_i := \{z_i^\nu \mid \nu \in X\}$ and let $q_i = \max_{\nu\in X} q_i^\nu$. Clearly $Z_i \ll f[Y_i]$ and $q_i \ll p_i$. We define $k_\nu(i) = z_i^\nu$ and we are done.

The other inclusion is easier and it is left to the reader.

On the other hand

$$\overline{f}(a\big((Y_i, p_i)_{i\in I}\big)) = \overline{f}\Big(\big\{(h(i), p_i)_{i\in I} \mid h : I \to B_D, h(i) \in Y_i\big\}\Big)$$

$$= \big\{(f(h(i)), p_i)_{i\in I} \mid h : I \to B_D, h(i) \in Y_i\big\} \downarrow \ .$$

Let $\mathcal{C}$ be this last set. The lemma is proved if we show that $\mathcal{C} = \mathcal{B}$. Recall that in the proof of theorem 2.8 we have shown that $\{(h(i), p_i)_{i\in I} \mid h' : I \to D', h(i) \in f[Y_i]\} = \{(f(h(i)), p_i)_{i\in I} \mid h : I \to B_D, h(i) \in Y_i\}$, so we are done.

To prove naturality now take $\mathcal{I} \in \mathcal{IV}(\mathcal{P}(D))$. We want to show that $\alpha \circ \mathcal{IV}(\mathcal{P}(f))(\mathcal{I}) = \mathcal{P}(\mathcal{IV}(f)) \circ \alpha(\mathcal{I})$.

$$\begin{array}{ccc} D & & \mathcal{IV}(\mathcal{P}(D)) \xrightarrow{\alpha} \mathcal{P}(\mathcal{IV}(D)) \\ {\scriptstyle f}\downarrow & & {\scriptstyle \mathcal{IV}(\mathcal{P}(f))}\downarrow \qquad\qquad \downarrow{\scriptstyle \mathcal{P}(\mathcal{IV}(f))} \\ \mathcal{D} & & \mathcal{IV}(\mathcal{P}(D)) \xrightarrow[\alpha]{} \mathcal{P}(\mathcal{IV}(D)). \end{array}$$

We do that by a chain of equations

$$\begin{aligned} \alpha(\mathcal{IV}(\mathcal{P}(f))(\mathcal{I})) &= \sup_{J\in\mathcal{IV}(\mathcal{P}(f))(\mathcal{I})} a(J) && \text{by definition of } \alpha \\ &= \sup_{J\ll f(I),\, I\in\mathcal{I}} a(J) && \text{by definition of } \mathcal{P}(\mathcal{IV}(f)) \\ &= \sup_{I\in\mathcal{I}} a(\overline{f}(I)) && \text{by cofinality} \\ &= \sup_{I\in\mathcal{I}} \overline{f}(a(I)) && \text{by lemma 4.18} \\ &= \sup_{H\ll a(I),\, I\in\mathcal{I}} \overline{f}(H) && \text{by cofinality} \\ &= \sup_{H\in\alpha(\mathcal{I})} \overline{f}(H) && \text{by definition of } \alpha \\ &= \mathcal{P}(\mathcal{IV}(f))(\alpha(\mathcal{I})) && \text{by definition of } \mathcal{P}(\mathcal{IV}(f)) \end{aligned}$$

□

To prove the other conditions we use the following fact:

Proposition 4.19. *Consider domains D, D', D'' with bases B, B', B''. Take functions $f : B \to B'$, $g : B' \to B''$ preserving the AB-relation. Then*

$$ext(g) \circ ext(f) = ext(g \circ f).$$

Thus if we prove the commutativity of a diagram in the category of abstract basis and monotonic functions, this carries over to the diagram constituted by their extensions.

Now we have to prove the commutativity of four diagrams. We start with

Proposition 4.20.

$$\begin{array}{ccccc}
\mathcal{IV}\circ\mathcal{IV}\circ\mathcal{P} & \xrightarrow{\mathcal{IV}\alpha} & \mathcal{IV}\circ\mathcal{P}\circ\mathcal{IV} & \xrightarrow{\alpha\mathcal{IV}} & \mathcal{P}\circ\mathcal{IV}\circ\mathcal{IV} \\
\downarrow{\scriptstyle \mu^{\mathcal{IV}}\mathcal{P}} & & & & \downarrow{\scriptstyle \mathcal{P}\mu^{\mathcal{IV}}} \\
\mathcal{IV}\circ\mathcal{P} & & \xrightarrow[\alpha]{} & & \mathcal{P}\circ\mathcal{IV}.
\end{array}$$

We know that for every (abstract) basis B the following diagram commutes (because it is essentially the diagram for the distributive law in the category $\mathbf{SET}$):

$$\begin{array}{ccc}
IV(IV(P(B))) & \xrightarrow{\mu^{IV}_{P(B)}} & IV(P(B)) \\
\downarrow{\scriptstyle IV(a_B)} & & \\
IV(P(IV(B))) & & \downarrow{\scriptstyle a_B} \\
\downarrow{\scriptstyle a_{IV(B)}} & & \\
P(IV(IV(B))) & \xrightarrow[P(\mu^{IV}_B)]{} & P(IV(B)).
\end{array}$$

Lemma 4.21. *Using the above notation we have*

- $\alpha_D = ext(a_B)$;
- $\alpha_{\mathcal{IV}(D)} = ext(a_{IV(B)})$;
- $\mu^{\mathcal{IV}}_{\mathcal{P}(D)} = ext(\mu^{IV}_{P(B)})$;
- $\mathcal{P}(\mu^{\mathcal{IV}}_D) = ext(P(\mu^{IV}_B))$;
- $\mathcal{IV}(\alpha_D) = ext(IV(a_B))$.

The first three equalities are true by definition, while some work is needed to show the other two. It can be helpful to state a more general result

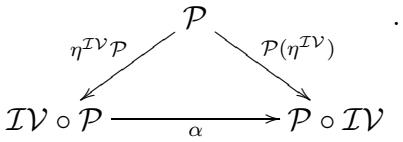
Proposition 4.22. *Let D, D' be continuous domains with basis B, B'. Let $f : B \to B'$ be a function preserving $\ll$. Then, using the above notation*

$$ext(P(f)) = \mathcal{P}(ext(f)), \quad ext(IV(f)) = \mathcal{IV}(ext(f)).$$

Lemma 4.21 together with lemma 4.13 and proposition 4.19 give us the proof of proposition 4.20.

The proof of two of the other diagrams is similar. A bit different is the following.

Proposition 4.23.



The difference is that η^{IV} does not preserve the AB-relation. But it is not difficult to check directly the commutativity of the diagram, using the definition of the domains as ideal completions.

□

We therefore have a monad structure for the functor $\mathcal{P} \circ \mathcal{IV}$.

4.4 A distributive law (equationally)

Following [AJ94] we introduce the notion of *Domain-algebra*. Let $\mathcal{E}$ be an inequational theory on some signature. A continuous domain-algebra for $\mathcal{E}$ is a continuous domain together with a Scott-continuous operation for every symbol in the signature satisfying the inequalities in $\mathcal{E}$.

The continuous quasi-cones defined above can be seen as domain-algebras. We have to see the scalar multiplication as a collection of unary operations, one for each positive real (and $+\infty$), and to require explicitly that the scalar multiplication be continuous in the first argument. (Another possibility would be to define multi-sorted domain algebras.)

An interesting theory on the signature $\{ \uplus \}$ is the theory (8)–(10) of semilattices augmented with:

- HP: $A \sqsubseteq A \uplus B$.

Its continuous domain-algebras are also called continuous join semi-lattices. It is known that $\mathcal{P}$ is the free continuous join semi-lattice. Similarly to what we have observed in the category $\mathbf{SET}$, we have the following result.

Definition 4.24. A *continuous QCJ-algebra* is a continuous domain algebra over the theory (1)–(12) + (HV) + (HP), with the extra requirement that the scalar multiplication be continuous in the first argument.

Theorem 4.25. *The monad on $\mathcal{P} \circ \mathcal{IV}$ obtained from the distributive law is the free continuous* $\mathbf{QCJ}$*-algebra.*

Proof: The proof of this theorem follows the same line of the proof of theorem 4.8. First we prove the freeness of $\mathcal{P} \circ \mathcal{IV}$, then we show the identity of the two monads.

Proposition 4.26. *If D is a continuous domain, then $\mathcal{P}(\mathcal{IV}(D)) \in \mathbf{QCJ}$.*

Proof: We define the operations in $P(IV(B_D))$ as follows:

$$\begin{aligned} X \oplus Y &:= \{\nu \oplus \xi \mid \nu \in X, \xi \in Y\} ; \\ pX &:= \{p\nu \mid \nu \in X\} ; \\ X \uplus Y &:= X \cup Y . \end{aligned}$$

These operations are monotonic with respect to $\prec$ and all the equations of Eq are true in $P(IV(B_D))$. Moreover:

Proposition 4.27. *With the notation used above, if $X \prec X'$ then for every Y, $X \prec X' \uplus Y$. If $X \prec X'$ and $p \ll q_1 + q_2$ then $pX \prec q_1X' \oplus q_2X'$.*

The first statement is obvious, from the definition of Hoare order. As for the second, assume $X \prec X'$. Take $\nu \in X$. We want to show that there is $\nu' \in q_1X' \oplus q_2X'$ such that $\nu \prec \nu'$. Since $X \prec X'$, there exists $\xi \in X'$ s.t. $\nu \prec \xi$. By lemma 4.9 $p\nu \prec q_1\xi \oplus q_2\xi$. And for sure $q_1\xi \oplus q_2\xi \in q_1X' \oplus q_2X'$. □

(Notice that this proof would not work, had we used the Egli-Milner or Smyth order on finite sets).

Define the operations in the ideal completion as follows:

$$\begin{aligned} \mathcal{I} \oplus \mathcal{J} &:= \{X \oplus Y \mid X \in \mathcal{I}, Y \in \mathcal{J}\} \downarrow ; \\ p\mathcal{I} &:= \{pX \mid X \in \mathcal{J}\} ; \\ \mathcal{I} \uplus \mathcal{J} &:= \{X \cup Y \mid X \in \mathcal{I}, Y \in \mathcal{J}\} \downarrow . \end{aligned}$$

Clearly these operations are well defined, continuous, and satisfy the equations. The inequation $\mathcal{I} \subseteq \mathcal{I} \uplus \mathcal{J}$ follows from $X \prec X' \Longrightarrow X \prec X' \cup Y$ and the roundedness of the ideals. The inequation $(p_1 + p_2)\mathcal{I} \subseteq p_1\mathcal{I} \oplus p_2\mathcal{I}$ follows from $p \ll q_1 + q_2, X \prec X' \Longrightarrow pX \prec q_1X' \oplus q_2X'$ and the roundedness of the ideals. It remains to show the continuity of the scalar multiplication. Take an ideal $\mathcal{I} \in \mathcal{P}(\mathcal{IV}(D))$. We want to prove that

$$\bigcup_{p<q} p\mathcal{I} = q\mathcal{I} .$$

that is for every X, we have $X \in q\mathcal{I}$ if and only if there exist $p \ll q$ s.t. $X \in p\mathcal{I}$. The "if" direction follows from the fact that $pY \prec qY \oplus 0Y = qY$. It remains the other inclusion.

Consider the case $q < \infty$ (the other being similar). Take $X \in q\mathcal{I}$. If $X = (,)_{i\in\emptyset}$ the statement holds. Otherwise, by roundedness there is $X' \in q\mathcal{I}$ s.t. $X \prec X'$. So for every $\nu \in X$ there is $\xi \in X',\ \nu \prec \xi$. Choose one such ξ_ν for each ν. Everything is finite, so no axiom of choice is invoked. We leave to the reader to proof that for every ν there exists ϵ_ν such that $\nu \prec (1-\epsilon_\nu)\xi_\nu$. Define ϵ to be the minimum among all the numbers $\epsilon_\nu, \nu \in X$ (they are finitely many). Clearly $X \prec (1-\epsilon)X'$. But $X' \in q\mathcal{I}$, therefore $X \in (1-\epsilon)q\mathcal{I}$. □

The following universal property holds.

Proposition 4.28. *For every continuous function $g : D \to \mathcal{E}$ where $\mathcal{E} \in \mathbf{QCJ}$ there is a unique $g^\dagger : \mathcal{P}(\mathcal{IV}(D)) \to \mathcal{E}$ (in the category $\mathbf{QCJ}$) s.t.*

$$\begin{array}{ccc} D & & \\ {\scriptstyle\eta}\downarrow & \searrow^{g} & \\ \mathcal{P}(\mathcal{IV}(D)) & \xrightarrow[g^\dagger]{} & \mathcal{E}. \end{array}$$

where $\eta(d) = \{(d,1)_{*\in\{*\}}\} \downarrow$. The assignment $g \mapsto g^\dagger$ is continuous.

Proof: Take the restriction of g to B_D. It has a unique homomorphic extension $\overline{g} : P(IV(B_D)) \to \mathcal{E}$. Defined by

$$\begin{aligned} \overline{g}\left((b,1)_{*\in\{*\}}\right) &:= g(b)\,; \\ \overline{g}\left((b_i,p_i)_{i\in I}\right) &:= \sum_{i\in I} p_i g(b_i)\,; \\ \overline{g}(X) &:= \bigcup_{\nu\in X} \overline{g}(\nu)\,. \end{aligned}$$

It can be shown that, if $X \prec Y$ then $\overline{g}(X) \sqsubseteq \overline{g}(Y)$. Let us call $g^\dagger$ the extension of $\overline{g}$ to $\mathcal{P}(\mathcal{IV}(D))$ (the ideal completion of $P(IV(B_D))$.) We recall that $g^\dagger(\mathcal{I}) := \bigsqcup^{\uparrow}_{X\in\mathcal{I}} \overline{g}(X)$.

We know that the function $g^\dagger$ is continuous. The continuity of the operations implies that $g^\dagger$ is also an homomorphism. Thus it is a morphism of the category. It remains to show that $g^\dagger(\eta(d)) = g(d)$

Now

$$g^\dagger\Big(\big\{\{(b,p)_{*\in\{*\}} \mid b \ll d,\ p<1\}\big\}\downarrow\Big) = \bigsqcup_{b\ll d,\, p<1}{}^{\uparrow}\,\overline{g}\Big(\big\{((b,p)_{*\in\{*\}}\big\}\Big)$$

$$= \bigsqcup_{b \ll d,\, p<1}{}^{\uparrow} pg(b) = \bigsqcup_{p<1}{}^{\uparrow} pg(d) = g(d)\ .$$

The last two equalities are a consequence of the continuity of g and of the scalar multiplication.

Again the to prove uniqueness we notice that $\overline{g}(X) = g^{\dagger}(X\downarrow)$.

$$\begin{array}{ccc} P(IV(B_D)) & & \\ \downarrow{\scriptstyle \iota} & \searrow^{\overline{g}} & \\ \mathcal{P}(\mathcal{IV}(D)) & \xrightarrow[g^{\dagger}]{} & \mathcal{E}. \end{array}$$

and again we omit the proof that the assignment $g \mapsto g^{\dagger}$ is continuous.

It is clear the functor and the unit are the same. As for the multiplication, notice that the multiplication generated by the freeness condition is the (continuous) extension of the homomorphic extension $\overline{id} : P \circ IV \circ P \circ IV \to P \circ IV$. The multiplication of the monad generated by the distributive law is $\mu^{\mathcal{P}}\mu^{\mathcal{IV}} \circ \mathcal{P}\alpha\mathcal{IV}$ which by proposition 4.19 and lemma 4.21 is equal to the continuous extension of $\mu^{P}\mu^{IV} \circ PaIV$. But we know that $\mu^{P}\mu^{IV} \circ PaIV = \overline{id}$, (as they are in fact the multiplication of the composite monad in $\mathbf{SET}$), therefore also their extensions coincide.

Let's look at some useful properties. If we define

$$\iota : P(IV(B)) \to \mathcal{P}(\mathcal{IV}(D))$$

as

$$\iota\big(\{(b_i^k, p_i^k)_{i\in I}\}\big) = \{(b_i^k, p_i^k)_{i\in I}\}\downarrow$$

it is not difficult to prove that

Proposition 4.29.

$$\iota(A \cup B) = \iota(A) \uplus \iota(B)$$
$$\iota(pA) = p\iota(A)$$
$$\iota(A + B) = \iota(A) \oplus \iota(B)$$
$$\iota(0) = \underline{0}$$

5 The Construction of Tix and Mislove

In this section we only outline the results. More details will appear in the author's PhD thesis.

If instead of the axiom (HV) we had added the more standard $(p+q)A = (pA \oplus qA)$ (13), the resulting free construction would be the one of Tix and Mislove, which still includes the equational distributive laws, but without any corresponding categorical distributive law.

Definition 5.1. [Tix99] A *continuous d-cone* is a continuous quasi-cone satisfying $(p+q)A = pA \oplus qA$. The corresponding category is called $\mathbf{CCONE}$. A *continuous join TM-cone* is a continuous domain algebra for the theory (1)–(13)+(HP) for which the scalar multiplication is continuous also in the first argument. The corresponding category is called $\mathbf{CJTM}$ A subset X of a continuous d-cone is *convex* if for every $x, y \in X$ and for every $p \in [0,1]$, we have that $px \oplus (1-p)y \in X$. If H is a continuous d-cone, we define

$$\mathcal{P}_{TM}(H) := \{X \subseteq H \mid X \neq \emptyset, \text{convex, Scott-closed}\}$$

Tix calls this construction the *convex hoare powercone*. With the sets ordered by inclusion, the addition and multiplication defined (essentially) pointwise, and the union defined as union followed by convex closure and by topological closure, we have that $\mathcal{P}_{TM}(H)$ is a continuous TM-cone.

Jones (and Kirch for our setting) showed that the powerdomain of valuations functor $\mathcal{V} : \mathbf{CONT} \to \mathbf{CCONE}$ is left adjoint of the forgetful functor. Tix in her thesis showed that the functor $\mathcal{P}_{TM}(H) : \mathbf{CCONE} \to \mathbf{CJTM}$ is left adjoint of the forgetful functor.

If B is a basis for D, finite valuations with the AB-relation induced by the splitting lemma are a basis for $\mathcal{V}(D)$. If B is a basis for the continuous d-cone H, finite generated convex subsets of $\overline{B}$ with a hoare-like AB-relation are a basis for $\mathcal{P}_{TM}(H)$.

6 Semantics of programs

We give an example of how to use the above constructions by giving semantics to a simple imperative language with probabilistic and nondeterministic primitives. First we introduce the operational model. We then introduce the language. We

give operational and denotational semantics to the language, and we state an adequacy theorem. Finally we compare briefly the computational meaning of our semantics with the one obtained using Tix-Mislove.

In the sequel we shall write $(x_i, p_i)_{i\in I}$ also to denote $\iota\big((x_i, p_i)_{i\in I}\big) \in \mathcal{IV}(X)$. We will use this notation even when I is not finite, to denote the lub of all its finite "truncations".

6.1 The operational model

Our operational model is similar to the probabilistic transition systems of [JLY01]. Our presentation is inspired by the alternating model of [Han91].

Definition 6.1. A probabilistic (unlabeled) synchronisation tree (PST) on a set of "states" S is a structure $(Nodes, Arcs, label_N, label_P)$ where

- $(Nodes, Arcs)$ is a tree;
- $Nodes = N \uplus P$: there are *Nondeterministic* nodes and *Probabilistic* nodes;
- $Arcs \subseteq (N \times P) \uplus (P \times N)$: an arc connects only nodes of different kind;
- $label_N : N \to S$: nondeterministic nodes are labeled by states;
- $label_P : Arcs \cap (P \times N) \to \overline{\mathbb{R}^+}$: arcs leaving probabilistic nodes are labeled with probabilities;

Definition 6.2. A deterministic scheduler $\mathcal{S}$ for a PST is a function $f_{\mathcal{S}} : N \to P$ such that if $f_{\mathcal{S}}(n) = p$ then $(n, p) \in Arcs$.

A deterministic[6] scheduler chooses for every nondeterministic node one of its probabilistic sons.

Definition 6.3. A probabilistic scheduler $\mathcal{S}$ for a PST is a function $f_{\mathcal{S}} : N \to P \to \overline{\mathbb{R}^+}$ such that if $f_{\mathcal{S}}(n)(p) \neq 0$ then $(n, p) \in Arcs$.

A probabilistic scheduler chooses for every deterministic node a discrete valuation over its sons. Notice that a deterministic scheduler can always be seen as a probabilistic scheduler.

[6]This is the standard term used in literature. It is not a fortunate choice because what we mean here is absence of probabilities. A better term could be *certain*.

The effect of a scheduler is to give a fully probabilistic model. A probabilistic scheduler is, in practice, labeling with probabilities the arcs going out of a nondeterministic node. Once every arc is endowed with probabilities we can talk of the probability of a path as the (possibly infinite) product of the probabilities of all its components.

Using probabilistic automata and schedulers we can give another motivation for our axiom (HV) and corresponding definition 4.3, which implies

$$\delta_x \sqsubseteq \tfrac{1}{2}\delta_x + \tfrac{1}{2}\delta_x \ .$$

Consider the example in figure 1. The figure represents two processes as proba-

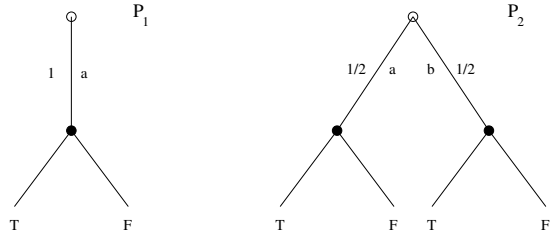


Figure 1: Processes

bilistic trees. The process P_1 allows two different ways of resolving the nondeterminism. The corresponding probability distributions are δ_T and δ_F. The process P_2 allows four different ways of resolving the nondeterminism, two of which give the probability distribution $\frac{1}{2}\delta_T + \frac{1}{2}\delta_F$. The process P_2 offers more opportunities, so in a Hoare fashion, we consider it better than P_1. Formally this is implied by $1\delta_x \sqsubseteq \frac{1}{2}\delta_x + \frac{1}{2}\delta_x$.

6.2 A simple imperative language

We present a small imperative language **L**. It has the following (abstract) syntactic categories:

- integers **Num**, ranged over by n;
- locations **Loc**, ranged over by X;
- finite probability distributions over integers **Prob**, ranged over by χ;

- arithmetical expressions **Aexp**, ranged over by a;
- boolean expressions **Bexp**, ranged over by b;
- commands **Comm**, ranged over by c.

The (abstract) BNF for the last three syntactic categories are as follows:

$$a ::= n \mid X \mid a + a \mid a - a \mid a * a$$

$$b ::= \mathbf{true} \mid \mathbf{false} \mid a = a \mid a \leq a \mid \neg b \mid b \wedge b \mid b \vee b$$

$$\begin{aligned} c ::= \quad & \mathbf{skip} \mid X := a \mid X := \chi \mid c; c \mid \\ & \mathbf{if}\ b\ \mathbf{then}\ c\ \mathbf{else}\ c \mid \\ & \mathbf{while}_i\ b\ \mathbf{do}\ c\ \ (i \in\ N) \mid \\ & \mathbf{while}\ b\ \mathbf{do}\ c \mid c\ \mathbf{or}\ c. \end{aligned}$$

We also need the notion of *state*. A state is a function $\sigma : \mathbf{Loc} \to \mathbf{Num}$. We call Σ the set of states. We call any pair $\langle c, \sigma \rangle$ a *configuration*. We denote the set of all configurations by Γ. The set Γ is ranged over by γ. To make the notation more uniform we introduce (at the metalevel) the empty command ϵ. We use it with the following meaning:

$$\langle \epsilon, \sigma \rangle \equiv \sigma\ ,$$

$$\epsilon; c \equiv c; \epsilon \equiv c\ .$$

We extend consequently the notion of configuration so that a state σ is a configuration $\langle c, \sigma \rangle$ where $c = \epsilon$.

The operational semantics for arithmetic and boolean expressions is as usual. The operational semantics of configurations is given by a PST built using the rules in table 1. It is intuitive how, using these rules, one can build a PST on the set of (extended) configurations.

Now given a configuration $\gamma := \langle c, \sigma \rangle$ and a scheduler $\mathcal{S}$ for the PST $\mathcal{T}(\gamma)$ with initial state labeled by γ, we consider the set of finite non-extensible labeled paths, $\mathcal{B}(\gamma, \mathcal{S})$ for the fully probabilistic tree obtained from $\mathcal{T}(\gamma)$ via the action of the scheduler $\mathcal{S}$. For every $s \in \mathcal{B}(\gamma, \mathcal{S})$ we define the probability of s, $\Pi(s)$, to be the product of the probability labels in s. We define $l(s)$ to be the label of the last node of s.

Definition 6.4. With $c, \sigma, \mathcal{S}$ as above, we define

$$v(\mathcal{S}, c, \sigma)(\sigma') = \sum_{\substack{l(s) = \sigma' \\ s \in \mathcal{B}(c, \sigma, \mathcal{S})}} \Pi(s)\ ;$$

$$\langle \mathbf{skip}, \sigma\rangle \xrightarrow{1} \sigma \qquad \frac{\langle a, \sigma\rangle \to n}{\langle X := a, \sigma\rangle \xrightarrow{1} \sigma[n/X]}$$

$$\langle X := \chi, \sigma\rangle (\xrightarrow{\chi(n)} \sigma[n/X]\ )_{n \in Supp(\chi)} \qquad \frac{\langle c, \sigma\rangle (\xrightarrow{p_i} \langle c_i, \sigma_i\rangle)_{i\in I}}{\langle c; c', \sigma\rangle (\xrightarrow{p_i} \langle c_i; c', \sigma_i\rangle)_{i\in I}}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{false}}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \xrightarrow{1} \langle c_1, \sigma\rangle} \qquad \frac{\langle b, \sigma\rangle \to \mathbf{true}}{\langle \mathbf{if}\ b\ \mathbf{then}\ c_0\ \mathbf{else}\ c_1, \sigma\rangle \xrightarrow{1} \langle c_0, \sigma\rangle}$$

$$\frac{\langle c, \sigma\rangle (\xrightarrow{p_i} \gamma_i)_{i\in I}}{\langle c\ \mathbf{or}\ c', \sigma\rangle (\xrightarrow{p_i} \gamma_i)_{i\in I}} \qquad \frac{\langle c', \sigma\rangle (\xrightarrow{p_j} \gamma_j)_{j\in J}}{\langle c\ \mathbf{or}\ c', \sigma\rangle (\xrightarrow{p_j} \gamma_j)_{j\in J}}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{false}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \xrightarrow{1} \sigma} \qquad \frac{\langle b, \sigma\rangle \to \mathbf{true}}{\langle \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle \xrightarrow{1} \langle c; \mathbf{while}\ b\ \mathbf{do}\ c, \sigma\rangle}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{false}}{\langle \mathbf{while}_i\ b\ \mathbf{do}\ c, \sigma\rangle \xrightarrow{1} \sigma} \qquad \frac{\langle b, \sigma\rangle \to \mathbf{true}}{\langle \mathbf{while}_{i+1}\ b\ \mathbf{do}\ c, \sigma\rangle \xrightarrow{1} \langle c; \mathbf{while}_i\ b\ \mathbf{do}\ c, \sigma\rangle}$$

Table 1: Operational semantics

$$
\begin{array}{rcl}
\mathcal{F}[\![\mathbf{skip}]\!]\sigma & = & \{(\sigma, 1)\} \\
\mathcal{F}[\![c_0 \ \mathbf{or} \ c_1]\!]\sigma & = & \mathcal{F}[\![c_1]\!]\sigma \cup \mathcal{F}[\![c_0]\!]\sigma \\
\mathcal{F}[\![X := a]\!]\sigma & = & \{(\sigma[n/X], 1)\} \ \text{where } n = [\![a]\!]\sigma \\
\mathcal{F}[\![\mathbf{if} \ b \ \mathbf{then} \ c_0 \ \mathbf{else} \ c_1]\!]\sigma & = & \left\{ \begin{array}{ll} \mathcal{F}[\![c_0]\!](\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{true} \\ \mathcal{F}[\![c_1]\!](\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{false} \end{array} \right. \\
\mathcal{F}[\![X := \chi]\!]\sigma & = & \{(\sigma[n/X], \chi(n))_{n \in Supp(\chi)}\} \\
\mathcal{F}[\![c_0; c_1]\!] & = & (\mathcal{F}[\![c_1]\!])^\dagger \circ \mathcal{F}[\![c_0]\!] \\
\mathcal{F}[\![\mathbf{while}_0 \ b \ \mathbf{do} \ c]\!]\sigma & = & \left\{ \begin{array}{ll} \{(\sigma, 1)\} & \text{if } [\![b]\!]\sigma = \mathbf{false} \\ \{\underline{0}\} & \text{if } [\![b]\!]\sigma = \mathbf{true} \end{array} \right. \\
\mathcal{F}[\![\mathbf{while}_{i+1} \ b \ \mathbf{do} \ c]\!]\sigma & = & \left\{ \begin{array}{ll} \{(\sigma, 1)\} & \text{if } [\![b]\!]\sigma = \mathbf{false} \\ \mathcal{F}[\![c; \mathbf{while}_i \ b \ \mathbf{do} \ c]\!](\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{true} \end{array} \right.
\end{array}
$$

Table 2: Denotational semantics for the finite fragment

$$
\begin{array}{rcl}
[\![\mathbf{skip}]\!] & = & \eta \\
[\![X := a]\!]\sigma & = & \eta(\sigma[n/X]) \ \text{ where } n = [\![a]\!]\sigma \\
[\![c_0 \ \mathbf{or} \ c_1]\!]\sigma & = & [\![c_1]\!]\sigma \cup [\![c_0]\!]\sigma \\
[\![X := \chi]\!]\sigma & = & \iota\big(\{(\sigma[n/X], \chi(n))_{n \in Supp(\chi)}\}\big) \\
[\![c_0; c_1]\!] & = & [\![c_1]\!]^\dagger \circ [\![c_0]\!] \\
[\![\mathbf{if} \ b \ \mathbf{then} \ c_0 \ \mathbf{else} \ c_1]\!]\sigma & = & \left\{ \begin{array}{ll} [\![c_0]\!](\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{true} \\ [\![c_1]\!](\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{false} \end{array} \right. \\
[\![\mathbf{while}_0 \ b \ \mathbf{do} \ c]\!]\sigma & = & \left\{ \begin{array}{ll} \eta(\sigma)\} & \text{if } [\![b]\!]\sigma = \mathbf{false} \\ \underline{0} & \text{if } [\![b]\!]\sigma = \mathbf{true} \end{array} \right. \\
[\![\mathbf{while}_{i+1} \ b \ \mathbf{do} \ c]\!]\sigma & = & \left\{ \begin{array}{ll} \eta(\sigma)\} & \text{if } [\![b]\!]\sigma = \mathbf{false} \\ [\![c; \mathbf{while}_i \ b \ \mathbf{do} \ c]\!](\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{true} \end{array} \right. \\
[\![\mathbf{while} \ b \ \mathbf{do} \ c]\!] & = & \mathbf{Fix}(\Phi) \\
\text{where} \quad \Phi(f)(\sigma) & = & \left\{ \begin{array}{ll} \eta(\sigma) & \text{if } [\![b]\!]\sigma = \mathbf{false} \ , \\ (f^\dagger \circ [\![c]\!])\sigma & \text{if } [\![b]\!]\sigma = \mathbf{true} \ . \end{array} \right.
\end{array}
$$

Table 3: Denotational semantics

$$iv(\mathcal{S}, c, \sigma) := (l(s), \Pi(s))_{s \in \mathcal{B}(c,\sigma,\mathcal{S})} .$$

This definition is in accordance with the intuitive interpretation of indexed valuations: here the indexes are the paths, and the indexing function is assigning to every path its final state.

6.3 Denotational semantics for the finite fragment

We now give a denotational semantics in terms of indexed valuations. This semantics is adequate with respect to deterministic schedulers: an indexed valuation is in the denotation of a configuration if there is a deterministic scheduler which realizes it.

For the finite fragment of the language we can work in the category $\mathbf{SET}$. The language $\mathbf{L}^-$ has the same syntax as $\mathbf{L}$ except that it does not include the constructor $\mathbf{while}\ b\ \mathbf{do}\ c$. The operational semantics of $\mathbf{L}^-$ is defined as for $\mathbf{L}$.

The denotational semantics

$$\mathcal{F}[\![c]\!] : \Sigma \to P(IV(\Sigma))$$

is defined in table 2. The IDV $(\sigma, p)_{*\in\{*\}}$ is denoted as (σ, p). Recall that the Kleisli extension for the monad $P \circ IV$ is denoted by $(-)^\dagger$. Its definition can be found in section 2.2.

Theorem 6.5 (Adequacy). *Let c be a command of $\mathbf{L}^-$ and ν be an indexed finite valuation in $IV(\Sigma)$. Then $\nu \in \mathcal{F}[\![c]\!]\sigma$ if and only if there exists a deterministic scheduler $\mathcal{S}$ for $\mathcal{T}(\langle c, \sigma\rangle)$ s.t. $\nu \sim iv(\mathcal{S}, c, \sigma)$.*

Proof: by well founded induction, the ordering being as follows. Let $maxt(c)$ be the maximum tag in a while command occurring in c (0 if there are no while commands). We say that $c_0 \preceq c_1$ if (1) $maxt(c_0) < maxt(c_1)$ or if (2) $maxt(c_0) = maxt(c_1)$ and c_0 is a subterm of c_1.

The nontrivial case is the sequential composition. Take a scheduler $\mathcal{S}$ for $\langle c_0; c_1, \sigma\rangle$. Such an $\mathcal{S}$ can be thought of as a scheduler $\mathcal{S}_0$ for $\langle c_0, \sigma\rangle$ together with schedulers $\mathcal{S}_u$ for $\langle c_1, l(u)\rangle$ for every finite $u \in \mathcal{B}(\langle c_0, \sigma\rangle, \mathcal{S}_0)$. (In the sequel we write $\mathcal{B}(c_0, \sigma, \mathcal{S})$ for $\mathcal{B}(\langle c_0, \sigma\rangle, \mathcal{S})$).

By induction hypothesis $(l(u), \Pi(u))_{u\in\mathcal{B}(c_0,\sigma,\mathcal{S}_0)} \in [\![c_0]\!]\sigma$ and for every u, $(l(t), \Pi(t))_{t\in\mathcal{B}(c_1,l(u),\mathcal{S}_u)} \in [\![c_1]\!]l(u)$. We have to show that

$$(l(s), \Pi(s))_{s\in\mathcal{B}(c_0;c_1,\sigma,\mathcal{S})} \in [\![c_1]\!]^\dagger([\![c_0]\!]\sigma) .$$

Recalling the definition of $f^\dagger$, it is enough to show that

$$(l(s), \Pi(s))_{s \in \mathcal{B}(c_0; c_1, \sigma, \mathcal{S})} \in [\![c_1]\!]^\dagger \left(\{ (l(u), \Pi(u))_{u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0)} \} \right) .$$

Let us define $h : \mathcal{B}(c_0, \sigma, \mathcal{S}_0) \to IV(\Sigma)$ as

$$h(u) = (l(t), \Pi(t))_{t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)} \in [\![c_1]\!] l(u) .$$

Therefore by definition of $f^\dagger$:

$$(l(t), \Pi(u)\Pi(t))_{\substack{u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0) \\ t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)}} \in [\![c_1]\!]^\dagger([\![c_0]\!]\sigma) .$$

Notice that a path $s \in \mathcal{B}(c_0; c_1, \sigma, \mathcal{S})$ is the concatenation of a path $u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0)$ together with a path $t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)$. Thus

$$(l(t), \Pi(u)\Pi(t))_{\substack{u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0) \\ t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)}} =$$

$$= (l(s), \Pi(s))_{s \in \mathcal{B}(c_0; c_1, \sigma, \mathcal{S})} .$$

Viceversa suppose $(\sigma_i, p_i)_{i \in I} \in [\![c_1]\!]^\dagger([\![c_0]\!]\sigma)$. Then there is $(\sigma_j, q_j)_{j \in J} \in [\![c_0]\!]\sigma$ and $h : J \to IV(\Sigma)$, say $h(j) = (\sigma^j_{k_j}, r^j_{k_j})_{k_j \in K_j}$ such that

$$h(j) \in [\![c_1]\!]\sigma_j$$

$$(\sigma_i, p_i)_{i \in I} = (\sigma^j_{k_j}, q_j r^j_{k_j})_{\substack{j \in J \\ k_j \in K_j}} .$$

By induction hypothesis there are $\mathcal{S}_0, \mathcal{S}_j$ such that

$$(\sigma_j, q_j)_{j \in J} = (l(u), \Pi(u))_{u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0)}$$

$$(\sigma^j_{k_j}, r^j_{k_j})_{k_j \in K_j} = (l(t), \Pi(t))_{t \in \mathcal{B}(c_1, \sigma_j, \mathcal{S}_j)}$$

The first equation tells us that $J = \mathcal{B}(c_0, \sigma, \mathcal{S}_0)$, $\sigma_j = l(u)$ and $q_j = \Pi(u)$. The second equation tells us that $K_u = \mathcal{B}(c_1, l(u), \mathcal{S}_u)$ and $r^j_{k_j} = \Pi(t)$. This enables us to rewrite the second as

$$(\sigma^j_{k_j}, r^j_{k_j})_{k_j \in K_j} = (l(t), \Pi(t))_{t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)}$$

So

$$(\sigma^j_{k_j}, q_j r^j_{k_j})_{\substack{j \in J \\ k_j \in K_j}} = (l(t), \Pi(u)\Pi(t))_{\substack{u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0) \\ t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)}} .$$

As above, combining the schedulers we get a scheduler $\mathcal{S}$ such that

$$iv(\mathcal{S}, c_0; c_1, \sigma) = (\sigma_i, p_i)_{i \in I} .$$

□

6.4 Denotational semantics for the full language

For the full language we work in $\mathbf{CONT}$. We give a denotational semantics to $\mathbf{L}$ in terms of $\mathcal{P}(\mathcal{IV}(\Sigma))$. Given a command of $\mathbf{L}$, we define its denotation

$$[\![c]\!] : \Sigma \to \mathcal{P}(\mathcal{IV}(\Sigma)) \ .$$

The definition is shown in table 3. Recall the behaviour of $\eta : \Sigma \to \mathcal{P}(\mathcal{IV}(\Sigma))$:

$$\eta(\sigma) = \{(\sigma, 1)\} \downarrow \ .$$

Again the symbol $(-)^\dagger$ denotes the Kleisli extension for the monad $\mathcal{P} \circ \mathcal{IV}$.

The adequacy theorem for the full language suffers the usual limitations due to the structure of the Hoare powerdomain, which involves only Scott closed sets.

Theorem 6.6. *Let c be a command of $\mathbf{L}$ and let $\nu \in \mathcal{IV}(\Sigma)$. Then $\nu \in [\![c]\!]\sigma$ iff for every ξ such that $\xi \ll \nu$ there exists a scheduler $\mathcal{S}$ for (c, σ) s.t. $iv(\mathcal{S}, c, \sigma) \sqsupseteq \xi$.*

We need some preliminary lemmas.

Observation 6.7. *Let c be a command of $\mathbf{L}^-$. Then $[\![c]\!]\sigma = \iota(\mathcal{F}[\![c]\!]\sigma)$.*

Proof: By structural induction. Notice that the definitions for $[\![c]\!]$ and $\mathcal{F}[\![c]\!]$ go in parallel with each other.

Proposition 6.8. *Let c be a command of $\mathbf{L}^-$. Then $\nu \in [\![c]\!]\sigma$ iff there exists $\nu' \in \mathcal{F}[\![c]\!]\sigma$ s.t. $\nu \sqsubseteq \iota(\nu')$.*

Proof: By theorem 6.5 and the characterization of Hoare powerdomain. □

Definition 6.9. Let c be a command of $\mathbf{L}$. Then $c^{(i)}$ is the command we obtain by substituting in c all the occurrences of $\mathbf{while}\ b\ \mathbf{do}\ c'$ with $\mathbf{while}_i\ b\ \mathbf{do}\ c'$.

Clearly $c^{(i)}$ is a command of $\mathbf{L}^-$, for every i. Therefore we have:

Proposition 6.10. *Let c be a command of $\mathbf{L}$ and ν be a finite indexed valuation $\in IV(\Sigma)$. For every i we have:*
$\iota(\nu) \in [\![c^{(i)}]\!]\sigma$ iff there exists a scheduler $\mathcal{S}$ for (c, σ) s.t. $iv(\mathcal{S}, c, \sigma) \sqsupseteq \nu$.

Proof: Clearly a scheduler $\mathcal{S}$ for (c, σ) restricts to a scheduler $\mathcal{S}_i$ for $(c^{(i)}, \sigma)$ and $v(\mathcal{S}, c, \sigma) \sqsupseteq v(\mathcal{S}_i, c^{(i)}, \sigma)$. On the contrary a scheduler $\mathcal{S}_i$ for $(c^{(i)}, \sigma)$ can be extended (possibly in many different ways) to a scheduler $\mathcal{S}$ for (c, σ), with the same inequality as above. This together with Proposition 6.8 and Theorem 6.5, gives us the statement. □

Proposition 6.11. *For every c, σ*

$$\sup_{i \in \mathcal{N}} [\![c^{(i)}]\!]\sigma = [\![c]\!]\sigma \ .$$

Proof: By structural induction, using the continuity of the operators defining the semantics. □

Coming to the proof of Theorem 6.6, we show the "only if" direction. For $\nu \in [\![c]\!]\sigma$ there are two cases.

1. There is $\nu' \in \mathcal{F}[\![c^{(i)}]\!]\sigma$ for some i, such that $\nu \sqsubseteq \iota(\nu')$. Then we invoke the Proposition 6.10, and we are done.

2. There is a net $\nu_{j_i} \in [\![c^{(i)}]\!]\sigma$ converging to ν. By Proposition 6.8 it is not restricting to assume that $\nu_{j_i} = \iota(\tilde{\nu}_{j_i})$ for some $\tilde{\nu}_{j_i} \in \mathcal{F}[\![c^{(i)}]\!]\sigma$. Then we have a net of schedulers $\mathcal{S}_{j_i}$ such that $\tilde{\nu}_{j_i} = iv(\mathcal{S}_{j_i}, c^{(i)}, \sigma)$.

   Now if $\xi \ll \nu$ there is a k_h such that $(iv(\mathcal{S}_{k_h}, c^{(h)}, \sigma)) \sqsupseteq \xi$. Now we can extend $\mathcal{S}_{k_h}$ to an $\mathcal{S}$ for (c, σ) with $(iv(\mathcal{S}, c, \sigma)) \sqsupseteq \xi$.

For the "if" direction, suppose that for every $\xi \ll \nu$ there exists a scheduler $\mathcal{S}_\xi$ with $iv(\mathcal{S}, c, \sigma) \sqsupseteq \xi$. This is in fact equivalent to saying that for every $\xi \ll \nu$ there exists a scheduler $\mathcal{S}_\xi$ with $iv(\mathcal{S}, c, \sigma) \gg \xi$. Therefore, for big enough i, $(iv(\mathcal{S}^i_\xi, c^{(i)}, \sigma)) \sqsupseteq \xi$ (where $\mathcal{S}^i_\xi$ is the truncation of $\mathcal{S}_\xi$ to $\mathcal{T}(\langle c^{(i)}, \sigma \rangle)$.

If for one of such $\mathcal{S}^i_\xi$, we have $iv(\mathcal{S}^i_\xi, c^{(i)}, \sigma) \sqsupseteq \nu$, then ν is in the denotation, by proposition 6.8. Otherwise notice that the all $iv(\mathcal{S}^i_\xi, c^{(i)}, \sigma)$ are in $[\![c]\!]\sigma$, then all the ξ are in the denotation. By Scott closure, ν, which is the directed lub of the ξ, must be in the denotation. □

We cannot hope that there always exists a scheduler which attains the limit valuation as the following example shows.

Let χ be such that $\chi(0) = \chi(1) = 1/2$. Assume $a \neq 0$. Define

$$\mathbf{loop} \equiv \mathbf{while\ true\ do\ skip}\ ;$$

$$c \equiv Y := 0; Z := 0; \mathbf{while}\ Z = 0\ \mathbf{do}\ c_0\ ;$$

$$c_0 \equiv (c_1; \mathbf{if}\ X \leq Y\ \mathbf{then}\ Z := a\ \mathbf{else\ loop})\ \mathbf{or}\ (Y := Y + 1)\ ;$$

$$c_1 \equiv (W := 0; \mathbf{while}\ W = 0\ \mathbf{do}\ (W := \chi; X := X + 1)\ .$$

Here there is no scheduler $\mathcal{S}$ which assigns probability 1 to a state where $Z = a$, but we can get as close to this as we want.

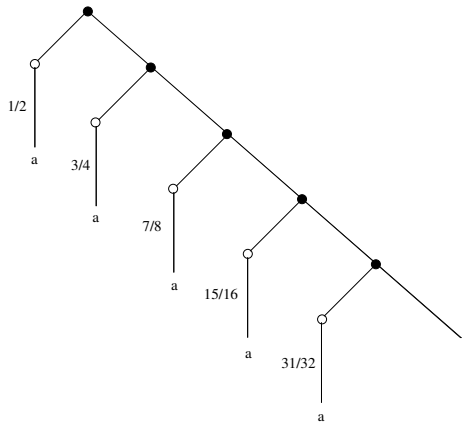


Figure 2: A counterexample

6.5 Denotational semantics using Tix-Mislove

The main feature of our theorems is that they involve deterministic schedulers. A semantics in terms of the Mislove-Tix functor is adequate with respect to probabilistic schedulers.

Theorem 6.12 (Adequacy). *Let c be a command of $\mathbf{L}^-$ and ν be an discrete valuation in $V(\Sigma)$. Then $\nu \in \mathcal{F}[\![c]\!]\sigma$ if and only if there exists a probabilistic scheduler $\mathcal{S}$ for $\mathcal{T}(\langle c, \sigma\rangle)$ s.t. $\nu = v(\mathcal{S}, c, \sigma)$*

Proof: by well founded induction. Again the nontrivial case is the sequential composition. Take a scheduler $\mathcal{S}$ for $\langle c_0; c_1, \sigma\rangle$. Such an $\mathcal{S}$ can be thought of as a scheduler $\mathcal{S}_0$ for $\langle c_0, \sigma\rangle$ together with schedulers $\mathcal{S}_u$ for $\langle c_1, l(u)\rangle$ for every finite $u \in \mathcal{B}(\langle c_0, \sigma\rangle, \mathcal{S}_0)$.

By induction hypothesis $v(\mathcal{S}_0, c_0, \sigma) \in [\![c_0]\!]\sigma$ and for every u, $v(\mathcal{S}_u, c_1, l(u)) \in [\![c_1]\!]l(u)$.

We have to show that

$$\lambda\sigma' \sum_{\substack{l(s)=\sigma' \\ s\in\mathcal{B}(c_0;c_1,\sigma,\mathcal{S})}} \Pi(s) \in [\![c_1]\!]^\dagger([\![c_0]\!]\sigma) \ .$$

Recalling the definition of $f^\dagger$, it is enough to show that

$$\lambda\sigma' \sum_{\substack{l(s)=\sigma' \\ s\in\mathcal{B}(c_0;c_1,\sigma,\mathcal{S})}} \Pi(s) \in [\![c_1]\!]^\dagger \left(\{ \, v(\mathcal{S}_0, c_0, \sigma) \, \} \right) \ .$$

Let us define $h : \Sigma \to V(\Sigma)$ as

$$h(\sigma'') = \sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \frac{\Pi(u)}{v(\mathcal{S}_0, c_0, \sigma)(\sigma'')} v(\mathcal{S}_u, c_1, \sigma'') \ .$$

Remember that, by definition:

$$\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \Pi(u) = v(\mathcal{S}_0, c_0, \sigma)(\sigma'') \ .$$

Therefore

$$\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \frac{\Pi(u)}{v(\mathcal{S}_0, c_0, \sigma)(\sigma'')} = 1$$

Since $[\![c_1]\!]\sigma''$ is convex, then $h(\sigma'') \in ([\![c_1]\!]\sigma'')$. Therefore by proposition 3.11:

$$\sum_{\sigma'' \in \Sigma} v(\mathcal{S}_0, c_0, \sigma)(\sigma'') h(\sigma'') \in [\![c_1]\!]^\dagger \left(\{ \, v(\mathcal{S}_0, c_0, \sigma) \, \} \right) \ .$$

But

$$\sum_{\sigma'' \in \Sigma} v(\mathcal{S}_0, c_0, \sigma)(\sigma'') h(\sigma'')(\sigma')$$

$$= \sum_{\sigma'' \in \Sigma} \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \Pi(u) \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \frac{\Pi(u)}{v(\mathcal{S}_0, c_0, \sigma)(\sigma'')} v(\mathcal{S}_u, c_1, \sigma'')(\sigma') \right) \right)$$

$$= \sum_{\sigma'' \in \Sigma} \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \frac{\Pi(u)}{v(\mathcal{S}_0, c_0, \sigma)(\sigma'')} \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \Pi(u) v(\mathcal{S}_u, c_1, \sigma'')(\sigma') \right) \right)$$

$$= \sum_{\sigma'' \in \Sigma} \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \frac{\Pi(u)}{v(\mathcal{S}_0, c_0, \sigma)(\sigma'')} \right) \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \Pi(u) v(\mathcal{S}_u, c_1, \sigma'')(\sigma') \right)$$

$$= \sum_{\sigma'' \in \Sigma} \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \Pi(u) v(\mathcal{S}_u, c_1, \sigma'')(\sigma') \right)$$

$$= \sum_{\sigma'' \in \Sigma} \left(\sum_{\substack{l(u)=\sigma'' \\ u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)}} \Pi(u) \left(\sum_{\substack{l(t)=\sigma' \\ t \in \mathcal{B}(c_1,\sigma'',\mathcal{S}_u)}} \Pi(t) \right) \right)$$

$$= \sum_{u \in \mathcal{B}(c_0,\sigma,\mathcal{S}_0)} \Pi(u) \left(\sum_{\substack{l(t)=\sigma' \\ t \in \mathcal{B}(c_1,l(u),\mathcal{S}_u)}} \Pi(t) \right)$$

$$= \sum_{\substack{l(s)=\sigma' \\ s \in \mathcal{B}(c_0;c_1,\sigma,\mathcal{S})}} \Pi(s) \ ,$$

and the thesis is proved. For the last step, notice that a path $s \in \mathcal{B}(c_0; c_1, \sigma, \mathcal{S})$ is the concatenation of a path $u \in \mathcal{B}(c_0, \sigma, \mathcal{S}_0)$ together with a path $t \in \mathcal{B}(c_1, l(u), \mathcal{S}_u)$.

Viceversa suppose that $\nu \in [\![c_1]\!]^\dagger([\![c_0]\!]\sigma)$. Then there exist $\xi \in [\![c_0]\!]\sigma$ and $h : \Sigma \to V(\Sigma)$ such that $h(\sigma'') \in [\![c_1]\!]\sigma''$ and $\nu = \sum_{\sigma''} \xi(\sigma'')h(\sigma'')$. By induction hypothesis the exist schedulers $\mathcal{S}_0$, $\mathcal{S}_{\sigma''}$ such that $\xi = v(\mathcal{S}_0, c_0, \sigma)$, and $h(\sigma'') = v(\mathcal{S}_{\sigma''}, c_1, \sigma'')$. Similar to what we did with deterministic scheduler we combine them to get a scheduler $\mathcal{S}$ such that $\nu = v(\mathcal{S}, c_0; c_1, \sigma)$. Notice that in this case the combined scheduler has some memoryless character: it behaves the same for every subtree rooted in a node labeled by a configuration $\langle c_1, \sigma'' \rangle$, regardless of the previous history.

□

We can interpret the semantics in table 3 as being of the form

$$[\![c]\!] : \Sigma \to \mathcal{P}_{TM}(\mathcal{V}(\Sigma)) \ .$$

The adequacy result is similar to the previous one, but it speaks of probabilistic schedulers.

Theorem 6.13. *Let c be a command of* **L** *and let $\zeta \in \mathcal{V}(\Sigma)$. Then $\zeta \in [\![c]\!]\sigma$ iff for every $\epsilon > 0$ there exists a probabilistic scheduler $\mathcal{S}$ for (c, σ) s.t. $v(\mathcal{S}, c, \sigma) \sqsupseteq (1 - \epsilon)\zeta$.*

7 Future Work

We have shown that a distributive law exists between the Hoare powerdomain and the Indexed Valuations. The question arises whether similar results hold for the Plotkin and the Smyth powerdomain. We believe that each nondeterministic powerdomain has its corresponding Indexed Valuation functor. The key is the axiom (HV). If we omit it we get a theory whose free domain-algebra distributes over the Plotkin powerdomain. If we replace it with

$$pA \oplus qA \sqsubseteq (p+q)A \quad (SV)$$

we get a theory whose free domain-algebras distribute over the Smyth powerdomain. These ideas have to be studied and a computational meaning has to be found for them.

It would be also interesting to find a concrete characterization of Indexed Valuations. In the category of sets they are but finite random variables. It seems promising to generalize this setting to random variables on suitable measure spaces.

Acknowledgments

Glynn Winskel contributed with essential suggestions to this work. In particular he had the idea of using indexes, while I was still using the more awkward multisets. Special thanks to Achim Jung for the very useful conversations during my visit to Birmingham. In particular he convinced me that the distributive law in the category of domains could be defined via the bases, without the need for a concrete representation. Thanks to Andrzej Filinski who showed me how the nondeterministic and probabilistic monads are combined in ML. Thanks to Alex Berg, Michael Mislove, Gordon Plotkin, Luigi Santocanale and Zhe Yang for useful discussions.

References

[AJ94] Samson Abramsky and Achim Jung. Domain theory. In *Handbook of Logic in Computer Science*, volume 3. Oxford, 1994.

[Bec69] Jon Beck. Distributive laws. In *Seminar on Triples and Categorical Homology Theory*, pages 119–140, 1969.

[Han91] Hans Hansson. *Time and Probability in Formal Design of Distributed systems*. PhD thesis, Uppsala University, 1991.

[JLY01] Bengt Jonsson, Kim Larsen, and Wang Yi. Probabilistic extensions of process algebras. In *Handbook of Process Algebras*. Elsevier, 2001.

[Jon90] Claire Jones. *Probabilistic Non-determinism*. PhD thesis, University of Edinburgh, 1990.

[Kir93] Olaf Kirch. Bereiche und Bewertungen. Master's thesis, Technische Hochschule Darmstadt, 1993.

[Mis00] Michael Mislove. Nondeterminism and probabilistic choice: Obeying the law. In *Proc. 11th CONCUR*, volume 1877 of *LNCS*, pages 350–364. Springer, 2000.

[Mog91] Eugenio Moggi. Notions of computation and monads. *Information and Computation*, 93(1):55–92, July 1991.

[Plo83] Gordon Plotkin. Domains. University of Edinburgh, 1983.

[SL95] Roberto Segala and Nancy Lynch. Probabilistic simulations for probabilistic processes. *Nordic Journal of Computing*, 2(2):250–273, 1995. An extended abstract appears in *Proc. 5th CONCUR*, Uppsala, Sweden, LNCS 836, pages 481–496, August 1994.

[Tix99] Regina Tix. *Continuous D-Cones: Convexity and Powerdomain Constructions*. PhD thesis, Technische Universität Darmstadt, 1999.

[Var85] Moshe Y. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In *Proc. 26th FOCS*, pages 327–338, 1985.

[Var01] Daniele Varacca. Issues in probabilistic semantics. Progress report, BRICS - Aarhus University, 2001.

Recent BRICS Report Series Publications

RS-02-38 Daniele Varacca. *The Powerdomain of Indexed Valuations*. September 2002. 54 pp. Short version appears in Plotkin, editor, *Seventeenth Annual IEEE Symposium on Logic in Computer Science*, LICS '02 Proceedings, 2002, pages 299–308.

RS-02-37 Mads Sig Ager, Olivier Danvy, and Mayer Goldberg. *A Symmetric Approach to Compilation and Decompilation*. August 2002. To appear in Neil Jones's Festschrift.

RS-02-36 Daniel Damian and Olivier Danvy. *CPS Transformation of Flow Information, Part II: Administrative Reductions*. August 2002. 9 pp. To appear in the *Journal of Functional Programming*. This report supersedes the earlier BRICS report RS-01-40.

RS-02-35 Patricia Bouyer. *Timed Automata May Cause Some Troubles*. August 2002. 44 pp.

RS-02-34 Morten Rhiger. *A Foundation for Embedded Languages*. August 2002. 29 pp.

RS-02-33 Vincent Balat and Olivier Danvy. *Memoization in Type-Directed Partial Evaluation*. July 2002. 18 pp. To appear in Batory and Consel, editors, *ACM SIGPLAN/SIGSOFT Conference on Generative Programming and Component Engineering*, GPCE '02 Proceedings, LNCS, 2002.

RS-02-32 Mads Sig Ager, Olivier Danvy, and Henning Korsholm Rohde. *On Obtaining Knuth, Morris, and Pratt's String Matcher by Partial Evaluation*. July 2002. 43 pp. To appear in Chin, editor, *ACM SIGPLAN ASIAN Symposium on Partial Evaluation and Semantics-Based Program Manipulation*, ASIA-PEPM '02 Proceedings, 2002.

RS-02-31 Ulrich Kohlenbach and Paulo B. Oliva. *Proof Mining: A Systematic Way of Analysing Proofs in Mathematics*. June 2002. 47 pp.

RS-02-30 Olivier Danvy and Ulrik P. Schultz. *Lambda-Lifting in Quadratic Time*. June 2002.

RS-02-29 Christian N. S. Pedersen and Tejs Scharling. *Comparative Methods for Gene Structure Prediction in Homologous Sequences*. June 2002. 20 pp.